Qualys Container Security

Release Notes

Version 1.22
February 20, 2023

What's New?

Delete ACR and AWS ECR Registry Connectors
Report Enhancements
Automatic Registry Scan Enhancements
SCA: Support to New Programming Languages
Administration: New Permissions for Sensor Profiles

API Changes

Refer to the Container Security API 1.22 Release Notes for the API changes in this release.

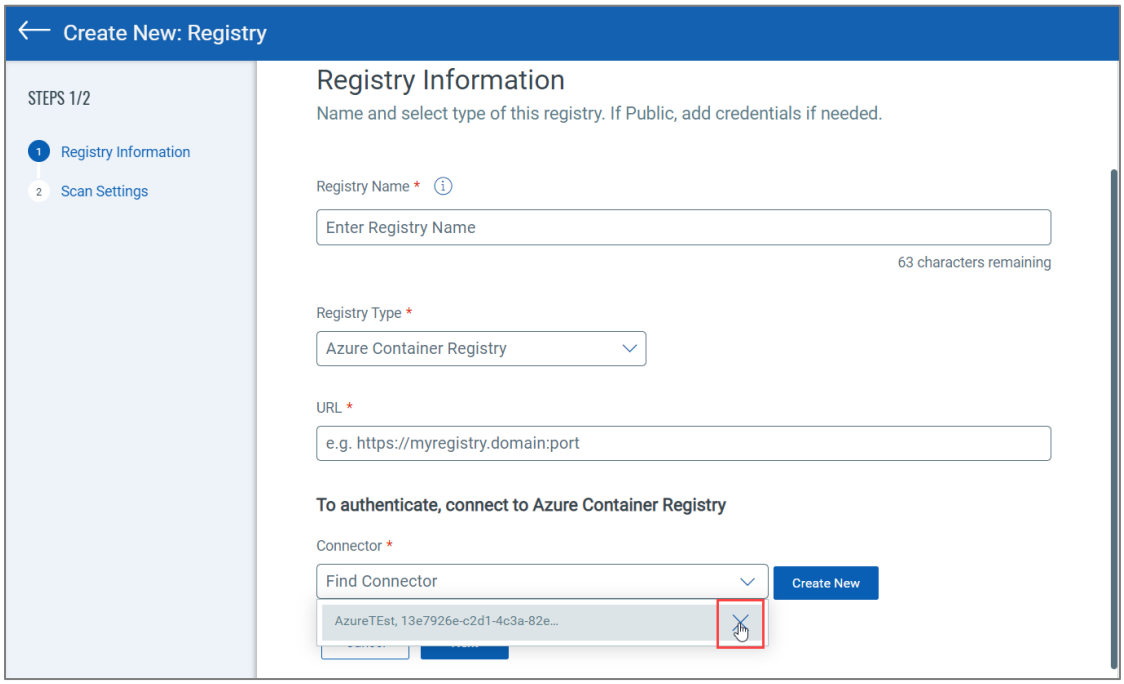
Issues Addressed

Qualys Container Security 1.22 brings you many more improvements and updates! Learn more

What's New?

Delete ACR and AWS ECR Registry Connectors

You can now delete misconfigured and unused connectors for ACR and AWS ECR registries from the **Connector** list while creating a new registry. The connectors must not be associated with any registries. An error message appears if you try to delete a connector associated with one or more registries.



Report Enhancements

You can now include the following attributes in your vulnerability reports:

- **Image Vulnerability Report**

New Attribute	Description
Image Label	Shows labels associated with an image. The labels appear in a comma-separated list in the report. For example, key:name value:CentOS Base Image, key:org.label-schema.description value:Reference Dockerfile containing software with known vulnerabilities., key:org.label-schema.docker.dockerfile

- **Container Vulnerability Report**

New Attribute	Description
Repository	Shows image repository information.

	For example, Registry:docker.io Repository:iojs Tag:latest
Kubernetes Attributes • POD Name • POD Label • POD UUID • POD Namespace • POD Controller • Node Name • Node is Master	Shows Kubernetes attributes to help you analyze your Kubernetes environment.

To show these attributes in the report, the following new check boxes have been introduced in the **Report Display** tab.

Container Vulnerability Report

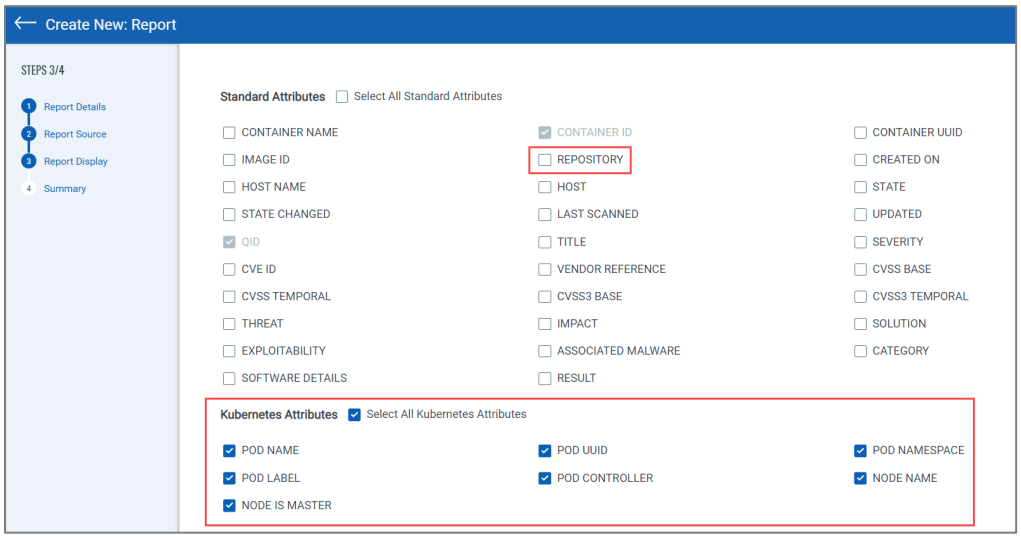
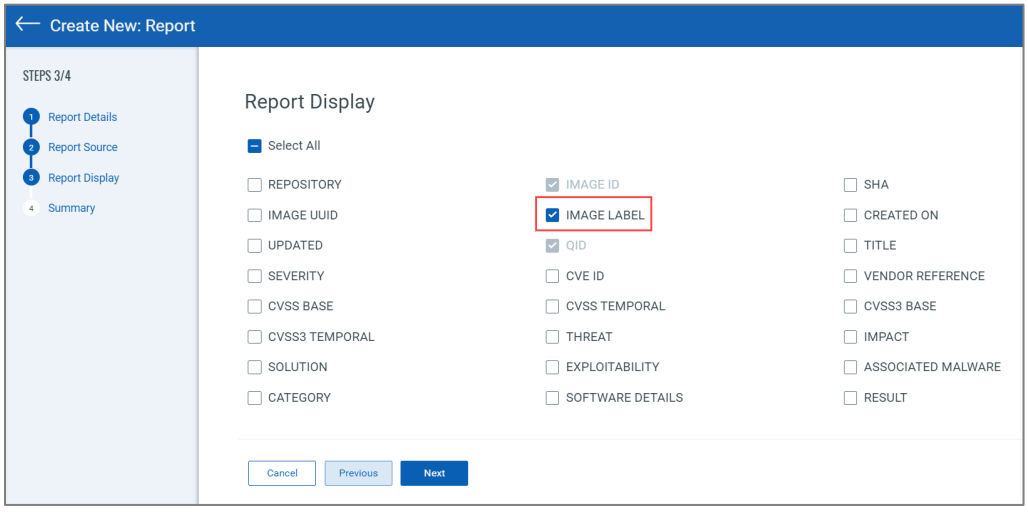


Image Vulnerability Report

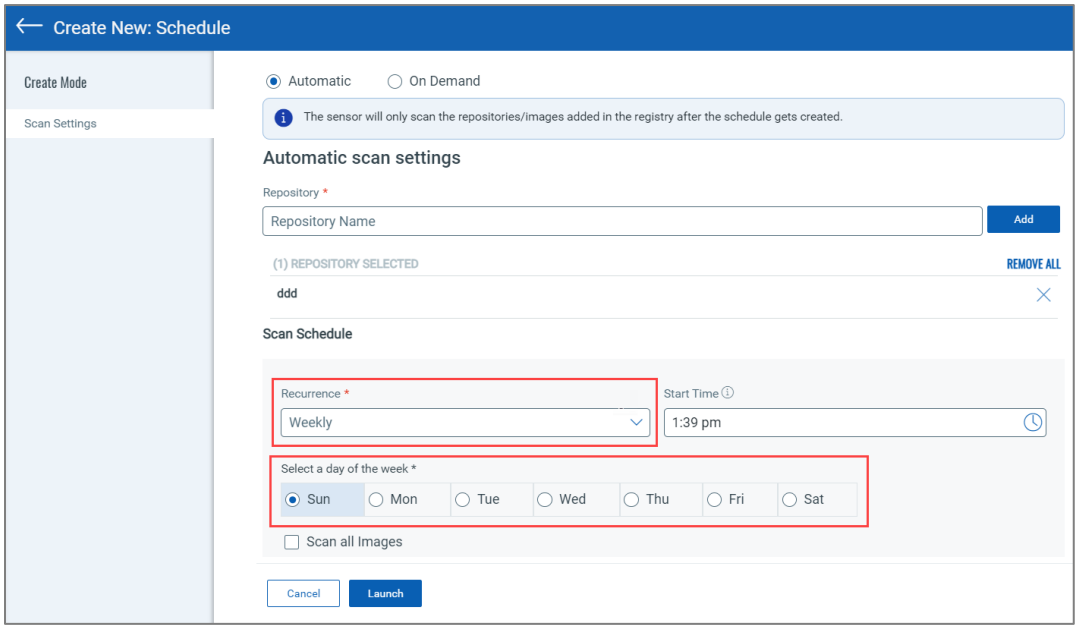


Automatic Registry Scan Enhancements

- The **Scan all images** option is now available for all registries. It scans all images from the specified repositories.

- The schedule creation for automatic registry scans is now simpler than before.
  You now have only two recurrence options, **Daily** and **Weekly**, to create recurrent scan schedules. When selecting **Weekly**, you need to specify a day and the time on which a scan will happen every week.

  The **Scan all images** option is available only when you select weekly recurrence.



SCA: Support to New Programming Languages

SCA scans can now detect the software packages based on the following programming languages:

- PHP
- Ruby
- Rust

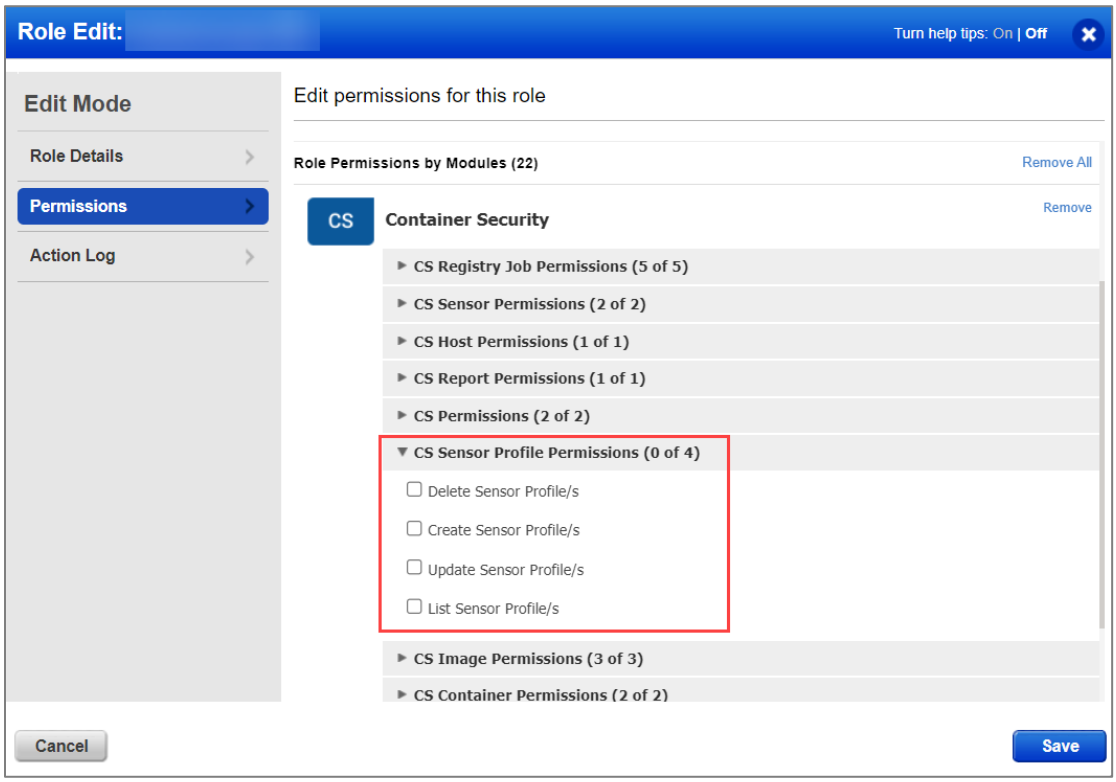
During an SCA scan, the following files are scanned for the packages based on PHP, Ruby, and Rust:

Language	Files
PHP	Composer.lock
Ruby	gemspec
Rust	Cargo.lock and Binaries built with cargo-auditable

Administration: New Permissions for Sensor Profiles

Manager users can now control access to Container Security sensor profiles. The users working on sensor profiles should get the sensor profile permissions configured for their roles to view the sensor profiles and perform various actions on them.

The following new permissions are added:



For more information about role permissions, see Qualys Administration Utility Online Help: Manage User Roles.

Issues Addressed

The following issues have been fixed with this release:

- On CRI-O runtime, in some cases, the status for deleted containers did not reflect correctly in the UI. This issue is now fixed.
- All sensors showed the same IP address after auto-upgrading to 1.16.0 or later. This issue is now fixed.
- The general sensor detected multiple IBM Java vulnerabilities without any information on vulnerable software. The vulnerable software information is now shown correctly.