HP Operations Smart Plug-in for Tuxedo

For HP Operations for UNIX (HPO) 9.0

Software Version: 5.00

User Guide

Document Release Date: November 2009
Software Release Date: November 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel486 is a U.S. trademark of Intel Corporation.

Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation.

OpenView® is a registered U.S. trademark of Hewlett-Packard Company.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle Reports, Oracle7, and Oracle7 Server are trademarks of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation in the U.S. and other countries.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Chapter:Architecture and Tuxedo SPI Components

The Smart Plug-In for Tuxedo is a preconfigured add-on module for the HP Operations (HPO) software. The Tuxedo SPI extends the OVO management environment to include Tuxedo systems and Tuxedo applications.

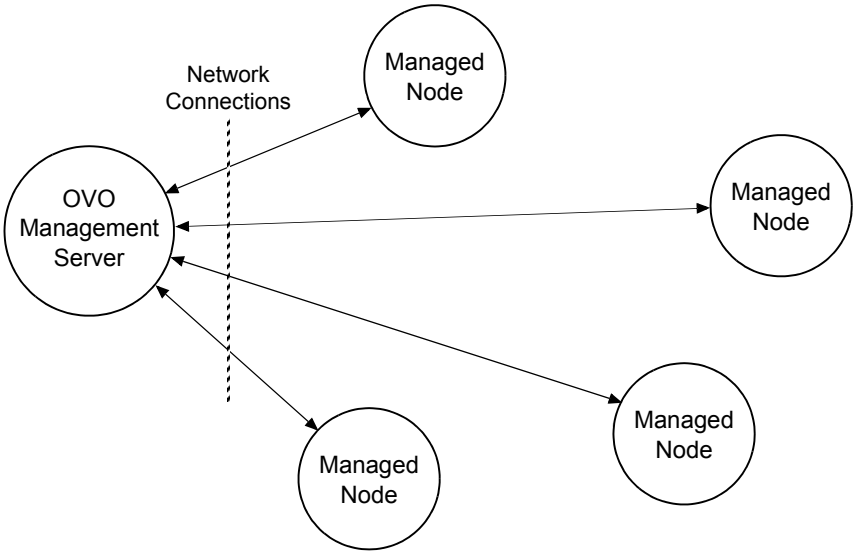
This chapter describes the architecture of HPO, Tuxedo, and the Tuxedo SPI.

HP OpenView IT/Operations (ITO) and HP OpenView VantagePoint Operations (VPO) have been renamed to HP Operations (HPO) for UNIX®. The name change has not yet been fully implemented across the HPO software and documentation. As a result, you may encounter references to all product names.

HP HPO Architecture

As shown in the following figure, the HPO architecture is based on communication between a management server and one or more managed nodes. The managed nodes are the computer machines monitored and controlled by HPO.

Figure 1 Simplified View of HP Operations Architecture



HPO server processes running on the central management server machine communicate with HPO agent processes running on the managed nodes. The HPO agent processes collect *events*—status changes or threshold violations—on the managed nodes and then forward relevant information in the form of HPO messages to the management server. The management server responds with actions to prevent or correct problems on the managed nodes.

Management Server

The HPO management server is the controlling element of the entire HPO system. It holds the HPO database and the HPO software, including the complete current configuration and the HPO agent software. During the installation of an HPO system, the HPO administrator downloads copies of the HPO agent software to the managed nodes.

HPO provides a graphical user interface (GUI) through which HPO administrators and operators can monitor and control the HPO software, the managed applications, and the hardware on which the applications run. A management server can support multiple HPO GUIs per server machine.

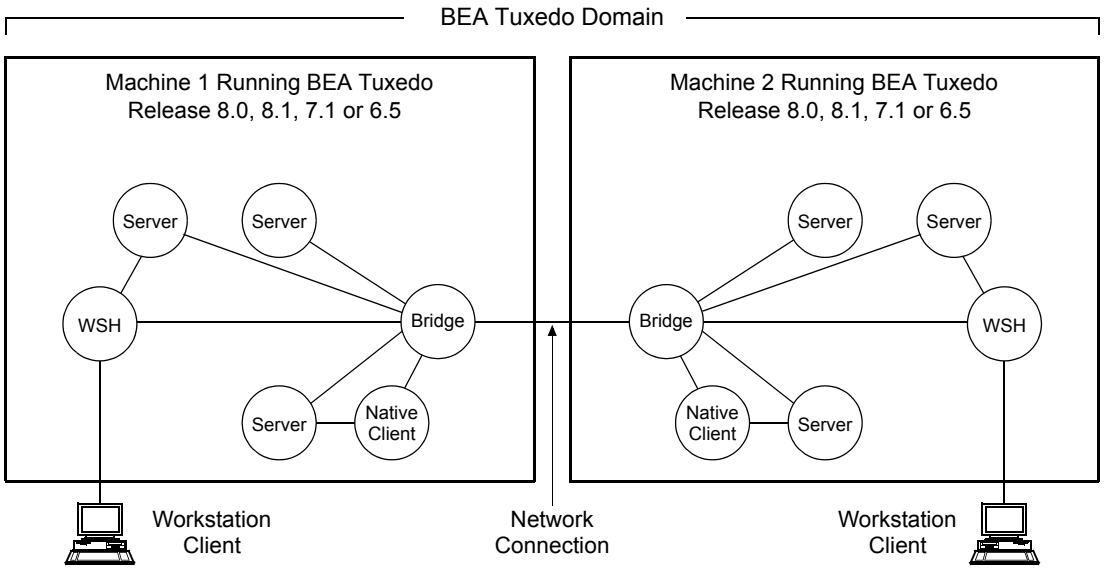
Managed Nodes

Once installed and running, the HPO agent software reads log files, console messages, and Simple Network Management Protocol (SNMP) traps—significant but unsolicited events. If so configured, the HPO message interceptor can intercept messages from any application running locally on a managed node.

BEA Tuxedo System Architecture

The following figure shows a Tuxedo domain, which is the basis of the Tuxedo system architecture.

Figure 2 Simplified View of BEA Tuxedo System Architecture



A Tuxedo domain, also known as a Tuxedo application, is a business software program, built upon the Tuxedo system, that is defined and controlled by a single configuration file—the UBBCONFIG file. A Tuxedo domain consists of one or more clients (local or remote), one or more servers, and one or more machines. It is administered as a single unit.

Tuxedo UBBCONFIG File

Each Tuxedo domain is controlled by a configuration file in which installation-dependent parameters are defined. The text version of the configuration file is referred to as `UBBCONFIG`, although the configuration file may have any name, as long as the content of the file conforms to the format described on the UBBCONFIG(5) reference page in Tuxedo File Formats and

Data Descriptions Reference. Typical configuration filenames begin with the string ubb, followed by a mnemonic string, such as simple in the filename ubbsimple.

Tuxedo Master Machine

The master machine, or master node, for a Tuxedo domain contains the domain's `UBBCONFIG` file, and is designated as the master machine in the `RESOURCES` section of the `UBBCONFIG` file. Starting, stopping, and administering a Tuxedo domain is done through the master machine.

In a multi-machine Tuxedo domain running different releases of the Tuxedo system software, the master machine must run the highest release of the Tuxedo system software in the domain.

Tuxedo Domain ID

The Domain ID for a Tuxedo domain is designated in the RESOURCES section of the UBBCONFIG file. It specifies the name of the Tuxedo domain.

Tuxedo Logical Machine ID

The logical machine ID (LMID) is designated in the MACHINES section of the UBBCONFIG file. There is an LMID entry for each machine in a Tuxedo domain.

Tuxedo TUXCONFIG File

The TUXCONFIG file is a binary version of the UBBCONFIG file. It is created by running the tmloadcf(1) command, which parses UBBCONFIG and loads the binary TUXCONFIG file to the location referenced by the TUXCONFIG environment variable. As with UBBCONFIG, the TUXCONFIG file may be given any name.

The master machine for a Tuxedo domain contains the master copy of the TUXCONFIG file. Copies of the TUXCONFIG file are propagated to every other machine in a Tuxedo domain—referred to as non-master machines—whenever the Tuxedo system is booted on the master machine.

Tuxedo TUXCONFIG Environment Variable

The TUXCONFIG environment variable defines the location on the master machine where the tmloadcf(1) command loads the binary TUXCONFIG file. It must be set to an absolute pathname ending with the device or system file where TUXCONFIG is to be loaded.

The TUXCONFIG pathname value is designated in the MACHINES section of the UBBCONFIG file. It is specified for the master machine and for every other machine in the Tuxedo domain. When copies of the binary TUXCONFIG file are propagated to non-master machines during system boot, the copies are stored on the non-master machines in accordance to the TUXCONFIG pathname values.

Tuxedo TUXDIR Environment Variable

The TUXDIR environment variable defines the installation directory of the BEA Tuxedo system software on the master machine. It must be set to an absolute pathname ending with the name of the installation directory.

The TUXDIR pathname value is designated in the MACHINES section of the UBBCONFIG file. It is specified for the master machine and for every other machine in the Tuxedo domain.

Tuxedo Management Information Base

The Tuxedo Management Information Base (TMIB) is a Tuxedo system component that provides a complete definition of the classes and their attributes that formally define a Tuxedo domain. Separate classes are designated for machines, servers, networks, and so on. The TMIB reference pages (TM_MIB(5), generic reference page MIB(5), ...) are defined in BEA Tuxedo File Formats and Data Descriptions Reference.

When a Tuxedo server becomes active, it advertises the names of its services in the Bulletin Board, which is the dynamic part of the TMIB. (A service is an application routine that a client can request.) The Tuxedo system uses the binary TUXCONFIG file on the master machine to construct the Bulletin Board, and propagates a copy of the TUXCONFIG to the non-master machines in the domain to set up the Bulletin Board on those machines. A Bulletin Board runs on each machine in a Tuxedo domain.

Tuxedo Distinguished Bulletin Board Liaison Server

The Distinguished Bulletin Board Liaison (DBBL) is a Tuxedo system administrative server that propagates the global changes to the TMIB and maintains the static part of the TMIB. The DBBL also coordinates the state of the different machines involved in the Tuxedo domain. There is only one DBBL for the entire domain, and it runs on the machine—the master machine—where the UBBCONFIG file resides.

The Bulletin Board Liaison (BBL) is a Tuxedo system administrative server that maintains the Bulletin Board—a runtime representation of the TMIB that is replicated on every machine in the Tuxedo domain. (The Bulletin Board is the where global or local state changes to the TMIB are posted.) The BBL coordinates changes to the local copy of the TMIB and verifies the sanity of the software programs that are active on the same machine as the BBL.

Tuxedo User Log

ULOG is a Tuxedo system central event user log. A ULOG file is a text file containing Tuxedo system error messages, warning messages, debugging messages, and information messages. The Tuxedo system creates a new ULOG file each day on each machine in a Tuxedo domain.

The full pathname of a ULOG file is as follows:

- If the variable ULOGPFX is set, its value becomes the prefix for the filename.
- If ULOGPFX is not set, ULOG becomes the prefix for the filename.

Each time a Tuxedo process calls the userlog(3c) function to write a message to the ULOG, userlog() determines the date and concatenates the month, day, and year to the prefix as mmddyy to set the name for the file. The first time a process writes to the ULOG, it first writes an additional message indicating the associated BEA Tuxedo system version.

Tuxedo System Events

The Tuxedo system reports system-defined events and application-defined events. System-defined events are situations (primarily failures) defined by the Tuxedo system, such as the exceeding of certain system capacity limits, server terminations, security violations, and network failures.

Application-defined events are situations defined by customer business programs. Both system-defined and application-defined events are received and distributed by the BEA Tuxedo EventBroker component, which also provides a system-wide summary of events.

Tuxedo Runtime Administrative Command

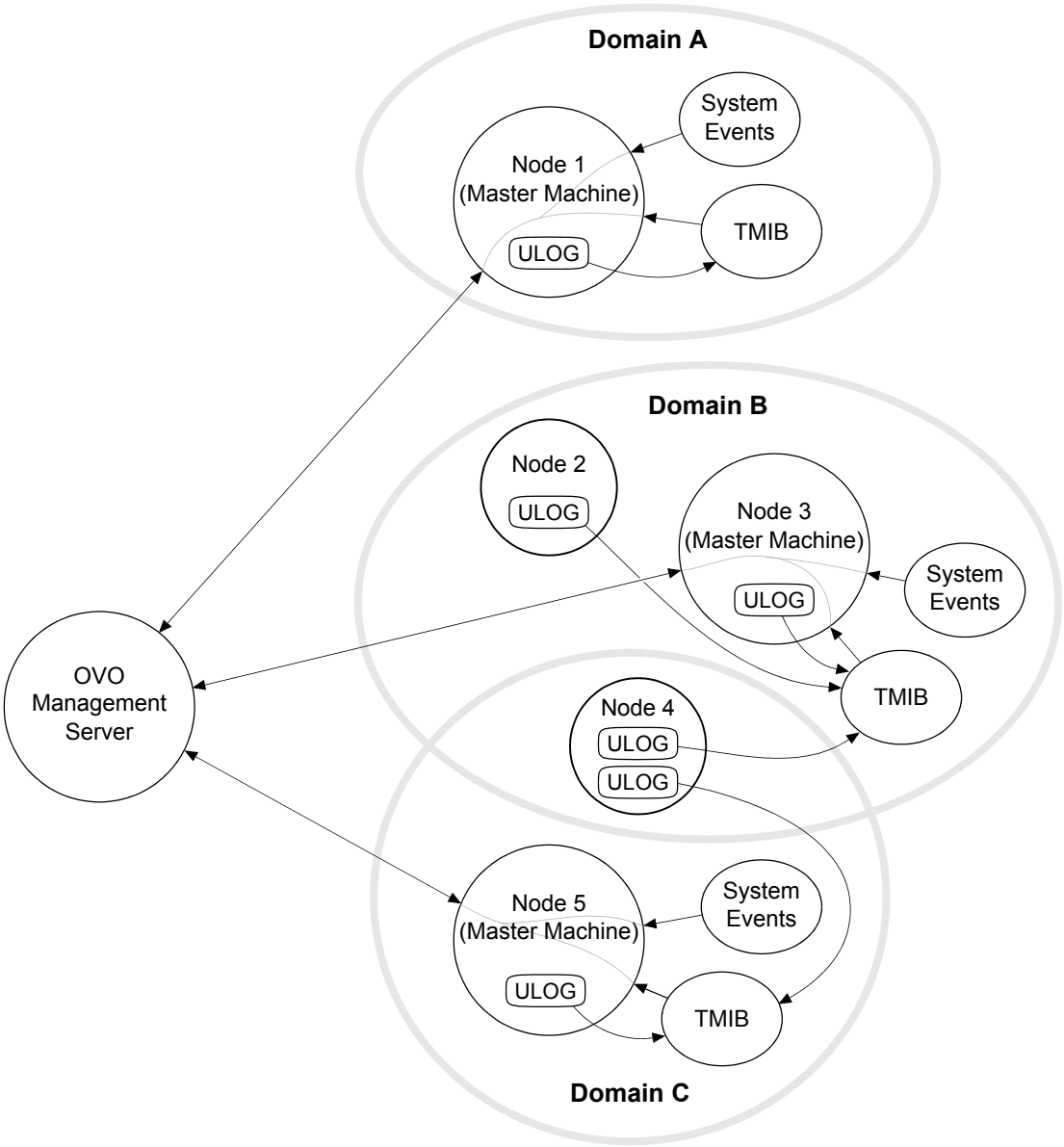
The Tuxedo bulletin board command interpreter, tmadmin(1), provides for the inspection and modification of Bulletin Boards and associated entities in a uniprocessor, multiprocessor, or network environment. Depending upon its invocation, tmadmin can join a Tuxedo domain as an administrative process or client via a running BBL.

HPO and Tuxedo SPI Architecture

The following figure shows how the Tuxedo architecture integrates with the HPO architecture. Each master machine in a managed Tuxedo domain provides the domain's ULOG messages, system events, and TMIB metrics to the management server.

Tuxedo SPI supports Tuxedo from BEA Systems/Oracle only and does not provide support for Tuxedo from other Independent Software Vendors (ISVs).

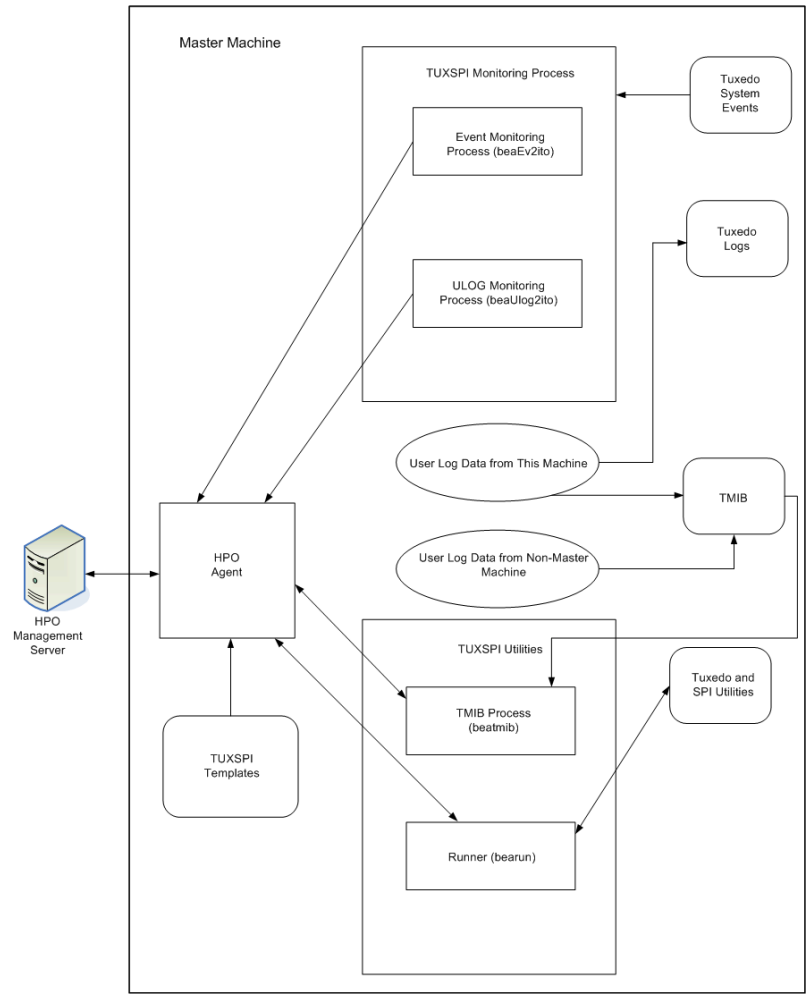
Figure 3 Simplified View of HPO and Tuxedo SPI Architecture



Managed Node Architecture

The following figure shows the relationships between agent processes, monitoring processes, and Tuxedo processes running on a Tuxedo master machine.

Figure 4 HPO and Tuxedo SPI Software on a Tuxedo Master Machine

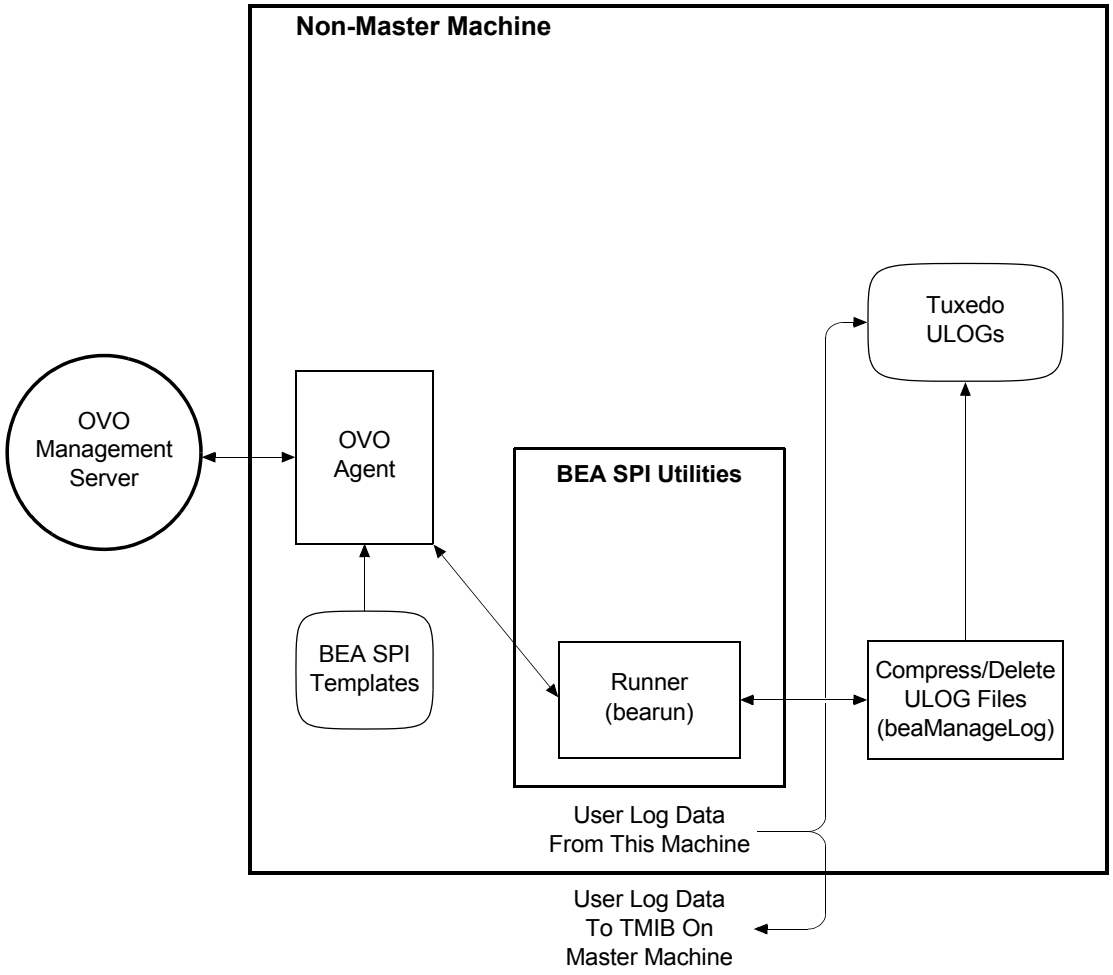


An HPO agent process runs on each managed node in an HPO system. Typically, the managed node starts the HPO agent upon system boot. The HPO agent in turn starts the platform processes needed to provide HPO services on that machine. If the HPO agent is not active, no HPO services are available on that machine.

The Tuxedo SPI managed node software performs the following major tasks:

- Receives monitoring information (ULOGs, system events, TMIB values) from the Tuxedo domain and forwards it to the HPO agent
- Receives instructions for administrative tasks (such as starting and stopping Tuxedo servers) from the HPO agent and forwards them to the Tuxedo domain
- Periodically compresses and deletes outdated ULOG files
- Monitors the beaEvt2ito and beaUlog2ito processes

Figure 5 HPO and Tuxedo SPI Software on a Tuxedo Non-Master Machine



Tuxedo SPI Managed Node Components

The Tuxedo SPI managed node software consists of the following components:

- TUXSPI Monitoring Processes
- TUXSPI Utilities
- TUXSPI Policies

TUXSPI Monitoring Processes

The TUXSPI monitoring processes are:

- beaUlog2ito, which monitors ULOG messages via the TMIB and forwards them to the HPO agent. The HPO agent consults a particular TUXSPI template to determine how to filter the ULOG messages. If the template indicates that a ULOG message should be forwarded, the HPO agent sends it to the management server.
- beaEvt2ito, which monitors Tuxedo system events and forwards them to the HPO agent.

TUXSPI Utilities

The Tuxedo SPI managed node software includes the following utilities:

- Runner (bearun)

  The bearun utility runs the Tuxedo utilities (tmadmin(1) and tmunloadcf(1)) and the Tuxedo SPI command line utilities. When you call a utility, bearun prepares the Tuxedo environment based on the invocation options and then invokes the utility.

- TMIB process (beatmib)

  The beatmib utility extracts information from the TMIB, processes the information, and forwards resulting messages to the HPO agent. The HPO agent calls `beatmib` according to schedules specified in the TUXSPI templates.

- Tuxedo SPI command line utilities

You can invoke the Tuxedo SPI command line utilities from a script or program.

TUXSPI Policies

A policy is a set of parameters that tells HPO how to monitor processes, log files, events, and messages. HPO uses policies to intercept messages from different message sources on a managed node and to monitor areas where predefined values or limits are exceeded. Policy administrators use configuration tools to set up message collection and monitoring services and to define filters and suppression criteria to refine and reduce information sent to the HPO management server.

The Tuxedo SPI managed node software sends Tuxedo ULOG messages, system event messages, and TMIB metrics to the HPO agent. The HPO agent uses the TUXSPI policies to determine whether or not to send the information to the management server. The HPO agent also uses the policies to determine whether or not it is time to execute a scheduled task.

The SPI for Tuxedo policy group contains the following policies groups:

- Tuxedo Data Collection
- Tuxedo EVT Mon
- Tuxedo MIB Mon
- Tuxedo SCHED Mon
- Tuxedo SPI Admin
- Tuxedo ULOG Mon

Tuxedo Data Collection

This policy group contains the following policies:

TUXSPI_ServerDataLog	Logs data for the SERVER class of Tuxedo.
TUXSPI_ClientDataLog	Logs data for the CLIENT class of Tuxedo.
TUXSPI_MessageDataLog	Logs data for the MESSAGE class of Tuxedo.

TUXSPI_MachineDataLog	Logs data for the MACHINE class of Tuxedo.
TUXSPI_AppQueueDataLog	Helps to collect data from the APPLICATIONQUEUESPACE metrics, APPLICATIONQUEUE metrics and APPQUEUETRANS metrics after integration with HP Performance products.
TUXSPI_GroupDataLog	Helps to collect data from the GROUP metrics after integration with HP Performance products.

Tuxedo EVT Mon

This policy group contains the following policies:

TUXEVT	Monitors Tuxedo system events.

Tuxedo MIB Mon

This policy group contains the following policies:

T_CLIENT-NUMCONV	Calculates the number of open conversions.
T_MACHINE-PCT_CLIENTS	Estimates the percentage of used client entries on the machine.
T_CLIENT-PCT_TRANBT	Estimates the percentage of aborted transactions on the client.
T_SERVER-PCT_TRANBT	Estimates the percentage of aborted transactions on the server.
T_CLIENT-NUMUNSOL	Counts the number of unsolicited messages in the queue.
T_MACHINE-PCT_WSCLIENTS	Estimates the percentage of used or WS client entries on the machine.
T_MSG-MSG_RTIME	Calculates the time after a message was read from the queue.

T_SERVER-NUMCONV_MIN	Counts the number of conversions opened by the server in a minute.
T_CLIENT-NUMREQ_MIN	Estimates the number of initiated requests in a minute.
T_SERVER-NUMQUEUE_MIN	Estimates the number of enqueue operations in a minute.
T_SERVER-NUMREQC_MIN	Estimates the number of completed requests in a minute.
TUXMON-5M	Runs the beatmib process every five minutes.
T_SERVER-NUMDEQUEUE_MIN	Estimates the number of dequeue operations in a minute.
T_SERVER-NUMPOST_MIN	Calculates the number of post operations in a minute.
T_CLIENT-NUMSUBSCRIBE_MIN	Calculates the number of subscriptions in a minute.
TUXMON-15M	Runs the beatmib process every 15 minutes.
T_APPQSPACE-PCT_MSG	Specifies the percentage of messages in the Tuxedo Application Queue space.
T_APPQSPACE-PCT_PROC	Specifies the percentage of processes accessing Tuxedo Application Queue space.
T_APPQSPACE-PCT_QUEUES	Specifies the percentage of queues filled in the Tuxedo Application Queue space.
T_APPQSPACE-PCT_TRANS	Specifies the percentage of transactions done in the Tuxedo Application Queue space.
T_APPQSPACE-FREE_DSK	Specifies the percentage of free disk space in the Tuxedo Application Queue space.

T_APPQSPACE-FREE_MEM	Specifies the percentage of free shared memory space in the Tuxedo Application Queue space.
T_APPQUEUE-CUR_MSG	Specifies the number of persistent (disk based) messages in the queue.
T_APPQUEUE-CUR_MEMMSG	Specifies the number of non-persistent (shared memory based) messages in the queue.
T_APPQUEUE-CUR_BLOCKS	Specifies the number of disk pages occupied by the queue.
T_APPQUEUE-CUR_SHAREDMEM	Specifies the amount of shared memory (in bytes) occupied by the queue.
T_APPQUEUE-TOTAL_MSG	Specifies the total number of messages residing in the queue (persistent + non-persistent).
T_GROUP-STATE	Specifies the state of the Tuxedo Server Groups.

Tuxedo SCHED Mon

This policy group contains the following policies:

TUXSPI_CHKULOGMON	Checks if the ULOG monitoring process is active.
TUXSPI_DELETEULOG	Deletes the ULOG files that are older than a specified time interval. The default time interval is once every day.
TUXSPI_CHKEVTMON	Checks if the event monitoring process is active.
TUXSPI_COMPRESSULOG	Compresses the ULOG files that are older than a specified time interval. The default time interval is once every day.

Tuxedo SPI Admin

This policy group contains the following policies:

TuxedoSPIMsg	Collects and handles internal Tuxedo SPI messages.

Tuxedo ULOG Mon

This policy group contains the following policies:

TUXLOG	Monitors Tuxedo ULOG messages.

2 Chapter:Tuxedo SPI Tools and Message Groups

The Tuxedo SPI adds a number of tools, tool groups, and message groups. This chapter describes the objects.

Tools in the HPO Tools Groups

The top Tuxedo SPI tool group TUXSPI contains 2 subgroups:

- Tuxedo Admin

You can use the tools in this tool group to perform administrative tasks specific to Tuxedo such as starting the Tuxedo server, stopping the Tuxedo server, viewing the Tuxedo configuration and so on.

- Tuxedo SPI Admin

You can use the tools in this tool group to perform adminstrative tasks specific to Tuxedo SPI such as adding a domain, configuring the SPI, managing event monitoring and so on.

Tuxedo Administration tools

The tool group Tuxedo Admin contains the following tools:

Force Tuxedo Stop

Forces all administration and application servers in the Tuxedo domain to shutdown even if clients are accessing the servers.

Show Servers

Displays the servers and the server statistics in the Tuxedo domain.

Show Services

Displays the Tuxedo services and the service statistics in the Tuxedo domain.

Show Transactions

Displays the transactions in the Tuxedo domain.

Show Tuxedo Cfg

Displays the Tuxedo configuration file (beamgr.conf) for the Tuxedo domain.

Show ULOG

Displays the ULOG file of the master machine for the current day. You can view the ULOG file for a specific day by specifying the day (in MMDDYYYY format) as a parameter.

For example, if you provide the -d 10272004 -d MYDOMAIN parameters with the Show ULOG tool, then the ULOG file for MYDOMAIN on 27 October, 2004 appears.

You can also use this tool to view the ULOG file of a managed non-master machine in the Tuxedo domain.

Start Adm Svrs

Starts all the administration servers in the Tuxedo domain.

Each Tuxedo managed node has the following administration servers:

- BRIDGE: An administration server that establishes the listening address of the machine
- Bulletin Board Liaison (BBL): An administration server that creates the shared memory Bulletin Board
- Distinguished Bulletin Board Liaison (DBBL) server: An administration server that manages the updates to the Bulletin Board
- Transaction Management Server (TMS):A Tuxedo managed node can have additional administration servers, such as the TMS, which handles transaction completion procedures.

Start App Svrs

Starts all the application servers in the Tuxedo domain.

Start Tuxedo

Starts all the administration and application servers in the Tuxedo domain.

Stop Adm Svrs

Stops all the administration servers in the Tuxedo domain.

Stop App Svrs

Stops all the application servers in the Tuxedo domain.

Stop Tuxedo

Stops all the administration and application servers in the Tuxedo domain.

Note:

After you turn off the Tuxedo system, the Tuxedo SPI software stops monitoring Tuxedo system events. To restart Tuxedo system event monitoring:

- Restart the Tuxedo system
- Use the Event Mon Stop and the Event Mon Start commands to stop and then restart Tuxedo system event monitoring

Tuxedo SPI Administration tools

The tool group Tuxedo Admin contains the following tools:

Add Domain

The tool adds:

- The domain to the target master machine
- The domain to the Tuxedo SPI configuration file (beamgr.conf) on any non-master machine in the domain running the Tuxedo SPI software

Configure Data Collection

Allows you to configure Tuxedo SPI integration with HP Performance products.

Note: If any modifications such as additions or deletions of Tuxedo servers are made in the SERVERS section of the UBBCONFIG file, then you must delete all the files that start with the name beaSvr and beaCli from the Tuxedo SPI configuration directory (<hpswinstalldir>/subagent/BEASPI/etc). <hpswinstalldir> is the directory in which HP Operations Manager is installed.

Configure SPI

Allows you to configure a master machine by creating and configuring the necessary data files on the master machine.

Delete Domain

The tool deletes:

- The domain from the target master machine
- The domain from the Tuxedo SPI configuration file (beamgr.conf) on any non-master machine in the domain running the Tuxedo SPI software

Event Mon Start

Starts event monitoring for the Tuxedo domain.

Event Mon Stop

Stops event monitoring for the Tuxedo domain.

Remove Tuxedo SPI

Removes Tuxedo SPI files and configuration directory that were installed during Tuxedo SPI installation from the managed node.

Service Discovery

Generates the service discovery XML file in the SPI config directory. This tool does not generate the service map.

Show Domains

Lists the configured Tuxedo domains that the Tuxedo SPI needs to monitor.

Ulog Mon: Add Nodes

Starts ULOG monitoring on one or more machines in the Tuxedo domain.

Ulog Mon: Del Nodes

Stops ULOG monitoring on the machines in the Tuxedo domain.

Ulog Mon: List Nodes

Lists the machines in the Tuxedo domain that have been configured for ULOG monitoring.

Version verify

Helps to know if there is any difference between Tuxedo SPI base product version and the Tuxedo SPI component version installed on the system.

Message Groups

The Tuxedo SPI creates two new Message groups:

- Tuxedo
- TUXSPI

3 Chapter:Distributing and Running the Tuxedo SPI

This chapter describes how to distribute and run the Tuxedo SPI agent software on a managed node.

Assumptions

It is assumed that you have already installed the Tuxedo SPI software on the management server as described in the installation guide. It also is assumed that you have distributed the OVO agent software to the managed nodes. For information on installing and distributing OVO software, see the HP OVO online documentation at http://hpat937.external.hp.com/lpe/doc_serv.

In the procedures that follow, the target managed node is a machine named alfred.mycompany, which is the master machine of a Tuxedo domain.

Step 1. Configure and Start the Tuxedo Domain

To configure and start the Tuxedo domain, follow these steps:

1. Create the UBBCONFIG file.
2. Generate the TUXCONFIG file.
3. Run tlisten and start the Tuxedo domain.

Step 2. Deploy the Tuxedo SPI instrumentation.

Deploy the following Tuxedo SPI instrumentation files present on the management server to the managed node:

- TUXSPI
- SPI Data Collector

Step 3. Run the Configure SPI tool

Run the Configure SPI tool to specify the Tuxedo master machen on which you want to start Tuxedo SPI.

Step 4. Add the Domain to the Tuxedo SPI Environment

To add the Tuxedo domain information to the Tuxedo SPI environment on the target managed node, run the Add Domain tool.

Step 5. Start Monitoring Domain System Events

Prerequisite: Before you start Tuxedo SPI event monitoring, you must boot the TMSYSEVT server.

To start monitoring system events for the Tuxedo domain, run Event Mon Start tool. This tool executes the event monitoring process (beaEvt2ito) in the background on all the machines in the Tuxedo domain.

Step 6. Start Monitoring Domain ULOG Messages

To start monitoring ULOG messages for the Tuxedo domain, run the ULOG Mon: Add Nodes tool.

The ULOG Mon:Add Nodes command starts the Tuxedo SPI beaUlog2ito process, which starts monitoring the ULOG messages for the specified machine in the Tuxedo domain via the TMIB on the target managed node.

You can run the Ulog Mon:Add Nodes command a number of times to start ULOG monitoring on other machines in the Tuxedo domain.

Step 7. Deploy Tuxedo SPI policies

In order to see Tuxedo messages or Tuxedo SPI messages you need to deploy Tuxedo SPI policies on the managed node.

4 Chapter:Performing Administrative Tasks

This chapter describes how to use the HPO graphical user interface (GUI) to perform Tuxedo SPI administrative tasks.

Using Customized Startup

With customized startup, you right-click a Tuxedo SPI tool icon for which you want to specify parameters, choose Start Customized... from the popup menu that appears, and then specify the parameters in the Additional Parameter field.

You can change many of the startup parameters of an application using the Start Customized wizard. You can change the node or nodes on which a tool is to start, the user name, or any call parameter that does not appear in the Command field. The only item that you cannot change is the Command call.

The following listings and table describe the bearun syntax for the tool call and the bearun syntax of the additional parameters.

Listing 0-1 bearun Application Call Syntax

```
bearun [-R][-N][-z] -C "BEA_subcommand"
```

Listing 0-2 bearun Application Parameters Syntax

```
bearun [-g][-G]{-N|-d Instance_Name|-a|-A|[-R -t TUXDIR -T TUXCONFIG]}[-c
config_file] -C command_name -X command_extension ...
```

..

Note that when the -R option is in the Application Call field, you must include the -t TUXDIR and -T TUXCONFIG options (but may *not* include the -d *Instance_Name*, -a, or -A options) in the Application Parameters field.

Option Name	Description
-R	Allows you to specify a Tuxedo domain with the -t *TUXDIR* -T *TUXCONFIG* options.
-N	Enables `bearun` to be executed without sourcing the Tuxedo environment.
-z	Indicates the use of a BEA subcommand that is Tuxedo-version independent.
-C	Signifies a BEA subcommand (enclosed in quotation marks) that appears immediately after this option.

Option Name	Description
-g	Creates a trace file for `bearun` and the invoked command (in /tmp directory for UNIX-based platforms and in the %TEMP% directory for Windows-based platforms).
-G	Creates a trace file for `bearun` and the invoked command (in the /tmp directory for UNIX-based platforms and in the %TEMP% directory for Windows-based platforms).
-d	Allows you to specify a Tuxedo domain by name.
-a	If you use this option, all domains on the selected master machine will be affected by the command.
-A	If you use this option, all domains on the selected non-master machine will be affected by the command.
-c	Specify the complete alternative path to the `beamgr.conf` file. If this is not specified a default is used (/opt/OV/subagent/BEASPI/etc/ for UNIX; \usr\OV\subagent\BEASPI\etc\ for Windows).
-X	Appends parameters to the TUXSPI subcommand specified by the -C option in the Application Call field of the Customized Startup window.

Add the application startup parameters to the Additional Parameters field, using the following tables as a reference, then click Finish. See the Legend at the end of the tables for parameter descriptions.

Table 1 TUXSPI Parameters for Customized Startup

	What Appears in Application Call Field
Application	**Application Startup Parameters**
Tuxedo Administration Group	
Add Domain	bearun -R –C “beaDiscover”
	`-t` *`TUXDIR`* `-T` *`TUXCONFIG`*
Configure SPI	beaSPIConfigure
	(no parameters)

Table 1 TUXSPI Parameters for Customized Startup (cont'd)

Application	What Appears in Application Call Field Application Startup Parameters
Delete Domain	bearun -z –C "beaDelDom"
	-X "-d *DomainID*"
Start Event Mon	bearun -C "beaEvtMon start"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Stop Event Mon	bearun -C "beaEvtMon stop"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Ulog Mon:Add Nodes	bearun -C "beaAddNodesUlogMon"
	{-d *DomainID* | -a | -A} -X "{*LMID_1* ... [*LMID_N*]| all}"
Ulog Mon:Del Nodes	bearun -C "beaDelNodesUlogMon"
	{-d *DomainID* | -a | -A} -X "{*LMID_1* ... [*LMID_N*]| all}"
Ulog Mon:List Nodes	bearun -C "beaListNodesUlogMon"
	{-d *DomainID* | -a | -A}
Show Domains	bearun –N –C "beaShowDom"
	(leave blank)
Version verify	shs_perl -S shs_collector.pl -t spi_tux_shs_task.xml -i spi_tux_shs_input.xml –verify
	(leave blank)
Tuxedo Application tool group	
Start Tuxedo	bearun -z –C "beaStartTux"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Stop Tuxedo	bearun -z –C "beaStopTux"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Force Tuxedo Stop	bearun -z –C "beaForceTux"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Start Adm Svrs	bearun -z –C "beaStartAdm"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Stop Adm Svrs	bearun -z –C "beaStopAdmin"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}

Table 1 TUXSPI Parameters for Customized Startup (cont'd)

Application	What Appears in Application Call Field Application Startup Parameters
Start App Svrs	bearun -z –C "beaStartSrvr"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Stop App Srvr	bearun -z –C "beaStopSrvr"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Show Servers	bearun -z –C "beaShowSvr"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Show Services	bearun -z –C "beaShowSvc"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Show Transactions	bearun -z –C "beaShowTx"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Show ULOG	bearun –C "beaulog"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*} -X "[-n *LMID*] [-d *mmddyy*]" defaults: selected master machine for -n option and today's date for -d option
Show Tuxedo Cfg	bearun -z –C "beaShowConf"
	{-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}
Show Domains	bearun –N –C "beaShowDom"
	(leave blank)

The "{}" symbols denote parameters that are required. The "[]" symbols denote parameters that are optional. The "|" symbols denote a choice.

Legend:

TUXDIR = Full pathname to the top-level installation directory for your Tuxedo application. The TUXDIR pathname is given in the text version of the Tuxedo configuration file (UBBCONFIG).

TUXCONFIG = Full pathname to the binary Tuxedo configuration file including file name. (The file name is usually tuxconfig.) The TUXCONFIG pathname is given in the text version of the Tuxedo configuration file (UBBCONFIG).

DomainID = Name of subject domain (DOMAINID in UBBCONFIG file).

In reference to: {-d *DomainID* | -a | -A | -R -t *TUXDIR* -T *TUXCONFIG*}:

-d *DomainID* = Uses domain specified by *DomainID*.

-a = Uses all domains of selected master machine.

-A = Uses all domains of selected non-master machine.

-R = Uses domain corresponding to specified *TUXDIR* and *TUXCONFIG*.

LMID_N = Logical machine ID string of node *N*. The LMID is given in the text version of the Tuxedo configuration file (UBBCONFIG).

TMIB Metrics

The TMIB metric is a value that the Tuxedo SPI calculates using the data from TMIB (TMIB attributes).

For example, the TMIB metric PCT_TRANABT, which is the percentage of transactions that are aborted is calculated as follows:

PCT_TRANABT=Number of aborted transactions/Total number of transactions

Here, the number of aborted transactions and the total number of transactions, which is the data necessary for the TMIB metric calculation are referred to as TMIB attributes.

The HP Operations agent uses the TMIB metric to verify if the thresholds specified in the policies (present in the MIB Monitor Policies group) are violated. Each TMIB metric has a MIB Monitor Policy associated with it. The policy specifies the threshold and the comparison for the TMIB metric.

Tuxedo SPI uses the TMIB metrics as follows:

- The beatmib utility uses the TMIB attributes to calculate the TMIB metric.
- The beatmib utility sends the TMIB metric to the HP Operations agent.
- The HP Operations agent compares the TMIB metric with the threshold set.
- If the threshold is violated, the HP Operations agent creates a message and sends it to the management server.
- You can change the values in the policies. Each TMIB metric monitoring policy provides instruction text for the TMIB metric.

Tuxedo SPI passes identifiers to HPOM for the TMIB metrics in each metrics group. The identifiers are passed as a set of HPOM option strings. The TMIB metrics are grouped as follows:

SERVER Class Metrics

Table 2 SERVER Class Metrics

Metric Name	Description
SVR_PCTGEN	Percentage of generations
SVR_NUMDEQUE_MIN	Number of dequeue operations
SVR_NUMENQUE_MIN	Number of enqueue operations
SVR_NUMREQ_MIN	Number of current requests
SVR_PCTTRANABT	Percentage of aborted transactions
SVR_NUMREQC_MIN	Total number of requests open
SVR_NUMREQ	Number of open asynchronous requests
SVR_NUMCONV_MIN	Total number of conversations
SVR_NUMPOST_MIN	Number of post operations
SVR_NUMTRANS_MIN	Number of transactions

CLIENT Class Metrics

Table 3 CLIENT CLASS METRICS

Metric Name	Description
CLI_IDLETIME	Client idle time
CLI_NUMDEQUE_MIN	Number of dequeue operations
CLI_NUMENQUE_MIN	Number of enqueue operations
CLI_NUMREQ_MIN	Number of current requests
CLI_ENCRYPTBITS	Encryption bits

Table 3 CLIENT CLASS METRICS

Metric Name	Description
CLI_NUMREQ	Number of open asynchronous requests
CLI_NUMCONV_MIN	Total number of conversations
CLI_NUMPOST_MIN	Number of post operations
CLI_NUMSUBSCI_MIN	Number of subscriptions
CLI_NUMTRANS_MIN	Number of transactions
CLI_PCTTRANABT	Percentage of aborted transactions
CLI_NUMUNSOL	Number of unsolicited messages
CLI_NUMCONV	Number of open conversations

MACHINE Class Metrics

Table 4 MACHINE Class Metrics

Metric Name	Description
MACH_PCT_ACC	Percentage of accessers
MACH_PCT_CLNTS	Percentage of clients
MACH_PCT_GTT	Percentage of GTT
MACH_PCT_WSCLNTS	Percentage of WSCLNTS
MAC_PCT_CONV	Percentage of conversations

MESSAGE Class Metrics

Table 5 MESSAGE Class Metrics

Metric Name	Description
MSG_PCTMSG_CB	Percentage of queue utilization
MSG_QNUM	Number of messages in the queue
MSG_RTIME	Last read time from the queue
MSG_STIM	Last write time from the queue

T_APPQSPACE Class Metrics

Table 6 T_APPQSPACE Class Metrics

Metric Name	Description
TA_APPQSPACENAME	Application Queue space name
TA_QMCONFIG	QMCONFIG path
TA_LMID	Machine LMID
TA_STATE	State of the queue space
TA_MAXMSG	Maximum number of messages the queue space can contain
TA_MAXPAGES	Maximum number of disk pages allocated

Table 6 T_APPQSPACE Class Metrics

Metric Name	Description
TA_MAXPROC	Maximum number of processes that can access the queue space
TA_MAXQUEUES	Maximum number of queues the queue space can contain
TA_MEMNONPERSIST	Amount of shared memory reserved for non-persistent messages
TA_MEMSYSTEMRESERVED	Amount of shared memory reserved for queuing (system use)
TA_MEMTOTALALLOCATED	Total amount of shared memory allocated for all queuing services
TA_CURMSG	Current number of messages in the queue space
TA_CURQUEUES	Current number of queues in the queue space
TA_CURMEMNONPERSIST	Current amount of memory consumed by non-persistent messages

T_APPQ Class Metrics

Table 7 T_APPQ Class Metrics

Metric Name	Description
TA_APPQNAME	Application Queue Name
TA_APPQSPACENAME	Application Qspace Name
TA_QMCONFIG	QMCONFIG path
TA_LMID	Machine LMID
TA_STATE	State of the queue
TA_APPQUEUEORDER	Application queue servicing order
TA_DEFDELIVERY	Default delivery policy
TA_CURBLOCKS	Number of disk pages consumed by the queue
TA_CURMSG	Number of persistent messages residing in the queue
TA_CURNONPERSISTBYTES	Amount of shared memory consumed by the queue
TA_CURNONPERSISTMSG	Number of non-persistent messages residing in the queue

T_APPQTRANS Class Metrics

Table 8 T_APPQTRANS Class Metrics

Metric Name	Description
TA_XID	Transaction ID
TA_APPQSPACENAME	Application Qspace name
TA_QMCONFIG	QMCONFIG path
TA_LMID	Machine LMID
TA_STATE	State of the transaction

T_GROUP Class Metrics

Table 9 T_GROUP Class Metrics

Metric Name	Description
TA_SRVGRP	Logical name of the Tuxedo Server group
TA_GRPNO	Group number associated with the server group
TA_LMID	Primary and secondary logical machine identifiers
TA_CURLMID	Current logical machine on which the server group is running
TA_STATE	State of the server group, ACTIVE, INACTIVE, and MIGRATING

Specifying Threshold Value with Metric ID

You can specify a threshold value with metric id in the policy command line. For example, the policy command in TUXMON-15M template would be:

```
bearun -a -C \"beatmib -m TUXMON-15M -
M2005,3008,4002,4003,4004,4005,4006,4007,4008,6001:65,6002:7
5,6003:60,6004,6005,6006:40,7001,7002,7003,7004,7005\""
```

In the above command, the threshold specified for metric 6001 is 65 and the threshold specified for metric 6006 is 40. In such cases, the values specified with the metric ids are taken as primary thresholds and opcmon calls are are made only if the calculated metric value exceeds this threshold value. This reduces the number of opcmon calls made. If no threshold value is specified at the command line, then opcmon calls are made for every calculated value.

In the above command, for metric 6001, opcmon call is made only if the calculated value (obtained by beatmib) exceeds 65.

Integrating with Service View

Tuxedo SPI supports integration with the Service Discovery Framework (SDF) to display the service map of a managed node. The service map is a hierarchical representation of the services discovered on a managed node. You can use the Service Discovery application to display the service map of a managed node.

Troubleshooting

Problem	The Tuxedo SPI uses the Tuxedo license file to determine the version of Tuxedo being run. If Tuxedo is booted with an older license file, the Tuxedo SPI will not be able to discover the Tuxedo domain. For example, this problem will occur if you boot Tuxedo 6.5 using a Tuxedo 6.4 license file

Solution	Configure the Tuxedo domain for the Tuxedo SPI manually: 1 Distribute templates to the Tuxedo master machine. 2 Run the `Configure SPI` application and verify that the file `/opt/OV/subagent/BEASPI/etc/beamgr.conf` exists. 3 Run the `Add Domain` application and type a valid TUXDID and TUXCONFIG path. 4 Open the `/opt/OV/subagent/BEASPI/etc/beamgr.conf`. file. At the end of the file, in the version section, replace Tuxedo version 64 with the appropriate version of Tuxedo. Append the following in the file: `TMAGENT` *domain $TUXDIR $TUXCONFIG Tux_UID mstr_mchn version* where TMAGENT is a keyword and must be entered exactly. *domain* is a unique domain name of the site. The domain name may be configured in the `UBBCONFIG` or `TUXCONFIG` file. If the domain name of the site is not configured in these files, use any name that uniquely identifies the domain (for example, mydomain!). *$TUXDIR* is the Tuxedo home directory that is defined by the TUXDIR environment variable (for example, `/home/tuxedo/tux8.0/`) *$TUXCONFIG* is the directory in which the TUXCONFIG file is located for this domain, as defined by the TUXCONFIG environment variable (for example, `/home/tuxedo/tuxapps/tuxconfig`). *Tux_UID* is the user ID that Tuxedo runs as (for example, 0, which is the root user). *mstr_mchn* is the name of the master machine on which Tuxedo is booted. The master machine name is configured in the `UBBCONFIG` file. The name must be in the same format as the output of the command “uname -n” and is NOT the LMID value. *version* is the version of Tuxedo and must be one of the following: **`65`** - Tuxedo version 6.5 running on a 32-bit system **`65_64bit`** - Tuxedo version 6.5 running on a 64-bit system **`71`** - Tuxedo version 7.1 running on a 32-or-64-bit system **`80`** - Tuxedo version 8.0/8.1 running on a 32-or-64-bit system

Using the Self-Healing Info Application

The Self-Healing Info application gathers system information as well as configuration, log and trace files of Tuxedo SPI when a problem occurs in the Tuxedo SPI.

All the gathered information and files are placed in a pre-defined output directory, thereby facilitating faster troubleshooting. Also, the data collector is used to gather real-time data, which reduces the probability of troubleshooting with stale data.

To greatly enhance troubleshooting, and access the search and cross-referencing capabilities of the HP Support web site, you can download and use the **Self-Healing Services** client software. Refer to the relevant section in the *HP OpenView Operations for UNIX SPI CD Installation Guide* for more information on how to download and use the software, and to set up the automatic link to the HP support web site.

If Self-Healing Services client is not installed and configured on the node being managed by the SPI, you can use the `Self-Healing Info` application to collect system information.

Whenever you encounter a problem with the Tuxedo SPI, run the data collector by launching the `Self-Healing Info` application in the `BEA SPI Tools` group.

Prior to using the Self-Healing Info application, turn on tracing and reproduce the problem, then run the application.

To launch the data collector on the node from where you want to gather data, drag the icon of the node and drop it on the `Self-Healing Info` application in the `BEA SPI Tools` application group window for the respective operating system. The output is placed as `/tmp/SPI_TUXEDO_support.tar` on UNIX nodes and as `C:\Temp\SPI_TUXEDO_support.zip` on Windows nodes. You can submit this file to HP Support for assistance or use this file to identify and correct the problem you encountered.

Depending on the Windows setting, the file may be a hidden file on some managed nodes. If you do not see the file, open **Windows Explorer** and from the `Tools` menu select the `View` tabbed page in the `Folder Options...` Under `Hidden Files and Folders`, select `Show Files and Folders`.

5 Chapter:Tuxedo System Events Supported by the Tuxedo SPI

The HPO agent uses the TUXEVT template to retrieve and monitor Tuxedo system events. If the template indicates that a system event message should be forwarded, the HPO agent reformats the message and sends it to the management server. For example, the TUXEVT template tells the HPO agent to suppress identical messages for a specified length of time. Thus, if a Tuxedo system event is generating multiple messages, HPO displays only one of the messages.

For each system event, the Tuxedo system provides values for the following variables: tuxEventsName, tuxEventsSeverity, tuxEventsLmid, tuxEventsTime, tuxEventsUsec, tuxEventsDescription, tuxEventsClass, tuxEventsUlogCat, tuxEventsUlogMsgNum.

The following table classifies the event descriptions:

Event Group	**Events**	
Bridge Events	networkConfig networkDropped networkFailure	networkFlow networkState
Client Events	clientConfig clientDied	clientSecurity clientState
Domain Events	resourceConfig	
Event Monitor Events	eventDelivery	eventFailure

Event Group	Events	
Machine Events	machineBroadcast	machineFullMaxWsClients
	machineConfig	machineMsgQ
	machineFullMaxAccessers	machinePartitioned
	machineFullMaxConv	machineSlow
	machineFullMaxGtt	machineState
Server Events	serverCleaning	serverMaxgen
	serverConfig	serverRestarting
	serverDied	serverState
	serverInit	serverTpExit
Transaction Events	transactionHeuristicAbort	transactionHeuristicCommit

Bridge Events

networkConfig

EVENT ID:	.sysNetworkConfig
SUMMARY:	A network configuration value changed.
SEVERITY:	Normal
DESCRIPTION:	A network configuration value changed.
RECOMMENDATION:	This is an informational message. No action is required.

networkDropped

EVENT ID:	.sysNetworkDropped
SUMMARY:	A network connection was dropped.
SEVERITY:	Critical
DESCRIPTION:	A network connection was dropped.
RECOMMENDATION:	• Check the original message to see which machines have a dropped bridge connection. • Make sure the network between machines is active. You can use ping to check the network.

networkFailure

EVENT ID:	.sysNetworkFailure
SUMMARY:	A network connection failed.

SEVERITY:	Critical
DESCRIPTION:	A network connection failed.
RECOMMENDATION:	• Check the original message to see which machines have a network failure. • Make sure the network between machines is active. You can use ping to check the network.

networkFlow

EVENT ID:	.sysNetworkFlow
SUMMARY:	A warning has occurred for the flow control between the machines specified in this message.
SEVERITY:	Warning
DESCRIPTION:	A warning has occurred for the flow control between the machines specified in this message.
RECOMMENDATION:	If this event happens frequently, it indicates that the specified machines are overloaded. Try to decrease the loads on the machines.

networkState

EVENT ID:	.sysNetworkState
SUMMARY:	A connection's state changed.
SEVERITY:	Normal
DESCRIPTION:	A connection's state changed.
RECOMMENDATION:	This is an informational message. No action is required.

Client Events

clientConfig

EVENT ID:	.sysClientConfig
SUMMARY:	A client's configuration changed.
SEVERITY:	Warning
DESCRIPTION:	A client's configuration changed.
RECOMMENDATION:	This is an informational message. No action is required.

clientDied

EVENT ID:	.sysClientDied
SUMMARY:	A client process died.
SEVERITY:	Warning
DESCRIPTION:	A client process died.
RECOMMENDATION:	Check the client machine to verify that it has died and try to determine why the client machine died.

clientSecurity

EVENT ID:	.sysClientSecurity
SUMMARY:	A client had an authentication failure.
SEVERITY:	Critical
DESCRIPTION:	A client had an authentication failure, which caused a security violation. If this message appears repeatedly, an unauthorized user is trying to log in to the system.
RECOMMENDATION:	Try to find the unauthorized user.

clientState

EVENT ID:	.sysClientState
SUMMARY:	A client changed its state.
SEVERITY:	Normal
DESCRIPTION:	A client changed its state.
RECOMMENDATION:	This is an informational message. No action is required.

Domain Events

resourceConfig

EVENT ID:	.sysResourceConfig
SUMMARY:	A domain's configuration changed.
SEVERITY:	Normal
DESCRIPTION:	A domain's configuration changed.
RECOMMENDATION:	This is an informational message. No action is required.

Event Monitor Events

eventDelivery

EVENT ID:	.sysEventDelivery
SUMMARY:	The system event monitor had a delivery failure.
SEVERITY:	Critical
DESCRIPTION:	The system event monitor had a delivery failure because it could not deliver asynchronous events.
RECOMMENDATION:	If the TMSYSEVT process is not running, start it. To start TMSYSEVT, you might need to modify the Tuxedo configuration file. (TMSYSEVT is a Tuxedo administration server process.)

eventFailure

EVENT ID:	.sysEventFailure
SUMMARY:	The system event monitor had a subsystem failure.
SEVERITY:	Critical
DESCRIPTION:	The system event monitor had a subsystem failure.
RECOMMENDATION:	If the TMSYSEVT process is not running, start it. To start TMSYSEVT, you might need to modify the Tuxedo configuration file. (TMSYSEVT is a Tuxedo administration server process.)

Machine Events

machineBroadcast

EVENT ID:	.sysMachineBroadcast
SUMMARY:	A machine failed to deliver a broadcast message.
SEVERITY:	Warning
DESCRIPTION:	The broadcast message was not delivered to certain clients because they were abnormally disconnected from the domain.
RECOMMENDATION:	Use the bbclean command in the tmadmin utility to clean the outstanding resources. After bbclean, the machine will automatically try to broadcast the message again.

machineConfig

EVENT ID:	.sysMachineConfig
SUMMARY:	A machine's configuration changed.
SEVERITY:	Normal
DESCRIPTION:	A machine's configuration changed.
RECOMMENDATION:	This is an informational message. No action is required.

machineFullMaxAccessers

EVENT ID:	.sysMachineFullMaxAccessers
SUMMARY:	A machine reached the MAXACCESSERS limit.

SEVERITY:	Warning
DESCRIPTION:	The domain does not have enough resources to handle all the accessers (clients).
RECOMMENDATION:	• Shut down the domain. • Increase the MAXACCESSERS parameter in the Tuxedo configuration file.

machineFullMaxConv

EVENT ID:	.sysMachineFullMaxConv
SUMMARY:	A machine reached the MAXCONV limit.
SEVERITY:	Warning
DESCRIPTION:	The domain does not have enough resources to handle all the conversations.
RECOMMENDATION:	• Shut down the domain. • Increase the MAXCONV parameter in the Tuxedo configuration file.

machineFullMaxGtt

EVENT ID:	.sysMachineFullMaxGtt
SUMMARY:	A machine reached the MAXGTT limit.
SEVERITY:	Warning
DESCRIPTION:	The domain does not have enough resources to handle all the global transactions.
RECOMMENDATION:	• Shut down the domain. • Increase the MAXGTT parameter in the Tuxedo configuration file.

machineFullMaxWsClients

EVENT ID:	.sysMachineFullMaxWsClients
SUMMARY:	A machine reached the MAXWSCLIENTS limit.

SEVERITY:	Warning
DESCRIPTION:	The domain does not have enough resources to handle all the workstation clients.
RECOMMENDATION:	• Shut down the domain. • Increase the MAXWSCLIENTS parameter in the Tuxedo configuration file.

machineMsgQ

EVENT ID:	.sysMachineMsgQ
SUMMARY:	A machine reached the MAXQUEUES limit.
SEVERITY:	Warning
DESCRIPTION:	The domain does not have enough resources to register all the Tuxedo queues.
RECOMMENDATION:	• Shut down the domain. • Increase the MAXQUEUES parameter in the Tuxedo configuration file.

machinePartitioned

EVENT ID:	.sysMachinePartitioned
SUMMARY:	A machine is partitioned.
SEVERITY:	Critical
DESCRIPTION:	A machine was partitioned, which means that it is no longer connected to the domain.
RECOMMENDATION:	• Use the psr command in the tmadmin utility to determine whether or not the machine is really partitioned. • If the machine is partitioned, use the rco command in the tmadmin utility to reconnect the machine.

machineSlow

EVENT ID:	.sysMachineSlow
SUMMARY:	A machine is slow in responding to the DBBL.

SEVERITY:	Warning
DESCRIPTION:	The communication between the DBBL and BBL processes is slow. This problem is usually caused by a slow network connection.
RECOMMENDATION:	If this message appears frequently, modify the Tuxedo configuration file. You may need to decrease one or more of the following configuration values: SCANUNIT, SANITYSCAN, DBBLWAIT, BBLQUERY.

machineState

EVENT ID:	.sysMachineState
SUMMARY:	A machine changed its state.
SEVERITY:	Normal
DESCRIPTION:	A machine changed its state.
RECOMMENDATION:	• Check the original message for the final state of the machine. • If the machine's state indicates that the machine is partitioned, use the psr command in the tmadmin utility to see if the machine is partitioned. • If the machine is partitioned, use the rco command in the tmadmin utility to reconnect the machine. • If the machine is activated, acknowledge this event.

Server Events

serverCleaning

EVENT ID:	.sysServerCleaning
SUMMARY:	The Tuxedo system is cleaning resources for an application server that died.
SEVERITY:	Critical
DESCRIPTION:	The Tuxedo system is cleaning resources for an application server that died.
RECOMMENDATION:	This event will be accompanied by additional events that indicate exactly what happened. Follow the instructions in the accompanying events.

serverConfig

EVENT ID:	.sysServerConfig
SUMMARY:	A server instance changed its configuration.
SEVERITY:	Normal
DESCRIPTION:	A server instance changed its configuration.
RECOMMENDATION:	This is an informational message. No action is required.

serverDied

EVENT ID:	.sysServerDied
SUMMARY:	A server instance died.

SEVERITY: Critical

DESCRIPTION: A server instance died.

RECOMMENDATION:

- Use the psr command in the tmadmin utility to verify that the server died.
- If the server died, wait until the message “The application server instance has been cleaned.” arrives.
- Wait at least one minute. If the message “The application server has been restarting.” arrives, the Tuxedo system automatically restarted the server.
- Use the psr command in the tmadmin utility to see if the server restart was successful.
- If the server restart was not successful, run the bbclean command and wait at least one minute to see if the Tuxedo system will automatically restart the server.
- Use the psr command in the tmadmin utility to see if the server restart was successful.
- If the Tuxedo system does not successfully restart the server, use the boot -i server command in the tmadmin utility to manually restart the server.

serverInit

EVENT ID:	.sysServerInit
SUMMARY:	A server instance failed during initialization.
SEVERITY:	Critical
DESCRIPTION:	A server instance failed during initialization.
RECOMMENDATION:	Check the server environment file /var/spool/appid/APPDIR.SYSROLE/ENVFILE to see if the necessary database instance is running.

serverMaxgen

EVENT ID:	.sysServerMaxgen
SUMMARY:	A server instance reached the MAXGEN limit.
SEVERITY:	Critical
DESCRIPTION:	A server instance reached the MAXGEN limit, which means that the server could not be restarted.
RECOMMENDATION:	Check the machine's ULOG file and report the problem to Customer Support.

serverRestarting

EVENT ID:	.sysServerRestarting
SUMMARY:	A server instance is restarting.
SEVERITY:	Critical
DESCRIPTION:	A server instance is restarting.
RECOMMENDATION:	Wait for the next message from the server which will indicate the server's status.

serverState

EVENT ID:	.sysServerState
SUMMARY:	A server instance changed its state.
SEVERITY:	Normal
DESCRIPTION:	A server instance changed its state.
RECOMMENDATION:	Check the original message to see the server's new state. • The possible server states are: • ACTIVE: The server was started. • SUSPENDED: The server was shut down. • RESTARTING: The server is restarting. • DEAD: The server is not running. Wait up to two minutes to see if the server is restarted. If not, restart the server manually by using the boot -i <server> command in the tmadmin utility.

serverTpExit

EVENT ID:	.sysServerTpExit
SUMMARY:	A server instance requested TPEXIT.
SEVERITY:	Critical
DESCRIPTION:	A server instance requested TPEXIT, which means that the server needs to shut down.
RECOMMENDATION:	None

Transaction Events

transactionHeuristicAbort

EVENT ID:	.sysTransactionHeuristicAbort
SUMMARY:	The Tuxedo system performed a heuristic abort for a transaction.
SEVERITY:	Critical
DESCRIPTION:	The Tuxedo system performed a heuristic abort for a transaction.
RECOMMENDATION:	None

transactionHeuristicCommit

EVENT ID:	.sysTransactionHeuristicCommit
SUMMARY:	The Tuxedo system performed a heuristic commit for a transaction.
SEVERITY:	Critical
DESCRIPTION:	The Tuxedo system performed a heuristic commit for a transaction.
RECOMMENDATION:	None

6 Chapter:TMIB Metrics

A TMIB metric is a value that the Tuxedo SPI calculates from TMIB attributes. For example, the TMIB metric PCT_TRANABT (percentage of transactions that are aborted) is the number of aborted transactions divided by the total number of transactions. The number of aborted transactions and the total number of transactions are TMIB attributes.

The default thresholds, which are listed in the metric descriptions, are guidelines and are not necessarily suitable for every system because each Tuxedo domain is unique.

This chapter describes the TMIB metrics and how the Tuxedo SPI handles them.

Naming Conventions

For the TMIB metrics that have names that end in “MIN,” the Tuxedo SPI calculates the metric based on the total value that has accumulated since the Tuxedo domain was booted up. For example, NUMPOST_MIN (number of post operations per minute) is the total number of post operations that have occurred since the Tuxedo domain booted divided by the number of minutes since the Tuxedo domain booted. These types of calculations are advantageous because they do not generate messages for short bursts of high activity.

The full name for each metric consists of the group name, a hyphen, and the metric name. For example, the full name for the PCT_WSCLIENTS metric, which is in the T_MACHINE group, is T_MACHINE-PCT_WSCLIENTS.

The number that precedes each metric’s name provides a quick way to refer to the metric. The beatmib utility uses these numbers. The table at the beginning of the descriptions lists the TMIB metrics and their corresponding numbers.

Templates

The HPO agent uses the policies in the Tuxedo MIB Mon group to determine when to run beatmib and which TMIB metrics to monitor.

Running beatmib

The HPO agent calls beatmib at the time intervals specified in the following TUXSPI templates, which are in the GRPTUXMON group:

TUXMON-15M	This policy tells the HPO agent to call beatmib every 15 minutes for the TMIB metrics listed in the policy.
TUXMON-1H	This policy tells the HPO agent to call beatmib every hour for the TMIB metrics listed in the policy.
TUXMON-5M	This policy tells the HPO agent to call beatmib every 5 minutes for the TMIB metrics listed in the policy.

Use the following methods to change an interval:

To change the interval for one TMIB metric:

1. Remove the TMIB metric from the policy that it is in.

   For example, the default interval for T_MACHINE-STATE is 5 minutes (as listed in the description for T_MACHINE-STATE). To remove this TMIB metric from its current policy, open the TUXMON-5M policy and remove 2001.

2. Add the TMIB metric to the desired policy.

   For example, if you want T_MACHINE-STATE to be monitored every 15 minutes, open the TUXMON-15M policy and add 2001.

To change the interval for a group of TMIB metrics:

1. Open the policy for the group you want to change.

   For example, if you want to change the interval for the TMIB metrics that are monitored every five minutes, open the TUXMON-5M policy.

2. Change the policy polling interval value.

For example, if you want these TMIB metrics to be monitored every 10 minutes, change the polling interval to 10 minutes. You might also want to change the policy name to reflect the new interval.

Monitoring the TMIB Metrics

Each TMIB metric monitoring policy (in the Tuxedo MIB Mon group) defines a threshold and a comparison. For each TMIB metric, the HPO and Tuxedo SPI software do the following:

1. The beatmib utility uses the TMIB values to calculate the TMIB metric.
2. The beatmib utility sends the TMIB metric to the HPO agent.
3. The HPO agent compares the TMIB metric to the threshold.
4. If the threshold has been violated, the HPO agent creates a message and sends it to the management server.

You can change the values in the templates. Each TMIB metric monitoring template also provides instruction text for the TMIB metric.

Identifiers

The Tuxedo SPI passes identifiers to HPO for the TMIB metrics in each metrics group. The identifiers are passed as a set of HPO option strings. This section covers:

- T_MACHINE identifiers
- T_SERVER identifiers
- T_CLIENT identifiers
- T_MSG identifiers
- T_APPQSPACE identifiers
- T_APPQ identifiers
- T_GROUP identifiers

T_MACHINE Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_MACHINE group.

DOMAINID	Logical name of the Tuxedo domain as defined in the Tuxedo SPI configuration file
LMID	Logical name of the machine
MASTER	Physical name of the master machine
PMID	Physical name of the machine
TUXCONFIG	Path and filename for the Tuxedo configuration file on the managed node
TUXDIR	Directory where the Tuxedo system is installed on the managed node

T_SERVER Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_SERVER group.

DOMAINID	Logical name of the Tuxedo domain as defined in the Tuxedo SPI configuration file
GRPNO	Identification number of the server group
LMID	Logical name of the machine
MASTER	Physical name of the master machine
SERVERNAME	Executable name of the application server
SRVGRP	Name of the server group
SRVID	Identification number of the server

T_CLIENT Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_CLIENT group.

CLIENTID	Identification number of the client
CLTNAME	Name of the client as defined in the TPINIT buffer when the TMIB metric was calculated
DOMAINID	Logical name of the Tuxedo domain as defined in the Tuxedo SPI configuration file
LMID	Logical name of the machine
MASTER	Physical name of the master machine
PID	PID of the client
USERNAME	User name

T_MSG Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_MSG group.

DOMAINID	Logical name of the Tuxedo domain as defined in the configuration file
LMID	Logical name of the machine
MASTER	Physical name of the master machine
MSGID	Identification number of the message

T_APPQSPACE Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_APPQSPACE group.

APPQSPACE NAME	Application queue space name
LMID	Logical name of the machine
SRVGRP	Name of the server group
QMCONFIG	QMCONFIG path of the Tuxedo Application queue

T_APPQ Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_APPQ group.

APPQSPACE NAME	Application queue space name
APPQUEUE NAME	Application queue name
LMID	Logical name of the machine
SRVGRP	Name of the server group
QMCONFIG	QMCONFIG path of the Tuxedo Application queue

T_GROUP Identifiers

The Tuxedo SPI software passes the following identifiers to HPO for TMIB metrics in the T_GROUP group.

SRVGRP	Name of the server group
GRPNO	Number of Tuxedo server group
LMID	Logical name of the machine

Descriptions

The following table provides easy access to the event descriptions when you are viewing this document online (in a Web browser or a PDF file):

Metric Group	Metrics	
T_MACHINE Metrics (2xxx)	2001: STATE	2005: PCT_CONV
	2003: PCT_ACCESSERS	2006: PCT_GTT
	2004: PCT_CLIENTS	2007: PCT_WSCLIENTS
T_SERVER Metrics (3xxx)	3008: PCT_GEN	3015: NUMTRAN_MIN
	3009: NUMNCONV_MIN	3016: PCT_TRANABT
	3010: NUMDEQUEUE_MIN	3017: NUMREQC_MIN
	3012: NUMENQUEUE_MIN	3018: NUMCONV
	3012: NUMPOST_MIN	3019: NUMREQ
	3013: NUMREQ_MIN	
T_CLIENT Metrics (4xxx)	4001: STATE	4008: NUMSUBSCRIBE_MIN
	4002: IDLETIME	4009: NUMTRAN_MIN
	4003: NUMCONV_MIN	4010: PCT_TRANABT
	4004: NUMDEQUEUE_MIN	4012: NUMUNSOL
	4005: NUMENQUEUE_MIN	4012: NUMCONV
	4006: NUMPOST_MIN	4013: ENCRYPTBITS
	4007: NUMREQ_MIN	4014: NUMREQ
T_MSG Metrics (5xxx)	5001: PCT_MSG_CBYTES	5003: MSG_RTIME
	5002: MSG_QNUM	5004: MSG_STIME
T_APPQSPACE Metrics (6xxx)	6001: PCT_MSG	6004: PCT_TRANS
	6002: PCT_PROC	6005: FREE_DSK
	6003: PCT_QUEUES	6006: FREE_MEM
T_APPQ Metrics (7xxx)	7001: CUR_MSG	7004: CUR_SHAREDMEM
	7002: CUR_MEMMSG	7005: TOTAL_MSG
	7003: CUR_BLOCKS	
T_GROUP Metrics (8xxx)	8001: STATE	

T_MACHINE Metrics

2001: STATE

SUMMARY:	State of the machine
SEVERITY:	Critical
DESCRIPTION:	The default threshold is 0 (partitioned). This threshold specifies an unacceptable machine state. A threshold violation indicates that a machine was partitioned, which means that it is no longer available. The most probable reasons for this are: • The network connection was broken. • One of the BRIDGE processes died. • The machine was shut down or crashed.
RECOMMENDATION:	• If the network connection was broken: Normally the BRIDGE process automatically reconnects the machine. Wait at least two minutes and then use the `pnw` command in the tmadmin utility on the master machine to determine whether or not the machine is still partitioned. If it is, use the rco command in the tmadmin utility to reconnect the machine. If the machine is still not reconnected, check the Tuxedo ULOG file for details. • If one of the BRIDGE processes died: Normally the BBL process automatically restarts the BRIDGE process. Wait at least two minutes and then use the pnw command in the tmadmin utility on the master machine to determine whether or not the machine is still partitioned. If it is, check the Tuxedo ULOG file for details. • If the machine was shut down or crashed: Use the pclean command in the tmadmin utility to clean up the Tuxedo bulletin board. Then use the tmboot -B <machine> command to reboot the machine.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Fault
POLICY:	T_MACHINE-STATE

2003: PCT_ACCESSERS

SUMMARY:	Percentage of used entries in the accesser table An accesser is a process that accesses a Tuxedo domain. Accessers include native and remote clients, servers, and administration processes.
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 80 percent • Critical: more than 90 percent This threshold specifies the maximum percentage of used entries. A threshold violation indicates that the accesser table is becoming too full, which can prevent additional accessers from accessing the Tuxedo domain.
RECOMMENDATION:	• Next time the Tuxedo domain is shut down, increase the MAXACCESSORS parameter in the Tuxedo configuration file's *RESOURCES or *MACHINE section. • Adjust the threshold for this TMIB metric in the T_MACHINE-PCT_ACCESSERS template.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_MACHINE-PCT_ACCESSERS

2004: PCT_CLIENTS

SUMMARY: Percentage of used entries in the client table

SEVERITY: Warning or Critical

DESCRIPTION: The default threshold is:

- Warning: more than 80 percent
- Critical: more than 90 percent

This threshold specifies the maximum percentage of used entries. A threshold violation indicates that the client table is becoming too full, which can prevent additional clients from accessing the Tuxedo domain.

RECOMMENDATION:

- Next time the Tuxedo domain is shut down, increase the MAXACCESSORS parameter in the Tuxedo configuration file's *RESOURCES or *MACHINE section.
- Adjust the threshold for this TMIB metric in the T_MACHINE-CLIENTS template.

DEFAULT INTERVAL: Every 5 minutes

MONITORING TYPE: Capacity

POLICY: T_MACHINE-CLIENTS

2005: PCT_CONV

SUMMARY: Percentage of used entries in the conversation table

SEVERITY: Warning or Critical

DESCRIPTION: The default threshold is:

- Warning: more than 80 percent
- Critical: more than 90 percent

This threshold specifies the maximum percentage of used entries. A threshold violation indicates that the conversation table is becoming too full, which can prevent clients from initiating additional Tuxedo conversations.

RECOMMENDATION:	• Next time the Tuxedo domain is shut down, increase the MAXCONV parameter in the Tuxedo configuration file's *RESOURCES or *MACHINE section. • Adjust the threshold for this TMIB metric in the T_MACHINE-PCT_CONV template.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_MACHINE-PCT_CONV

2006: PCT_GTT

SUMMARY:	Percentage of used entries in the open transactions table
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 80 percent • Critical: more than 90 percent This threshold specifies the maximum percentage of used entries. A threshold violation indicates that the open transactions table is becoming too full, which can prevent clients from initiating additional transactions.
RECOMMENDATION:	• Next time the Tuxedo domain is shut down, increase the MAXGTT parameter in the Tuxedo configuration file's *RESOURCES or *MACHINE section. • Adjust the threshold for this TMIB metric in the T_MACHINE-PCT_GTT template.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_MACHINE-PCT_GTT

2007: PCT_WSCLIENTS

SUMMARY:	Percentage of used entries in the /WS client table
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 80 percent • Critical: more than 90 percent This threshold specifies the maximum percentage of used entries. A threshold violation indicates that the /WS client table is becoming too full, which can prevent additional /WS clients from accessing the Tuxedo domain.

RECOMMENDATION:
- Next time the Tuxedo domain is shut down, increase the MAXWSCLIENTS parameter in the Tuxedo configuration file's *MACHINE section.
- You might also need to increase the MAXACCESSOR parameter.
- Adjust the threshold for this TMIB metric in the T_MACHINE-PCT_WSCLIENTS template.

DEFAULT INTERVAL: Every 5 minutes

MONITORING TYPE: Capacity

POLICY: T_MACHINE-PCT_WSCLIENTS

T_SERVER Metrics

3008: PCT_GEN

SUMMARY:	Percentage of available restarts that the server had used
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 20 percent • Critical: more than 50 percent This threshold specifies the maximum percentage of available restarts that a server can use. A threshold violation indicates that server is getting close to using all available restarts, which means that it will eventually be unable to restart.
RECOMMENDATION:	Check the Tuxedo ULOG file to determine why the server is failing.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-PCT_GEN

3009: NUMCONV_MIN

SUMMARY:	Average number of conversations per minute
SEVERITY:	Critical
DESCRIPTION:	The default threshold is more than 20 conversations per minute. This threshold specifies the maximum number of open conversations the server can participate in per minute. A threshold violation indicates that the server is handling a high number of conversions, which means that too many internal Tuxedo resources are being used. This situation can prevent additional clients from communicating with the server and can decrease the server's throughput.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of open conversations does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMCONV_MIN

3010: NUMDEQUEUE_MIN

SUMMARY:	Average number of dequeue operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 100 operations per minute. This threshold specifies the maximum number of dequeue operations the server can perform per minute. A threshold violation indicates that the server is performing a high number of dequeue operations, which can cause disk I/O operations to become necessary. This situation can degrade the system performance.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of dequeue operations does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMDEQUEUE_MIN

3012: NUMENQUEUE_MIN

SUMMARY:	Average number of enqueue operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 100 operations per minute. This threshold specifies the maximum number of enqueue operations the server can perform per minute. A threshold violation indicates that the server is performing a high number of enqueue operations, which can cause disk I/O operations to become necessary. This situation can degrade the system performance.

RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of enqueue operations does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMENQUEUE_MIN

3012: NUMPOST_MIN

SUMMARY:	Average number of post operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 50 operations per minute. This threshold specifies the maximum number of post operations the server can perform per minute. A threshold violation indicates that the server is performing a high number of post operations, which can cause the system load to become excessively high.
RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of post operations does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMPOST_MIN

3013: NUMREQ_MIN

SUMMARY:	Average number of requests per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 150 requests per minute. This threshold specifies the maximum number of requests the server can initiate per minute. A threshold violation indicates that the server is initiating a high number of requests, which can cause the system load to become excessively high.

RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of requests does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMREQ_MIN

3015: NUMTRAN_MIN

SUMMARY:	Average number of transactions per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 150 transactions per minute. This threshold specifies the maximum number of transactions the server can initiate per minute. A threshold violation indicates that the server is initiating a high number of transactions, which can cause the system load to become excessively high.
RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of transactions does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMTRAN_MIN

3016: PCT_TRANABT

SUMMARY:	Percentage of transactions that were aborted
SEVERITY:	Critical
DESCRIPTION:	The default threshold is more than 5 percent. This threshold specifies the maximum percentage of transactions that the server can abort. A threshold violation indicates that one or both of the following situations occurred: • The server needed to abort transactions because the transactions returned unexpected results. • The Tuxedo system forced the server to abort transactions because problems occurred between the application server and the database or between the Transaction Management Server (TMS) and the database.
RECOMMENDATION:	• Make sure that the database and all servers connected to the database are running. • Check the Tuxedo ULOG file for problems that the servers reported. • If no problems were reported, check the business logic in your server, which might indicate inconsistent or unexpected data from the database.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Fault
POLICY:	T_SERVER-PCT_TRANABRT

3017: NUMREQC_MIN

SUMMARY:	Average number of completed requests per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 150 requests per minute. This threshold specifies the maximum number of requests that the server can complete per minute. A threshold violation indicates that the server is completing a high number of requests, which can cause the system load to become excessively high.
RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of requests does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_SERVER-NUMREQC_MIN

3018: NUMCONV

SUMMARY:	Number of conversations that are open
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 5 conversations per minute. This threshold specifies the maximum number of open conversations the server can participate in simultaneously. A threshold violation indicates that there are too many open conversions, which means that too many internal Tuxedo resources are being used. This situation can prevent additional clients from communicating with the server and can decrease the server's throughput.

RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of open conversations does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_SERVER-NUMCONV

3019: NUMREQ

SUMMARY:	Number of open asynchronous requests
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 10 open requests • Critical: more than 15 open requests This threshold specifies the maximum number of asynchronous requests the server can handle. A threshold violation indicates that there are too many asynchronous requests, which means that too many internal Tuxedo resources are being used. This situation prevents additional clients and servers from communicating with the server until the server processes and closes a request.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of asynchronous requests does not degrade system performance, the server can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the server.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Fault
POLICY:	T_SERVER-NUMREQ

T_CLIENT Metrics

4001: STATE

SUMMARY:	Client state
SEVERITY:	Critical
DESCRIPTION:	The default threshold is 0 (inactive). This threshold specifies an unacceptable client state. A threshold violation indicates that the client was abnormally disconnected from a server. It can be difficult to determine why this problem occurred. The reasons can range from a bug in the code to an unexpected input from a user.
RECOMMENDATION:	• If the client is an interactive client that communicates with the user, discuss the problem with the development team. • If the client is a batch program that feeds data into the system, ask the development team to check the client code and data input for abnormalities.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Fault
POLICY:	T_CLIENT-STATE

4002: IDLETIME

SUMMARY:	Client idle time, which is the time during which the client is connected to the Tuxedo domain but not communicating with it. During client idle time, the client uses resources that other clients or servers might need.
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 60 minutes. This threshold specifies the maximum client idle time. A threshold violation indicates that the client is hogging resources that could be used by other clients or servers.

RECOMMENDATION: Disconnect the client by doing one of the following:

- Ask the user to disconnect.
- Use operating system utilities to disconnect the client.

DEFAULT INTERVAL: Every 15 minutes

MONITORING TYPE: Capacity

POLICY: T_CLIENT-IDLETIME

4003: NUMCONV_MIN

SUMMARY:	Number of conversations per minute
SEVERITY:	Critical
DESCRIPTION:	The default threshold is more than 20 conversations per minute. This threshold specifies the maximum number of conversations the client can open per minute. A threshold violation indicates that the client is opening so many conversations that it might be creating unnecessary internal processing that delays normal processing.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of open conversations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMCONV_MIN

4004: NUMDEQUEUE_MIN

SUMMARY:	Number of dequeue operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 100 operations per minute. This threshold specifies the maximum number of dequeue operations the client can perform per minute. A threshold violation indicates that the client is performing a high number of dequeue operations, which can cause disk I/O operations to become necessary. This situation can degrade the system performance.

RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of dequeue operations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMDEQUEUE_MIN

4005: NUMENQUEUE_MIN

SUMMARY:	Number of enqueue operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 100 operations per minute. This threshold specifies the maximum number of enqueue operations the client can perform per minute. A threshold violation indicates that the client is performing a high number of enqueue operations, which can cause disk I/O operations to become necessary. This situation can degrade the system performance.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of enqueue operations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMENQUEUE_MIN

4006: NUMPOST_MIN

SUMMARY:	Number of post operations per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 50 operations per minute. This threshold specifies the maximum number of post operations the client can perform per minute. A threshold violation indicates that the client is performing a high number of post operations, which can cause the system load to become excessively high.

RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of post operations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMPOST_MIN

4007: NUMREQ_MIN

SUMMARY:	Number of requests per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 150 requests per minute. This threshold specifies the maximum number of requests the client can initiate per minute. A threshold violation indicates that the client is initiating a high number of requests, which can cause the system load to become excessively high.
RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of requests does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMREQ_MIN

4008: NUMSUBSCRIBE_MIN

SUMMARY:	Number of subscribe operations per minute
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 20 subscriptions per minute • Critical: more than 50 subscriptions per minute This threshold specifies the maximum number of subscribe operations the client can initiate per minute. A threshold violation indicates that the client is initiating a high number of subscribe operations, which can cause disk I/O operations to become necessary. This situation can degrade the system performance.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of subscribe operations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMSUBSCRIBE_MIN

4009: NUMTRAN_MIN

SUMMARY:	Number of transactions per minute
SEVERITY:	Warning
DESCRIPTION:	The default threshold is more than 1000 transactions per minute. This threshold specifies the maximum number of transactions the client can initiate per minute. A threshold violation indicates that the client is initiating a high number of transactions, which can cause the system load to become excessively high.

RECOMMENDATION:	Check the operating system and Tuxedo system values for CPU load, disk I/O operations, and outstanding messages in the IPC queues. As long as a high number of transactions does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMTRAN_MIN

4010: PCT_TRANABT

SUMMARY:	Percentage of transactions that were aborted
SEVERITY:	Critical
DESCRIPTION:	The default threshold is more than 5 percent. This threshold specifies the maximum percentage of transactions that the client can abort. A threshold violation indicates that one or both of the following situations occurred: • The client needed to abort transactions because the transactions returned unexpected results. • The Tuxedo system forced the client to abort transactions because problems occurred between the server and the database or between the Transaction Management Server (TMS) and the database.
RECOMMENDATION:	• Make sure that the database and all servers connected to the database are running. • Check the Tuxedo ULOG file for problems that the servers reported. • If no problems were reported, check the business logic in your server, which might indicate inconsistent or unexpected data from the database.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Fault
POLICY:	T_CLIENT-PCT_TRANABT

4012: NUMUNSOL

SUMMARY:	Number of unsolicited messages in the client queue
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 5 unsolicited messages in the queue • Critical: more than 10 unsolicited messages in the queue This threshold specifies the maximum number of unsolicited messages in the client queue. A threshold violation indicates that the high number of unsolicited messages can cause the queue to fill up, which means that there would not be space for additional messages from the servers. When the queue is full, the client stores incoming message to disk or discards them.
RECOMMENDATION:	Use the ipcs command to check the space left in the queue. If the queue frequently becomes full, do one or more of the following: • Increase the queue length. • On the client, unsubscribe some of the events. • Check the configuration parameters that are related to message queuing: MSGMNB, MSGSEG, MSGSSZ, and MSGMAX. Increase these values if necessary.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_CLIENT-NUMUNSOL

4012: NUMCONV

SUMMARY:	Number of conversations that are open
SEVERITY:	Critical
DESCRIPTION:	The default threshold is more than 5 conversations per minute. This threshold specifies the maximum number of open conversations the client can participate in simultaneously. A threshold violation indicates that there are too many open conversions, which means that too many internal Tuxedo resources are being used. This situation can prevent additional clients from communicating with the server and can decrease the server's throughput.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of open conversations does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_CLIENT-NUMCONV

4013: ENCRYPTBITS

SUMMARY:	Encryption level for client connections. For secured applications, the encryption level should be at least 40.
SEVERITY:	Critical
DESCRIPTION:	The default threshold is less than 40 bytes. This threshold specifies unacceptable encryption levels. A threshold violation indicates that the client is causing a security threat to the Tuxedo domain.

RECOMMENDATION:	• Use the operating system utilities to disconnect the client. • Check the Tuxedo configuration file and ULOG file to determine why the Tuxedo system accepted the connection.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Security
POLICY:	T_CLIENT-ENCRYPTBITS

4014: NUMREQ

SUMMARY:	Number of open asynchronous requests
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 10 open requests • Critical: more than 15 open requests This threshold specifies the maximum number of asynchronous requests the client can handle. A threshold violation indicates that there are too many asynchronous requests, which means that too many internal Tuxedo resources are being used. This situation prevents additional clients and servers from communicating with the server until the client processes and closes a request.
RECOMMENDATION:	Ask the development team to review the source code. As long as a high number of asynchronous requests does not degrade system performance, the client can continue to run as is. Otherwise, use the tmshutdown or kill utilities to shut down the client.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_CLIENT-NUMREQ

T_MSG Metrics

5001: PCT_MSG_CBYTES

SUMMARY:	Percentage of used space in the server queues
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 50 percent • Critical: more than 75 percent This threshold specifies the maximum amount of used space. A threshold violation indicates that the server queues are becoming too full, which can cause the Tuxedo system to store buffers in temporary files on the disk. This situation can decrease system performance. It can also cause Tuxedo synchronous requests, asynchronous requests, and other Tuxedo ATMI calls to return error messages if the queues are full.
RECOMMENDATION:	Start additional instances of the application server to handle the load. To start a server instance, use the `boot` command in the tmadmin utility. If the Tuxedo system does not let you start additional server instances, shut down the Tuxedo system and reconfigure it by adding more servers to the *SERVERS section or by increasing MAX in the *SERVERS section. If the situation is critical, you can use the tmconfig utility to reconfigure the system online. Additionally, you can check the configuration parameters that are related to message queuing: MSGMNB, MSGSEG, MSGSSZ, and MSGMAX. Increase these values if necessary.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Capacity
POLICY:	T_MSG-PCT_MSG_CBYTES

5002: MSG_QNUM

SUMMARY:	Number of outstanding messages in the server queues
SEVERITY:	Warning or Critical
DESCRIPTION:	The default threshold is: • Warning: more than 2 messages • Critical: more than 5 messages This threshold specifies the maximum number of outstanding messages. A threshold violation indicates that the Tuxedo domain is not processing the messages fast enough, which causes clients to wait longer than necessary for results.
RECOMMENDATION:	Start additional instances of the application server to handle the load. To start a server instance, use the boot command in the tmadmin utility. If the Tuxedo system does not let you start additional server instances, shut down the Tuxedo system and reconfigure it by adding more servers to the *SERVERS section or by increasing MAX in the *SERVERS section. If the situation is critical, you can use the tmconfig utility to reconfigure the system online. Additionally, you can check the configuration parameters that are related to message queuing: MSGMNB, MSGSEG, MSGSSZ, and MSGMAX. Increase these values if necessary.
DEFAULT INTERVAL:	Every 5 minutes
MONITORING TYPE:	Performance
POLICY:	T_MSG-MSG_QNUM

5003: MSG_RTIME

SUMMARY:	Length of time, in minutes, since a message was read from a server queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 60 minutes. This threshold specifies the maximum length of time for a message to wait in a server queue. A threshold violation indicates that the Tuxedo domain is probably not using the server.
RECOMMENDATION:	Minimize the number of server instances
DEFAULT INTERVAL:	Every hour
MONITORING TYPE:	Performance
POLICY:	T_MSG-MSG_RTIME

5004: MSG_STIME

SUMMARY:	Length of time, in minutes, since a message was written to a server queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 60 minutes. This threshold specifies the maximum length of time for a server queue not to be written to. A threshold violation indicates that the Tuxedo domain is probably not using the server.
RECOMMENDATION:	Minimize the number of server instances
DEFAULT INTERVAL:	Every hour
MONITORING TYPE:	Performance
POLICY:	T_MSG-MSG_STIME

T_APPQSPACE Metrics

6001: PCT_MSG

SUMMARY:	Percentage of messages in the Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 75. This threshold specifies the maximum number of messages in the Tuxedo Application Queue space. A threshold violation indicates that percentage of messages in theTuxedo Application Queue space is increasing, which can prevent more messages from coming into queues in the Queue space.
RECOMMENDATION:	Increase the number of messages in the Queue space to accomodate more messages.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQSPACE-PCT_MSG

6002: PCT_PROC

SUMMARY:	Percentage of processes accessing Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 80. This threshold specifies the maximum number of processes in the Tuxedo Application Queue space. A threshold violation indicates that percentage of processes accessing the Application Queue space is increasing, which can prevent more processes from accessing the Queue space.
RECOMMENDATION:	Increase the number of processes in the Queue space, so that more processes can access the Queue space.

DEFAULT INTERVAL: Every 15 minutes

MONITORING TYPE: Capacity

POLICY: T_APPQSPACE-PCT_PROC

6003: PCT_QUEUES

SUMMARY:	Percentage of queues filled in the Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 80. This threshold specifies the maximum number of queues in the Tuxedo Application Queue space. A threshold violation indicates that the number of Tuxedo Application Queues is increasing. This happens when application queues are created with Tuxedo system running.
RECOMMENDATION:	Increase the number of queues in the Queue space. This condition occurs rarely.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQSPACE-PCT_QUEUES

6004: PCT_TRANS

SUMMARY:	Percentage of transactions done in the Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 80. This threshold specifies the maximum number of transactions done in the Tuxedo Application Queue space. A threshold violation indicates that a number of transactions are taking place, which can prevent other transaction from srarting.
RECOMMENDATION:	Increase the number of transactions in the Queue space, so that more transactions are possible in the Queue space.

DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQSPACE-PCT_TRANS

6005: FREE_DSK

SUMMARY:	Percentage of free disk space in the Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 40 and the reset value is 80. This threshold specifies the percentage of free disk space into the Tuxedo Application Queue space. This is a minimum threshold. A threshold violation indicates that the free disk space in the queue space is decreasing.
RECOMMENDATION:	Increase the amount of disk blocks in the queue space, so that there is enough amount of disk blocks in the queue space to hold more persistent messages.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQSPACE-FREE_DSK

6006: FREE_MEM

SUMMARY:	Percentage of free shared memory space in the Tuxedo Application Queue space
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 50 and the reset value is 85. This threshold specifies the percentage of free shared memory space into the Tuxedo Application Queue space. This is a minimum threshold. A threshold violation indicates that the shared memory space in the queue space is decreasing. This template is available for Tuxedo 7 and above only.
RECOMMENDATION:	Increase the amount of shared memory in the queue space.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQSPACE-FREE_MEM

T_APPQ Metrics

7001: CUR_MSG

SUMMARY:	Number of persistent (disk based) messages in the queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 6. The threshold specifies the number of persistent (disk based) messages in the queue. A threshold violation indicates that the number of current disk-based messages in the queue is increasing.
RECOMMENDATION:	Increase the number of messages in the Queue space to accommodate more messages.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQUEUE-CUR_MSG

7002: CUR_MEMMSG

SUMMARY:	Number of non-persistent (shared memory based) messages in the queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 3. The threshold specifies the number of non-persistent (shared memory based) messages in the queue. A threshold violation indicates that the number of current disk-based messages in the queue is increasing. This template is available for Tuxedo 7 and above only.
RECOMMENDATION:	Increase the number of messages in the Queue space to accommodate more messages.

DEFAULT INTERVAL: Every 15 minutes

MONITORING TYPE: Capacity

POLICY: T_APPQUEUE-CUR_MEMMSG

7003: CUR_BLOCKS

SUMMARY:	Number of disk pages occupied by the queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 5. The threshold specifies the number of disk pages occupied by the queue. A threshold violation indicates that the number of disk pages used by the queue is increasing. There may not be sufficient pages left for more persistent messages.
RECOMMENDATION:	If the threshold is violated frequently, do one of the following: • Create more queues using queue create in the specified Queue space and use the newly created queues in the applications. • Increase the number of disk pages allocated for the Queue space.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQUEUE-CUR_BLOCKS

7004: CUR_SHAREDMEM

SUMMARY:	Amount of shared memory (in bytes) occupied by the queue
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 5000. The threshold specifies the amount os shared memory occupied by the queue. A threshold violation indicates that the amount of shared memory blocks used by the queue is increasing. There may not be sufficient shared memory left for more non-persistent messages. This template is available for Tuxedo 7 and above only.

DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQUEUE-CUR_SHAREDMEM

7005: TOTAL_MSG

SUMMARY:	Total number of messages residing in the queue (persistent + non-persistent)
SEVERITY:	Warning
DESCRIPTION:	The default threshold is 10. The threshold specifies the total number of messages currently in the queue. A threshold violation indicates that the total number of messages currently in the queue is increasing.
RECOMMENDATION:	Increase the number of messages in the Queue space to accommodate more messages.
DEFAULT INTERVAL:	Every 15 minutes
MONITORING TYPE:	Capacity
POLICY:	T_APPQUEUE-TOTAL_MSG

T_GROUP Metrics

8001: STATE

SUMMARY:	State of the Tuxedo Server Groups
SEVERITY:	Critical or Nil
DESCRIPTION:	The default threshold is: • Critical: 1 • Nil: 2 The Critical threshold violation indicates that the state of the Tuxedo Server Groups has changed to Inactive. The Nil threshold violation indicates that the state of the Tuxedo Server Groups has changed to Migrating.
RECOMMENDATION:	• Inactive state of the Server Group indicates that T_GROUP object is defined and inactive. Check if the Tuxedo system is booted. • Migrating state of Server Group indicates that T_GROUP object is defined and currently in a state of migration to the secondary logical machine. The secondary logical machine listed in the TA_LMID does not match TA_CURLMID.
DEFAULT INTERVAL:	Every hour
MONITORING TYPE:	Fault or Normal
POLICY:	T_GROUP-STATE

7 Chapter:Tuxedo SPI Command Line Utilities

The Tuxedo SPI supports the following command line utilities in addition to other command line utilities:

- bearun
- beaDiscover
- beaDelDom
- beaEvtMon
- beaAddNodesUlogMon
- beaDelNodesUlogMon
- beaListNodesUlogMon
- beamwadatalog
- beasvdisc

You can include these utilities in scripts and programs that you create.

bearun

DESCRIPTION:	Runs the Tuxedo utilities and the Tuxedo SPI command line utilities. The bearun utility prepares the Tuxedo environment based on the specified options and invokes the specified BEA subcommand.
CALLING SEQUENCE:	`bearun [-g] [-G] [-N][-z][-G] -C "subcommand" [-d DomainID | -a | -A | -R -t TUXDIR -T TUXCONFIG] [-X "options_applied to_subcommand"]`

OPTIONS AND ARGUMENTS:	`-g, -G`
	Creates a trace file for `bearun` and the invoked command (in /tmp directory for UNIX-based platforms and in the %TEMP% directory for Windows-based platforms).
	`-d DomainID`
	Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target machine.
	Format: string up to 26 characters.
	-a
	If you use this option, all domains on the selected master machine will be affected by the command.
	-A
	If you use this option, all domains on the selected non-master machine will be affected by the command.
	`-R -t TUXDIR -T TUXCONFIG`
	Allows you to specify a Tuxedo domain with the `-t TUXDIR -T TUXCONFIG` options. *TUXDIR* is the directory on the target machine where the Tuxedo system is installed, and *TUXCONFIG* is the path and filename for the binary Tuxedo configuration file on the target machine. *TUXDIR* and *TUXCONFIG* are given in the `UBBCONFIG` file for the domain.
	-X
	You use this option to append parameters to the BEA subcommand specified by the `-C` option in the `bearun` application call.
	`-C subcommand`
	Shell script or compiled program. Typically, BEA subcommand is a Tuxedo utility or a Tuxedo SPI command line utility.

DETAILS:	This utility lets you define an action in a template. The action can be automatic or operator-initiated.
	
	For the ULOG and system event templates (TUXLOG and TUXEVT), *DomainID* is available in the OBJECT variable. To associate an action with one of these templates, set *DomainID* to $OBJECT. For example:
	
	`bearun -d $OBJECT -C subcommand`
	
	For the TMIB templates (GRPTUXMON), *DomainID* is available in the OPTION(DOMAINID) variable. To associate an action with one of these templates, set *DomainID* to $OPTION(DOMAINID). For example:
	
	`bearun -d $OPTION(DOMAINID) -C subcommand`
	
	For example, to use bearun to display the current Tuxedo configuration, define the following action:
	
	`bearun -d $OPTION(DOMAINID) -C tmunloadcf`
	
	If desired, select the annotate checkbox to annotate the command output to the message that is generated by the template.

RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • The Tuxedo SPI configuration file (beamgr.conf) is not available. • Syntax error in the calling sequence. • *DomainID* is not unique. • *TUXDIR* is not valid. • *TUXCONFIG* file is not found.

beaDiscover

DESCRIPTION:	Adds information about a Tuxedo domain to the Tuxedo SPI environment on a target master machine and any non-master machine in the domain running the Tuxedo SPI software. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -w -C "beaDiscover" -R -t` *`TUXDIR`* `-T` *`TUXCONFIG`*
OPTIONS AND ARGUMENTS:	`-R -t` *`TUXDIR`* `-T` *`TUXCONFIG`* Allows you to specify a Tuxedo domain with the `-t` *`TUXDIR`* `-T` *`TUXCONFIG`* options. *`TUXDIR`* is the directory on the target machine where the Tuxedo system is installed, and *`TUXCONFIG`* is the path and filename for the binary Tuxedo configuration file on the target machine. *`TUXDIR`* and *`TUXCONFIG`* are given in the `UBBCONFIG` file for the domain.
DETAILS:	This utility updates the Instances section in the Tuxedo SPI configuration file (`beamgr.conf`) on the target master machine and any non-master machine in the domain running the Tuxedo SPI software.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • The Tuxedo SPI configuration file (`beamgr.conf`) is not available. • Syntax error in the calling sequence. • Target node is *not* a master machine. • *`TUXDIR`* is not valid. • *`TUXCONFIG`* file is not found.

beaDelDom

DESCRIPTION:	Deletes information about a Tuxedo domain from the Tuxedo SPI environment on a target master machine and any non-master machine in the domain running the Tuxedo SPI software. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -w -N -C "beaDelDom" -X "-d DomainID"`
OPTIONS AND ARGUMENTS:	`-d DomainID` Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target master machine and any non-master machine in the domain running the Tuxedo SPI software. Format: string up to 26 characters.
DETAILS:	This utility deletes the domain from the Tuxedo SPI configuration file (beamgr.conf) on the target master machine and any non-master machine in the domain running the Tuxedo SPI software.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • The Tuxedo SPI configuration file (beamgr.conf) is not available. • Syntax error in the calling sequence. • Target node is *not* a master machine. • *DomainID* is not unique. • *TUXDIR* is not valid. • *TUXCONFIG* file is not found.

beaEvtMon

DESCRIPTION:	Starts and stops system event monitoring for a Tuxedo domain and shows system event monitoring status for a domain. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -C "beaEvtMon" {-d` *`DomainID`* `| -a | -A | -R -t` *`TUXDIR`* `-T` *`TUXCONFIG`*`} -X [status | start | stop]`
OPTIONS AND ARGUMENTS:	`-d` *`DomainID`* Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target master machine. Format: string up to 26 characters. -a If you use this option, all domains on the selected master machine will be affected by the command. -A If you use this option, all domains on the selected non-master machine will be affected by the command. `-R -t` *`TUXDIR`* `-T` *`TUXCONFIG`* Allows you to specify a Tuxedo domain with the `-t` *`TUXDIR`* `-T` *`TUXCONFIG`* options. *`TUXDIR`* is the directory on the target machine where the Tuxedo system is installed, and *`TUXCONFIG`* is the path and filename for the binary Tuxedo configuration file on the target machine. *`TUXDIR`* and *`TUXCONFIG`* are given in the `UBBCONFIG` file for the domain. -X You use this option to append parameter status, start, or stop to the BEA subcommand beaEvtMon. The default is status.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *`DomainID`* is not unique. • *`TUXDIR`* is not valid. • *`TUXCONFIG`* is not found.

beaAddNodesUlogMon

DESCRIPTION:	Starts ULOG monitoring on one or machines in a Tuxedo domain. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -C "beaAddNodesUlogMon" {-d` *`DomainID`* `| -a | -A} -X "{`*`LMID_1`* `... [`*`LMID_N`*`] | all}"`
OPTIONS AND ARGUMENTS:	`-d` *`DomainID`* Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target master machine. Format: string up to 26 characters. -a If you use this option, all domains on the selected master machine will be affected by the command. -A If you use this option, all domains on the selected non-master machine will be affected by the command. -X You use this option to append one or more logical machine IDs (LMIDs) or `all` to the BEA subcommand `beaAddNodesUlogMon`. The LMIDs for a Tuxedo domain are given in the `UBBCONFIG` file for the domain.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *`DomainID`* is not unique. • *`TUXDIR`* is not valid. • *`TUXCONFIG`* file is not found.

beaDelNodesUlogMon

DESCRIPTION:	Stops ULOG monitoring on one or more machines in a Tuxedo domain. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -C "beaDelNodesUlogMon" {-d` *`DomainID`*`| -a | -A} -X "{`*`LMID_1`* `...` `[`*`LMID_N`*`] | all}"`
OPTIONS AND ARGUMENTS:	`-d` *`DomainID`* Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target master machine. Format: string up to 26 characters. -a If you use this option, all domains on the selected master machine will be affected by the command. -A If you use this option, all domains on the selected non-master machine will be affected by the command. -X You use this option to append one or more logical machine IDs (LMIDs) or `all` to the BEA subcommand `beaDelNodesUlogMon`. The LMIDs for a Tuxedo domain are given in the `UBBCONFIG` file for the domain.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *`DomainID`* is not unique. • *`TUXDIR`* is not valid. • *`TUXCONFIG`* file is not found.

beaListNodesUlogMon

DESCRIPTION:	Shows ULOG monitoring for the machines in a Tuxedo domain. You can run this command *only* on a master machine.
CALLING SEQUENCE:	`bearun -C "beaListNodesUlogMon" {-d DomainID | -a | -A}`
OPTIONS AND ARGUMENTS:	`-d DomainID` Identification string for the domain as given in the `UBBCONFIG` file for the domain. This value enables the Tuxedo SPI to identify the domain on the target master machine. Format: string up to 26 characters. -a If you use this option, all domains on the selected master machine will be affected by the command. -A If you use this option, all domains on the selected non-master machine will be affected by the command.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *DomainID* is not unique. • *TUXDIR* is not valid. • *TUXCONFIG* file is not found.

beamwadatalog

DESCRIPTION:	Logs Tuxedo system data and application data into configured datasources in OVPA or CODA.
CALLING SEQUENCE:	`bearun -a -C "beamwadatalog"`
OPTIONS AND ARGUMENTS:	-a If you use this option, all domains on the selected master machine will be affected by the command. -C Signifies a BEA subcommand (enclosed in quotation marks) that appears immediately after this option.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *TUXDIR* is not valid. • *TUXCONFIG* file is not found. • Unable to connect to Tuxedo system. • Data collection fails due to invalid metric ID. • The Tuxedo SPI configuration file, beamgr.conf is not available.

beasvdisc

DESCRIPTION:	Constructs the service XML that is given to the OVO service discovery framework. The discovery framework will add this service XML into the existing model so that Tuxedo service map is displayed on the java console.
CALLING SEQUENCE:	`bearun -A -C "beasvdisc"`
OPTIONS AND ARGUMENTS:	-A If you use this option, all domains on the selected non-master machine will be affected by the command. -C Signifies a BEA subcommand (enclosed in quotation marks) that appears immediately after this option.
RETURN VALUE:	This utility returns a non-zero value if one of the following errors occurs: • Syntax error in the calling sequence. • Target node is *not* a master machine. • *TUXDIR* is not valid. • *TUXCONFIG* file is not found. • Unable to connect to Tuxedo system. • Data collection fails due to invalid metric ID. • The Tuxedo SPI configuration file, beamgr.conf is not available.

Index

E

F

G

I

M

N

O

P

R

S

T

U

W