Container Security - Registry Scanning

Using Qualys Container Security you can scan public and private registries. Public registries are cloud accessible registries hosted on Amazon, Azure and Google. While, private registries are on-premise registries deployed on a private network such as those hosted using Artifactory or Nexus. Qualys supports scanning only authenticated registries.

Note: Currently you can only scan V2 type of registries with Qualys Container Security.

How do I scan registries?

From the Container Security app from your Qualys Cloud Platform, download the sensor image. Deploy the sensor as a registry sensor (with -r command) in the network where the sensor can communicate with the registry and Qualys.

Create a new registry and set up a scanning schedule on the repository that you need the security posture of. You can perform an on-demand or a scheduled scan. As Scheduled scans are incremental, only the new images that are added to the configured repository since the last scan will be considered.

Refer to the Qualys Container Security User Guide for information on how to set up a registry scan.

How does registry scanning work?

Registry scanning is divided into two phases:
- Listing phase
- Scanning phase

Listing Phase

In the Listing phase, the Container Security sensor calls Docker Registry v2 APIs to collect all the image metadata information for the repository provided in the registry scan schedule.
Qualys sensor makes catalog, tag, manifest and config API calls to collect information and this information is displayed on the UI. Based on the filters defined in the schedule by the user (e.g., scan images created in last 14 days), the images are queued for scanning.

Note - For public registries (cloud accessible), Qualys makes the Docker Registry API calls and fetches information to feed the sensors for performing an image scan. In case of private registries, as Qualys cannot connect to them, the sensor performs both listing and scanning actions and sends information to Qualys.

Scanning Phase

Sensors which are provisioned as registry sensors, poll Qualys periodically to see if any images are queued for scanning. Qualys assigns only a subset of discovered images to the sensor for scanning. The response payload includes image details along with authentication credentials required to pull image from the registry.

Copyright 2019 by Qualys, Inc. All Rights Reserved.

Qualys Registry Sensor pulls these images from the registry and gathers and pushes the information (snapshot) to Qualys Cloud. Qualys then runs signatures on the collected information and generates a vulnerability report which can be viewed on the Container Security UI.

If the repository has a lot of images to scan, the overall scanning time might be longer than usual. You can install multiple registry sensors to distribute the scanning payload to reduce the scan time and view the results faster.

Last updated: January 16, 2019