Docker content Trust

Docker Content Trust (DCT) provides the ability to use digital signatures for data sent to and received from remote Docker registries. These signatures allow client-side or runtime verification of the integrity and publisher of specific image tags.

It is the responsibility of the image publisher to decide if an image tag is signed or not.

Image consumers can enable DCT to ensure that images they use were signed. If a consumer enables DCT, they can only pull, run, or build with trusted images. Enabling DCT is a bit like applying a “filter” to your registry. Consumers “see” only signed image tags and the less desirable, unsigned image tags are “invisible” to them.

Signing Images with Docker Content Trust

* To sign a Docker Image you will need a delegation key pair. These keys can be generated locally using $ docker trust key generate or generated by a certificate authority.

docker trust key generate jeff

* Next we will need to add the delegation public key to the Notary server; this is specific to a particular image repository in Notary

docker trust signer add --key cert.pem jeff registry.example.com/admin/demo

* Finally, we will use the delegation private key to sign a particular tag and push it up to the registry.

docker trust sign registry.example.com/admin/demo:1

* Alternatively, once the keys have been imported an image can be pushed with the $ docker push command, by exporting the DCT environmental variable.

export DOCKER\_CONTENT\_TRUST=1

docker push registry.example.com/admin/demo:1

Approach in our environment

Need to modify our existing playbook that creates and pushes image to include these steps so that all our images are signed before pushing.

These steps require

* DOCKER\_CONTENT\_TRUST\_REPOSITORY\_PASSPHRASE
* DOCKER\_CONTENT\_TRUST\_ROOT \_PASSPHRASE
* DOCKER\_CONTENT\_TRUST\_SIGNER \_PASSPHRASE
* KEY

Creating a template in TSS and can fetch these values from TSS to make it dynamic

A prerequisite for signing an image is a Docker Registry with a Notary server attached (Such as the Docker Hub .

Deploy Notary Server

<https://docs.docker.com/engine/security/trust/deploying_notary/>