Runtime Infrastructure - Bug #5362

Handshake failure while testing the simple web cllient

05/12/2021 07:41 PM - Sergey Ivanovskiy

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Igor Skornyakov	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
billable:	No	**case_num:**	
vendor_id:	GCD		

Description

Related issues:

Related to Runtime Infrastructure - Bug #5388: handshake failure while testin...	**Closed**

History

#1 - 05/13/2021 07:25 AM - Greg Shah

- Description updated

From Sergey:

> Could you observe the same exceptions while working with the web client?

```
[05/12/2021 17:08:02 MSK] (com.goldencode.p2j.net.SSL:WARNING) handshake failure

javax.net.ssl.SSLException: bad record MAC
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:214)
        at sun.security.ssl.SSLEngineImpl.fatal(SSLEngineImpl.java:1729)
        at sun.security.ssl.SSLEngineImpl.readRecord(SSLEngineImpl.java:987)
        at sun.security.ssl.SSLEngineImpl.readNetRecord(SSLEngineImpl.java:913)
        at sun.security.ssl.SSLEngineImpl.unwrap(SSLEngineImpl.java:783)
        at javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:626)
        at com.goldencode.p2j.net.SSL.unwrap(SSL.java:484)
        at com.goldencode.p2j.net.SSL.handshake(SSL.java:386)
        at com.goldencode.p2j.net.SSL.run(SSL.java:256)
        at com.goldencode.p2j.net.SSL.notify(SSL.java:247)
        at com.goldencode.p2j.net.BlockingSSL.processInput(BlockingSSL.java:207)
        at com.goldencode.p2j.net.BlockingSSL.checkInput(BlockingSSL.java:113)
        at com.goldencode.p2j.net.NIOSslSocket.lambda$new$1(NIOSslSocket.java:172)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
Caused by: javax.crypto.BadPaddingException: bad record MAC
        at sun.security.ssl.EngineInputRecord.decrypt(EngineInputRecord.java:238)
        at sun.security.ssl.SSLEngineImpl.readRecord(SSLEngineImpl.java:980)
        at sun.security.ssl.SSLEngineImpl.readNetRecord(SSLEngineImpl.java:913)
        at sun.security.ssl.SSLEngineImpl.unwrap(SSLEngineImpl.java:783)
        at javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:626)
        at com.goldencode.p2j.net.SSL.unwrap(SSL.java:484)
        at com.goldencode.p2j.net.SSL.handshake(SSL.java:386)
        at com.goldencode.p2j.net.SSL.run(SSL.java:256)
        at com.goldencode.p2j.net.SSL.notify(SSL.java:247)
        at com.goldencode.p2j.net.BlockingSSL.processInput(BlockingSSL.java:207)
        at com.goldencode.p2j.net.BlockingSSL.checkInput(BlockingSSL.java:113)
        at com.goldencode.p2j.net.NIOSslSocket.lambda$new$1(NIOSslSocket.java:172)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
```

#2 - 05/13/2021 07:25 AM - Greg Shah

From Igor:

> I've not seen this, but, as far as I remember, in such situation a new SSL handshake will be initiated, so it is not a fatal error.

#3 - 05/13/2021 07:26 AM - Greg Shah

If this is non-fatal, then perhaps we should reduce the logging level so that it is only seen when there is a more detailed logging enabled. We don't need to create the impression that there are problems under normal circumstances when there really is no issue.

#4 - 05/26/2021 11:40 AM - Eric Faulhaber

- Related to Bug #5388: handshake failure while testing customer app added

#5 - 05/26/2021 02:48 PM - Sergey Ivanovskiy

I observed the case when the server threw

```
[05/26/2021 19:40:41 MSK] (com.goldencode.p2j.net.SSL:WARNING) handshake failure
javax.net.ssl.SSLException: bad record MAC
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:214)
        at sun.security.ssl.SSLEngineImpl.fatal(SSLEngineImpl.java:1729)
        at sun.security.ssl.SSLEngineImpl.readRecord(SSLEngineImpl.java:987)
        at sun.security.ssl.SSLEngineImpl.readNetRecord(SSLEngineImpl.java:913)
        at sun.security.ssl.SSLEngineImpl.unwrap(SSLEngineImpl.java:783)
        at javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:626)
        at com.goldencode.p2j.net.SSL.unwrap(SSL.java:484)
        at com.goldencode.p2j.net.SSL.handshake(SSL.java:386)
        at com.goldencode.p2j.net.SSL.run(SSL.java:256)
        at com.goldencode.p2j.net.SSL.notify(SSL.java:247)
        at com.goldencode.p2j.net.BlockingSSL.processInput(BlockingSSL.java:207)
        at com.goldencode.p2j.net.BlockingSSL.checkInput(BlockingSSL.java:113)
        at com.goldencode.p2j.net.NIOSslSocket.lambda$new$1(NIOSslSocket.java:172)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
Caused by: javax.crypto.BadPaddingException: bad record MAC
        at sun.security.ssl.EngineInputRecord.decrypt(EngineInputRecord.java:238)
        at sun.security.ssl.SSLEngineImpl.readRecord(SSLEngineImpl.java:980)
        at sun.security.ssl.SSLEngineImpl.readNetRecord(SSLEngineImpl.java:913)
        at sun.security.ssl.SSLEngineImpl.unwrap(SSLEngineImpl.java:783)
        at javax.net.ssl.SSLEngine.unwrap(SSLEngine.java:626)
        at com.goldencode.p2j.net.SSL.unwrap(SSL.java:484)
        at com.goldencode.p2j.net.SSL.handshake(SSL.java:386)
        at com.goldencode.p2j.net.SSL.run(SSL.java:256)
        at com.goldencode.p2j.net.SSL.notify(SSL.java:247)
        at com.goldencode.p2j.net.BlockingSSL.processInput(BlockingSSL.java:207)
        at com.goldencode.p2j.net.BlockingSSL.checkInput(BlockingSSL.java:113)
        at com.goldencode.p2j.net.NIOSslSocket.lambda$new$1(NIOSslSocket.java:172)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
```

but it occurred after the web client created a web socket connection after the embedded fonts were uploaded but the application window was not. Then the web socket connection had been restored. It looks like a bug. The server should shutdown a web client iff such SSL exception was thrown. Correct?

#6 - 05/26/2021 02:49 PM - Sergey Ivanovskiy

To clarify #5362-5 I added messages logs for the js web client

```
websocket is opened. p2j.socket.js:4624:18
1: MSG_CREATE_WINDOW of length 6 done in 24 p2j.socket.js:4376:18
2: CAPTURE_MOUSE of length 2 done in 0 p2j.socket.js:4376:18
3: MSG_IS_FONT_INSTALLED of length 50 done in 2 p2j.socket.js:4376:18
4: MSG_CREATE_FONT of length 58 done in 16 p2j.socket.js:4376:18
5: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
6: MSG_IS_FONT_INSTALLED of length 32 done in 1 p2j.socket.js:4376:18
7: MSG_CREATE_FONT of length 40 done in 15 p2j.socket.js:4376:18
8: MSG_DERIVE_FONT of length 9 done in 1 p2j.socket.js:4376:18
9: MSG_IS_FONT_INSTALLED of length 26 done in 4 p2j.socket.js:4376:18
10: MSG_IS_FONT_INSTALLED of length 28 done in 2 p2j.socket.js:4376:18
11: MSG_CREATE_FONT of length 217396 done in 24 p2j.socket.js:4376:18
downloadable font: kern: Too large subtable (font-family: "Open Sans" style:normal weight:400 stretch:100 src
index:0) source: data:application/x-font-truetype;base64,AAEAAAATAQAABAAwRFNJR54SRB0AAzucAAAVdEdERUYAJgOvAAM3f
AAAAB5HUE9TCzcPNwADN5wAAAA4R1NVQg4r … k2BOG8QrV5WUyxbhmmcz0SspE8jsvrxZsQOkKZnsHYiZJId3D5vKFPvU1ElMdA7IPS5vIMkD
zejlD9AhObNWGdX7rL2sqTi9sNUMo9ljrbCVtGhYw+LXKf+RpMcAAA==
downloadable font: Table discarded (font-family: "Open Sans" style:normal weight:400 stretch:100 src index:0)
source: data:application/x-font-truetype;base64,AAEAAAATAQAABAAwRFNJR54SRB0AAzucAAAVdEdERUYAJgOvAAM3fAAAAB5HUE
9TCzcPNwADN5wAAAA4R1NVQg4r … k2BOG8QrV5WUyxbhmmcz0SspE8jsvrxZsQOkKZnsHYiZJId3D5vKFPvU1ElMdA7IPS5vIMkDzejlD9AhO
bNWGdX7rL2sqTi9sNUMo9ljrbCVtGhYw+LXKf+RpMcAAA==
12: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
13: MSG_IS_FONT_INSTALLED of length 26 done in 2 p2j.socket.js:4376:18
14: MSG_IS_FONT_INSTALLED of length 28 done in 1 p2j.socket.js:4376:18
15: MSG_CREATE_FONT of length 36 done in 16 p2j.socket.js:4376:18
16: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
17: MSG_IS_FONT_INSTALLED of length 26 done in 4 p2j.socket.js:4376:18
18: MSG_IS_FONT_INSTALLED of length 28 done in 0 p2j.socket.js:4376:18
19: MSG_CREATE_FONT of length 36 done in 12 p2j.socket.js:4376:18
20: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
21: MSG_IS_FONT_INSTALLED of length 26 done in 1 p2j.socket.js:4376:18
22: MSG_IS_FONT_INSTALLED of length 28 done in 2 p2j.socket.js:4376:18
23: MSG_CREATE_FONT of length 36 done in 18 p2j.socket.js:4376:18
24: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
25: MSG_IS_FONT_INSTALLED of length 22 done in 3 p2j.socket.js:4376:18
26: MSG_CREATE_FONT of length 30 done in 14 p2j.socket.js:4376:18
27: MSG_DERIVE_FONT of length 9 done in 0 p2j.socket.js:4376:18
28: MSG_SET_UPLOAD_FILE_SIZE_LIMITS of length 9 done in 0 p2j.socket.js:4376:18
30: MSG_CLIENT_READY of length 1 done in 1 p2j.socket.js:4376:18
31: MSG_GET_DESKTOP_DIMENSION of length 5 done in 0
```

that shows the message #30 is MSG_CLIENT_READY. If the web client breaks at the middle, then the js web client misses the main application.

#7 - 05/26/2021 02:51 PM - Greg Shah

If we cannot recover the session, then we need to exit the web client. BUT if possible, we should try to reconnect the websocket without exiting the web client.

#8 - 09/01/2021 11:24 AM - Greg Shah

Igor: Do you think this is this resolved by your changes in #5388?

#9 - 09/01/2021 11:41 AM - Igor Skornyakov

Greg Shah wrote:

> Igor: Do you think this is this resolved by your changes in #5388?

Greg,
Yes, I believe that it was the same problem.

#10 - 09/01/2021 12:33 PM - Greg Shah

- % Done changed from 0 to 100

- Status changed from New to Closed

- Assignee set to Igor Skornyakov

Sergey: If you see this again, we will re-open the problem.