Qualys Container Security

Release Notes for Sensor

Version 1.28
August 14, 2023

What's New?

Malware Detection Powered by Qualys Deep Learning AI

With this release, Qualys Container Security introduces malware detection, powered by Qualys Deep Learning AI, providing you with an effective way to protect against malware threats. You can now scan your container images for any potential malware files and ensure that no malicious container images are deployed into the production environment.

Some of its key benefits include:

- **Early Detection:** It detects malware threats at the early stage in the container lifecycle and ensures the integrity of container images is maintained in the registry.
- **High Accuracy:** It detects malwares with high precision, even when the malware is new or unknown.

To perform a malware scan for your images, you need to install the registry sensor with the following parameter:

Argument	Examples
--perform-malware-detection	• **Using docker run:** `docker run -d --restart on-failure --cpus=0.2 -v /var/run/docker.sock:/var/run/docker.sock:ro -v <client cert directory on the docker host>:/root/.docker -v /usr/local/qualys/sensor/data:/usr/local/qualys/qpa/data -e ACTIVATIONID=<Activation id> -e CUSTOMERID=<Customer id> -e POD_URL=<PODURL> -e DOCKER_TLS_VERIFY=1 -e DOCKER_HOST=<IPv4 or FQDN>:<port#> --net=host --name qualys-container-sensor qualys/qcs-sensor:latest --log-level 5 --registry-sensor` **`--perform-malware-detection`** • **Using installsensor.sh:** `sudo ./installsensor.sh ActivationId=<Activation id> CustomerId=<Customer id> Storage=/usr/local/qualys/sensor/data -s -r` **`--perform-malware-detection`** • **Using yaml file:** Add the "--perform-malware-detection" parameter to args:

Copyright 2023 by Qualys, Inc. All Rights Reserved.

	`args: ["--k8s-mode", "--registry-sensor", "--perform-malware-detection"]`

Notes:

- Malware scanning is supported only on:
  - **Sensors**: Registry sensor (x86_64 architecture only)
  - **OS**: Linux
  - **Runtimes**: Docker, containerd, and CRI-O.
- In case of existing sensors, you need to reinstall the sensor with the `--perform-malware-detection` argument.
- The `--sca-scan-timeout-in-seconds` or `SCAScanTimeoutInSeconds` argument is now used for setting a timeout for malware detection along with SCA and secret detection.
- For efficient malware scanning, it is recommended to allocate 1 CPU core for the sensor. For instance:
  - When using the InstallSensor.sh script, by default 20% of the host's CPUs are utilized by the sensor container. If the host has 8 CPU cores, the total CPU limit applied to the sensor container would be 0.2 * 8 = 1.6 CPU cores.
  - When using dockerrun, by default all CPUs of the host are fully utilized for the sensor container.
  - In Kubernetes, to allocate 1 CPU core for the sensor container, regardless of the number of cores available on the host system, set the CPU limit value to 1.

    Example:

    ```
    resources:
        limits:
            cpu: "1"
    ```

For more information, see Sensor Deployment Guide.

Issue Addressed

The following issue has been fixed with this release:

Registry scans failed because the registry sensor could not log in to a registry due to the presence of special characters in the login password.