Foreman - Bug #25104

Permissions for roles can be modified even if user does not have :edit_roles permission

10/02/2018 01:39 PM - Ondřej Pražák

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

It is possible to add and remove permissions to a role even if current_user does not have :edit_role permission. The cause is that filters cannot exist without association to a role but their permissions do not take it into consideration. When filter is created, it is always associated to a role and that role has access to permissions through filter, so even if role record has not been modified, the role itself gained new permissions through associations.

We should turn filters into a proper nested resource that would fully depend on a role.

Steps to reproduce:

1) create a role with the following permissions: :view_roles, :view_filters, :create_filters, :update_filters, :destroy_filters
2) create a new user named Bob, assign him role created in step 1 and then log in as Bob
3) go to Administer -> Roles, then click on 'Filters' button for a role that is not locked, which will show you index of filters and edit buttons in the Action table column

History

#1 - 10/16/2018 07:05 AM - Lukas Zapletal

- Category set to Users, Roles and Permissions

- Triaged changed from No to Yes

#2 - 11/21/2018 10:22 AM - Aditi Puntambekar

- Assignee set to Aditi Puntambekar

#3 - 12/17/2018 12:38 PM - Aditi Puntambekar

Is the expected result here that although we have edit filter permission for Bob, but since no edit role permission, then Edit Action shouldn't appear for Filter resource as well ? As in Edit action for any resource should appear only if edit_roles permission is applied ?

#4 - 12/18/2018 07:10 AM - Ondřej Pražák

It is expected that users will not be authorized to add new permissions to roles by creating/updating filters if they do not have :edit_roles permission. If users do not have :edit_roles permission, they should not be allowed to modify roles.

#5 - 06/03/2019 06:17 AM - Aditi Puntambekar

- Assignee deleted (Aditi Puntambekar)