Qualys Container Security

Release Notes

Version 1.11
August 6, 2021

Here's what's new in Container Security 1.11!

Policy Compliance Now Supported for Registry Sensors

Define Ignored System Calls for Policies from the UI

Container Security 1.11 brings you more improvements and updates! Learn more

Policy Compliance Now Supported for Registry Sensors

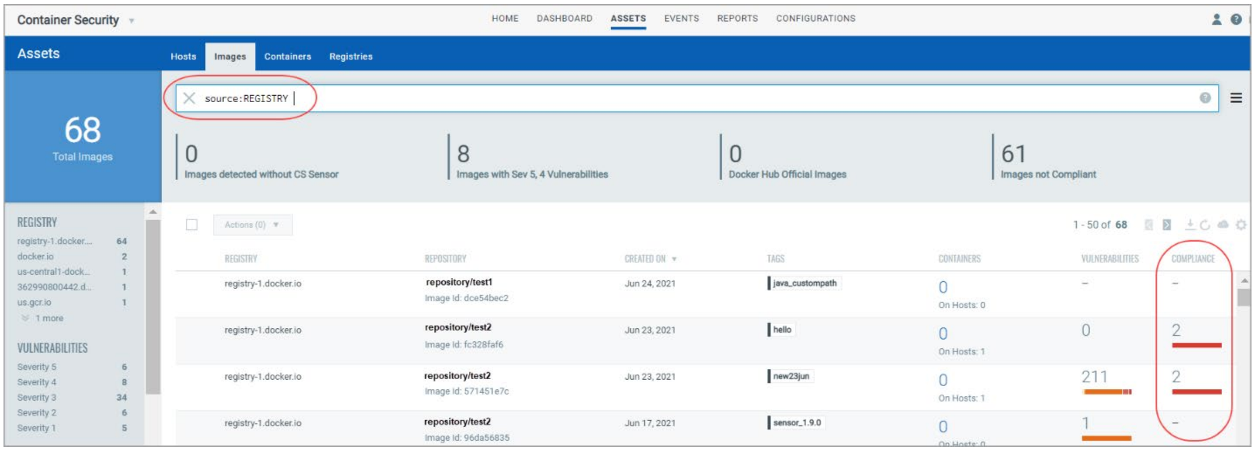
When Policy Compliance (PC) scanning was first introduced in Container Security, it was supported only for General and CI/CD mode. Now Registry mode is also supported. This means that the PC manifest will be assigned to registry sensors, and compliance scanning will be performed along with vulnerability scanning on your registry images. Note that the Policy Compliance Scanning feature was enabled for all customers starting in the last Container Security release.

Prerequisites

- Update your sensors to Container Security Sensor 1.9 or later
- Launch new registry scans to start collecting compliance data

How it works

The Qualys container sensor runs an additional scan of configurations in containers, images and uploads additional scan metadata to the Qualys backend. Based on the scan metadata, the backend performs an assessment against various industry standard benchmarks and controls for compliance assessment. The compliance scans of containers, images will be transparent to customers and will function in a similar real-time cloud native manner like the existing vulnerability scanning feature.



source:REGISTRY

68 Total Images

0 Images detected without CS Sensor

8 Images with Sev 5, 4 Vulnerabilities

0 Docker Hub Official Images

61 Images not Compliant

REGISTRY	
registry-1.docker....	64
docker.io	2
us-central1-dock...	1
362990800442.d...	1
us.gcr.io	1
1 more	

VULNERABILITIES	
Severity 5	6
Severity 4	8
Severity 3	34
Severity 2	6
Severity 1	5

1 - 50 of 68

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES	COMPLIANCE
registry-1.docker.io	repository/test1 Image Id: dce54bec2	Jun 24, 2021	java_custompath	0 On Hosts: 0	–	–
registry-1.docker.io	repository/test2 Image Id: fc328faf6	Jun 23, 2021	hello	0 On Hosts: 1	0	2
registry-1.docker.io	repository/test2 Image Id: 571451e7c	Jun 23, 2021	new23jun	0 On Hosts: 1	211	2
registry-1.docker.io	repository/test2 Image Id: 96da56835	Jun 17, 2021	sensor_1.9.0	0 On Hosts: 0	1	–

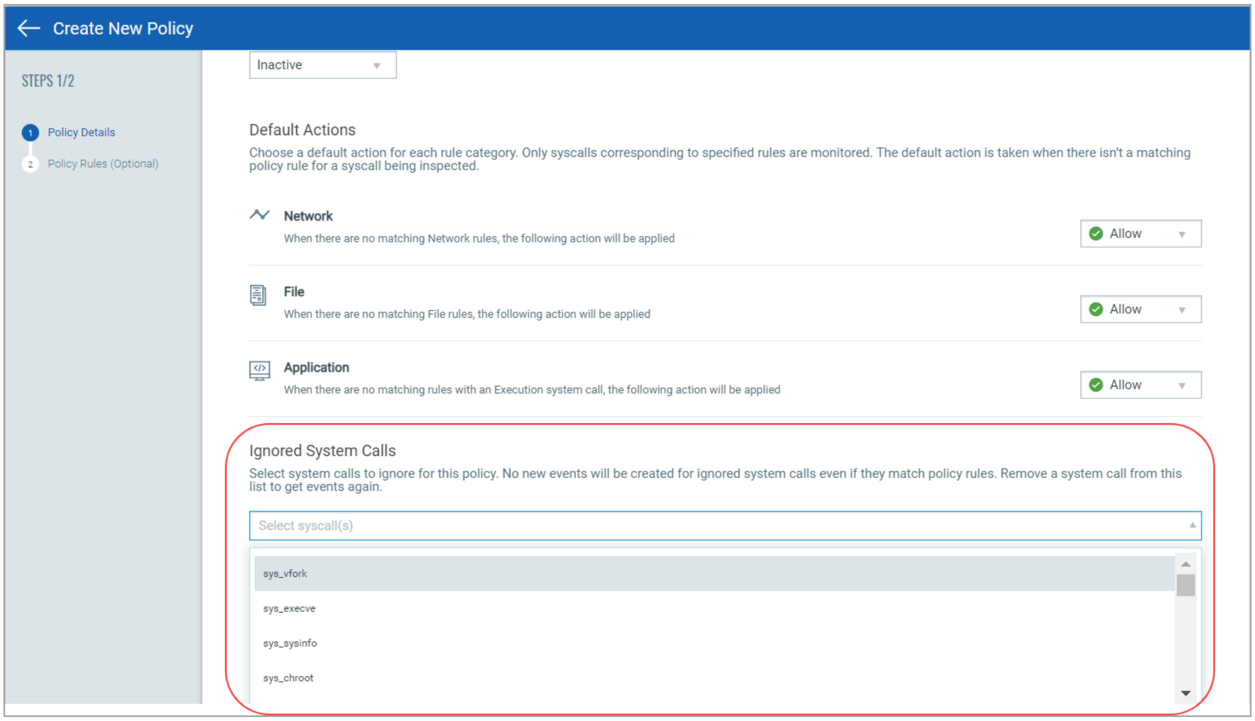
Define Ignored System Calls for Policies from the UI

Applicable when Container Runtime Security (CRS) is enabled.

Now, when defining a runtime policy, you can add a list of system calls that you want to ignore for the policy. When a system call is ignored, no new events will be created for the system call even if it matches one of the policy rules. This will save you from having to modify all the rules that include a particular system call you want to ignore. If you want to start getting events for an ignored system call in the future, simply edit the policy to remove the system call from the ignored system calls list. You'll be able to remove individual system calls or clear the entire list.

How to ignore system calls

Go to **Configurations** > **Runtime Policies** and create or edit a policy. Scroll to the bottom of the **Policy Details** tab. This is where you'll see the new **Ignored System Calls** section. Add one or more system calls from the drop-down list.



Inactive

Default Actions

Choose a default action for each rule category. Only syscalls corresponding to specified rules are monitored. The default action is taken when there isn't a matching policy rule for a syscall being inspected.

Network
When there are no matching Network rules, the following action will be applied — Allow

File
When there are no matching File rules, the following action will be applied — Allow

Application
When there are no matching rules with an Execution system call, the following action will be applied — Allow

Ignored System Calls

Select system calls to ignore for this policy. No new events will be created for ignored system calls even if they match policy rules. Remove a system call from this list to get events again.

Select syscall(s)

Issues Addressed

- We fixed an issue where existing AWS connectors were not visible in the UI when editing or creating scan jobs for AWS registry scanning.
- Now you'll get the correct results when searching sensors using the "or" operator (example: sensorType:CICD or sensorType:GENERAL).
- In the CS API documentation for Fetch a list of software installed on a container (/containers/{containerId}/software), we changed the default value for sort to name:asc.