



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](#)

[Delete sensors, images and containers](#)

[Limit sensor CPU usage](#)

[Use different sensor installers](#)

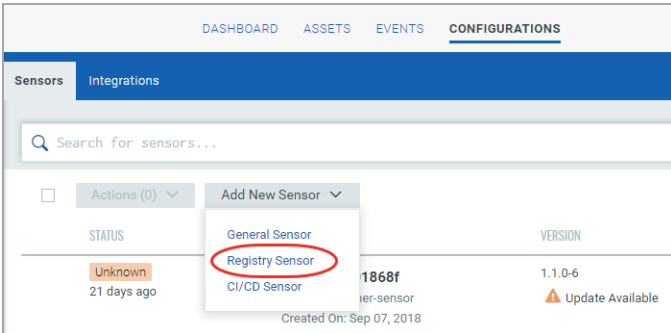
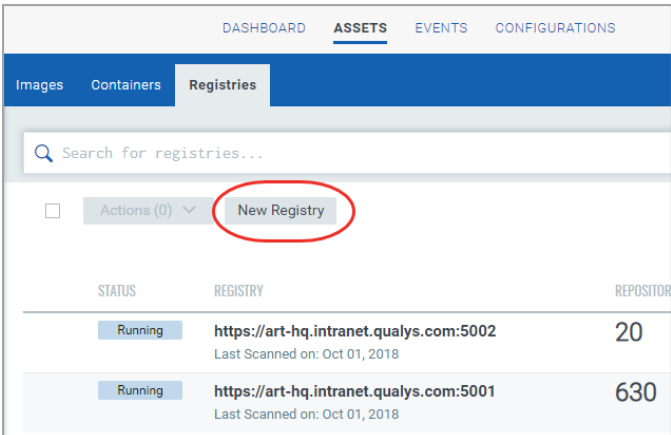
[View vulnerability age](#)

[View container host information](#)

[Use cases on home page](#)

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.

<p>As a prerequisite you must install the registry sensor on a docker host which has access to the registry to pull images to scan.</p>	<p>Docker host configuration</p> <p>Docker version - 1.12 or later.</p> <p>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.</p> <p>Connectivity - Docker host should have connectivity to the Registry to be scanned.</p> <p>To validate connectivity, perform a successful docker login from the host to the Registry.</p> <pre>docker login <registryurl> (No protocol)</pre> <p>For Example,</p> <pre>docker login myregistry.com:5001</pre>
<p>To download the sensor, simply go to Configurations > Sensors, click Add New Sensor and then select Registry Sensor.</p> <p>You need to append --registry-sensor or -r to the sensor install command to install the sensor for registry scan.</p>	
<p>You need to add a registry in order to scan it for vulnerabilities. Go to Assets > Registries, and click New Registry.</p> <p>Ensure that registry sensor deployed on the docker host is in running state.</p>	

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.

The screenshot shows the 'Create New Registry' interface at Step 1 of 2. The main section is 'Registry Information'. A yellow warning box at the top states: 'Registry sensor required. Ensure that a registry sensor is deployed on a docker host which has access to the registry to pull images to scan.' Below this, there are fields for 'Registry Type' (with a dropdown menu and a red arrow pointing to it labeled 'Select public or private registries'), 'URL' (with a placeholder 'e.g. https://myregistry.domain:port'), 'Username', and 'Password'. A 'Next' button is visible at the bottom right.

For AWS ECR, you can create a connector to connect to your AWS account.

The screenshot shows the 'Registry Type: AWS Connector' configuration page. It has two main sections: 'Connector Details' and 'Specify cross account ARN'. 'Connector Details' includes fields for 'Name' and 'Description'. 'Specify cross account ARN' includes fields for 'Qualys AWS Account ID', 'External ID', and 'Role ARN'. On the right side, there is a 'Create A Role For Cross-Account Access' section with a numbered list of steps: 1. Log in to Amazon Web Services (AWS) Console, 2. Go to the IAM service, 3. Go to Roles and click 'Create Role', 4. Under 'Select type of trusted entity' choose 'Another AWS account', 5. Find the policy titled 'AmazonEC2ContainerRegistryReadOnly' and select the check box next to it, 6. Enter a role name (e.g. QualysCloudViewRole) and click 'Create role', 7. Click on the role you just created to view details. Copy the Role ARN value and paste it into the connector details. There are 'Cancel' and 'Create Connector' buttons at the bottom.

You can choose to scan immediately (On Demand scan) or on an ongoing basis (Automatic scan).

The screenshot shows the 'Create New Registry' interface at Step 2 of 2, 'Scan Settings'. It asks to 'Choose scan type to set scan settings parameters.' The 'Scan Type' dropdown is set to 'Automatic', with a red arrow pointing to it labeled 'Scan immediately or on schedule'. Below this are 'Automatic scan setting parameters' including a 'Repository' field with an 'Add' button, and a 'Scan every day at' field set to '2:13pm'. A 'Launch' button is at the bottom right.

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.

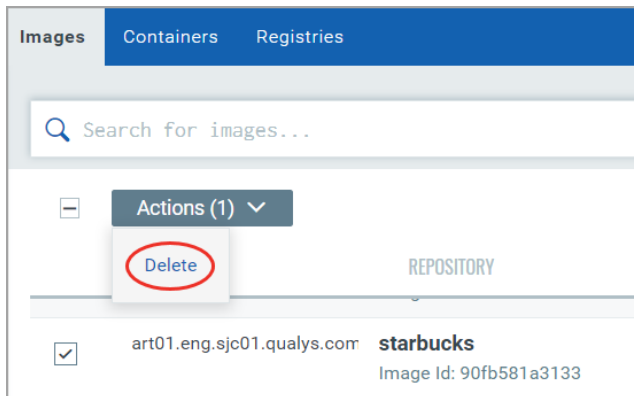
To get the total count of vulnerable images in a registry, go to Registries tab, and click View Details in the Quick Actions Menu of a registry.

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
dockregtest01.eng.sjc01.ql...	aristotle Image ID: 5182e96772bf	Aug 06, 2018	centos	3 On Hosts: 1	8
docker.io	redis Image ID: 4e8db158f18d	Aug 04, 2018	latest	1 On Hosts: 1	2
docker.io	cassandra Image ID: 605bb6b1fe7d	Aug 02, 2018	latest	1 On Hosts: 1	3
-	Image ID: e1dd67948a1c	Jul 31, 2018	-	0 On Hosts: 0	7
docker.io	httpld Image ID: 11426a19f1a2	Jul 31, 2018	latest	1 On Hosts: 1	3
docker.io	consul Image ID: 48ba92b70c9f	Jul 30, 2018	latest	1 On Hosts: 1	7

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.

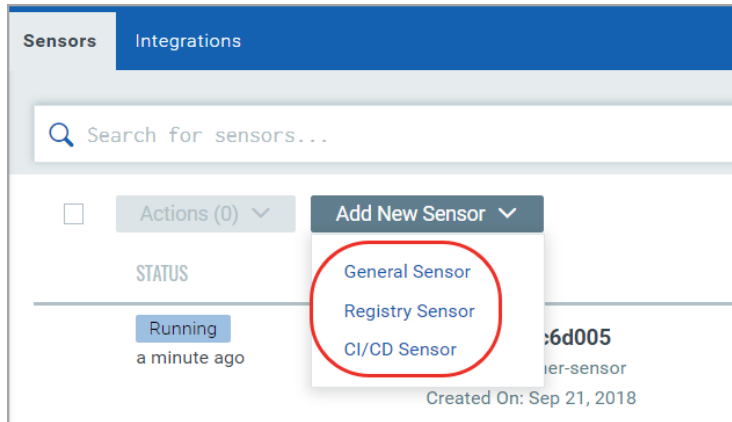
Limit sensor CPU usage

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).

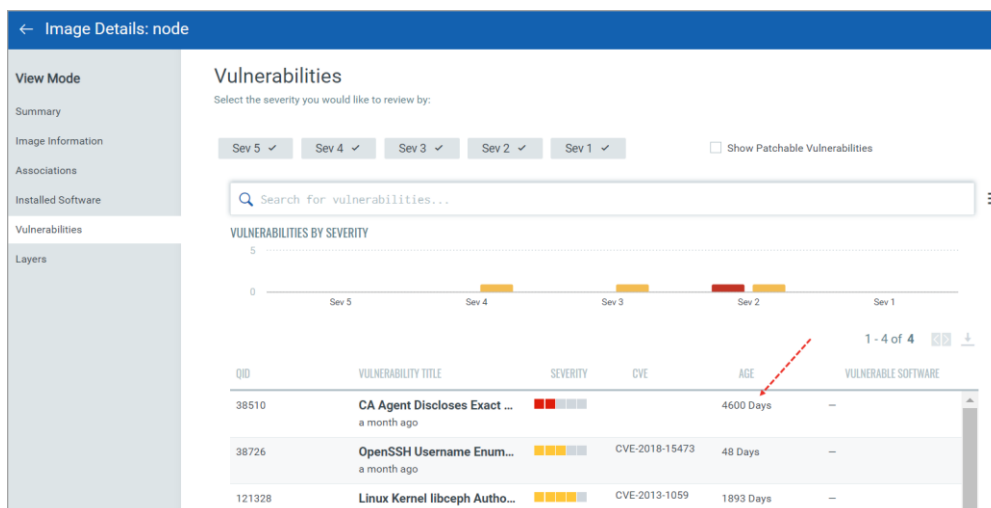
UI options are provided for convenience purpose. Basically all three options contain the same tar file. The difference is the additional commands you need to run for installing the sensor for Registry and CI/CD scanning.

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`

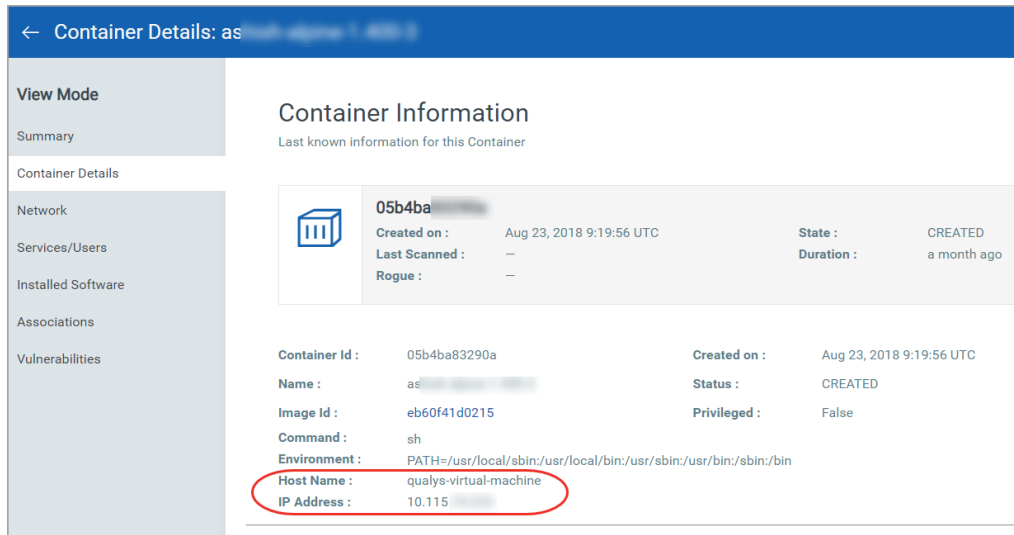
View vulnerability age

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.

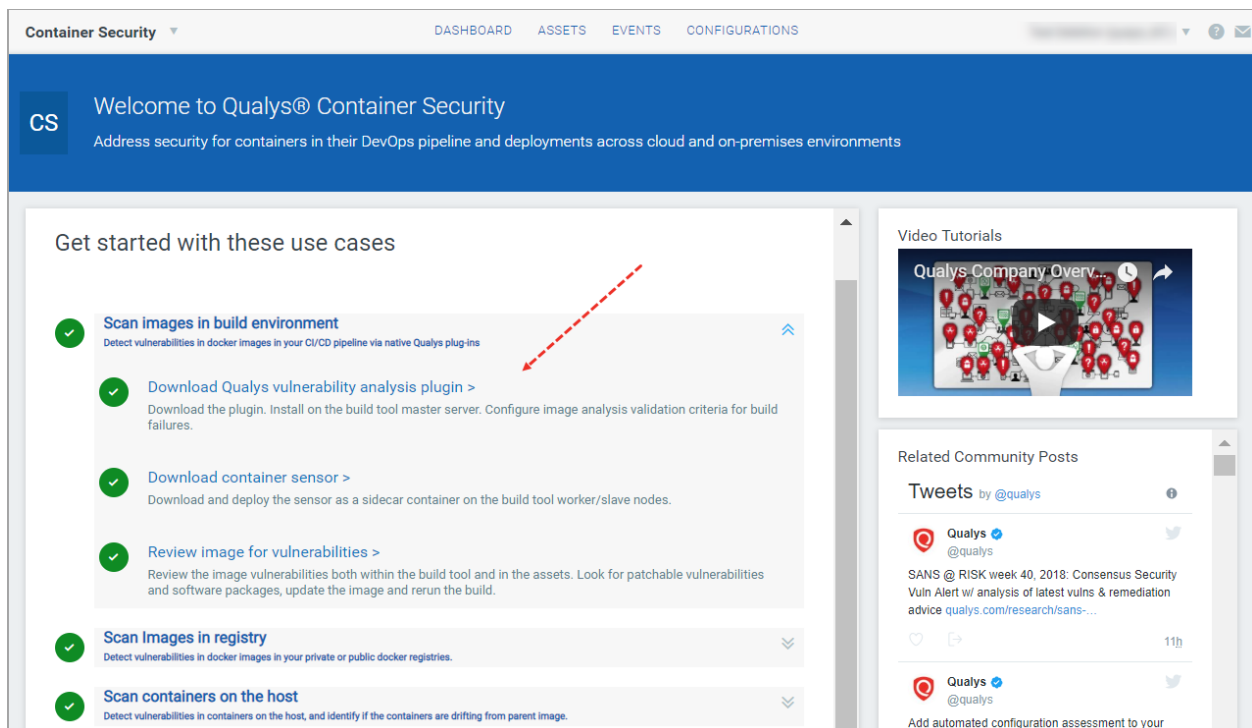


The screenshot shows the 'Container Details' page for a container named 'as'. The 'Host Name' and 'IP Address' are circled in red. The 'Host Name' is 'qualys-virtual-machine' and the 'IP Address' is '10.115...'. The 'Container Information' section shows the container was created on Aug 23, 2018 9:19:56 UTC and is in a 'CREATED' state. The 'Environment' section shows the path: 'PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin'.

Field	Value
Container Id	05b4ba83290a
Name	as
Image Id	eb60f41d0215
Command	sh
Environment	PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
Host Name	qualys-virtual-machine
IP Address	10.115...

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.



The screenshot shows the 'Container Security' home page. The 'Get started with these use cases' section is highlighted with a red dashed arrow. The use cases listed are:

- Scan images in build environment
- Download Qualys vulnerability analysis plugin >
- Download container sensor >
- Review image for vulnerabilities >
- Scan Images in registry
- Scan containers on the host

The 'Video Tutorials' section shows a video titled 'Qualys Company Overv...'. The 'Related Community Posts' section shows tweets from @qualys, including one about 'SANS @ RISK week 40, 2018: Consensus Security Vuln Alert w/ analysis of latest vulns & remediation advice'.