

Presenting



HARBOR™

and its components for container security

Solène Evesque – Orange - 2020

Overview



CNCF Community

« An open source trusted cloud native registry project that stores, signs, and scans content. »

Functions :

- Docker registry
- Image Signer
- Image Scanner
- (Helm Charts registry)

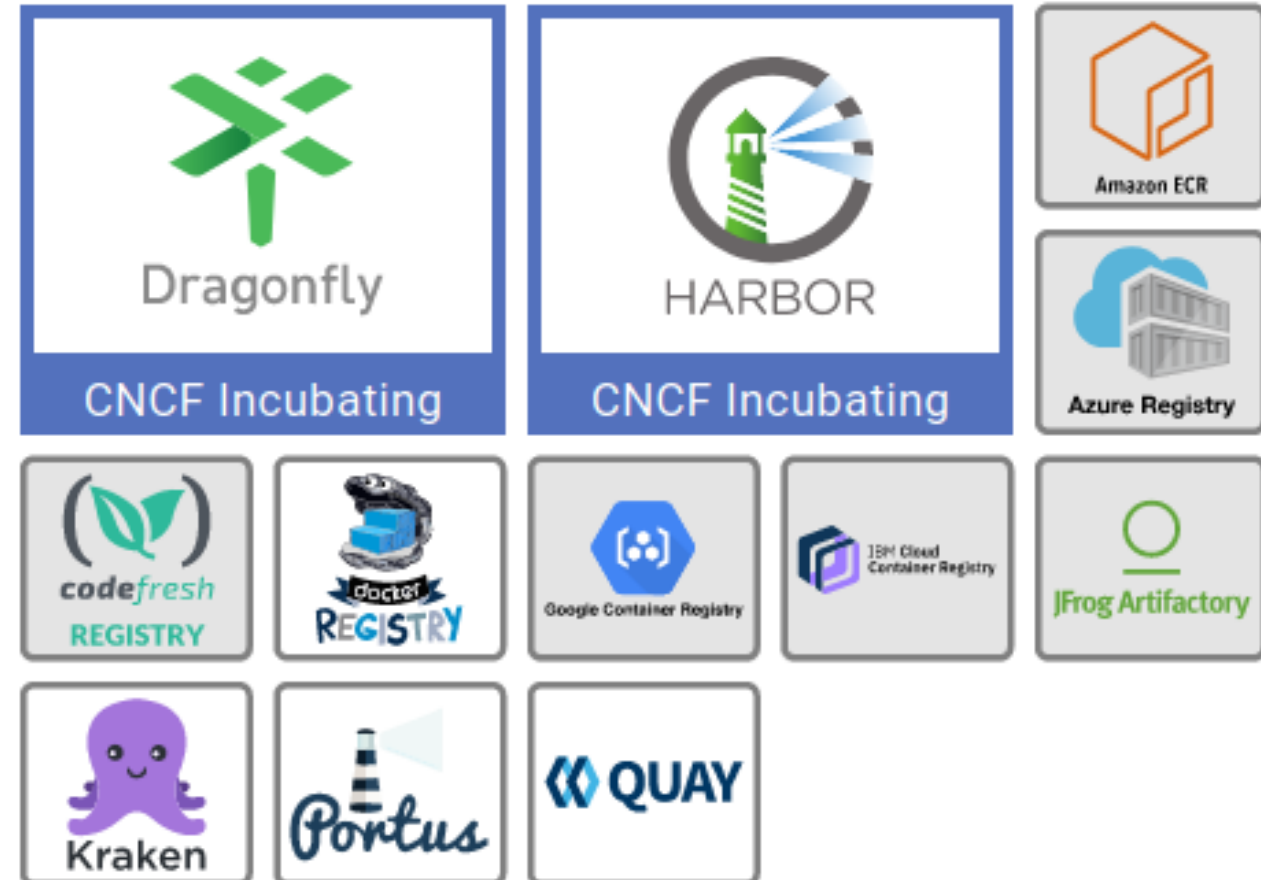
4 years

Over 9000 commits

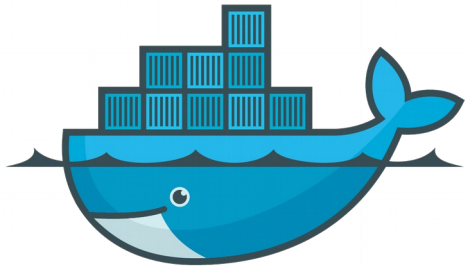
Over 12k stars on Github
passing CII best practices

Renewed documentation

Container Registry



Implemented tools



docker

Docker registry

Stores Docker images in projects, with different accesses and restrictions.



Notary Signer

Signing images ensure they are known and therefore secured.



Clair scanner

Clair can scan images, get packages CVEs, their severity, description and fix.



Chart Museum

A way of storing Helm Charts.

Security solutions



Web interface

Harbor

Search Harbor...

English

admin

Projects

PROJECTS 0_{PRIVATE} 2_{PUBLIC} 2_{TOTAL}

REPOSITORIES 0_{PRIVATE} 97_{PUBLIC} 97_{TOTAL}

All Projects

+ NEW PROJECT X DELETE

<input type="checkbox"/>	Project Name	Access Level	Role	Repositories Count	Chart Count	Creation Time
<input type="checkbox"/>	library	Public	Project Admin	1	0	3/11/20, 10:01 AM
<input type="checkbox"/>	onap	Public	Project Admin	96	0	3/11/20, 10:50 AM

1 - 2 of 2 items

API EXPLORER

Project management and repositories

onap System Admin

Summary **Repositories** Helm Charts Members Labels Logs

[REGISTRY CERTIFICATE](#) [PUSH IMAGE DOCKER](#)

[X DELETE](#)

<input type="checkbox"/>	Name	Tags
<input type="checkbox"/>	onap/aaf_cass	1
<input type="checkbox"/>	onap/aaf_config	1
<input type="checkbox"/>	onap/aaf_core	1
<input type="checkbox"/>	onap/aai-graphadmin	1
<input type="checkbox"/>	onap/aai-resources	1
<input type="checkbox"/>	onap/aai-schema-service	1
<input type="checkbox"/>	onap/aai-traversal	1
<input type="checkbox"/>	onap/alpine	1
<input type="checkbox"/>	onap/api-handler-infra	1

onap System Admin

Summary Repositories Helm Charts Members Labels Logs Robot Accounts Tag Retention Tag Imm

Project registry Public
Making a project registry public will make all repositories accessible to everyone.

Deployment security Enable content trust
Allow only verified images to be deployed.

Prevent vulnerable images from running.
Prevent images with vulnerability severity of Low and above from being deployed.

Vulnerability scanning Automatically scan images on push
Automatically scan images when they are pushed to the project registry.

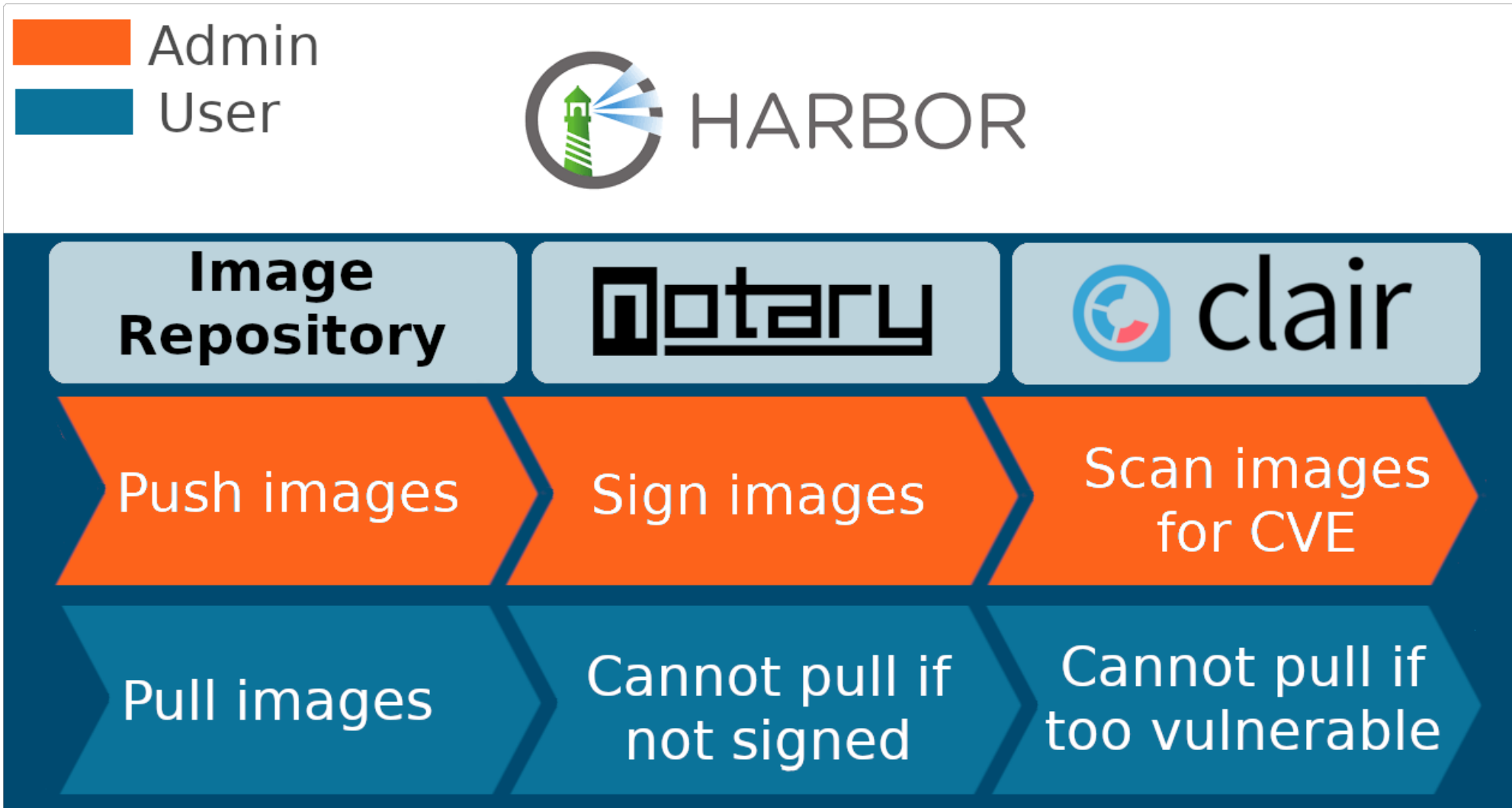
CVE whitelist
Project whitelist allows vulnerabilities in this list to be ignored in this project when pushing and pulling image.
You can either use the default whitelist configured at the system level or click on 'Project whitelist' to create
Add individual CVE IDs before clicking 'COPY FROM SYSTEM' to add system whitelist as well.

System whitelist Project whitelist

[ADD](#) [COPY FROM SYSTEM](#)

Expires at Never expires

Notary signing and Clair scanning





Tag	Size	Pull Command	Vulnerabilities	Signed
latest	59.10MB		• 99 Total • 52 Fixable	

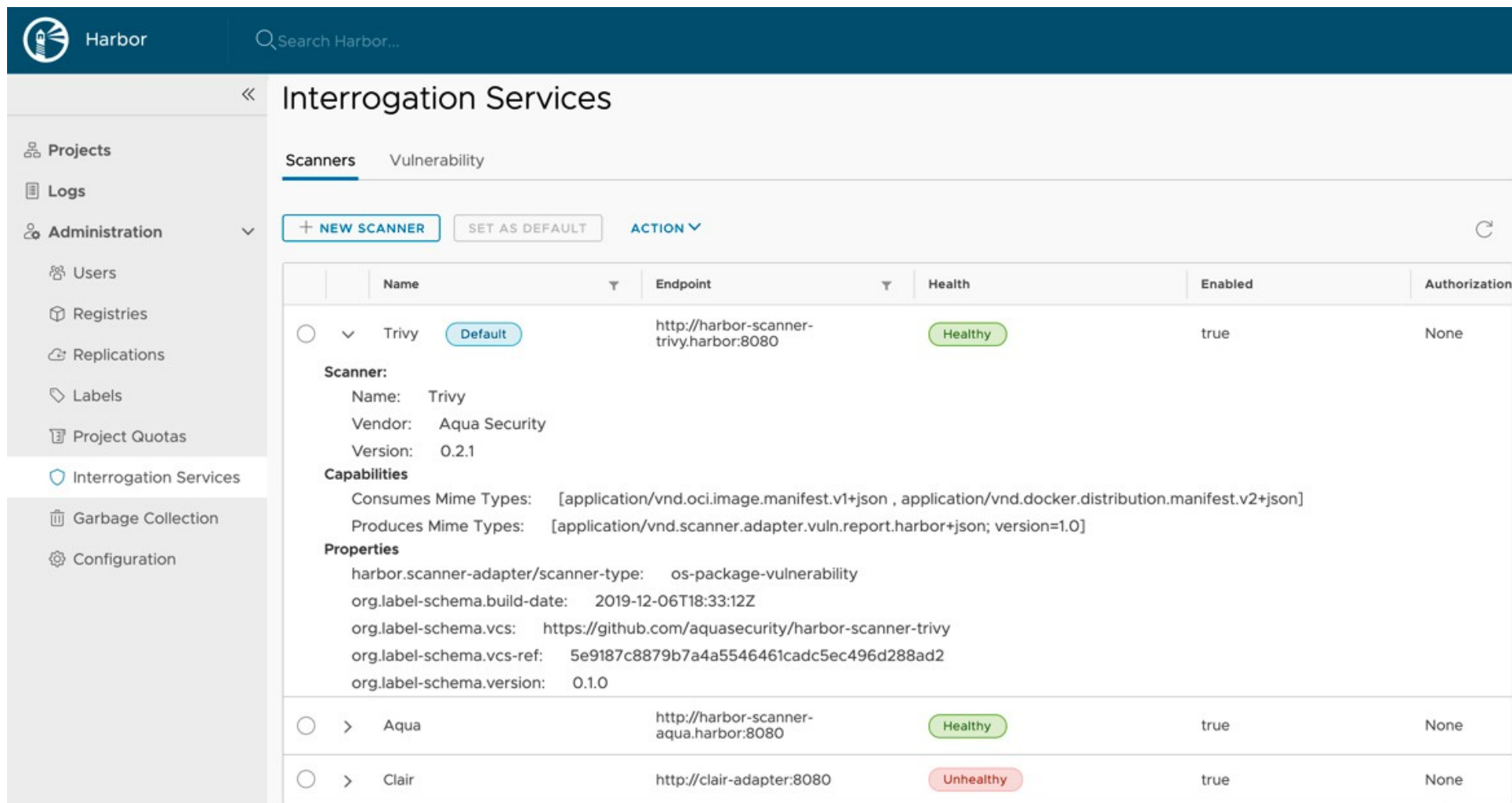
```
export DOCKER_CONTENT_TRUST=1
export DOCKER_CONTENT_TRUST_SERVER=https://<ip-address-of-your-server>
```

```
root@harbor:~] docker pull harbor-test.com/library/opensuse:42.2
No trust data for 42.2
```

Scanners

Available scanners :

- Clair (default)
- Trivy (native)
- Anchore
- DoSec



The screenshot shows the Harbor web interface for 'Interrogation Services'. The left sidebar contains navigation options: Projects, Logs, Administration (Users, Registries, Replications, Labels, Project Quotas), Interrogation Services (selected), Garbage Collection, and Configuration. The main content area is titled 'Interrogation Services' and has tabs for 'Scanners' and 'Vulnerability'. Below the tabs are buttons for '+ NEW SCANNER', 'SET AS DEFAULT', and 'ACTION'. A table lists the configured scanners:

	Name	Endpoint	Health	Enabled	Authorization
<input type="radio"/>	Trivy Default	http://harbor-scanner-trivy.harbor:8080	Healthy	true	None
Scanner: Name: Trivy Vendor: Aqua Security Version: 0.2.1 Capabilities Consumes Mime Types: [application/vnd.oci.image.manifest.v1+json , application/vnd.docker.distribution.manifest.v2+json] Produces Mime Types: [application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0] Properties harbor.scanner-adapter/scanner-type: os-package-vulnerability org.label-schema.build-date: 2019-12-06T18:33:12Z org.label-schema.vcs: https://github.com/aquasecurity/harbor-scanner-trivy org.label-schema.vcs-ref: 5e9187c8879b7a4a5546461cad5ec496d288ad2 org.label-schema.version: 0.1.0					
<input type="radio"/>	Aqua	http://harbor-scanner-aqua.harbor:8080	Healthy	true	None
<input type="radio"/>	Clair	http://clair-adapter:8080	Unhealthy	true	None

Users Management, quotas, garbage collection, main settings

Users

[+ NEW USER](#) [SET AS ADMIN](#) [ACTIONS](#)

<input type="checkbox"/>	Name	Administrator	Email	Registration time
<input type="checkbox"/>	toto	No	toto@test.com	3/11/20, 1:49 PM

1 - 1 of 1 items

Garbage Collection

[Garbage Collection](#) [History](#)

Current Schedule: Weekly ⓘ

[EDIT](#) [GC NOW](#)

Project Quotas

Default artifact count per project: unlimited [EDIT](#)

Default disk space per project: unlimited

	Project	Owner	Count	Storage
⋮	onap	admin	<div style="width: 100%;"><div style="width: 100%;">100 of unlimited</div></div>	<div style="width: 17.85%;"><div style="width: 17.85%;">17.85</div></div>
⋮	library	admin	<div style="width: 1%;"><div style="width: 1%;">1 of unlimited</div></div>	<div style="width: 59.1%;"><div style="width: 59.1%;">59.1M</div></div>

Configuration

[Authentication](#) [Email](#) [System Settings](#)

Auth Mode ⓘ [Database](#) ▾

Allow Self-Registration ⓘ

[SAVE](#) [CANCEL](#)

Replication rules

Edit Replication Rule

Name *

Description

Replication mode Push-based ⓘ Pull-based ⓘ

Source registry * ▾

Source resource filter

Name: ⓘ

Tag: ⓘ

Resource: ⓘ

Destination namespace ⓘ

Trigger Mode * ▾

Override ⓘ

Enable rule

< [Projects](#)

library

System Admin

[Summary](#) [Repositories](#) [Helm Charts](#)

<input type="checkbox"/>	Name
<input type="checkbox"/>	library/freeradius-server

API Swagger

Scan



GET

`/scans/all/metrics` Get the metrics of the latest scan all process



GET

`/repositories/{repo_name}/tags/{tag}/scan/{uuid}/log` Get scan log



GET

`/scans/schedule/metrics` Get the metrics of the latest scheduled scan all process



POST

`/repositories/{repo_name}/tags/{tag}/scan` Scan the image.

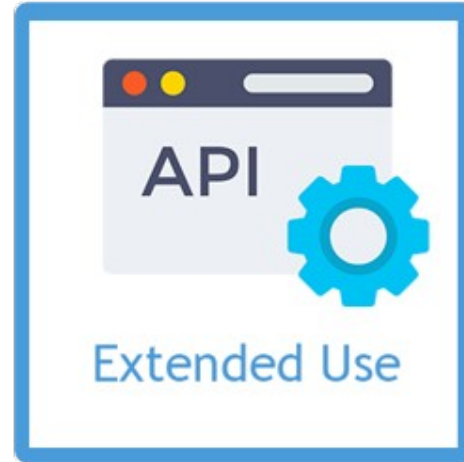


GET

`/repositories/{repo_name}/tags/{tag}/scan` Get the scan report



Extended Use

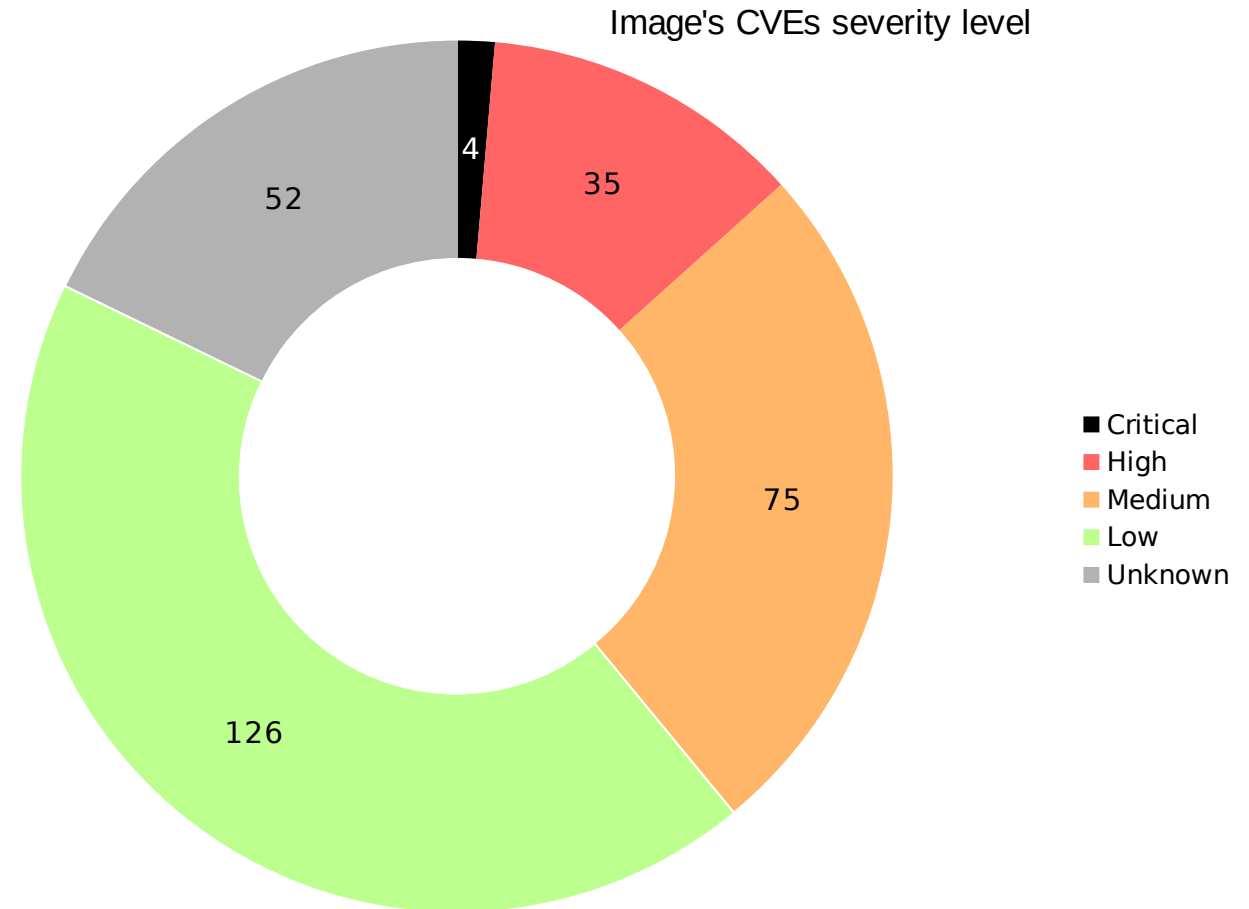


Security scan report

Collect CVE data about the platform's images

Display :

- Graphics about overall situation
- List of repositories, sorted by severity levels
- Sub-list of CVEs for each repositories, their description and fix



Webhook alerts

Image scan completed

IMAGE SCAN COMPLETED

Repository namespace name, repository name, tag scanned, image name, number of critical issues, number of major issues, number of minor issues, last scan status, scan completion time timestamp, vulnerability information (CVE ID description, link to CVE, criticality, URL for any fix), username of user who performed scan

```
▼ "scan_overview":
  ▼ "application/vnd.scanner.adapter.vuln.report.html":
    "report_id": "316b8602-691d-11ea-a774-427b9d69"
    "scan_status": "Success"
    "severity": "High"
    "duration": 4
    ► "summary": 3 properties
    "start_time": "2020-03-18T13:34:29.231976Z"
    "end_time": "2020-03-18T13:34:33.099684Z"
    ► "scanner": 3 properties
```

Details **POST** /

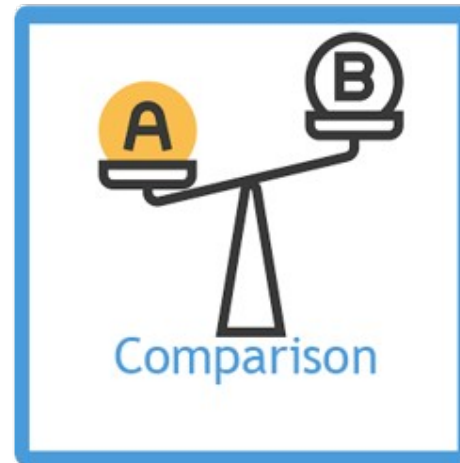
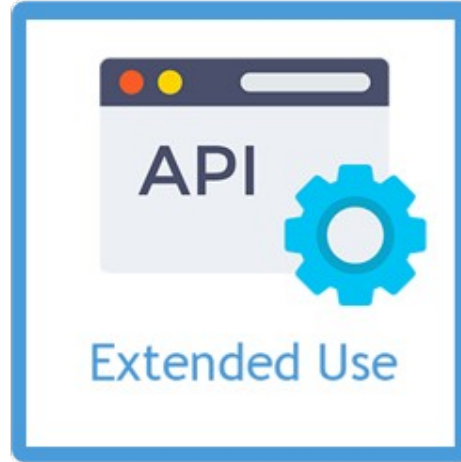
Headers ▶ (6) headers

Body

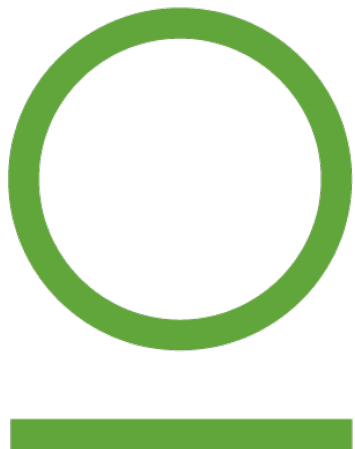
RAW PRETTY **STRUCTURED**

```
▼ "root":
  "type": "scanningCompleted"
  "occur_at": 1584538473
  "operator": "auto"
  ▼ "event_data":
    ▼ "resources":
      ▼ 0:
        "digest": "sha256:7e5e7ec375970ad8bbb63"
        "tag": "2.1.15"
        "resource_url": "core.harbor.onap.eu/on"
        ► "scan_overview": 1 property
    ▼ "repository":
      "name": "aaf_cass"
      "namespace": "onap"
      "repo_full_name": "onap/aaf_cass"
      "repo_type": "public"
```


Comparison



Other container registries



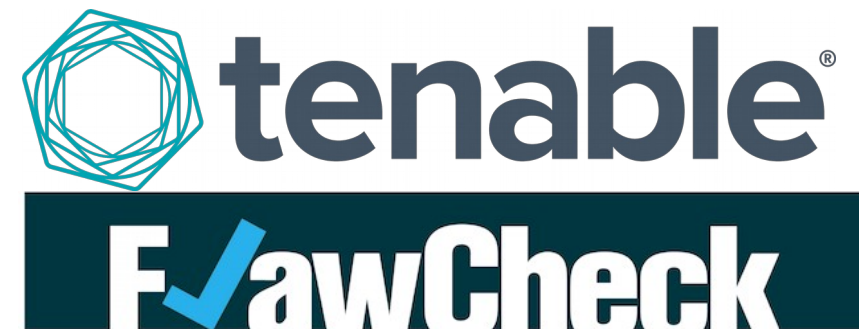
JFrog Artifactory

Not specialized in security
Can store Artifacts



CoreOS Quay

Not free
Focused on security
Manages deployment
Works with GitHub registries



Tenable (FlawCheck)

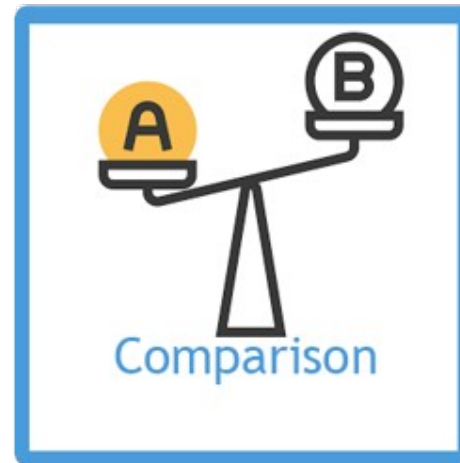
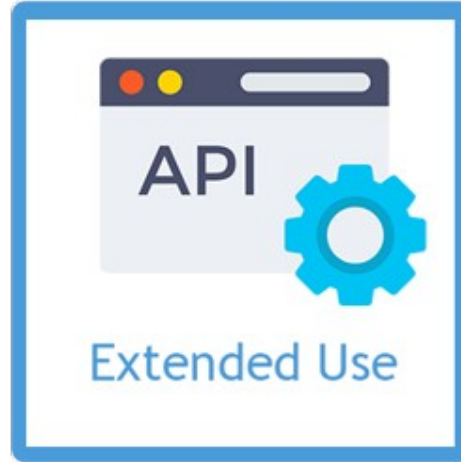
Not OpenSource
FlawCheck is now part of Tenable
which is a wide network security
solution (not only containers)

Demo

```
ubuntu@aio-by-os-infra-manager:~/custom_hook$ python3 hook.py
* Serving Flask app "hook" (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on http://0.0.0.0:5001/ (Press CTRL+C to quit)
```

Details	POST /
Headers	▶ (6) headers
Body	RAW PRETTY STRUCTURED
	<pre>▼ "root": "type": "scanningCompleted" "occur_at": 1584538473 "operator": "auto" ▼ "event_data": ▼ "resources": ▼ 0: "digest": "sha256:7e5e7ec375970ad8bbb63" "tag": "2.1.15" "resource_url": "core.harbor.onap.eu/on ▶ "scan_overview": 1 property ▼ "repository": "name": "aaf_cass" "namespace": "onap" "repo_full_name": "onap/aaf_cass" "repo_type": "public"</pre>

Conclusion



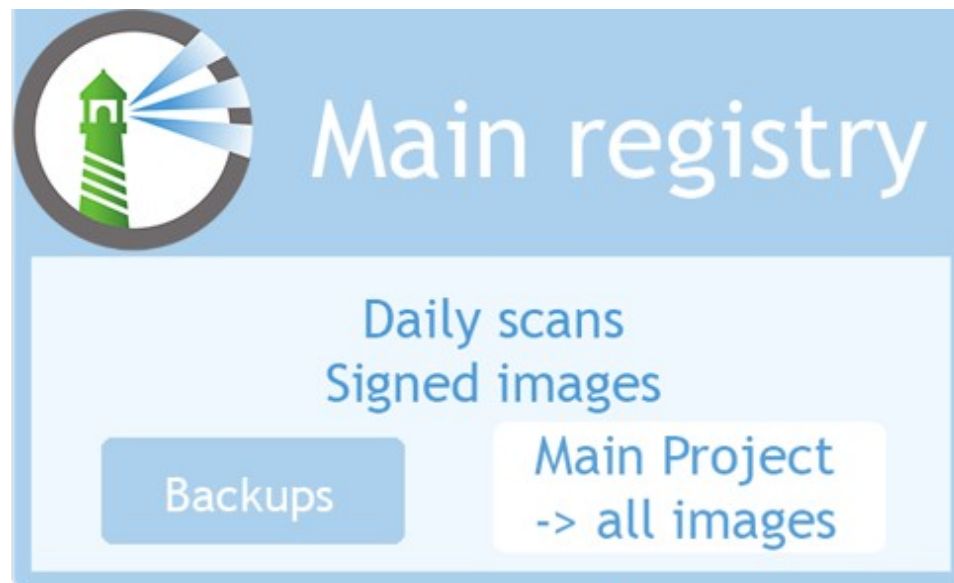
Maturity

Harbor Users



Replace Nexus3 with Harbor

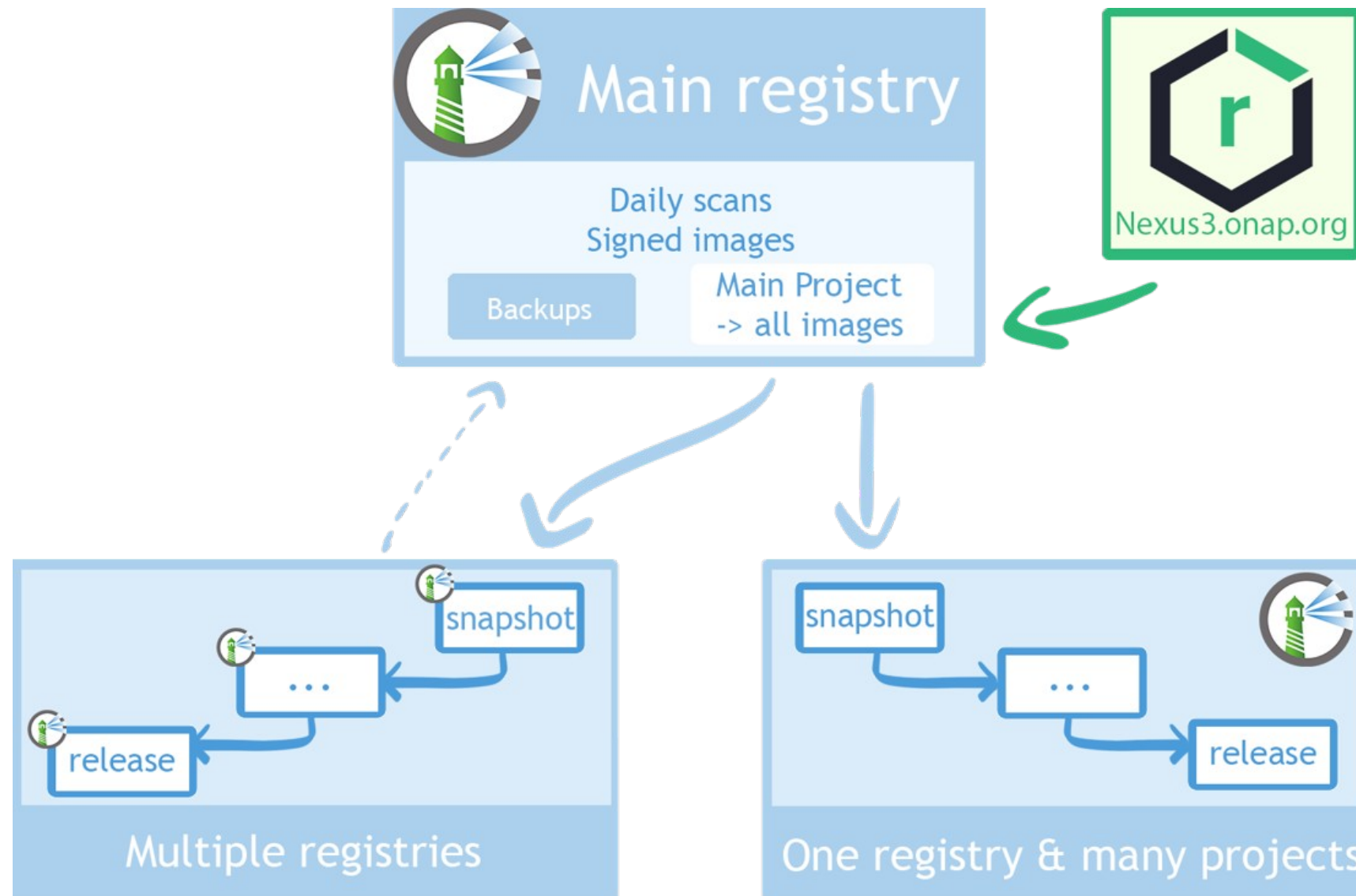
- You can schedule **daily or weekly scans** on every images
- **Backups** done easily with replication
- You can **sign** these images and ensure you are pulling the right image
- Accessible Webhook notifications for **real time events notifications**



Cascading projects

If many stages before release :

- **Precise and focused scan reports** for each stages
- **Easy backups** for each stages
- Clean way of **sorting projects**



Thanks

Harbor in the CNCF website :

Official Harbor website : goharbor.io

More questions ? solene.evesque@orange.com