Installer - Bug #25759

Installer works only when foreman_ssl_ca exists

12/30/2018 09:25 AM - Dor Pinhas

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

Description

Hello,

I'm running Foreman and Proxy on the same box, Foreman is signed with a known CA.
I implemented CAChain to validate SSL connection.

I faced SSL verification problem when deploying a dynflow service, after lots of troubleshooting found the below doc:
https://theforeman.org/2015/11/foreman-ssl.html

```
'make sure foreman_ssl_ca is not defined in /etc/foreman-proxy/settings.yaml and it will read the 
CA from the main foreman settings.'
```

Once removed foreman_ssl_ca - Foreman was able to verify dynflow requests.
Currently, I want to change the installer answer file to allow that change, tried to remove that line from foreman-answers.yaml and got the below exception:

```
 /Stage[main]/Foreman_proxy::Register/Foreman_smartproxy[TLV1 proxy]: Exception SSL_connect return
ed=1 errno=0 state=error: certificate verify failed in get request to: https://theforeman.eng.lab.
tlv.redhat.com/api/v2/smart_proxies?search=name=%22TLV1%20proxy%22
```

This make sense because Foreman is tried to register the proxy and couldn't verify the proxy without the CAChain.
Whne greped that argument I found the foreman_proxy module is using that

```
[root@theforeman ~]# grep -ir "foreman_ssl_ca" /etc
/etc/foreman-installer/scenarios.d/foreman-answers.yaml.pem:  foreman_ssl_ca:
/etc/foreman-installer/scenarios.d/foreman-answers.yaml.pem:  server_foreman_ssl_ca:
/etc/foreman-installer/scenarios.d/foreman-answers.yaml:  foreman_ssl_ca: /etc/pki/tls/certs/RHCha
in.cer
/etc/foreman-installer/scenarios.d/foreman-answers.yaml:  server_foreman_ssl_ca: /etc/pki/tls/cert
s/RHChain.cer
/etc/foreman-installer/scenarios.d/foreman-answers.yaml.rh:  foreman_ssl_ca: /etc/pki/tls/certs/RH
Chain.cer
/etc/foreman-installer/scenarios.d/foreman-answers.yaml.rh:  server_foreman_ssl_ca:
/etc/foreman-proxy/settings.yml::foreman_ssl_ca: /etc/pki/tls/certs/RHChain.cer
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/manifests/register.pp:      ssl
_ca          => pick($foreman_proxy::foreman_ssl_ca, $foreman_proxy::ssl_ca),
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/manifests/init.pp:# $foreman_ss
l_ca::              SSL CA used to verify connections when accessing the Foreman API.
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/manifests/init.pp:  Optional[St
dlib::Absolutepath] $foreman_ssl_ca = $::foreman_proxy::params::foreman_ssl_ca,
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/manifests/params.pp:  $foreman_
ssl_ca  = undef
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/manifests/plugin/ansible.pp:  $
foreman_ssl_ca = pick($::foreman_proxy::foreman_ssl_ca, $::foreman_proxy::ssl_ca)
```

```
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/settings.yml.erb:<% unless [nil, :undefined, :undef].include?(scope.lookupvar("foreman_proxy::foreman_ssl_ca")) -%>
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/settings.yml.erb::foreman_ssl_ca: <%= scope.lookupvar("foreman_proxy::foreman_ssl_ca") %>
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/settings.yml.erb:#:foreman_ssl_ca: ssl/certs/ca.pem
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/plugin/ansible.cfg.erb:verify_certs = <%= @foreman_ssl_ca %>
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/plugin/dynflow_core.yml.erb:<% if [nil, :undefined, :undef].include?(scope.lookupvar("foreman_proxy::foreman_ssl_ca")) -%>
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/plugin/dynflow_core.yml.erb:#:foreman_ssl_ca: ssl/certs/ca.pem
/etc/puppetlabs/code/environments/production/modules/foreman_proxy/templates/plugin/dynflow_core.yml.erb::foreman_ssl_ca: <%= scope.lookupvar("foreman_proxy::foreman_ssl_ca") %>
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/server.pp:# $foreman_ssl_ca::            SSL CA of the Foreman server
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/server.pp:  Optional[Stdlib::Absolutepath] $foreman_ssl_ca = $::puppet::server_foreman_ssl_ca,
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/server/config.pp:      ssl_ca         => pick($::puppet::server::foreman_ssl_ca, $::puppet::server::ssl_ca_cert),
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/init.pp:# $server_foreman_ssl_ca::                  SSL CA of the Foreman server
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/init.pp:  Optional[Stdlib::Absolutepath] $server_foreman_ssl_ca = $puppet::params::server_foreman_ssl_ca,
/etc/puppetlabs/code/environments/production/modules/puppet/manifests/params.pp:  $server_foreman_ssl_ca   = undef
/etc/puppetlabs/code/environments/production/modules/foreman/lib/puppet/functions/foreman/foreman.rb:        http.ca_file = tfmproxy[:foreman_ssl_ca]
/etc/puppetlabs/code/environments/production/modules/foreman/lib/puppet/parser/functions/foreman.rb:        http.ca_file = tfmproxy[:foreman_ssl_ca]
/etc/smart_proxy_dynflow_core/settings.yml::foreman_ssl_ca: /etc/pki/tls/certs/RHChain.cer
```

How can i modify the installer that proxy/settings.yaml won't have the foreman_ssl_ca but the puppet module that does the deployment does?

History

#1 - 12/30/2018 04:04 PM - Ewoud Kohl van Wijngaarden

https://github.com/theforeman/puppet-foreman_proxy is the puppet module that manages the file. In particular https://github.com/theforeman/puppet-foreman_proxy/blob/master/templates/settings.yml.erb is the template that's used. It is possible that it used to be possible to pass in an empty string but along the way we became stricter. However,

> Once removed foreman_ssl_ca - Foreman was able to verify dynflow requests.

This sounds wrong. The code usually doesn't verify the CA if none is given. It probably works because it simply isn't validating at all:

https://github.com/theforeman/smart-proxy/blob/b0b675fb94599b6790120662d192375b800eb08d/lib/proxy/request.rb#L65-L75

It may be possible dynflow behaves different though.

#2 - 04/23/2020 01:40 PM - Zach Huntington-Meath

- Triaged changed from No to Yes