Installer - Bug #31574

The Artemis client certificate is not updated in truststore if it changes

01/05/2021 03:07 PM - Eric Helms

Status:	Closed		
Priority:	Normal		
Assignee:	Eric Helms		
Category:	Foreman modules		
Target version:	2.5.0		
Difficulty:		**Fixed in Releases:**	2.5.0
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:	1951662	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-certs/pull/320, https://github.com/theforeman/puppet-certs/pull/323		

Description

The java-client cert and key in /etc/pki/katello are correctly updated, and are a valid pair =>

```
[root@dhcp-2-190 certs]# openssl x509 -noout -modulus -in java-client.crt  | openssl md5
(stdin)= d74483a4ae79b6b2a6ea09afe1b21095
[root@dhcp-2-190 certs]# openssl rsa -noout -modulus -in ../private/java-client.key | openssl md5
(stdin)= d74483a4ae79b6b2a6ea09afe1b21095
```

However, candlepin's truststore doesn't know about the new java-client.crt (called 'artemis-client' in the store) =>

```
[root@dhcp-2-190 certs]# keytool -list -keystore truststore
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

Your keystore contains 2 entries

artemis-client, Dec 10, 2020, trustedCertEntry,
Certificate fingerprint (SHA1): 17:91:F0:47:4C:18:8B:19:57:49:D3:4C:1E:05:38:D9:59:66:82:3B
```

Compare that fingerprint to /etc/pki/katello/certs/java-client.crt =>

```
[root@dhcp-2-190 certs]# openssl x509 -noout -fingerprint -sha1 -inform pem -in java-client.crt
SHA1 Fingerprint=2C:E3:3C:D1:B3:A5:01:EF:B7:5E:00:5D:6B:87:DF:6B:CA:28:A3:56
```

They should match, but don't

Associated revisions

Revision de946a47 - 04/21/2021 04:04 PM - Ewoud Kohl van Wijngaarden

Fixes #31574: Ensure truststore certificates get updated when they change

Revision 9074ba6d - 04/26/2021 04:08 PM - Eric Helms

Refs #31574: Compare SHA256 fingerprints when checking truststore

The default on some operating systems such as EL7 is to print the
SHA1 fingerprint of a certificate. The java truststore reports
the SHA-256 fingerprint and thus we need to explicitly check the
same fingerprint type.

History

#1 - 01/05/2021 03:13 PM - Ewoud Kohl van Wijngaarden

- Subject changed from The Artemis client certificate is not updated in truststore if it changes

to The Artemis client certificate is not updated in truststore if it changes

- Category set to Foreman modules

- Triaged changed from No to Yes

On a related note: I'm wondering if we can store the CA in the truststore rather than the actual certificate. The CA is less likely to change and we already verify the exact DN anyway. Wouldn't that be sufficient? (It would still need to be idempotent and consistent with the CA though so the update code should still be there.)

#2 - 01/06/2021 05:18 PM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/puppet-certs/pull/311 added

#3 - 01/14/2021 06:42 PM - The Foreman Bot

- Pull request https://github.com/theforeman/puppet-certs/pull/312 added

#4 - 03/17/2021 11:38 PM - The Foreman Bot

- Pull request https://github.com/theforeman/puppet-certs/pull/320 added

#5 - 04/13/2021 01:09 PM - Eric Helms

- Target version set to 2.5.0

#6 - 04/20/2021 04:53 PM - Eric Helms

- Bugzilla link deleted (1897360)

#7 - 04/20/2021 04:53 PM - Eric Helms

- Bugzilla link set to 1951662

#8 - 04/21/2021 04:04 PM - The Foreman Bot

- Fixed in Releases 2.5.0 added

#9 - 04/21/2021 05:01 PM - Ewoud Kohl van Wijngaarden

- Status changed from Ready For Testing to Closed

Applied in changeset puppet-certs|de946a474eb951419cc2c5ff62ada9956c7242a8.

#10 - 04/26/2021 12:48 PM - The Foreman Bot

- Pull request https://github.com/theforeman/puppet-certs/pull/323 added

#11 - 04/27/2021 07:13 PM - Eric Helms

- Pull request deleted (https://github.com/theforeman/puppet-certs/pull/311, https://github.com/theforeman/puppet-certs/pull/312)