Foreman - Bug #32213

changing "admin" parameter of user-group with non-admin user is accepted but nothing changed

03/26/2021 11:12 AM - Marek Hulán

Status:	Closed		
Priority:	Normal		
Assignee:	Marek Hulán		
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:		**Fixed in Releases:**	2.5.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:	1848981	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/8414		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1848981

Description of problem:
When trying to update "admin" parameter of user-group with non-admin user change is accepted, but nothing happen.
WebUI seems already prepared as when trying the same with non-admin user checkbox for Administrator is not visible

How reproducible: Always

Steps to Reproduce:
1. Create non-admin user with roles below

view_filters, create_filters, edit_filters, destroy_filters
view_usergroups, create_usergroups, edit_usergroups, destroy_usergroups view_roles, create_roles, edit_roles, destroy_roles
view_external_usergroups, create_external_usergroups, edit_external_usergroup, destroy_external_usergroups
view_bookmarks, create_bookmarks, edit_bookmarks, destroy_bookmarks
attach_subscriptions, unattach_subscriptions
escalate_roles
view_organizations
view_authenticators

2. Create new usergroup
3. Attempt to change "admin" parameter of user-group with hammer or API as below

   1. hammer --config /root/.hammer/non_admin_user_config.yml user-group update --id 1 --admin 1

or

   1. curl -X PUT -H "Content-Type: application/json" -u user:password -d \'{"admin": \'1\'}\' https://`hostname -f`/api/usergroups/1/

Actual results:
hammer: User group [group] updated.
API: {"admin":false,"created_at":"2020-06-16 14:10:11 UTC","updated_at":"2020-06-16 14:27:08 UTC","name":"group","id":1,"external_usergroups":[],"usergroups":[],"users":[],"roles":[]}

Expected results:
Not allowing operation with non-admin user and show warning message.'

Associated revisions

Revision 744f9bd0 - 04/04/2021 02:08 PM - Marek Hulán

Fixes #32213 - inform user about wrong use of admin flag

Our API filters the admin attribute of user group API via strong params
for non-admin users. Therefore when non-admin tries to create or update
a user group admin flag, it is silently ignored even and the user group

correctly remains as is. Only admins can set this attribute.

From user perspective, this is not great. It's confusing why the explicitly set attribute is ignored. The user should be informed about the reason.

This patch removes the attribute filtering for the API and adds a model validation, which register the proper validation error which is then presented to the user.

The UI does not require any change since the flag is is not even displayed to the user. For security reason the flag continue to be filtered for the UI path. The validation in this case is another security level but in general should never be triggered through UI.

The API in this case returns 422 because the actual model is not valid. Technically this could also be 403 since user does not have enough permissions, but that would be confusing, since that status is for the case users don't have the edit_usergroups permission at all. 422 is more consistent with other cases, e.g. when user tries to set attribute to link the object he/she does not have view permission for.

History

#1 - 03/26/2021 11:32 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Marek Hulán

- Pull request https://github.com/theforeman/foreman/pull/8414 added

#2 - 04/04/2021 02:08 PM - The Foreman Bot

- Fixed in Releases 2.5.0 added

#3 - 04/04/2021 03:01 PM - Marek Hulán

- Status changed from Ready For Testing to Closed

Applied in changeset foreman|744f9bd00597710883c6db1dfa37f3ca22cc18c5.

#4 - 05/05/2021 02:33 PM - Tomer Brisker

- Category set to Users, Roles and Permissions