Your supermarket company has a Docker server where they want to run a simple web service in a container. This web service provides a list of the various kinds of tea sold in each of the company's stores. However, Docker Content Trust on the server is enabled to bolster the overall security. The tea service cannot run on the server because the image is not currently signed.

Your task is to create a new tag for the image, sign it, and then push it to a private registry. Once you have done this, run the image to verify that you can successfully execute the image with Docker Content Trust enabled.

Here is some important information to keep in mind as you work through this lab:

1. The signed image should be stored in the IP-10-0-1-102:443/content-dca-tea repository. Generate a trusted key and add yourself as a signer for this repository.

2. The unsigned image is already pulled on the server and is called linuxacademycontent/content-dca-tea:1.

3. The server is already configured to use the private registry, which is IP-182.18.177.46. You do not need to log in to the registry or configure certificate trust settings for the registry.

4. Create a new tag for the image. The new tag should be IP-182.18.177.46/content-dca-tea:1.

5. Sign the new tag and push it to the private registry.

Once you have pushed the signed image, you should be able to run it with the line shown here: docker run -d -p 8080:80 ip-10-0-1-102:443/content-dca-tea:1. Once the image is running, you can test it with curl localhost:8080. You should see a JSON list generated for the various kinds of tea.

Good luck!

Generate a Trust Key and Add Yourself as a Signer to the New Repository

1. Generate a trusted key.

docker trust key generates Sravanthi

2. Create a new passphrase for your key when prompted.

passphrase : sravanthi95

repeat passphrase : sravanthi95

3. Add yourself as a signer to the ip-182.18.177.46:443/content-dca-tea repository.

docker trust signer add sravanthi ip-182.18.177.46

/content-dca-tea --key sravanthi.crt

Create passphrases for the new root key and new repository key when prompted.

1. Create a new tag for the image.

2. Sign the image and push it to the registry.

3. Enter the passphrase you created earlier for the trust key.

4. Verify that you can run the signed image.

If you want to test the image further, you can query the tea list web service. (You should see generated JSON data that contains a list of the various kinds of tea.)