SELinux - Bug #9523

Puppet master crashes on AVC when blocking setattr after logrotate

02/24/2015 04:02 AM - Gerwin Krist

Status:	Closed		
Priority:	High		
Assignee:	Gerwin Krist		
Category:	General Foreman		
Target version:	1.8.0		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.7.2
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman-selinux/pull/46		

Description

Problem description
Once a week our puppet master stops working and the puppet clients are spitting out errors. We are seeing this on a freshly installed 1.7.2 on RHEL 7 (Selinux enabled).

Observations

It seems the problems starts when the weekly logrotate is done:

```
Feb 23 03:22:19 i-foreman puppet-master[92076]: failed to set mode 644 on /var/log/puppet/http.log
: Permission denied - /var/log/puppet/http.log
Feb 23 03:22:19 i-foreman puppet-master[92076]: (/File[/var/log/puppet/http.log]/mode) change from
 0644 to 0640 failed: failed to set mode 644 on /var/log/puppet/http.log: Permission denied - /var
/log/puppet/http.log
Feb 23 03:22:19 i-foreman puppet-master[92076]: Could not prepare for execution: Got 1 failure(s)
while initializing: File[/var/log/puppet/http.log]: change from 0644 to 0640 failed: failed to set
 mode 644 on /var/log/puppet/http.log: Pe
rmission denied - /var/log/puppet/http.log
```

I also get an AVC at the same time:

```
type=AVC msg=audit(1424658139.219:23310): avc:  denied  { setattr } for  pid=92076 comm="ruby" nam
e="http.log" dev="vda2" ino=131193 scontext=system_u:system_r:passenger_t:s0 tcontext=system_u:obj
ect_r:puppet_log_t:s0 tclass=file
```

So my guess it's a bug in the selinux policy.

Agent log output

```
Feb 23 10:09:04 d-hpwtest start-puppet-agent: /usr/share/ruby/vendor_ruby/puppet/agent.rb:87:in `e
xit': no implicit conversion from nil to integer (TypeError)

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/agent.rb:87:
in `block in run_in_fork'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/agent.rb:84:
in `fork'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/agent.rb:84:
in `run_in_fork'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/agent.rb:43:
in `block in run'
```

```
Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:179:in `call'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:179:in `controlled_run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/agent.rb:41:
in `run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/daemon.rb:16
3:in `block in run_event_loop'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/jo
b.rb:49:in `call'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/jo
b.rb:49:in `run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/sc
heduler.rb:39:in `block in run_ready'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/sc
heduler.rb:34:in `each'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/sc
heduler.rb:34:in `run_ready'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/scheduler/sc
heduler.rb:11:in `run_loop'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/daemon.rb:17
9:in `run_event_loop'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/daemon.rb:14
2:in `start'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application/
agent.rb:377:in `main'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application/
agent.rb:323:in `run_command'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:371:in `block (2 levels) in run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:477:in `plugin_hook'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:371:in `block in run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/util.rb:479:
in `exit_on_fail'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/application.
rb:371:in `run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/util/command
_line.rb:137:in `run'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/share/ruby/vendor_ruby/puppet/util/command
_line.rb:91:in `execute'

Feb 23 10:09:04 d-hpwtest start-puppet-agent: from /usr/bin/puppet:8:in `<main>'
```

Associated revisions

Revision 639a8ed2 - 03/09/2015 10:22 AM - Gerwin Krist

fixes #9523 - Allow passenger_t access to puppet_log_t

History

#1 - 02/24/2015 04:44 AM - Dominic Cleal

- Project changed from Foreman to SELinux

- Subject changed from Puppet master stops working every week to Puppet master crashes on AVC when blocking setattr after logrotate

- Category changed from 56 to General Foreman

Seems there's probably a bug in the Puppet logrotate configuration too if it's creating files with mode 0644 instead of 0640.

#2 - 02/24/2015 04:58 AM - Gerwin Krist

FYI:

```
/var/log/puppet/*log {
  missingok
  notifempty
  create 0644 puppet puppet
  sharedscripts
  postrotate
    pkill -USR2 -u puppet -f 'puppet master' || true
    [ -e /etc/init.d/puppet ] && /etc/init.d/puppet reload > /dev/null 2>&1 || true
  endscript
}
```

#3 - 02/24/2015 05:05 AM - Dominic Cleal

Ah yes, it'd be worth raising that small discrepancy over at https://tickets.puppetlabs.com/browse/PUP

https://github.com/puppetlabs/puppet/blob/3.7.4/lib/puppet/defaults.rb#L405 shows the internal configuration that Puppet's trying to assert.

#4 - 03/02/2015 07:58 AM - Gerwin Krist

@Dominic Cleal
Was checking if I can write a patch for the policy. But I don't know if there is a policy for selinux policies :-) I see 2 options:

1. allow passenger_t access to puppet_log_t
2. change /var/log/puppet/(http.log*) to passenger_log_t

Please let me know if you other ideas and I will check if I can fix it :-)

#5 - 03/02/2015 08:25 AM - Dominic Cleal

I think option (1), allowing access to puppet_log_t would be right. You'd need to add setattr here:

https://github.com/theforeman/foreman-selinux/blob/develop/foreman.te#L264

#6 - 03/06/2015 05:43 AM - Gerwin Krist

Made a patch and tested (forced logrotate) it. But I want to wait for the regular logrotation (this monday) and see if that works too. Then will do a pull request.

#7 - 03/09/2015 08:35 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman-selinux/pull/46 added

- Pull request deleted ()

#8 - 03/09/2015 08:47 AM - Gerwin Krist

No problems either with the normale logrotate. Did a pull request

#9 - 03/09/2015 11:01 AM - Anonymous

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 639a8ed2f24ef7a5a6f4348c5824a498e102c913.

#10 - 03/09/2015 11:36 AM - Dominic Cleal

- Assignee set to Gerwin Krist

- translation missing: en.field_release set to 28