Đề tài: MQTT broker mosquitto ( bảo mật SSL/TLS và username, password)

MQTT là gì? Nó hoạt động ra làm sao ? Có mấy phiên làm việc

MQTT broker

MQTT client

Ở trong MQTT Broker thì nó có rất nhiều công ty hỗ trợ cho việc setup môi trường hoặc là mình có thể sử dụng luôn mqtt Broker mà họ hỗ trợ

Ví dụ như : mosquitto , hivemq , thingsboard

* Mình sử dụng mosquitto
* Và mình setup trên máy local

Hoạt động dựa trên cơ chế publish / subscribe, ngoài ra thì nó còn hỗ trợ qOS(3 cái , bọn cậu đọc nhớ)

https://tapit.vn/hieu-dung-ve-moi-quan-qos-giua-publisher-va-subscriber-trong-giao-thuc-mqtt/

PUBLISH mình gửi message tới 1 topic nào đó ( topic mình quy định sẵn rồi)

* Ví dụ gửi message : test data tới topic : /dev/test và topic này sẽ chứa message test data -> 1 client sẽ subscribe tới topic đó và nhận được dữ liệu đó

SUBSCRIBE : tức là mình đăng ký 1 topic cụ thể nào đó

->ví dụ như mình đki topic: /dev/test , mình sẽ nhận được dữ liệu là : test data

Đồng thời có thể SUB và PUB

1 phiên của nó : xác thực ( mình cần những cái gì : địa chỉ broker, port , những file cấu hình liên quan: ssl/tls , username và pwd của mqtt ( nếu có))

Broker url : 192.168.1.27

File .ca hoặc .pem tls/ssl

User và pwd

Kết nối tới broker: kết nối hoàn thành , mình có thể trao đổi dữ liệu

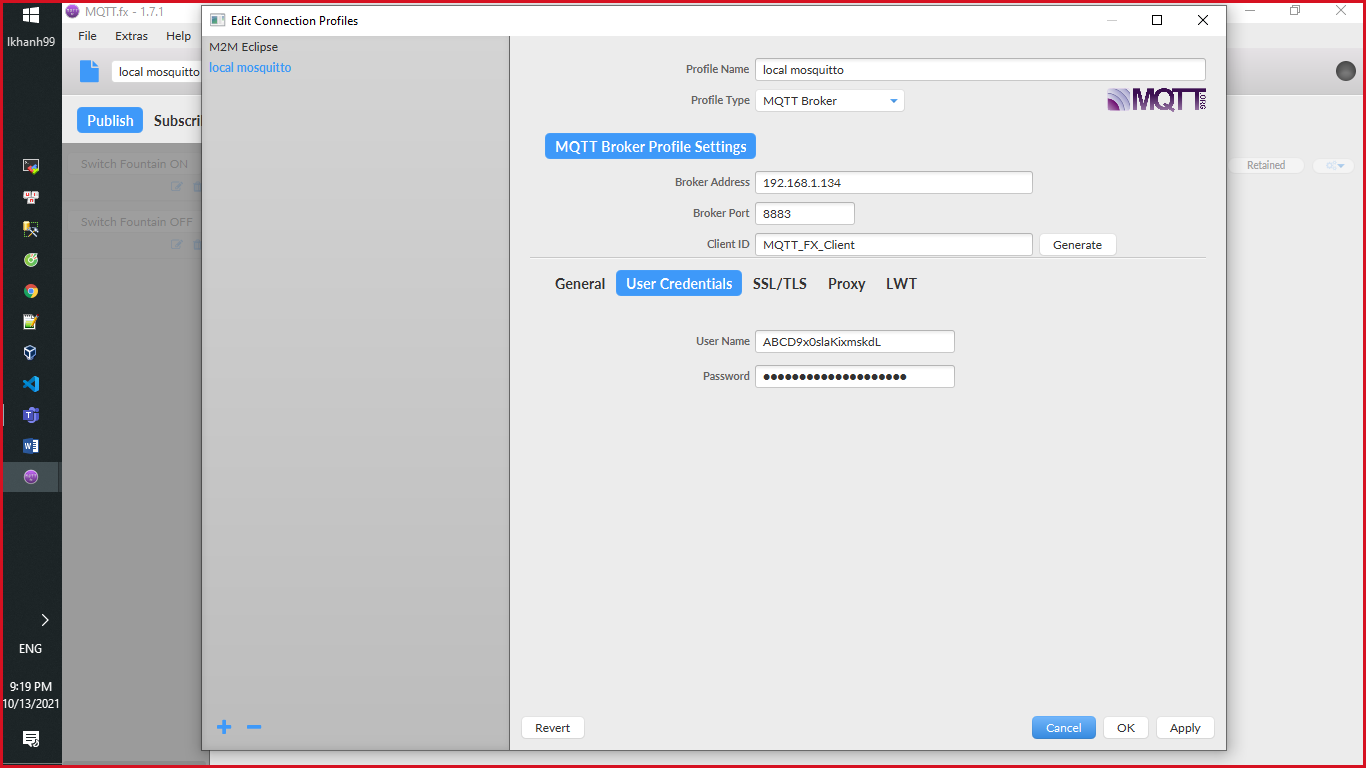
Trao đổi dữ liệu ( PUB /SUB) : nếu mình dùng tls/ssl -> nó sẽ mã hóa dữ liệu

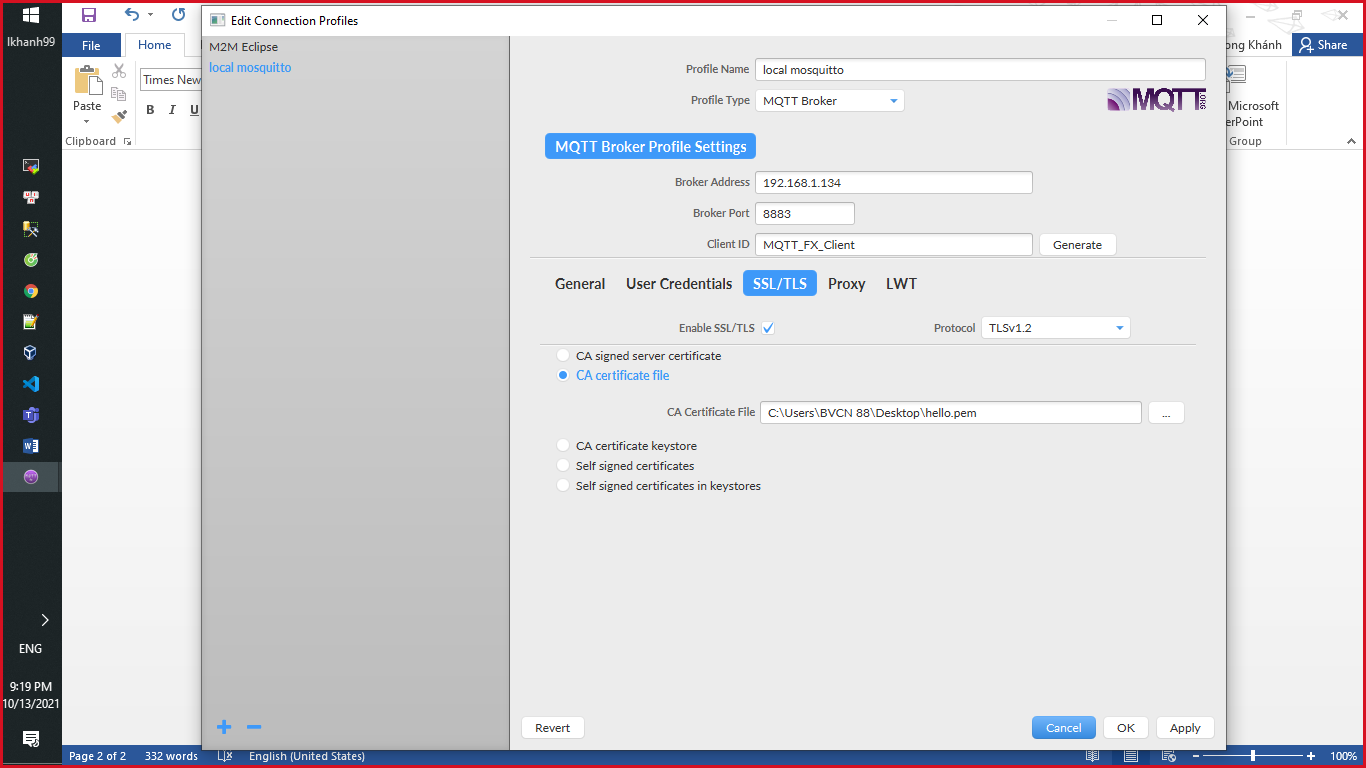
PUB topic /dev/test và gửi msg: test

SUB topic /test/dev và nhận msg từ client nào đó

Kết thúc(gửi dữ liệu xong) : tùy xem qos là bnh nữa

Ví dụ qos là 3 , thì mình phải xác nhận xem nó gửi dữ liệu tới hay chưa -> trả về 1 ID nào đó





Việc mình setup môi trường cho mosquitto trên máy của mình -> broker( Dung lượng -> chính cái raspberry có khỏe không)

Việc mình connect với broker đó -> client

Hoặc là mình dùng esp32 hoặc esp8266 -> kết nối tới mqtt broker -> client

Đề tài mình bảo mật những gì

-Bảo mật tính xác thực:

+) TLS/SSL

+) user và pwd

-Bảo mật dữ liệu

+)TLS /SSL

Còn mình tạo ra file \*python chỉ để test truyền/ nhận dữ liệu thôi -> kiểu là chứng minh cho cô thấy mình đã dùng ssl/tls , username và pwd cho mqtt broker đó

<https://www.hostinger.vn/huong-dan/https-tls-ssl-la-gi>

* Nó là một chứng chỉ

Đầu tiên, mình cài MQTT mosquitto broker trên máy localhost của mình

sudo apt-get install mosquitto

thêm file user và pwd

thêm những tệp tin file ssl/tls

port dùng ssl/tls

Cách tạo username/pwd trên mqtt broker

sudo mosquitto\_passwd -c /etc/mosquitto/pwfile TYPE\_YOUR\_USERNAME\_HERE

* Tạo ra 1 file -> cần thêm file này vào file cấu hình mqtt broker

Thêm 2 dòng sau

Allow\_anonymous false

Password\_file (folder file)

Cách tạo file ssl/tls trên openssl

Cài gói openssl ( sudo apt-get install openssl)

**openssl genrsa -des3 -out ca.key 2048**

**openssl req -new -x509 -days 1826 -key ca.key -out ca.crt**

**openssl genrsa -out server.key 2048**

**openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 360**

**Thêm những file cần thiết vào file .cnf**

* **Khởi động lại broker trên localhost**

**Sudo systemctl restart mosquitto**