Foreman - Bug #18430

IPA users from AD trusts do not populate attributes or group membership

02/08/2017 02:25 PM - Jason Nance

Status:	New		
Priority:	High		
Assignee:			
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.13.4
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Foreman 1.13.4 installed on a FreeIPA-joined CentOS 7.3+ host with --foreman-ipa-authentication true passed to foreman-installer successfully authenticates a user which is created in FreeIPA, honors its IPA group membership as it pertains to Foreman groups, and creates the Foreman bits so that the user profile appears in Foreman under Administer->Users (and in groups in Administer->User Groups.

However, a user that is known to FreeIPA via a trust with Active Directory does not work correctly.

During login in to the Foreman web UI with ad-user\@lab.gen.zone (where lab.gen.zone is the trusted AD domain), the following log messages are observed:

```
==> /var/log/httpd/foreman-ssl_access_ssl.log <==
172.16.246.97 - ad-user@lab.gen.zone [08/Feb/2017:13:06:28 -0600] "POST /users/login HTTP/1.1" 302
 112 "https://sl2mmgplsat0001.ipa.lab.gen.zone/users/login" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /hosts HTTP/1.1" 302 139 "https://sl2mmgplsat0
001.ipa.lab.gen.zone/users/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"

==> /var/log/httpd/foreman-ssl_error_ssl.log <==
[Wed Feb 08 13:06:28.252329 2017] [ssl:warn] [pid 92440] [client 172.16.246.97:63146] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/login
[Wed Feb 08 13:06:28.351328 2017] [:notice] [pid 92440] mod_authnz_pam: PAM authentication passed
for user ad-user@lab.gen.zone
[Wed Feb 08 13:06:28.359131 2017] [:error] [pid 92440] dbus call GetUserAttr returned value 0 inst
ead of DBUS_TYPE_DICT_ENTRY
[Wed Feb 08 13:06:28.490678 2017] [ssl:warn] [pid 92440] [client 172.16.246.97:63146] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/login
[Wed Feb 08 13:06:28.516367 2017] [ssl:warn] [pid 92440] [client 172.16.246.97:63146] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/login

==> /var/log/foreman/production.log <==
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Started POST "/users/login" for 172.16.246.97 at 2017-02-08
 13:06:28 -0600
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Processing by UsersController#login as HTML
2017-02-08 13:06:28 d5c9bcb4 [app] [I]   Parameters: {"utf8"=>"□", "authenticity_token"=>"X38u65bZ
IW2eZibgK+QFXQNt19x6Yb1KTGQiEzJu7TeIrPIfFEvepOmLzBHtPlXod7zl5GyPAoHNAvRs70M/bA==", "login"=>{"logi
n"=>"ad-user@lab.gen.zone", "password"=>"[FILTERED]"}, "commit"=>"Login"}
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Expire fragment views/tabs_and_title_records-7 (0.2ms)
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Expire fragment views/tabs_and_title_records-7 (0.1ms)
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Redirected to https://sl2mmgplsat0001.ipa.lab.gen.zone/host
s
2017-02-08 13:06:28 d5c9bcb4 [app] [I] Completed 302 Found in 120ms (ActiveRecord: 12.2ms)
2017-02-08 13:06:28 c1120385 [app] [I] Started GET "/hosts" for 172.16.246.97 at 2017-02-08 13:06:
```

```
28 -0600
2017-02-08 13:06:28 c1120385 [app] [I] Processing by HostsController#index as HTML
2017-02-08 13:06:28 c1120385 [app] [I] Redirected to https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
2017-02-08 13:06:28 c1120385 [app] [I] Filter chain halted as :require_mail rendered or redirected
2017-02-08 13:06:28 c1120385 [app] [I] Completed 302 Found in 15ms (ActiveRecord: 2.0ms)
2017-02-08 13:06:28 c1120385 [app] [I] Started GET "/users/7-ad-userlab-gen-zone/edit" for 172.16.
246.97 at 2017-02-08 13:06:28 -0600
2017-02-08 13:06:28 c1120385 [app] [I] Processing by UsersController#edit as HTML
2017-02-08 13:06:28 c1120385 [app] [I]   Parameters: {"id"=>"7-ad-userlab-gen-zone"}
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered common/_edit_habtm.html.erb (0.2ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered taxonomies/_loc_org_tabs.html.erb (0.8ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered users/_form.html.erb (29.9ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered users/edit.html.erb within layouts/application (
30.4ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered layouts/_application_content.html.erb (0.4ms)

==> /var/log/httpd/foreman-ssl_access_ssl.log <==
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /users/7-ad-userlab-gen-zone/edit HTTP/1.1" 20
0 5679 "https://sl2mmgplsat0001.ipa.lab.gen.zone/users/login" "Mozilla/5.0 (Windows NT 10.0; Win64
; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /webpack/bundle-d65c367369a195962269.css HTTP/
1.1" 200 7538 "https://sl2mmgplsat0001.ipa.lab.gen.zone/users/7-ad-userlab-gen-zone/edit" "Mozilla
/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safa
ri/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /assets/application-87d75a160b45ffe154a8a3d972
c116bb493bd1186c406d74d1447fc3cfe39929.css HTTP/1.1" 200 62442 "https://sl2mmgplsat0001.ipa.lab.ge
n.zone/users/7-ad-userlab-gen-zone/edit" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
7.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /assets/users-461edfb36b719f0743b1d176a854300f
c29a0d7ee8008710709b65bfc5452d8d.js HTTP/1.1" 200 478 "https://sl2mmgplsat0001.ipa.lab.gen.zone/us
ers/7-ad-userlab-gen-zone/edit" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /assets/password_strength-04d727d4a3b1ca40d729
06ea76c9b7024e7071467d48a494f01b0c15491ac424.js HTTP/1.1" 200 3948 "https://sl2mmgplsat0001.ipa.la
b.gen.zone/users/7-ad-userlab-gen-zone/edit" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
t/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36"
172.16.246.97 - - [08/Feb/2017:13:06:28 -0600] "GET /webpack/bundle-d65c367369a195962269.js HTTP/1
.1" 200 137085 "https://sl2mmgplsat0001.ipa.lab.gen.zone/users/7-ad-userlab-gen-zone/edit" "Mozill
a/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Saf
ari/537.36"

==> /var/log/httpd/foreman-ssl_error_ssl.log <==
[Wed Feb 08 13:06:28.674344 2017] [ssl:warn] [pid 92440] [client 172.16.246.97:63146] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.678011 2017] [ssl:warn] [pid 92440] [client 172.16.246.97:63146] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.681981 2017] [ssl:warn] [pid 94251] [client 172.16.246.97:63151] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.682233 2017] [ssl:warn] [pid 94251] [client 172.16.246.97:63151] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.682433 2017] [ssl:warn] [pid 94278] [client 172.16.246.97:63152] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.682674 2017] [ssl:warn] [pid 94278] [client 172.16.246.97:63152] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.682816 2017] [ssl:warn] [pid 92436] [client 172.16.246.97:63154] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
[Wed Feb 08 13:06:28.683094 2017] [ssl:warn] [pid 92436] [client 172.16.246.97:63154] AH02227: Fai
led to set r->user to 'SSL_CLIENT_S_DN_CN', referer: https://sl2mmgplsat0001.ipa.lab.gen.zone/user
s/7-ad-userlab-gen-zone/edit
```

```
==> /var/log/foreman/production.log <==
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_user_dropdown.html.erb (2.8ms)
2017-02-08 13:06:28 c1120385 [app] [I] Read fragment views/tabs_and_title_records-7 (0.1ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_organization_dropdown.html.erb (6.7ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_location_dropdown.html.erb (7.1ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_org_switcher.html.erb (14.4ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_submenu.html.erb (1.7ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_submenu.html.erb (1.5ms)
2017-02-08 13:06:28 c1120385 [app] [I] Write fragment views/tabs_and_title_records-7 (0.9ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered home/_topbar.html.erb (65.5ms)
2017-02-08 13:06:28 c1120385 [app] [I]   Rendered layouts/base.html.erb (67.4ms)
2017-02-08 13:06:28 c1120385 [app] [I] Completed 200 OK in 127ms (Views: 97.2ms | ActiveRecord: 7.
9ms)

==> journalctl -f <==
Feb 08 13:06:28 sl2mmgplsat0001.ipa.lab.gen.zone httpd[92440]: pam_sss(foreman:auth): authenticati
on success; logname= uid=48 euid=48 tty= ruser= rhost=172.16.246.97 user=ad-user@lab.gen.zone
```

The password is accepted, but the user is immediately taken to the "Edit User" page with the following error message in the web UI:

```
Error: An email address is required, please update your account details.
```

The user name field is populated, but the first name, surname, and email address fields are blank. In AD, this user has a first and last name, but no email address.

After filling out the form and clicking "Submit", the Foreman displays a message that the update was successful, but the user is denied permission to everything:

```
Permission denied You are not authorized to perform this action.
Please request one of the required permissions listed below from a Foreman administrator:
view_hosts
```

The ad-user\@lab.gen.zone user intermittently appears and disappears under "Administer->Users", but group membership is not honored and no privileges granted.

In my setup administrative access is granted via a Foreman group called global-admins, which consumes the "external" group lxeng (which is an IPA group).

The local OS is aware of the group membership of both users:

```
$ id ipa-user
uid=10013(ipa-user) gid=10013(ipa-user) groups=10013(ipa-user),10011(lxeng),10007(lxusers)
$ id ad-user@lab.gen.zone
uid=21113(ad-user@lab.gen.zone) gid=21113(ad-user@lab.gen.zone) groups=21113(ad-user@lab.gen.zone)
,10011(lxeng),20513(domain users@lab.gen.zone)
```

History

#1 - 02/08/2017 02:26 PM - Jason Nance

The backslash before the at sign is not included when attempting to login. That is and editing mistake when opening this issue.

#2 - 02/09/2017 03:15 AM - Dominic Cleal

- Subject changed from IPA users from AD trusts do not work to IPA users from AD trusts do not receive group membership

- Category set to Users, Roles and Permissions

It's unclear from the description whether the "global-admins" group is assigned to the Foreman user or not - are you reporting that the external user group association isn't working, so the group isn't auto-assigned? Or do view_hosts permissions not work when the user is assigned to the group manually?

If auto-assignment isn't working then the bug is more likely in mod_lookup_identity rather than Foreman, which only receives environment variables from the web server module showing group membership. (Particularly if it works for other types of user account.)

#3 - 02/09/2017 08:49 AM - Jason Nance

global-admins is a Foreman group. lxeng is an external group added to global-admins.

I'm unable to assign ad-user to the group directly as it isn't showing up in Foreman as a user (I reported that it intermittently shows up but it appears that the actual case is rare for the AD trust user to be visible at all).

So I guess I'm reporting three things:

- Attributes (first name, last name) of users known via an IPA AD trust aren't recognized/imported by Foreman
- Users known via an IPA AD trust aren't being populated in Foreman on first login
- External group membership of users known via an IPA AD trust isn't honored, but this may actually be a symptom of the previous item

The "normal" IPA stuff I provided was just to show that in general my Foreman/IPA integration is working and that the users are similar in terms of group membership.

#4 - 02/09/2017 09:21 AM - Dominic Cleal

- Subject changed from IPA users from AD trusts do not receive group membership to IPA users from AD trusts do not populate attributes or group membership

Jason Nance wrote:

> I'm unable to assign ad-user to the group directly as it isn't showing up in Foreman as a user (I reported that it intermittently shows up but it appears that the actual case is rare for the AD trust user to be visible at all).

Not sure I see how this could happen, the user list UI is pretty simple (unless you have some feature like orgs/locations and context set, or are using a non-admin user).

The ID is shown in your log (Started GET "/users/7-ad-userlab-gen-zone/edit) and so you can always view that same URL (/users/7/edit) to view/edit the account as an administrator.

> So I guess I'm reporting three things:
>
> - Attributes (first name, last name) of users known via an IPA AD trust aren't recognized/imported by Foreman
> - Users known via an IPA AD trust aren't being populated in Foreman on first login
> - External group membership of users known via an IPA AD trust isn't honored, but this may actually be a symptom of the previous item

These are probably all issues in mod_lookup_identity then.

I don't think it has any debugging capability (unless SSSD logs data on its behalf), but you might be able to debug it manually by reconfiguring it to set other environment variables of the account. This may give you enough information to file a bug against that module.