Redmine - Defect #5976

Uniqueness of User model fields is not checked sufficiently

2010-07-27 19:14 - Holger Just

Status:	Confirmed	**Start date:**	2010-07-27
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	Candidate for next major release		
Resolution:		**Affected version:**	

Description

Although, the User model defines :login and :mail as unique, it is not guaranteed that these are indeed unique in the database. Parallel requests can insert the exactly same users (apart from the id) if the transaction overlap.

Therefore I propose to add a unique-index to the database to ensure uniqueness. Also, I propose to always save the login in lowercase to properly use that index. There still has to be checked if that correctly works with the legacy mixed case logins (after r3807, r3813 because of #2473).

History

#1 - 2013-01-15 10:14 - Daniel Felix

Well some kind of check is good, but if the database use some database driver which is transaction save, there shouldn't be some kind of duplicate.

Anyway, a check if the username/mail is available would be good.

#2 - 2013-01-15 10:14 - Daniel Felix

- Category set to Accounts / authentication

#3 - 2013-01-15 18:44 - Holger Just

Daniel Felix wrote:

> Well some kind of check is good, but if the database use some database driver which is transaction save, there shouldn't be some kind of duplicate.

Well, no. Only the DBMS itself can ensure uniqueness constraints, at least with the transaction level typically used. And if there are no constraints defined, they will not be ensured naturally.

#4 - 2013-01-15 18:55 - Etienne Massip

- Status changed from New to Confirmed

- Target version set to Candidate for next minor release

Indeed, the unique indexes are necessary (this is even documented in AR).

#5 - 2013-01-15 18:56 - Etienne Massip

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

#6 - 2013-01-15 19:45 - Daniel Felix

Holger Just wrote:

> Well, no. Only the DBMS itself can ensure uniqueness constraints, at least with the transaction level typically used.

I know Holger, but I think this was some kind of misunderstanding.
With database driver I meaned things like InnoDB (transaction save) and MyIsam (not save, but faster), well it would be better if I called them database engines instead of drivers.

Well even a constraint in the db won't help if the database engine has no transaction support. ;-)

But anyway... beside this... I totally agree with you. This should be handled by some constraint, but there should be still some indicator if this username or mail is already in use before sending the registration to redmine. Just in case of the user friendliness.

#7 - 2013-01-15 20:08 - Etienne Massip

Daniel Felix wrote:

> Holger Just wrote:
>
> > Well, no. Only the DBMS itself can ensure uniqueness constraints, at least with the transaction level typically used.
>
> I know Holger, but I think this was some kind of misunderstanding.
> With database driver I meaned things like InnoDB (transaction save) and MyIsam (not save, but faster), well it would be better if I called them database engines instead of drivers.
>
> Well even a constraint in the db won't help if the database engine has no transaction support. ;-)

Please see #9685 and AR#validates_uniqueness_of.

My concern is more about the Users table storing Groups which have no mail...

#8 - 2013-01-16 19:39 - Etienne Massip

Allowing a mail adress to be used for different users is often asked for so I don't think it would be a great idea to add a unique index here; about the login there's no MTI in RoR and neither sqlite, mysql or postgresql support unique indexes without considering null values.

So we could either have a table per class (will require more work in more code locations) or fill the login column with the name of the Group (Anonymous type has only one record).