ISSA Journal April 2017

Security Assurance of Docker Containers: Part 1

By Stefan Winkel
stefan@winkelsnet.com

Appendix Section B
Setting up Docker Content Trust Sandbox

```
#Add an entry for the notaryserver to /etc/hosts:
$ sudo sh -c 'echo "127.0.0.1 notaryserver" >> /etc/hosts'

#Add an entry for the sandboxregistry to /etc/hosts
$ sudo sh -c 'echo "127.0.0.1 sandboxregistry" >> /etc/hosts'

#Make the notarysandbox/notarytest directory structure
$ mkdir notarysandbox && cd notarysandbox && mkdir notarytest && cd notarytest

#Create a Dockerfile with the following content:

      FROM debian:jessie

      ADD https://master.dockerproject.org/linux/amd64/docker /usr/bin/docker
      RUN chmod +x /usr/bin/docker \
        && apt-get update \
        && apt-get install -y \
        tree \
        vim \
        git \
        ca-certificates \
        --no-install-recommends

      WORKDIR /root
      RUN git clone -b trust-sandbox https://github.com/docker/notary.git
      RUN cp /root/notary/fixtures/root-ca.crt /usr/local/share/ca-
      certificates/root-ca.crt
      RUN update-ca-certificates

      ENTRYPOINT ["bash"]

# Build the test container
$ docker build -t notarysandbox .

# Change to back to the root of your Notarysandbox directory
```

```
$ cd ../../notarysandbox

# Clone the Notary project
$ git clone -b trust-sandbox https://github.com/docker/notary.git

# Clone the distribution project.
$ git clone https://github.com/docker/distribution.git

# Change to the Notary project directory.
$ cd notary

# Build the server image and run service on the local box
# mkdir notary2
$ git clone https://github.com/docker/notary.git
$ cd notary
$ docker-compose up -d

# Setup a local version of the Docker Registry v2
# Change to the notarysandbox/distribution directory.
$ cd ../../../notarysandbox/distribution

# Build the sandboxregistry server
$ docker build -t sandboxregistry .

#Start the sandboxregistry server
$ docker run -p 5005:5005 --name sandboxregistry sandboxregistry &

# Start the notarysandbox and link it to the running notary_notaryserver_1 and
sandboxregistry containers. The links allow communication among the containers.

$ docker run -it -v /var/run/docker.sock:/var/run/docker.sock --link
notary_notaryserver_1:notaryserver --link sandboxregistry:sandboxregistry
notarysandbox
```