redmineorg-copy202205 - Vote #66199

Create a new type of role for not project specific maintenance

2022/05/09 14:22 - Admin Redmine

ステータス:	New	**開始日:**	2009/12/16
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Permissions and roles_17	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/4427	**status_id:**	1
category_id:	17	**tracker_id:**	2
version_id:	0	**plus1:**	6
issue_org_id:	4427	**affected_version:**	
author_id:	2784	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	9		

説明

The current role / permission concept is based on the assumption that everything of the daily work is done inside of projects. While this is true most of the time, there are more and more cases where things are done outside the scope of a project.

One example of this is the new permission to create projects as a non-admin user (#2963). This is allowed, if a user has that right in at least one project (checked by performing a global permission check). If she has that permission she can create projects anywhere in the project tree (at least if I understood the feature correctly).

However, this is not what I would expect from that permission. I expected, that a user with that permission were able to create a subproject on the project with that permission only. That permission being consequently project specific. The opportunity to create projects anywhere in the project tree is something that I would expect from an admin user only.

Another example is the creation of trackers and issue states and its management (workflows et al.), or the creation of custom fields. This is currently only possible to admin users.

In large installations which are used by many different organizational units of a company, this can lead to a large indirection, as it is not feasible to have a huge amount of real admins with the ability to look in every project. So requests to have certain features added have to be directed to one of the few admin users.

To solve this, I propose an additional type of role. These new roles can be assigned to a user but no project. They should allow to grant a user certain global rights, like the creation of global projects, custom fields, new trackers, ... The goal is to prevent the misusage of global permission checks as done by he "create project" permission check in the @ProjectsController@

I think, these new roles could be fairly easily patched into the existing permission model and providing similar functionality as the global check. But the permissions / roles are explicitly declared by the user, who can then better understand the consequences of certain permissions.

journals

I'll second that.

In addition to the examples provided by Holger, I would like to see a "user manager" role that would allow a user (IT staff) to create new users and assign them to groups. The rationale is that offloading some "grunt work" without giving my IT staff access to all projects, since some of them contain confidential information.

I agree that it would be a real improvement.

For the "create project" example, we could distinguish "create project" and "create subproject" permissions.

The first one would let the user create a root project, the second permission would only

allow creation of subprojects inside his projects.

+1 see also #6670

+1 see also #6800 (same feature, different solution proposal)

+1 a special role for user management would be great

+1 as a new user it was the first "flaw" I noticed. I had to create a fake project so that I could give permission to create projects without giving Admin powers (which shouldn't be treated lightly). I'm sure there are other powers that could be useful to hand to a non admin user.

+1. I also think that some "global" permissions (such as "create project") have to be assigned (by admin) per user, not per projects.

Also the way "create projects" is currently granted (as a per project permission) has a security problem: any who has permission to specify members in any of the projects, can grant "create project" to himself or to anybody else.

+1

I think it is necessary to have system level roles for creating and editing custom queries shared between projects.

Currently, only admin can create / edit this, and the actual project manager can not complete the work.

As a result, the following problem arises.

1. Admin privilege will be added only for creating / editing shared queries,
   It is an obstacle to managing accounts with "least privilege principle".

2. Increase in the load of admin, decrease in business operation speed.

I suggest adding the following role to set at the system level.

1. Permission to create shared custom queries that are valid for the entire system (assuming role-based permission management)
   add_system_shared_rolebased_queries

2. Authorization to edit system-level custom queries you created (role-based permission management)
   edit_system_shared_created_rolebased_queries

I think that admin is the only authority to create and edit custom queries available for all users and all projects.

I summarized previous proposal so far.

Please fill in any additional suggestions.

> create projects as a non-admin user # description,note-6
> This is allowed, if a user has that right in at least one project (checked by performing a global permission check).
> If she has that permission she can create projects anywhere in the project tree (at least if I understood the feature correctly).
>
> creation of trackers and issue states and its management (workflows et al.), or the creation of custom field # description
>
> "user manager" role that would allow a user (IT staff) to create new users and assign them to groups. #note-1,note-5
>
> I agree that it would be a real improvement. #note-2 Jean-Philippe Lang
>
> creating and editing custom queries shared between projects. #note-8

related_issues
relates,Closed,4431,Non-admin user cannot create project :for revision 3174 relates,Closed,6728,how to assign global rights? relates,New,6670,Admin rights should not override rights given through roles duplicates,Closed,6800,howto assign global rights

履歴

#1 - 2022/05/10 17:24 - Admin Redmine

- カテゴリ を Permissions and roles_17 にセット