Vulnerability Analysis Plugin for Bamboo

Version 1.6.0.0

November 26, 2019
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 Vulnerability Analysis Plugin for Bamboo.

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 Vulnerability Analysis Plugin 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 docker 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 Vulnerability Analysis Plugin for Bamboo

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

Follow the steps to get started with Container Security plugin for Bamboo.

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 Bamboo 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.
- Bamboo CICD tool version 5.14.0.1 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 Bamboo server 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.

Bamboo plugin 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

Vulnerability Analysis Plugin for Bamboo should be deployed on the Bamboo server. Qualys Container Security Sensor should be installed where the docker daemon is running. If the docker daemon is running on Bamboo agent, install the Sensor on Bamboo agent. If the docker daemon is running on a remote host, install the sensor over there.

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

Install the Plugin

1) On Qualys Cloud Platform, go to Configurations > Integrations to download the Bamboo plugin (Qualys Docker Image Analyzer Plugin).

2) Upload the plugin to your Bamboo tool. Go to Administration > Add-ons and upload the Qualys bamboo plugin jar file.

Scanning CI/CD images

Configure the Bamboo plugin 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/bamboo_home/certs.
# Docker URLs (unix socket or TCP) to be used in various docker deployment scenarios

<table>
<thead>
<tr>
<th>Deployment scenario</th>
<th>Sensor location</th>
<th>Docker URL to be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job executed by Bamboo server AND Docker host == Bamboo server</td>
<td>Bamboo server host</td>
<td>UNIX unix:///var/run/docker.sock</td>
</tr>
<tr>
<td>Job executed by Bamboo server AND Docker Host == Remote docker host (any machine other than Bamboo server or agent)</td>
<td>Remote docker host</td>
<td>TCP path of the Remote Docker host: tcp://&lt;ip_of_RDH&gt;:&lt;port&gt; For example, tcp://10.115.67.61:2375</td>
</tr>
<tr>
<td>Job executed by Bamboo agent AND Docker host == Bamboo agent</td>
<td>Bamboo agent</td>
<td>UNIX unix:///var/run/docker.sock</td>
</tr>
<tr>
<td>Job executed by Bamboo agent AND Docker Host == Remote docker host (any machine other than Bamboo server or agent)</td>
<td>Remote docker host</td>
<td>TCP path of the Remote Docker host: tcp://&lt;ip_of_RDH&gt;:&lt;port&gt; For example, tcp://10.115.67.61:2375</td>
</tr>
</tbody>
</table>
Start Using the Plugin

Qualys recommends to set up the Bamboo Plugin after the docker 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 bamboo plan. In the Tasks tab, click Add Task, and simply search for “Qualys” to get the Qualys Docker Image Analyzer Plugin addon you uploaded earlier. Click the Qualys addon to add it as a task.

While setting up the plugin you can either provide a global configuration or a local configuration for Qualys Container Security. Global configuration can be set once and used for multiple projects.

To set a global configuration, go to Administration > Add-ons, then in the left pane under ADD-ONS, find and click Qualys Docker Image Analyzer Plugin. Then, provide the configuration details listed below.
If you want to set a local configuration, in the Tasks tab, select Qualys Docker Image Analyzer Plugin, and then select the Configure locally option. Note: Selecting the “Use Global Config” option here will let the task use the global configuration you have set under Administration > Add-ons > Qualys Docker Image Analyzer Plugin.

See Configuration Details

Define docker image Ids

In the plugin configuration there is a field called image IDs/Image Names. This field is only available for local configuration. Set this to the docker image Ids or names you want to report on.

Enter a single string value like imageIds: ‘a1b2c3d4e5f6’ or a comma-separated list like imageIds: ’a1b2c3d4e5f6,abcdef123456’. Specify an image name in the format repo:tag.

The plugin will only pull a report for the image Ids/names 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 global or local 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.

You can also define docker image Ids in a variable and specify the variable as the value. Alternatively, you can inject bamboo variables using a task.

Using the WebHook

You can forward Bamboo job results to a WebHook URL.

You can set a global WebHook URL under Administration > Add-ons > Qualys Docker Image Analyzer Plugin, or a WebHook URL for local configuration in the Tasks tab for a plan, by selecting Qualys Docker Image Analyzer Plugin.

Note: WebHook URL specified under local configuration, for a particular project, will always take preference over the global WebHook URL specified under Administration > Add-ons > Qualys Docker Image Analyzer Plugin.

WebHook data sample

```json
{
  "buildNumber": 135,
  "planName": "Bamboo Docker Image Analyzer Plugin 1.6.0.0 - Default Job",
  "planKey": "BDIAP1-BCPIFBCNATC-JOB1",
  "buildStatus": "Failed",
  "failReason": [
    {
      "imageId": "10c550a8b09e",
      "software": {
        "configured": "xz-utils, ABC, sed, UCF, unzip, TZDATA=2019a-0+deb9u1",
```
"found": "sed=4.5-3.fc30"
},
"severities": {
  "1": {
    "configured": 0,
    "found": 1
  }
},
"cvss": {
  "configured": 1.9,
  "found": 6,
  "version": 2
}
]
"images": [
{
  "imageId\name": "fedora\httpd",
  "imageId": "10c550a8b09e",
  "uuid": "71295b15-5ef5-3202-aa10-ee78c0b54f37",
  "sha": "10c550a8b09ec47729c1bb6e7a0dea57d9c5895a7e137aldad181f41ca27cc9",
  "size": 321297635,
  "repo": [
    {
      "registry": "docker.io",
      "tag": "latest",
      "repository": "fedora\httpd"
    }
  ],
  "operatingSystem": "Fedora 30",
  "layersCount": 7,
  "dockerVersion": "17.06.0-ce",
  "architecture": "amd64",
  "vulnerabilities": {
    "totalVulnerabilities": 6,
    "typeDetected": {
      "Confirmed": 1,
      "Potential": 5
    },
    "severity": {
      "Potential": {
        "1": 1,
        "2": 0,
        "3": 4,
        "4": 0,
        "5": 0
      },
      "Confirmed": {
Start Using the Plugin
Using the WebHook

```
"1": 0,
"2": 1,
"3": 0,
"4": 0,
"5": 0
```
**Configuration Details**

Provide the following configuration details:

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

2. Click Test Connection to verify that the plugin can call the Qualys Container Security API.

3. data collection frequency.

4. build failure conditions.

5. docker image IDs / image names to check for vulnerabilities.

6. forward Bamboo job results to a WebHook URL.

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 one report for each docker image in the build. Multiple image Ids will result in multiple reports. In a build, click the job which includes Qualys plugin, to see vulnerability details for the docker image.

Note: If case of multiple image Ids, the build fails even if one image Id matches the fail condition. The build summary will show details of the image which matched the fail condition.

The Build Summary provides a dashboard view of your security posture. Go to Vulnerabilities for a list of detected QIDs, Installed Software to see software detected on the docker image, and Layers to view a list of layers the image is made of.
Debugging and Troubleshooting

Where are the logs?

Bamboo logs are located at the following places on Linux.

Server logs - `<bamboo_server_home>/logs/atlassian-bamboo.log`

Agent logs - `<bamboo_agent_home>/logs/atlassian-bamboo.log`

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.

<table>
<thead>
<tr>
<th>Code</th>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>No content</td>
<td>Qualys sensor is processing data. You’ll see 200 OK when complete.</td>
</tr>
<tr>
<td>200</td>
<td>OK</td>
<td>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.</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error</td>
<td>Qualys service is down or there was an issue processing data.</td>
</tr>
<tr>
<td>400</td>
<td>Bad request</td>
<td>Qualys API server is unable to understand the request.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The credentials used for Qualys API server are incorrect or the user does not have access to the APIs.</td>
</tr>
</tbody>
</table>

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 docker 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.

Error: The trustAnchors parameter must be non-empty

The following error is seen in console logs when the trustStore used by Java for SSL connection between Bamboo Server/Agent and Qualys, is not found, couldn’t be opened (permission issue), or is empty:

java.lang.RuntimeException: Unexpected error:
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be non-empty

You can fix this issue by reconfiguring/updating the certificates (ca-certs) present on the host where the Bamboo Server or Agent is installed. We have provided sample commands for CentOS and Ubuntu. Use the commands specific to the host OS running your Bamboo Server/Agent.

CentOS:

yum install -y ca-certificates
update-ca-trust force-enable
sudo ln -s /etc/ssl/your-cert.pem /etc/pki/ca-trust/source/anchors/your-
cert.pem
update-ca-trust

Alternative commands for CentOS:
yum reinstall ca-certificates
update-ca-trust

Ubuntu:
sudo update-ca-certificates -f
sudo /var/lib/dpkg/info/ca-certificates-java.postinst configure

Want to contact Support?
Access online support information at www.qualys.com/support/
You’ll typically need to provide the following information for Qualys Bamboo plugin issues:
  - Bamboo version
  - Java version on which Bamboo is running
  - Version of the Qualys Vulnerability Analysis Plugin
  - Bamboo server-agent topology
  - Whether the Docker daemon is on Bamboo server or Bamboo agent or remote host