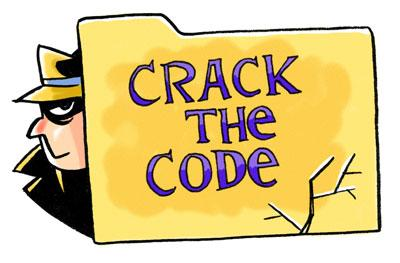
Blog – Cracking the SSL Code



You have a working Splunk environment, and decide to utilize the deployment server functionality to make the deployment of apps and management of configuration files easier.

You start by setting up the serverclass.conf file for the forwarder as the following:

[global]

continueMatching = true

whitelist.0 = \*

restartSplunkd = false

[serverClass:forwarder\_serverclass]

whitelist.0 = \*spkfwd\*

[serverClass:forwarder\_serverclass:app:forwarder\_inputs]

[serverClass:forwarder\_serverclass:app:forwarder\_outputs]

Next, you set up the deploymentclient.conf on the forwarder as follows:

$SPLUNK\_HOME/etc/system/local

[deployment-client]

clientName = <forwarder\_serverclass>

$SPLUNK\_HOME/etc/apps/all\_deploymentclient/local/deploymentclient.conf

[deployment-client]

[target-broker:deploymentServer]

targetUri =< deploymenteserverIP>:<mgmtport>

You check the deployment server to make sure that the forwarder is phoning home!

./splunk list deploy-clients

Even with the proper configuration, the forwarder was still not phoning home to the deployment server!! What is going on??

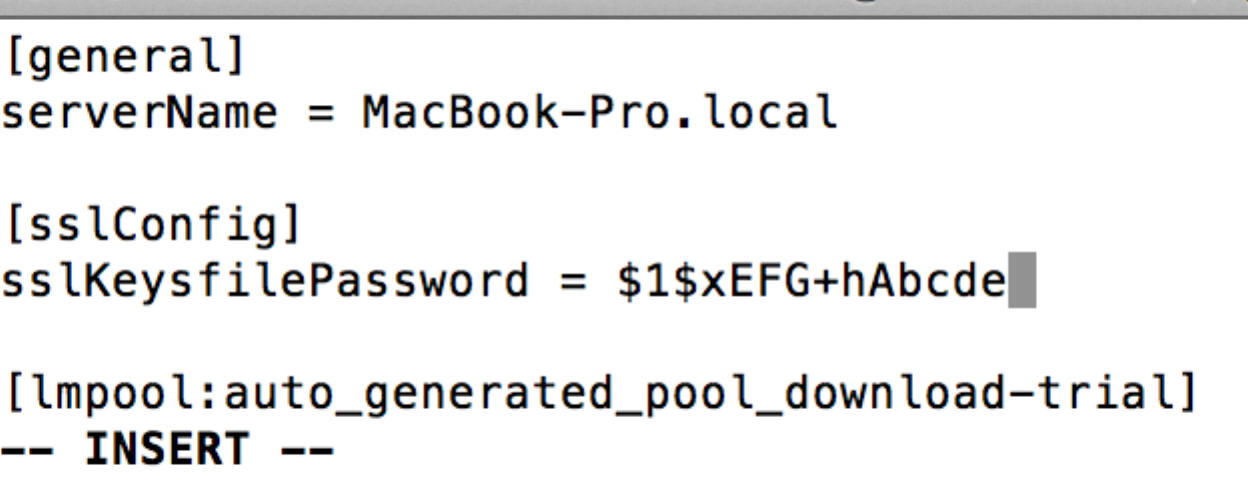
Upon further investigation, the following error was identified in splunkd.log on the forwarder:

**ERROR SSLCommon - Can't read key file /opt/splunkforwarder/etc/auth/server.pem errorno=101077092 error:06065064:digital envelope routines:EVP\_DecryptFinal\_ex:baddecrypt**

**ERROR ServerConfig - Couldn't initialize SSL Context for HTTPClient in ServerConfig**

But you never set a password so why are you getting this error???

This error stems from the SSL password in the server.conf configuration. Splunk automatically creates this password the first time the Splunk instance is started. When cloning instances of Splunk or upgrading an instance, the SSL certificate can become **invalid** and can cause issues when attempting to communicate with other instances.

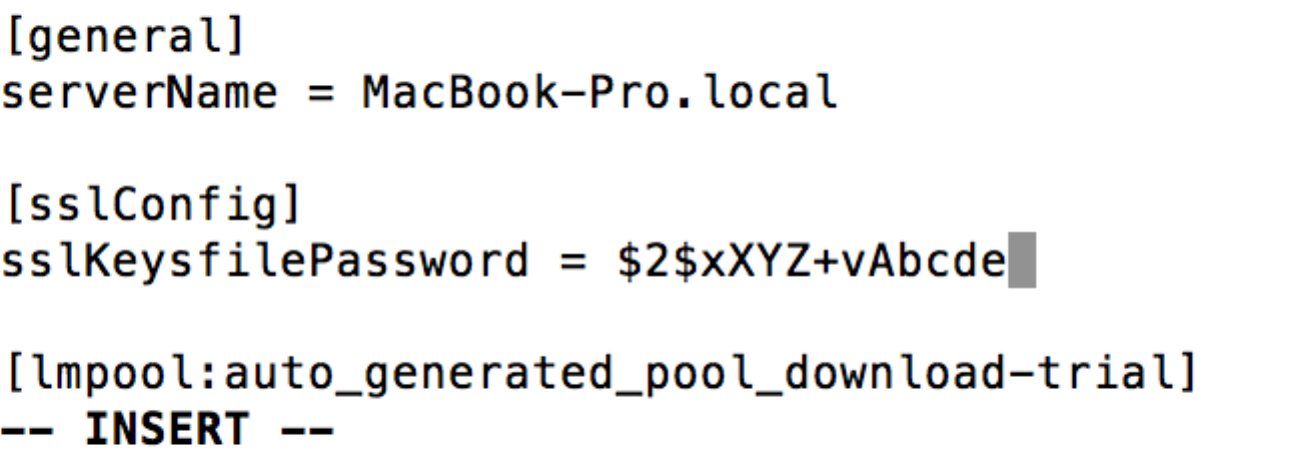


How do I fix this issue??

Go into the server.conf file and change the sslKeysfilePassword to **password**. Then restart the instance for Splunk to assign a new SSL password in the server.conf file.



The new password will allow the forwarder to effectively phone home to the deployment server and the environment set up is now complete!



Another code is cracked!