

Container Security v1.x

Release Notes for Sensor

Version 1.2.3

January 24, 2019

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

Support for OpenShift

You can now deploy the Container Sensor in OpenShift. For deploy instructions refer to the Appendix in the [Qualys Container Security User Guide](#).

Support for updating Sensor in Kubernetes

The Container Sensor package now comes with a script to perform a rolling update on Kubernetes nodes to update all existing Sensors to the latest version. For update instructions refer to the Appendix in the [Qualys Container Security User Guide](#).

LZMA compression for Sensor data uploaded to Qualys

The Sensor now runs LZMA compression on registry jobs status summary, events, and inventory data before uploading it to the Qualys Cloud. This reduces the network bandwidth required to transmit data to Qualys.

Auto update for build number change

Auto-update of the Container Sensor will now happen even for build number changes. For example the Sensor will now auto-update from version 1.2.3.xx1 to 1.2.3.xx2, and so on.

Restrict CPU usage on intermittent / scanning containers

Similar to restricting CPU usage for the Container Sensor on a Docker Host, you can now restrict CPU usage on intermittent / scanning containers spawned from the container image being scanned. Once you set the required CPU usage limit for the Sensor, the same CPU usage limit gets imposed on the intermittent / scanning containers spawned from the container image being scanned.

Customize the log file size to optimize disk usage

The qpa.log files are now compressed before being rotated in order to optimize disk usage. Contact Qualys Support to customize the log file size and number of files stored on rotation.