
KubeCon
CloudNativeCon
OPEN SOURCE SUMMIT
China 2023

Advancements in Harbor

Yan Wang, VMware
Chenyu Zhang, VMware

Agenda

- Introduction
- Feature Recap
  - Security Hub
  - OCI Distribution Spec v1.1
  - Other Enhancements
- Demo
- Future Outlook
- Collaboration

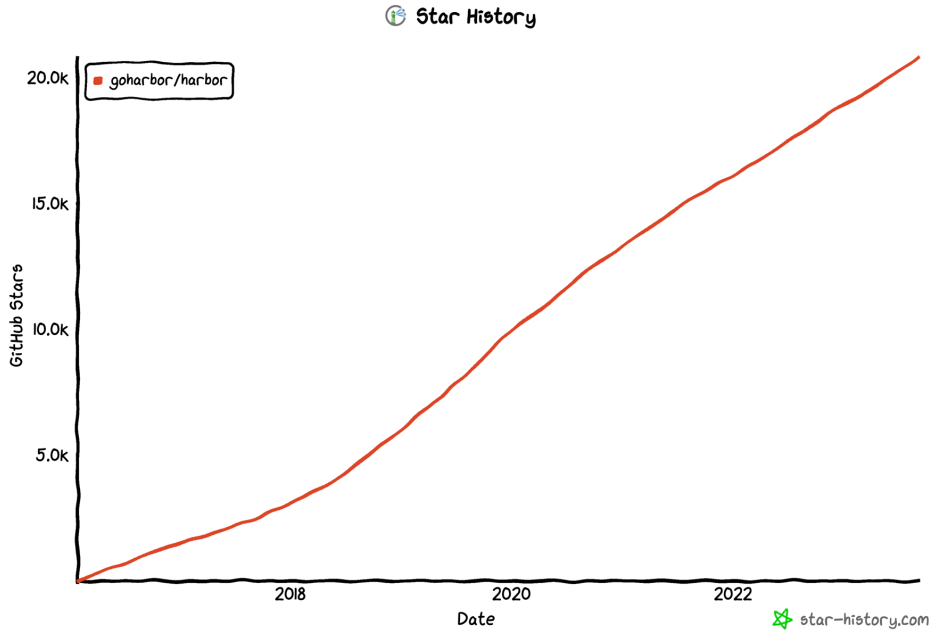
Introduction

HARBOR

What is Harbor?

Harbor is an open source registry that secures artifacts with policies and role-based access control, ensures images are scanned and free from vulnerabilities, and signs images as trusted. Harbor, a CNCF Graduated project, delivers compliance, performance, and interoperability to help you consistently and securely manage artifacts across cloud native compute platforms like Kubernetes and Docker.

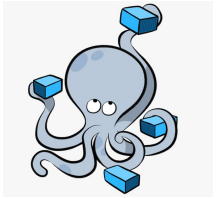
https://goharbor.io



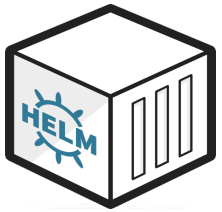
Key Features

- Access Control
  - RBAC, Project Isolation
- Artifact Distribution
  - Replication, Proxy Cache, P2P Preheat
- Security & Compliance
  - Security Hub, Vulnerability Scan, Artifact Signature, CVE Export
- Policy & Maintainability
  - Quota, Immutability, Retention, Garbage Collection, Log Rotation
- Extensibility
  - OIDC/LDAP Authentication, Webhook, Pluggable Scanner, Robot Account

Installation



Docker Compose



Helm Chart

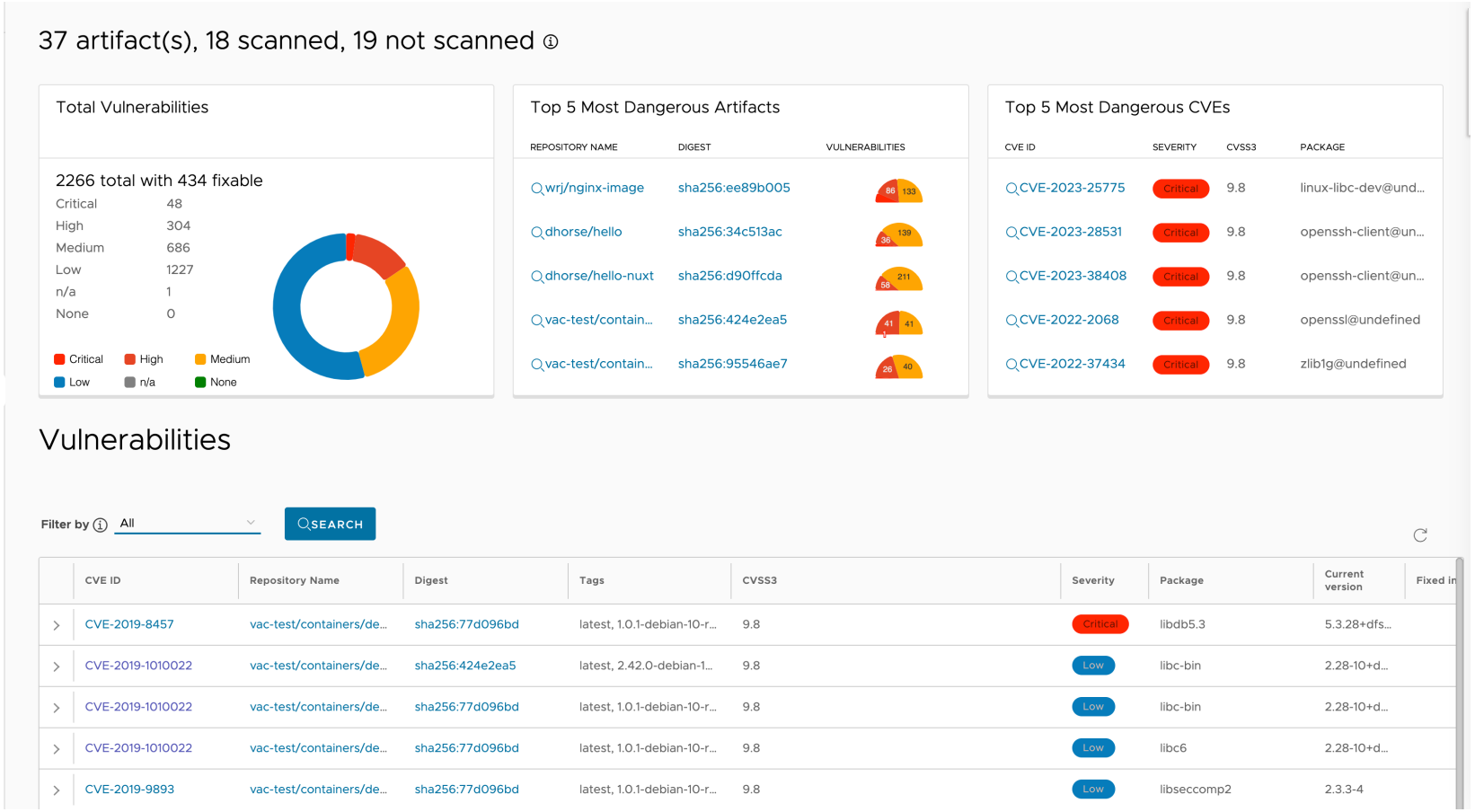
Kubernetes Operator

Architecture

Feature

Security Hub

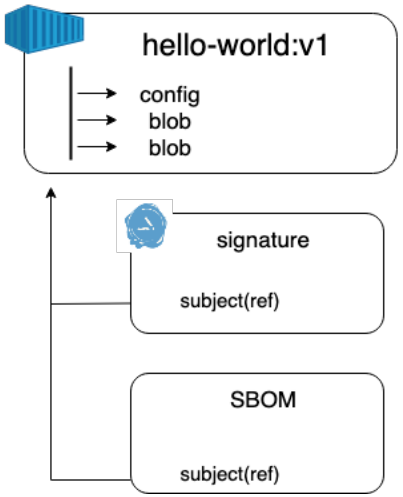
- Provide a comprehensive and centralized overview of the present security status of artifacts stored within the Harbor.
- Highlight top dangerous artifacts and CVEs.
- Search vulnerabilities by attributes such as CVE ID, severity, project, repository, digest and etc.

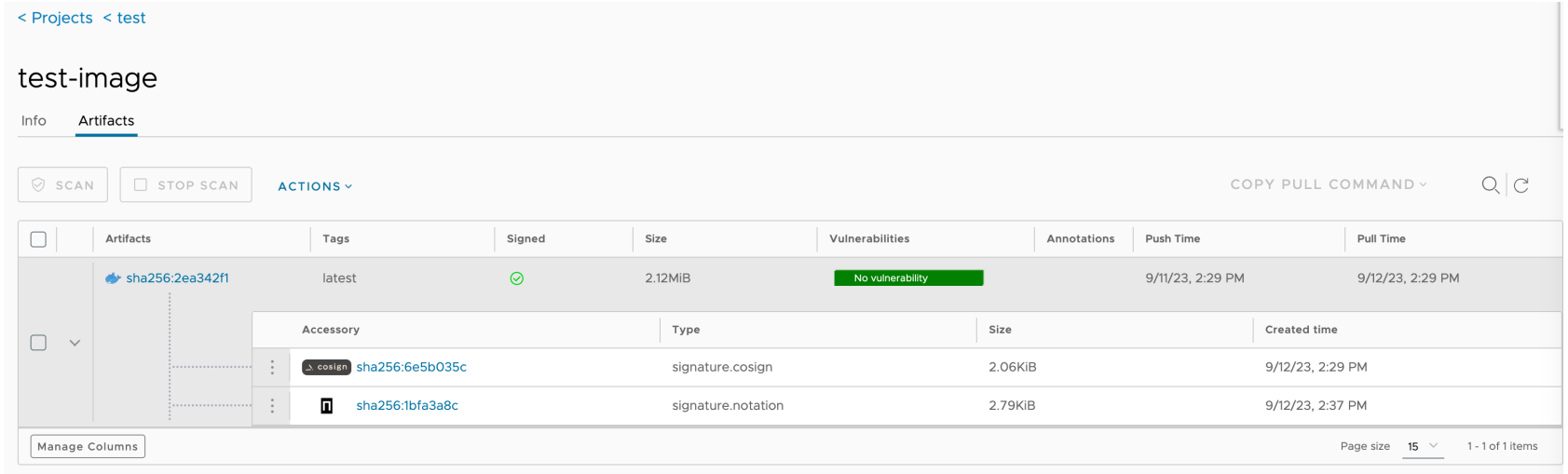


Feature

OCI Distribution Spec v1.1.0-rc2

- Recognize and build the linkage of artifacts by using the subject attribute.
- Support stores the Notation signature and Nydus conversion as referrers.
- Implemented the Referrers API.

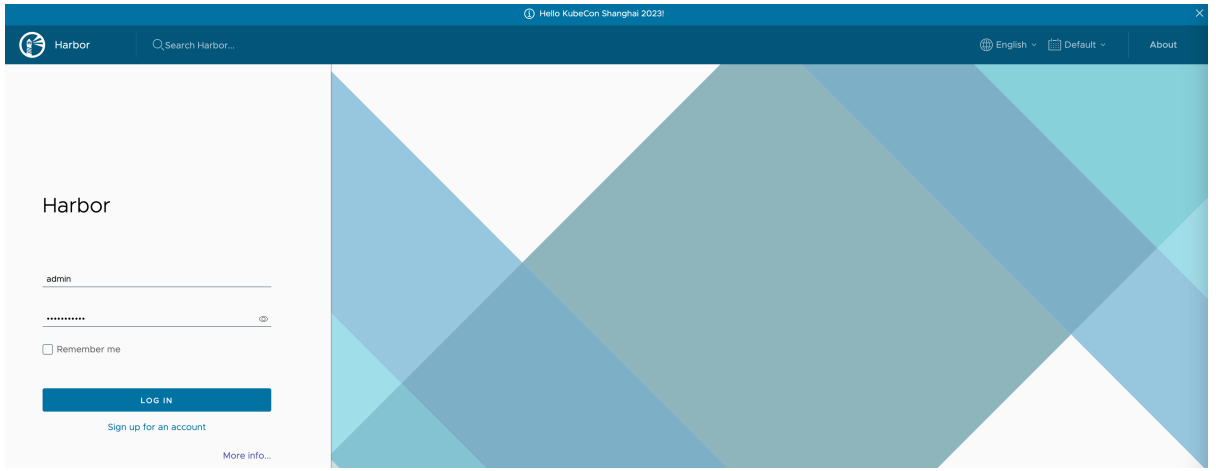


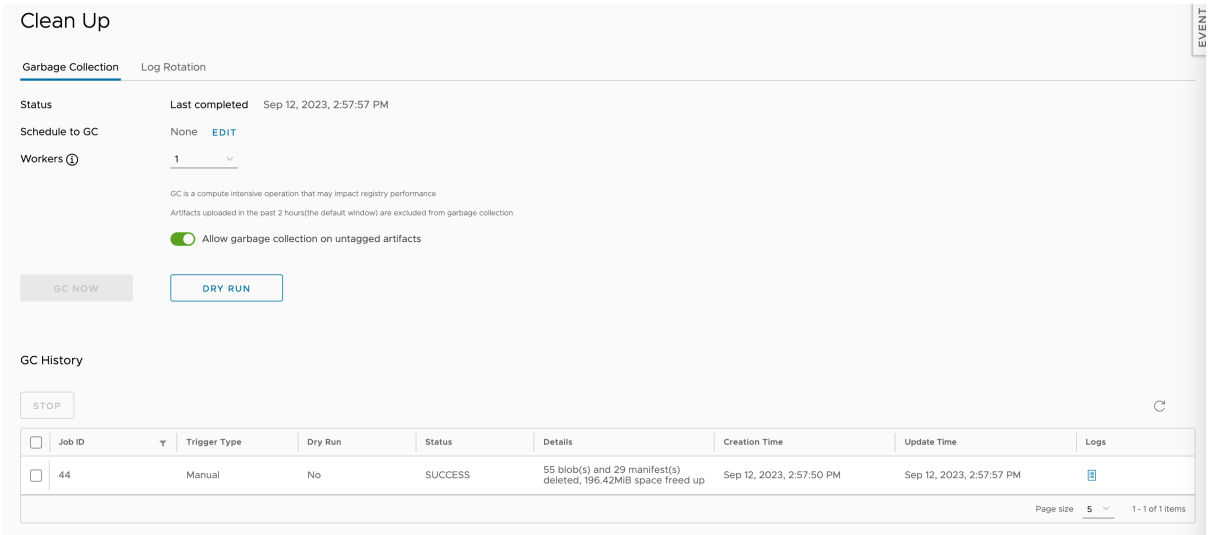


Enhancement

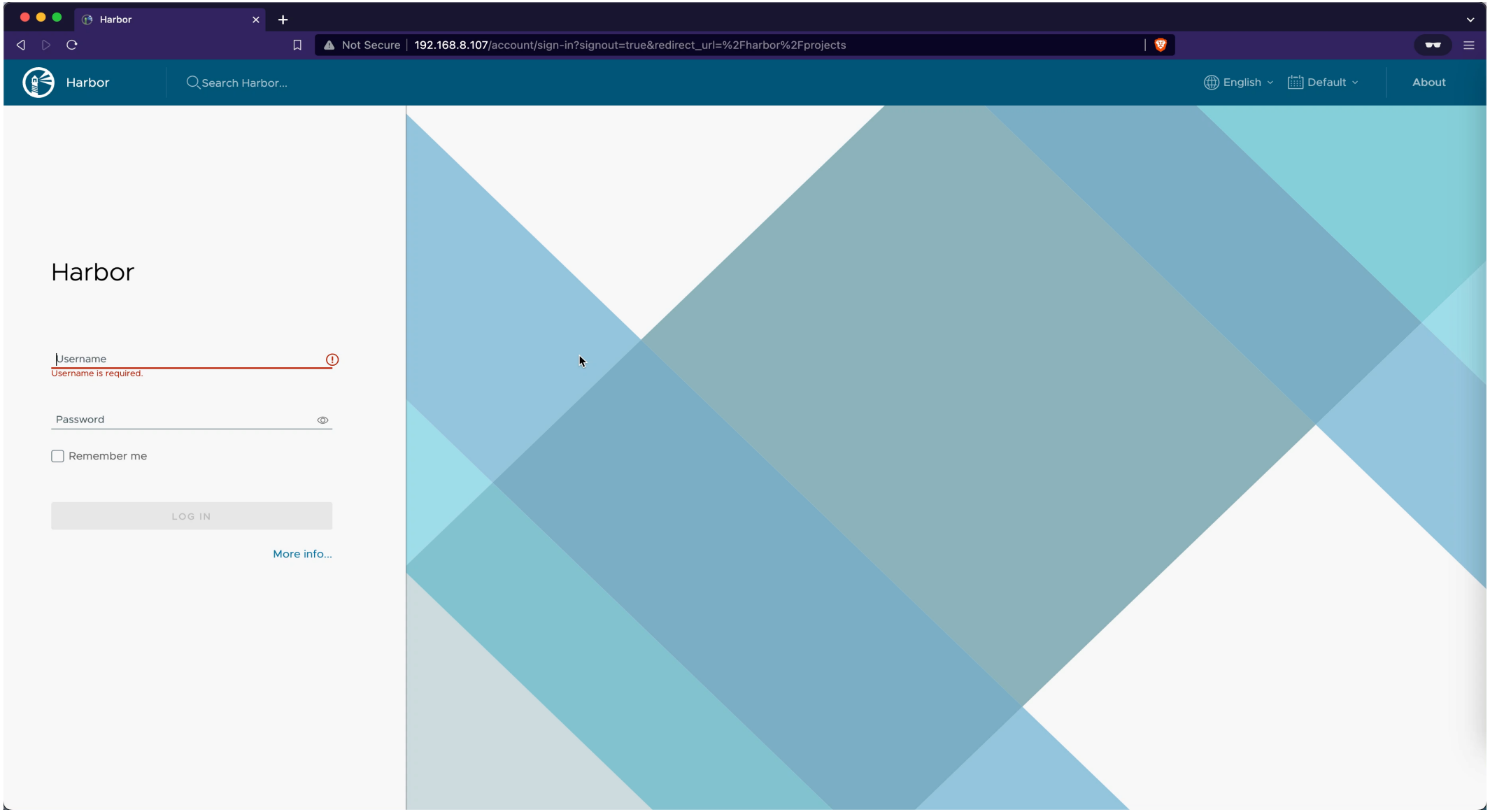
Function Enhancements

- Customizable message banner to provide more comprehensive and detailed information for upcoming maintenance or admin activities.
- Improved visibility with detailed GC execution history and enable the parallel deletion for faster GC duration.
- Introduce a new mechanism utilizing Redis for optimize lock of quota during the high concurrent pushing to same project.





Demo


Harbor
Not Secure | 192.168.8.107/account/sign-in?signout=true&redirect_url=%2Fharbor%2Fprojects
Harbor
Search Harbor...
English
Default
About
Harbor
Username
Username is required.
Password
Remember me
LOG IN
More info...

Future Outlook

Compatible with OCI Distribution Spec v1.1

- Guide a new field *artifactType* on the manifest to denote a custom, non-image artifact.
- Introduce the new filed *subject* on the manifest to link the artifact to others.
- Enable the new referrer API to query the relationships between the artifacts. Optionally support the filter by *artifactType*.

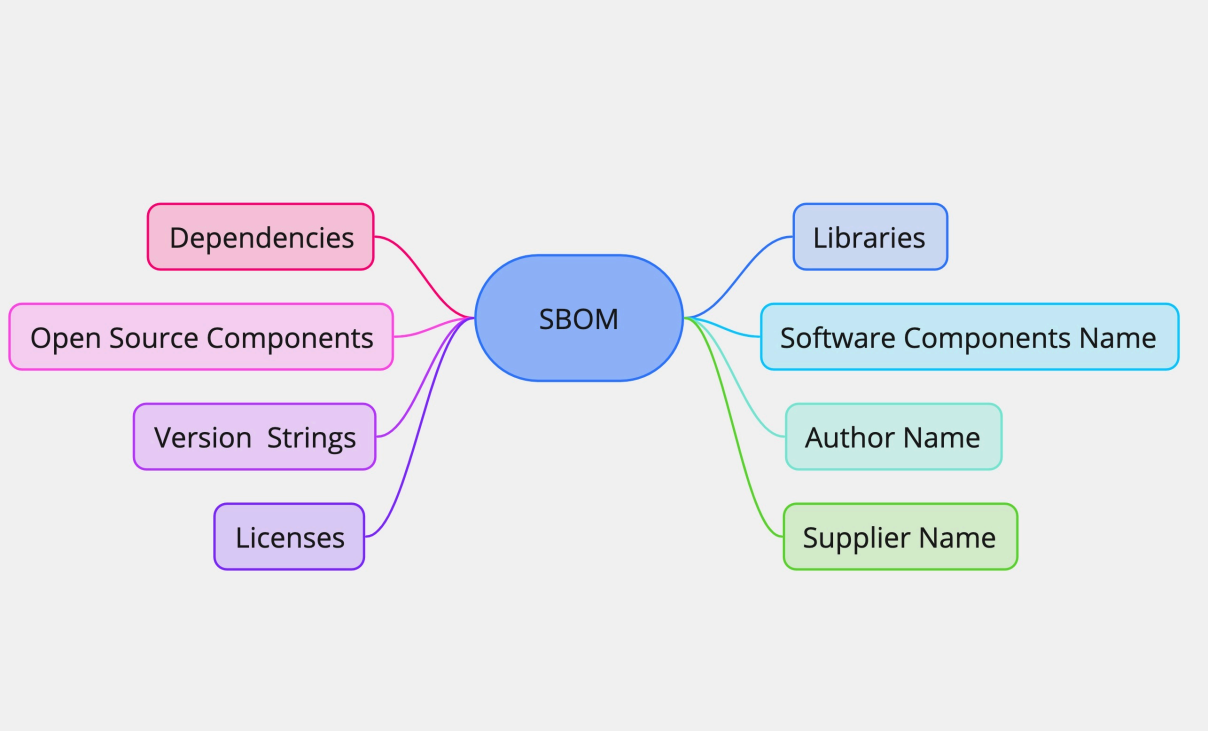
```
// new field 'subject' introduced in the manifest for building the relationships
{
...
  "subject": {
    "mediaType": "application/vnd.oci.image.manifest.v1+json",
    "digest": "sha256:5b0bca...",
    "size": 7682
  },
...
}

// new API endpoint for querying the relationships
{
  "schemaVersion": 2,
  "mediaType": "application/vnd.oci.image.index.v1+json",
  "manifests": [
    {
      "mediaType": "application/vnd.oci.image.manifest.v1+json",
      "size": 1234,
      "digest": "sha256:a1a1a1...",
      "artifactType": "application/vnd.example.sbom.v1",
      "annotations": {
        "org.opencontainers.artifact.created": "2022-01-01T14:42:55Z",
        "org.example.sbom.format": "json"
      }
    },
    {
      "mediaType": "application/vnd.oci.image.manifest.v1+json",
      "size": 1234,
      "digest": "sha256:a2a2a2...",
      "artifactType": "application/vnd.example.signature.v1",
      "annotations": {
        "org.opencontainers.artifact.created": "2022-01-01T07:21:33Z",
        "org.example.signature.fingerprint": "abcd"
      }
    }
  ]
}
```

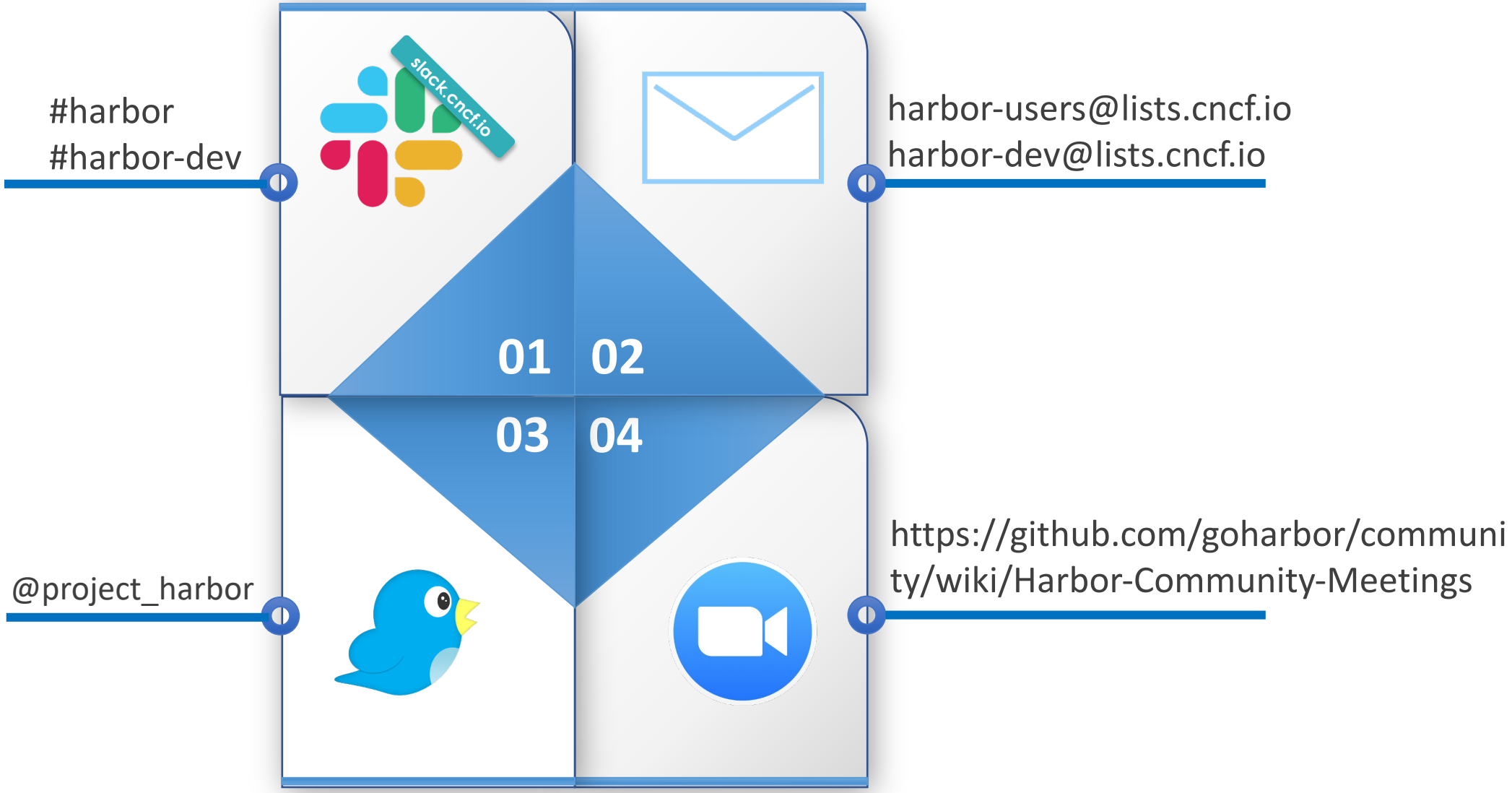
Future Outlook

Software Bill of Materials

- Generate SBOMs for OCI Artifact automatically.
- Faster vulnerabilities scan of the artifact by scanning the SBOMs.
- Visual management and analysis for SBOMs such as export, download or view.
- Integration with Security Hub provides a high-level global security perspective.
- The security alerts or post actions driven based on the compliance policy.



Collaboration



Thank You!