OwnTracks and Mosquitto Private Broker with TLS

sgauche **25d**

I used the RaspPi AIO installer for Home Assistant and am now trying to get mosquitto running with TLS enabled to eventually use with OwnTracks. I would like my location information to be as secure as possible. I do have SSL set up for http, I'm not sure if this is affecting things.

I decided to generate self-signed certificates. I used the shell script at the bottom of the **OwnTracks TLS** page to generate certificates. Here is the **direct link** to the script.

I downloaded the shell script to `/home/pi/Download/mosquitto_certs`. Then un-commented and edited the `HOSTLIST` setting to include my Home Assistant URL. then ran the script with `sudo bash ./generate-CA.sh`. This generated `ca.crt`, `ca.key`, `ca.srl`, `raspberrypi.crt`, `raspberrypi.csr`, and `raspberrypi.key`.

Then I made a directory in /etc/mosquitto called `certs`.
`sudo mkdir /etc/mosquitto/certs`

Then I changed to that directory.
`cd /etc/mosquitto/certs`
And copied `ca.crt`, `ca.key`, `raspberrypi.crt`, and `raspberrypi.key` to the `certs` folder. Then gave permission to mosquitto to access those files.
`sudo chown mosquitto:mosquitto *`

Next, I edited the pre-made mosquitto.conf that must have been included with the AIO installer.
`sudo nano /etc/mosquitto/mosquitto.conf`

Here are the edits I made to that file:
Lines 134-138:

```
# Port to use for the default listener.
#port 1883
port 8883
#listener 8883
protocol websockets
```

Lines 189-196:

```
cafile /etc/mosquitto/certs/ca.crt
#capath

# Path to the PEM encoded server certificate.
certfile /etc/mosquitto/certs/raspberrypi.crt

# Path to the PEM encoded keyfile.
keyfile /etc/mosquitto/certs/raspberrypi.key
```

Line 203:

```
tls_version tlsv1
```

Line 212:

```
require_certificate true
```

Line 217:

```
use_identity_as_username true
```

Now, I need to generate client certificates for Home Assistant.

```
cd /home/pi/Downloads/mosquitto_certs
sudo bash ./generate-CA.sh client hass
```

Which generated `hass.crt`, `hass.csr`, and `hass.key`.
I created a new directory to store these certs for Home Assistant.

```
sudo mkdir /home/hass/.homeassistant/certs
cd /home/hass/.homeassistant/certs
```

Then I copied the three files generated for hass to this new directory and gave permission to hass to access them.

```
sudo chown hass:hass *
```

This is what I added to my Home Assistant configuration for Home Assistant.

```
mqtt:
  broker: 127.0.0.1
  port: 8883
  client_id: home-assistant-1
  username: !secret mqtt_user
  password: !secret mqtt_password
  client_key: /home/hass/.homeassistant/certs/hass.key
  client_cert: /home/hass/.homeassistant/certs/hass.crt
```

And then for OwnTracks:

```
device_tracker:
  platform: owntracks
  max_gps_accuracy: 200
```

When I reboot the Raspberry Pi, Home Assistant shows this error:

```
16-09-13 22:43:49 homeassistant.components.device_tracker: Error setting up
Traceback (most recent call last):
  File "/srv/hass/hass_venv/lib/python3.4/site-packages/homeassistant/compor
    if not platform.setup_scanner(hass, p_config, tracker.see):
  File "/srv/hass/hass_venv/lib/python3.4/site-packages/homeassistant/compor
    mqtt.subscribe(hass, LOCATION_TOPIC, owntracks_location_update, 1)
  File "/srv/hass/hass_venv/lib/python3.4/site-packages/homeassistant/compor
    MQTT_CLIENT.subscribe(topic, qos)
  File "/srv/hass/hass_venv/lib/python3.4/site-packages/homeassistant/compor
    _raise_on_error(result)
  File "/srv/hass/hass_venv/lib/python3.4/site-packages/homeassistant/compor
    raise HomeAssistantError('Error talking to MQTT: {}'.format(result))
homeassistant.exceptions.HomeAssistantError: Error talking to MQTT: 1
```

Not sure what is wrong. Any help would be appreciated, and I'll definitely update some documentation if we can get this figured out!

sgauche 25d

I also enabled logging for mosquitto with log_level 16. Here is the output of the log file. It looks like Home Assistant is trying to connect repeatedly but is getting SSL errors.

```
pi@raspberrypi:~ $ cat /tmp/mosquitto.log
1473872715: mosquitto version 1.4.9 (build date 2016-08-15 13:41:01-0400) st
1473872715: Config loaded from /etc/mosquitto/mosquitto.conf.
1473872715: Opening websockets listen socket on port 8883.
1473872744: SSL_accept failed 1 / error:00000001:lib(0):func(0):reason(1)
1473872744: SSL_accept failed skt 7: error:00000001:lib(0):func(0):reason(1)
1473872744: close: just_kill_connection
1473872744: not calling back closed
1473872744: SSL_accept failed 2 / error:00000002:lib(0):func(0):system lib
1473872750: close: just_kill_connection
1473872750: not calling back closed
1473872754: SSL_accept failed 2 / error:00000002:lib(0):func(0):system lib
1473872755: SSL_accept failed 5 / error:00000005:lib(0):func(0):DH lib
1473872755: SSL_accept failed skt 8: error:00000005:lib(0):func(0):DH lib
1473872755: close: just_kill_connection
1473872755: not calling back closed
1473872755: SSL_accept failed 1 / error:00000001:lib(0):func(0):reason(1)
1473872755: SSL_accept failed skt 7: error:00000001:lib(0):func(0):reason(1)
1473872755: close: just_kill_connection
1473872755: not calling back closed
1473872756: SSL_accept failed 2 / error:00000002:lib(0):func(0):system lib
1473872757: SSL_accept failed 1 / error:00000001:lib(0):func(0):reason(1)
1473872757: SSL_accept failed skt 7: error:00000001:lib(0):func(0):reason(1)
1473872757: close: just_kill_connection
1473872757: not calling back closed
1473872757: SSL_accept failed 5 / error:00000005:lib(0):func(0):DH lib
1473872757: SSL_accept failed skt 8: error:00000005:lib(0):func(0):DH lib
1473872757: close: just_kill_connection
1473872757: not calling back closed
```

sgauche 25d

I tried using the MQTT protocol instead of websockets by changing the protocol line in the mosquitto.conf file. That still doesn't work but returns different errors in the mosquitto.log.

```
pi@raspberrypi:~ $ cat /tmp/mosquitto.log
1473873042: mosquitto version 1.4.9 (build date 2016-08-15 13:41:01-0400) st
1473873042: Config loaded from /etc/mosquitto/mosquitto.conf.
1473873042: Opening ipv4 listen socket on port 8883.
1473873042: Opening ipv6 listen socket on port 8883.
1473873073: New connection from 127.0.0.1 on port 8883.
1473873073: OpenSSL Error: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong
1473873073: Socket error on client <unknown>, disconnecting.
```

```
1473873078: New connection from 127.0.0.1 on port 8883.
1473873085: OpenSSL Error: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong
1473873085: Socket error on client <unknown>, disconnecting.
1473873085: New connection from 127.0.0.1 on port 8883.
1473873086: OpenSSL Error: error:140940E5:SSL routines:SSL3_READ_BYTES:ssl h
1473873086: Socket error on client <unknown>, disconnecting.
1473873086: New connection from 127.0.0.1 on port 8883.
1473873086: OpenSSL Error: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong
1473873086: Socket error on client <unknown>, disconnecting.
1473873086: New connection from 127.0.0.1 on port 8883.
1473873087: OpenSSL Error: error:140940E5:SSL routines:SSL3_READ_BYTES:ssl h
1473873087: Socket error on client <unknown>, disconnecting.
```

aelg305 **25d**

I know it may sound like an stupid question, however, did you updated/changed the values from the script from owntracks.org site to your own custom settings?......

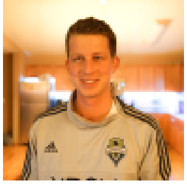
sgauche **25d**

@aleg305 The only thing I changed in the generate-CA.sh file was the `HOSTLIST` variable. I un-commented it and added the URL I use to access Home Assistant.
For Example:

```
HOSTLIST="homeassistant.duckdns.org"
```

sgauche **25d**

This issue seems potentially related.



Issue: MQTT: CloudMQTT certificate verify failed

opened by **ryanborstelmann** on **2016-06-29**

```
Make sure you are running the latest version of Home
Assistant before reporting an issue.
You should only file an issue if...
```