Installer - Bug #15550

SSL Certificate mismatch when installing with the installer

06/30/2016 08:00 AM - Callum Scott

Status:	Closed		
Priority:	Normal		
Assignee:	Dominic Cleal		
Category:	foreman-installer script		
Target version:	1.13.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.12.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-puppet/pull/444		

Description

I consistently get the following error in the foreman-ssl_error_ssl.log

[Thu Jun 30 11:41:00.650431 2016] [ssl:emerg] [pid 6384] AH02238: Unable to configure RSA server private key
[Thu Jun 30 11:41:00.650484 2016] [ssl:emerg] [pid 6384] SSL Library Error: error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch

A modulus check of the certificates shows them to be good, and deleting and recreating the certs using the puppet tools give the same results.

Im attempting the install on a vanilla Centos7 box. Specifically the above error was generated on a vagrant box using the puppet labs nocm centos7 box, but i get it on Backspace and AWS VM's also.

To recreate spin up a box and follow the installation quick start guide. No additional options were setup for the installer.

Related issues:

Has duplicate Installer - Bug #15302: Ordering of certificate generation caus...	**Duplicate**	**06/06/2016**

Associated revisions

Revision a282dff4 - 10/18/2016 06:38 PM - Dominic Cleal

fixes #15550 - start Puppet agent after server is running

Ensures no race condition will occur between the generate CA step of the
server configuration and the agent starting up, generating its own
private key.

closes GH-444

History

#1 - 07/01/2016 06:35 AM - Callum Scott

There is a SSLCARevocationFile Directive that points to /etc/puppetlabs/puppet/ssl/crl.pem which doesn't exist.

Changing SSLCARecovationFile to SSLCARecovationPath and omitting the file name from above works.

#2 - 07/01/2016 06:42 AM - Dominic Cleal

The file should be generated by the Puppet CA generation, along with /etc/puppetlabs/puppet/ssl/ca/. If the CA isn't generated at all then the agent probably already has a certificate of its own (from another CA?) and so the installation step may be skipped.

#3 - 07/11/2016 08:51 AM - Nux Ro

Dominic Cleal wrote:

> The file should be generated by the Puppet CA generation, along with /etc/puppetlabs/puppet/ssl/ca/. If the CA isn't generated at all then the agent probably already has a certificate of its own (from another CA?) and so the installation step may be skipped.

Hi,

I am also hitting this problem on a fresh CentOS 7 install. HTTPD fails to start after having run foreman-installer:
"AH02238: Unable to configure RSA server private key
SSL Library Error: error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch"

It's not clear what's the workaround here. Please advise.

#4 - 07/27/2016 02:13 PM - Daniel Augustin

I can also confirm the above behavior with a fresh centos 7 installation on VirtualBox.

Here is the history, should be reproducible:

```
yum -y update
yum -y localinstall https://yum.puppetlabs.com/puppetlabs-release-pc1-el-7.noarch.rpm
yum -y localinstall https://yum.theforeman.org/releases/1.12/el7/x86_64/foreman-release.rpm
yum -y install epel-release virt-who
yum -y install foreman-installer
foreman-installer \
  --enable-foreman-plugin-ansible \
  --enable-foreman-plugin-bootdisk \
  --enable-foreman-plugin-dhcp-browser \
  --enable-foreman-plugin-docker \
  --enable-foreman-plugin-puppetdb \
  --enable-foreman-compute-libvirt \
  --enable-foreman-compute-openstack \
  --enable-foreman-compute-ovirt \
  --enable-foreman-proxy-plugin-pulp \
  --enable-foreman-proxy-plugin-remote-execution-ssh

# tail -2 /var/log/httpd/foreman-ssl_error_ssl.log
[Wed Jul 27 20:05:36.959424 2016] [ssl:emerg] [pid 16115] AH02238: Unable to configure RSA server private key
[Wed Jul 27 20:05:36.959441 2016] [ssl:emerg] [pid 16115] SSL Library Error: error:0B080074:x509 certificate r
outines:X509_check_private_key:key values mismatch
```

#5 - 07/28/2016 03:03 PM - Daniel Lobato Garcia

I tried to debug this a bit with rfkrocktk on IRC - https://gist.github.com/dLobatog/a573481138ced85cefd96ff0508e98c9 seemed to workaround the issue (the 2nd time foreman-installer finished successfully)

#6 - 07/30/2016 04:03 AM - Daniel Augustin

The gist above results in a starting httpd, however chrome complains about SSL with "ERR_SSL_SERVER_CERT_BAD_FORMAT". Firefox connects, though. I think there is something very wrong in the new way of generating certificates.

#7 - 08/23/2016 11:47 AM - bryan cochrane

I ran through the gist and foreman-installer still gives some errors.

```
/opt/puppetlabs/bin/puppet cert --generate ee-puppet returned 24 instead of one of [0]
 /Stage[main]/Puppet::Server::Config/Exec[puppet_server_config-generate_ca_cert]/returns: change from notrun t
o 0 failed: /opt/puppetlabs/bin/puppet cert --generate ee-puppet returned 24 instead of one of [0]
```

Something went wrong! Check the log for ERROR-level output

#8 - 08/24/2016 06:46 AM - bryan cochrane

The certificate file from 05-foreman-ssl.conf is the puppet generated /etc/puppetlabs/puppet/ssl/certs/hostname.pem. Has anyone tried replacing with a valid cert from a CA or a self signed cert?

#9 - 10/17/2016 05:54 AM - Dominic Cleal

- Has duplicate Bug #15302: Ordering of certificate generation causes private key mismatch added

#10 - 10/17/2016 07:17 AM - Dominic Cleal

- Status changed from New to Ready For Testing

- Assignee set to Dominic Cleal

- Pull request https://github.com/theforeman/puppet-puppet/pull/444 added

I think this can occur due to a race generating the private key between the Puppet agent starting, and the "puppet cert generate $fqdn" command run by the installer.

The agent will create a private key, but nothing else as it's not got a master or CA, while the generate command will create a private key for the host and then sign it with a new CA cert. If the agent process is still generating the key while the generate command has already written its key, the key will then be overwritten with the agent's key, which differs from the key used for the generated cert.

This can be seen if you slow down the key generation in the agent by editing ssl/key.rb in the Puppet installation, adding sleep 5 if ARGV == ['agent'] into the #generate method, deleting the SSL dir, then running service puppet start and puppet cert generate $fqdn in parallel. The key/cert will not match as the key is overwritten by the slower agent.

#11 - 10/18/2016 06:47 PM - Anonymous

- Status changed from Ready For Testing to Closed

PR merged

#12 - 10/21/2016 09:22 AM - Dominic Cleal

- translation missing: en.field_release set to 190