Qualys Container Scanning Connector for Azure DevOps

User Guide

Version 1.0.1

September 7, 2020

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide 4

About Qualys 4
Qualys Support 4
About Container Security Documentation 4

Container Security Overview 5

What data does Container Security collect? 6
Qualys Container Scanning Connector for Azure DevOps 6

Get Started 7

What you'll need 7
Recommended setup for server-agent deployment 8
Install the Plugin 9
Scanning CI/CD images 10

Start Using the Plugin 11

Define container image Ids 12
Qualys API Server URL 14

View Your Qualys Report 15

Debugging and Troubleshooting 16

HTTP codes in API response 16
Plugin times out, no report seen 16
Want to contact Support? 17

What's New 18

About this Guide

Welcome to Qualys Container Security! We'll help you get acquainted with the Qualys solutions for securing your Container environments like Images, Containers and Docker Hosts using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

About Container Security Documentation

This document provides information about using the Qualys Container Scanning Connector for Azure DevOps.

For information on using the Container Security UI to monitor vulnerabilities in Images, Containers, and Registries, refer to the Qualys Container Security User Guide.

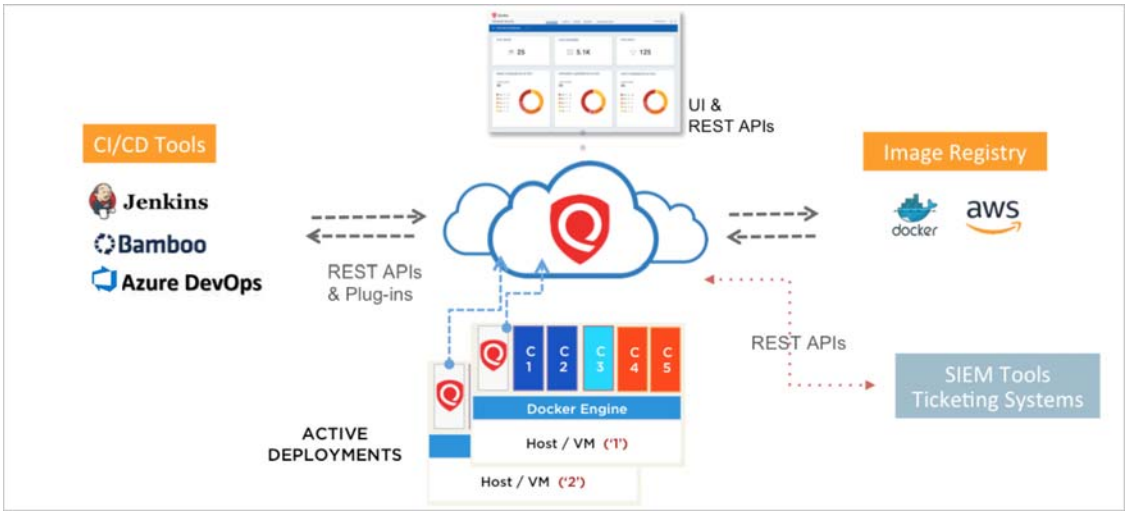
For information on deploying the sensor on MAC, CoreOS, and various orchestrators and cloud environments, refer to the Qualys Container Sensor Deployment Guide.

For information on using the Container Security API, refer to the Qualys Container Security API Guide.

For information on the Jenkins plugin, see Qualys Container Scanning Connector for Jenkins.

Container Security Overview

Qualys Container Security provides discovery, tracking, and continuously protecting container environments. This addresses vulnerability management for images and containers in their DevOps pipeline and deployments across cloud and on-premise environments.



With this version, Qualys Container Security supports

- Discovery, inventory, and near-real time tracking of container environments

- Vulnerability analysis for images and containers

- Vulnerability analysis for registries

- Integration with CI/CD pipeline using APIs (DevOps flow)

- Uses new 'Container Sensor' – providing native container support, distributed as container image

Upon installation, the sensor does automatic discovery of Images and Containers on the deployed host, provides a vulnerability analysis of them, and additionally it monitors and reports on the docker related events on the host. The sensor lists and scans registries for vulnerable images. The sensor container runs in non-privileged mode. It requires a persistent storage for storing and caching files.

Currently, the sensor only scans Images and Containers. For getting a vulnerability posture on the Host, you would require Qualys Cloud Agents or a scan through Qualys Virtual Scanner Appliance.

What data does Container Security collect?

The Qualys Container Security sensor fetches the following information about Images and Containers in your environment:

- **Inventory of Images and Containers** in your environment from commands such as **`docker ps`** that lists all containers.

- **Metadata information** about Images and Containers from commands such as **`docker inspect`** and **`docker info`** that fetches low level information on docker objects.

- **Event information** about Images and Containers from the docker host for docker events like created, started, killed, push, pull, etc.

- **Vulnerabilities** found on Images and Containers. This is the output of the vulnerability management manifests run for identifying vulnerability information in Images and Containers. This is primarily software package listing, services running, ports, etc.

For example, package manager outputs like **`rpm -qa`**, **`npm`**. This is supported across various Linux distributions (CentOS, Ubuntu, CoreOS, etc) and across images like Python, NodeJS, Ruby, and so on.

Qualys Container Scanning Connector for Azure DevOps

Qualys Container Security provides a plugin for Azure DevOps to get the security posture for the container images built via the tool. The plugin can be configured to fail or pass the container image builds based on the vulnerabilities detected.

Get Started

Follow the steps to get started with Qualys Container Scanning Connector for Azure DevOps.

What you'll need

- A valid Qualys subscription with the Container Security application activated.

- Access to Qualys Container Security application API endpoint from your build host.

- Requires the container sensor for CI/CD environment to be installed on the Azure DevOps build host. Refer to Qualys Container Security Sensor Deployment Guide for instructions on installing the container cicd sensor. You must pass the following parameter while deploying the sensor for CI/CD environment `--cicd-deployed-sensor or -c`.

- Azure DevOps CICD tool version 1.0 or later.

- Internet connection for agent to be able to connect to the Qualys Cloud Platform. Install sensor with proxy option if agent is running behind proxy.

- The Azure DevOps services and agents should have an open connection to the Qualys Cloud Platform in order to get data from the Qualys Cloud Platform for vulnerability reporting.

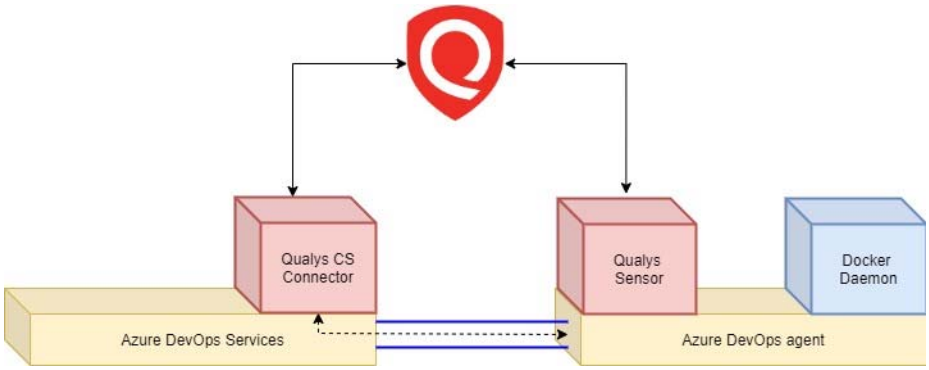
Qualys Container Scanning Connector automatically tags images built out of CI/CD pipeline with the tag **qualys_scan_target:<image-id>** to mark them for scanning and only those images are scanned for vulnerabilities. Once the scanning is over, Qualys Container Sensor will remove the tag. However, if an image has no other tag applied to it other than 'qualys_scan_target:<image-id>', the sensor will retain the tag to avoid removal of the image from the host.

Note: Qualys Container Security does not support scanning images in Docker-in-Docker setup as the sensor cannot listen to events generated by the inner Docker.

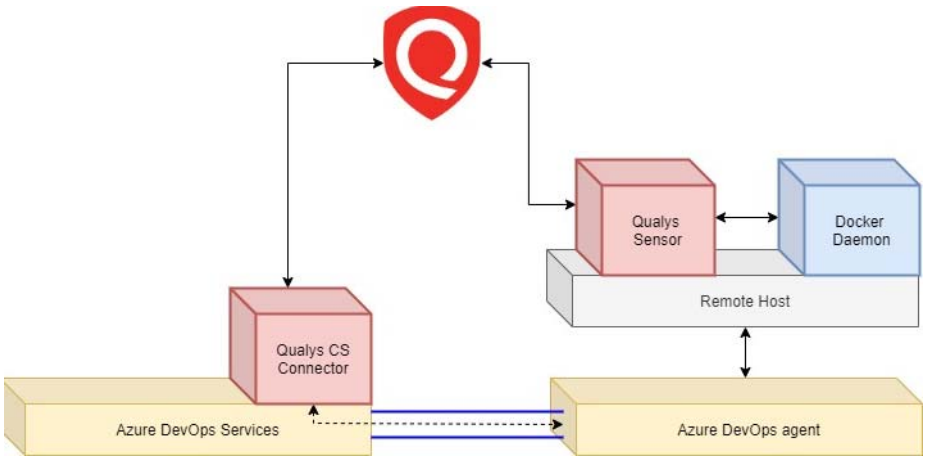
Recommended setup for server-agent deployment

Qualys Container Scanning Connector for Azure DevOps should be deployed on the Azure DevOps services. Qualys Container Security Sensor should be installed where the docker daemon is running. If the docker daemon is running on Azure DevOps agent, install the Sensor on Azure DevOps agent. If the docker daemon is running on a remote host, install the sensor over there.

Following figure shows the docker daemon running on Azure DevOps agent.



Following figure shows the docker daemon running on a remote host.



Install the Plugin

You can install the Qualys Container Scanning Connector for Azure DevOps from Azure DevOps marketplace.

Installing the plugin from Azure DevOps marketplace

1) To install the plugin from Azure DevOps marketplace, login to your Azure DevOps instance.

2) Click the  icon on the top pane at the right side of the page and choose Browse marketplace. Optionally, Click to Extensions on the left pane and click Browse marketplace located at the top right side of the right pane. The browser will open Azure DevOps marketplace page that displays plugins/extensions for Azure DevOps.

3) In the search bar, enter Qualys to search for all the Qualys plugins.

4) Click the Qualys Container Scanning Connector plugin in the plugin list.

5) Click Get it free. You will be navigated to the Visual Studio|Marketplace screen.

6) Select the organization from the drop-down and click Install to install the plugin in your Azure DevOps instance. You can see the installed plugin in the Installed tab when you navigate to Organization Settings > Extension.

The Qualys Container Scanning Connector gets installed/updated in your Azure DevOps instance. In case of update, your existing configuration will continue to work. In case of fresh install, perform the configuration steps provided further in this document.

Scanning CI/CD images

Configure the Qualys Container Scanning Connector to automatically tag CI/CD images with 'qualys_scan_target:<image-id>'.

Docker URL: Docker REST API URL / Docker socket path. Only unix:/// and tcp:// protocols allowed.

Cert File Path: If you are using remote server enabled https, you can provide a specific folder location which contains the files ca.pem, cert.pem and key.pem. For example, /var/home/certs.

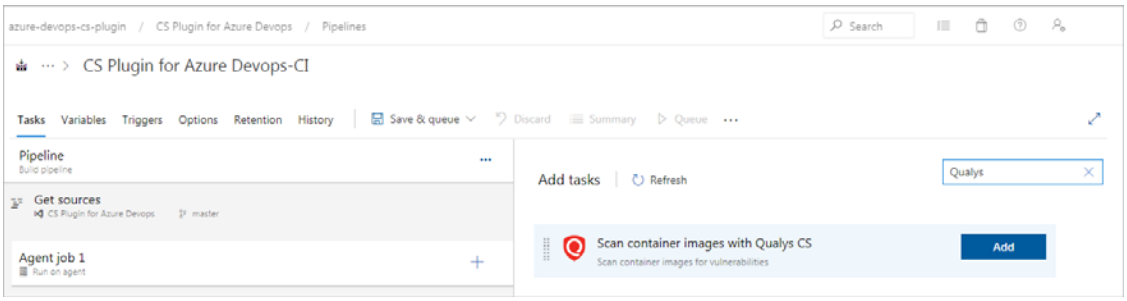
Docker URLs (unix socket or TCP) to be used in various docker deployment scenarios

Deployment scenario	Sensor location	Docker URL to be used
Job executed by Azure DevOps agent AND Docker host == Azure DevOps agent	Azure DevOps agent	UNIX unix:///var/run/docker.sock
Job executed by Azure DevOps agent AND Docker Host == Remote docker host (any machine other than Azure DevOps agent)	Remote docker host	TCP path of the Remote Docker host: tcp://<ip_of_RDH>:<port> For example, tcp://10.115.67.61:2375

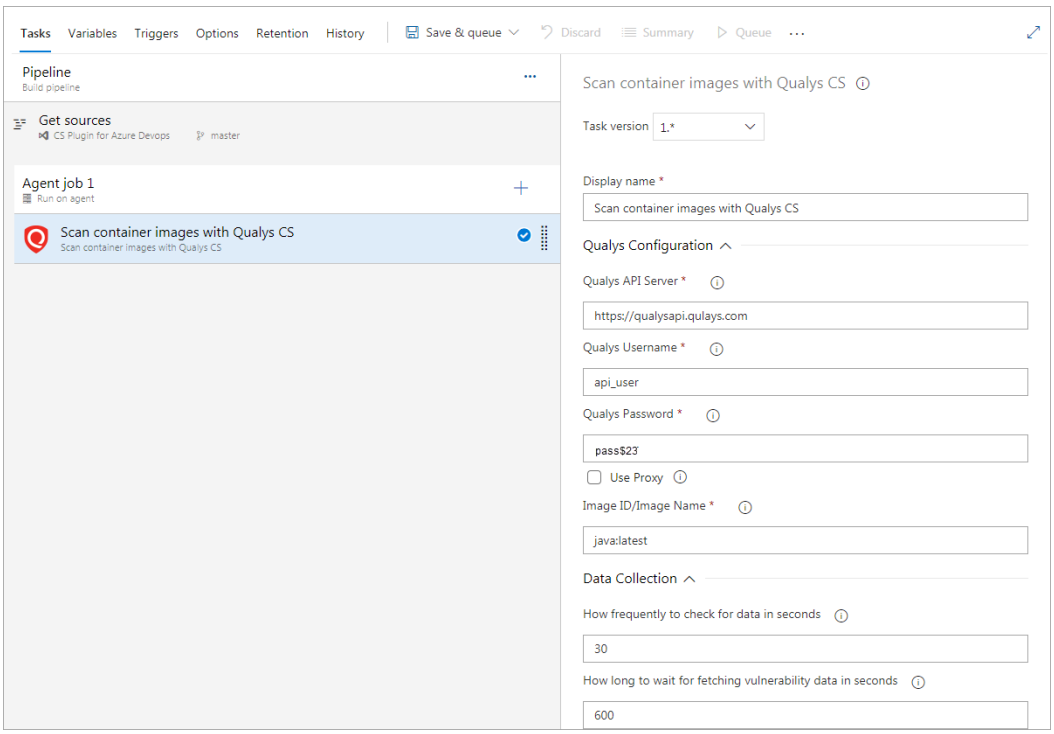
Start Using the Plugin

Qualys recommends to set up the Qualys Container Scanning Connector after the container image is built, and before the image is pushed to the registry. Ensure that you do not delete the image before the plugin setup is complete.

You can use this plugin as a task in your Azure DevOps pipeline. After installing the Qualys Container Scanning Connector, you see this plugin as a task in your pipeline. In the Tasks tab, click Add Task under your agent job, and simply search for “Qualys” to get the “Scan container images with Qualys CS Plugin” task. Select the task and click Add to add it as a task. You will see the task under the agent.



Click the “Scan container images with Qualys CS Plugin” task. Now configure the plugin.



See Configuration Details

Define container image Ids

In the plugin configuration there is a field called image ID/Image Name. Set this to a single container image Id or name you want to report on.

Enter a single string value like imageId: 'a1b2c3d4e5f6'. We also support SHA value of the image as the input to image ID. Specify an image name in the format `repo:tag`.

The plugin will only pull a report for the image Id/name you specify. If you provide an image name, the plugin fetches the corresponding image ID. The plugin tries to fetch the image ID using the docker socket path configured in configuration. If your docker host is running locally to build tool/agent, the docker socket path is unix:///var/run/docker.sock; whereas if your docker host is running remotely, the docker socket path is the TCP URL to the remote docker host. See Scanning CI/CD images.

Alternatively, you can also provide image id through an environment variable. Get the image id of the container image using the program created in earlier stages of the build and provide that id in the 'imageId' argument. For example, in pipeline script, you can get the image id by executing shell script and store it in an environment variable. And then use the same environment variable in 'ImageId' argument to provide the image id.

Configuration Details

Provide the following configuration details:

(1) API login information (Select Use Proxy to provide proxy information).

Note: Due to Azure DevOps limitations password string is visible on UI. To avoid disclosing password, use pipeline variable.

(2) container image ID / image name for which you want to check for vulnerabilities.

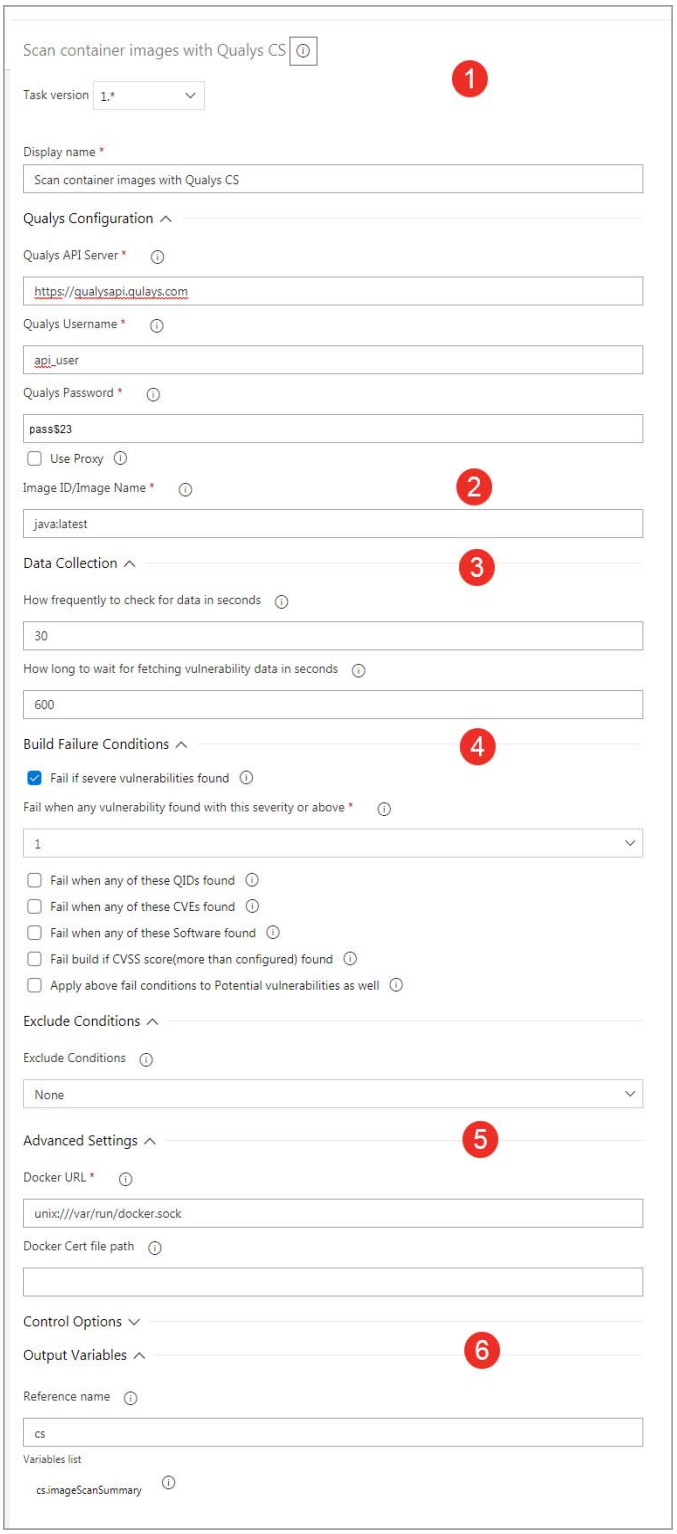
(3) data collection frequency.

(4) build failure conditions.

5) specify the docker daemon URL in the Advance Settings section for plugin to connect to the docker daemon and tag the images specified in the input.

(6) specify the variable in the Output Variable section. The Output variable will contain the result of evaluation of the image vulnerabilities data against the build failure conditions. This is an optional setting and CS extension does not control the formatting of the JSON file. Hence, to have output in the proper JSON format, use any JSON specific utility. For example, in case of NodeJS script runner, you can add this line, "console.log (JSON.stringify($(qcs.imageScanSummary)))" in the code along with the Output Variable from Qualys task as input to print the file in the proper JSON format. ('qcs.imageScanSummary' is the output variable created in qualys task with 'qcs' provided as reference name by user)

When you're ready, click Save Configuration.



Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

View Your Qualys Report

The plugin will generate report for the container image in the build. In a build, click the job which includes Qualys plugin and navigate to 'Qualys Image Scan Result', to see vulnerability details for the container image.

The reports shows vulnerabilities data in multiple tabs. 1) The Build Summary shows the criteria against which vulnerabilities are evaluated. These criteria are the configured failure conditions. A criteria is violated when vulnerabilities found in the scan matches one or more values set in the failure conditions for the criteria. 2) The Image Statistics provides a dashboard view of your security posture. 3) Go to Vulnerabilities for a list of detected QIDs, 4) Installed Software to see software detected on the container image, and 5) Layers to view a list of layers the image is made of.

Sample Build Summary view

Sample Image Statistics view

Debugging and Troubleshooting

HTTP codes in API response

All API calls and their responses are logged by the plugin and are visible in the Console Output. Here are the HTTP response codes you may see during plugin execution.

Code	Error	Description
204	No content	Qualys sensor is processing data. You'll see 200 OK when complete.
200	OK	You would see this code in two situations: 1) You might have received partial data from Qualys where image details are available but vulnerability data is not available. 2) Vulnerability data is also available. This is usually the last call, after which the thread for that image Id stops.
500	Internal server error	Qualys service is down or there was an issue processing data.
400	Bad request	Qualys API server is unable to understand the request.
401	Unauthorized	The credentials used for Qualys API server are incorrect or the user does not have access to the APIs.

If you don't see any API calls being made...

Make sure you're correctly passing image Ids to the plugin. When the plugin starts the execution, it will print the image Ids provided and you can see this in the Console Output. Check that the container image Ids you provided are printed.

Plugin times out, no report seen

The plugin is designed to keep polling the Qualys API until the configured timeout period is reached. If it does not get vulnerability data from Qualys within this period, it stops. In this case, the plugin will fail the build only if you have set any fail-on conditions. Otherwise, it will not fail the build. You will not see any report links since the plugin could not get vulnerability data, and could not prepare a report.

How to fix this?

On the Qualys Cloud Platform, go to Container Security > Assets > Images and verify if the image for which you are checking the vulnerabilities is present in the Images list.

If the image is not present console logs have the following entry:

```
Get scan result API for image e0111ddfea06 returned code : 404;
HTTP Code: 404. Image: Not known to Qualys. Vulnerabilities: To be
processed.. API Response : {"errorCode":"CMS-2002","message":"Data not
available for given Image Id.","timestamp":1554568122039}
```

Ensure that the Qualys Container Sensor is installed on the host where image is being built.

If the image is present, console logs have the following entry:

```
Get scan result API for image cef4ca723229 returned code : 200;
Waiting for vulnerabilities data from Qualys for image id cef4ca723229
HTTP Code: 200. Image: known to Qualys. Vulnerabilities: To be processed.
```

Wait for the vulnerabilities data to be uploaded to the Qualys Cloud Platform.

Want to contact Support?

Access online support information at www.qualys.com/support/

You'll typically need to provide the following information for Qualys Container Scanning Connector issues:

- Version of the Qualys Container Scanning Connector

- Azure DevOps services-agent topology - Whether the Docker daemon is on Azure DevOps agent or Remote host-agent topology

- Pipeline build console logs

What's New

Issue Fixed in 1.0.1

We fixed an issue to allow Qualys Container Security Connector for Azure DevOps to accept special characters in passwords as per the Qualys password policy.