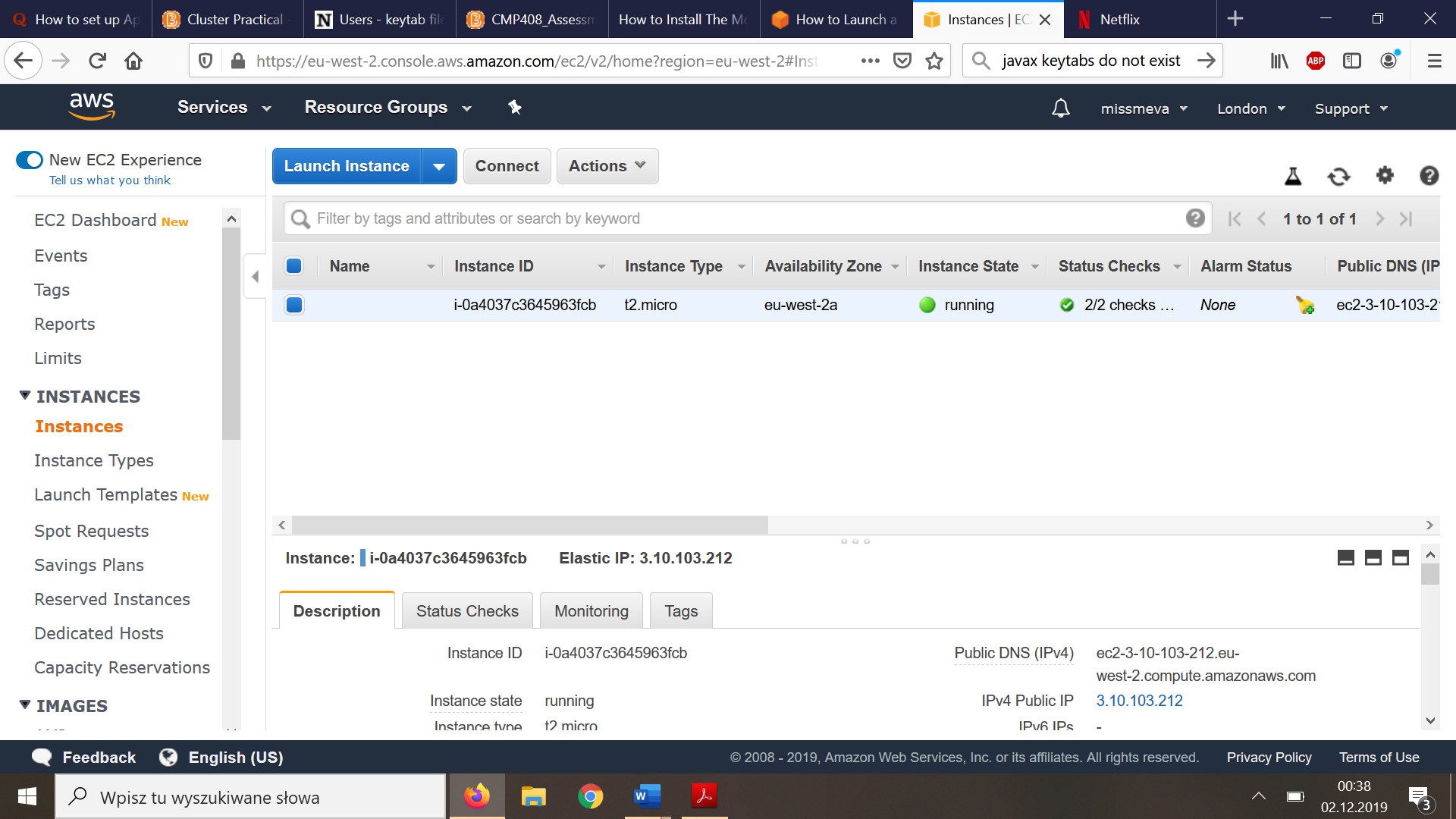
MQTT Mosquitto Broker

Setting up a virtual server

The first step to launching an EC2 instance at AWS was making the choice on the AMI (Amazon Machine Image) to be used for the project purposes. Out of 17 available AMIs, representing the distributions of the operating systems such as Ubuntu, Microsoft Windows, Amazon Linux 2 or Red Hat, the choice fell on the server based on the OS deemed as secure and best suited for the development, as well as facilitating the installation of open-source software (in this case mosquitto message broker) - Ubuntu Server 18.04 LTS. Regarding the limitations of the AWS Free Tier, granting 750 hours of EC2 usage, the only available instance type was t2.micro offering a single virtual CPU, gibibyte of data and 6 CPU units per hour. Finally, the AMI has been linked with the default security group *launch-wizard2* and the instance has been launched.



Security group

In terms of the security group, the default settings of the group did not allow any incoming traffic, which is related with Amazon’s policy of total control over the access to the resources purchased and/or utilized the client. Establishing the rules began with defining SSH connection, which has been created for the communication purposes between the devices and has been set to port 22 with the inbound traffic allowed only from the IP of the current device, so that the connection attempt from any other source was automatically refused. Next, the MQTT listening port 8883 has been added to the list in order to enable communication between publisher and the MQTT server. Once the changes has been reflected in the configuration file of the mosquitto server, the publisher and subscriber script could be implemented.

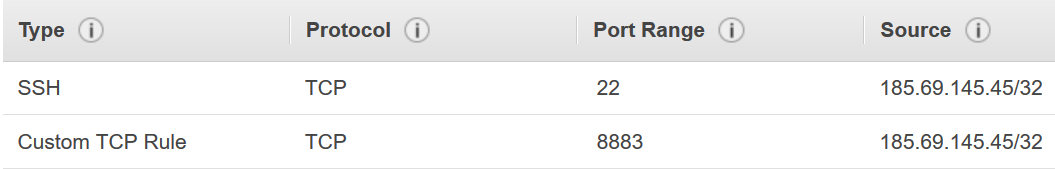


Fig.1 Security group – inbound rules

Security features

Regarding the security of the infrastructure, its main aspect was the establishment of the AWS security group, designed to refuse connection attempts from unauthorized sources. In order to encrypt the communication the listener has been set to port 8883, which is commonly used SSL encryption. Although SSL configuration would significantly increase system’s security ad robustness, it was not implemented due to the lack of access to the private domain name and hence the cost efficient solution was deemed as a priority. Finally, the MQTT password has been encrypted (Fig.2) and the port 1883 has been removed from security group settings.

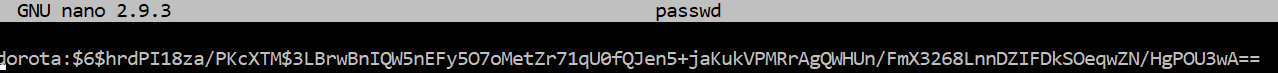


Fig.2 MQTT password in the encrypted form

References:

Cope, S. (2019). *How to Install The Mosquitto MQTT Broker on Linux (Ubuntu)*. [online] Steves-internet-guide.com. Available at: [http://www.steves-internet-guide.com/install-mosquitto-linux/?fbclid=IwAR2zW0FnauVPe5AkW0AJ8Z6h-GXYIWv\_LBgklBgA0eW\_kK-4ECbzq6YPG3w](http://www.steves-internet-guide.com/install-mosquitto-linux/?fbclid=IwAR2zW0FnauVPe5AkW0AJ8Z6h-GXYIWv_LBgklBgA0eW_kK-4ECbzq6YPG3w%20)