OpenFaas-Compliance-Validation-Proposal

Monday, March 18, 2019 9:24 AM

Proposal : Introduce Function Image compliance validation in OpenFaaS

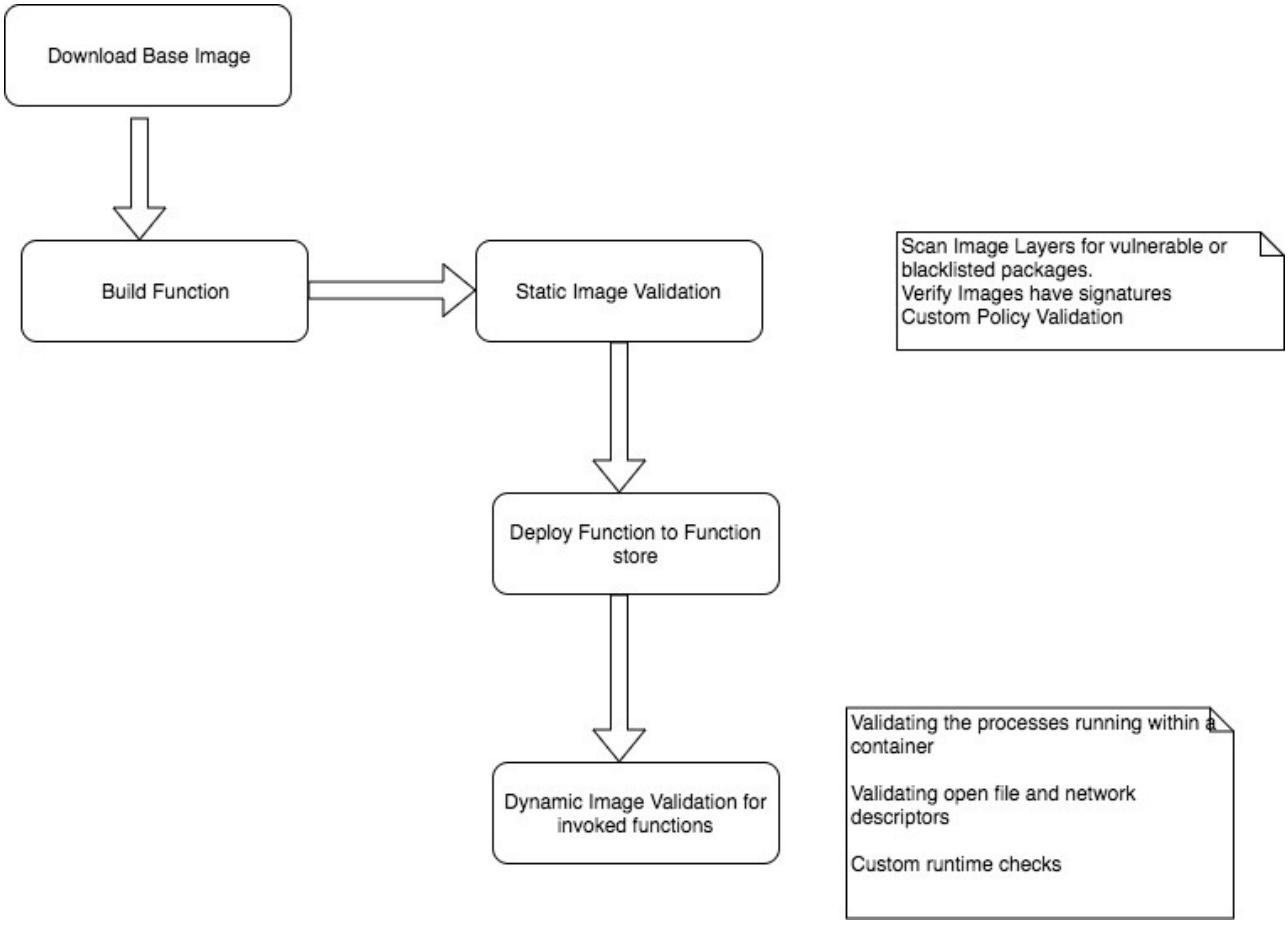
Abstract:

It would be useful to provide a mechanism in OpenFaaS to validate container images used for building functions deployed to the OpenFaaS function store.

There are two phases of validation:

- Function image build-phase validation
- Function image runtime validation.

Here is what the OpenFaaS function image validation pipeline would like:



Function Image build-phase validation:

This would be exposed as an option within **faas-cli**. When this option is invoked an image validator module will be invoked during the build process that would validate the images used for building functions against the rules specified by the end user. The following activities would be performed as a part of the validation

- Scanning image layers for vulnerable packages
- Verifying that images being used have signatures
- Any custom user policy validation.

If any of the validation rules fail, then the function build process is aborted and the user must restart the build process after rectifying the reported problems.

Function Image runtime validation:

This phase would validate the function images that are currently executing in the cluster to check for the following:

- Images being used are from a trusted source
- Validate the list of open file and network descriptors within a container
- Custom runtime checks on the function image

If any of the validation rules fail, then the function service is terminated and the user must rectify the reported problems in order to get the function deployed and executing again.

Existing mechanisms:

Signature validation and compliance scan

Currently, VMWare Harbor and Quay support signature validation and vulnerability analysis**.** Docker provides Docker Content Trust as well as compliance scanning for their images. However, the above workflow is repository agnostic and would work well in lot of other environments where **dockerhub** is the repository of choice while complementing the current efforts for Harbor.

Additionally, Docker Content Trust mechanism is Trust On First Use (TOFU) based. Also, it is not guaranteed to be switched on using the environment variables under all deployment scenarios.

Specifying policies for container validation

Open Policy Agent is a framework that provides policy based control for cloud environments. This however is only for runtime validation of container images and would need to be evaluated for the ease of integration into OpenFaaS.

Google provides a container structural test framework that can be used to validate the content of the images.

Proposed scope of work:

From our perspective we propose the following two additions to OpenFaaS:

1. A functionality within **faas-cli** to validate images during build time. The scope of validation would be limited to performing vulnerability analysis. The framework would be extensible for plugging in additional validations later.
2. Develop a custom admission controller web hook to perform dynamic validation of container images for vulnerabilities. Again, the custom admission controller can be enhanced to add more custom validations or integrate with the open policy framework at a later stage based on user feedback.

References:

Anchore - https://anchore.com/compliance/
Chef Inspec - https://blog.chef.io/2017/03/22/docker-container-compliance-with-inspec/
Clair - https://github.com/coreos/clair