docker daemon TLS

- create directories:

```
mkdir -p ${HOME}/.docker
mkdir -p /etc/docker/certs
```

- create certificates:

```
docker run --rm -v $(pwd)/.docker:/certs paulczar/omgwtfssl
sudo cp ~/.docker/ca.pem /etc/docker/ssl/ca.pem
chown -R $USER ~/.docker
# añadir IPs correspondientes
docker run --rm -v /etc/docker/ssl:/server \
    -v $(pwd)/.docker:/certs \
    -e SSL_IP=127.0.0.1,172.17.8.101 \
    -e SSL_DNS=docker.local -e SSL_KEY=/server/key.pem \
    -e SSL_CERT=/server/cert.pem paulczar/omgwtfssl
```

- test manual:

```
sudo systemctl stop docker.service
dockerd \
    --tlsverify \
    --tlscacert=/etc/docker/certs/ca.pem \
    --tlscert=/etc/docker/certs/cert.pem \
    --tlskey=/etc/docker/certs/key.pem \
    -H=0.0.0.0:2376
docker --tlsverify \
    --tlscacert=${HOME}/.docker/ca.pem \
    --tlscert=${HOME}/.docker/cert.pem \
    --tlskey=${HOME}/.docker/key.pem \
    -H=127.0.0.1:2376 version
```

- configurar dockerd:

```
sudo cp /lib/systemd/system/docker.service /etc/systemd/system/docker.service
```

- modificar el fichero:

  /etc/systemd/system/docker.service

```
...
ExecStart=/usr/bin/dockerd -H fd:// -H tcp://0.0.0.0:2376 -H
unix:///var/run/docker.sock\
  --tlsverify \
  --tlscacert=/etc/docker/certs/ca.pem \
  --tlskey=/etc/docker/certs/key.pem \
  --tlscert=/etc/docker/certs/cert.pem
...
```

  - se puede quitar el acceso a usuarios locales sacando el **-H unix:///var/run/docker.sock**

- rearrancar:

```
sudo systemctl daemon-reload
```

```
sudo systemctl restart docker
```

- dejar por defecto el cliente (si se ha quitado el acceso a través del socket):

```
export DOCKER_HOST=tcp://127.0.0.1:2376 DOCKER_TLS_VERIFY=1
DOCKER_CERT_PATH=~/.docker
```

/via: https://docs.docker.com/engine/security/protect-access/
/via: https://tech.paulcz.net/2016/01/secure-docker-with-tls/ (OLD, 2016, el service no funciona)
/via: https://riptutorial.com/docker/example/17079/enable-remote-access-with-tls-on-systemd