Foreman - Bug #7048

[RFE] Ability to configure default role for users who come in from LDAP

08/12/2014 12:57 PM - Bryan Kearney

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1110557	**Red Hat JIRA:**	
Pull request:			

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1110557
Today, the default role is always anonymous. It would be good to allow users to cofnigure the default role which is used when users come in from LDAP.

History

#1 - 08/12/2014 01:04 PM - Dominic Cleal

- Status changed from New to Feedback

The way this is meant to work is that you assign the role to a user group, then configure the user group via external user groups to sync with one of your LDAP groups (same works for Kerberos/REMOTE_USER type integration). Given that you can assign roles to groups, it doesn't make much sense to try and force roles into LDAP.

#2 - 08/18/2014 04:06 AM - Dominic Cleal

- Status changed from Feedback to Rejected

#3 - 10/30/2014 06:16 PM - Cliff Wells

Dominic Cleal wrote:

> The way this is meant to work is that you assign the role to a user group, then configure the user group via external user groups to sync with one of your LDAP groups (same works for Kerberos/REMOTE_USER type integration). Given that you can assign roles to groups, it doesn't make much sense to try and force roles into LDAP.

It seems the bug report is badly misunderstood. Currently, when a user who is in LDAP logs into the UI for the first time, they cannot view anything. An admin must manually assign them a Foreman role. It would be nice to be able to configure Foreman to select a different default role for these new users (e.g. Viewer).

This has nothing to do with putting anything into LDAP.

#4 - 10/31/2014 02:59 AM - Marek Hulán

I think Dominic is right. User that comes to foreman for the first time cannot view anything only if he has no usergroups. The way it's supposed to work is that user belongs to some user group in LDAP (e.g. viewers), there is already a user group viewers in foreman and both user groups are associated in foreman. Also let's suppose that we have view_* permissions assigned to viewers foreman user group (through role). When user logs into foreman (even for the first time), foreman looks up all user groups in ldap that the user belongs to and finds associated foreman internal user groups (viewers) and associate them with user. Since user now belongs to viewers user group he also has all view_* permissions. Same applies to other authentication sources (whatever supported by mod_lookup_identity) that gives us list of remote user groups.