Software signing is an important aspect of security. It provides us with a greater sense of confidence that the software we're running on your systems has not been tampered with after being released by the software publisher. Docker Content Trust establishes signing for Docker images. In this lesson, we will briefly discuss what Docker Content Trust is. Additionally, we will cover how to sign images, run signed images, plus how to enable, and disable Docker Content Trust.

Relevant Documentation

- https://docs.docker.com/engine/security/trust/content_trust/#push-trusted-content

Lesson Reference

In order to follow along with this lesson, a Docker Hub account is required. An account can be created for free at https://hub.docker.com.

First, log in to Docker Hub. Enter your Docker Hub credentials when prompted.

```
docker login
```

Generate a delegation key pair. We can enter a passphrase of our choosing, but make note of it as we will need it later on in the lesson.

```
cd ~/
docker trust key generate <your docker hub username>
```

Then we'll add ourselves as a signer to an image repository. Once again, be sure to make note of the passphrases used.

```
docker trust signer add --key <your docker hub username>.pub <your docker hub username> <your docker hub user
```

Create and build a simple Docker image with an unsigned tag, and then push it to Docker Hub:

```
mkdir ~/dct-test
cd dct-test
vi Dockerfile
```

```
FROM busybox:latest

CMD echo It worked!
```

```
docker build -t <your docker hub username>/dct-test:unsigned
docker push <your docker hub username>/dct-test:unsigned
```

Run the image to verify whether it can run successfully:

```
docker run <your docker hub username>/dct-test:unsigned
```

Next, enable Docker content trust and attempt to run the unsigned image again:

Note: We should see it fail.

```
export DOCKER_CONTENT_TRUST=1
docker run <your docker hub username>/dct-test:unsigned
```

Build and push a signed tag to the repo. Enter the passphrase — this will be the one that was chosen earlier when running the `docker trust key generate` command:

```
docker build -t <your docker hub username>/dct-test:signed .
docker trust sign <your docker hub username>/dct-test:signed
```

Run it to verify that the signed image can run properly with Docker Content Trust enabled:

```
docker image rm <your docker hub username>/dct-test:signed .
docker run <your docker hub username>/dct-test:signed
```

Turn off Docker Content Trust and attempt to run the unsigned image again:

Note: It should work this time.

```
export DOCKER_CONTENT_TRUST=0
docker run <your docker hub username>/dct-test:unsigned
```