Database sessions: Session temporarily lost during update (critical race condition in write) | Tiki Wiki CMS Groupware :: Development
Database sessions: Session temporarily lost during update (critical race condition in write)

Status
Open

Subject
Database sessions: Session temporarily lost during update (critical race condition in write)

Version
15.x
18.x

Category
- Regression

Resolution status
New

Submitted by
Philippe Cloutier

Volunteered to solve
Victor Emanouilov

Keep informed
Marc Laporte

Lastmod by
Philippe Cloutier

Rating
★★★★★ (0)

Description
When the session_storage preference is set to Database, some requests can misbehave due to a critical section in tikisession-pdo.php. This happens during concurrent requests, when one request is in the middle of a call to Session::write(). write() executes 2 queries, one which deletes the session (if it exists), and one which (re)creates the session. When write() is blocked between these 2 requests, 2 critical race conditions can occur. Assuming a first request is in between these 2 queries:

1. If request #2 concurrently reads the sessions table, it will fail to find the session, causing Zend\Session\Container::getDefaultManager()->start() (in tiki-setup_base.php) to start a new session instead of resuming the session. This will cause:
    1. A multiplication of entries in the sessions table
    2. PHPSESSID to change unduly
    3. A loss of session data (in practice)
    4. The message "session cookie validation failed" to be logged in the system log.
2. If the first race condition does not occur, but request #2 executes the DELETE in write() before request #1 has re-inserted the row, then whichever request finishes write() last will fail, due to an attempt to insert an existing row (the message will look like "Duplicate entry 'glmk0tl75dmi9rrkdfbgt7mr47' for key 'PRIMARY'").

Symptoms

Images not displaying

This can be seen easily in a custom blog based on a wiki page in our Foncierpedia website. That page uses the LIST plugin to display posts with the author's avatar. Each time the page is loaded, there is one request to tiki-show_user_avatar.php per author, which redirects via HTTP 302 to tiki-download_file.php. The page currently has posts from 6 authors, so each load causes at least 6 requests using tiki-setup_base.php approximately simultaneously. In this context, the bug is very often visible, roughly 1 load every 5. To make it even more obvious, the critical section can be lengthened by calling sleep(2) between the 2 SQL queries in write(). With that, we see the bug almost on each load of the wiki page. The main symptom is that some images fail to display, due to race condition #2. This is very easy to reproduce with Tiki 15, since avatars are not cached, but in Tiki 18, tiki-show_user_avatar.php can return a 304 Not Modified, so if this doesn't reproduce on the first attempt, a full reload will be needed (Ctrl+F5 in Firefox).

This can also be reproduced with a wiki page which simply calls the IMG plugin. I used the following:

```
{img src="tiki-download_file.php?fileId=6818&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=5810&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=5152&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=6974&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=5800&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=6889&amp;display=y" width="100px"} {img src="tiki-download_file.php?fileId=7052&amp;display=y" width="100px"}
```

Other

We are also experiencing abnormal user disconnections on the site. These are harder to reproduce, but likely related.
Related commit: r45249

Logs

There are multiple messages in the actionlog. A query like the following can help see the pattern:

```
SELECT FROM_UNIXTIME(lastModif), `tiki_actionlog`.* FROM `tiki_actionlog` ORDER BY ip, lastModif
```

Related commit: r56775

Source

This is a regression from r24568.

Solution

A patch for Tiki 15 is attached.

Importance

7

Easy to solve?

8

Priority
56

Demonstrate Bug (Tiki 19+)
Please demonstrate your bug on show2.tiki.org

Version: trunk ▼

Demonstrate Bug (older Tiki versions)

Ticket ID
6911

Created
Friday 09 November, 2018 21:41:58 GMT-0000
by Philippe Cloutier

LastModif
Wednesday 14 November, 2018 20:13:11 GMT-0000

Comments

Marc Laporte 09 Nov 18 21:49 GMT-0000

Wow!

This is some impressive detective work. Well done!

Philippe Cloutier 09 Nov 18 21:52 GMT-0000

I have a solution ready for this. Will submit a patch next week.

Philippe Cloutier 13 Nov 18 17:39 GMT-0000

This was previously reported by Eduard González Massot on tikiwiki-users in thread "Error loading images".

Relevant commit about unexplained logouts: https://sourceforge.net/p/tikiwiki/code/45249
Commit adding debug information: https://sourceforge.net/p/tikiwiki/code/56775

Attachments

filename	created	hits	comment	version	filetype

session_write_race_condition_fix.diff	13 Nov 18 14:35 GMT-0000	0	

The original document is available at https://dev.tiki.org/item6911-Database-sessions-Session-temporarily-lost-during-update-critical-race-condition-in-write