Foreman - Bug #9494

Users are not added to groups based on LDAP group membership

02/20/2015 05:03 PM - Phillip Schichtel

Status:	New		
Priority:	Normal		
Assignee:	Daniel Lobato Garcia		
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.7.2
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

I connect my foreman instance to our LDAP server for user login and groups.
The LDAP server is an OpenLDAP instance managed through GOsa².

The structure:

dc=tld
dc=domain
_ou=int
__ou=groups
_____cn=group1
_cn=group2
__ou=people
_____cn=First User
__cn=Second User

user objectclasses:
- gosaAccount
- gosaMailAccount
- inetOrgPerson
- organisationalPerson
- person
- posixAccount
- shadowAccount
rdn: cn=Firstname Surname

group objectclasses:
- gosaAcl
- groupOfNames
- posixGroup
relevant attributes: cn (name), member (full DN of a user), memberUid (uid value of a user)

Foreman adds the server as a posix server and has ou=int,dc=domain,dc=tld as the base DN and
ou=groups,ou=int,dc=domain,dc=tld as the group DN and user auto creation is enabled.
User attribute mappings:

login -> uid
first name -> givenName
surname -> sn
email address -> mail
picture -> jpegPhoto

The user group:
In foreman: Group1 with Admin as the Role
In LDAP: cn=group1,ou=int,dc=domain,dc=tld

Adding the external LDAP group to the foreman group as well as logging in with LDAP credentials works perfectly fine.

The users however do not receive their groups.

I think the problem might be related to this query from the refresh-group.log:
SELECT "users".* FROM "users" WHERE "users"."login" IN ('firstname1 surname1', 'firstname2 surname2') ORDER BY firstname

History

#1 - 02/23/2015 04:24 AM - Dominic Cleal

- Category changed from Authentication to Users, Roles and Permissions

Files

refresh-group.log	3.5 KB	02/20/2015	Phillip Schichtel
save-group.log	4.36 KB	02/20/2015	Phillip Schichtel