Installer - Bug #28043
Crane port 5000 presenting default Certificate Chain instead of Server Chain
10/11/2019 12:35 PM - Ewoud Kohl van Wijngaarden

Status: Closed
Priority: Normal
Assignee: Ewoud Kohl van Wijngaarden
Category: Foreman modules
Target version: Difficulty:
Pull request: https://github.com/theforeman/puppet-for eman_proxy_content/pull/211
Triaged: No
Fixed in Releases: 1.24.0
Bugzilla link: 1754598

Description
When using custom certs, the CA chain presented is the Default CA where Katello is configured to expect the Server CA. This isn't a problem without custom certs because then those are the same chain.

# egrep Cert /etc/httpd/conf.d/03-crane.conf
SSLCertificateFile   "/etc/pki/katello/certs/katello-apache.crt"
SSLCertificateKeyFile   "/etc/pki/katello/private/katello-apache.key"
SSLCertificateChainFile   "/etc/pki/katello/certs/katello-default-ca.crt"   --> Wrong? This should be katello-server-ca.crt
SSLCACertificateFile   "/etc/pki/katello/certs/katello-default-ca.crt"

The ssl verification issue can been seen when there is an Intermediate CA along with ROOT CA. If a client connecting crane only has Root CA in the trust store, ssl verification will fail.

Example :

# openssl s_client -connect sat65.lab.box:5000 -CAfile ./rootCA.pem
CONNECTED(00000003)
depth=0 C = IN, ST = MH, L = PNQ, O = Satellite, OU = Unix Admins, CN = sat65.lab.box
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = IN, ST = MH, L = PNQ, O = Satellite, OU = Unix Admins, CN = sat65.lab.box
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
  0 s:C = IN, ST = MH, L = PNQ, O = Sysmgmt, OU = Unix Admins, CN = sat65.lab.box
  1:i:C = IN, ST = MH, L = PNQ, O = Intermediate CA, OU = CA Support, CN = Intermediate CA
  1:s:C = US, ST = North Carolina, L = Raleigh, O = Katello, OU = SomeOrgUnit, CN = sat65.lab.box
  2:i:C = US, ST = North Carolina, L = Raleigh, O = Katello, OU = SomeOrgUnit, CN = sat65.lab.box

How reproducible:
clients connecting to crane registry will face this only in case there is more than 1 CA in chain and client only has root CA in trust store.

Steps to Reproduce:
1. Install Custom SSl Certs on Katello signed by a Root CA - > Intermediate CA > Katello Cert
2. Put Root CA in a systems's trust store. Do not register it to Katello as it will put full chain in anchors and trust i.e. katello-server-ca.crt
3. Use any Container Software on that system to connect to crane with https and notice ssl verification errors
Actual results:
Certs cannot be verified

Expected results:
In SSLCertificateChainFile option of apache configuration, it should have katello-server-ca.crt to serve SSL chain correctly

Associated revisions
Revision 0ac8571f - 10/12/2019 12:33 AM - Ewoud Kohl van Wijngaarden
Fixes #28043 - Crane uses the Katello server CA
Katello is configured to expect the server CA, but the default CA was actually being configured.

History
#1 - 10/11/2019 12:39 PM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/puppet-foreman_proxy_content/pull/211 added

#2 - 10/11/2019 12:40 PM - Ewoud Kohl van Wijngaarden
- Assignee changed from Eric Helms to Ewoud Kohl van Wijngaarden
- Category set to Foreman modules

#3 - 10/11/2019 12:41 PM - Ewoud Kohl van Wijngaarden
- Description updated

#4 - 10/12/2019 12:33 AM - The Foreman Bot
- Fixed in Releases 1.24.0 added

#5 - 10/12/2019 01:01 AM - Ewoud Kohl van Wijngaarden
- Status changed from Ready For Testing to Closed

Applied in changeset puppet-foreman_proxy_content|0ac8571f96891bca3901f8edd3967074402a9081.