

## Foreman - Bug #17794

### Users created via external delegation API don't get usergroups on first login

12/20/2016 03:40 AM - Daniel Lobato Garcia

<b>Status:</b> New	
<b>Priority:</b> Normal	
<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> 1406295	<b>Red Hat JIRA:</b>
<b>Pull request:</b> <a href="https://github.com/theforeman/foreman/pull/4119">https://github.com/theforeman/foreman/pull/4119</a>	
<b>Description</b> Cloned from <a href="https://bugzilla.redhat.com/show_bug.cgi?id=1406295">https://bugzilla.redhat.com/show_bug.cgi?id=1406295</a> Description of problem:  Customer has an user who logs in via external delegation (REMOTE_USER). This user is created automatically upon login. The user is not authenticated using regular Satellite LDAP authentication sources, but through the 'authorized login delegation' setting.  When the user is created in this manner, it will not get its usergroups until the next time the cron job runs, or unless the admin clicks on refresh external user groups.  Version-Release number of selected component (if applicable): 6.2.4, but it shows up in nightly and upstream even.  How reproducible: Always  Steps to Reproduce: 1. Setup some external user groups linked to Satellite user groups 2. Login via external delegation (krb5 ticket, for example) 3. Notice how the users, even if they are in the external user groups, do not get updated.  Expected results: The user groups should be updated when the user logs in for all Authentication sources where "Usergroup sync" is checked.	

#### History

##### #1 - 12/20/2016 03:54 AM - Dominic Cleal

- Category set to Authentication

- Status changed from New to Assigned

Are the REMOTE\_USER\_GROUP\_\* variables set correctly? The description doesn't mention them - if only REMOTE\_USER is set then this would be normal. It shouldn't rely on LDAP connectivity or refreshing.

[#3892](#) implements this.

##### #2 - 12/20/2016 04:34 AM - Daniel Lobato Garcia

They are not set, the issue here is that they were expecting REMOTE\_USER logins to check in all LDAP auth sources as they don't want to add more configuration for REMOTE\_USER\_GROUP. They worked around it by running the cron very often - it will find a login shared by the REMOTE\_USER and the ActiveDirectory auth source and put users from auth source "EXTERNAL" into external usergroups linked to LDAP.

In the end, our code already checks in LDAP auth sources during cron or manual refresh, so it's just a matter of checking on login for external users too.

Foreman doesn't deal well with 'logins' that happen to be in multiple authentication sources. E.g: I create an 'admin' user on FreeIPA and AD. Then on Foreman I'll get added to all external user groups (linked to both FreeIPA and AD) even if my user.authentication\_source is just FreeIPA. It's not great but this scenario happens rarely (or ever?) I believe.

Things like this (AD provides krb5 tokens that I use for REMOTE\_USER, but the REMOTE\_USER isn't linked to AD in Foreman) are more or less

common.

Aside from patching the code to deal with that scenario, I think we should be providing this info to the Foreman admin users. "Hey you seem to have a user with the same login in 2 auth sources (external and AD). Be warned about this and that".

**#3 - 12/20/2016 04:43 AM - The Foreman Bot**

- Status changed from Assigned to Ready For Testing
- Pull request <https://github.com/theforeman/foreman/pull/4119> added

**#4 - 12/20/2016 04:58 AM - Dominic Cleal**

Then on Foreman I'll get added to all external user groups (linked to both FreeIPA and AD) even if my user.authentication\_source is just FreeIPA. It's not great but this scenario happens rarely (or ever?) I believe.

Users with a different authentication source to the external user group shouldn't be linked - the list of users from the auth source when refreshing the external user group should be filtered to only those with the same auth source.

This is likely buggy behaviour and shouldn't be relied upon like this, not built upon to force-refresh LDAP external user groups when using external auth sources.

**#5 - 12/20/2016 09:54 AM - Daniel Lobato Garcia**

- Target version set to 1.15.5

**#6 - 01/24/2017 09:57 AM - Daniel Lobato Garcia**

- Target version changed from 1.15.5 to 169

**#7 - 02/18/2017 10:23 AM - Brad Buckingham**

- Target version deleted (169)

**#8 - 02/21/2017 09:52 AM - Daniel Lobato Garcia**

- Target version set to 1.11.0

**#9 - 07/20/2017 10:33 AM - Marek Hulán**

- Target version changed from 1.11.0 to 1.17.0-RC2

**#10 - 08/08/2017 08:36 AM - Marek Hulán**

- Target version changed from 1.17.0-RC2 to 1.18.0-RC2

**#11 - 08/14/2017 03:39 PM - Marek Hulán**

- translation missing: en.field\_release set to 240

**#12 - 08/29/2017 05:57 AM - Marek Hulán**

- Target version changed from 1.18.0-RC2 to 214

**#13 - 09/20/2017 09:27 AM - Marek Hulán**

- Target version changed from 214 to 1.16.0-RC2

**#14 - 10/23/2017 03:09 PM - Marek Hulán**

- Target version changed from 1.16.0-RC2 to 1.16.0-RC1

**#15 - 10/30/2017 01:51 PM - Marek Hulán**

- Target version changed from 1.16.0-RC1 to 1.16.2

**#16 - 11/16/2017 08:13 AM - Daniel Lobato Garcia**

- Status changed from Ready For Testing to New
- translation missing: en.field\_release deleted (240)

Resetting status as this isn't really a bug but a hack to fix communication if your LDAP management IT & Foreman admins cannot agree to provide

REMOTE\_USER\_GROUP variables.

**#17 - 11/21/2017 07:52 AM - Marek Hulán**

- *Target version changed from 1.16.2 to 1.16.1*

**#18 - 12/12/2017 11:51 AM - Marek Hulán**

- *Target version changed from 1.16.1 to 238*