Redmine - Defect #23655

Restricted permissions for non member/anonymous on a given project not working

2016-08-24 16:02 - Alexander Schittler

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:	3.1.7		
Resolution:	Fixed	**Affected version:**	3.1.3

Description

When assigning a custom role "Non-member user", permission inheritance is broken (or simply undefined behavior because the Yes/No/Never model does not apply) on some views, when:

- The default "Non-member user" role has *View Issue* and *Issue Visibility* set to all.
- The custom assigned role has *View Issue*, but *Issue Visibility* set to created and assigned.

With this setup, the user will be able to see Issues not related to them at /issues, but /issues/<id> will throw a 403.

This might affect other features that use role-based filtering too (e.g. Time Logs, Users).

Associated revisions

Revision 15750 - 2016-08-30 21:24 - Jean-Philippe Lang

Fixed that restricted custom permissions on for non member/anonymous does not work (#23655).

Revision 15765 - 2016-08-31 18:51 - Jean-Philippe Lang

Merged r15750 (#23655).

Revision 15766 - 2016-08-31 18:52 - Jean-Philippe Lang

Merged r15750 (#23655).

Revision 15767 - 2016-08-31 18:52 - Jean-Philippe Lang

Merged r15750 (#23655).

History

#1 - 2016-08-24 17:02 - Toshi MARUYAMA

- Status changed from New to Needs feedback

I cannot reproduce on vanilla Redmine 3.1.6.
I think this is fixed by #20206.

#2 - 2016-08-24 18:32 - Holger Just

I can reproduce it on 3.2-stable (the Affected version is set to 3.1.3 since this is the latest version available in the custom field). The actual issue was found on a Redmine 3.2.1.

#20206 fixes a related issue for the default non-member role. Now with a custom non-member role, the problem is back. It is however important to strictly reproduce the setup described by Alexander: you need the default non-member role to have the Issue visibility set to all. You also need a **different** role with restricted issue visibility assigned as non-member role for the specific project.

The result is that Project.allowed_to_condition first considers the default non-member role and adds statements since the default role has the permission to view all issues. However, the custom role has not. Now the bug is that Project.allowed_to_condition does not consider custom default-roles in this first step. They are only considered later in User#projects_by_role.

I think a quick patch could look like this (mostly untested):

```
diff --git a/app/models/project.rb b/app/models/project.rb
index 197f45e..9f177ee 100644
--- a/app/models/project.rb
+++ b/app/models/project.rb
```

```
@@ -197,7 +197,7 @@ class Project < ActiveRecord::Base
         if role.allowed_to?(permission)
           s = "#{Project.table_name}.is_public = #{connection.quoted_true}"
           if user.id
-            s = "(#{s} AND #{Project.table_name}.id NOT IN (SELECT project_id FROM #{Member.table_name} WHERE user_id = #{user.id}))"
+            s = "(#{s} AND #{Project.table_name}.id NOT IN (SELECT project_id FROM #{Member.table_name} LEFT OUTER JOIN #{Principal.table_name} ON #{Member.table_name}.user_id = #{Principal.table_name}.id WHERE #{Member.table_name}.user_id = #{user.id} OR #{Principal.table_name}.type IN ('GroupAnonymous', 'GroupNonMember')))"
           end
           statement_by_role[role] = s
         end
```

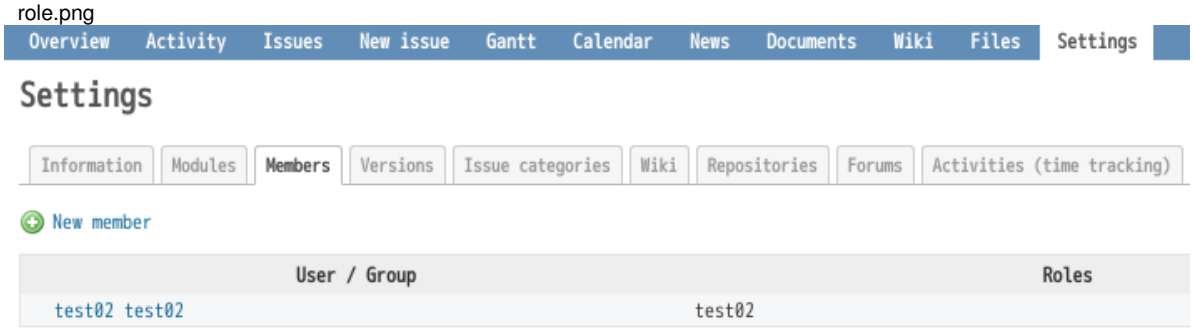
#3 - 2016-08-25 04:12 - Toshi MARUYAMA

- File project-setting.png added

- File role.png added

I still cannot reproduce on 3.2-stable.
I cannot understand "You also need a different role with restricted issue visibility assigned as non-member role for the specific project."

role.png



#4 - 2016-08-25 11:27 - Holger Just

- File desired_member_settings.png added

toshio harita: The role (test02 in your case) needs to be assigned to the project for Non member users, that is, you don't assign the role to an actual user but you set it a custom non-member role for the project. The user can not be an explicit member of the project. This feature to set a custom non-member role was added in #17976.

The settings screen should thus look like this:

desired_member_settings.png

#5 - 2016-08-25 13:39 - Toshi MARUYAMA

- Status changed from Needs feedback to Confirmed

- Target version set to 3.1.7

I got it.

#6 - 2016-08-30 21:26 - Jean-Philippe Lang

- Subject changed from Permissions model applied inconsistently to Restricted permissions for non member/anonymous on a given project not working

- Status changed from Confirmed to Resolved

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

Fixed in r15750, thanks for pointing this out.

#7 - 2016-08-31 18:52 - Jean-Philippe Lang

- Status changed from Resolved to Closed

#9 - 2018-05-08 10:41 - Jens Stein

- File Redmine-2018-05-08-10-19-33.png added

- File TicketViewer - Rollen - Redmine-2018-05-08-10-30-58.png added

It seems as if the problem is back:
I added the group "Nicht-Mitglieder" (which is the translated version of "Non member users") in a role called "TicketViewer" to some of our projects and authenticated (so not anonymous) users are not able to view the issues in the project.

```
Informationen
```

```
Redmine 3.3.4.stable.16947
```

I add screenshots of the added role in an example project and the roles configuration.
Maybe i made a error on setting it up.

Is there any other way to ensure a group (and it should be a dynamically changing group of authenticated users - e.g. employees which don't belong to the project as reporters, developers or any other set of roles/functions within the project), let's call them authenticated non-members,

- authenticated non-members are able to view tickets
- authenticated non-members are not able to view any other module
- authenticated non-members are enabled to add themselves to the watchlist
- authenticated non-members won't receive any news or forum notifications

Any advice, tipps, workarounds?

Thanks in advance,

JT

Files

project-setting.png	18.7 KB	2016-08-25	Toshi MARUYAMA
role.png	43.2 KB	2016-08-25	Toshi MARUYAMA
desired_member_settings.png	109 KB	2016-08-25	Holger Just
Redmine-2018-05-08-10-19-33.png	12.1 KB	2018-05-08	Jens Stein
TicketViewer - Rollen - Redmine-2018-05-08-10-30-58.png	47.8 KB	2018-05-08	Jens Stein