Installer - Bug #26088
httpd fails to start after installing capsule in FIPS mode
02/19/2019 04:22 PM - Ivan Necas

Status: Closed
Priority: Normal
Assignee: Ivan Necas
Category: Foreman modules
Target version: 1.22.0

Pull request: https://github.com/theforeman/puppet-certs/pull/243

Triage: No

Bugzilla link: 1678322

Description

Steps to Reproduce:
1. install katello server in fips mode
2. try to install capsule in fips mode

Actual results:
the installer on capsule fails, the httpd fails with

> /var/log/httpd/katello-reverse-proxy_error_ssl.log <
AH02252: incomplete client cert configured for SSL proxy (missing or encrypted private key?)

Expected results:
capsule installed as expected

Additional info:
Combining "Note: Apache httpd mod_ssl [SSLProxyMachineCertificateFile] does not support PKCS#8 key format." from
https://access.redhat.com/solutions/3214421 and "You can't [use BEGIN RSA PRIVATE KEY] because the format isn't allowed in
FIPS mode because it uses MD5 for key derivation." from
http://openssl.6102.n7.nabble.com/Not-getting-quot-RSA-quot-keyword-for-a-key-in-fips-mode-td58588.html, it gives us the only
option of not using SSLProxyMachineCertificateFile for the capsule.

I was not able to find any reason why to set the SSLProxyMachineCertificateFile for defining
the rhsm proxy (my tests showed that the proxying the client requests with consumer certicates
worked just find), but if anyone can think of one reason, please speak up.

Related issues:
Related to Foreman - Feature #3511: As a security person, I would like Forem... Resolved
Has duplicate Installer - Bug #24974: The kato configure is generating incorr... Duplicate

Associated revisions
Revision 4143a1f0 - 02/25/2019 01:52 PM - Ivan Necas
Fixes #26088 - ensure RSA word for SSLProxyMachineCertificateFile

Apaches's SSLProxyMachineCertificateFile is not able to find a key
wrapped in "-----BEGIN PRIVATE KEY-----", which is the format that is
generated when running the server in FIPS mode. It seems that just making
sure the RSA word is there make Apache happy to find the key.

I've added 'force_rsa' option for the cert files resources to enforce the
RSA word to be there when wrapping the private key + used that to
generate the client bundle for SSL proxy to use it.
History

#1 - 02/19/2019 04:23 PM - Ivan Necas
- Assignee changed from Lukas Zapletal to Ivan Necas
- Status changed from New to Assigned
- Category changed from Foreman Proxy Content to Installer
- Subject changed from httpd fails to start after installing capsule in FIPS mode to httpd fails to start after installing capsule in FIPS mode

#2 - 02/19/2019 04:56 PM - Ewoud Kohl van Wijngaarden
- Category changed from Installer to Foreman modules
- Project changed from Katello to Installer

#3 - 02/19/2019 04:59 PM - Eric Helms
- Is duplicate of Bug #24974: The kafo configure is generating incorrect 'foreman-proxy-client-bundle.pem' which is not allowing httpd service to start added

#4 - 02/19/2019 05:00 PM - Eric Helms
- Status changed from Assigned to Duplicate

#5 - 03/05/2019 05:29 PM - Ewoud Kohl van Wijngaarden
- Target version set to 1.22.0
- Status changed from Duplicate to Closed
- Fixed in Releases 1.20.3, 1.21.1, 1.22.0 added

This was the one that was actually merged.

#6 - 03/05/2019 05:30 PM - Ewoud Kohl van Wijngaarden
- Pull request https://github.com/theforeman/puppet-certs/pull/242 added

#7 - 03/05/2019 05:30 PM - Ewoud Kohl van Wijngaarden
- Related to Feature #3511: As a security person, I would like Foreman to run in FIPS mode added

#8 - 03/05/2019 05:31 PM - Ewoud Kohl van Wijngaarden
- Is duplicate of deleted (Bug #24974: The kafo configure is generating incorrect 'foreman-proxy-client-bundle.pem' which is not allowing httpd service to start)

#9 - 03/05/2019 05:31 PM - Ewoud Kohl van Wijngaarden
- Has duplicate Bug #24974: The kafo configure is generating incorrect 'foreman-proxy-client-bundle.pem' which is not allowing httpd service to start added

#10 - 03/28/2019 08:55 AM - Tomer Brisker
- Pull request https://github.com/theforeman/puppet-certs/pull/243 added
- Pull request deleted (https://github.com/theforeman/puppet-certs/pull/242)

#11 - 07/01/2019 03:25 PM - Ewoud Kohl van Wijngaarden
- Fixed in Releases deleted (1.20.3)

#12 - 07/01/2019 03:26 PM - Ewoud Kohl van Wijngaarden
This was released as puppet-certs 4.4.3 but Katello 3.10 includes 4.4.2. There likely won't be a Katello 3.10.2 to include this.