Our RHEV manager is behind a firewall & so from Foreman server we opened up port 443 for management through the API & 5900-6011 for console access.

Things didn't work, connection timed out. I narrowed it down to some code in app/models/compute_resources/foreman/model/ovirt.rb, lines 218ff:

def cacert
cia_url = URI.parse(url)
cia_url.path = "\ca.crt"
cia_url.scheme = "http"
cia_url.port = 8080 if ca_url.port  8443
cia_url.port = 80 if ca_url.port  443
Net::HTTP.get(ca_url).to_s
end

It's fetching the (normally) self-signed CA certificate over an unencrypted channel & later on using this to validate the SSL connection. This is in effect no different to connecting directly over SSL & disabling certificate verification, but it does mean that port 80 or 8080 needs to be opened up as well which there seems no need to do.

I see 2 options:

1. Connect over SSL to retrieve the CA certificate, but disable certificate verification.
2. Retrieve & store the CA certificate only when the compute resource is added & display a warning to user around connecting to insecure site.

I prefer 2, but this is more work to implement. I have already written the trivial patch for 1 & will submit a pull request for this soon.

Thanks,
Jimmi

Associated revisions

Revision 6a85948c - 12/31/2013 02:49 PM - Jimmi Dyson
fixes #3896 Retrieve OVirt CA certificate via same URL scheme as API URL by disabling SSL verification

History

#1 - 12/17/2013 08:13 PM - Dominic Cleal
- Status changed from New to Ready For Testing
- Assignee set to Jimmi Dyson
- Target version set to 1.9.3

https://github.com/theforeman/foreman/pull/1097
#2 - 12/31/2013 03:31 PM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 6a85948c0f0e29a29e86f3c290db08a80cbe6e6a52.

#3 - 01/02/2014 03:29 PM - Dominic Cleal
- Legacy Backlogs Release (now unused) set to 2