Installer - Bug #25359

Missing "-name" option on "openssl pkcs12" command may cause incorrect nickname added to the katello nssdb

10/31/2018 04:19 PM - Chris Roberts

Status:	Resolved		
Priority:	Normal		
Assignee:	Chris Roberts		
Category:	Foreman modules		
Target version:			
Difficulty:	easy	**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:	1577014	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-certs/pull/223		

Description

escription of problem:
Below is the steps that satellite-installer create the Qpid broker certficate to the katello nssdb

1) Delete the "broker" certificate from nssdb

Executing 'certutil ~~-D -d /etc/pki/katello/nssdb -n 'broker'~~
---

2) Import broker certificate to nssdb. It looks like something strange could happen here. Certutil returns 0 exit code but the "broker" certificate was not created. I am also not able to reproduce it but it happened in a case.

Executing 'certutil ~~-A -d '/etc/pki/katello/nssdb' -n 'broker' -t ',,' -a -i '/etc/pki/katello/certs/satellite.example.com-qpid-broker.crt'~~
---

3) Convert the broker private key and certificate to pkcs12 format. There is a problem in this command. It should pass a certname option ("-name broker") but it didn't. Therefore, a "pfx" file without nickname was created.

Executing 'openssl pkcs12 ~~in /etc/pki/katello/certs/satellite.example.com-qpid-broker.crt -inkey /etc/pki/katello/private/satellite.example.com-qpid-broker.key -export -out '/etc/pki/katello/satellite.example.com-qpid-broker.pfx' -password 'file:/etc/pki/katello/nssdb/nss_db_password-file'~~
---

4) Import the generated "pfx" file to nssdb using pk12util command. Since no nickname is provided by the "pfx" file, it will generate a nickname in the format of "{Common Name} - {Org}". In this case "satellite.example.com - SomeOrg".

Executing 'pk12util ~~-i '/etc/pki/katello/satellite.example.com-qpid-broker.pfx' -d '/etc/pki/katello/nssdb' -w '/etc/pki/katello/nssdb/nss_db_password-file' -k '/etc/pki/katello/nssdb/nss_db_password-file'~~

To prevent the above issue, I suggest to add "-name broker" to the "openssl pkcs12" command in step (3). I also think that the "certutil -A" command in step (2) is not needed. Since we are going to import both broker private key and ssl certificate using "pk12util" command in step (4), why do we still need to run "certutil -A"?

Reproducing from terminal:

$ certutil ~~-L -d .~~

Certificate Nickname Trust Attributes
SSL,S/MIME,JAR/XPI

amqp-client ,,
ca CT,C,c

```
$ openssl pkcs12 -in /etc/pki/katello/certs/mysatellite-example.com-qpid-broker.crt -inkey
/etc/pki/katello/private/mysatellite-example.com-qpid-broker.key -export -out '/etc/pki/katello/mysatellite-example.com-qpid-broker.pfx'
-password 'file:/etc/pki/katello/nssdb/nss_db_password-file'

pk12util -i '/etc/pki/katello/mysatellite-example.com-qpid-broker.pfx' -d '/etc/pki/katello/nssdb' -w
'/etc/pki/katello/nssdb/nss_db_password-file' -k '/etc/pki/katello/nssdb/nss_db_password-file'
--------------------
pk12util: no nickname for cert in PKCS12 file.    <============================== ########## Complain about missing
nickname ###########
pk12util: using nickname: mysatellite-example.com - Katello <============================== ########## "{Common
Name} - {Org}" nickname is used ###########
pk12util: PKCS12 IMPORT SUCCESSFUL
-------------------------

certutil -L -d .
--------------------
Certificate Nickname                                         Trust Attributes
SSL,S/MIME,JAR/XPI

amqp-client                                                  ,,
ca                                                           CT,C,c
mysatellite-example.com - Katello                            u,u,u   <==============================
-------------------------
```

Associated revisions

Revision fc3ad9a9 - 10/31/2018 05:03 PM - Chris Roberts

Fixes #25359 - Add name flag to openssl pkcs12 nsddb key/cert convert.

History

#1 - 10/31/2018 06:03 PM - Chris Roberts

- Status changed from New to Resolved

- Pull request https://github.com/theforeman/puppet-certs/pull/223 added