

Smart Proxy - Bug #6505

Puppet certificate permission issue on Ubuntu Trusty

07/07/2014 06:30 AM - Phil Ingram

Status:	Resolved	
Priority:	Normal	
Assignee:		
Category:		
Target version:		
Difficulty:		Fixed in Releases:
Triaged:		Found in Releases:
Bugzilla link:		Red Hat JIRA:
Pull request:		

Description

The foreman-proxy user is a member of the puppet group, but the default permissions on the puppet directories do not permit members of the puppet group to get through to the private_keys folder - where the private key is also improperly moded.

I have created a host with forman and assigned the foreman-proxy puppet module to the host.

```
root@spl:~# puppet agent -t -v
Info: Retrieving plugin
Info: Loading facts in /var/lib/puppet/lib/facter/iptables_persistent_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/concat_basedir.rb
Info: Loading facts in /var/lib/puppet/lib/facter/root_home.rb
Info: Loading facts in /var/lib/puppet/lib/facter/ip6tables_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/pe_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/iptables_version.rb
Info: Loading facts in /var/lib/puppet/lib/facter/facter_dot_d.rb
Info: Loading facts in /var/lib/puppet/lib/facter/puppet_vardir.rb
Info: Caching catalog for spl.domain.name
Info: Applying configuration version '1404703198'
Error: /Stage[main]/Foreman_proxy::Register/Foreman_smartproxy[spl.domain.name]: Could not evaluate: Connection refused - connect(2)
Notice: Finished catalog run in 0.90 seconds
```

Manually starting the service shows the issue

```
root@spl:/var/lib/puppet/ssl# /etc/init.d/foreman-proxy restart
* Restarting foreman-proxy foreman-proxy

        Unable to access the SSL keys. Are the values correct in settings.yml and do permissions allow reading?: Permission denied - /var/lib/puppet/ssl/private_keys/spl.domain.name.pem
        from /usr/share/foreman-proxy/lib/smart_proxy.rb:65:in `rescue in <class:SmartProxy>'
```

```
root@spl:/var/lib/puppet/ssl# ls -lha
total 32K
drwxrwx--- 7 puppet root  4.0K Jul  7 09:12 .
drwxr-x--x 9 puppet puppet 4.0K Jul  7 09:12 ..
drwxr-xr-x 2 puppet root  4.0K Jul  7 09:12 certificate_requests
drwxr-xr-x 2 puppet root  4.0K Jul  7 09:12 certs
-rw-r--r-- 1 puppet puppet 2.0K Jul  7 09:12 crt.pem
drwxr-x--- 2 puppet root  4.0K Jul  7 09:12 private
drwxr-x--- 2 puppet root  4.0K Jul  7 09:12 private_keys
drwxr-xr-x 2 puppet root  4.0K Jul  7 09:12 public_keys
```

```
root@spl:/var/lib/puppet/ssl# ls -lha private_keys/
total 12K
drwxr-x--- 2 puppet root  4.0K Jul  7 09:12 .
drwxrwx--- 7 puppet root  4.0K Jul  7 09:12 ..
```

```
-rw----- 1 puppet puppet 3.2K Jul  7 09:12 sp1.domain.name.pem
```

I am able to "chmod o+x" on the puppet and ssl directories, but I can not fix this issue with the private_keys folder or key file because of:

/usr/lib/ruby/vendor_ruby/puppet/defaults.rb

```
  :hostprivkey => {
    :default => "$privatekeydir/$certname.pem",
    :type    => :file,
    :mode    => 0600,
    :owner   => "service",
    :desc    => "Where individual hosts store and look for their private key."
  },
<output omitted>
  :privatekeydir => {
    :default => "$ssldir/private_keys",
    :type    => :directory,
    :mode    => 0750,
    :owner   => "service",
    :desc    => "The private key directory."
  },
```

History

#1 - 05/01/2016 12:21 PM - Anonymous

- Status changed from *New* to *Resolved*

This was fixed by setting the permissions also in puppet.conf.