Redmine - Patch #35217

Replace use of Digest::MD5 / Digest::SHA1 with ActiveSupport::Digest

2021-05-07 05:02 - Jens Krämer

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BĂLTEANU	**% Done:**	0%
Category:	Code cleanup/refactoring	**Estimated time:**	0.00 hour
Target version:	6.0.0		

Description

Rails introduced ActiveSupport::Digest to allow central configuration of the actual digest implementation that is used throughout Rails. This is helpful in environments where certain digest implementations (most notably, MD5) are not available, i.e. to be FIPS compliant.

The attached patch replaces all uses of Digest::SHA1 and Digest::MD5 with ActiveSupport::Digest. Without further configuration, this will result in Digest::SHA1 being used in all these instances since that's the current Rails default. This can be changed by users via the config.active_support.hash_digest_class setting , i.e.:

```
Rails.application.config.active_support.hash_digest_class = OpenSSL::Digest::SHA256
```

Related issues:

Related to Redmine - Patch #40652: Replace MD5 with SHA256 when creating the ... **Closed**

Associated revisions

Revision 22816 - 2024-05-07 20:36 - Marius BĂLTEANU

Replaces use of Digest::MD5 / Digest::SHA1 with ActiveSupport::Digest (#35217).

Patch by Jens Krämer (@jkraemer).

History

#1 - 2021-05-07 15:14 - Pavel Rosický

thanks for working on this!

however, the OpenID change isn't safe. The SHA1 algorithm is hardcoded here and your change will break it.
https://github.com/redmine/redmine/blob/49e323ae7af2998fc2785319643a9ac5bc93c425/lib/plugins/open_id_authentication/test/mem_cache_store_test.rb#L126

https://github.com/openid/ruby-openid do support SHA256, maybe add an option to choose it? It has to be a separate option, it can't depend on Rails.application.config.active_support.hash_digest_class

the second missing part is gravatars https://github.com/redmine/redmine/blob/master/lib/plugins/gravatar/lib/gravatar.rb#L68
as discussed in https://www.redmine.org/boards/2/topics/65253 I don't think there's a way to support this feature without MD5, so if the digest isn't available, the feature has to be disabled.

#2 - 2024-05-01 10:13 - Marius BĂLTEANU

Pavel Rosický wrote in #note-1:

> thanks for working on this!
>
> however, the OpenID change isn't safe. The SHA1 algorithm is hardcoded here and your change will break it.
> https://github.com/redmine/redmine/blob/49e323ae7af2998fc2785319643a9ac5bc93c425/lib/plugins/open_id_authentication/test/mem_cache_store_test.rb#L126
>
> https://github.com/openid/ruby-openid do support SHA256, maybe add an option to choose it? It has to be a separate option, it can't depend on Rails.application.config.active_support.hash_digest_class

The openid plugin was removed so these issues are no longer available.

> the second missing part is gravatars https://github.com/redmine/redmine/blob/master/lib/plugins/gravatar/lib/gravatar.rb#L68
> as discussed in https://www.redmine.org/boards/2/topics/65253 I don't think there's a way to support this feature without MD5, so if the digest isn't available, the feature has to be disabled.

It seems that gravatar supports now also SHA256: https://docs.gravatar.com/avatars/hash/.

Should we take this change into consideration for 6.0.0? Jens, do you have any updated patch?

#3 - 2024-05-02 06:24 - Jens Krämer

I would suggest to just swap out MD5 for SHA256 for the Gravatar use case. It seems not practical to tie this to the hash_digest_class configuration, so let's just hard code the algorithm suggested by the Gravatar docs here.

#4 - 2024-05-02 17:06 - Marius BĂLTEANU

Jens Krämer wrote in #note-3:

> I would suggest to just swap out MD5 for SHA256 for the Gravatar use case. It seems not practical to tie this to the hash_digest_class configuration, so let's just hard code the algorithm suggested by the Gravatar docs here.

Agree, I've posted the patch in #40652.

#5 - 2024-05-02 19:14 - Pavel Rosický

yeah, it looks like https://www.gravatar.com does support SHA256 now, it wasn't supported at the time when I wrote the comment (3 years ago)

no other objections then :)

#6 - 2024-05-02 22:21 - Marius BĂLTEANU

- Related to Patch #40652: Replace MD5 with SHA256 when creating the hash for gravatar URL added

#7 - 2024-05-02 22:23 - Marius BĂLTEANU

- Assignee set to Marius BĂLTEANU

- Target version set to 6.0.0

#8 - 2024-05-07 20:37 - Marius BĂLTEANU

- Category set to Code cleanup/refactoring

- Status changed from New to Closed

Patch committed, thanks Jens, Pavel!

Files

0001-replaces-uses-of-Digest-MD5-and-Digest-SHA1-with-AS-.patch	11.1 KB	2021-05-07	Jens Krämer