SELinux - Bug #19223

AVC denied from logrotate sending signal to foreman-proxy unit

04/07/2017 11:07 AM - Jason Nance

Status:	Needs design		
Priority:	Normal		
Assignee:			
Category:	Smart proxy		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.13.4
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The postrotate script in /etc/logrotate.d/foreman-proxy is blocked via SELinux and results in log files not getting released.

```
type=USER_AVC msg=audit(1491468305.905:16288): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='avc:  denied  { stop } for auid=0 uid=0 gid=0 path="/usr/lib/systemd/system/foreman-proxy.service" cmdline="/bin/systemctl kill --signal=SIGUSR1 foreman-proxy" scontext=system_u:system_r:logrotate_t:s0-s0:c0.c1023 tcontext=system_u:object_r:systemd_unit_file_t:s0 tclass=service  exe="/usr/lib/systemd/systemd" sauid=0 hostname=? addr=? terminal=?'
```

System is a CentOS 7 host with released updates as of 2017-4-7.

candlepin-selinux-0.9.54.6-1.el7.noarch
foreman-1.13.4-1.el7.noarch
foreman-selinux-1.13.4-1.el7.noarch
katello-3.2.2-1.el7.noarch
katello-selinux-3.0.1-1.el7.noarch
libselinux-2.5-6.el7.x86_64
libselinux-python-2.5-6.el7.x86_64
libselinux-utils-2.5-6.el7.x86_64
logrotate-3.8.6-12.el7.x86_64
pulp-selinux-2.9.3-1.el7.noarch
selinux-policy-3.13.1-102.el7_3.15.noarch
selinux-policy-targeted-3.13.1-102.el7_3.15.noarch

Related issues:

Copied from SELinux - Bug #19053: Proxy continues to write to deleted file af...	**Closed**

History

#1 - 04/07/2017 11:10 AM - Jason Nance

- Copied from Bug #19053: Proxy continues to write to deleted file after log rotation added

#2 - 04/10/2017 09:26 AM - Dominic Cleal

- Subject changed from AVC denied trying to rotate logs to AVC denied from logrotate sending signal to foreman-proxy unit

- Category set to Smart proxy

Fedora already permits logrotate to stop units without specific labels, however to fix this properly the foreman_proxy module should perhaps include a init_startstop_service macro call, and the unit file should be labelled appropriately.

(Or to support logrotation without the foreman_proxy module, this can also be fixed in packaging by using a regular kill without systemd support, which is permitted.)

#3 - 09/19/2017 05:21 AM - Radosław Piliszek

This still affects Foreman (tested 1.15.4)

Any progress on this? Can I be of any help?

#4 - 09/19/2017 06:30 AM - Marek Hulán

I'm afraid there has been no progress, if you have SELinux knowledge, contributing to our policies at https://github.com/theforeman/foreman-selinux is highly appreciated

#5 - 09/19/2017 08:04 AM - Lukas Zapletal

- Tracker changed from Bug to Support

So the problem here is the standard practice is to send SIGHUP to daemons to release log files after rotating, base RHEL SELinux policy includes rules to allow logrotate to send this via systemctl reload command. Our proxy only supports SIGUSR1 which is not standard and therefore the only way supporting this is by doing changes in our SELinux policy. This includes creating two types, domain, macro, file contexts - this is too complicated. It is much better to follow what is expected and change our service to respond to reload properly, then we can change our logrotate script as well.

Please see http://projects.theforeman.org/issues/19053#note-25 for futher discussion.

To test this, perform two changes:

https://github.com/theforeman/smart-proxy/pull/544/files
https://github.com/theforeman/foreman-packaging/pull/1814/files

Then do systemctl daemon-reload and restart logrotate.

Please report if that helped here.
I looked into modifying our SELinux policy and it is a complex change, I think it is much easier to do changes in service file to do the reload properly.

#6 - 09/19/2017 08:47 AM - Daniel Lobato Garcia

- Tracker changed from Support to Bug

- translation missing: en.field_release set to 240

Marking as 1.16.

#7 - 09/20/2017 06:26 AM - Radosław Piliszek

I applied both patches, reloaded systemd, restarted foreman-proxy (to fix the current log), ran logrotate (it is scheduled daily via cron, no service used) and it worked. No errors, logging works. Thanks.

#8 - 09/20/2017 07:07 AM - Radosław Piliszek

For another bug with logrotate please see Issue #21032.

#9 - 10/23/2017 12:55 PM - Daniel Lobato Garcia

- Status changed from New to Closed

Thanks for the feedback, closing as resolved.

#10 - 10/23/2017 01:06 PM - Radosław Piliszek

Where was this resolved? PRs were closed without merging and there is no mention in changelogs about this being fixed.

#11 - 10/23/2017 01:21 PM - Ewoud Kohl van Wijngaarden

- Status changed from Closed to Needs design

- translation missing: en.field_release deleted (240)

I'll agree this wasn't resolved but it's no longer targeted for 1.16.0 since we need to figure out what's the correct place to solve it.

#12 - 10/27/2017 07:46 AM - Lukas Zapletal

Yeah I believe this can be closed now, folks do not like my proposal of handling signal so this needs to be incorporated into our SELinux policy. Feel free to drop PR there, we need few rules and new macro perhaps.