

Foreman - Bug #7221

Edit organization displays associated resources for use w/o permissions

08/21/2014 03:35 PM - Thomas McKay

Status: Closed	
Priority: Normal	
Assignee: Thomas McKay	
Category: Users, Roles and Permissions	
Target version: 1.7.0	
Difficulty:	Fixed in Releases:
Triaged:	Found in Releases:
Bugzilla link: 1132675	Red Hat JIRA:
Pull request: https://github.com/theforeman/foreman/pull/1731	
Description	
<p>A user with the below permissions can incorrectly see the following on an organization edit page. Note that because the tabs are displayed the list of resources available in each are also displayed. This implies that the choices are not being reduce to show only those available to a specific user.</p> <p>What I mean is that if user A has a filter that allowed them to only see "Alterator default" Template, then the list should contain only that template. It is my guess that this is not the case. Maybe worth a separate bug but suspect it is all related.</p> <p>If no permission for resource at all, do not render tab at all. For limited permissions, display only those resources that are accessible.</p> <p>Smart Proxies Subnets Compute Resources Media Templates Domains Realms Environments Host Groups Locations Parameters</p> <pre>Name, Count, Resource, Search, Permissions, Organizations, Locations SAM Administrator, 1, Katello::ActivationKey, "", "view_activation_keys, create_activation_keys, edit_activation_keys, destroy_activation_keys", , "" SAM Administrator, 1, Katello::System, "", "view_content_hosts, create_content_hosts, edit_content_hosts, destroy_content_hosts", , "" SAM Administrator, 1, Katello::ContentView, "", "view_content_views", , "" SAM Administrator, 1, Katello::HostCollection, "", "view_host_collections, create_host_collections, edit_host_collections, destroy_host_collections", , "" SAM Administrator, 1, Katello::KTEEnvironment, "", "view_lifecycle_environments", , "" SAM Administrator, 1, Katello::Product, "", "view_products, sync_products", , "" SAM Administrator, 1, Organization, "", "view_organizations, create_organizations, edit_organizations, destroy_organizations, assign_organizations, view_subscriptions, attach_subscriptions, unattach_subscriptions, import_manifest, delete_manifest", , "" SAM Administrator, 1, Role, "", "view_roles, create_roles, edit_roles, destroy_roles", , "" SAM Administrator, 1, Filter, "", "view_filters, create_filters, edit_filters, destroy_filters", , "" SAM Administrator, 1, User, "", "view_users, create_users, edit_users, destroy_users", , "" SAM Administrator, 1, Usergroup, "", "view_usergroups, create_usergroups, edit_usergroups, destroy_usergroups", , ""</pre>	
Related issues:	
Related to Foreman - Bug #6760: Models should ensure the authorization of ass...	New 07/23/2014
Related to Foreman - Bug #7337: organizations UI does not filter resources to...	Closed 09/03/2014
Related to Foreman - Bug #7335: organizations UI "All users" toggle not check...	Closed 09/03/2014

Associated revisions

Revision ae255b3c - 09/15/2014 03:41 AM - Thomas McKay

fixes #7221 - do not display areas of the org/loc UI unless view rbac

corrected 'template' to 'templates'

History

#1 - 08/21/2014 03:35 PM - Thomas McKay

- Bugzilla link set to 1132675

#2 - 08/22/2014 03:47 AM - Dominic Cleal

- Related to Bug #6760: Models should ensure the authorization of associated objects before associating them to the model added

#3 - 08/22/2014 03:47 AM - Dominic Cleal

- Category changed from Web Interface to Users, Roles and Permissions

#4 - 08/29/2014 01:35 PM - Thomas McKay

- Assignee set to Thomas McKay

#5 - 08/29/2014 01:47 PM - Thomas McKay

From IRC

```
<thomasmckay> ehelms: working #7221 what should the perms be to view and edit associations with org/loc? https://github.com/foreman/foreman/blob/develop/app/views/taxonomies/_form.html.erb#L16
<nudnik> ehelms: #7221 is http://theforeman.org/issues/7221 "Bug #7221: Edit organization displays associated resources for use w/o permissions - Foreman"
<thomasmckay> i think that page should just check view permission on the resource to show the tab
<thomasmckay> and then edit perm on at least org to adjust associations. should edit perm on the smart-proxy, in this case, also be required?
<ehelms> thomasmckay: depends how you look at it, are you changing the org or the object? does adding an organization to a smart proxy change the proxy, the organization or both?
<ehelms> thomasmckay: I lean towards just the object
<thomasmckay> i'd say both since you are basically letting it be used in that org
<thomasmckay> ehelms: your vote is edit perm on the resource, but not require edit on the org?
<thomasmckay> should you be able to create a subnet in an org you don't have edit perm on?
<thomasmckay> i guess yes... yeah, i think you're right
<thomasmckay> so view on org but edit on resource
<ehelms> thomasmckay: that's how katello at least works when you think about it
```

#6 - 09/02/2014 06:10 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Target version set to 1.7.4

- Pull request <https://github.com/foreman/foreman/pull/1731> added

- Pull request deleted ()

#7 - 09/03/2014 10:56 AM - Dominic Cleal

- Related to Bug #7337: organizations UI does not filter resources to associate based upon RBAC added

#8 - 09/03/2014 10:57 AM - Dominic Cleal

- Related to Bug #7335: organizations UI "All users" toggle not checking permissions for being displayed added

#9 - 09/10/2014 07:22 AM - Anonymous

- Target version changed from 1.7.4 to 1.7.3

#10 - 09/15/2014 03:57 AM - Dominic Cleal

- translation missing: en.field_release set to 21

#11 - 09/15/2014 04:02 AM - Thomas McKay

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset [ae255b3caf953b43b2387bedc78a6a258b2b8b33](#).