Qualys Container Security v1.x

Release Notes

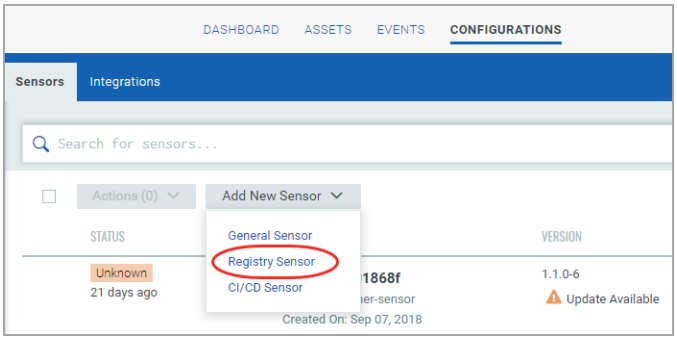
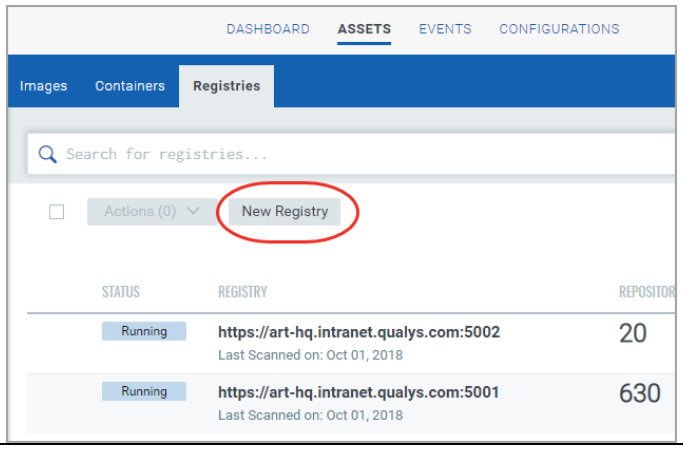
Version 1.4
October 31, 2018

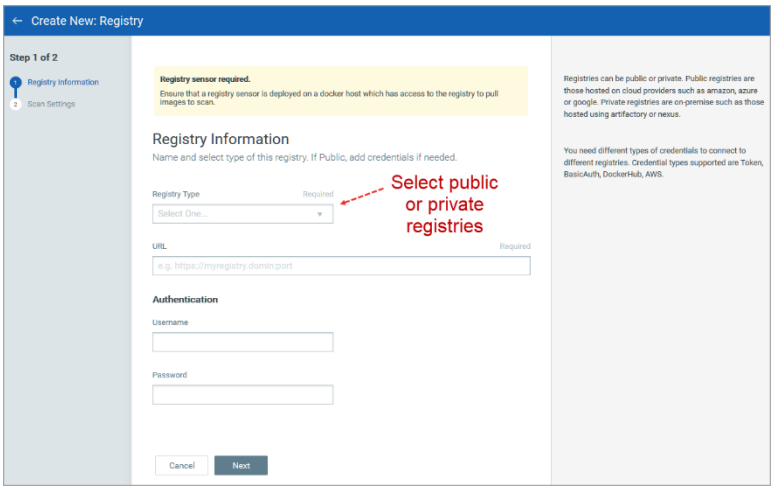
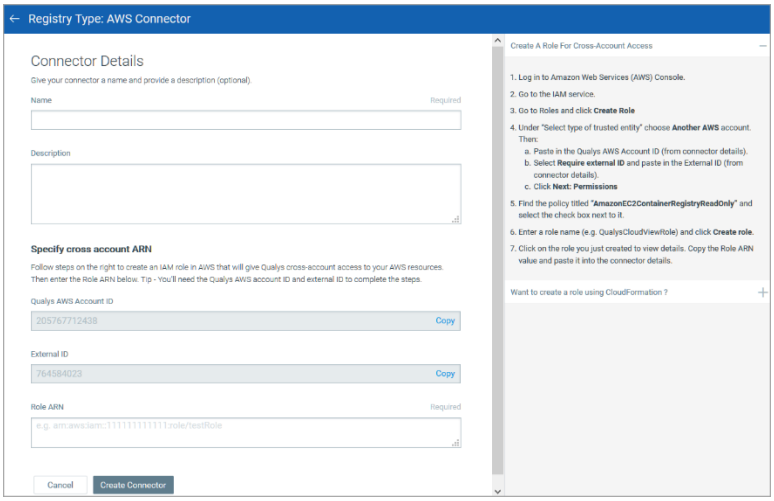
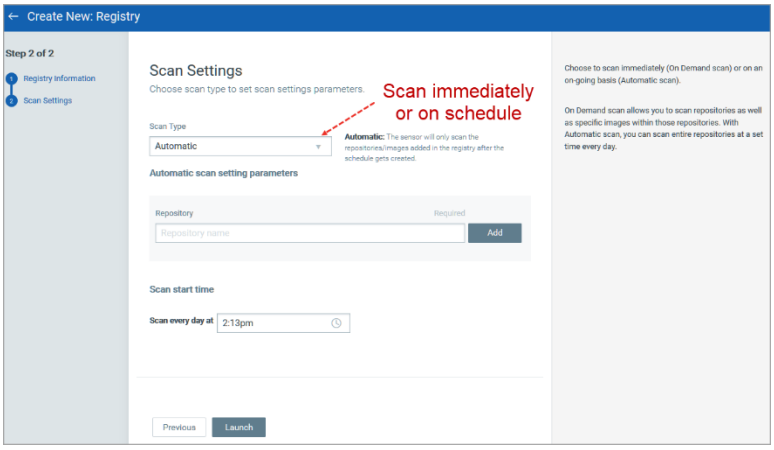
Here's what's new in Container Security 1.4!

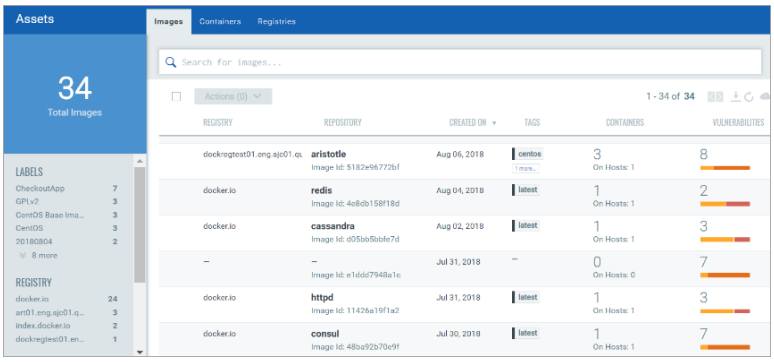
Scan registries for vulnerabilities

Container Security now supports scanning image registries for vulnerabilities. You can scan public and private registries for vulnerable images. Public registries are those hosted on cloud providers such as amazon, azure or google. Private registries are on-premise such as those hosted using artifactory or nexus.

As a prerequisite you must install the registry sensor on a docker host which has access to the registry to pull images to scan.	Docker host configuration
	
	Docker version - 1.12 or later.
	
	Disk space on docker host - Minimum 20 GB of free space on the partition where docker is installed. This is required to scan registry images. Additionally, 1 GB of free space is required for persistent storage.
	
	Connectivity - Docker host should have connectivity to the Registry to be scanned.
	
	To validate connectivity, perform a successful docker login from the host to the Registry.
	
	`docker login <registryurl> (No protocol)`
	
	For Example,
	
	`docker login myregistry.com:5001`

To download the sensor, simply go to Configurations > Sensors, click Add New Sensor and then select Registry Sensor. You need to append --registry-sensor or -r to the sensor install command to install the sensor for registry scan.	
You need to add a registry in order to scan it for vulnerabilities. Go to Assets > Registries, and click New Registry. Ensure that registry sensor deployed on the docker host is in running state.	

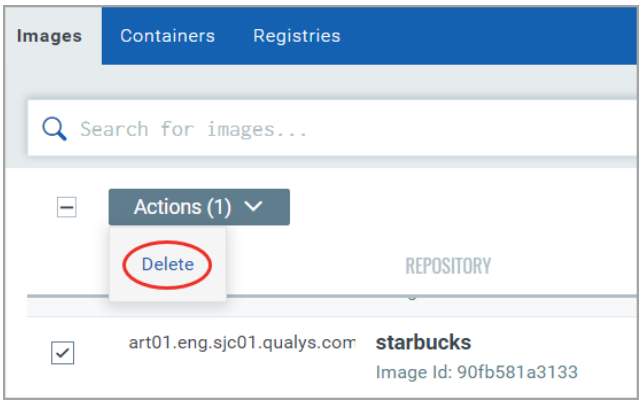
In order to perform vulnerability analysis you need to connect to the registries using credentials. You need different types of credentials to connect to different registries. Credential types supported are Token, BasicAuth, DockerHub, AWS.	
For AWS ECR, you can create a connector to connect to your AWS account.	
You can choose to scan immediately (On Demand scan) or on an ongoing basis (Automatic scan). On Demand scan allows you to scan repositories as well as specific images within those repositories. With Automatic scan, you can scan entire repositories at a set time every day.	

Once you connect to the registry, Container Security pulls the inventory data and performs vulnerability scans on repositories and images within the registries. Vulnerable images are listed on the Images tab. To get the total count of vulnerable images in a registry, go to Registries tab, and click View Details in the Quick Actions Menu of a registry.	

Delete sensors, images and containers

You can now delete Sensors, Images and Containers from your account.

To delete, simply select one or more Sensors, Images or Containers in the respective tabs, click Actions, and then click Delete.



You can only delete sensors with UNKNOWN status.

Images with active containers (CREATED, RUNNING, STOPPED, PAUSED) associated with them, cannot be deleted.

You can delete any container in any state.

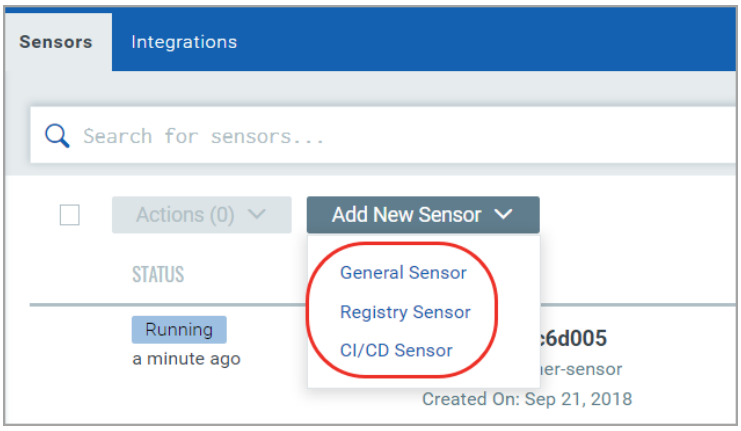
Limit sensor CPU usage

You can now limit the CPU consumption of a sensor by providing the following information in the sensor install script (installsensor.sh) during sensor installation. You can provide a value between 0 – 100 %.

For example, `CpuUsageLimit=30`

Use different sensor installers

Container Security Sensor download option now displays various sensor types.



General Sensor: Scan any host other than registry / build (CI/CD).

Registry Sensor: Scan images in a registry (public / private).

CI/CD Sensor: Scan images on CI/CD pipeline (Jenkins / Bamboo).

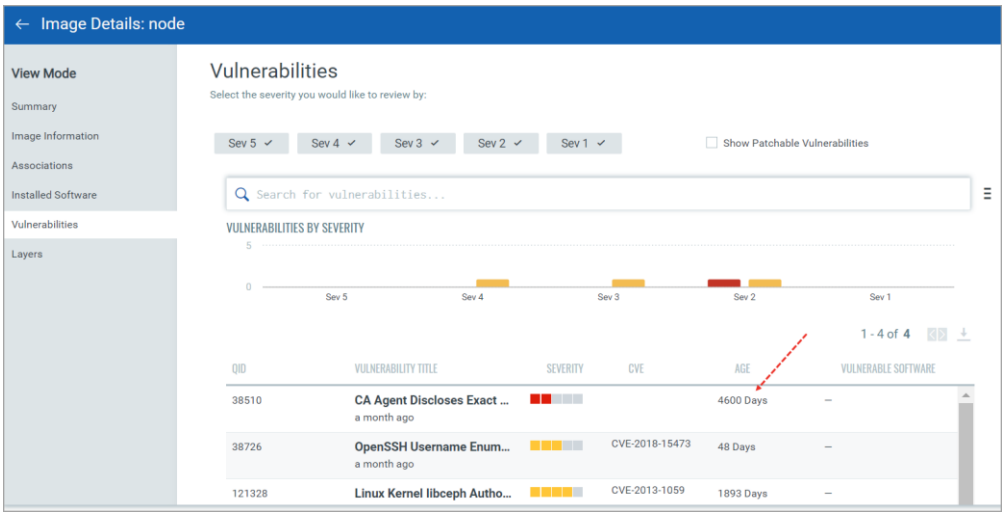
UI options are provided for convenience purpose. Basically all three options contain the same tar file. The difference is the additional commands you need to run for installing the sensor for Registry and CI/CD scanning.

For Registry you need to append the install command with --registry-sensor or -r

For CI/CD you need to append the install command with --cicd-deployed-sensor or -c

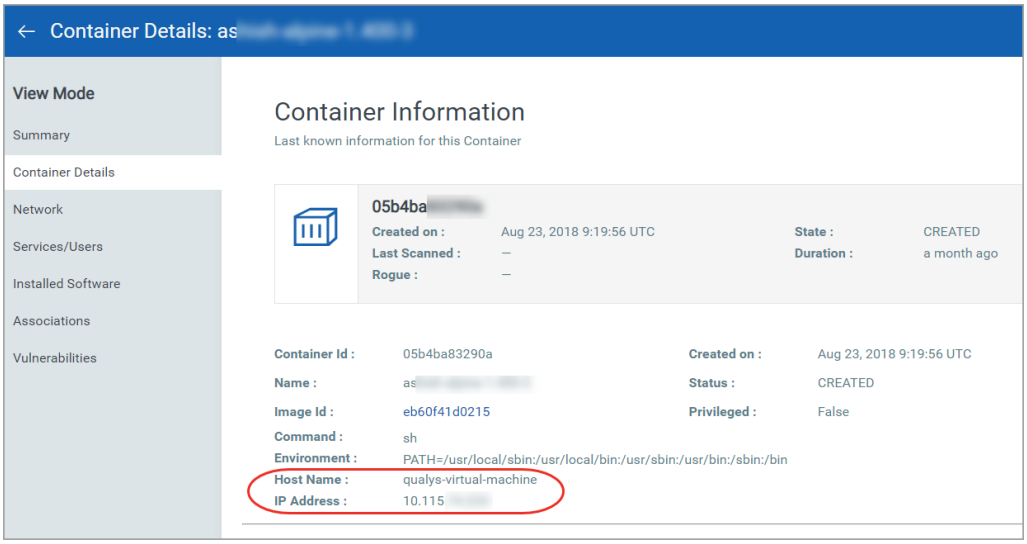
View vulnerability age

You can now view the age of a vulnerability in the image details / container details view. The age value is displayed in days. Age is calculated from the point Qualys published the vulnerability.



View container host information

Container details now display the host name and IP address of the host the container is installed on.



Use cases on home page

Want to scan images in build, registry or host? You can now quick get started from the Container Security home page. Expand a use case to get to the required steps quickly.