SELinux - Support #24616

Passenger does not transition into passenger_t domain

08/14/2018 06:11 PM - Alex Kinneer

Status:	Resolved		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Triaged:	No	**Found in Releases:**	1.17.3, 1.18.0
Fixed in Releases:			

Description

Steps:
1. Minimal install of CentOs 7.4, with SELinux enabled
2.

```
sudo yum -y install https://yum.puppetlabs.com/puppet5/puppet5-release-el-7.noarch.rpm
```

3.

```
sudo yum -y install http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

4.

```
sudo yum -y install https://yum.theforeman.org/releases/1.18/el7/x86_64/foreman-release.rpm
```

5.

```
sudo yum -y install foreman-installer
```

6. Place foreman-answers.yaml file -- foreman-selinux param is left as default (undef), database parameters are configured to point to an external host with postgresql already installed and running.
7.

```
foreman-installer
```

Among the output will be the following, but the installer **does not fail** and reports everything is ready upon completion:

```
libsemanage.semanage_pipe_data: Child process /usr/libexec/selinux/hll/pp failed with code: 255. (
No such file or directory).
foreman: libsepol.policydb_read: policydb module version 19 does not match my version range 4-17
foreman: libsepol.sepol_module_package_read: invalid module in module package (at section 0)
foreman: Failed to read policy package
libsemanage.semanage_direct_commit: Failed to compile hll files into cil files.
 (No such file or directory).
OSError: No such file or directory
ValueError: Type foreman_container_port_t is invalid, must be a port type
```

8. Attempt to connect to web UI, receive the following error dump:

```
could not connect to server: Permission denied
    Is the server running on host "<HOST>" (<IP>) and accepting
    TCP/IP connections on port 5432?
 (PG::ConnectionBad)
  /opt/theforeman/tfm/root/usr/share/gems/gems/pg-0.21.0/lib/pg.rb:59:in `initialize'
  /opt/theforeman/tfm/root/usr/share/gems/gems/pg-0.21.0/lib/pg.rb:59:in `new'
  /opt/theforeman/tfm/root/usr/share/gems/gems/pg-0.21.0/lib/pg.rb:59:in `connect'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/postgresql_adapter.rb:697:in `connect'
```

```
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/postgresql_adapter.rb:221:in `initialize'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/postgresql_adapter.rb:38:in `new'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/postgresql_adapter.rb:38:in `postgresql_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:759:in `new_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:803:in `checkout_new_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:782:in `try_to_checkout_new_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:743:in `acquire_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:500:in `checkout'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:374:in `connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_adapters/abstract/connection_pool.rb:931:in `retrieve_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_handling.rb:116:in `retrieve_connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/connecti
on_handling.rb:88:in `connection'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/schema_m
igration.rb:20:in `table_exists?'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/schema_m
igration.rb:24:in `create_table'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/activerecord-5.1.6/lib/active_record/migratio
n.rb:1125:in `initialize'
  /usr/share/foreman/app/registries/foreman/plugin.rb:321:in `new'
  /usr/share/foreman/app/registries/foreman/plugin.rb:321:in `pending_migrations'
  /usr/share/foreman/app/registries/foreman/plugin.rb:265:in `permission'
  /opt/theforeman/tfm/root/usr/share/gems/gems/foreman_discovery-12.0.2/lib/foreman_discovery/engi
ne.rb:50:in `block (3 levels) in <class:Engine>'
  /usr/share/foreman/app/registries/foreman/plugin.rb:249:in `instance_eval'
  /usr/share/foreman/app/registries/foreman/plugin.rb:249:in `security_block'
  /opt/theforeman/tfm/root/usr/share/gems/gems/foreman_discovery-12.0.2/lib/foreman_discovery/engi
ne.rb:49:in `block (2 levels) in <class:Engine>'
  /usr/share/foreman/app/registries/foreman/plugin.rb:72:in `instance_eval'
  /usr/share/foreman/app/registries/foreman/plugin.rb:72:in `register'
  /opt/theforeman/tfm/root/usr/share/gems/gems/foreman_discovery-12.0.2/lib/foreman_discovery/engi
ne.rb:45:in `block in <class:Engine>'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/initializable.rb:30:
in `instance_exec'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/initializable.rb:30:
in `run'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/initializable.rb:59:
in `block in run_initializers'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:228:in `block in tsort_each'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:350:in `block (2 levels) in each_strongly_connect
ed_component'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:431:in `each_strongly_connected_component_from'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:349:in `block in each_strongly_connected_componen
t'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:347:in `each'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:347:in `call'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:347:in `each_strongly_connected_component'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:226:in `tsort_each'
  /opt/rh/rh-ruby24/root/usr/share/ruby/tsort.rb:205:in `tsort_each'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/initializable.rb:58:
in `run_initializers'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/application.rb:353:i
n `initialize!'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/railtie.rb:185:in `p
ublic_send'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/railties-5.1.6/lib/rails/railtie.rb:185:in `m
```

```
ethod_missing'
  /usr/share/foreman/config/environment.rb:5:in `<top (required)>'
  /opt/rh/rh-ruby24/root/usr/share/rubygems/rubygems/core_ext/kernel_require.rb:55:in `require'
  /opt/rh/rh-ruby24/root/usr/share/rubygems/rubygems/core_ext/kernel_require.rb:55:in `require'
  config.ru:5:in `block in <main>'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/rack-2.0.3/lib/rack/builder.rb:55:in `instanc
e_eval'
  /opt/theforeman/tfm-ror51/root/usr/share/gems/gems/rack-2.0.3/lib/rack/builder.rb:55:in `initial
ize'
  config.ru:1:in `new'
  config.ru:1:in `<main>'
  /usr/share/passenger/helper-scripts/rack-preloader.rb:112:in `eval'
  /usr/share/passenger/helper-scripts/rack-preloader.rb:112:in `preload_app'
  /usr/share/passenger/helper-scripts/rack-preloader.rb:158:in `<module:App>'
  /usr/share/passenger/helper-scripts/rack-preloader.rb:29:in `<module:PhusionPassenger>'
  /usr/share/passenger/helper-scripts/rack-preloader.rb:28:in `<main>'
```

9. Install postgresql client and test same connection parameters manually: database connect is successful.

Workaround:
1. setenforce 0
2. Reload web UI page -- now loads successfully.

audit.log shows numerous errors, of the following three types:

```
type=AVC msg=audit(1534268634.110:304): avc:  denied  { name_connect } for  pid=1848 comm="ruby" d
est=5432 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:postgresql_port_t:s0 tcl
ass=tcp_socket
type=SYSCALL msg=audit(1534268634.110:304): arch=c000003e syscall=42 success=no exit=-13 a0=7 a1=7
620c90 a2=10 a3=7ffd64da5198 items=0 ppid=1847 pid=1848 auid=4294967295 uid=997 gid=994 euid=997 s
uid=997 fsuid=997 egid=994 sgid=994 fsgid=994 tty=(none) ses=4294967295 comm="ruby" exe="/opt/rh/r
h-ruby24/root/usr/bin/ruby" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1534268634.110:304): proctitle=72756279002F7573722F73686172652F7061737365
6E6765722F68656C7065722D736372697074732F7261636B2D7072656C6F616465722E7262
type=AVC msg=audit(1534268634.245:305): avc:  denied  { fowner } for  pid=1858 comm="chmod" capabi
lity=3  scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:system_r:httpd_t:s0 tclass=capabil
ity
type=SYSCALL msg=audit(1534268634.245:305): arch=c000003e syscall=268 success=no exit=-1 a0=ffffff
ffffffff9c a1=1309120 a2=1c0 a3=7ffeca864ba0 items=0 ppid=903 pid=1858 auid=4294967295 uid=0 gid=0
 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="chmod" exe="/usr/bin/
chmod" subj=system_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1534268634.348:315): avc:  denied  { block_suspend } for  pid=903 comm="Passeng
erHelper" capability=36  scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:system_r:httpd_t:
s0 tclass=capability2
type=SYSCALL msg=audit(1534268634.348:315): arch=c000003e syscall=233 success=yes exit=0 a0=9 a1=2
 a2=500000014 a3=12dc440 items=0 ppid=899 pid=903 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=
0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="PassengerHelper" exe="/usr/libexec/passeng
er/PassengerHelperAgent" subj=system_u:system_r:httpd_t:s0 key=(null)
```

I believe this is a recent regression, as it was working as recently as last Friday with 1.17 (a current install of 1.17 following exact same previously successful steps now fails).

History

#1 - 08/14/2018 06:14 PM - Alex Kinneer

- Description updated

#2 - 08/15/2018 07:57 AM - Lukas Zapletal

- Tracker changed from Bug to Support

- Project changed from Foreman to SELinux

- Subject changed from foreman-selinux package (silently) failing on default install; blocks connection to external postgresql host to Passenger does not transition into passenger_t domain

- Priority changed from High to Normal

Hello,

our policy **does** allow connection to postgres on any host, your problem is that passenger process did not change from httpd_t to passneger_t. This usually happens when you have some custom repositories enabled and installer installs incorrect version of passenger. We only support the version we test against which is tfm-rubygem-passenger from "foreman" repository. For some puppet version there can be "passenger" package installed but installer will ignore this non-SCL version as it is used for puppet master.

```
# rpm -qa | grep passenger
tfm-rubygem-passenger-4.0.18-9.12.el7.x86_64
passenger-4.0.53-4.el7.x86_64
tfm-rubygem-passenger-native-libs-4.0.18-9.12.el7.x86_64
mod_passenger-4.0.53-4.el7.x86_64
tfm-rubygem-passenger-native-4.0.18-9.12.el7.x86_64
```

Only these repositories must be enabled:

```
# yum repolist
repo id                                          repo name
           status
base/7/x86_64                                    CentOS-7 - Base
            9,911
centos-sclo-rh/x86_64                            CentOS-7 - SCLo rh
            7,984
centos-sclo-sclo/x86_64                          CentOS-7 - SCLo sclo
              767
*epel/x86_64                                     Extra Packages for Enterprise Linux 7 - x86_64
           12,642
extras/7/x86_64                                  CentOS-7 - Extras
              370
foreman/x86_64                                   Foreman 1.19
              463
foreman-plugins/x86_64                           Foreman plugins 1.19
              245
foreman-rails/x86_64                             Rails SCL for Foreman 1.19
              167
puppet5/x86_64                                   Puppet 5 Repository el 7 - x86_64
               85
updates/7/x86_64                                 CentOS-7 - Updates
            1,054
```

If you want to use untested version of passenger, just do not load "foreman" policy as it will not be compatible.

#3 - 08/15/2018 08:01 AM - Lukas Zapletal

- Status changed from New to Feedback

Correction, passenger is an apache module and tfm-rubygem-passenger is Ruby part of it. They all must come from "foreman" yum repo, not "epel".

#4 - 08/15/2018 03:01 PM - Alex Kinneer

I haven't installed any custom repositories. The steps listed in the description are literally all that I did -- and that's basically just following the quickstart guide from the Foreman manual, run against a clean-slate install of minimal CentOS 7. To highlight what I mentioned in the description, a key observation is that those **exact** same steps, and I mean **exact same** (they were scripted, actually) worked as recently as five days ago. It would seem that whatever version of passenger is being installed, it is being done by foreman-installer based only on the repos the Foreman manual instructs to be configured. Perhaps an untested version of passenger somehow erroneously made it into the Foreman repo? Or could there be some other package dependency being pulled from a CentOS mirror, for which the latest version on the mirror has advanced to a new incompatible version?

Net effect is that the quickstart installation instructions in the manual for the latest version produce a broken install for a fairly standard setup scenario. In my mind, this looks like something that ought to qualify as a high priority issue.

This is the repolist from the affected host:

```
[root@foreman centos]# yum repolist
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.osuosl.org
 * epel: mirror.steadfastnet.com
 * extras: mirrors.advancedhosters.com
 * updates: centos.mirror.constant.com
repo id                                                    repo name
                                  status
!base/7/x86_64                                             CentOS-7 - Base
                                   9,911
```

```
!centos-sclo-rh/x86_64                                  CentOS-7 - SCLo rh
                                                7,984
!centos-sclo-sclo/x86_64                                CentOS-7 - SCLo sclo
                                                  767
*!epel/x86_64                                           Extra Packages for Enterprise Linux 7 - x86_64
                                               12,642
!extras/7/x86_64                                        CentOS-7 - Extras
                                                  370
!foreman/x86_64                                         Foreman 1.18
                                                  561
!foreman-plugins/x86_64                                 Foreman plugins 1.18
                                                  291
!puppet5/x86_64                                         Puppet 5 Repository el 7 - x86_64
                                                   85
!tfm-ror51/x86_64                                       Rails 5.1 SCL
                                                  167
!updates/7/x86_64                                       CentOS-7 - Updates
                                                1,042
```

#5 - 08/16/2018 08:46 AM - Lukas Zapletal

Such an issue is high severity for sure, once confirmed. Thanks for reporting.

I am unable to reproduce this with 1.18, I just installed it this morning with more-or-less default settings and everything works fine. Few unrelated denials:

```
[root@foreman ~]# ausearch -m AVC
----
time->Thu Aug 16 08:24:43 2018
type=PROCTITLE msg=audit(1534404283.888:133): proctitle=2F7362696E2F6B65786563002D70002D2D636F6D6D616E642D6C69
6E653D424F4F545F494D4147453D2F766D6C696E757A2D332E31302E302D3836322E31312E362E656C372E7838365F363420726F20636F
6E736F6C653D747479302072645F4E4F5F504C594D4F55544820636F6E736F6C653D74747953302C313135323030
type=SYSCALL msg=audit(1534404283.888:133): arch=c000003e syscall=2 success=no exit=-13 a0=7ffc71d62f5f a1=0 a
2=1b6 a3=7ffc71d60d20 items=0 ppid=923 pid=9795 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=
0 fsgid=0 tty=(none) ses=4294967295 comm="kexec" exe="/usr/sbin/kexec" subj=system_u:system_r:kdump_t:s0 key=(
null)
type=AVC msg=audit(1534404283.888:133): avc:  denied  { read } for  pid=9795 comm="kexec" name="vmlinuz-3.10.0
-862.11.6.el7.x86_64" dev="vda2" ino=82 scontext=system_u:system_r:kdump_t:s0 tcontext=system_u:object_r:unlab
eled_t:s0 tclass=file
----
time->Thu Aug 16 08:24:43 2018
type=PROCTITLE msg=audit(1534404283.888:134): proctitle=2F7362696E2F6B65786563002D70002D2D636F6D6D616E642D6C69
6E653D424F4F545F494D4147453D2F766D6C696E757A2D332E31302E302D3836322E31312E362E656C372E7838365F363420726F20636F
6E736F6C653D747479302072645F4E4F5F504C594D4F55544820636F6E736F6C653D74747953302C313135323030
type=SYSCALL msg=audit(1534404283.888:134): arch=c000003e syscall=2 success=no exit=-13 a0=7ffc71d62f5f a1=0 a
2=1b6 a3=24 items=0 ppid=923 pid=9795 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=(none) ses=4294967295 comm="kexec" exe="/usr/sbin/kexec" subj=system_u:system_r:kdump_t:s0 key=(null)
type=AVC msg=audit(1534404283.888:134): avc:  denied  { read } for  pid=9795 comm="kexec" name="vmlinuz-3.10.0
-862.11.6.el7.x86_64" dev="vda2" ino=82 scontext=system_u:system_r:kdump_t:s0 tcontext=system_u:object_r:unlab
eled_t:s0 tclass=file
----
time->Thu Aug 16 08:24:43 2018
type=PROCTITLE msg=audit(1534404283.888:135): proctitle=2F7362696E2F6B65786563002D70002D2D636F6D6D616E642D6C69
6E653D424F4F545F494D4147453D2F766D6C696E757A2D332E31302E302D3836322E31312E362E656C372E7838365F363420726F20636F
6E736F6C653D747479302072645F4E4F5F504C594D4F55544820636F6E736F6C653D74747953302C313135323030
type=SYSCALL msg=audit(1534404283.888:135): arch=c000003e syscall=2 success=no exit=-13 a0=7ffc71d62f5f a1=0 a
2=0 a3=7ffc71d60ce0 items=0 ppid=923 pid=9795 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
fsgid=0 tty=(none) ses=4294967295 comm="kexec" exe="/usr/sbin/kexec" subj=system_u:system_r:kdump_t:s0 key=(nu
ll)
type=AVC msg=audit(1534404283.888:135): avc:  denied  { read } for  pid=9795 comm="kexec" name="vmlinuz-3.10.0
-862.11.6.el7.x86_64" dev="vda2" ino=82 scontext=system_u:system_r:kdump_t:s0 tcontext=system_u:object_r:unlab
eled_t:s0 tclass=file
```

Can you help me identifying what you configured differently? You said external postgres database? Can you attach the answer file perhaps?

#6 - 08/23/2018 04:34 PM - Alex Kinneer

I was out for a few days, but issue still appears to be reproducible for me. This is my answers file:

```
# Format:
# <classname>: false - don't include this class
# <classname>: true - include and use the defaults
# <classname>:
#   <param>: <value> - include and override the default(s)
#
```

```
# See params.pp in each class for what options are available

---
foreman:
  foreman_url: https://<HOST_FQDN>
  puppetrun: false
  unattended: true
  unattended_url:
  authentication: true
  passenger: true
  passenger_ruby: /usr/bin/tfm-ruby
  passenger_ruby_package: tfm-rubygem-passenger-native
  plugin_prefix: tfm-rubygem-foreman_
  use_vhost: true
  servername: <HOST_FQDN>
  serveraliases:
  - foreman
  ssl: true
  custom_repo: true
  repo: stable
  configure_epel_repo: true
  configure_scl_repo: true
  selinux:
  gpgcheck: true
  version: present
  plugin_version: present
  db_manage: false
  db_type: postgresql
  db_adapter: postgresql
  db_host: <DB_HOST_FQDN>
  db_port: 5432
  db_database: foreman_db_prod
  db_username: foreman
  db_password: <DB_PASSWORD>
  db_sslmode:
  db_root_cert:
  db_pool: 5
  db_manage_rake: true
  app_root: /usr/share/foreman
  manage_user: true
  user: foreman
  group: foreman
  user_groups:
  - puppet
  rails_env: production
  puppet_home: /var/lib/puppet
  puppet_ssldir: /etc/puppetlabs/puppet/ssl
  locations_enabled: false
  organizations_enabled: false
  passenger_interface:
  vhost_priority: '05'
  server_port: 80
  server_ssl_port: 443
  server_ssl_ca: /etc/httpd/ssl/crt/ca_bundle.pem
  server_ssl_chain: /etc/httpd/ssl/crt/ca_bundle.pem
  server_ssl_cert: /etc/httpd/ssl/crt/<HOST_FQDN>.crt
 server_ssl_certs_dir: ''
  server_ssl_key: /etc/httpd/ssl/private/<HOST_FQDN>.key
  server_ssl_crl: ''
  server_ssl_protocol:
  client_ssl_ca: /etc/puppetlabs/puppet/ssl/certs/ca.pem
  client_ssl_cert: /etc/puppetlabs/puppet/ssl/certs/<HOST_FQDN>.pem
  client_ssl_key: /etc/puppetlabs/puppet/ssl/private_keys/<HOST_FQDN>.pem
  keepalive: true
  max_keepalive_requests: 100
  keepalive_timeout: 5
  oauth_active: true
  oauth_map_users: false
  oauth_consumer_key: <OAUTH_KEY>
  oauth_consumer_secret: <OAUTH_SECRET>
  passenger_prestart: true
  passenger_min_instances: 1
  passenger_start_timeout: 90
  admin_username: admin
  admin_password: <ADMIN_PASSWORD>
```

```
  admin_first_name:
  admin_last_name:
  admin_email: akinneer@nvidia.com
  initial_organization: Nvidia Corporation
  initial_location:
  ipa_authentication: false
  http_keytab: /etc/httpd/conf/http.keytab
  pam_service: foreman
  ipa_manage_sssd: true
  websockets_encrypt: true
  websockets_ssl_key: /etc/httpd/ssl/private/<HOST_FQDN>.key
  websockets_ssl_cert: /etc/httpd/ssl/crt/<HOST_FQDN>.crt
  logging_level: debug
  logging_type: file
  logging_layout: pattern
  loggers: {}
  email_config_method: database
  email_conf: email.yaml
  email_source: email.yaml.erb
  email_delivery_method:
  email_smtp_address:
  email_smtp_port: 25
  email_smtp_domain:
  email_smtp_authentication: none
  email_smtp_user_name:
  email_smtp_password:
  telemetry_prefix: fm_rails
  telemetry_prometheus_enabled: false
  telemetry_statsd_enabled: false
  telemetry_statsd_host: 127.0.0.1:8125
  telemetry_statsd_protocol: statsd
  telemetry_logger_enabled: false
  telemetry_logger_level: DEBUG
  dynflow_pool_size: 5
  jobs_service:
  dynflow_in_core: true
  hsts_enabled: true
foreman::cli:
  foreman_url: https://<HOST_FQDN>
  version: installed
  manage_root_config: true
  username:
  password:
  refresh_cache: false
  request_timeout: 120
  ssl_ca_file: /etc/puppetlabs/puppet/ssl/certs/ca.pem
  hammer_plugin_prefix: tfm-rubygem-hammer_cli_
foreman::cli::openscap: false
foreman_proxy: false
puppet:
  version: present
  user: puppet
  group: puppet
  dir: /etc/puppetlabs/puppet
  codedir: /etc/puppetlabs/code
  vardir: /opt/puppetlabs/puppet/cache
  logdir: /var/log/puppetlabs/puppet
  rundir: /var/run/puppetlabs
  ssldir: /etc/puppetlabs/puppet/ssl
  sharedir: /opt/puppetlabs/puppet
  manage_packages: true
  dir_owner: root
  dir_group:
  package_provider:
  package_source:
  port: 8140
  listen: false
  listen_to: []
  pluginsync: true
  splay: false
  splaylimit: '1800'
  autosign: /etc/puppetlabs/puppet/autosign.conf
  autosign_entries: []
  autosign_mode: '0664'
  autosign_content:
```

```
autosign_source:
runinterval: 1800
usecacheonfailure: true
runmode: service
unavailable_runmodes: []
cron_cmd:
systemd_cmd:
systemd_randomizeddelaysec: 0
agent_noop: false
show_diff: false
module_repository:
configtimeout:
ca_server:
ca_port:
ca_crl_filepath:
prerun_command:
postrun_command:
dns_alt_names: []
use_srv_records: false
srv_domain: <DOMAIN>
pluginsource: puppet:///plugins
pluginfactsource: puppet:///pluginfacts
additional_settings: {}
agent_additional_settings: {}
agent_restart_command: /usr/bin/systemctl reload-or-restart puppet
classfile: $statedir/classes.txt
hiera_config: $confdir/hiera.yaml
auth_template: puppet/auth.conf.erb
allow_any_crl_auth: false
auth_allowed:
- $1
client_package:
- puppet-agent
agent: true
remove_lock: true
report: true
client_certname: <HOST_FQDN>
puppetmaster:
systemd_unit_name: puppet-run
service_name: puppet
syslogfacility:
environment: production
server: true
server_admin_api_whitelist:
- localhost
- <HOST_FQDN>
server_manage_user: true
server_user: puppet
server_group: puppet
server_dir: /etc/puppetlabs/puppet
server_ip: 0.0.0.0
server_port: 8140
server_ca: true
server_ca_crl_sync: false
server_crl_enable:
server_ca_auth_required: true
server_ca_client_whitelist:
- localhost
- <HOST_FQDN>
server_http: false
server_http_port: 8139
server_http_allow: []
server_reports: foreman
server_implementation: puppetserver
server_passenger: true
server_puppetserver_dir: /etc/puppetlabs/puppetserver
server_puppetserver_vardir: /opt/puppetlabs/server/data/puppetserver
server_puppetserver_rundir: /var/run/puppetlabs/puppetserver
server_puppetserver_logdir: /var/log/puppetlabs/puppetserver
server_puppetserver_version: 5.1.0
server_service_fallback: true
server_passenger_min_instances: 2
server_passenger_pre_start: true
server_passenger_ruby:
server_httpd_service: httpd
```

```
server_external_nodes: /etc/puppetlabs/puppet/node.rb
server_cipher_suites:
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
server_config_version:
server_connect_timeout: 120000
server_git_repo: false
server_dynamic_environments: false
server_directory_environments: true
server_default_manifest: false
server_default_manifest_path: /etc/puppet/manifests/default_manifest.pp
server_default_manifest_content: ''
server_environments:
- production
server_environments_owner: puppet
server_environments_group:
server_environments_mode: '0755'
server_envs_dir: /etc/puppetlabs/code/environments
server_envs_target:
server_common_modules_path:
- /etc/puppetlabs/code/environments/common
- /etc/puppetlabs/code/modules
- /opt/puppetlabs/puppet/modules
- /usr/share/puppet/modules
server_git_repo_mode: '0755'
server_git_repo_path: /opt/puppetlabs/puppet/cache/puppet.git
server_git_repo_group: puppet
server_git_repo_user: puppet
server_git_branch_map: {}
server_idle_timeout: 1200000
server_post_hook_content: puppet/server/post-receive.erb
server_post_hook_name: post-receive
server_storeconfigs_backend:
server_app_root: /etc/puppetlabs/puppet/rack
server_ruby_load_paths:
- /opt/puppetlabs/puppet/lib/ruby/vendor_ruby
server_ssl_dir: /etc/puppetlabs/puppet/ssl
server_ssl_dir_manage: true
server_ssl_key_manage: true
server_ssl_protocols:
- TLSv1.2
server_ssl_chain_filepath: /etc/puppetlabs/puppet/ssl/ca/ca_crt.pem
server_package:
server_version:
server_certname: <HOST_FQDN>
server_enc_api: v2
server_report_api: v2
server_request_timeout: 60
server_ca_proxy:
server_strict_variables: false
server_additional_settings: {}
server_rack_arguments: []
server_foreman: true
server_foreman_url: https://<HOST_FQDN>
server_foreman_ssl_ca:
server_foreman_ssl_cert:
server_foreman_ssl_key:
server_foreman_facts: true
server_puppet_basedir: /opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet
server_puppetdb_host:
server_puppetdb_port: 8081
server_puppetdb_swf: false
server_parser: current
server_environment_timeout:
server_jvm_java_bin: /usr/bin/java
server_jvm_config: /etc/sysconfig/puppetserver
server_jvm_min_heap_size: 2G
server_jvm_max_heap_size: 2G
server_jvm_extra_args: -Djruby.logger.class=com.puppetlabs.jruby_utils.jruby.Slf4jLogger
server_jvm_cli_args:
server_jruby_gem_home: /opt/puppetlabs/server/data/puppetserver/jruby-gems
server_max_active_instances: 2
server_max_requests_per_instance: 0
```

```
  server_max_queued_requests: 0
  server_max_retry_delay: 1800
  server_use_legacy_auth_conf: false
  server_check_for_updates: true
  server_environment_class_cache_enabled: false
  server_allow_header_cert_info: false
  server_web_idle_timeout: 30000
  server_puppetserver_jruby9k: false
  server_puppetserver_metrics: true
  server_metrics_jmx_enable: true
  server_metrics_graphite_enable: false
  server_metrics_graphite_host: 127.0.0.1
  server_metrics_graphite_port: 2003
  server_metrics_server_id: <HOST_FQDN>
  server_metrics_graphite_interval: 5
  server_metrics_allowed:
  server_puppetserver_experimental: true
  server_puppetserver_trusted_agents: []
  server_compile_mode:
foreman::plugin::ansible: false
foreman::plugin::azure: false
foreman::plugin::bootdisk: false
foreman::plugin::chef: false
foreman::plugin::cockpit: false
foreman::plugin::default_hostgroup: false
foreman::plugin::dhcp_browser: false
foreman::plugin::digitalocean: false
foreman::plugin::discovery: {}
foreman::plugin::docker: false
foreman::plugin::expire_hosts: false
foreman::plugin::hooks: {}
foreman::plugin::host_extra_validator: false
foreman::plugin::memcache: false
foreman::plugin::monitoring: false
foreman::plugin::omaha: false
foreman::plugin::openscap: false
foreman::plugin::ovirt_provision: false
foreman::plugin::puppetdb: false
foreman::plugin::remote_execution: {}
foreman::plugin::salt: false
foreman::plugin::setup: {}
foreman::plugin::tasks:
  package: tfm-rubygem-foreman-tasks
  automatic_cleanup: false
  cron_line: 45 19 * * *
foreman::plugin::templates: false
foreman::compute::ec2: false
foreman::compute::gce: false
foreman::compute::libvirt: false
foreman::compute::openstack: false
foreman::compute::ovirt: false
foreman::compute::rackspace: false
foreman::compute::vmware: false
foreman_proxy::plugin::abrt: false
foreman_proxy::plugin::ansible: false
foreman_proxy::plugin::chef: false
foreman_proxy::plugin::dhcp::infoblox: false
foreman_proxy::plugin::dhcp::remote_isc: false
foreman_proxy::plugin::discovery: false
foreman_proxy::plugin::dns::infoblox: false
foreman_proxy::plugin::dhcp::remote_isc: false
foreman_proxy::plugin::discovery: false
foreman_proxy::plugin::dns::infoblox: false
foreman_proxy::plugin::dns::powerdns: false
foreman_proxy::plugin::dynflow: false
foreman_proxy::plugin::monitoring: false
foreman_proxy::plugin::omaha: false
foreman_proxy::plugin::openscap: false
foreman_proxy::plugin::pulp: false
foreman_proxy::plugin::remote_execution::ssh: false
foreman_proxy::plugin::salt: false
```

#7 - 08/27/2018 09:05 AM - Lukas Zapletal

Could you attach/pastebin full puppet log? That's output of foreman-installer -v. I need to see the initial run to see order of puppet module execution.

#8 - 08/27/2018 03:01 PM - Alex Kinneer

- File foreman_setup.log added

Attached the requested log data.

#9 - 08/28/2018 01:03 PM - Lukas Zapletal

- Status changed from Feedback to Closed

Now I understand the problem, the root issue is that your OS is not updated therefore selinux stack is old and cannot load our new policy which was likely built against CentOS 7.5. The error is:

```
# foreman-selinux-enable
foreman: libsepol.policydb_read: policydb module version 19 does not match my version range 4-17
```

This prevents the policy from being loaded, therefore foreman stays in httpd_t and it cannot connect to postgresql because httpd_t is not allowed to do so.

Workaround: Update your system to latest and greatest CentOS, or at least all selinux packages and kernel. Restart the system. Then enable foreman policy via foreman-selinux-enable and restart all Foreman services (httpd basically).

Here are logs from the build:

http://koji.katello.org/kojifiles/packages/foreman-selinux/1.18.1/1.el7/data/logs/noarch/installed_pkgs.log

I am going to close this issue, further discussion at https://community.theforeman.org/t/minimum-centos-version-requirement-for-1-18-is-7-5/10908

#10 - 10/15/2018 09:18 AM - Tomer Brisker

- Status changed from Closed to Resolved

Files

foreman_setup.log	209 KB	08/27/2018	Alex Kinneer