Container Security

Release Notes for Sensor

Version 1.3.2

March 12, 2020

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

Launch sensor without persistent storage

You can now run the sensor without using persistent storage on host. In this case data is not stored on host but stored at the /usr/local/qualys/qpa/data folder relative to the Sensor.

To facilitate this, two new install parameters are introduced:

- **--sensor-without-persistent-storage** : Run the sensor without using persistent storage on host.

- **--read-only** : Run sensor in read-only mode. In this mode the sensor uses persistent storage on host.

The sensor should be run either with "--sensor-without-persistent-storage" option or with "--read-only" option, and not with both options enabled together.

If you want to install the Sensor without persistent storage, exclude the "Storage" option, and include the "--sensor-without-persistent-storage" option in the installer script. It is recommended to use the "--enable-console-logs" option along with "--sensor-without-persistent-storage" to preserve the logs.

Note: When the sensor is run without persistent storage, a considerable increment is observed in CPU utilization, Disk I/O and scan duration.

If you want to use persistent storage and run the sensor in "--read-only" mode, ensure that there is enough disk space available on the Docker host to save and extract the container images.

Security enhancements for the Sensor

As an additional security measure we have added the "privileged=false" flag to Kubernetes deployment file to ensure there is no possibility of privilege escalation.