D4Science Infrastructure - Incident #414

services.d4science cannot connect to pop3 isti sometimes

Jul 23, 2015 10:03 AM - Massimiliano Assante

Status:	Closed	**Start date:**	Jul 23, 2015
Priority:	High	**Due date:**	
Assignee:	_InfraScience Systems Engineer	**% Done:**	100%
Category:	Other	**Estimated time:**	0.00 hour
Target version:	UnSprintable		
Infrastructure:	Production		

Description

I've noticed that sometimes (upon portal restarts) the periodic task which checks the emails of services.d4science (but it was also happening on dev.d4science) returns a javax.mail.MessagingException: Connect failed exception due to some security.validator.ValidatorException (The whole stack trace is attached in the following)

In my code I explicitly set to accept any certificate, however sometimes i still get this exception. Also, if this exception is thrown at portal startup then the mail periodic task will always fail.

I tried to google it and i found this:

... it will only be able to connect to that application if it can trust it. The way trust is handled in the Java world is that you have a keystore (typically $JAVA_HOME/lib/security/cacerts) or also known as the truststore. This contains a list of all the known CA certificates and Java will only trust certificates that are signed by those CA certificate or public certificates that exist within that keystore.

Can we try this out? I mean can we try to install the certificate for pop3 isti in our machine? Should this solve the problem? Any other suggestion?

javax.mail.MessagingException: Connect failed;
nested exception is:
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at com.sun.mail.pop3.POP3Store.protocolConnect(POP3Store.java:213)
at javax.mail.Service.connect(Service.java:364)
at javax.mail.Service.connect(Service.java:245)
at org.gcube.portal.socialmail.PeriodicTask.check(PeriodicTask.java:140)
at org.gcube.portal.socialmail.PeriodicTask.run(PeriodicTask.java:75)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:471)
at java.util.concurrent.FutureTask.runAndReset(FutureTask.java:304)
at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$301(ScheduledThreadPoolExecutor.java:178)
at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExecutor.java:293)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
at java.lang.Thread.run(Thread.java:744)
Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1884)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:276)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:270)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1341)
at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:153)
at sun.security.ssl.Handshaker.processLoop(Handshaker.java:868)
at sun.security.ssl.Handshaker.process_record(Handshaker.java:804)
at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1016)
at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1312)
at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1339)
at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1323)
at com.sun.mail.util.SocketFetcher.configureSSLSocket(SocketFetcher.java:543)
at com.sun.mail.util.SocketFetcher.createSocket(SocketFetcher.java:348)
at com.sun.mail.util.SocketFetcher.getSocket(SocketFetcher.java:236)
at com.sun.mail.pop3.Protocol.(Protocol.java:112)

at com.sun.mail.pop3.POP3Store.getPort(POP3Store.java:264)
at com.sun.mail.pop3.POP3Store.protocolConnect(POP3Store.java:207)
... 11 more
Caused by: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:385)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:292)
at sun.security.validator.Validator.validate(Validator.java:260)
at sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:326)
at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:231)
at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:126)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1323)
... 24 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(SunCertPathBuilder.java:196)
at java.security.cert.CertPathBuilder.build(CertPathBuilder.java:268)
at sun.security.validator.PKIXValidator.doBuild(PKIXValidator.java:380)
... 30 more

History

#1 - Jul 23, 2015 11:22 AM - Massimiliano Assante

- Status changed from New to In Progress

#2 - Jul 23, 2015 11:24 AM - Massimiliano Assante

- Status changed from In Progress to Feedback

- Assignee changed from Massimiliano Assante to Andrea Dell'Amico

I'm not sure how to get the isti pop3 mail server certificate and where to put it, Andrea or Luca could you help with this?

#3 - Jul 23, 2015 12:01 PM - Andrea Dell'Amico

What hostname are you using to connect to the service? I see that pop.isti.cnr.it is the same host as mx.isti.cnr.it but the certificate, at least for https, is valid only for mx.isti.cnr.it. The issuer CA is "TERENA SSL CA", an intermediate CA that has "USERTRUST Network" as root CA.
They should both be present on the default keyring distributed with the jdk, so it's possible that the error is caused by the hostname mismatch.

#4 - Jul 23, 2015 12:07 PM - Massimiliano Assante

I'm using pop.isti.cnr.it as hostname, if I understand changing the hostname to mx.isti.cnr.it may solve the problem? Also any idea on why sometimes (most of the times) no exception is thrown and other times it is?

#5 - Jul 23, 2015 12:21 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> I'm using pop.isti.cnr.it as hostname, if I understand changing the hostname to mx.isti.cnr.it may solve the problem? Also any idea on why sometimes (most of the times) no exception is thrown and other times it is?

Hm. There's more than server maybe, rotated by dns or some proxy. And I see that the dns gives different answers for pop.isti.cnr.it and mx.isti.cnr.it. So I think that the safest way is to grab the certificate and add it to the keyring.

The command to grab the remote public certificate is:

```
openssl s_client -showcerts -connect pop.isti.cnr.it:995 </dev/null
```

You can save the output in a file and then add to the default keyring, or create a different keyring. The cerificate I obtained is self signed, and that explains the java exceptions. Why it doesn't always fail, I don't know.

#6 - Jul 23, 2015 02:17 PM - Massimiliano Assante

- Status changed from Feedback to In Progress

thanks, i did save the output onto a file named pop-isti-cnr.it.cer but have no idea on how to add it to the default keyring, any hint?

#7 - Jul 23, 2015 02:42 PM - Andrea Dell'Amico

One consideration, first: you should use a different keytool file, otherwise if (when) the jdk is upgraded you loose the modifications.

The options that you need to pass to the jdk to point it to a different keyring are something like (from my old documentation regarding Jboss):

```
-Djavax.net.ssl.trustStore=/etc/pki/jvm/jbossas.jks \
 -Djavax.net.ssl.trustStorePassword=<password> \
 -Djavax.net.ssl.keyStorePassword=<password> \
 -Djavax.net.ssl.keyStore=/etc/pki/jvm/jbossas.jks \
 -Djavax.net.ssl.keyStoreType=jks
```

The tools to create/modify a keyring are very low level. There's a java graphical tool called portecle that you can manage to run on OSX, otherwise the only option is the keytool command.
To add a certificate to the default keyring, which has 'changeit' as default password (not a problem since you do not use it to store private keys):

```
keytool -import -alias <cert_name> -keyalg RSA -keystore /path/to/the/default/keyring \
    -dname "cn=pop.isti.cnr.it" -keypass changeit \
    -storepass changeit -file pop-isti-cnr.it.cer
```

#8 - Jul 23, 2015 02:53 PM - Massimiliano Assante

- Status changed from In Progress to Paused

- Assignee changed from Andrea Dell'Amico to Tommaso Piccioli

- Priority changed from Urgent to High

ok, this is too low-level for me :), I'll pause the ticket and let you guys deal with it when you can.

#9 - Jul 23, 2015 03:18 PM - Andrea Dell'Amico

- Status changed from Paused to In Progress

- Assignee changed from Tommaso Piccioli to _InfraScience Systems Engineer

Give me a couple of hours and then you'll have your keyring.

#10 - Jul 23, 2015 03:23 PM - Massimiliano Assante

very good, I'd need it on 6 machines: services.d4science.org, i-marine.d4science.org, descramble.d4science.org, egip.d4science.org, newportal.i-marine.d4science.org and dev.d4science.org

#11 - Jul 23, 2015 04:46 PM - Andrea Dell'Amico

- File cacerts_isti added

I've added the modified cacerts file. The password is still the default one.

#12 - Jul 23, 2015 05:05 PM - Andrea Dell'Amico

I put the file on every machine you listed. The java options to add to the tomcat startup are:

```
-Djavax.net.ssl.trustStore=/etc/ssl/cacerts_isti
```

#13 - Jul 23, 2015 05:05 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

- % Done changed from 0 to 70

#14 - Jul 23, 2015 05:08 PM - Massimiliano Assante

- Status changed from Feedback to In Progress

ok I'll restart the portals tonight with the setting for tomcat

#15 - Jul 23, 2015 05:09 PM - Massimiliano Assante

- Status changed from In Progress to Paused

#16 - Jul 23, 2015 06:56 PM - Massimiliano Assante

- Status changed from Paused to In Progress

#17 - Jul 23, 2015 07:20 PM - Massimiliano Assante

- Status changed from In Progress to Resolved

- % Done changed from 70 to 100

the portals have been restarted, all of them have succeeded to connect to popisti this time, problem seems fixed.

#18 - Jul 24, 2015 03:23 PM - Andrea Dell'Amico

- Status changed from Resolved to Closed

Files

cacerts_isti	82.2 KB	Jul 23, 2015	Andrea Dell'Amico