

Pulp - Task #946

Develop a plan to improve Pulp's authentication offerings

05/04/2015 09:24 PM - rbarlow

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

Description

Right now Pulp uses httpd's REMOTE_USER environment variable to authenticate remote users, except for the /login call. This is great, except that /login works in a way that causes our users lots of trouble. Right now, /login uses a username:password combo to authenticate, and if successful /etc/pki/pulp/ca.crt is used to generate a client SSL certificate. This /etc/pki/pulp/ca.crt file is far too tempting for our users, and I think that it might be trust to say that 100% of people's SSL issues are related to messing with this file. We need a plan to rethink the /login call so that it does not require any such file, and no such file should be generated by our RPM!

Some things to think about:

- It would be nice if Pulp and pulp-admin used something like a session key instead of a client SSL cert by default
- Since Pulp trusts REMOTE_USER, admins are still free to generate their own SSL client certs if they please. We should document how to form the CN for this to work, and we should ensure that pulp-admin can still be configured to use such a cert if it's provided
- Kerberos should work!
- Really, any httpd auth module should work.

Deliverable

- A set of stories that achieve a better set of authentication user stories than we currently achieve (nebulous!)
- Remember that these changes are very likely backwards incompatible when you file them

I think this is important, because I and others have lost a lot of time supporting users who have tried to use that file as a CA and have really confused their Pulp installations. If we improve Pulp such that that file no longer exists (and none like it), we will save ourselves more time than it takes to make this change, and at the same time we will greatly improve our authentication offerings!

Related issues:

Related to Pulp - Task #2090: Create a plan for user/auth in 3.0

CLOSED - CURRENTRELEASE

History

#1 - 05/04/2015 09:56 PM - bmbouter

- Sprint Candidate set to Yes
- Tags deleted (Sprint Candidate)

#2 - 05/08/2015 08:07 PM - bmbouter

- Groomed set to No

#3 - 06/08/2015 03:10 PM - mhrivnak

- Groomed changed from No to Yes

Consider using django's session support.

Consider HMAC.

This is high priority because we have spent a lot of time on auth problems related to users mis-using our current auth features.

#4 - 06/26/2015 06:42 PM - dkliban@redhat.com

Another thing to consider is the need for the client to be aware of having been authenticated with the server or not. The client should be able to check if any method of authentication has been used before or during (-u and -p) a command. If a user is not authenticated, then the client should only be able to send requests for status and login end points.

#5 - 07/13/2015 05:27 PM - mhrivnak

- Priority changed from High to Normal

#7 - 05/04/2016 03:20 PM - mhrivnak

- Sprint Candidate changed from Yes to No

#8 - 09/01/2016 03:01 PM - amacdona@redhat.com

- Related to Task #2090: Create a plan for user/auth in 3.0 added

#9 - 04/12/2019 09:06 PM - bmbouter

- Status changed from NEW to CLOSED - WONTFIX

#10 - 04/12/2019 09:12 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](#).

#11 - 04/15/2019 10:49 PM - bmbouter

- Tags Pulp 2 added