check for too many issuers in custom SSL certs

11/26/2019 04:08 PM - Ewoud Kohl van Wijngaarden

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Eric Helms</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td><a href="https://github.com/theforeman/foreman-installer/pull/413">https://github.com/theforeman/foreman-installer/pull/413</a></td>
</tr>
<tr>
<td>Triaged:</td>
<td>No</td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td>1709848</td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td>2.0.0</td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

**Description of problem:**

Attempting to update custom SSL certs using the following documented procedure:

https://access.redhat.com/documentation/en-us/red_hat_satellite/6.4/html/installing_satellite_server_from_a_connected_network/performing_additional_configuration_on_satellite_server#configuring_satellite_server_with_custom_server_certificate

and

https://access.redhat.com/solutions/1273623

fails and results in a non-working Satellite server due to failures in qpid and foreman_proxy:

```bash
[ERROR 2019-04-23T13:53:30 main] /Stage[main]/Katello::Qpid/Qpid::Config::Queue[katello_event_queue]/Qpid::Config_cmd[ensure queue katello_event_queue]/Exec[qpid-config ensure queue katello_event_queue]/returns: change from 'notrun' to [0] failed: 'qpid-config --ssl-certificate /etc/pki/katello/certs/satellite.example.org-qpid-broker.crt --ssl-key /etc/pki/katello/private/satellite.example.org-qpid-broker.key -b amqps://localhost:5671 add queue katello_event_queue --durable' returned 1 instead of one of [0]
```

and

```bash
[ERROR 2019-04-23T13:53:30 main] /Stage[main]/Foreman_proxy::Register/Foreman_smartproxy[satellite.example.org]: Could not evaluate: Exception SSL_connect returned=1 errno=0 state=unknown state: excessive message size in get request to: https://satellite.example.org/api/v2/smart_proxies?search=name=%22satellite.example.org%22
```

**Steps to Reproduce:**

1. Create a certificate file with more than 32 issuers.
2. Attempt to update certificates using procedure above.

**Actual results:**

Certificate update fails, even though katello-certs-check succeeds.

**Expected results:**

Certificates should be updated successfully with above documented procedure.

**Additional info:**

The customer identified two problems with the documented procedure in his environment:

1. The "--certs-update-all" flag is required and not listed in the instructions above.
2. The CA bundle used must not contain too many certs; if so the certs must be split into separate files. Currently, 'katello-certs-check' succeeds even though the large bundle will break later components.

**Associated revisions**

Revision 809edefe - 11/26/2019 08:32 PM - Ewoud Kohl van Wijngaarden

05/09/2020 1/2
Fixes #28367 - Add a max issuers check

Too many certificates in the bundle breaks various tools. By keeping an upper limit of 32 it should be safe since only the chain for the server certificate should be included.

https://access.redhat.com/solutions/3406401 describes this as well, but requires a login.

History

#1 - 11/26/2019 04:27 PM - The Foreman Bot
- Status changed from New to Ready For Testing
- Pull request https://github.com/theforeman/foreman-installer/pull/413 added

#2 - 11/26/2019 08:32 PM - The Foreman Bot
- Fixed in Releases 2.0.0 added

#3 - 11/26/2019 09:01 PM - Ewoud Kohl van Wijngaarden
- Status changed from Ready For Testing to Closed

Applied in changeset installer|809edefecf39815af2e2555368307e860f9356cf.