Pulp - Story #172

[RFE] Allow authentication of users against LDAP Group objects

02/19/2015 01:48 AM - ncoghlan@redhat.com

Status:	CLOSED - WONTFIX	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Sprint/Milestone:			
Platform Release:		**Tags:**	Pulp 2
Groomed:	No	**Sprint:**	
Sprint Candidate:	No	**Quarter:**	

Description

++ This bug was initially created as a clone of Bugzilla Bug #828072 ++

Description of problem:

Description of problem:

LDAP group queries are currently only possible if the LDAP server provides "memberOf" attributes (or an equivalent) on User objects. RFC2307 compliant servers that only store group membership on the Group objects cannot be queried.

The "base" attribute assumes "ou=Users" and the filter setting queries the attributes of the returned user objects. There's currently no way I can see to turn this around and query ou=Group to see if the user id is present in the group member list.

--- Additional comment from ncoghlan@redhat.com at 06/14/2012 06:34:23 ---

I created BZ#831937 to request an alternative approach that I believe would be superior: allowing Pulp to be configured to delegate the REST API authentication and authorisation checks to the web server.

--- Additional comment from ncoghlan@redhat.com at 07/13/2012 00:29:58 ---

After creating the patch attached to BZ#831937, I realised the two issues (Apache level authentication & authorisation and better LDAP integration) are actually fairly orthogonal. I also realised I don't need the enhanced LDAP authorisation right now, but I suspect it may become more important in the future to map different LDAP filters to different roles rather than being limited to a single filter->role mapping as is the case now.

I did do some design work before deciding I didn't actually need the feature yet, and this RFE seems like a better place to capture that than the mailing list (copied from https://www.redhat.com/archives/pulp-list/2012-June/msg00052.html):

==========
The current LDAP authorization support is rather limited - consisting solely of the "filter" option in the [ldap] config settings, along with the "default-role" setting in that section.

This is limited in three ways:
- it doesn't handle web server level preauthentication in the absence of LDAP
- it only allows LDAP filters against users (not LDAP groups), which is a problem if the LDAP server doesn't provide "memberOf" attributes on user records
- it doesn't allow for per-role LDAP filters

To deal with the first limitation, I plan to add a "default-role" option to the [security] section of the config file that is automatically granted to **all** users when first created. LDAP authenticated users would then get both the security default role **and** the ldap default role (if any) when they first logged in. Both default-role entries become optional.

For the latter two limitations, I plan to implement a couple of new
configuration sections: "ldap-user-roles" and "ldap-group-roles"

The format of these new sections are currently going to be:

[ldap-user-roles]
role-name: <LDAP user filter>

[ldap-group-roles]
role-name: <LDAP group filter>

The role names are only checked against the database when a user logs in
via web server preauthentication. If the role name doesn't exist, that
results in a warning in the Pulp log file but is otherwise ignored.

When a user is created implicitly (either via LDAP authentication or web
server preauthentication) the following automatic role assignment checks
will be performed:

If security.default-role is defined:
the new user is granted that role
If LDAP is configured and the username matches a uid in LDAP (taking
ldap.filter into account):
If ldap.default-role is defined:
the new user is granted that role
For each role:role-filter pair in ldap-user-roles:
If (&(uid=<username>)<role-filter>) returns a non-empty list:
the new user is granted that role
For each role:role-filter pair in ldap-group-roles:
If (&(uid=<username>)<role-filter>) returns a non-empty list:
the new user is granted that role
If, after all this, the user has no roles assigned:
They are not authorized for any access, and the login attempt fails
Otherwise, the user is created and more specific role-based
authorization checks proceed as usual
==========

Hope this helps for the great 2.0 auth refactor :)

Associated revisions

Revision a0964ac5 - 03/25/2015 02:28 PM - bmbouter

Merge pull request #172 from bmbouter/fix-2-6-0-release-notes

Fixes URL in 2.6.0 release notes

History

#1 - 04/12/2019 07:39 PM - bmbouter

- Status changed from NEW to CLOSED - WONTFIX

#2 - 04/12/2019 07:42 PM - bmbouter

Pulp 2 is approaching maintenance mode, and this Pulp 2 ticket is not being actively worked on. As such, it is being closed as WONTFIX. Pulp 2 is still accepting contributions though, so if you want to contribute a fix for this ticket, please reopen or comment on it. If you don't have permissions to reopen this ticket, or you want to discuss an issue, please reach out via the developer mailing list.

#3 - 04/15/2019 11:20 PM - bmbouter

- Tags Pulp 2 added