KubeCon | CloudNativeCon

Europe 2024

Leveraging OCI 1.1 for Enhanced SBOM Integration and Vulnerability Scanning in Harbor

Shengwen Yu, Broadcom - Harbor

Anais Urlichs (for Teppei Fukuda), Aqua Security

Who are we?

Shengwen Yu

- Software Engineer at Broadcom
- Maintainer of Harbor with 3 + years in the cloud native space
- Doctor Who fan
- https://github.com/zyyw

Teppei Fukuda

- Open Source Software Engineer at Aqua Security
- Creator of Trivy
- Manga enthusiast
- https://github.com/knqyf263

Agenda

- Introduction and Background
- OCI spec v1.1.0 and Referrers API
- SBOM integration in Harbor
- Harbor pluggable-scanner-spec v1.2
- harbor-scanner-trivy Integration
- Demo
- Summary and Q&A

Harbor and Trivy Introduction

- CNCF Graduated Project
- 22k stars on GitHub
- Accepted into the CNCF in 2018
- website: goharbor.io

- Open Source Security Scanner
- 21k stars on GitHub
- Founded by Teppei
- website: trivy.dev

Introduction and Background

SBOMs & the Value of Investing in SBOM Generation

- Reduce costs of security incidents
- Better understanding of Software Supply Chain

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

Total cost of a data breach

Figure 1. Measured in USD millions

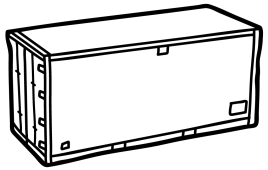
Source: IBM Cost of data breach report 2023

Per-record cost of a data breach

Figure 2. Measured in USD

SBOMs and OCI Registries

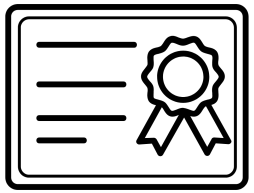
Artifacts



Container Image

Deployment Chart

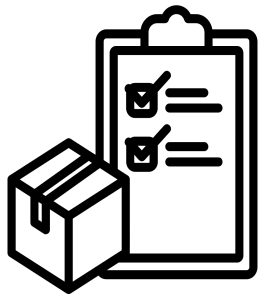
Signature



Attestation

"The Open Container Initiative (OCI) defines the specifications and standards for container technologies. This includes the API for working with container registries, known formally as the OCI Distribution Specification."

SBOMs and OCI Registries

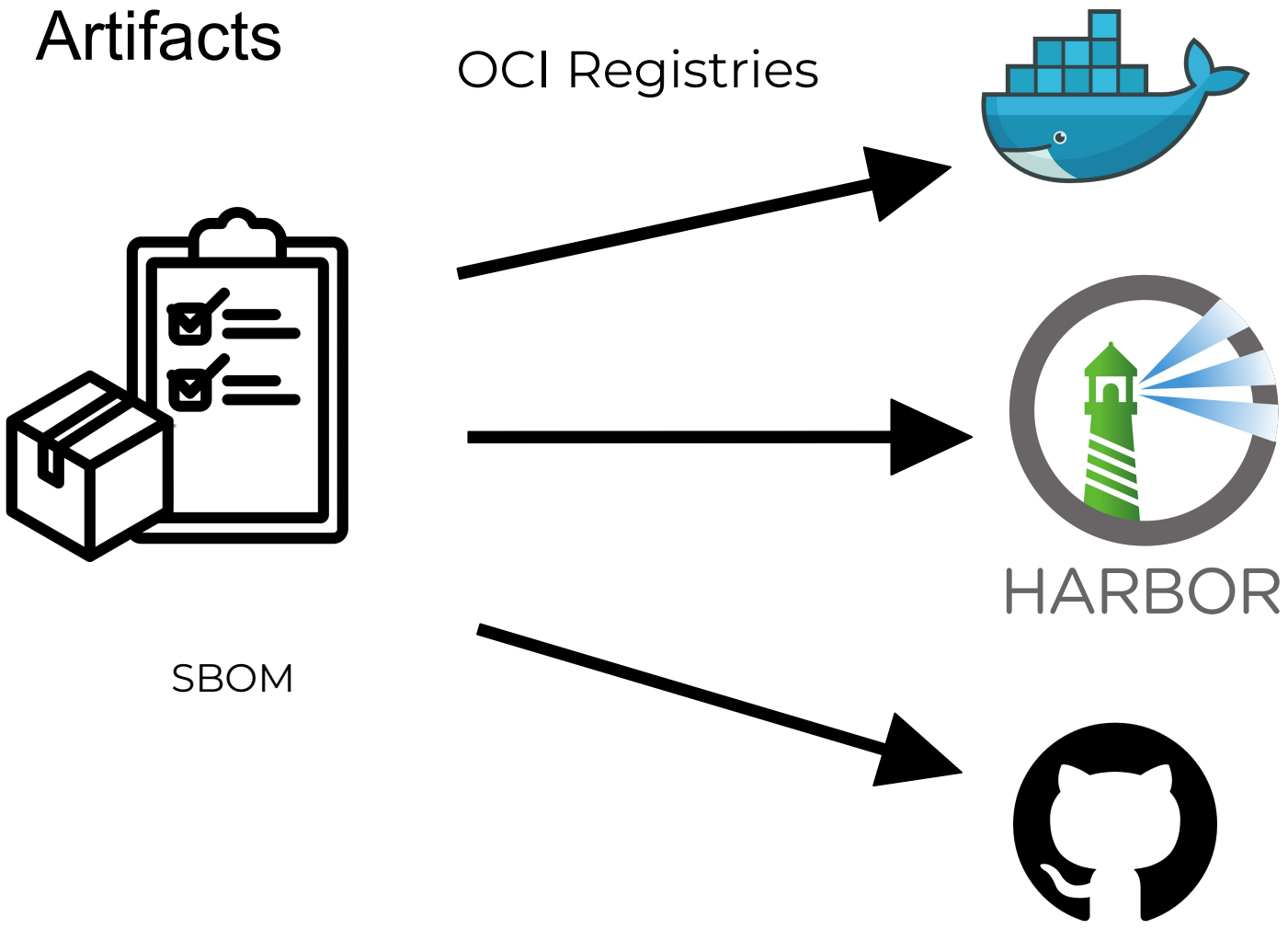


SBOM

```
❯ trivy image --format spdx-json --output result.json alpine:3.15.5

❯ cat result.json
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "alpine:3.15.5",
  "documentNamespace": "http://aquasecurity.github.io/trivy/container_image/
alpine:3.15.5-943cb918-0031-4fb3-af5b-19591d58ae0a",
  "creationInfo": {
    "creators": [
      "Organization: aquasecurity",
      "Tool: trivy-0.49.1"
    ],
    "created": "2024-03-07T15:36:59Z"
  },
  "packages": [
    {
      "name": "alpine",
      "SPDXID": "SPDXRef-OperatingSystem-e203598d7c09a662",
      "versionInfo": "3.15.5",
      "downloadLocation": "NONE",
      "filesAnalyzed": false,
      "primaryPackagePurpose": "OPERATING-SYSTEM"
    },
    {
      "name": "alpine-baselayout",
      "SPDXID": "SPDXRef-Package-e83565c0cc4a6e11",
      "versionInfo": "3.2.0-r18",
```

SBOMs and OCI Registries



With OCI v1.0, Registries cannot correlate resources e.g. SBOM to Container Image.

For that they need OCI v1.1.0

OCI spec v1.1.0 and Referrers API

Endpoints

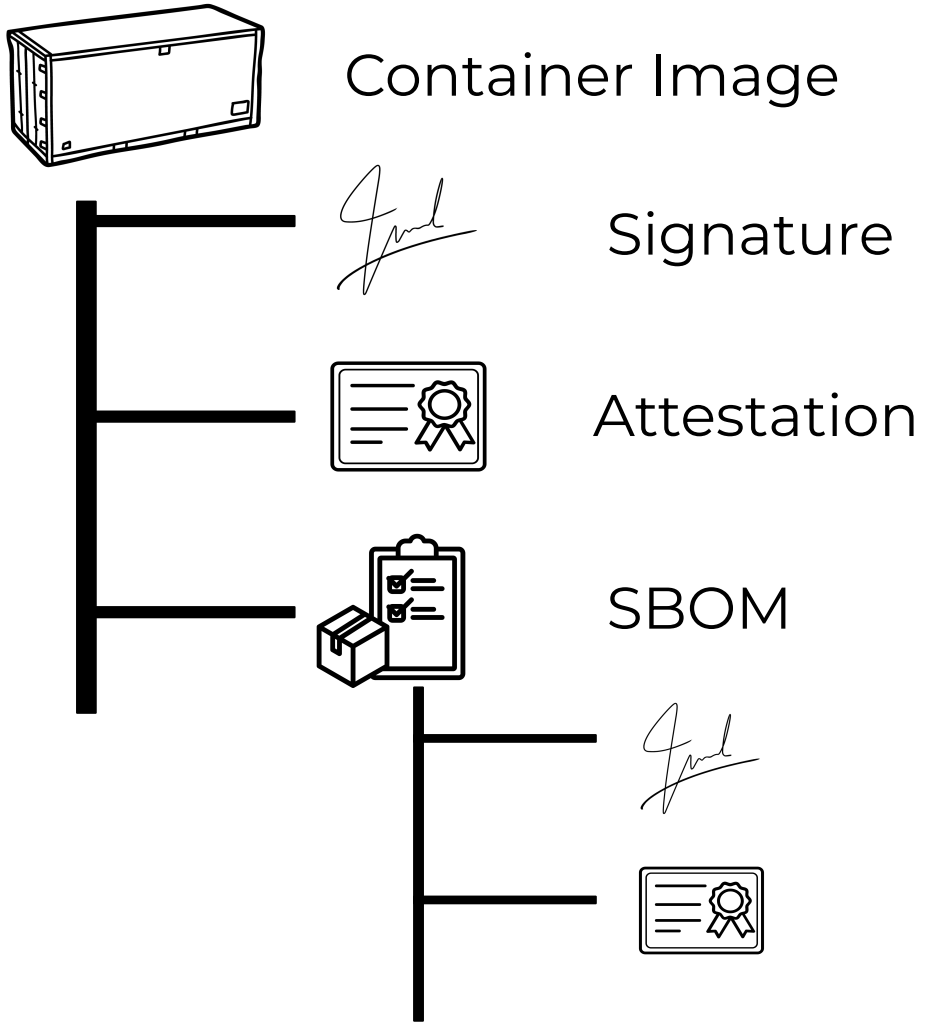
ID	Method	API Endpoint	Success	Failure
end-1	`GET`	`/v2/`	`200`	`404` / `401`
end-2	`GET` / `HEAD`	`/v2/<name>/blobs/<digest>`	`200`	`404`
end-3	`GET` / `HEAD`	`/v2/<name>/manifests/<reference>`	`200`	`404`
end-4a	`POST`	`/v2/<name>/blobs/uploads/`	`202`	`404`
end-4b	`POST`	`/v2/<name>/blobs/uploads/?digest=<digest>`	`201` / `202`	`404` / `400`
end-5	`PATCH`	`/v2/<name>/blobs/uploads/<reference>`	`202`	`404` / `416`
end-6	`PUT`	`/v2/<name>/blobs/uploads/<reference>?digest=<digest>`	`201`	`404` / `400`
end-7	`PUT`	`/v2/<name>/manifests/<reference>`	`201`	`404`
end-8a	`GET`	`/v2/<name>/tags/list`	`200`	`404`
end-8b	`GET`	`/v2/<name>/tags/list?n=<integer>&last=<integer>`	`200`	`404`
end-9	`DELETE`	`/v2/<name>/manifests/<reference>`	`202`	`404` / `400` / `405`
end-10	`DELETE`	`/v2/<name>/blobs/<digest>`	`202`	`404` / `405`
end-11	`POST`	`/v2/<name>/blobs/uploads/?mount=<digest>&from=<other_name>`	`201`	`404`
end-12a	`GET`	`/v2/<name>/referrers/<digest>`	`200`	`404` / `400`
end-12b	`GET`	`/v2/<name>/referrers/<digest>?artifactType=<artifactType>`	`200`	`404` / `400`
end-13	`GET`	`/v2/<name>/blobs/uploads/<reference>`	`204`	`404`

Source

OCI spec v1.1.0 and Referrers API

Endpoints [Source]

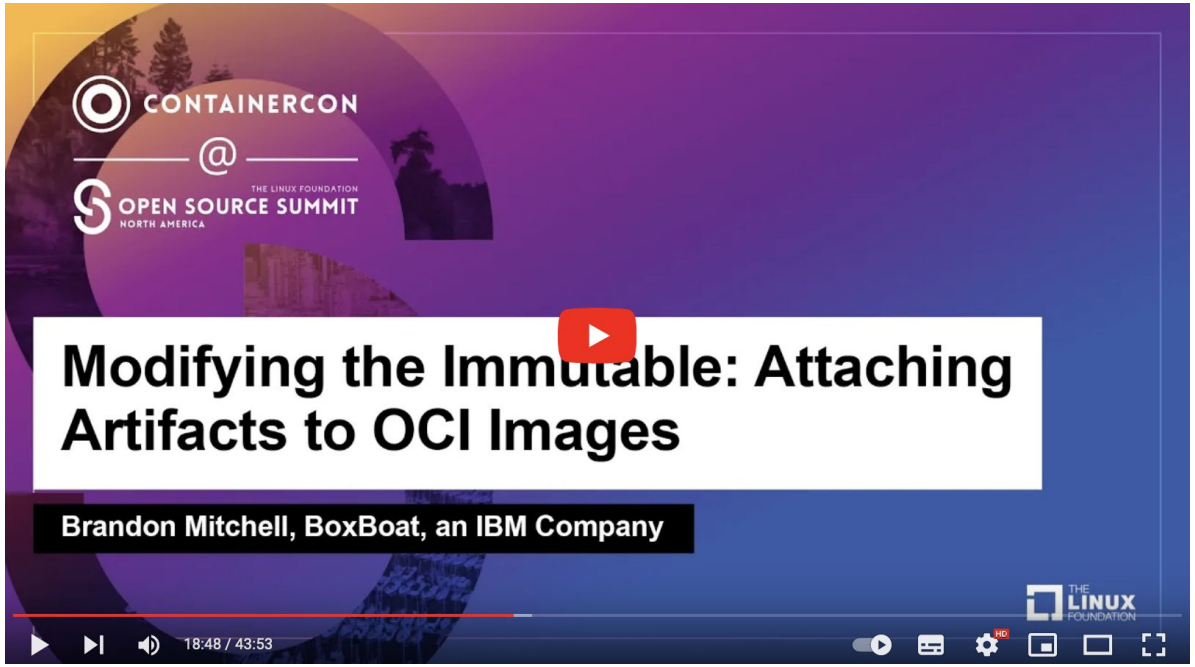
ID	Method	API Endpoint	Success	Failure
end-1	`GET`	`/v2/`	`200`	`404` / `401`
end-2	`GET` / `HEAD`	`/v2/<name>/blobs/<digest>`	`200`	`404`
end-3	`GET` / `HEAD`	`/v2/<name>/manifests/<reference>`	`200`	`404`
end-4a	`POST`	`/v2/<name>/blobs/uploads/`	`202`	`404`
end-4b	`POST`	`/v2/<name>/blobs/uploads/?digest=<digest>`	`201` / `202`	`404` / `400`
end-5	`PATCH`	`/v2/<name>/blobs/uploads/<reference>`	`202`	`404` / `416`
end-6	`PUT`	`/v2/<name>/blobs/uploads/<reference>?digest=<digest>`	`201`	`404` / `400`
end-7	`PUT`	`/v2/<name>/manifests/<reference>`	`201`	`404`
end-8a	`GET`	`/v2/<name>/tags/list`	`200`	`404`
end-8b	`GET`	`/v2/<name>/tags/list?n=<integer>&last=<integer>`	`200`	`404`
end-9	`DELETE`	`/v2/<name>/manifests/<reference>`	`202`	`404` / `400` / `405`
end-10	`DELETE`	`/v2/<name>/blobs/<digest>`	`202`	`404` / `405`
end-11	`POST`	`/v2/<name>/blobs/uploads/?mount=<digest>&from=<other_name>`	`201`	`404`
end-12a	`GET`	`/v2/<name>/referrers/<digest>`	`200`	`404` / `400`
end-12b	`GET`	`/v2/<name>/referrers/<digest>?artifactType=<artifactType>`	`200`	`404` / `400`
end-13	`GET`	`/v2/<name>/blobs/uploads/<reference>`	`204`	`404`



OCI spec v1.1.0 and Referrers API

Link

Link



SBOM integration in Harbor

One concept :

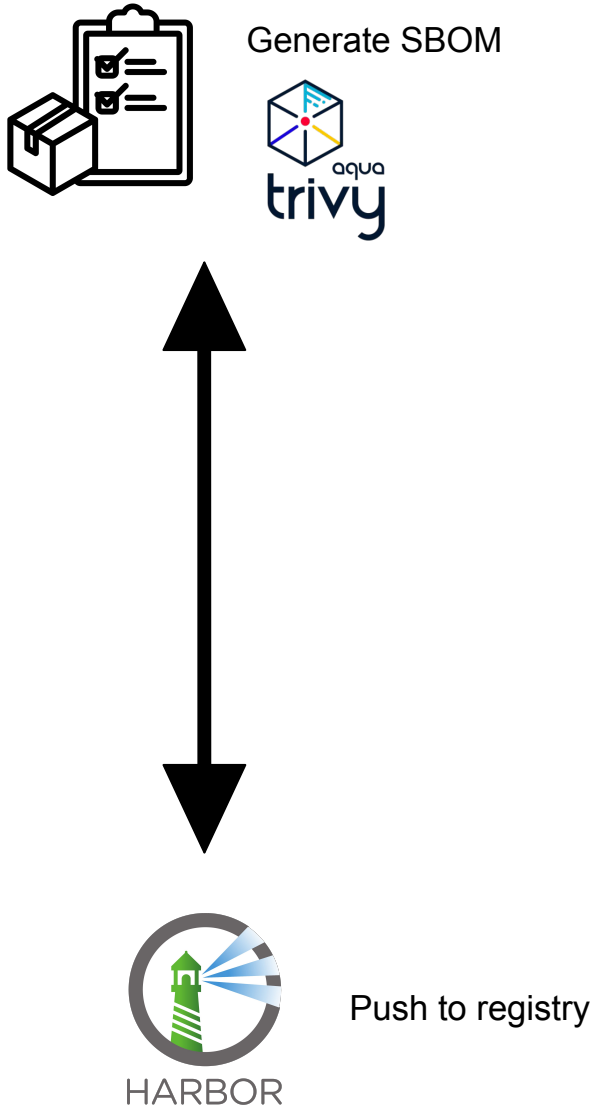
- Accessory

Two methods - associate an SBOM file to an artifact

- **Manually** push an SBOM file using *third-party CLI tools*
  - trivy
  - oras
- SBOM **auto-generation** on artifact push to Harbor

One planned feature

- Scan SBOM for vulnerabilities



SBOM integration in Harbor

Accessory

What is an accessory?

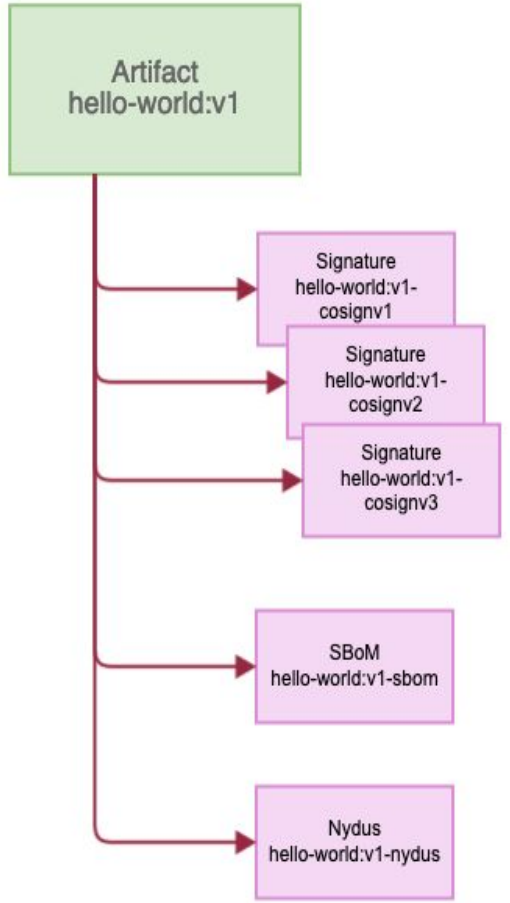
- Just like an ordinary OCI artifact
- **But** linked to a subject artifact via **subject descriptor**
- **artifact_accessory** table storing the relationship between subject artifact and accessory
- N:1, one single subject artifact can have multiple accessories

Why accessory?

- Extend Harbor's capabilities of storing extra data
  - SBOM
  - Signature: cosign, notation
- Incorporate OCI spec 1.1 and referrers API

Accessory Life-Cycle management

- Delete independently
- Garbage collected along with its subject artifact
- Replicated together with its subject artifact



References:

- https://github.com/goharbor/community/blob/main/proposals/new/accessory.md
- https://github.com/goharbor/community/blob/main/proposals/new/distribution-1.1-adoption.md

Associate an SBOM file to an artifact: Manually

Generate an SBOM file with trivy:

```
~$ trivy image --format spdx-json --output alpine.spdx.json alpine:3.15.5
~$ trivy image --format cyclonedx --output alpine.cyclonedx.json alpine:3.15.5
```

Trivy:

```
~$ trivy referrer put --insecure --subject 10.202.250.19/library/alpine:3.15.5  -f alpine.spdx.json
```

Oras:

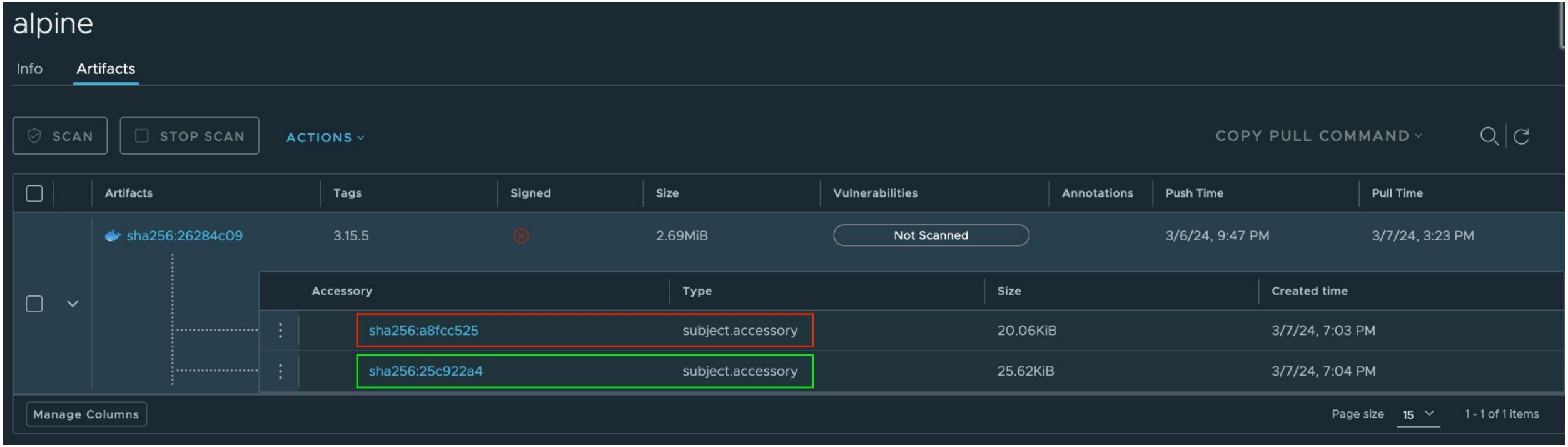
```
~$ oras attach 10.202.250.19/library/alpine:3.15.5 --artifact-type sbom/example alpine.cyclonedx.json
```

SBOM integration in Harbor

KubeCon CloudNativeCon Europe 2024

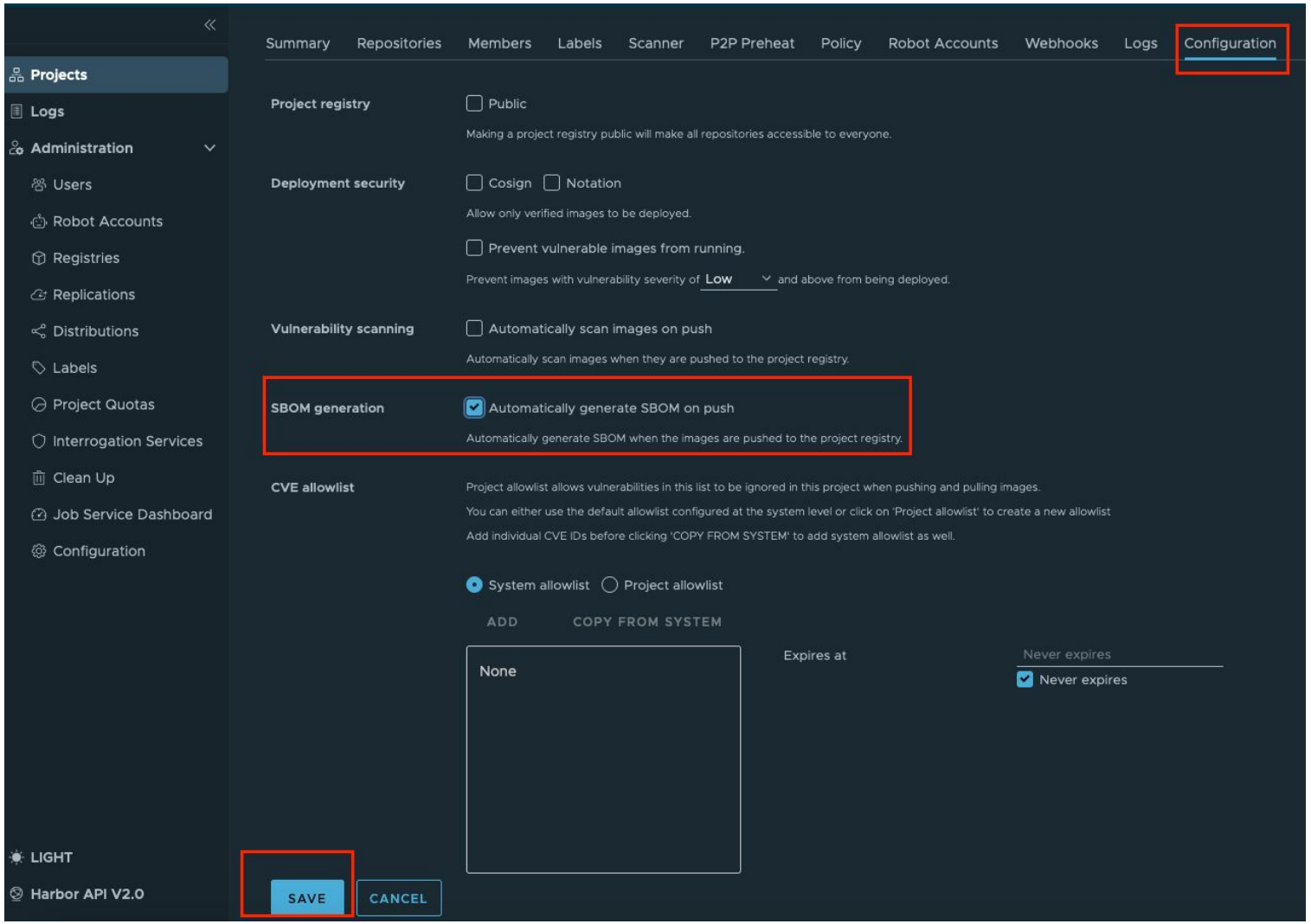
Associate an SBOM file to an artifact: Manually

```
ubuntu@shengwen:~/kubecon-2024/sbom-files/alpine-3.15.5$ IMAGE=10.202.250.194/library/alpine:3.15.5
ubuntu@shengwen:~/kubecon-2024/sbom-files/alpine-3.15.5$ oras discover -o tree $IMAGE
10.202.250.194/library/alpine@sha256:26284c09912acfc5497b462c5da8a2cd14e01b4f3ffa876596f5289dd8eab7f2
├── application/spdx+json
│   └── sha256:a8fcc525fc114f66993c8c2decd1e519314b67554000e86bead93c4ff44bbf73
└── application/vnd.oci.empty.v1+json
    └── sha256:25c922a4c8975597cc1fac87e5a04d65b68159018f4e6826d892d19b38eded66
```



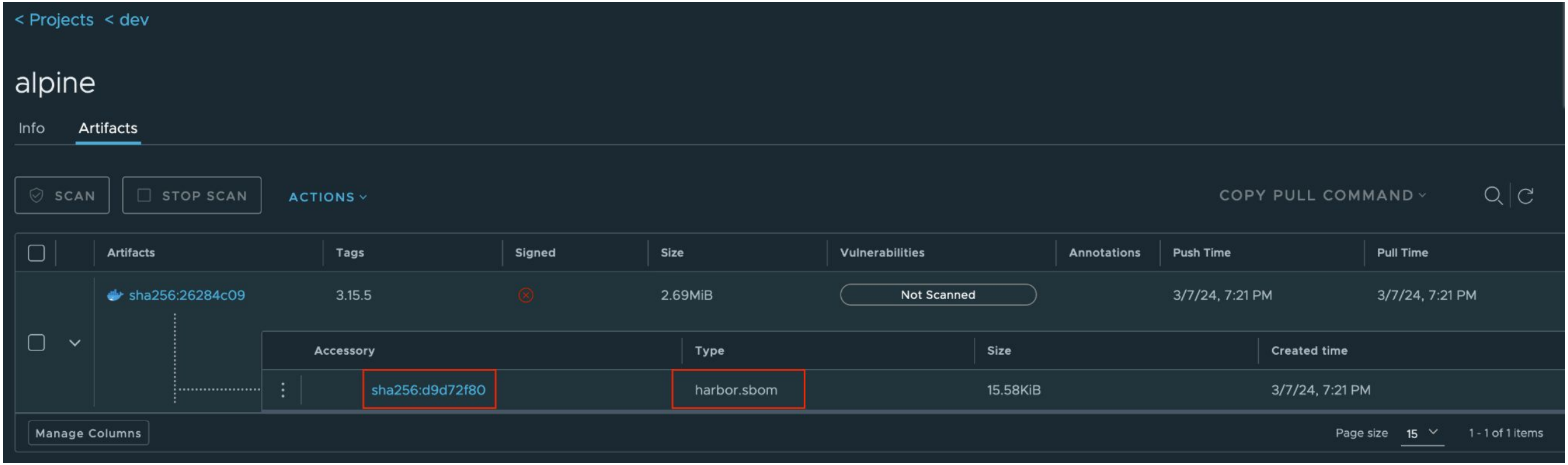
SBOM integration in Harbor

Associate an SBOM file to an artifact: Auto-generation



SBOM integration in Harbor

Associate an SBOM file to an artifact: Auto-generation



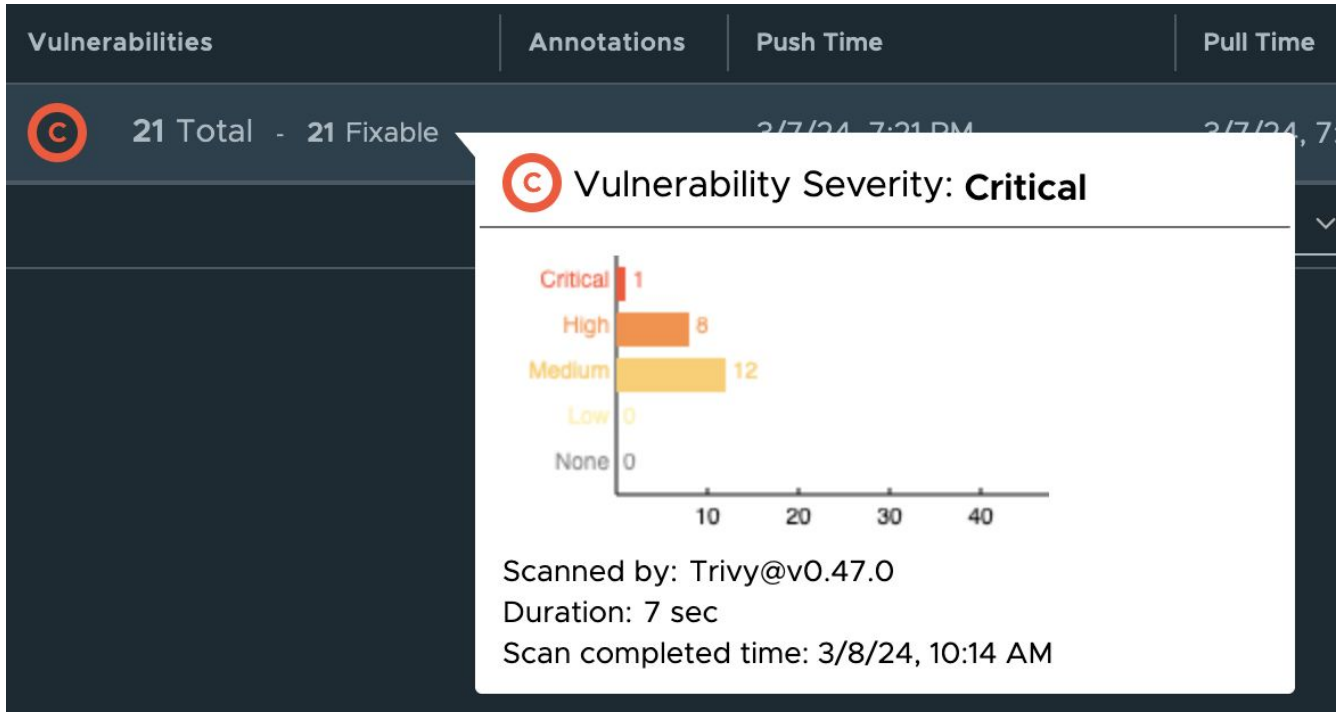
Scan SBOM for vulnerabilities

Feature planned:

- Configurable via system settings
- Only scan the SBOM automatically generated via Harbor built-in trivy-adapter
- Fallback to scan the subject artifact itself if no SBOM presents

Benefits:

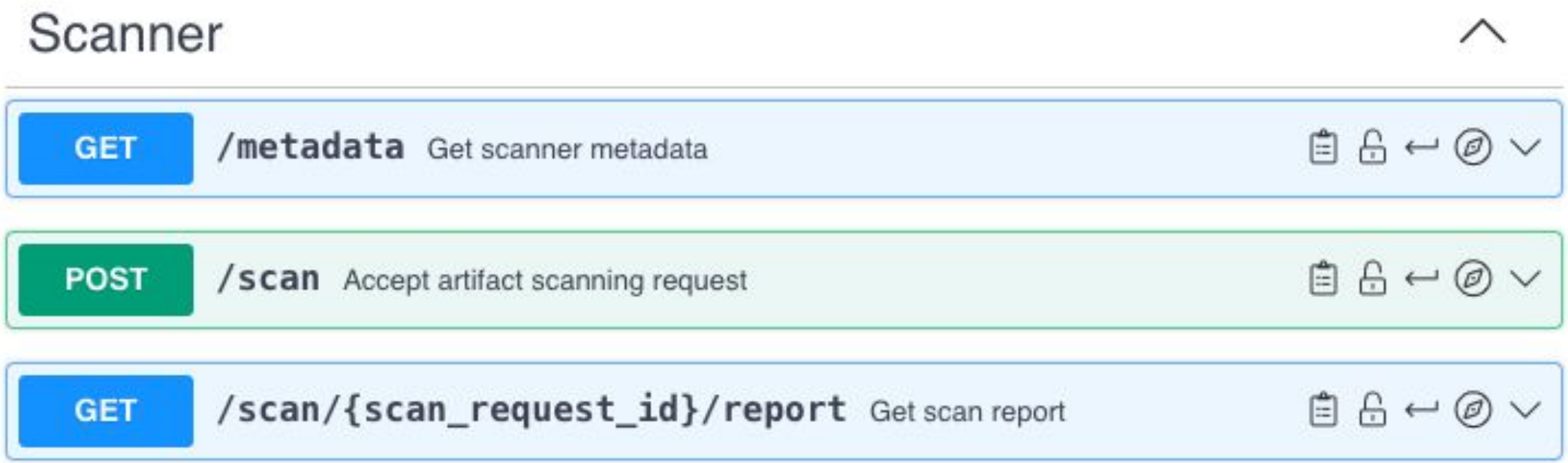
- Increasing efficiency
- Comprehensive visibility



Harbor pluggable-scanner-spec v1.2

KubeCon CloudNativeCon Europe 2024

API Overview



References:

- https://github.com/goharbor/pluggable-scanner-spec/blob/master/api/spec/scanner-adapter-openapi-v1.2.yaml

Harbor pluggable-scanner-spec v1.2

/metadata

```
docker exec -it trivy-adapter curl localhost:8080/api/v1/metadata | jless
```

```
1 ▼     {scanner: {…}, capabilities: […], properties: {…}}
2   ▷ scanner:      {name: "Trivy", vendor: "Aqua Security", version: "v0.47.0"}
7   ▷ capabilities:      [{…}, {…}]
35  ▷ properties:      {"env.SCANNER_TRIVY_DEBUG_MODE": "false", "env.SCANNER_TRI
```

```
"scanner": {
  "name": "Trivy",
  "vendor": "Aqua Security",
  "version": "v0.47.0"
},
```

Harbor pluggable-scanner-spec v1.2

/metadata

```
"properties": {
  "env.SCANNER_TRIVY_DEBUG_MODE": "false",
  "env.SCANNER_TRIVY_IGNORE_UNFIXED": "false",
  "env.SCANNER_TRIVY_INSECURE": "false",
  "env.SCANNER_TRIVY_OFFLINE_SCAN": "false",
  "env.SCANNER_TRIVY_SECURITY_CHECKS": "vuln",
  "env.SCANNER_TRIVY_SEVERITY": "UNKNOWN,LOW,MEDIUM,HIGH,CRITICAL",
  "env.SCANNER_TRIVY_SKIP_JAVA_DB_UPDATE": "false",
  "env.SCANNER_TRIVY_SKIP_UPDATE": "false",
  "env.SCANNER_TRIVY_TIMEOUT": "5m0s",
  "env.SCANNER_TRIVY_VULN_TYPE": "os,library",
  "harbor.scanner-adapter/scanner-type": "os-package-vulnerability",
  "harbor.scanner-adapter/vulnerability-database-next-update-at": "20
  "harbor.scanner-adapter/vulnerability-database-updated-at": "2024-0
  "org.label-schema.build-date": "unknown",
  "org.label-schema.vcs": "https://github.com/aquasecurity/harbor-sca
  "org.label-schema.vcs-ref": "none",
  "org.label-schema.version": "dev"
}
```

```
"capabilities": [
  {
    "type": "vulnerability",
    "consumes_mime_types": [
      "application/vnd.oci.image.manifest.v1+json",
      "application/vnd.docker.distribution.manifest.v2+json"
    ],
    "produces_mime_types": [
      "application/vnd.security.vulnerability.report; version=1.1"
    ]
  },
  {
    "type": "sbom",
    "consumes_mime_types": [
      "application/vnd.oci.image.manifest.v1+json",
      "application/vnd.docker.distribution.manifest.v2+json"
    ],
    "produces_mime_types": [
      "application/vnd.security.sbom.report+json; version=1.0"
    ],
    "additional_attributes": {
      "sbom_media_types": [
        "application/spdx+json",
        "application/vnd.cyclonedx+json"
      ]
    }
  }
],
```

Harbor pluggable-scanner-spec v1.2

/scan

ScanRequest

```
{
    "registry": {
        "url":"https://harbor.example.com",
        "authorization": "Basic xxxxxxx"
    },
    "artifact": {
        "repository": "library/alpine",
        "digest": "sha256:26284c09912acfc5497b462c5da8a2cd14e01b4f3ffa876596f5289dd8eab7f2",
        "tag": "3.15.5",
        "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
    },
    "enabled_capabilities": [{
        "type": "sbom",
        "produces_mime_types": [
            "application/vnd.security.sbom.report+json; version=1.0"
        ],
        "parameters": {
            "sbom_media_types": ["application/spdx+json"]
        }
    }]
}
```

Harbor pluggable-scanner-spec v1.2

/scan

ScanResponse → 202

```
{
    "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
}
```

ErrorResponse →

400 - Bad request. e.g.: Received invalid JSON or wrong type of JSON values.
422 - Received invalid field.
500 - Internal server error.
501 - The scanner has no capability to handle this scan request.

Harbor pluggable-scanner-spec v1.2

/scan/{scan_request_id}/report

Query Path:

Vulnerability

GET /api/v1/scan/{scan_request_id}/report

SBOM

GET /api/v1/scan/{scan_request_id}/report?sbom_media_type=application/spdx+json (url encode)

Accept Header:

Vulnerability

Accept: application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0
Accept: application/vnd.security.vulnerability.report; version=1.1
Accept: application/vnd.scanner.adapter.vuln.report.raw

SBOM

Accept: application/vnd.security.sbom.report+json; version=1.0

Harbor pluggable-scanner-spec v1.2

/scan/{scan_request_id}/report ?sbom_media_type=application/spdx+json


```
{
  "generated_at": "2021-03-09T11:40:28.154072066Z",
  "artifact": {
     "repository": "library/alpine",
     "digest": "sha256:26284c09912acfc5497b462c5da8a2cd14e01b4f3ffa876596f5289dd8eab7f2",
     "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
  },
  "scanner": {
      "name": "Trivy",
      "vendor": "Aqua Security",
      "version": "v0.47.0"
  },
  "vendor_attributes": {
    "spec-version": "1.5",
    "create-by": "trivy",
    "create-time": "1695368355"
  },
  "media_type": "application/spdx+json",
  "sbom": {
    "spdxVersion": "SPDX-2.2",
    ...
  }
}
```

Quick Recap: harbor-scanner-trivy Integration

README | Code of conduct | Apache-2.0 license

release v0.30.22 GitHub Build Actions go report A+ license Apache-2.0 docker pulls / aquasec 66k
docker pulls / goharbor 4.5M

Harbor Scanner Adapter for Trivy

The Harbor Scanner Adapter for Trivy is a service that translates the Harbor scanning API into Trivy commands and allows Harbor to use Trivy for providing vulnerability reports on images stored in Harbor registry as part of its vulnerability scan feature.

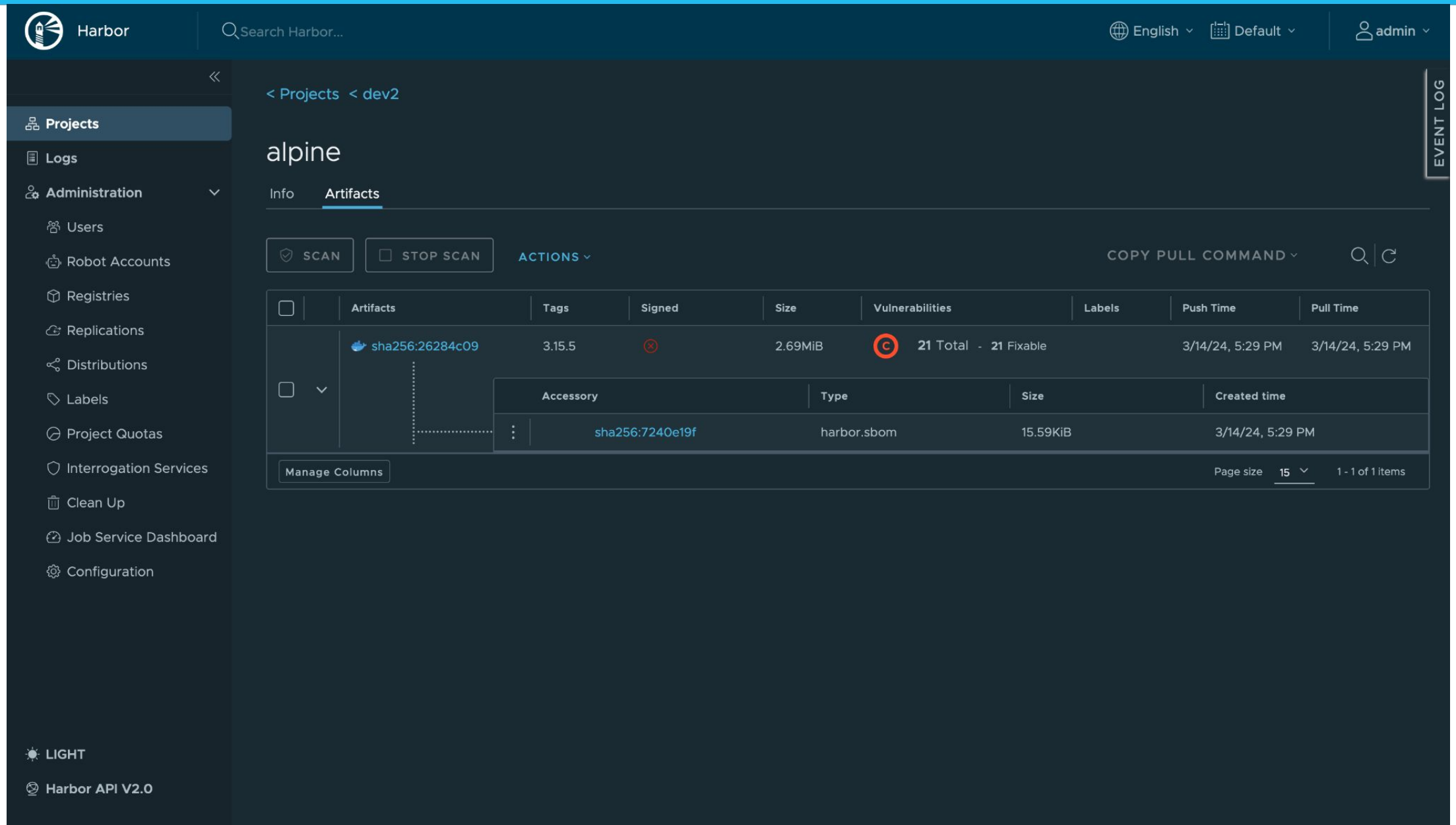
Harbor asks Trivy:
"What capabilities do you have?"

The harbor-scanner-trivy tells Harbor:
"Here are the capabilities I implement:
SBOM, vulnerability scanning"

pluggable-scanner-spec
v1.2

harbor-scanner-trivy
Implementing the
pluggable-scanner-spec
v1.2

Demo


Harbor
Search Harbor...
English
Default
admin
< Projects < dev2
alpine
Info
Artifacts
SCAN
STOP SCAN
ACTIONS
COPY PULL COMMAND
EVENT LOG
Projects
Logs
Administration
Users
Robot Accounts
Registries
Replications
Distributions
Labels
Project Quotas
Interrogation Services
Clean Up
Job Service Dashboard
Configuration
LIGHT
Harbor API V2.0
Artifacts
Tags
Signed
Size
Vulnerabilities
Labels
Push Time
Pull Time
sha256:26284c09
3.15.5
2.69MiB
21 Total - 21 Fixable
3/14/24, 5:29 PM
3/14/24, 5:29 PM
Accessory
Type
Size
Created time
sha256:7240e19f
harbor.sbom
15.59KiB
3/14/24, 5:29 PM
Manage Columns
Page size 15
1 - 1 of 1 items

Resources

- OCI image-spec v1.1.0: https://github.com/opencontainers/image-spec/releases/tag/v1.1.0
- OCI distribution-spec v1.1.0: https://github.com/opencontainers/distribution-spec/releases/tag/v1.1.0
- Harbor scanner-adapter-spec v1.2: https://github.com/goharbor/pluggable-scanner-spec/blob/master/api/spec/scanner-adapter-openapi-v1.2.yaml
- Harbor Scanner Adapter for Trivy: https://github.com/aquasecurity/harbor-scanner-trivy
- trivy-plugin-referrer: https://github.com/aquasecurity/trivy-plugin-referrer
- Harbor accessory proposal: https://github.com/goharbor/community/blob/main/proposals/new/accessory.md
- Harbor adoption for distribution 1.1: https://github.com/goharbor/community/blob/main/proposals/new/distribution-1.1-adoption.md

Questions?

https://cloud-native.slack.com/messages/harbor

Thank You !