Container Security

Release Notes for Sensor

Version 1.9.0
August 12, 2021

Here’s what’s new in the Container Security Sensor!

Policy Compliance Now Supported for Registry Sensors

When Policy Compliance (PC) scanning was first introduced in Container Security, it was supported only for General and CI/CD mode. Now Registry mode is also supported. This means that the PC manifest will be assigned to registry sensors, and compliance scanning will be performed along with vulnerability scanning on your registry images. Note that the Policy Compliance Scanning feature was enabled for all customers starting in the last Container Security release.

Prerequisites

- Update your sensors to version 1.9 or later
- Launch new registry scans to start collecting compliance data

How it works

The Qualys container sensor runs an additional scan of configurations in images and uploads additional scan metadata to the Qualys backend. Based on the scan metadata, the backend performs an assessment against various industry standard benchmarks and controls for compliance assessment. The compliance scans of images will be transparent to customers and will function in a similar real-time cloud native manner like the existing vulnerability scanning feature.

Sensor Now Supported in Kubernetes (Docker Runtime) with TKGI

The Container Security Sensor is now supported in a Kubernetes environment with TKGI (Tanzu Kubernetes Grid Integrated) and Docker Runtime. The steps are the same as other deployments in Kubernetes with Docker Runtime, except for one change specific to the TKGI setup. In TKGI, docker.sock is not available at the /var/run location. You must locate docker.sock on your worker nodes and change the socket-volume mapping in the cssensor-ds.yml file.

For example, if docker.sock is found at /var/vcap/data/sys/run/docker/docker.sock, then you would change the socket-volume mapping under volumes like this:

```
volumes:
  - name: socket-volume
    hostPath:
      path: /var/vcap/data/sys/run/docker
      type: Directory
```

Please refer to the Sensor Deployment Guide for deployment instructions.

CBL-Mariner Linux Now Supported

The Qualys Container Security Sensor is now supported for CBL-Mariner Linux. The sensor can now scan docker images and containers based on the CBL-Mariner Linux Operating System. This is supported for static and dynamic scanning. The Container Security backend will be able to evaluate the scan data for CBL-Mariner and report on vulnerabilities.

Mask Environment Variables for Images and Containers

This sensor release introduces a new option called --mask-env-variable that when used will mask/remove environment variables for images and containers. The environment variables will be masked/removed in sensor logs and in the Container Security UI.

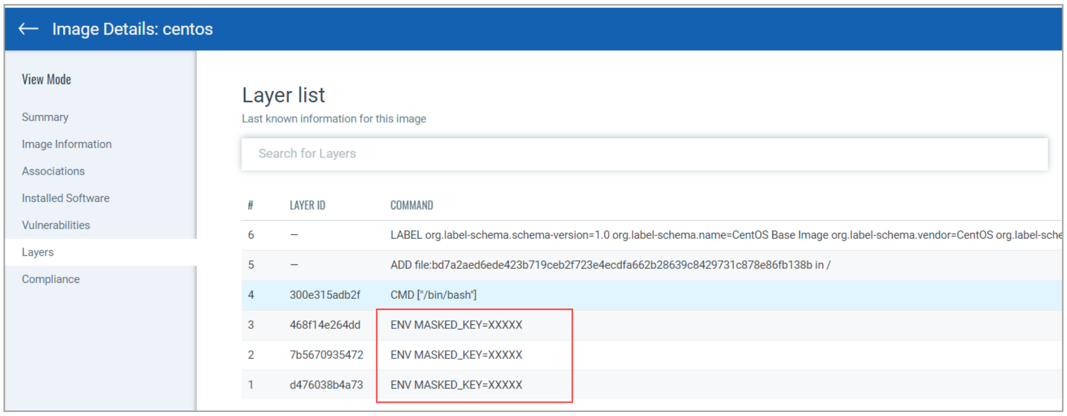
Use --mask-env-variable as a command line parameter for “installsensor.sh” script or provide it as a command or args parameter when deploying a sensor. Here’s a sample args value with the new option specified:

args: ["--k8s-mode", "--mask-env-variable"]

In the Container Security UI you’ll see that environment variable values are either masked or removed when this new option is used.

Image Details

In Image Details, under Layers, you’ll see a masked value “ENV MASKED_KEY=XXXXX” for environment variable names and values. See the sample below.



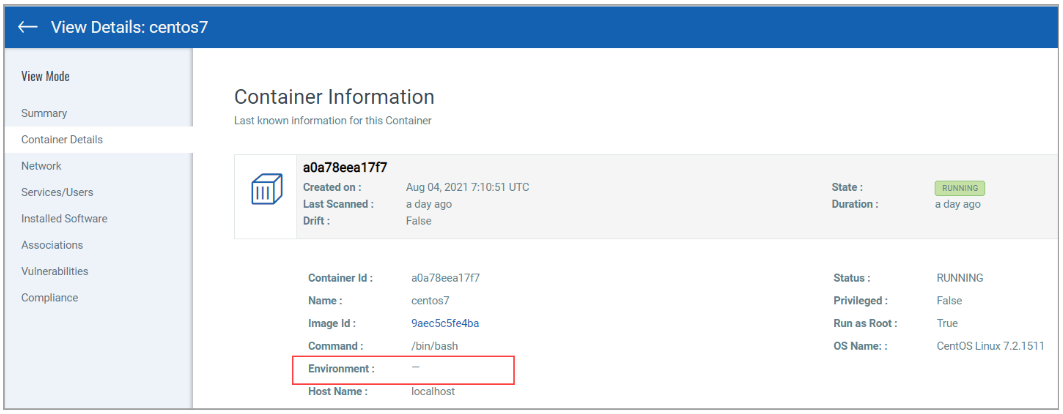
Layer list

Last known information for this image

#	LAYER ID	COMMAND
6	–	LABEL org.label-schema.schema-version=1.0 org.label-schema.name=CentOS Base Image org.label-schema.vendor=CentOS org.label-sche
5	–	ADD file:bd7a2aed6ede423b719ceb2f723e4ecdfa662b28639c8429731c878e86fb138b in /
4	300e315adb2f	CMD ["/bin/bash"]
3	468f14e264dd	ENV MASKED_KEY=XXXXX
2	7b5670935472	ENV MASKED_KEY=XXXXX
1	d476038b4a73	ENV MASKED_KEY=XXXXX

Container Details

In Container Details, you’ll see a single dash next to Environment when environment variables have been masked/removed. See the sample below.



Container Information

Last known information for this Container

a0a78eea17f7

Created on :	Aug 04, 2021 7:10:51 UTC	**State :**	RUNNING
Last Scanned :	a day ago	**Duration :**	a day ago
Drift :	False		

Container Id :	a0a78eea17f7	**Status :**	RUNNING
Name :	centos7	**Privileged :**	False
Image Id :	9aec5c5fe4ba	**Run as Root :**	True
Command :	/bin/bash	**OS Name: :**	CentOS Linux 7.2.1511
Environment :	–		
Host Name :	localhost		

Sensor Can Detect New Oracle Java QIDs

Recently released Oracle Java QIDs can now be detected by the Qualys Container Security sensor. The sensor can detect the presence of vulnerable Java packages on your docker images and containers.

Learn more about the QID detections: QID Spotlight: Enhanced Oracle Java Discovery

Issues Addressed

- We have stopped the processing of noisy events generated by Containerd Runtime. There were a lot of events getting generated and the sensor was continuously processing these events.
- We fixed an issue where a single container was being picked up for scanning continuously. Each time a new manifest is downloaded we scan the eligible asset (image or container). An unexpected container scan failure on manifest refresh (after a successful scan) resulted in the wrong manifest association for the container.