Ruby master - Bug #9774

Net::HTTP failure to validate certificate

04/24/2014 02:39 PM - dougalcorn (Doug Alcorn)

Status:	Closed		
Priority:	Normal		
Assignee:	naruse (Yui NARUSE)		
Target version:			
ruby -v:	ruby 2.0.0p451 (2014-02-24 revision 45167) [x86_64-darwin13.1.0]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN

Description

I'm trying to make an https connection to a host that uses a self-signed certificate. I've downloaded the certificate into a directory of my project and named it based on the fingerprint of the certificate. Using the openssl command line tool, I can verify the certificate. All examples below use an exported environment variable REMOTE_HOST for the hostname I'm connecting to.

```
echo | openssl s_client -CApath ./config/certs/ -connect ${REMOTE_HOST}:${REMOTE_PORT} 2>&1 | grep -i verify
verify return:1
    Verify return code: 0 (ok)
```

I've tried to do the same thing in ruby using this simple script stored in bin/test-net-http.rb:

```
require 'net/http'
require 'net/https'
require 'uri'

ca_path = File.join(File.dirname(__FILE__), "../config/certs")
url = URI.parse "https://#{ENV['REMOTE_HOST']}/authenticate/upauth"
auth_params = {
  uname: "test",
  pswd: "test"
}

http = Net::HTTP.new(url.host, url.port)
http.set_debug_output $stderr
http.use_ssl = (url.scheme == 'https')
if (File.directory?(ca_path) && http.use_ssl?)
  http.ca_path = ca_path
  http.verify_mode = OpenSSL::SSL::VERIFY_PEER
  http.verify_depth = 5
else
  http.verify_mode = OpenSSL::SSL::VERIFY_NONE
end
request = Net::HTTP::Post.new(url.path)
request.set_form_data(auth_params)
response = http.request(request)

puts response.inspect
```

When I run it from the command line as ruby ./bin/test-net-http.rb, I get this stack trace:

```
opening connection to <REMOTE_HOST>:443...
opened
starting SSL for <REMOTE_HOST>:443...
SSL established
Conn close because of connect error SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate verify failed
/Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:918:in `connect': SSL_connect returned=1 errno=0 state=SSLv3 read server certificate verify failed (OpenSSL::SSL::SSLError)
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:918:in `block in connect'
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/timeout.rb:52:in `timeout'
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:918:in `connect'
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:862:in `do_start'
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:851:in `start'
    from /Users/dalcorn/.rbenv/versions/2.0.0-p451/lib/ruby/2.0.0/net/http.rb:1367:in `request'
    from ./bin/test-net-http.rb:24:in `<main>'
```

What I can't tell is the reason the certificate failed to verify. One thing that's different about this cert is that it's a multihost certificate using x509v3 subject alternative names. So, the hostname of REMOTE_HOST mismatches the common name of the cert.

Same results in:

- ruby 1.9.3p448 (2013-06-27 revision 41675) [x86_64-darwin12.5.0]
- ruby 2.0.0p451 (2014-02-24 revision 45167) [x86_64-darwin13.1.0]
- ruby 2.1.0p0 (2013-12-25 revision 44422) [x86_64-darwin13.0]

History

#1 - 06/06/2014 03:00 PM - pfrasa (Pierpaolo Frasa)

I can confirm this bug on Mac OS X Mavericks with Ruby 2.1.1.

I actually didn't specify a ca_path, but imported the self-signed certificate into the Mac OS X keychain. The behaviour is the same however:

```
require 'net/http'
http = Net::HTTP.new('someurl', 443)
http.use_ssl = true
http.start
=> OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=SSLv3 read server certificate B: certificate v
erify failed
```

This bug does not arise with Ruby 1.9.3-p484, where the connection opens normally.

#2 - 07/16/2014 05:48 AM - nagachika (Tomoyuki Chikanaga)

Hello.

I've encounter the similar issue on Mac OS X Mavericks with Ruby 2.0.0-p481 and 2.1.2.
But in my case, the problem is server configuration about intermediate certificate.
The right configuration (SSSLCertificateChainFile of httpd.conf) fixes the problem.
Just for reference.

#3 - 07/26/2014 05:37 PM - naruse (Yui NARUSE)

- Status changed from Open to Feedback

Could you show the site to reproduce on my Mavericks?

#4 - 08/11/2019 05:52 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Feedback to Closed