

## Foreman - Bug #37021

### katello-certs-check should succeed if intermediates are presented without root

01/03/2024 05:36 AM - Kevin Keane

<b>Status:</b> New	
<b>Priority:</b> Normal	
<b>Assignee:</b>	
<b>Category:</b>	
<b>Target version:</b>	
<b>Difficulty:</b>	<b>Fixed in Releases:</b> 3.10.0
<b>Triaged:</b> No	<b>Found in Releases:</b>
<b>Bugzilla link:</b>	<b>Red Hat JIRA:</b>
<b>Pull request:</b>	
<b>Description</b>	
<p>The katello-certs-check utility requires that the provided certificate chain contains not just all intermediate certs, but also the root certificate.</p> <p>It should accept a certificate bundle that contains only intermediate certificates, as long as the root is globally installed on the server. This is in keeping with RFCs, and also because some CAs (Sectigo in my case) only provide intermediate certificates.</p> <p>To achieve that, the openssl verify line should be changed to replace the -CAfile argument with the -untrusted argument.</p> <pre>CHECK=\$(openssl verify -untrusted \$CA_BUNDLE_FILE -purpose sslserver -verbose \$CERT_FILE 2&gt;&amp;1)</pre> <p>How to reproduce:</p> <p>Obtain a certificate, key, and corresponding intermediate certificates. Ensure that the intermediate certificates do not include a self-signed root certificate.</p> <p>Then run:</p> <pre>katello-certs-check -c &lt;certfile&gt;.pem -k &lt;keyfile&gt;.pem -b &lt;ca intermediate bundle&gt;.pem</pre> <p>Expected result:</p> <pre>... Checking CA bundle against the certificate file: [OK] ...</pre> <p>Actual result:</p> <pre>... Checking CA bundle against the certificate file: [FAIL]  The &lt;intermediate&gt;.pem does not verify the &lt;certificate&gt;.pem C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust RSA Certification Authority error 2 at 2 depth lookup: unable to get issuer certificate error &lt;certifict&gt;.pem: verification failed ...</pre>	

#### History

#1 - 01/03/2024 06:14 AM - Kevin Keane

When fixing this issue, foreman-maintain also need to be fixed the same way.