Redmine - Feature #29041

Update session token only once per minute

2018-06-17 19:57 - Pavel Rosický

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Performance	**Estimated time:**	0.00 hour
Target version:	5.0.0		
Resolution:	Fixed		

Description

this is simmilar to #28952

if Rails.application.config.redmine_verify_sessions is enabled, basically each read request triggers an update to tokens table. This is bad for performance because it blocks the database.
My patch transforms the update query into a select query that doesn't block on heavy load. We could actually update the token only once per hour which is the minimum available setting for Setting.session_lifetime and Setting.session_timeout, but redmine modifications could use smaller values, so I choose 1 minute interval. Smaller session_timeout then 1 minute won't work now, but I think such small timeout doesn't make much sense.

Related issues:

Related to Redmine - Feature #28952: Update User#last_login_on only once per ...	**Closed**

Associated revisions

Revision 21376 - 2022-01-22 05:04 - Go MAEDA

Update session token only once per minute (#29041).

Patch by Pavel Rosický.

History

#1 - 2018-06-17 20:43 - Marius BĂLTEANU

- Related to Feature #28952: Update User#last_login_on only once per minute added

#2 - 2018-06-18 11:06 - Pavel Rosický

- File user.rb.patch added

#3 - 2018-11-08 19:28 - Pavel Rosický

ping Marius BALTEANU

#4 - 2018-11-10 08:45 - Marius BĂLTEANU

Pavel Rosický wrote:

> ping Marius BALTEANU

Pong. I've missed something?

#5 - 2018-12-01 18:54 - Pavel Rosický

if you have time, could you review? https://www.redmine.org/attachments/20901/user.rb.patch

GET requests shouldn't update a database all the time. It's even more relevant for #29513

disabling Rails.application.config.redmine_verify_sessions isn't an option because it makes Redmine vulnerable

are there any security concerns about this change?

#6 - 2022-01-20 08:29 - Go MAEDA

- File 29041.patch added

- Target version set to Candidate for next major release

Combined user.rb.patch and sessions_controller_test.rb.patch.

#7 - 2022-01-20 15:35 - Holger Just

I support the approach to reduce write traffic to the database. With this patch, the write contention on the tokens table and the Redmine database in general should be reduced quite a bit.

At first, I though that we would need to check whether we have only one valid token for the maximum query too. Turns out that there is a unique index on the tokens.value column in the database. As such, we are guaranteed to have only exactly zero or one token with a given value in the database. As both of these cases are checked by the patch, I think it should be fine and as secure as the previous version.

The slight reduction in accuracy is acceptable as the value is only used for session expiration where the difference of at most one minute is negligible. Enforcing session timeouts of less than one minute is not useful and does not need to be supported as it would effectively reduce the session to be only useful for (more-or-less) a single request.

#8 - 2022-01-21 01:10 - Go MAEDA

- Target version changed from Candidate for next major release to 5.0.0

Setting the target version to 5.0.0.

#9 - 2022-01-22 05:04 - Go MAEDA

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch. Thank you.

Files

user.rb.patch	644 Bytes	2018-06-17	Pavel Rosický
sessions_controller_test.rb.patch	865 Bytes	2018-06-17	Pavel Rosický
user.rb.patch	665 Bytes	2018-06-18	Pavel Rosický
29041.patch	1.64 KB	2022-01-20	Go MAEDA