

## Foreman - Bug #14407

### foreman-rake ldap:refresh\_usergroups ends in endless loop with external user group in Active Directory

03/31/2016 02:35 AM - Daniel Lobato Garcia

<b>Status:</b>	Duplicate	
<b>Priority:</b>	High	
<b>Assignee:</b>	Daniel Lobato Garcia	
<b>Category:</b>	Authentication	
<b>Target version:</b>		
<b>Difficulty:</b>		<b>Fixed in Releases:</b>
<b>Triaged:</b>		<b>Found in Releases:</b>
<b>Bugzilla link:</b>	1261997	<b>Red Hat JIRA:</b>
<b>Pull request:</b>		

#### Description

Cloned from [https://bugzilla.redhat.com/show\\_bug.cgi?id=1261997](https://bugzilla.redhat.com/show_bug.cgi?id=1261997)

Description of problem:

While attaching Satellite 6.1.1 to Active Directory using the built in LDAP provider, I found that when adding "external user group" to automatically assign a role to an Active Directory account, `foreman-rake ldap:refresh\_usergroups` is ending up in a end-less loop

Version-Release number of selected component (if applicable):

foreman-1.7.2.34-1.el7sat.noarch

How reproducible:

Always

Steps to Reproduce:

```
hammer> auth-source ldap info --id=4
Id: 4
Name: system-rhev.gsslab.rdu.redhat.com
LDAPS?: false
Port: 389
Server Type: AuthSourceLdap
Account Username: RHEV\sre_system
Base DN: cn=users,dc=rhev,dc=gsslab,dc=rdu,dc=redhat,dc=com
LDAP filter:
Automatically Create Accounts?: true
Login Name Attribute: sAMAccountName
First Name Attribute: givenName
Last Name Attribute: sn
Email Address Attribute: mail
Photo Attribute:
hammer> user-group info --id=2
Id: 2
Name: Admin
Users:
  sre_test2
User groups:
External user groups:
  sre_sat6
Roles:
  Viewer
  View hosts
  Tasks Reader
  Tasks Manager
  Site manager
  Red Hat Access Logs
```

```

Manager
Edit partition tables
Edit hosts
Discovery Reader
Discovery Manager
Boot disk access
Access Insights Viewer
Access Insights Admin
Created at:          2015/09/10 09:36:27
Updated at:          2015/09/10 09:36:27

hammer> user-group external info --user-group Admin --id=2
Id:          2
Name:        sre_sat6
Auth source: system-rhev.gsslab.rdu.redhat.com

ldapsearch -LLL -x -h rhev-ad.gsslab.rdu2.redhat.com -D "RHEV\sre_system" -W -b "cn=users,dc=rhev,dc=gsslab,dc=rdu,dc=redhat,dc=com" '(sAMAccountName=sre_test1)'
Enter LDAP Password:
dn: CN=Test 1. Reber,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Test 1. Reber
sn: Reber
givenName: Test
initials: 1
distinguishedName: CN=Test 1. Reber,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
instanceType: 4
whenCreated: 20150910080741.0Z
whenChanged: 20150910081516.0Z
displayName: Test 1. Reber
uSNCreated: 676204
memberOf: CN=sre_sat6,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
uSNChanged: 676228
name: Test 1. Reber
objectGUID:: ocosGfW7ekKk7EfhTZFH6g==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 130863534640478484
lastLogoff: 0
lastLogon: 130863534735478484
pwdLastSet: 130863460614552568
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAAAA1xQhMV2+kD5S4cm/ngQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: sre_test1
sAMAccountType: 805306368
userPrincipalName: sre_test1@rhev.gsslab.rdu.redhat.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
dsCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 130863465167973044

ldapsearch -LLL -x -h rhev-ad.gsslab.rdu2.redhat.com -D "RHEV\sre_system" -W -b "cn=users,dc=rhev,dc=gsslab,dc=rdu,dc=redhat,dc=com" '(sAMAccountName=sre_test2)'
Enter LDAP Password:
dn: CN=Test2 Reber,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user

```

```
objectClass: inetOrgPerson
cn: Test2 Reber
sn: Reber
givenName: Test2
distinguishedName: CN=Test2 Reber,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,
  DC=com
instanceType: 4
whenCreated: 20150910123829.0Z
whenChanged: 20150910135100.0Z
displayName: Test2 Reber
uSNCreated: 676274
memberOf: CN=sre_sat6,CN=Users,DC=rhev,DC=gsslab,DC=rdu,DC=redhat,DC=com
uSNChanged: 676299
name: Test2 Reber
objectGUID:: Syvv33EYOUajgPatGfUtew==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 130863666600942818
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAALxQhMV2+kD5S4cm/ogQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: sre_test2
sAMAccountType: 805306368
userPrincipalName: sre_test2@rhev.gsslab.rdu.redhat.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=rhev,DC=gsslab,DC=rdu,
  DC=redhat,DC=com
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 130863623932659008
```

Login with an Active Directory Account, which is member of sre\_sat6 and check on whether permissions are being assigned

#### Actual results:

User does not have any role assigned and when running `foreman-rake ldap:refresh\_usergroups`, the command does not finish

#### Expected results:

Role automatically assigned to user or at least when `foreman-rake ldap:refresh\_usergroups` is run

#### Additional info:

I checked the `foreman-rake ldap:refresh\_usergroups` command and found that it does a end-less loop in  
/opt/rh/ruby193/root/usr/share/gems/gems/ldap\_fluff-0.3.2/lib/ldap\_fluff/active\_directory.rb

When I comment the below section and manually defining `users` the command is successful and the user defined has the correct role assigned

```
... active_directory.rb
[...]
def users_from_search_results(search, method)
  users = ["sre_test2"]

  search.send(method).each do |member|
    entry = @member_service.find_by_dn(member).first
    objectclasses = entry.objectclass.map(&:downcase)
#
#     if (%w(organizationalperson person) & objectclasses).present?
#       users << @member_service.get_login_from_entry(entry)
#     elsif (%w(organizationalunit group) & objectclasses).present?
#       users << users_for_gid(entry.cn.first)
#     end
end
```

```
users.flatten.uniq
end
```

[...]

Uncommenting "users << users\_for\_gid(entry.cn.first)" will cause the loop to occur again

---

**Related issues:**

Is duplicate of Foreman - Bug #13608: LDAP Authentication failure: stack leve...

**Closed**

**02/08/2016**

---

**History****#1 - 03/31/2016 03:00 AM - Dominic Cleal**

- *Description updated*
- *Category set to Authentication*
- *Status changed from New to Need more information*

Could you please try with a current version? ldap\_fluff 0.3.2 is old and a few group lookup bugs have been fixed since.

**#2 - 05/17/2017 03:48 PM - Anonymous**

- *Status changed from Need more information to Resolved*

no reaction, closing. I can't access that BZ.

**#3 - 05/18/2017 02:44 AM - Marek Hulán**

- *Status changed from Resolved to Duplicate*

Sorry for that, it was closed as dup of [#13608](#)

**#4 - 05/18/2017 02:44 AM - Marek Hulán**

- *Is duplicate of Bug #13608: LDAP Authentication failure: stack level too deep added*