

Wikiprint Book

Title: ESGF_SSLHandshakeException

Subject: TracMeteo - ESGF_SSLHandshakeException

Version: 13

Date: 01/20/2022 11:40:53 PM

Table of Contents

| | |
|----------------|---|
| Info exception | 3 |
| Produced by | 4 |
| Code in github | 4 |

Info exception

https://blogs.oracle.com/java-platform-group/entry/diagnosing_tls_ssl_and_https

<https://code.google.com/p/zaproxy/issues/detail?id=290>

<http://stackoverflow.com/questions/6353849/received-fatal-alert-handshake-failure-through-sslhandshakeexception>

<http://stackoverflow.com/questions/6383207/how-to-use-tlsv1-or-sslv3-for-first-handshakeclient-hello-in-java>

Exception:

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
```

Debug output:

```

trigger seeding of SecureRandom
done seeding SecureRandom
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% No cached client session
*** ClientHello, TLSv1
RandomCookie:  GMT: 1414437400 bytes = { 141, 161, 100, 14, 170, 248, 62, 119, 104, 169, 61, 146, 199, 29, 125, 247, 244,
Session ID:  {}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC
Compression Methods:  { 0 }
Extension elliptic_curves, curve names: {secp256r1, sect163k1, sect163r2, secp192r1, secp224r1, sect233k1, sect233r1, sect
Extension ec_point_formats, formats: [uncompressed]
***
[write] MD5 and SHA1 hashes:  len = 177
0000: 01 00 00 AD 03 01 54 4F   9A 18 8D A1 64 0E AA F8   .....TO....d...
0010: 3E 77 68 A9 3D 92 C7 1D   7D F7 F4 7B CB A4 5D EE   >wh.=.....].
0020: 43 E3 3C 9A 39 E9 00 00   46 00 04 00 05 00 2F 00   C.<.9...F...../.
0030: 35 C0 02 C0 04 C0 05 C0   0C C0 0E C0 0F C0 07 C0   5.....
0040: 09 C0 0A C0 11 C0 13 C0   14 00 33 00 39 00 32 00   .....3.9.2.
0050: 38 00 0A C0 03 C0 0D C0   08 C0 12 00 16 00 13 00   8.....
0060: 09 00 15 00 12 00 03 00   08 00 14 00 11 00 FF 01   .....
0070: 00 00 3E 00 0A 00 34 00   32 00 17 00 01 00 03 00   ..>...4.2.....
0080: 13 00 15 00 06 00 07 00   09 00 0A 00 18 00 0B 00   .....
0090: 0C 00 19 00 0D 00 0E 00   0F 00 10 00 11 00 02 00   .....
00A0: 12 00 04 00 05 00 14 00   08 00 16 00 0B 00 02 01   .....
00B0: 00                                .
main, WRITE: TLSv1 Handshake, length = 177
[write] MD5 and SHA1 hashes:  len = 173
0000: 01 03 01 00 84 00 00 00   20 00 00 04 01 00 80 00   .....
0010: 00 05 00 00 2F 00 00 35   00 C0 02 00 C0 04 01 00   .../.5.....
0020: 80 00 C0 05 00 C0 0C 00   C0 0E 00 C0 0F 00 C0 07   .....
0030: 05 00 80 00 C0 09 06 00   40 00 C0 0A 07 00 C0 00   .....@.....
0040: C0 11 00 C0 13 00 C0 14   00 00 33 00 00 39 00 00   .....3..9..
0050: 32 00 00 38 00 00 0A 07   00 C0 00 C0 03 02 00 80   2..8.....
0060: 00 C0 0D 00 C0 08 00 C0   12 00 00 16 00 00 13 00   .....
0070: 00 09 06 00 40 00 00 15   00 00 12 00 00 03 02 00   ...@.....
0080: 80 00 00 08 00 00 14 00   00 11 00 00 FF 54 4F 9A   .....TO.
0090: 18 8D A1 64 0E AA F8 3E   77 68 A9 3D 92 C7 1D 7D   ...d...>wh.=....
00A0: F7 F4 7B CB A4 5D EE 43   E3 3C 9A 39 E9           .....].C.<.9.
main, WRITE: SSLv2 client hello message, length = 173
[Raw write]: length = 175
0000: 80 AD 01 03 01 00 84 00   00 00 20 00 00 04 01 00   .....
0010: 80 00 00 05 00 00 2F 00   00 35 00 C0 02 00 C0 04   ...../.5.....

```

```

0020: 01 00 80 00 C0 05 00 C0 0C 00 C0 0E 00 C0 0F 00 .....
0030: C0 07 05 00 80 00 C0 09 06 00 40 00 C0 0A 07 00 .....@.....
0040: C0 00 C0 11 00 C0 13 00 C0 14 00 00 33 00 00 39 .....3..9
0050: 00 00 32 00 00 38 00 00 0A 07 00 C0 00 C0 03 02 ..2..8.....
0060: 00 80 00 C0 0D 00 C0 08 00 C0 12 00 00 16 00 00 .....
0070: 13 00 00 09 06 00 40 00 00 15 00 00 12 00 00 03 .....@.....
0080: 02 00 80 00 00 08 00 00 14 00 00 11 00 00 FF 54 .....T
0090: 4F 9A 18 8D A1 64 0E AA F8 3E 77 68 A9 3D 92 C7 O....d...>wh.=..
00A0: 1D 7D F7 F4 7B CB A4 5D EE 43 E3 3C 9A 39 E9 .....].C.<.9.
[Raw read]: length = 5
0000: 15 03 01 00 02 .....
[Raw read]: length = 2
0000: 02 28 .(
main, READ: TLSv1 Alert, length = 2
main, RECV TLSv1 ALERT: fatal, handshake_failure
main, called closeSocket()
main, handling exception: javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure

```

Avoid exception:

VM arguments

```

-Djavax.net.ssl.trustStore=/home/terryk/.esg/esg-truststore.ts -Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.debug=all -Dhttps.protocols="TLSv1,SSLv3"

```

Program arguments:

```

--oid userOpenIDURL -P password --output outputfil

```

Get property in code:

```

System.getProperty("https.protocols")

```

Set property in code:

```

System.setProperty("https.protocols", "TLSv1,SSLv3");

```

Produced by

modifications in /usr/local/tomcat/conf/server.xml (not sure)

```

sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
instead of
sslProtocol="TLS"

```

Code in github

[?https://github.com/ESGF/esgf-getcert.git](https://github.com/ESGF/esgf-getcert.git)