Securing Your Docker Registry



David Clinton
LINUX SYSTEM ADMINISTRATOR

www.bootstrap-it.com/docker-images | www.bootstrap-it.com/blog



Using CA certificates

Using self-signed certificates

Configure login authentication



Using CA certificates

Using self-signed certificates

Configure login authentication



Using CA certificates

Using self-signed certificates

Configure login authentication

Applying a CA-provided Certificate

Copy CA-provided Certificates:

```
mkdir ~/certs
cp stuff.* certs
```

Copy CA-provided Certificates:

```
mkdir ~/certs
cp stuff.* certs
[if you received an intermediary certificate:]
cat stuff.crt intermediate-stuff.pem > ~/certs/stuff.crt
```

Adding Certs at Run-time:

```
docker run -d -p 5000:5000 --restart=always --name registry \
  -v `pwd`/certs:/certs \
  -e REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt \
  -e REGISTRY_HTTP_TLS_KEY=/certs/stuff.key \
  registry
```

Adding Certs to a Dockerfile:

```
FROM registry

ADD /certs/ /home/

ENV REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt
REGISTRY_HTTP_TLS_KEY=/certs/stuff.key

EXPOSE 5000
```

Add config.yml file to container:

Applying a Self-signed Certificate



Create local domain

Generate self-signed cert

Copy cert file to the Docker client



Create local domain

Generate self-signed cert

Copy cert file to the Docker client

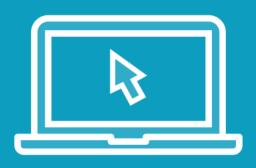


Create local domain

Generate self-signed cert

Copy cert file to the Docker client

User Authentication



Create a user account

Enforce password login for Docker Registry



Create a user account

Enforce password login for Docker Registry



(error message:) "http: server gave HTTP response to HTTPS client"

```
-e REGISTRY_HTTP_TLS_KEY=/certs/stuff.key \
```

ENV REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt REGISTRY_HTTP_TLS_KEY=/certs/stuff.key

http:

tls:

certificate: /home/ubuntu/certs/stuff.crt

key: /home/ubuntu/certs/stuff.key



(error message:) "http: server gave HTTP response to HTTPS client"

-e REGISTRY_HTTP_TLS_KEY=/certs/stuff.key \

ENV REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt REGISTRY_HTTP_TLS_KEY=/certs/stuff.key

http:

tls:

certificate: /home/ubuntu/certs/stuff.crt

key: /home/ubuntu/certs/stuff.key



(error message:) "http: server gave HTTP response to HTTPS client"

-e REGISTRY_HTTP_TLS_KEY=/certs/stuff.key \

ENV REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt REGISTRY_HTTP_TLS_KEY=/certs/stuff.key

http:

tls:

certificate: /home/ubuntu/certs/stuff.crt

key: /home/ubuntu/certs/stuff.key



```
(error message:) "http: server gave HTTP response to HTTPS client"
```

```
-e REGISTRY_HTTP_TLS_KEY=/certs/stuff.key \
```

```
ENV REGISTRY_HTTP_TLS_CERTIFICATE=/certs/stuff.crt REGISTRY_HTTP_TLS_KEY=/certs/stuff.key
```

http:

certificate: /home/ubuntu/certs/stuff.crt key: /home/ubuntu/certs/stuff.key



-v `pwd`/config.yml:/etc/docker/registry/
config.yml \

cp ca.crt /etc/docker/certs.d/stuff.com:5000/

auth:

htpasswd:

realm: basic-realm

path: /home/ubuntu/auth/htpasswd



```
-v `pwd`/config.yml:/etc/docker/registry/
config.yml \
```

cp ca.crt /etc/docker/certs.d/stuff.com:5000/

auth:

htpasswd:

realm: basic-realm

path: /home/ubuntu/auth/htpasswd



```
-v `pwd`/config.yml:/etc/docker/registry/
config.yml \
```

cp ca.crt /etc/docker/certs.d/stuff.com:5000/

auth:

htpasswd:

realm: basic-realm

path: /home/ubuntu/auth/htpasswd