# Foreman - Feature #12272

## Support for multiple certificates in ca.crt for oVirt

10/22/2015 04:09 PM - Vasyl "vk"

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | Ori Rabin | | |
| **Category:** | Compute resources - oVirt | | |
| **Target version:** | 1.15.0 | | |
| **Difficulty:** | | **Fixed in Releases:** | |
| **Triaged:** | | **Found in Releases:** | 1.5.3 |
| **Bugzilla link:** | 1304424 | **Red Hat JIRA:** | |
| **Pull request:** | https://github.com/theforeman/foreman/pull/4411 | | |

**Description**

In app/models/compute_resources/foreman/model/ovirt.rb ca_cert_store() function stores retrieved ca.crt in OpenSSL::X509::Store object.
The problem is, OpenSSL::X509::Certificate.new(cert) only takes into account the last certificate in cert.
If cert contains more than one certificate (which is quite common on production systems these days), only last certificate in the chain will be added to the store, and SSL verification in oVirt will not work.
This blocks the Foreman usage with RHEV-M.
The code below fixed issue for me, though I'm not a real Ruby programmer and am sure there's better way to do this.
Main idea is certificates should be split and added to the OpenSSL::X509::Store one by one.

```
    def ca_cert_store cert
      return if cert.blank?
      s = OpenSSL::X509::Store.new
      splitcert = ""
      cert_arr = []
      i = 0
      cert.each_line do |line|
        splitcert += line
        if line =~ /-----END [^\-]+-----/
           cert_arr << splitcert
           splitcert = ""
        end
      end
      cert_arr.each do |c|
        s.add_cert(OpenSSL::X509::Certificate.new(c.to_s))
      end
      s
    end
```

I can send a pull request if the above approach is fine.

### Associated revisions

**Revision 4c351621 - 03/27/2017 06:58 AM - Ori Rabin**

Fixes #12272 - Support multiple certificates in ovirt resource

### History

**#1 - 10/23/2015 09:20 AM - Lukas Zapletal**

AFAIK Foreman supports chain of CA certificates in this field. From our web UI helper text: "Optionally provide a CA, or a correctly ordered CA chain. If left blank, a self-signed CA will be populated automatically by the server during the first request". Make sure the order is correct. I have tested this and OpenSSL seems to work. Tested on RHEL, what platform do you use?

**#2 - 02/01/2016 10:03 AM - Christophe Roux**

I am having the exact same issue  (on RHEL7m Satellite 6.1.6) and the proposed workaround is working.

It really seems that the command OpenSSL::X509::Certificate.new(cert) is only taking the last cert.

```
require 'openssl'
require 'socket'

cert=File.read("./rhevm.pem")
s=OpenSSL::X509::Certificate.new(cert)

cert_store=OpenSSL::X509::Store.new.add_cert(s)

ssl_context = OpenSSL::SSL::SSLContext.new
ssl_context.cert_store = cert_store
ssl_context.set_params(verify_mode: OpenSSL::SSL::VERIFY_PEER)

tcp_socket = TCPSocket.open 'rhevm.example.com', 443
ssl_socket = OpenSSL::SSL::SSLSocket.new tcp_socket, ssl_context
ssl_socket.connect
```

is returning,

```
SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed (OpenSSL::SSL::SSLError)
```

but the following using add_file method (which the doc clearly says support multiple certificates)

```
require 'openssl'
require 'socket'

cert_store=OpenSSL::X509::Store.new.add_file("./rhevm.pem")

ssl_context = OpenSSL::SSL::SSLContext.new
ssl_context.cert_store = cert_store
ssl_context.set_params(verify_mode: OpenSSL::SSL::VERIFY_PEER)

tcp_socket = TCPSocket.open 'rhevm.example.com', 443

ssl_socket = OpenSSL::SSL::SSLSocket.new tcp_socket, ssl_context

ssl_socket.connect
```

Works fine

#### #3 - 03/23/2017 08:57 AM - Ori Rabin

*- Status changed from New to Assigned*

*- Assignee set to Ori Rabin*

#### #4 - 03/26/2017 09:22 AM - The Foreman Bot

*- Status changed from Assigned to Ready For Testing*

*- Pull request https://github.com/theforeman/foreman/pull/4411 added*

#### #5 - 03/27/2017 04:20 AM - Ori Rabin

*- Bugzilla link set to 1304424*

#### #6 - 03/27/2017 07:01 AM - Ori Rabin

*- Status changed from Ready For Testing to Closed*

*- % Done changed from 0 to 100*

Applied in changeset 4c3516219692e729204a1cd4a12283c61c8e3b62.

#### #7 - 03/29/2017 07:53 AM - Ohad Levy

*- translation missing: en.field_release set to 209*

#### #8 - 04/04/2017 06:01 AM - Ivan Necas

*- Target version set to 1.12.2*