

Pulp - Story #97

As a contributor, I rest easy knowing SELinux is Enforcing in the Pulp3 Vagrant environment

01/08/2015 04:50 PM - cduryee

Status:	NEW	Start date:	
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0:00 hour
Sprint/Milestone:		QA Contact:	
Platform Release:		Complexity:	
Blocks Release:		Smash Test:	
Backwards Incompatible:	No	Verified:	No
Groomed:	No	Verification Required:	No
Sprint Candidate:	No	Sprint:	
Tags:	Pulp 3 installer, SELinux		

Description

The real deliverables are in the checklist, but here is some extra info on how to compile it.

To compile and install the Pulp SELinux with Ansible for Vagrant you will need to:

- Install selinux-policy-devel rpm with ansible
- Compile the policy similar to make NAME=celery -f /usr/share/selinux/devel/Makefile DISTRO=fedora24 except with ansible
- Install the policy using Ansible
- Have ansible call the restorecon script or fixfiles (see checklist item) so that all the right restorecon calls occur. Stay DRY with these calls if possible.[0]
- If necessary, have the policy use "developer layout" .fc files to cause the .te compiled policies to be compatible with the layout used by Vagrant.

Use the ps -awfuxZ | grep celery to verify it is becoming the celery_t security label type. Similarly httpd should get an httpd security type. Then do some testing with Pulp and SELinux enabled.

[0]: <https://github.com/pulp/pulp/blob/master/server/selinux/server/relabel.sh>

Related issues:

Related to Pulp - Task #843: Make pulp-selinux versioned independently from p...	CLOSED - WONTFIX
Duplicated by Pulp - Issue #2792: syncing an importer has SELinux denials	CLOSED - DUPLICATE
Blocked by Pulp - Story #3809: As a user, I can run Pulp 3 with SELinux enfor...	ASSIGNED

History

#1 - 01/08/2015 07:34 PM - rbarlow

+1

#2 - 01/08/2015 09:45 PM - bmbouter

- Tracker changed from Issue to Story

- Subject changed from allow pulp dev setup to work with selinux enabled to Allow Pulp dev setup to work with SELinux enabled

I think the scope of the problem is a lot bigger than this story identifies. It's not just the pulp-dev.py script. The "developer layout" that pulp-dev.py produces will not run correctly with SELinux enabled [0]. Does this user expect to be able to develop Pulp with SELinux enabled? If so, that will not be so easy to accomplish.

Here's a recap of the thinking that got us here. The developer layout versus what an RPM lays out are substantially different. Poking holes in the production policy to allow for development activities doesn't make sense. This leads to the conclusion that for Pulp development to happen with SELinux enabled, Pulp would need a SELinux policy specifically for development. The first policy took a few weeks to write and test on all the platforms so it would likely take a similar level of effort to make a Pulp SELinux policy. Also any change in the developer layout will also need to have changes in the Pulp developer SELinux policy. Those changes need to be tested on all the platforms, so easy changes all of a sudden become a lot

more painful. It would be good to have one, but we never could prioritize this activity in front of other more pressing work. I'm also not sure we can commit to maintaining such a thing. This caused me to document that Pulp can't be developed with SELinux enabled at this time.

https://pulp-dev-guide.readthedocs.org/en/latest/contributing/dev_setup.html?highlight=selinux#selinux

#3 - 04/03/2015 09:21 PM - bmbouter

- Related to Task #843: Make pulp-selinux versioned independently from pulp-server added

#4 - 04/08/2016 05:43 PM - bmbouter

- Related to deleted (Task #843: Make pulp-selinux versioned independently from pulp-server)

#5 - 04/08/2016 05:43 PM - bmbouter

- Parent task set to #1826

#6 - 04/08/2016 05:44 PM - bmbouter

- Related to Task #843: Make pulp-selinux versioned independently from pulp-server added

#7 - 04/08/2016 07:15 PM - bmbouter

- Tags SELinux added

#8 - 04/08/2016 07:17 PM - bmbouter

- Parent task deleted (#1826)

#9 - 11/11/2016 10:46 PM - bmbouter

- Checklist item [] enable SELinux in vagrant environment on master and 3.0-dev added

- Checklist item [] Have vagrant+ansible compile the Pulp SELinux policy and install it added

- Checklist item [] verify that the celery processes and streamer are running with the expected security contexts added

- Checklist item [] Create some developer docs on how to compile and install the SELinux policy in case users need to do it manually added

- Subject changed from Allow Pulp dev setup to work with SELinux enabled to Pulp vagrant environments should run with SELinux enabled

- Description updated

I'm rewriting the contents of the bug with an engineering plan of how to accomplish the title.

#10 - 11/11/2016 10:47 PM - bmbouter

- Sprint Candidate changed from No to Yes

#11 - 11/14/2016 09:14 PM - bmbouter

- Description updated

#12 - 11/14/2016 09:17 PM - dkliban@redhat.com

- Groomed changed from No to Yes

#13 - 06/05/2017 07:42 PM - bmbouter

- Duplicated by Issue #2792: syncing an importer has SELinux denials added

#14 - 06/05/2017 07:51 PM - bmbouter

- Subject changed from Pulp vagrant environments should run with SELinux enabled to As a contributor, I rest easy knowing SELinux is Enforcing in the Pulp3 Vagrant environment

- Groomed changed from Yes to No

- Tags Pulp 3 added

Rewriting to be Pulp3 specific. With active development occurring on Pulp3, it is not as useful to continue having this track the SELinux Vagrant issue for Pulp2.

#15 - 06/05/2017 08:17 PM - amacdona@redhat.com

I would like to see all of this in a completely separate Ansible role.

#16 - 06/05/2017 10:33 PM - bmbouter

- *Description updated*

@asmacdo, I agree. I added a checklist item. I also removed two leftover checklist items from when I edited it earlier. I also updated the diff some too to reflect the update from earlier today.

#17 - 09/14/2018 03:56 PM - amacdona@redhat.com

- *Sprint Candidate changed from Yes to No*

#18 - 11/28/2018 08:18 PM - amacdona@redhat.com

- *Blocked by Story #3809: As a user, I can run Pulp 3 with SELinux enforcing added*

#19 - 11/28/2018 08:19 PM - amacdona@redhat.com

- *Tags Pulp 3 installer added*

#20 - 04/26/2019 10:40 PM - bmbouter

- *Tags deleted (Pulp 3)*