QGIS Application - Bug report #15687
SSL connection does not update CAs

2016-10-10 12:58 AM - Luigi Pirelli

Status:	Closed		
Priority:	Normal		
Assignee:	Larry Shaffer		
Category:	Authentication system		
Affected QGIS version:	2.14.5	**Regression?:**	No
Operating System:	Windows	**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	end of life
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	23610

Description

I found a misalignement in SSL Root Certificate Authorities (CAs) caching at least in WIN. This bug has been found developing a solution to #15617

ABSTRACT
A brief description of the bug(?) and after a detailed step procedure to reproduce it:
Any SO has a SSL conf has a list of CAs. These are used to setup the ssl communication to verify if peer cert can be trusted or not. If the system CAs list change this would affect the subsequent connection.
I found that if I remove or add a CA, next connections "remember" the previous CA list for a while (some minutes).

to reproduce the error I tried to connect to https://qgis.boundlessgeo.com that is signed by:
"AddTrust CA External CA Root"
By default AddTrust is not present in Windows CAs. But.
- if it is present it can be removed using "certmgr.msc"
- if not present y can be automatically added by OS just browsing in a windows keystore capable browser (no Firefox) the following link: https://qgis.boundlessgeo.com/plugins/plugins.xml
  The OS will check the URL CA and will check if it can be trusted, and if so, it will be added in the keystore.

PREMISE:
To generate sslError I ued to connect to a erroneous OWS service, eg WMS or WFS. The reason is to use only pure c++ code.
The steps to reproduce the errors are on WIN7 (but should be the same on any win OS):
- remove AddTrust CA if present
- in QGIS trying to connect to https://qgis.boundlessgeo.com/plugins/plugins.xml using wms service (=> only c++ code)
- => sslError dialog will be opened. !!! Abort it and not push the Ignore button !!!
- load https://qgis.boundlessgeo.com/plugins/plugins.xml in Explorer and verify that "AddTrust" has been added in certmgr.msc
- executing the following python code in console

```
QgsAuthManager.instance().rebuildCaCertsCache()
QgsAuthManager.instance().rebuildCertTrustCache()
QgsAuthManager.instance().rebuildTrustedCaCertsCache()
QgsAuthManager.instance().rebuildIgnoredSslErrorCache()
```

  You can verify that new CA is updated in qgis in settings->options->authentication->Manage Certificates->Authorities
- tried to reconnect to https://qgis.boundlessgeo.com/plugins/plugins.xml using wms service
- !!!continuing!!! to have sslError dialog
- waiting a while (5'?) I'm able to receive a WMS error => no more sslError

The procedure to reproduce the bug can be also inverted:
1. started qgis having the CA AddTrust installed (no sslerror)
2. connect to wms service https://qgis.boundlessgeo.com/plugins/plugins.xml => wms error but not sslError dialog

3. removed AddTrust
4. executed the following python code in console

```
QgsAuthManager.instance().rebuildCaCertsCache()
QgsAuthManager.instance().rebuildCertTrustCache()
QgsAuthManager.instance().rebuildTrustedCaCertsCache()
QgsAuthManager.instance().rebuildIgnoredSslErrorCache()
```

You can verify that CA is removed in qgis in settings->options->authentication->Manage Certificates->Authorities
5. connect to WMS => still wms error but not sslError dialog
6. after a while the sslError come back connecting to WMS service

History

#1 - 2016-10-10 06:04 AM - Luigi Pirelli

not confirmed on Linux.

removing or adding CA and running "update-ca-certificates" (debian/ubuntu) and then:
QgsAuthManager.instance().rebuildCaCertsCache()
QgsAuthManager.instance().rebuildCertTrustCache()
QgsAuthManager.instance().rebuildTrustedCaCertsCache()
QgsAuthManager.instance().rebuildIgnoredSslErrorCache()
affect immediately the sslError.

OpenSSL 1.0.2d 9 Jul 2015

#2 - 2016-10-10 06:26 AM - Luigi Pirelli

my OSGeo4W qgis is using ssl version:

ssleay.dll v1.0.1.7

#3 - 2016-10-13 03:38 AM - Luigi Pirelli

I did a "brutal" test substituing ssleay.dll and libeay.dll with 1.0.2 version: https://indy.fulgan.com/SSL/openssl-1.0.2j-x64_86-win64.zip
choosed among that listed here: https://wiki.openssl.org/index.php/Binaries
This substitution didn't solve the issue!

#4 - 2017-04-30 11:56 PM - Giovanni Manghi

- Description updated
- Easy fix? set to No
- Regression? set to No

#5 - 2019-03-09 03:08 PM - Giovanni Manghi

- Resolution set to end of life
- Status changed from Open to Closed

End of life notice: QGIS 2.18 LTR

Source:
http://blog.qgis.org/2019/03/09/end-of-life-notice-qgis-2-18-ltr/

QGIS 3.4 has recently become our new Long Term Release (LTR) version. This is a major step in our history – a long term release version based on the massive updates, library upgrades and improvements that we carried out in the course of the 2.x to 3x upgrade cycle.

We strongly encourage all users who are currently using QGIS 2.18 LTR as their preferred QGIS release to migrate to QGIS 3.4. This new LTR version will receive regular bugfixes for at least one year. It also includes hundreds of new functions, usability improvements, bugfixes, and other goodies. See the relevant changelogs for a good sampling of all the new features that have gone into version 3.4

Most plugins have been either migrated or incorporated into the core QGIS code base.

We strongly discourage the continued use of QGIS 2.18 LTR as it is now officially unsupported, which means we'll not provide any bug fix releases for it.

You should also note that we intend to close all bug tickets referring to the now obsolete LTR version. Original reporters will receive a notification of the ticket closure and are encouraged to check whether the issue persists in the new LTR, **in which case they should reopen the ticket**.

If you would like to better understand the QGIS release roadmap, check out our roadmap page! It outlines the schedule for upcoming releases and will help you plan your deployment of QGIS into an operational environment.

The development of QGIS 3.4 LTR has been made possible by the work of hundreds of volunteers, by the investments of companies, professionals, and administrations, and by continuous donations and financial support from many of you. We sincerely thank you all and encourage you to collaborate and support the project even more, for the long term improvement and sustainability of the QGIS project.