Timeout Settings PeopleSoft 8.48

ORACLE | PeopleSoft.

Jim Pastorino, Oracle Technical Support, February 2007.

TABLE OF CONTENTS

OVERVIEW

Timeout Settings

Because there are numerous components involved when deploying PeopleSoft applications to a browser transaction, setting timeout intervals involves setting configuration parameters at multiple levels. For instance, you need to set the timeout values at both the web server and the application server level.

The topics in this section describe the following information for setting the timeout values at each level, from the browser to the database.

General Rule to Follow for PIA Timeout Settings

The general rule to follow would be that the timeout values increase as you get farther from the servers. Draw a diagram so it is easier to see. The farthest (and thus, longest timeout) would be Load Balancer/Proxy/Firewall, followed by the browser (webprofile - session.timeout and session.warning; the user timeout will also be set to this value), followed by the tuxedo receive timeout in the webprofile, followed by the Jolt Client Cleanup timeout, followed by the application server service timeouts for the PS processes, followed by the database. You don't want to have one expire higher up the chain, because threads will then be left processing farther down the line.

TIMEOUT DEFINITIONS

The following tables document the timeout settings that appear throughout PeopleTools 8.48.

WEB SERVER			
Timeout Setting	Location	Description	Shipped Default
session-timeout	web.xml (specific location of file dependent upon web server vendor)	Determines the time period that can elapse before the web server (WebLogic or WebSphere) will remove the HttpSession. This is akin to an *abandoned session cleanup timeout*. **If this value is set less than the sessionTimeout in your webprofile it will not result in the termination of the user's online session. The HttpSession will be removed but the user's session will remain valid due to the presence of cookie in the user's browser. Adjusting this setting will affect the user by causing their state (which is stored in the HttpSession) to be lost.** **If this setting is too high it will affect resource utilization on the web server.** **Ideally the value of this setting will be the same as the sessionTimeout in your webprofile. This will prevent state loss AND dangling HttpSessions on the web server.**	20 mins
Timeout	Httpd.conf Apache OAS	The amount of time that the server will wait for receipts and transmissions during communications. Timeout should be set to the same value specified for the Tuxedo Receive Timeout in your Webprofile.	300 Seconds

APPLICATION SERVER			
Timeout Setting	Location	Description	Shipped Default
JOLT Listener / Client Cleanup Timeout	psappsrv.cfg	The inactive interval permitted for the server-side JoltSession. Raising this value can keep unnecessary server-side resources allocated. Setting this value too low can cause the reinstantiation of resources for a client who has surpassed their inactivity interval. **Note: this value will not affect the user experience; it has a server side performance impact. Evidence has come to light that an optimal value for this setting is 5 - 10 minutes. This setting should be set slightly higher than any of the PS processes for your domain, i.e. PSAPPSRV, PSQRYSRV.**	10 mins
JOLT Listener / Init Timeout	psappsrv.cfg	The amount of time allowed for the JSL process to start. **It is not necessary to adjust this setting.**	5 mins
Workstation Listener / Client Cleanup Timeout	psappsrv.cfg	The inactive interval permitted for the server-side Workstation Listener Session. **Raising this value can keep unnecessary server-side resources allocated. Setting this value can cause the re-instantiation of resources for a client who has surpassed their inactivity interval.** **Note: this value is only required for three-tier connections. It does not affect PIA users.**	60 mins
Workstation Listener / Init Timeout	psappsrv.cfg	The amount of time allowed for the WSL process to start. **Note: this value is only required for three-tier connections.**	5 mins

		The customer should not adjust this setting.	
Domain Settings / Spawn Threshold	psappsrv.cfg	This is the rate at which PSAPPSRV processes will spawn and decay. The last two digits determine the spawn ratio. The first two digits determine the decay ratio. Using the default value as an example, we see that an extra PSAPPSRV process will be spawned if there is at least 1 outstanding service request on the Application Server request queue for one second or more. This spawning will continue until Max Instances is reached. For the decay rate of 1, 600, if less than 1 service request is on the Application Server request queue for ten minutes (600 seconds), a server process is decayed. **Note: This value is only relevant if PSAPPSRV / Max instances > PSAPPSRV / Min Instances.**	1,600:1,1
For each server process / Service Timeout	psappsrv.cfg	The time period permitted for the service to run in the process in question. If the service has not completed within the allotted time period Tuxedo will terminate the server processing being run and then restart the server process. **This value should be set to the longest that any service is expected to take for that particular server.**	**Different value per server** PSAPPSRV: 300 secs (5 mins) PSSAMSRV: 300 secs PSQCKSRV: 300 secs PSQRYSRV: 1200 secs (20 mins) PSBRKHND_dflt: 1200 secs PSSUBHND_dflt: 1200 secs PSPUBHND_dflt: 1200 secs A value of 0 will infer an infinite timeout on any service. This is the setting that most of the internal developer templates assume.

If using PUBSUB PSBRKDSP_dflt / Restart Period PSSUBDSP_dflt / Restart Period PSPUBDSP_dflt / Restart Period	psappsrv.cfg	Refers to how long the dispatcher will wait before re-dispatching a message if the associated handler has not started processing it.	120 secs
If using ACE (Analytic Calculation Engine) PSANALYTICSRV/ Analytic Instance Idle Timeout	psappsrv.cfg	Number of minutes an analytic instance will remain loaded without being accessed when it is auto-loaded by the analytic grid or when a PeopleCode program loads the instance with a timeout value of -1. Setting this to zero will disable timeouts for auto-loaded instances.	30 mins
TM_RESTARTSRV TIMEOUT	psappsrv.ubx (and then UBBGENned[1] into psappsrv.env)	The time period that a domain server process PSAPPSRV, PSWATCHSRV, PSSAMSRV etc, is allowed to remain in Restarting mode before it is killed by the BBL. This was intended to resolve processes hanging during restart. This setting is defaulted in the $PS_HOME/appserv/*.UBX files. **If this value needs to change, you must change the value in the UBX template file and then recreate your domain.**	60 secs

[1] Configurable settings for the Application Server require modification through domain configuration within psadmin.

PROCESS SCHEDULER			
Timeout Setting	Location	Description	Shipped Default
Process Scheduler / Reconnection Interval	psprcs.cfg	Interval in seconds between attempts to reconnect to database when the connection is lost.	300 secs
Process Scheduler / Authentication Timeout	psprcs.cfg	This parameter indicates the duration in minutes allotted before PeopleTools' security module will timeout authenticating a process released by Process Scheduler. The timer starts from the time Process Scheduler initiates the request	5 mins
Tuxedo Settings/ Spawn Threshold	psprcs.cfg	This is the rate at which the Distribution Server processes will spawn and decay. The last two digits determine the spawn ratio. The first two digits determine the decay ratio. Using the default value as an example, we see that an extra PSDSTSRV process will be spawned if there is at least 1 outstanding service request on the request queue (queue named 'base') for one second or more. This spawning will continue until Max Instances is reached. For the decay rate of 1, 600, if less than 1 service request is on the request queue for ten minutes (600 seconds), a server process is decayed. **Note: This value is only relevant if PSDSTSRV / Max instances > PSDSTSRV / Min Instances.**	1,600:1,1
RemoteCall / RCCBL Timeout	psprcs.cfg	This parameter indicates the duration in seconds to run a Remote Call within an Application Engine program before it is terminated.	300 secs

All configurable settings for the Process Scheduler require modification through domain configuration within psadmin.

SEARCH SERVER			
Timeout Setting	Location	Description	Shipped Default
Domain Settings / Spawn Threshold	pssrchsrv.cfg	This is the rate at which PSSRCHSRV processes will spawn and decay. Last two digits determine the spawn ratio. The first two digits determine the decay ratio. Using the default value as an example, we see that an extra PSSRCHSRV process will be spawned if there is at least 1 outstanding service request on the request queue for one second or more. This spawning will continue until Max Instances is reached. For the decay rate of 1, 600, if less than 1 service request is on the request queue for ten minutes (600 seconds), a server process is decayed. **Note: This value is only relevant if PSSRCHSRV / Max instances > PSSRCHSRV / Min Instances.**	1,600:1,1
PSSRCHSRV / Service Timeout	pssrchsrv.cfg	This parameter indicates the duration in seconds to run a Search service within a Search domain.	300 secs
TM_RESTARTSRVTIMEOUT	pssrchsrv.ubx (and then UBBGENned into pssrchsrv.env)	The time period that a domain server process PSSRCHSRV, is allowed to remain in Restarting mode before it is killed by the BBL. This was intended to resolve processes hanging during restart. This setting is defaulted in the $PS_HOME/appserv/Search/*.UBX files. **If this value needs to change, you must change the value in the UBX template file and then recreate your domain.**	60 secs

All configurable settings for the Search Server require modification through domain configuration within psadmin.

Most of the following values formerly resided on the web Server for PeopleTools 8.1x in the configuration.properties file. These settings are now stored on the database and primarily accessible from PIA. The specific profile type is prompted during the PIA installation but can be changed directly after the PIA installation by editing the configuration.properties file on your web server.

Profiles include

- DEV: standard developer options
- TEST: standard testing options
- PROD: standard production options
- KIOSK: like PROD but has additional settings relevant to KIOSK usage
- STANDALONE:

WEB PROFILE			
Setting	Navigation Route	Description	Shipped Default
Inactivity Warning (authenticated users)	PeopleTools->Web Profile->Web Profile Configuration->Security	Specify the number of seconds the portal should wait before warning users that their browser session is about to expire. They have the option of continuing with their current session by clicking the OK button in the warning message. If a user doesn't respond, the session ends and the expired connection page appears. The default value of this field is 1080 seconds. (18 minutes)	All profiles: 1080 secs
Inactivity Logout (authenticated users)		Specify the value in seconds of the inactivity timeout interval that applies to the PeopleSoft application for which the user is currently authenticated. When the interval passes with no user activity, the user's browser displays the page specified by the Expire Page - Page field on the Web Profile Configuration - Look and Feel page. Note: Depending on the application implementation, authenticated users might also experience an HTTP session inactivity timeout; see the authUserHttpInterval set in the Custom Properties (for 8.44) for further discussion.	All profiles: 1200 secs
HTTP Session Inactivity (authenticated users)		This is the authenticated user equivalent of the public user's http interval on the security page. If not set, the http interval for an authenticated user is the same value as the inactivity logout. It is specified in seconds	All profiles: 0 secs
HTTP Session Inactivity (Public		Unlike Authenticated Users, Public users are not logged out of their	DEV, KIOSK profile: 1200 secs

Users)		PeopleSoft application after an interval of time. But this field specifies the interval of inactivity after which time the web server will release their HTTP session. This will cause PIA to release their application states from memory. If the user takes another link they will regain access to the application at the search dialog. This setting prevents an overload of web server resources for inactive public users.	TEST, PROD, STANDALONE profiles: not set
Disconnect Timeout		This means that the client connection must be retained throughout the session. If the connection becomes invalid (due to one of the other timeouts) the session will be expired. Note: If 0 is specified, the Jolt client attempts to connect the Jolt Server Handler in RETAINED mode. If > 0 is specified, the Jolt client attempts to connect JSH in RECONNECT mode.	All profiles: 0
Send Timeout		This is the number of seconds that is permitted to elapse between the sending of the Jolt Request from the client (servlet) and its full receipt on the application server. **This could require an increase in value where a large amount of data is being sent to the application server and/or the network is slow.**	All profiles: 50 secs
Receive Timeout		The amount of time permitted to elapse between the issue of a Jolt Request from the client (servlet) and the arrival of the ensuing response from the application server. **This value should be set equal or greater than the maximum online service timeout value on the application server. This**	All profiles: 600 secs

		value should be considerably larger than the tuxedo_send_timeout **above.** **Ideally this timeout would also be greater than the SANITY SCAN (BLOCKTIME * SCANUNIT). ICE Report 691739000 has been opened to address this issue.**	

OTHER SETTINGS THROUGH PIA

A number of additional timeouts may be set through PIA. These setting reflect changes at the database level that may pertain to different groups of users.

Setting	Navigation Route	Description	Shipped Default
PS TOKEN	PeopleTools->Security->Security Objects->Single Signon	Defines the time window of a token over which a system (database) will trust a single signon token from the same or another content provider. **Note: As long as a user remains signed on, the expiration of the PS Token will not impact the user in any way. In other words this is only relevant during the GetCertificate request during Single Signon.**	720 minutes (12 hours)
Permission List	PeopleTools->Security->Permissions & Roles->Permission Lists	The administrator may select the appropriate permission list and apply a customized timeout. For a chosen permission list the administrator may elect to never time out or to timeout after a specific time period. **Note: If a user belongs to multiple permission lists, the largest value of those candidate permission lists is applied to the user's session during signon. The permission list timeout is only effective if it's value is *less* than that configured on the web server (see session timeouts on the Web Server tab). This implies that all of the permission list timeouts for a particular user must be less than the session Timeout on the web server to be affective.** **Finally, if the permission list timeout is successful in overriding the session timeout on the web server it *will not* affect the warningTimeout.**	0 (No timeout)

WEB SERVER FILE LOCATIONS

APACHE

- Httpd.conf

<APACHE_HOME/Apache/conf

ORACLE APPLICATION SERVER

- configuration.properties

<OAS_Home>/j2ee/PIA_DOMAIN/applications/<PIA_SITE>/PORTAL/WEB-INF/psftdocs/<PIA_SITE>

- web.xml

<OAS_Home>/j2ee/PIA_DOMAIN/applications/<PIA_SITE>/PORTAL/WEB-INF

- httpd.conf

<OAS_Home>/Apache/Apache/conf

WEBLOGIC

- configuration.properties file

<PS_HOME>/webserv/<DOMAIN-NAME>/applications/peoplesoft/PORTAL/WEB-INF/psftdocs/<PIASITE>

- web.xml

<PS_HOME>/webserv/<DOMAIN-NAME>/applications/peoplesoft/PORTAL/WEB-INF

WEBSPHERE

- configuration.properties

<PS_HOME>/webserv/MACHINENode_MACHINENode_SERVER_NAME1/peoplesoft.ear/PORTAL/WEB-INF/psftdocs/<PIA_SITE>

- web.xml

<PS_HOME>/webserv/MACHINENode_MACHINENode_SERVER_NAME1/peoplesoft.ear/PORTAL/WEB-INF