How to add an eStreamer client:

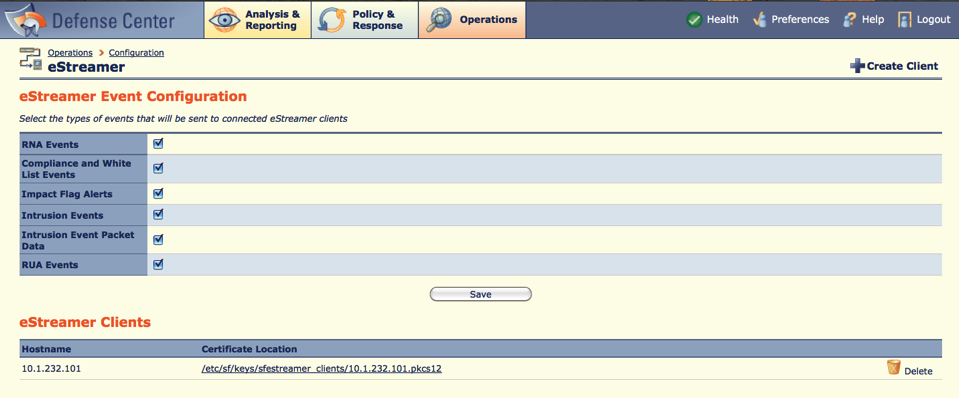
By

Andrew Thanalertvisuti, Solutions Architect, Splunk Inc.

1. Go to Operations 🡪 Configuration 🡪 eStreamer



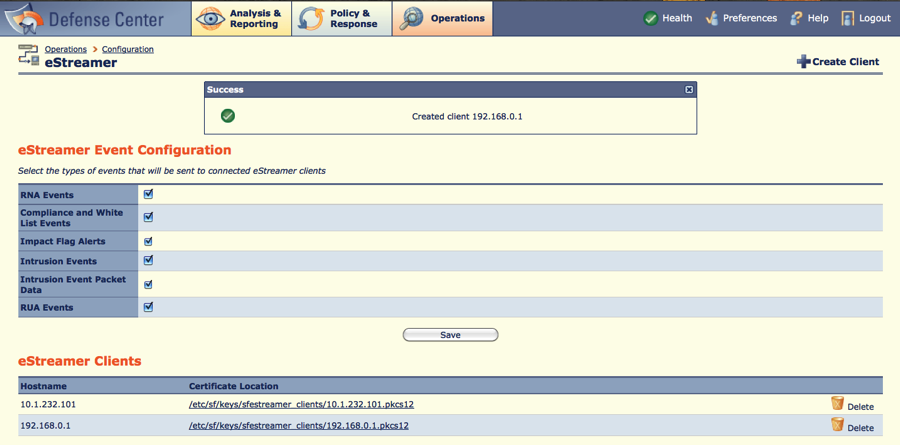
2. Click on Create Client.



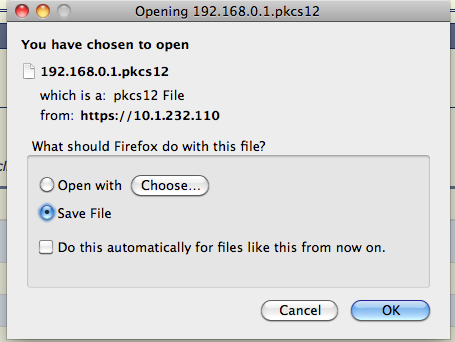
3. Enter a hostname or an IP address of the client that will connect to eStreamer server (i.e. Defense Center). Then click Save.



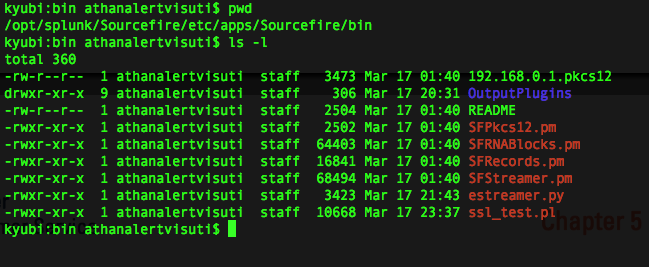
4. Click on the created client Certificate Location.



5. Save the certificate.



6. Copy the certificate to the eStreamer client’s system (inside Splunk for Sourcefire app’s directory)



7. Edit $SPLUNK\_HOME/etc/apps/Sourcefire/default/config.ini. Under [server] stanza, input the IP address of the eStreamer server (i.e. Defense Center). For example:

[server]

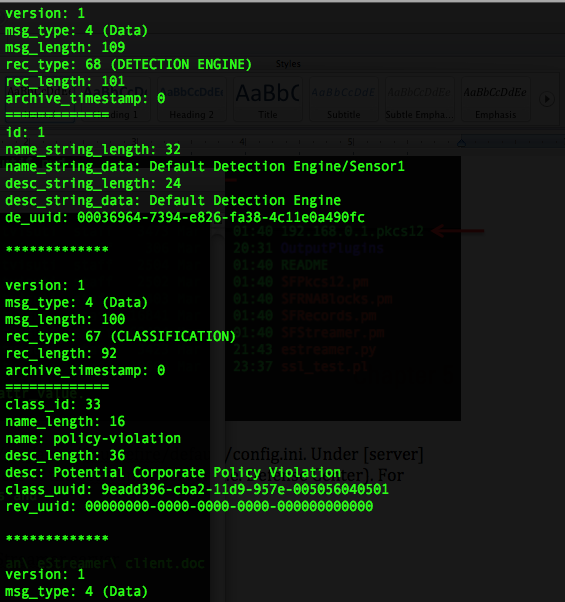
# IP address of eStreamer server

ip = 10.0.0.1

8. Try to test the connection from your eStreamer client to eStreamer server by running the following command (assuming the server ip is 10.0.0.1):

$ $SPLUNK\_HOME/etc/apps/Sourcefire/bin/ssl\_test.pl 10.0.0.1

If everything is set up correctly, the above command should return you many results from the eStreamer server, as shown in the following figure:



9. Now you are ready to start using Splunk for Sourcefire App!