



Qualys Container Security

Release Notes for CRS Instrumentation

Version 2.2.2

June 17, 2021

Here's what's new in Container Runtime Security (CRS) Instrumentation 2.2.2!

[Additional Images Supported for CLI CRS Instrumentation](#)

[Non-root Google Distroless Image Instrumentation through CLI Mode](#)

Additional Images Supported for CLI CRS Instrumentation

Instrumentation is supported for container images with certain libc/glibc versions. With this release, we've added support for the versions listed below. This new support is available when instrumenting images using CLI mode.

Operating System: Alpine 3.12.1
libc/glibc version: musl-1.1.24-r9

Docker image version: ubuntu:18.04
libc/glibc version: glibc_2.27-3ubuntu1.4

Non-root Google Distroless Image Instrumentation through CLI Mode

Some users ran into issues with non-root Google distroless image instrumentation. To fix these issues, please note the following requirements when instrumenting a non-root Google distroless image and launching a container from it.

- The minimum Docker version required to instrument a non-root Google distroless image is v17.09.0-ce (or above).

- In order for the CRS instrumentation to work properly, only the user ID defined in the Docker file should be used to launch the instrumented container. Optionally, you can use a root user other than the user defined in the Docker file.