Foreman - Bug #23994

It is possible to update template in organizations user does not have permission for when importing a template

06/19/2018 07:50 AM - Ondřej Pražák

Status:	Closed		
Priority:	High		
Assignee:	Ondřej Pražák		
Category:	Templates		
Target version:	1.18.0		
Difficulty:		**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/5725, https://github.com/theforeman/foreman/pull/5798		

Description

Steps to reproduce:

1) Create non-admin user_a with Manager role in OrgA and LocA only, same for user_b, OrgB and LocB
2) try importing a new template as user_a into OrgB and LocB with the following command:

```
curl -H "Accept: application/json" -H "Content-Type: application/json" -k -X POST -u user_a:change
me https://$(hostname)/api/v2/provisioning_templates/import -d '{ "provisioning_template": {"name"
: "An org test", "template": "<%#\nkind: PXELinux\nname: An org test\nmodel: ProvisioningTemplate\
norganizations:\n - OrgB\nlocations:\n - LocB\n%>\ntest"}, "options": {"verbose": "true", "associa
te": "always"} }' | json_reformat
```

You will not be permitted to do so as expected.

3) Now import the template into OrgA, LocA as user_a, which succeeds:

```
curl -H "Accept: application/json" -H "Content-Type: application/json" -k -X POST -u user_a:change
me https://$(hostname)/api/v2/provisioning_templates/import -d '{ "provisioning_template": {"name"
: "An org test", "template": "<%#\nkind: PXELinux\nname: An org test\nmodel: ProvisioningTemplate\
norganizations:\n - OrgA\nlocations:\n - LocA\n%>\ntest"}, "options": {"verbose": "true", "associa
te": "always"} }' | json_reformat
```

4) Try importing template with the same name as user_b into LocB and OrgB:

```
curl -H "Accept: application/json" -H "Content-Type: application/json" -k -X POST -u user_b:change
me https://$(hostname)/api/v2/provisioning_templates/import -d '{ "provisioning_template": {"name"
: "An org test", "template": "<%#\nkind: PXELinux\nname: An org test\nmodel: ProvisioningTemplate\
norganizations:\n - OrgB\nlocations:\n - LocB\n%>\ntest again"}, "options": {"verbose": "true", "a
ssociate": "always"} }' | json_reformat
```

The result will be a successfully imported template with the template assigned to LocB and OrgB only, user_b was thus able to update something he does not have permissions for and user_a can no longer use that template since it was removed from OrgA and LocA and its original content likely overwritten with whatever user_b posted.

Associated revisions

Revision 943bc1a2 - 06/28/2018 12:15 PM - Ondřej Pražák

Fixes #23994 - Do not update templates out of scope

History

#1 - 06/21/2018 08:36 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Ondřej Pražák

- Pull request https://github.com/theforeman/foreman/pull/5725 added

#2 - 06/26/2018 09:43 AM - Tomer Brisker

- translation missing: en.field_release set to 330

- Triaged set to Yes

#3 - 06/28/2018 01:02 PM - Ondřej Pražák

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 943bc1a277e543d13893ded9ead1459b3c664789.

#4 - 07/09/2018 01:51 PM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman/pull/5798 added