Redmine - Defect #10949

"User.current.allowed_to" does not consider the role permission when the user is administrator

2012-05-16 17:30 - Antoine Rodriguez

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Permissions and roles	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix	**Affected version:**	2.0.0

Description

Hi,

I try to create an advanced plugin like the "field_permission" plugin.

I've set a permission, let's say "view_description" in my *init.rb*

Then in the *"_form.html.erb"* I've put this code in order to filter the description block:

```
<% if not User.current.allowed_to?(:view_description, @project, :global => true).nil? %>
<% if @issue.safe_attribute? 'description' %>
<p>
  <label><%= l(:field_description) %></label>
  <%= link_to_function image_tag('edit.png'),
    'Element.hide(this); Effect.toggle("issue_description_and_toolbar", "appear", {duration:0.3})'
 unless @issue.new_record? %>
  <%= content_tag 'span', :id => "issue_description_and_toolbar", :style => (@issue.new_record? ?
nil : 'display:none') do %>
    <%= f.text_area :description,
                    :cols => 60,
                    :rows => (@issue.description.blank? ? 10 : [[10, @issue.description.length / 50
].max, 100].min),
                    :accesskey => accesskey(:edit),
                    :class => 'wiki-edit',
                    :no_label => true %>
  <% end %>
</p>
<% end %>
```

The symptoms are

- that normal accounts respond to the if statement correctly depending if they have the permission or not. This is ok
- admin accounts, with role that applies, do not take in consideration this filter and the allowed_to method always respond true and do not correspond to the view_description permission.

Environment:

- Redmine version: 2.0.0.stable
- Ruby version: 1.8.7 (x86_64-linux)
- Rails version: 3.2.3
- Environment: production
- Database adapter: MySQL

History

#1 - 2012-05-16 17:43 - Etienne Massip

Yes but as the user is admin he should be allowed, shouldn't he?

#2 - 2012-05-16 18:24 - Antoine Rodriguez

Not if the admin user is inside a role that apply for the project and the permission says no. (even if the admin user can modify the role ....)

Why making the administrative users different than regular users in the application of the roles and permissions ?

If he want to have the permission he set himself to do so but if he doesn't want the permission he should be able to do so. no ?

Typical use in the fields : the description is never used and will never be used in a project (for instance) : why seeing and edit the field description if it is never used in that specific project (via roles) ?

If this doesn't make sense so why allow administrative users being part of a role ? (which would apply for another bug then)

Best regards,

#3 - 2012-05-16 18:44 - Etienne Massip

I agree with you but I think Redmine's admin is allowed to everything and that you're right, assigning a specific role to an admin user has no impact on what he can or can't do.

I guess that the idea is that the administrator is some kind of "root" user and that users who are admin should better use a distinct regular account in their everyday work.

Edit: has **no** impact

#4 - 2012-05-16 20:03 - Antoine Rodriguez

I see your point. It means that those same administrators must have two accounts .... which is not quite good in management.

However since the administrators can set whenever they want the priviledges it still fits the idea of "root user"...

Considering this point, by making this function react correctly with administrators is finally a kind of aestetics more than a security matter.

But this aestetic point is quite important in order to have the same project experience than user. (avoid noises)

Another approach would be to make a distinguised method that include the roles that administrators are included.

Or, if all must be ignored and set to true then it is a bug that we can assign an administrative account to a role.

Now, in version 1.4.0 to 2.0.0 we are half/half : we can assign roles and permissions to adminitrators accounts but it has no effect.

By the way, in my personal point of view, the admin account should be the only "root" user. the administrators must have a little less priviledges. One difference must be that only root can do the global settings of redmine and the administrators can administers the projects .... But this is out of context in this ticket.

Best regards,

#5 - 2012-05-17 13:27 - Mischa The Evil

- Description updated

This is actually the behavior that was implemented in Redmine 1.4.0 with r8707 for issue #2323.

(Also fixed formatting of issue description.)

#6 - 2012-05-18 08:27 - Antoine Rodriguez

Indeed.

But why I can't have it to work like this ?

- My code is incorrect ? (in that case please tell me what I need to put in order to test it)
- Is it a bug ?

Best regards,

#7 - 2012-05-21 08:31 - Antoine Rodriguez

bump :)

#8 - 2012-05-21 19:09 - Jean-Philippe Lang

- Category changed from Plugin API to Permissions and roles

- Status changed from New to Closed

- Resolution set to Wont fix

I'm closing it because it works like this by design.

- administrators have all permissions on all projects (since the very first version of Redmine)
- administrators are allowed to do any status transition that is defined in the workflow (that is what r8707 fixed) but this is not related to your question since you're only checking for a permission