Qualys Container Security

Release Notes for Sensor

Version 1.24
April 17, 2023

What's New?

JFrog Private Registry: Authenticating with Access Tokens
Securing AWS Fargate on Private Cloud Platforms (PCP)
SCA Scanning: Support for CRI-O Runtime

API Changes

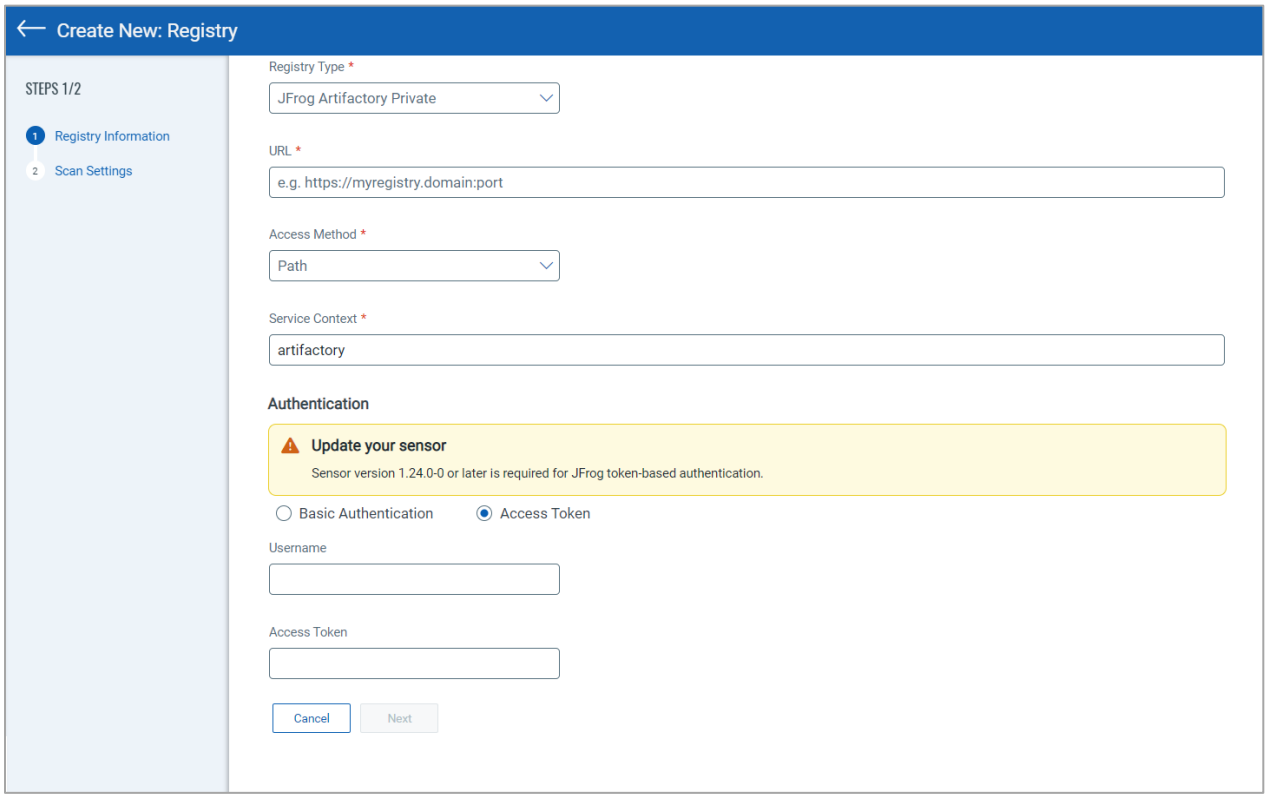
Refer to the Container Security API 1.24 Release Notes for the API changes in this release.

What's New?

JFrog Private Registry: Authenticating with Access Tokens

The registry sensor can now connect with the JFrog Artifactory Private Registry using access tokens. You can generate an access token on the JFrog platform and use it for authenticating the sensor. For more information about JFrog access tokens, see JFrog Documentation.

It is recommended to use a non-expiring token to avoid the need for repeated authentication. This allows you to maintain a continuous connection without having to repeatedly re-authenticate. If your token has expired, the authentication would fail with an error message.



Securing AWS Fargate on Qualys Private Cloud Platform (PCP)

Container Security enables you to secure AWS Fargate by performing vulnerability and compliance scans on container images whenever an AWS ECS Fargate task is launched.

With this release, you can use Container Security to secure AWS Fargate on Qualys Private Cloud Platforms (PCP). Previously, this feature was available on only Qualys Shared Cloud Platform (SCP).

We have provided guidelines for establishing connectivity between AWS Lambda and CodeBuild functions, and your Private Cloud Platform that hosts Qualys Container Security servers. While these guidelines are recommended, you can use alternative methods to set up connectivity. See Securing AWS Fargate on Qualys Private Cloud Platform (PCP).

For more information about scanning container images in AWS Fargate, see Sensor Deployment Guide.

SCA Scanning: Support for CRI-O Runtime

The support for SCA scanning has been extended to the CRI-O runtime, making SCA scanning available to a broader range of environments. Previously, it was available only for the docker and containerd runtimes.

For CRI-O runtime to support SCA, it is required to launch the sensor with privilege rights. The following parameter is added in the 'cssensor-crio-ds.yml' to launch the sensor in privileged mode:

```
securityContext:
     privileged: true
```

For more information about SCA scanning, see Online help: SCA Scanning and Sensor Deployment Guide.