

Installer - Bug #37063

Add feature in katello-certs-check to verify if CA bundle has any certificates with trust rules

01/18/2024 05:48 PM - Joniel Pasqualetto

<div>Status:Closed</div> <div>Priority:Normal</div> <div>Assignee:</div> <div>Category:</div> <div>Target version:</div> <div>Difficulty:</div> <div>Triaged:No</div> <div>Bugzilla link:2259026</div> <div>Pull request:https://github.com/theforeman/foreman-installer/pull/909</div>	<div>Fixed in Releases:3.11.0</div> <div>Found in Releases:</div> <div>Red Hat JIRA:</div>
<div>Description</div> <div>Description of problem:</div> <p>Trust rules on a certificate indicate what are the accepted uses for it. Some users may have a CA bundle where one of the certificates includes trust rules (maybe incorrectly).</p> <p>The default validation done by katello-certs-check does not complain about it. The bundle can be used without problems on Satellite 6.14+ but fails on 6.13 (at least, didn't check older versions).</p> <p>Also, when thinking about clients of Satellite, RHEL8+ can trust the bundle that contains trust rules but RHEL7 will have problems (when using libcurl) trusting that.</p> <p>So, accepting a bundle like this will potentially break the Satellite installation (foreman-proxy is the component failing on 6.13 when using it) and also break the access to Satellite for RHEL7 hosts.</p> <div>Version-Release number of selected component (if applicable):</div> <div>How reproducible:</div> <div>Steps to Reproduce:</div> <div>1. Have a CA certificate and add a trust rule to it:</div> <div>~~</div> <div>openssl x509 -in ca_cert.pem -addtrust serverAuth -out ca_trust_rule.pem</div> <div>~~</div> <div>2. Check with katello-certs-check and there will be no complaints about it.</div> <div>Actual results:</div> <p>katello-certs-check does not complaint about having a CA bundle in a format that may break satellite and/or client access to satellite</p> <div>Expected results:</div> <p>katello-certs-check should point that there is an issue with the bundle</p> <div>Additional info:</div>	

Associated revisions

Revision 931b6fcd - 04/03/2024 05:27 PM - Joniel Pasqualetto

Fixes #37063 - Add feature in katello-certs-check to verify if CA bundle has any certificates with trust rules

- Add feature to verify if provided CA bundle has certificates with trust rules
- Add test case for the new feature

- Fix indentation on function check-ca-bundle-size

History

#1 - 01/18/2024 05:55 PM - The Foreman Bot

- Status changed from New to Ready For Testing
- Pull request <https://github.com/theforeman/foreman-installer/pull/909> added

#2 - 04/03/2024 05:27 PM - The Foreman Bot

- Fixed in Releases 3.11.0 added

#3 - 04/03/2024 06:00 PM - Joniel Pasqualetto

- Status changed from Ready For Testing to Closed

Applied in changeset [installer|931b6fcd9c583c9ede62373a09c7b4e9ca85b0c4](#).