Qualys Container Security v1.x

Release Notes

Version 1.4

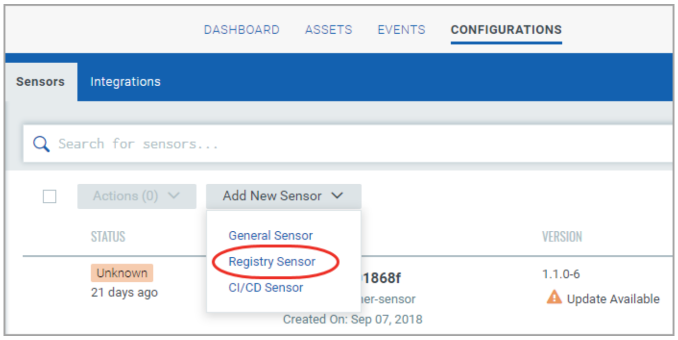
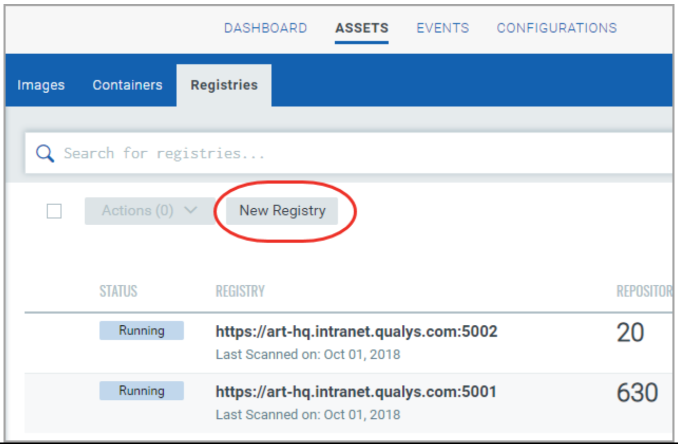
October 31, 2018

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

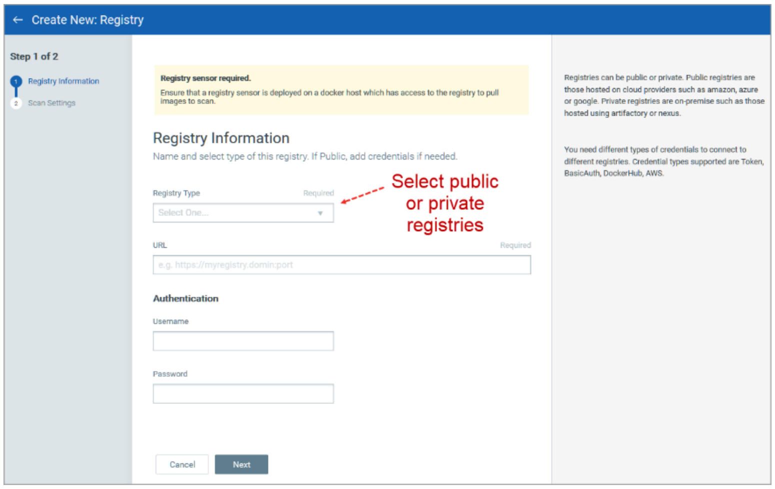
Scan registries for vulnerabilities

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.	 DASHBOARD ASSETS EVENTS CONFIGURATIONS Sensors Integrations Search for sensors... Actions (0) Add New Sensor General Sensor Registry Sensor CI/CD Sensor STATUS VERSION Unknown 21 days ago 1868f ier-sensor Created On: Sep 07, 2018 1.1.0-6 Update Available
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.	 DASHBOARD ASSETS EVENTS CONFIGURATIONS Images Containers Registries Search for registries... Actions (0) New Registry STATUS REGISTRY REPOSITOR Running https://art-hq.intranet.qualys.com:5002 Last Scanned on: Oct 01, 2018 20 Running https://art-hq.intranet.qualys.com:5001 Last Scanned on: Oct 01, 2018 630

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.



Create New: Registry

Step 1 of 2

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.

Registry Information

Name and select type of this registry. If Public, add credentials if needed.

Registry Type: Select One... (Required)

URL: e.g. https://myregistry.domin:port (Required)

Authentication

Username:

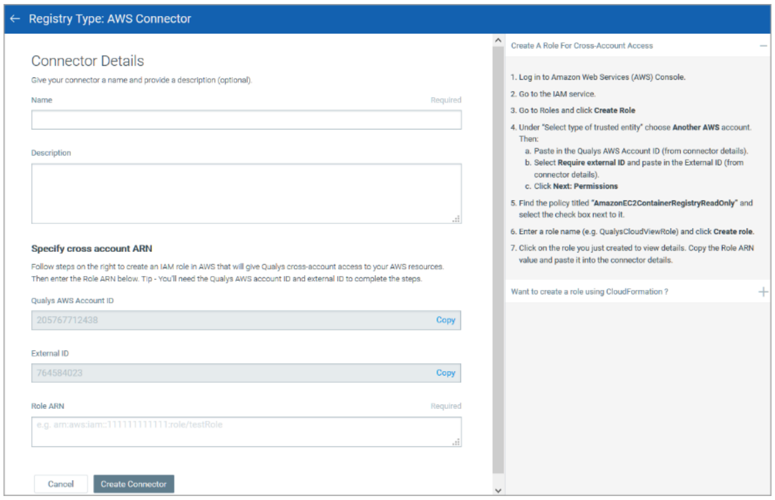
Password:

Select public or private registries

Registries can be public or private. 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.

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.



Registry Type: AWS Connector

Connector Details

Give your connector a name and provide a description (optional).

Name: (Required)

Description:

Specify cross account ARN

Follow steps on the right to create an IAM role in AWS that will give Qualys cross-account access to your AWS resources. Then enter the Role ARN below. Tip - You'll need the Qualys AWS account ID and external ID to complete the steps.

Qualys AWS Account ID: 205767712438

External ID: 764584023

Role ARN: e.g. arn:aws:iam::111111111111:role/testRole (Required)

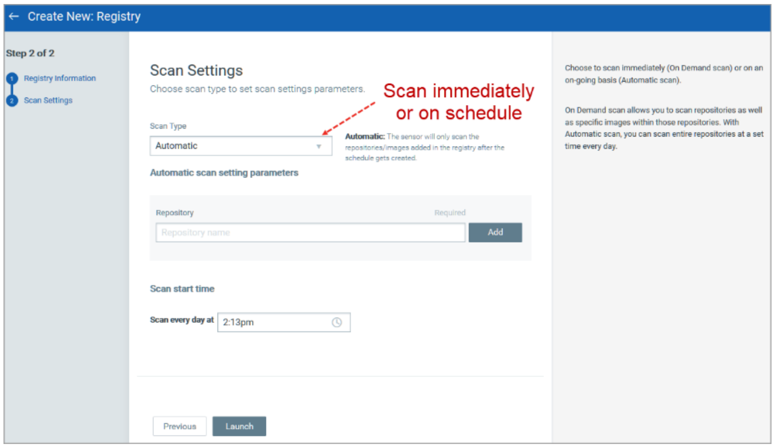
Create A Role For Cross-Account Access

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. Then:
   a. Paste in the Qualys AWS Account ID (from connector details).
   b. Select **Require external ID** and paste in the External ID (from connector details).
   c. Click **Next: Permissions**
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.

Want to create a role using CloudFormation ?

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.



Create New: Registry

Step 2 of 2

Scan Settings

Choose scan type to set scan settings parameters.

Scan Type: Automatic

Automatic: The sensor will only scan the repositories/images added in the registry after the schedule gets created.

Automatic scan setting parameters

Repository: Repository name (Required)

Scan start time

Scan every day at 2:13pm

Scan immediately or on schedule

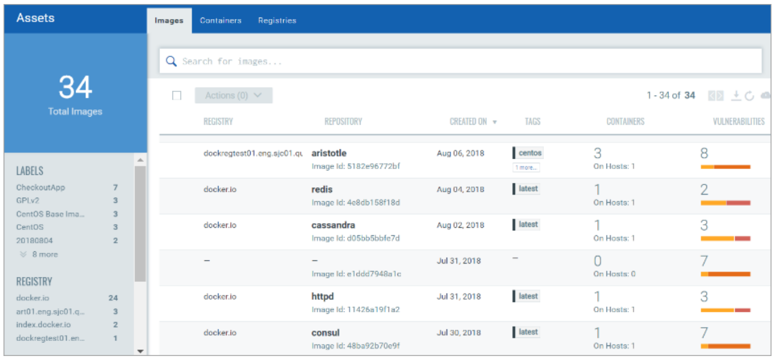
Choose to scan immediately (On Demand scan) or on an on-going basis (Automatic scan).

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.



34
Total Images

LABELS

CheckoutApp	7
GPLv2	3
CentOS Base Ima...	3
CentOS	3
20180804	2

8 more

REGISTRY

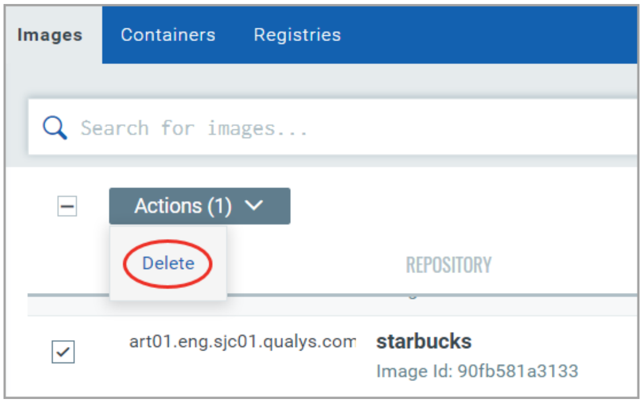
docker.io	24
art01.eng.sjc01.q...	3
index.docker.io	2
dockregtest01.en...	1

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
dockregtest01.eng.sjc01.qu	**aristotle** Image Id: 5182e96772bf	Aug 06, 2018	centos 1 more...	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: d05bb5bbfe7d	Aug 02, 2018	latest	1 On Hosts: 1	3
–	– Image Id: e1ddd7948a1c	Jul 31, 2018	–	0 On Hosts: 0	7
docker.io	**httpd** Image Id: 11426a19f1a2	Jul 31, 2018	latest	1 On Hosts: 1	3
docker.io	**consul** Image Id: 48ba92b70e9f	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.



☑ art01.eng.sjc01.qualys.com **starbucks**
Image Id: 90fb581a3133

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.

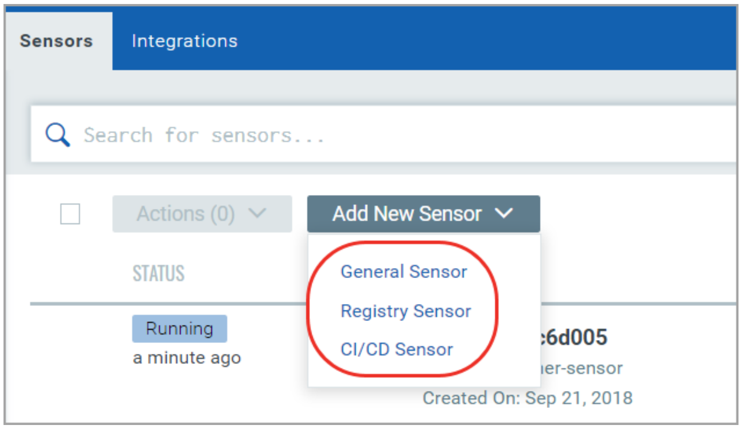
Limit sensor CPU usage

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).

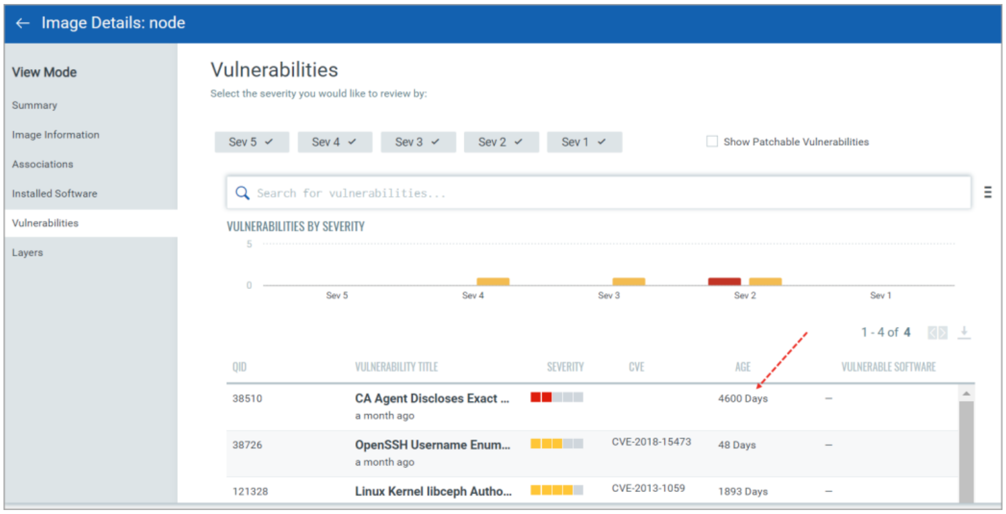
UI options are provided for convenience purpose. Basically all three options contain the same tar file. The difference is the additional commands you need to run for installing the sensor for Registry and CI/CD scanning.

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

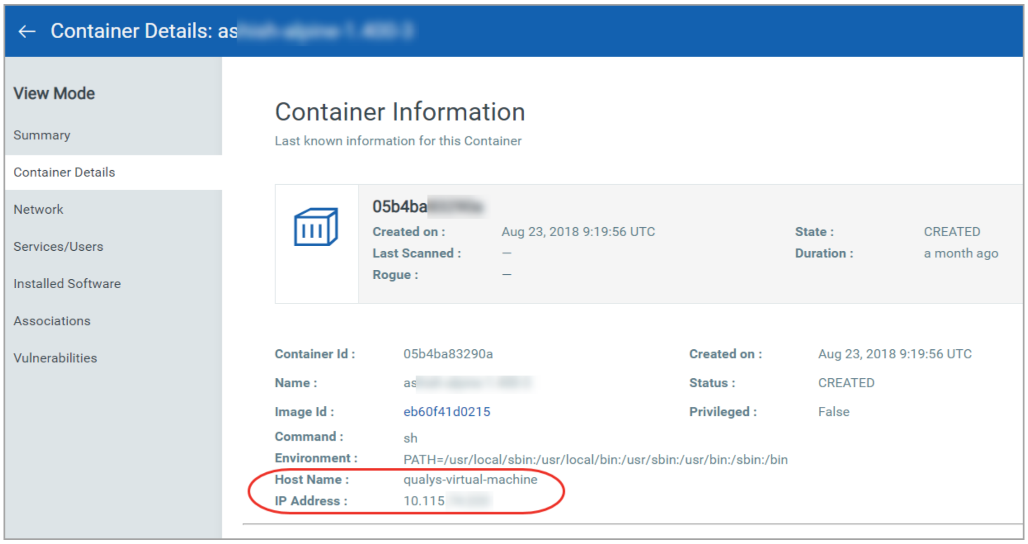
You can now view the age of a vulnerability in the image details / container details view. The age value is displayed in days. Age is calculated from the point Qualys published the vulnerability.



QID	VULNERABILITY TITLE	SEVERITY	CVE	AGE	VULNERABLE SOFTWARE
38510	CA Agent Discloses Exact ... a month ago	🟥🟥⬜⬜⬜		4600 Days	–
38726	OpenSSH Username Enum... a month ago	🟨🟨🟨⬜⬜	CVE-2018-15473	48 Days	–
121328	Linux Kernel libceph Autho...	🟨🟨🟨🟨⬜	CVE-2013-1059	1893 Days	–

View container host information

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



← Container Details: as[redacted]

View Mode

- Summary
- Container Details
- Network
- Services/Users
- Installed Software
- Associations
- Vulnerabilities

Container Information

Last known information for this Container

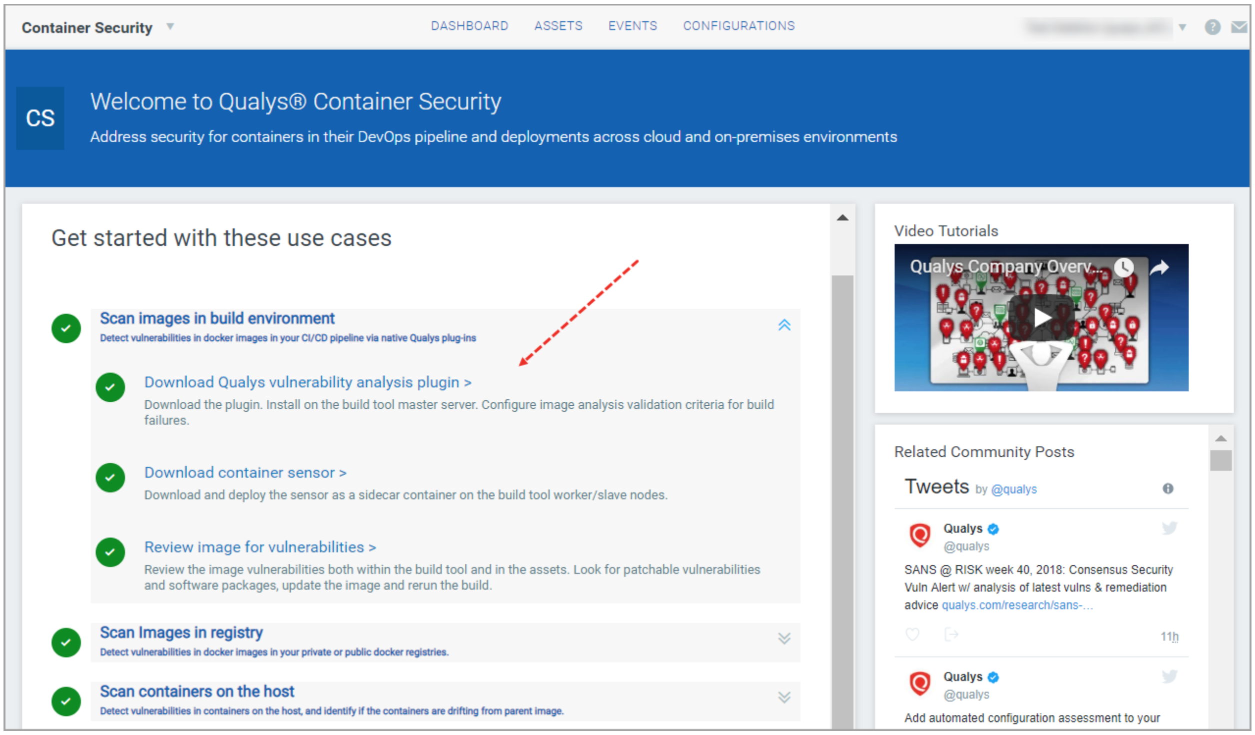
05b4ba[redacted]

Created on :	Aug 23, 2018 9:19:56 UTC	State :	CREATED
Last Scanned :	–	Duration :	a month ago
Rogue :	–		

Container Id :	05b4ba83290a	Created on :	Aug 23, 2018 9:19:56 UTC
Name :	as[redacted]	Status :	CREATED
Image Id :	eb60f41d0215	Privileged :	False
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[redacted]		

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.



Welcome to Qualys® Container Security

Address security for containers in their DevOps pipeline and deployments across cloud and on-premises environments

Get started with these use cases

✓ **Scan images in build environment**
Detect vulnerabilities in docker images in your CI/CD pipeline via native Qualys plug-ins

- ✓ Download Qualys vulnerability analysis plugin >
  Download the plugin. Install on the build tool master server. Configure image analysis validation criteria for build failures.
- ✓ Download container sensor >
  Download and deploy the sensor as a sidecar container on the build tool worker/slave nodes.
- ✓ Review image for vulnerabilities >
  Review the image vulnerabilities both within the build tool and in the assets. Look for patchable vulnerabilities and software packages, update the image and rerun the build.

✓ **Scan Images in registry**
Detect vulnerabilities in docker images in your private or public docker registries.

✓ **Scan containers on the host**
Detect vulnerabilities in containers on the host, and identify if the containers are drifting from parent image.

Video Tutorials

Related Community Posts

Tweets by @qualys

Qualys @qualys
SANS @ RISK week 40, 2018: Consensus Security Vuln Alert w/ analysis of latest vulns & remediation advice qualys.com/research/sans-...
11h

Qualys @qualys
Add automated configuration assessment to your