Ruby master - Bug #11033
OpenSSL related threading issues in Ruby 2.1 and 2.2

04/04/2015 12:08 AM - tknerr (Torben Knerr)

Status: Closed
Priority: Normal
Assignee: openssl
Target version: ruby -v:
Backport: 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE

Description

I'm experiencing some problems with multiple https connections in Ruby 2.1 and 2.2, whilst in Ruby 2.0 everything is working fine.

This happens on a Windows 7 (64-bit) box in the context of installing multiple gems in parallel via bundlers BUNDLE_JOBS=<n> setting.

What I see are multiple OpenSSL::SSL::SSLError: SSL_read: cert already in hash table warnings and at some more or less random point it bails out because it cannot install a gem. When I repeat the bundle install command it will get past that gem and fail at a later one. I can repeat until all gems are installed.

This is the stacktrace I get for every of the ssl warnings:

```
... Installing polyglot 0.3.5
4: polyglot (0.3.5) from X:/home/.gem/ruby/2.2.0/specifications/polyglot-0.3.5.gemspec

OpenSSL::SSL::SSLError: SSL_read: cert already in hash table
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/openssl/buffering.rb:182:in `sysread_nonblock'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/openssl/buffering.rb:182:in `read_nonblock'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/net/protocol.rb:153:in `rbuf_fill'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/net/protocol.rb:134:in `readuntil'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/net/protocol.rb:144:in `readline'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http/response.rb:39:in `read_status_line'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http/response.rb:28:in `read_new'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http.rb:1414:in `block in transport_request'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http.rb:1411:in `catch'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http.rb:1411:in `transport_request'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/http.rb:1384:in `request'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/request.rb:154:in `perform_request'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/request.rb:109:in `fetch'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:346:in `request'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:231:in `fetch_http'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:247:in `fetch_http'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:267:in `fetch_path'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:302:in `cache_update_path'
X:/tools/ruby-2.2.1/lib/ruby/2.2.0/rubygems/remote_fetcher.rb:168:in `download'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/rubygems_integration.rb:544:in `download_gem'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/fetcher.rb:63:in `download_gem_from_url'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/source/rubygems.rb:370:in `install'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/installer.rb:107:in `install_gem_from_spec'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/installer.rb:287:in `block in install_in_parallel'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/worker.rb:55:in `call'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/worker.rb:55:in `apply_func'
X:/tools/ruby-2.2.1/lib/ruby/gems/2.2.0/gems/bundler-1.9.2/lib/bundler/worker.rb:50:in `block in process_queue'
```

06/07/2020
This is originally reported here (with a bit more details):
https://github.com/bundler/bundler/issues/3545

Any ideas?

Might it be a regression of #8386?

---

**Revision 9eb2007 - 06/14/2017 09:49 AM - rhe**

crypto: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit history since v2.0.3 (imported at r57482) can be found at:

https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
test/test_pkey_ec: do not use dummy 0 order
test/test_ssl: fix typo in test_sysread_and_syswrite
ssl: check return value of SSL_set_fd()
Fix typos
test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
tool/sync-with-trunk: 'LASY' -> 'LAST'
x509store: clear error queue after calling X509_LOOKUP_load_file()
extconf.rb: simplify searching libraries logic

Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
Fix typos

Vladimir Rybas (1):
Fix documentation for OpenSSL::Cipher#final

nobu (2):
openssl: fix broken openssl check
openssl: fix broken openssl check

usa (1):
Search SSL libraries by testing various filename patterns

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@59081 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

---

**Revision 59081 - 06/14/2017 09:49 AM - rhenium (Kazuki Yamaguchi)**

openssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit history since v2.0.3 (imported at r57482) can be found at:

https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
test/test_pkey_ec: do not use dummy 0 order
test/test_ssl: fix typo in test_sysread_and_syswrite
ssl: check return value of SSL_set_fd()
Fix typos
test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
tool/sync-with-trunk: 'LASY' -> 'LAST'
x509store: clear error queue after calling X509_LOOKUP_load_file()
extconf.rb: simplify searching libraries logic
Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
Fix typos

Vladimir Rybas (1):
Fix documentation for OpenSSL::Cipher#final

nobu (2):
openssl: fix broken openssl check
 openssl: fix broken openssl check

usa (1):
Search SSL libraries by testing various filename patterns

Revision 59081 - 06/14/2017 09:49 AM - rhe
openssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit history since v2.0.3 (imported at r57482) can be found at:

https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
test/test_pkey_ec: do not use dummy 0 order
test/test_ssl: fix typo in test_sysread_and_syswrite
ssl: check return value of SSL_set_fd()
Fix typos
test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
tool/sync-with-trunk: 'LASY' -> 'LAST'
x509store: clear error queue after calling X509_LOOKUP_load_file()
extconf.rb: simplify searching libraries logic
Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
Fix typos

Vladimir Rybas (1):
Fix documentation for OpenSSL::Cipher#final

nobu (2):
openssl: fix broken openssl check
 openssl: fix broken openssl check

usa (1):
Search SSL libraries by testing various filename patterns

Revision 59081 - 06/14/2017 09:49 AM - rhe
openssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit history since v2.0.3 (imported at r57482) can be found at:

https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

Jun Aruga (1):
Update .travis.yml and Dockerfile
Kazuki Yamaguchi (9):
test/test_pkey_ec: do not use dummy 0 order
test/test_ssl: fix typo in test_sysread_and_syswrite
ssl: check return value of SSL_set_fd()
Fix typos
test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
tool/sync-with-trunk: 'LASY' -> 'LAST'
x509store: clear error queue after calling X509_LOOKUP_load_file()
extconf.rb: simplify searching libraries logic
Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
Fix typos

Vladimir Rybas (1):
Fix documentation for OpenSSL::Cipher#final

nobu (2):
openssl: fix broken openssl check
openssl: fix broken openssl check

usa (1):
Search SSL libraries by testing various filename patterns

Revision 127c8a21 - 06/30/2017 12:42 PM - usa (Usaku NAKAMURA)

- ext/openssl/ossl_x509store.c: clear error queue after calling X509_LOOKUP_load_file()

X509_LOOKUP_load_file(), which ends up calling
X509_load_cert_crl_file() internally, may leave error entries in the queue even when it returns
non-zero value (which indicates success).

This will be fixed by OpenSSL 1.1.1, but can be worked around by
clearing the error queue ourselves.

Fixes: [Backport #11033]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59235 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 59235 - 06/30/2017 12:42 PM - usa (Usaku NAKAMURA)

- ext/openssl/ossl_x509store.c: clear error queue after calling X509_LOOKUP_load_file()

X509_LOOKUP_load_file(), which ends up calling
X509_load_cert_crl_file() internally, may leave error entries in the queue even when it returns
non-zero value (which indicates success).

This will be fixed by OpenSSL 1.1.1, but can be worked around by
clearing the error queue ourselves.

Fixes: [Backport #11033]

Revision b08e0ade - 08/03/2017 01:43 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 58742,59081: [Backport #11033]

Search SSL libraries by testing various filename patterns

* ext/openssl/extconf.rb (find_openssl_library): should search by more flexible
  method, especially for LibreSSL on Windows.

openssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit
history since v2.0.3 (imported at r57482) can be found at:
https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].
Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
- test/test_pkey_ec: do not use dummy 0 order
- test/test_ssl: fix typo in test_sysread_and_syswrite
- ssl: check return value of SSL_set_fd()
- Fix typos
- test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
- tool/sync-with-trunk: 'LASY' -> 'LAST'
- x509store: clear error queue after calling X509_LOOKUP_load_file()
- extconf.rb: simplify searching libraries logic
- Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
- Fix typos

Vladimir Rybas (1):
- Fix documentation for OpenSSL::Cipher#final

nobu (2):
- openssl: fix broken openssl check
- openssl: fix broken openssl check

usa (1):
- Search SSL libraries by testing various filename patterns

Revision 59489 - 08/03/2017 01:43 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) 58742,59081: [Backport #11033]

Search SSL libraries by testing various filename patterns

* ext/openssl/extconf.rb (find_openssl_library): should search by more flexible
  method, especially for LibreSSL on Windows.

openssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit
history since v2.0.3 (imported at r57482) can be found at:
  https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

----------------------------------------------------------------
Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
- test/test_pkey_ec: do not use dummy 0 order
- test/test_ssl: fix typo in test_sysread_and_syswrite
- ssl: check return value of SSL_set_fd()
- Fix typos
- test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
- tool/sync-with-trunk: 'LASY' -> 'LAST'
- x509store: clear error queue after calling X509_LOOKUP_load_file()
- extconf.rb: simplify searching libraries logic
- Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
- Fix typos

Vladimir Rybas (1):
- Fix documentation for OpenSSL::Cipher#final

nobu (2):
- openssl: fix broken openssl check
- openssl: fix broken openssl check

usa (1):
- Search SSL libraries by testing various filename patterns
Just double-checked whether it might be a RubyGems issue.

So I downgraded Rubygems to 2.4.4 (the version that ships with Ruby 2.0, where everything works), but still the same behaviour => not related to RubyGems, more likely a core issue

Seems to be a Windows specific issue. I did NOT experience this on my Ubuntu 14.04 box with Ruby 2.1.5p273.

#3 - 09/13/2015 03:23 AM - zzak (Zachary Scott)
- Assignee set to openssl

#4 - 06/14/2017 01:23 AM - Iristyle (Ethan Brown)
Also seeing this issue crop up in AppVeyor - specifically under Ruby 2.4 testing. We haven't seen this in previous Ruby builds (note that Rubyninstaller changed how Ruby is built in the 2.4 installers).

Such an example is at https://ci.appveyor.com/project/puppetlabs/puppet/build/4.1.0.5694/job/jkk5rbf49ou92yc8

#5 - 06/14/2017 04:57 AM - rhenium (Kazuki Yamaguchi)
- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: REQUIRED

[Bug #8386] is unrelated to this. The X509_load_cert_crl_file() function called from OpenSSL::X509::Store#add_file is leaking error in the OpenSSL error queue. This is fixed in OpenSSL's master branch a while ago. https://github.com/openssl/openssl/commit/c0452248ea1a59a41023a4765ef7d9825e80a62b

I'm adding a workaround to ruby/openssl for previous versions of OpenSSL.

#6 - 06/14/2017 09:49 AM - Anonymous
- Status changed from Open to Closed

Applied in changeset trunk|r59081.

dlssl: import v2.0.4

Import Ruby/OpenSSL 2.0.4. Only bug (and typo) fixes. The full commit history since v2.0.3 (imported at r57482) can be found at:

https://github.com/ruby/openssl/compare/v2.0.3...v2.0.4

This contains the fix for [Bug #11033].

Jun Aruga (1):
Update .travis.yml and Dockerfile

Kazuki Yamaguchi (9):
test/test_pkey_ec: do not use dummy 0 order
test/test_ssl: fix typo in test_sysread_and_syswrite
ssl: check return value of SSL_set_fd()
Fix typos
test/test_x509store: skip OpenSSL::TestX509Store#test_set_errors
tool/syscalls-with-trunk: "LASY" -> "LAST"
x509store: clear error queue after calling X509_LOOKUP_load_file()
extconf.rb: simplify searching libraries logic
Ruby/OpenSSL 2.0.4

SHIBATA Hiroshi (1):
Fix typos

Vladimir Rybas (1):
Fix documentation for OpenSSL::Cipher#final

nobu (2):
openssl: fix broken openssl check
openssl: fix broken openssl check
usa (1):
Search SSL libraries by testing various filename patterns

#7 - 06/19/2017 01:41 PM - Iristyle (Ethan Brown)
This ticket is marked as closed - but I only see OpenSSL 2.0.4 in the trunk branch on GitHub per
https://github.com/ruby/ruby/commit/9eb92007b6c2a2b2bf1e0d31c3381144e51e2b2c14.
I do not see the updated OpenSSL in the 2.4 branch at https://github.com/ruby/ruby/tree/ruby_2_4/ext/openssl.
This is becoming a fairly critical problem for our automated testing in AppVeyor. Will the fix be backported to 2.4 as the ticket originally states?
Thanks!

#8 - 06/19/2017 03:26 PM - rhenium (Kazuki Yamaguchi)
- File for-ruby-2-3-backport-805882145bde.patch added

Now that openssl is a default gem, you can just update it before running 'bundle install':

gem install openssl -v '>= 2.0.4'

Anyway, I would like that patch to go to earlier versions of Ruby, too.
2.4 stable maintainer: Can you backport r59081? (I guess r58742 needs to be applied first.)
2.3 stable maintainer: I've attached a patch that applies on top of ruby_2_3.

#9 - 06/19/2017 03:37 PM - usa (Usaku NAKAMURA)
- Backport changed from 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: REQUIRED to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED

rhenium (Kazuki Yamaguchi) wrote:

2.3 stable maintainer: I've attached a patch that applies on top of ruby_2_3.

Oh, thank you!
I'll check and merge it later.

#10 - 06/23/2017 09:28 PM - Iristyle (Ethan Brown)
Thank you rhenium (Kazuki Yamaguchi) - I had not realized that openssl is packaged differently for Ruby 2.4

I have a pull request open to Puppet to address the problem by building / installing the openssl gem - https://github.com/puppetlabs/puppet/pull/6011.
It adds roughly 3 minutes to the time it takes to execute Ruby 2.4 based jobs.
It would be nice if precompiled platform-specific Windows gems were available, which would eliminate the additional 3 minute wait, but this will work for now.

Thanks!

#11 - 06/30/2017 12:43 PM - usa (Usaku NAKAMURA)
- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED to 2.2: UNKNOWN, 2.3: DONE, 2.4: REQUIRED

#12 - 08/03/2017 01:43 PM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 2.2: UNKNOWN, 2.3: DONE, 2.4: REQUIRED to 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE

ruby_2_4 r59489 merged revision(s) 58742,59081.

#13 - 02/17/2018 05:58 AM - nobu (Nobuyoshi Nakada)
- Description updated

Files
for-ruby-2-3-backport-805882145bde.patch 2.89 KB 06/19/2017 rhenium (Kazuki Yamaguchi)