Scanning images in Google Container Registry (GCR)

Table of Contents

Introduction

Black Duck can scan container images stored in Google Container Registry (GCR). Scan results are sent to your Black Duck instance to provide vulnerability, license, and operational risk results on the open source software components identified in the GCR image.

There are two ways to scan container images in GCR:

- By using Synopsys Detect on a local workstation.
- Invoking Synopsys Detect in Cloud Build.

These methods are described in more detail in the following section:

Using Synopsys Detect on a local workstation

Ensure that you satisfy the following prerequisites before you can scan images in GCR by using Synopsys Detect.

- One or more container images stored in GCR (For more information about publishing and storing images in GCR, refer to the container registry topic about pushing and pulling images.)
- Installed and initialized the gcloud CLI
- Installed Docker

To locally scan container images stored in ECR, follow these steps:

1. Authenticate with GCR. Synopsys recommends using *gcloud* as a Docker credential helper by running the following command. Other options are also available.

   Generate Docker Login for GCR (Linux)

   ```
   gcloud auth configure-docker
   ```

2. Invoke Synopsys Detect, by providing at least the following:

   Synopsys Detect - Scanning Images

   ```
   bash <(curl -s https://detect.synopsys.com/detect.sh) \
   --blackduck.url=<URL> \
   --blackduck.api.token=<token> \
   --detect.docker.image=<Image URI> \
   --detect.project.name=<Project Name>
   ```

Using the Synopsys Cloud Build Scanner

Another way to scan Docker Images in GCR is by Invoking Synopsys Detect from Google Cloud Build.

Scanning an image from GCR

To scan an existing image from GCR, first pull and save the image to TAR. Detect can then be invoked against the TAR.

Sample build specification YAML to scan an image in GCR

Scanning and attesting an image from GCR

Using Binary Authorization? The Synopsys Cloud Build Scanner can write Container Analysis Notes to Attestors.

This is the preferred workflow when using Detect to attest an image since the image must be present in GCR before an attestation can be created.

If performing an attestation, you'll add a few extra arguments to the Synopsys Cloud Build Scanner Step. Navigate to Attest an Image for Binary Authorization for information on setting up your attestor and keys.

Sample Build Specification YAML to Scan and Attest an Image in GCR

Scanning an Image as Quality Gate before pushing to GCR

To scan a freshly built image that's not yet present in GCR, save to TAR after you build the image and scan. This can be configured to stop the image being pushed to GCR if Detect fails.

Sample Build Specification YAML to Scan an Image before pushing to GCR