Foreman - Bug #9947
CVE-2015-1844 - GET /api/hosts doesn't respect organization/location membership

03/30/2015 09:28 AM - Andy Taylor

Status: Closed
Priority: Normal
Assignee: Marek Hulán
Category: Organizations and Locations
Target version: 1.7.5

Description
I created a new user with a dedicated role with the following permissions:

Host/managed: view_hosts

The user is a member of 1 organization and 2/4 locations. When logging in via the web interface, the user can only see the hosts belonging to that 1 organization/2 locations. However, an API call via /api/hosts lists the hosts of all organizations and all locations. The only way I could fix this was by applying a location/organization restriction to the view_hosts filter on the role.

Related issues:
- Related to Foreman - Refactor #10025: Move taxonomy related methods and scope... Closed 04/06/2015
- Related to Discovery - Bug #10005: CVE-2015-1844 - Discovery hosts are not re... Closed 04/02/2015
- Related to Foreman - Bug #10918: Provisioning templates no longer resolve/ava... Feedback 06/24/2015
- Blocked by Foreman - Bug #9967: Unit tests do not isolate user setup Closed 03/31/2015

Associated revisions
Revision abe910f2 - 04/09/2015 11:23 AM - Marek Hulán
Fixes #9947 - restrict user taxonomies if none is set

Revision 5ddb3741 - 04/13/2015 07:49 AM - Marek Hulán
Fixes #9947 - restrict user taxonomies if none is set
(cherry picked from commit abe910f2a46f4eccf1349263d0b4751ed46ff200)

Revision c5a4e31c - 04/27/2015 09:30 AM - Marek Hulán
Fixes #9947 - restrict user taxonomies if none is set
(cherry picked from commit abe910f2a46f4eccf1349263d0b4751ed46ff200)

Conflicts:
app/models/report.rb
test/unit/host_test.rb

History
#1 - 03/30/2015 09:34 AM - Dominic Cleal
- Category changed from API to Organizations and Locations
#2 - 03/30/2015 10:54 AM - Marek Hulán
- Status changed from New to Assigned
- Assignee set to Marek Hulán

#3 - 03/30/2015 11:17 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman/pull/2273 added
- Pull request deleted ()

#4 - 03/31/2015 05:01 AM - Dominic Cleal
- Subject changed from GET /api/hosts doesn't respect organization/location membership to CVE-2015-1844 - GET /api/hosts doesn't respect organization/location membership

#6 - 04/01/2015 06:28 AM - Marek Hulán
- Bugzilla link set to 1208071

#7 - 04/01/2015 06:36 AM - Marek Hulán
- Blocked by Bug #9967: Unit tests do not isolate user setup added

#8 - 04/01/2015 06:36 AM - Marek Hulán
- Legacy Backlogs Release (now unused) set to 40

#9 - 04/09/2015 06:08 AM - Dominic Cleal
- Related to Refactor #10025: Move taxonomy related methods and scopes to Host::Base added

#10 - 04/09/2015 06:06 AM - Dominic Cleal
- Related to Bug #10005: CVE-2015-1844 - Discovery hosts are not restricted to user taxonomies added

#11 - 04/09/2015 12:01 PM - Marek Hulán
- % Done changed from 0 to 100
- Status changed from Ready For Testing to Closed

Applied in changeset abe910f2a46f4ecc1f349263d0b4751ed46ff200.

#12 - 04/09/2015 01:16 PM - Daniel Lobato Garcia
Warning for the release notes: this PR will make global (unscoped by organization/location) objects invisible to all users except for admins. If you want to make global objects you should assign them to all taxonomies.

#13 - 06/24/2015 07:09 AM - Dominic Cleal
- Related to Bug #10918: Provisioning templates no longer resolve/available for non-admin users in Foreman 1.7.5 added