docker security

- SSL, TLS: https://docs.docker.com/engine/security/protect-access/
- https://www.labkey.org/Documentation/wiki-page.view?name=dockerTLS
- https://docs.docker.com/engine/security/apparmor/
- `docker context` → https://docs.docker.com/engine/context/working-with-contexts/

- https://tech.paulcz.net/2016/01/secure-docker-with-tls/
- `docker run –rm -v $(pwd)/.docker:/certs paulczar/omgwtfssl`

creación certificados

- CA:

```
openssl genrsa -out ca-key.pem 4096
openssl req -x509 -new -nodes -key ca-key.pem -days 3650 -out ca.pem -subj
'/CN=docker-CA'
```

openssl-ca.cnf

```
    [req]
    req_extensions = v3_req
    distinguished_name = req_distinguished_name
    [req_distinguished_name]
    [ v3_req]
    basicConstraints = CA:FALSE
    keyUsage = nonRepudiation, digitalSignature, keyEncipherment
    extendedKeyUsage = serverAuth, clientAuth
```

- client:

```
openssl genrsa -out client-key.pem 4096
openssl req -new -key client-key.pem -out client-cert.csr -subj '/CN=docker-
client' -config openssl-ca.cnf
openssl x509 -req -in client-cert.csr -CA ca.pem -CAkey ca-key.pem -
CAcreateserial -out client-cert.pem -days 3650 -extensions v3_req -extfile
openssl-ca.cnf
```

- daemon:

```
sudo mkdir /etc/docker/ssl
sudo chmod 700 /etc/docker/ssl
sudo cp ca.pem /etc/docker/ssl
sudo vim /etc/docker/ssl/openssl.cnf
sudo openssl genrsa -out /etc/docker/ssl/daemon-key.pem 4096
sudo openssl req -new -key /etc/docker/ssl/daemon-key.pem -out
/etc/docker/ssl/daemon-cert.csr -subj '/CN=docker-daemon' -config
/etc/docker/ssl/openssl.cnf
sudo openssl x509 -req -in /etc/docker/ssl/daemon-cert.csr -CA
/etc/docker/ssl/ca.pem -CAkey ca-key.pem -CAcreateserial -out
/etc/docker/ssl/daemon-cert.pem -days 3650 -extensions v3_req -extfile
/etc/docker/ssl/openssl.cnf
```

openssl-daemon.cnf

```
[req]
req_extensions = v3_req
distinguished_name = req_distinguished_name
[req_distinguished_name]
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = yourtestweb | yourprodweb
DNS.2 = yourtestrserve | yourprodrserve
IP.1 = 127.0.0.1
IP.2 = 10.0.0.87 | 10.10.0.37
```

- change dockerd