

Foreman - Bug #9125

LDAP group inheritance not working

01/26/2015 05:47 PM - Ashton Davis

Status: New	
Priority: Normal	
Assignee:	
Category: Users, Roles and Permissions	
Target version:	
Difficulty:	Fixed in Releases:
Triaged:	Found in Releases:
Bugzilla link:	Red Hat JIRA:
Pull request:	
Description	
There are two issues here. They both seem to be more Foreman related than Katello.	
Process: 1) Create user group in Foreman (called Foretello Admins), check "Administrator" box. 2) Link an LDAP group to Foretello Admins (LDAP Group: "Admins") 3) Have a user in "Admins" log into the system.	
Expected behavior: 4) User logs in, should have administrator privileges.	
Actual behavior: 4) User logs in, has no permissions.	
Additional issue: This isn't a huge deal, since I have so few new users. But I don't run around as the 'admin' user, I stay logged in as 'adavis', with explicit 'administrator' privileges checked for my user. When step 4 fails, I would open 'Users' from the 'Administer' menu and select the user. But unlike in the past, now the user who failed to log in doesn't appear. I have to log out of adavis and back in as admin in order to see the 'new' user, and assign them permissions.	
Related issues:	
Related to Foreman - Bug #9040: External Group Mapping not working	New 01/19/2015

History

#1 - 01/27/2015 03:15 AM - Marco Helmerich

- Related to Bug #9040: External Group Mapping not working added

#2 - 01/27/2015 04:43 AM - Dominic Cleal

- Category set to Users, Roles and Permissions

Does the user group get assigned to the user, or not? If it doesn't, then the issue is the LDAP group mapping, if not and the user is part of the group, then the 'admin' flag isn't being inherited.

If it doesn't get assigned, could you list a few more details about your LDAP configuration:

1. type of LDAP server, and what type you have selected in the LDAP Auth Source configuration
2. base and group base DN settings for the auth source
3. DN of the group and user
4. version of Foreman

#3 - 02/10/2015 06:54 PM - Ashton Davis

Sorry Dominic, I forgot to fill out what you asked.

- 1) Had been backed by a POSIX schema on an OpenLDAP compliant server. Now we're testing with AD. Same issue.
- 2) BaseDN is just dc=[domain],dc=com, group base DN is the same.

3) Example:

cn=Ashton Davis,ou=users,ou=[location],ou=[country],dc=[domain],dc=[com]

cn=ForemanAdmins,ou=groups,ou=[location],ou=[country],dc=[domain],dc=[com]

4) Katello 2.1.1 (Foreman 1.7.2)

There are actually TWO issues here, as I've discovered. Though I am logged in as an administrator (as adavis), I can't see users who have logged in for the first time in the users menu, whether I've set a context or not. In order to see users who haven't been assigned a group, I have to sign in as admin and clear my context (no org, no loc) in order to see the users in the list. I suspect the two issues are related.