# Qualys Container Security

## Release Notes

Version 1.9
April 8, 2021

Here's what's new in Container Security 1.9!



Container Security 1.9 brings you more improvements and updates! Learn more

## Compliance Information Now Available in the UI

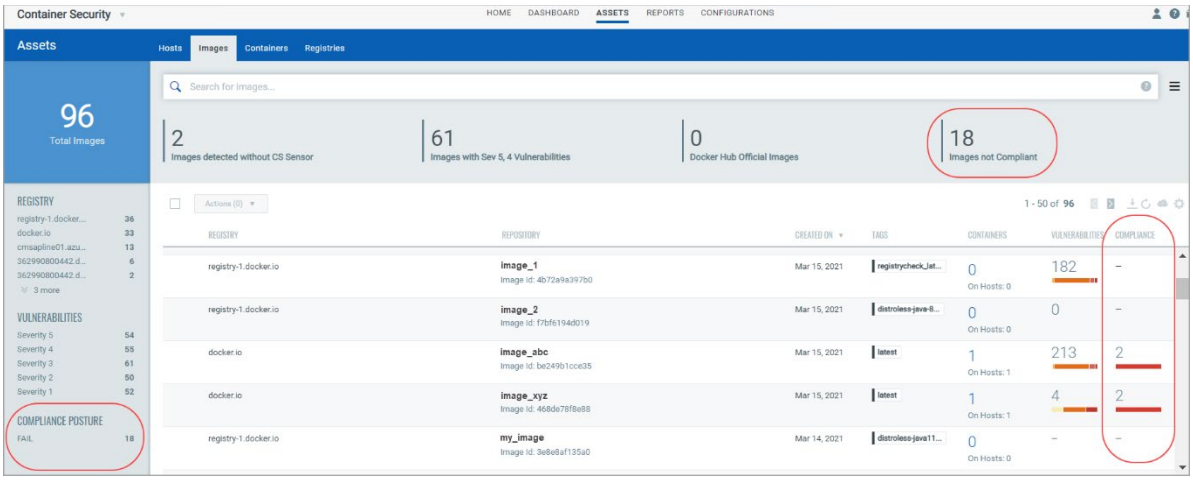
Applicable when the CS Policy Compliance scanning feature is enabled for your subscription.

In Container Security 1.8 we introduced Policy Compliance support. For the initial release, configuration assessment related information was provided via API endpoints only. Starting with Container Security 1.9, you can also view compliance information for your running containers and container images within the Container Security UI.

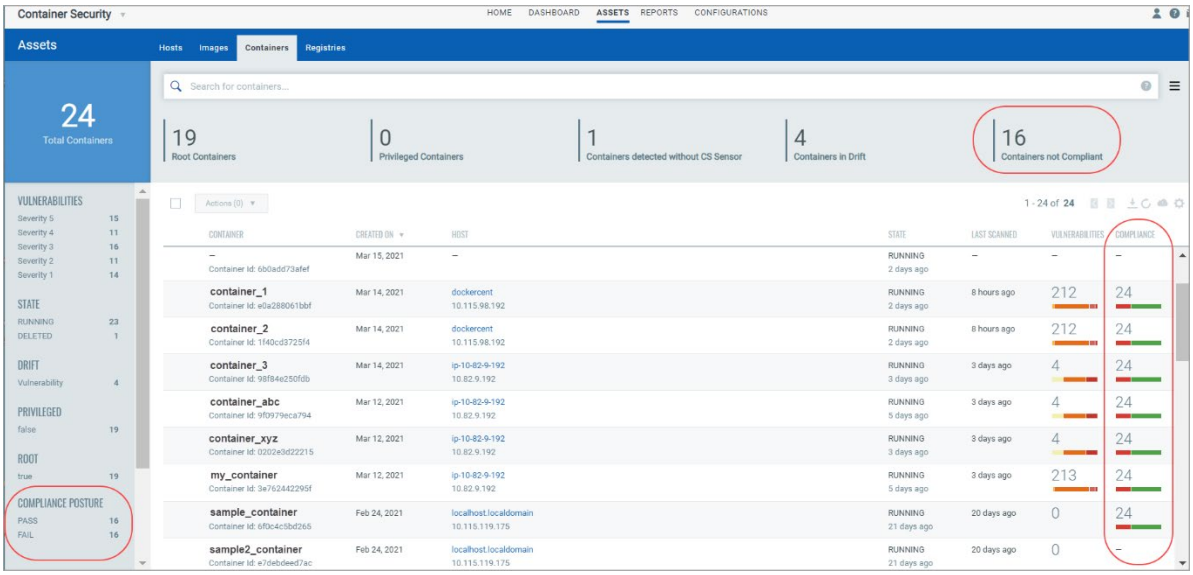
### View compliance information in the UI

On the **Images** list and **Containers** list, you'll see a new column called **Compliance** with the number of controls that have a posture of PASS and FAIL for running images/containers. Above the list you'll see the number of images/containers that are not compliant, meaning they have at least one Failed control. Use the quick filter on the left side to search images/containers by compliance posture (PASS, FAIL).

Here's a sample **Images** list:

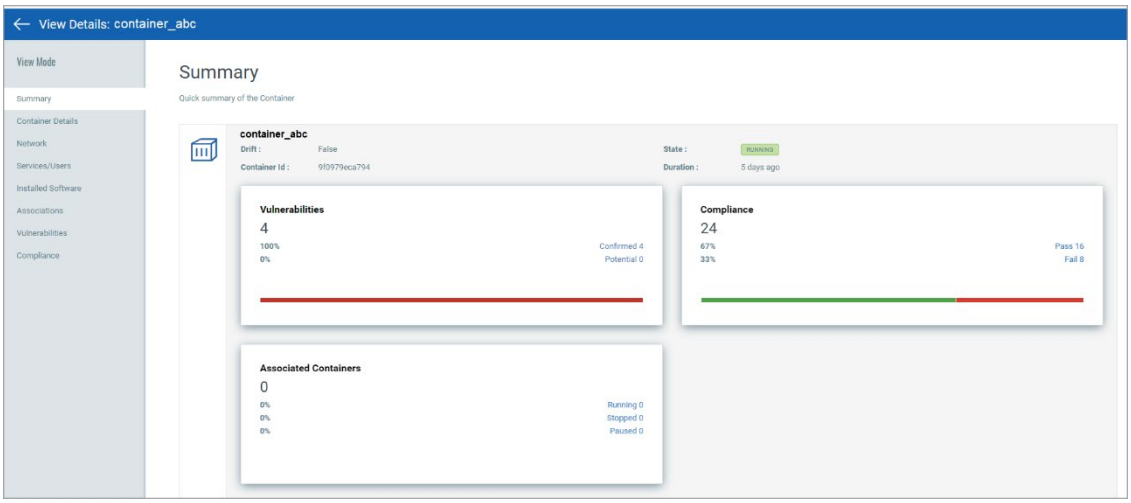



Here's a sample **Containers** list:

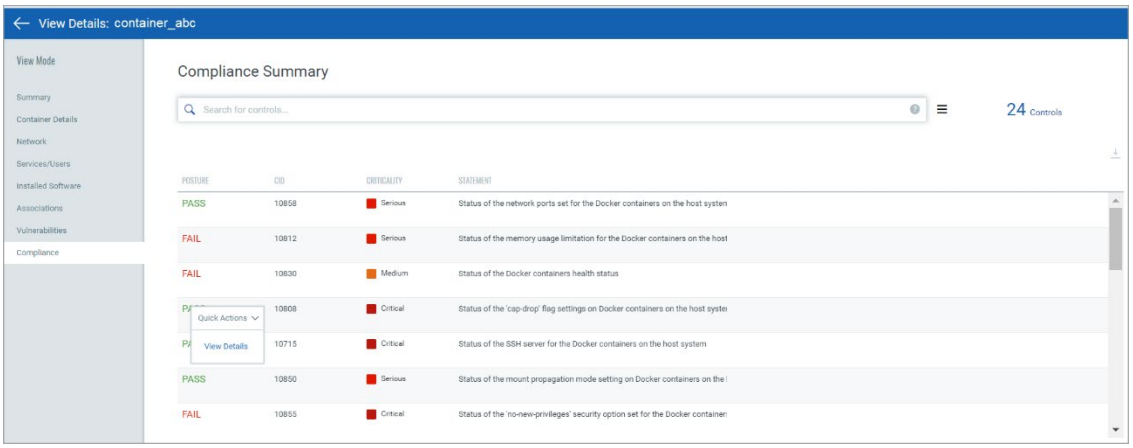


Drill down into the details for any image or container to see additional compliance information, including the list of controls that were evaluated and control details - Control ID (CID), criticality, statement, category and technologies.

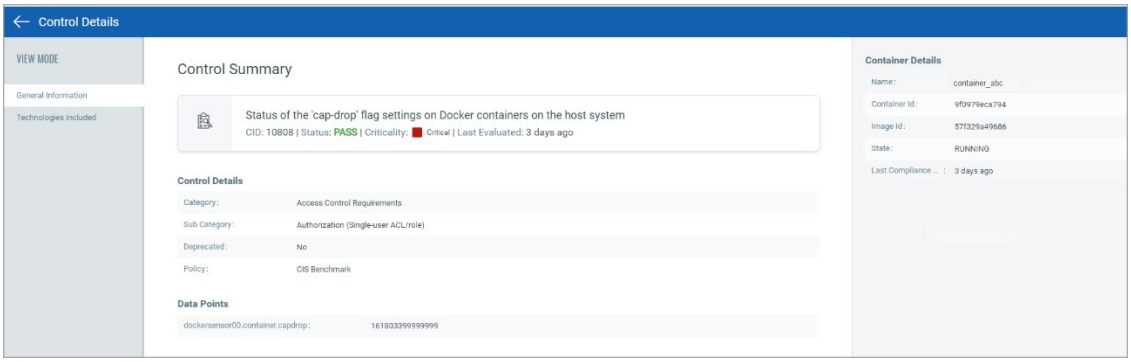
On the **Summary** tab in the image/container details, you'll see a new section for **Compliance** with the number and percentage of controls that have a status of Pass and Fail.




On the **Compliance** tab in the image/container details, you'll see the list of controls that were evaluated with the posture status, CID, criticality and statement.

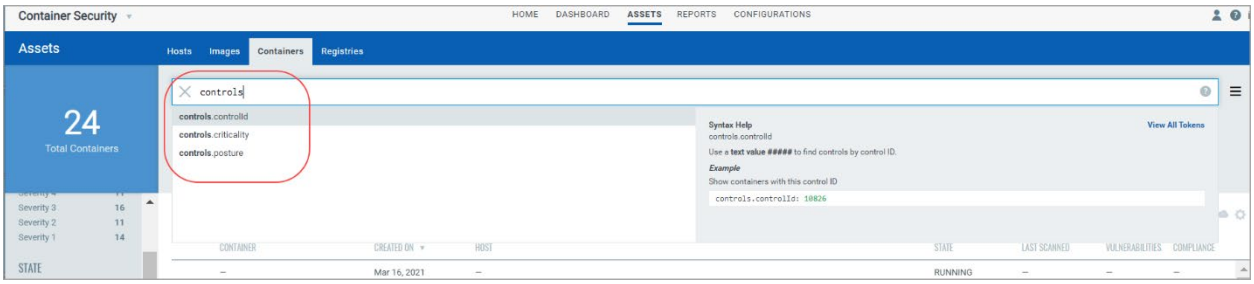



Click **View Details** for any control to get more details like the category, policy and technologies.



### New search tokens for controls

We added new tokens that allow you to easily find images/containers by control ID, control criticality (MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT) and control posture (PASS, FAIL). These tokens are available on the **Images** tab and the **Containers** tab.



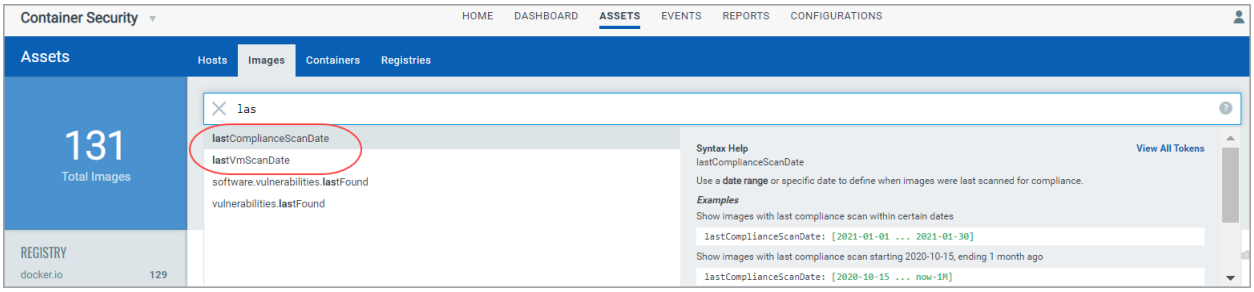

As mentioned earlier, compliance information can also be fetched using Compliance APIs. You can fetch compliance posture for an image or container, fetch control details, or fetch a list of controls. See the Compliance section of the Container Security API Guide for more information.

## Last Scan Date Token Changes

Please note the following search token changes when searching images or containers:

- We renamed lastScanned to lastVmScanDate. Use this token to search for images/containers based on when they were last scanned for vulnerabilities.

- We added lastComplianceScanDate. Use this token to search for images/containers based on when they were last scanned for compliance.

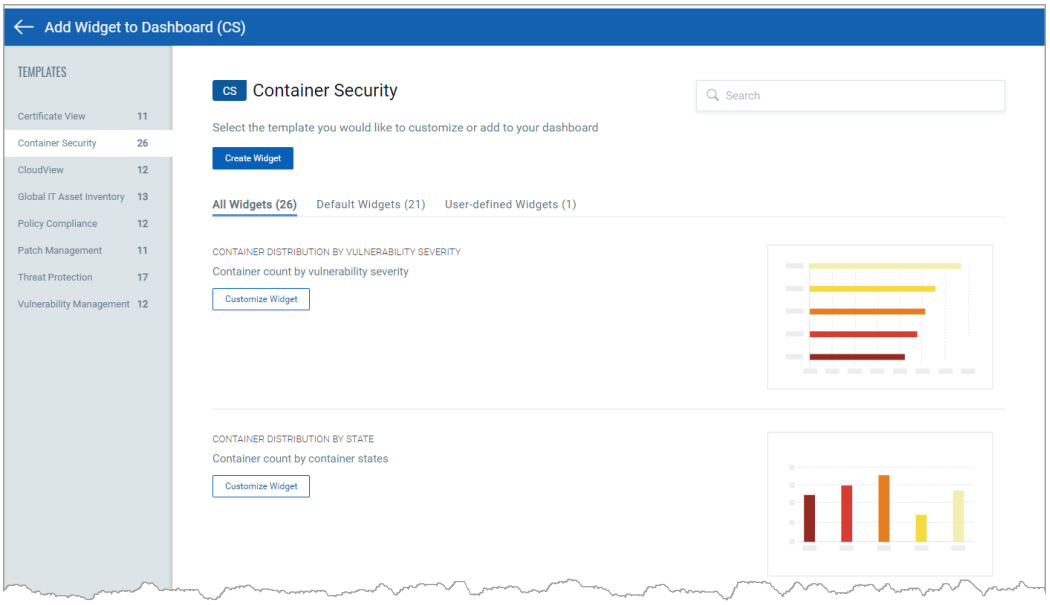



## Unified Dashboard (UD) Support for Container Security

Dashboards help you visualize your container environment assets, see your threat exposure, leverage saved searches, and fix priority of vulnerabilities quickly.

We have integrated Unified Dashboard (UD) with Container Security. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use the default Container Security dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your view. For help creating widgets, dashboards, templates and more, please refer to the Unified Dashboard online help.




## New Software Group By Options for Dashboard Widgets

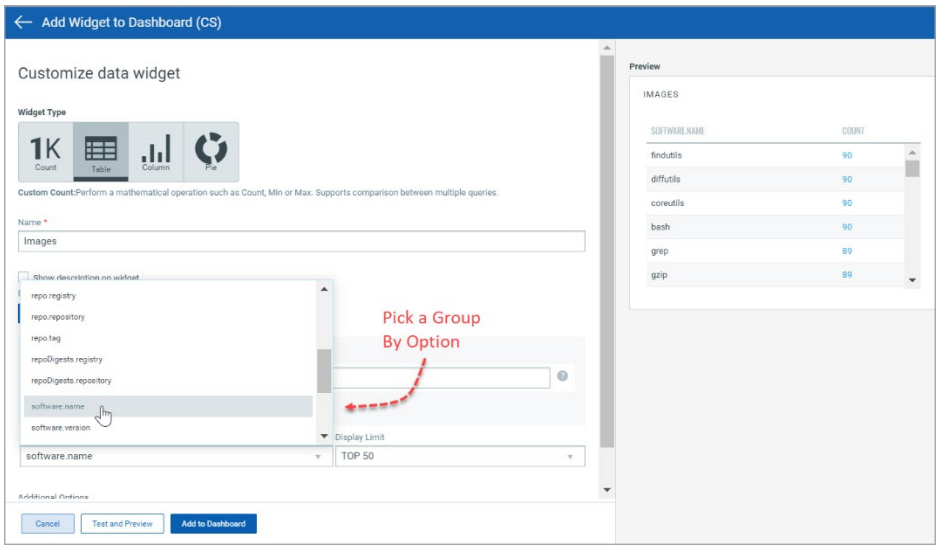
When creating a widget for your Container Security dashboard, you'll see new Group By options for software name and version. Use Group By options for widget types Table, Column and Pie.

When you display results by Image, you'll see these new Group By options (as shown in the example):

- software.name
- software.version

When you display results by Container, you'll see these new Group By options:

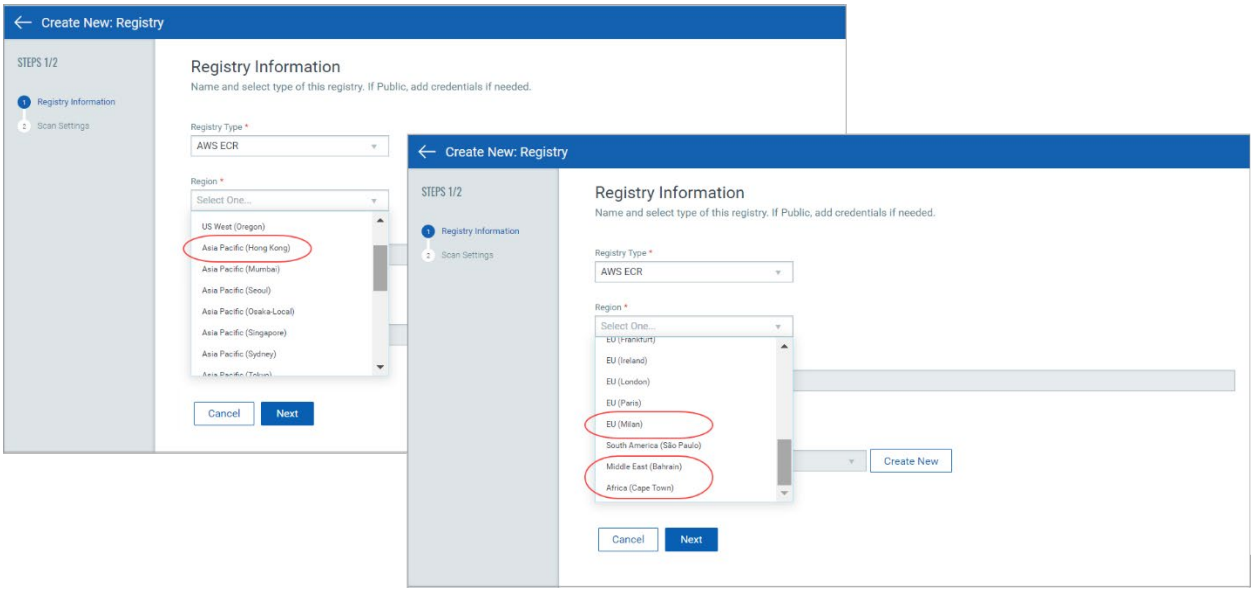
- drift.software.name
- drift.software.version



## More AWS EC2 Regions Supported

We added support for the following AWS regions:
- Asia Pacific (Hong Kong)
- EU (Milan)
- Middle East (Bahrain)
- Africa (Cape Town)

You'll see newly supported regions when creating an AWS EC2 registry. To do this, go to **Assets** > **Registries**, and click **New Registry**. Pick registry type: AWS EC2, and then pick the region you're interested in from the **Region** menu. Scroll through the list to see all supported regions.




## CRS Instrumentation Updates

These changes apply when your subscription has Container Runtime Security (CRS) enabled. To learn more, please refer to the Container Runtime Security User Guide.

We've expanded our support for CRS instrumentation in this release, as described below. This new support is available whether you're instrumenting images using CLI mode or using the Instrumenter service.

### Additional Images Supported for CRS Instrumentation

Instrumentation is supported for container images with certain libc/glibc versions. With this release, we've added support for the following libc/glibc versions:

Operating System: Centos 7
libc/glibc version: glibc-2.17-323.el7_9.x86_64

Operating System: Alpine 3.9
libc/glibc version: musl-1.1.20-r5.apk

Operating System: Alpine 3.11
libc/glibc version: musl-1.1.24-r3 x86_64

### CRS Instrumentation Supported for Non-Root Based Images

Now you can instrument container images that do not run as root and have limited access to resources. How does it work? User 0 is used to perform instrumentation instead of User root.

### CRS Instrumentation Supported for Google Java Distroless Images

This new support allows CRS instrumentation of Google distroless images when the glibc package is installed at the standard path (not a custom path). All Debian based distroless images are supported like java, python.

## Issues Addressed

- Introduced a new error code (cms-1319) for public registry scan job failure. The error appears in the UI as: scan job status FINISHED with error “Docker pull failure. Docker Pull Rate Limit Reached”
- Fixed an issue where Policy > Rules > Application Rule page appeared blank when a rule action value had mixed case.
- Fixed an issue where the wrong Copyright year was shown on the Home page.
- We improved the error message that appears when you create a policy with the same name as another policy.
- We removed the text “Where are my Windows hosts?” which appeared on the Hosts tab and was overlapping with the host count.
- Fixed a discrepancy between the Image and Container counts on the Hosts tab and the count on the Images and Containers tabs.
- Fixed an issue where customer could not delete a registry and the error “Failed to delete registry as an associated schedule is currently running” appeared when there was a past On Demand scan job that had an error.
- Fixed an issue where customer was not able to instrument an image when the source was both host and registry.
- Fixed an issue where the Created and Updated dates for CRS policy rules showed a value of Jan 01, 0001.
- We fixed UI issues for customers using Internet Explorer 11.
- Made fixes to support Docker Hub 429 error code related to rate limiting.