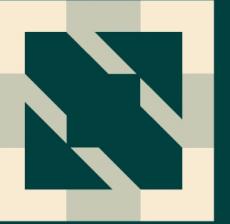


KubeCon



CloudNativeCon

S OPEN SOURCE SUMMIT

China 2023



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

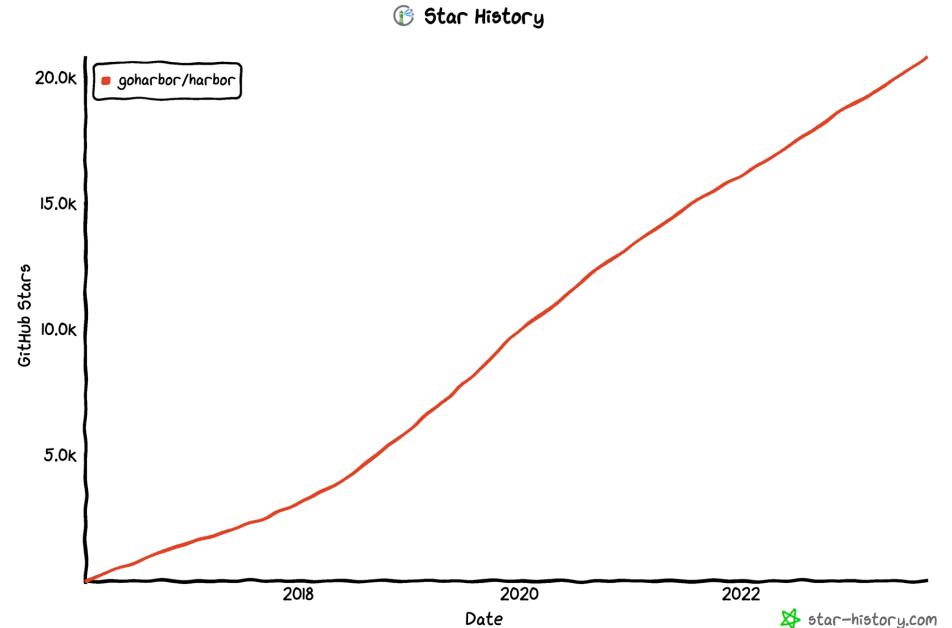
Introduction



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.

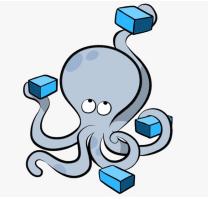
<https://goharbor.io>



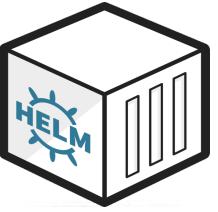
Key Features

- 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.

37 artifact(s), 18 scanned, 19 not scanned 

Total Vulnerabilities

2266 total with 434 fixable

Critical	48
High	304
Medium	686
Low	1227
n/a	1
None	0



Top 5 Most Dangerous Artifacts

REPOSITORY NAME	DIGEST	VULNERABILITIES
wrj/nginx-image	sha256:ee89b005	
dhorse/hello	sha256:34c513ac	
dhorse/hello-nuxt	sha256:d90ffcd4	
vac-test/container... vac-test/container...	sha256:424e2ea5 sha256:9554ae7	 

Top 5 Most Dangerous CVEs

CVE ID	SEVERITY	CVSS3	PACKAGE
CVE-2023-25775	Critical	9.8	linux-libc-dev@und...
CVE-2023-28531	Critical	9.8	openssh-client@un...
CVE-2023-38408	Critical	9.8	openssh-client@un...
CVE-2022-2068	Critical	9.8	openssl@undefined
CVE-2022-37434	Critical	9.8	zlib1g@undefined

Vulnerabilities

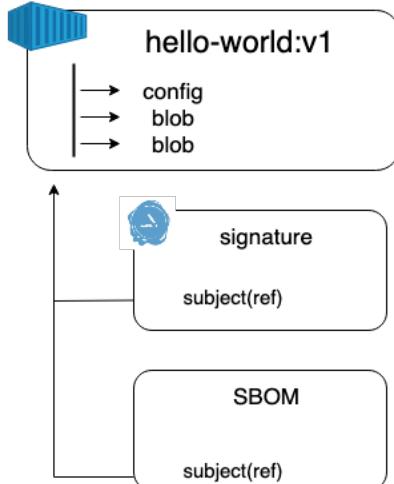
Filter by  All   SEARCH

CVE ID	Repository Name	Digest	Tags	CVSS3	Severity	Package	Current version	Fixed in
CVE-2019-8457	vac-test/containers/de...	sha256:77d096bd	latest, 1.0.1-debian-10-r...	9.8		libdb5.3	5.3.28+dfs...	
CVE-2019-1010022	vac-test/containers/de...	sha256:424e2ea5	latest, 2.42.0-debian-1...	9.8		libc-bin	2.28-10+d...	
CVE-2019-1010022	vac-test/containers/de...	sha256:77d096bd	latest, 1.0.1-debian-10-r...	9.8		libc-bin	2.28-10+d...	
CVE-2019-1010022	vac-test/containers/de...	sha256:77d096bd	latest, 1.0.1-debian-10-r...	9.8		libc6	2.28-10+d...	
CVE-2019-9893	vac-test/containers/de...	sha256:77d096bd	latest, 1.0.1-debian-10-r...	9.8		libseccomp2	2.3.3-4	

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.



< Projects < test

test-image

Info		Artifacts																	
<input type="checkbox"/>	Artifacts	Tags	Signed	Size	Vulnerabilities	Annotations	Push Time	Pull Time											
<input type="checkbox"/>	sha256:2ea342f1	latest		2.12MiB	No vulnerability		9/11/23, 2:29 PM	9/12/23, 2:29 PM											
		<table border="1"> <thead> <tr> <th>Type</th> <th>Size</th> <th>Created time</th> </tr> </thead> <tbody> <tr> <td>Accessory</td> <td></td> <td></td> </tr> <tr> <td>signature.cosign</td> <td>2.06KiB</td> <td>9/12/23, 2:29 PM</td> </tr> <tr> <td>signature.notation</td> <td>2.79KiB</td> <td>9/12/23, 2:37 PM</td> </tr> </tbody> </table>						Type	Size	Created time	Accessory			signature.cosign	2.06KiB	9/12/23, 2:29 PM	signature.notation	2.79KiB	9/12/23, 2:37 PM
Type	Size	Created time																	
Accessory																			
signature.cosign	2.06KiB	9/12/23, 2:29 PM																	
signature.notation	2.79KiB	9/12/23, 2:37 PM																	
<input type="checkbox"/> Manage Columns																			
Page size <input type="button" value="15"/> 1 - 1 of 1 items																			

Enhancement

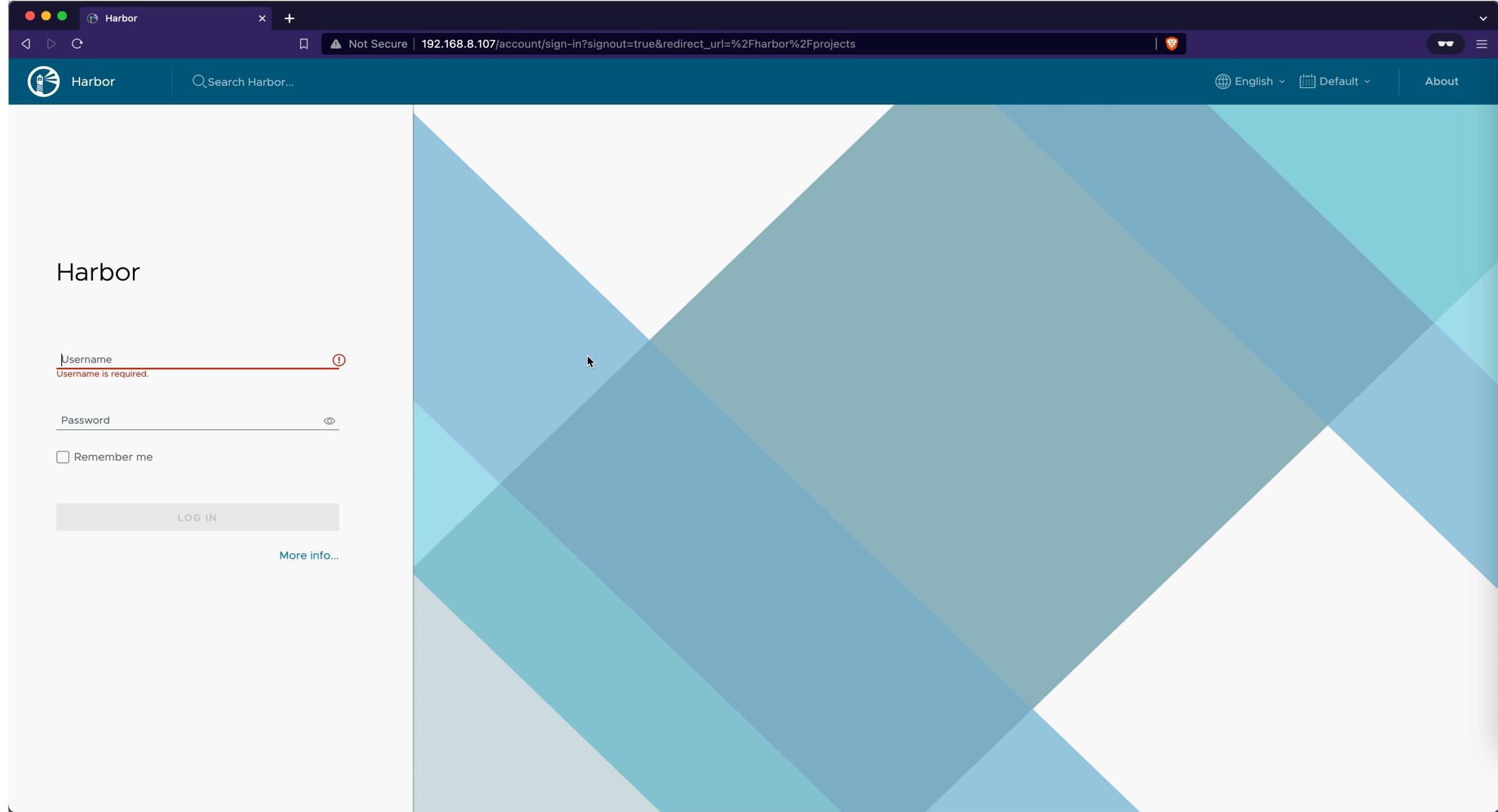
Function Enhancements

- 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.

The screenshot displays two main sections of the Harbor UI. The top section shows the login page with fields for 'admin' and 'password', a 'Remember me' checkbox, and a 'LOG IN' button. The bottom section shows the 'Clean Up' page under the 'Garbage Collection' tab. It includes a status bar showing 'Last completed' at 'Sep 12, 2023, 2:57:57 PM', a 'Schedule to GC' dropdown set to 'None', a 'Workers' dropdown set to '1', and a note about GC being a compute intensive operation. There is also a checkbox for 'Allow garbage collection on untagged artifacts'. Below this is a 'DRY RUN' button. The bottom section also shows a 'GC History' table with one entry:

Job ID	Trigger Type	Dry Run	Status	Details	Creation Time	Update Time	Logs
44	Manual	No	SUCCESS	55 blob(s) and 29 manifest(s) deleted, 196.42MB space freed up	Sep 12, 2023, 2:57:50 PM	Sep 12, 2023, 2:57:57 PM	View Logs

Demo



Future Outlook

Compatible with OCI Distribution Spec v1.1

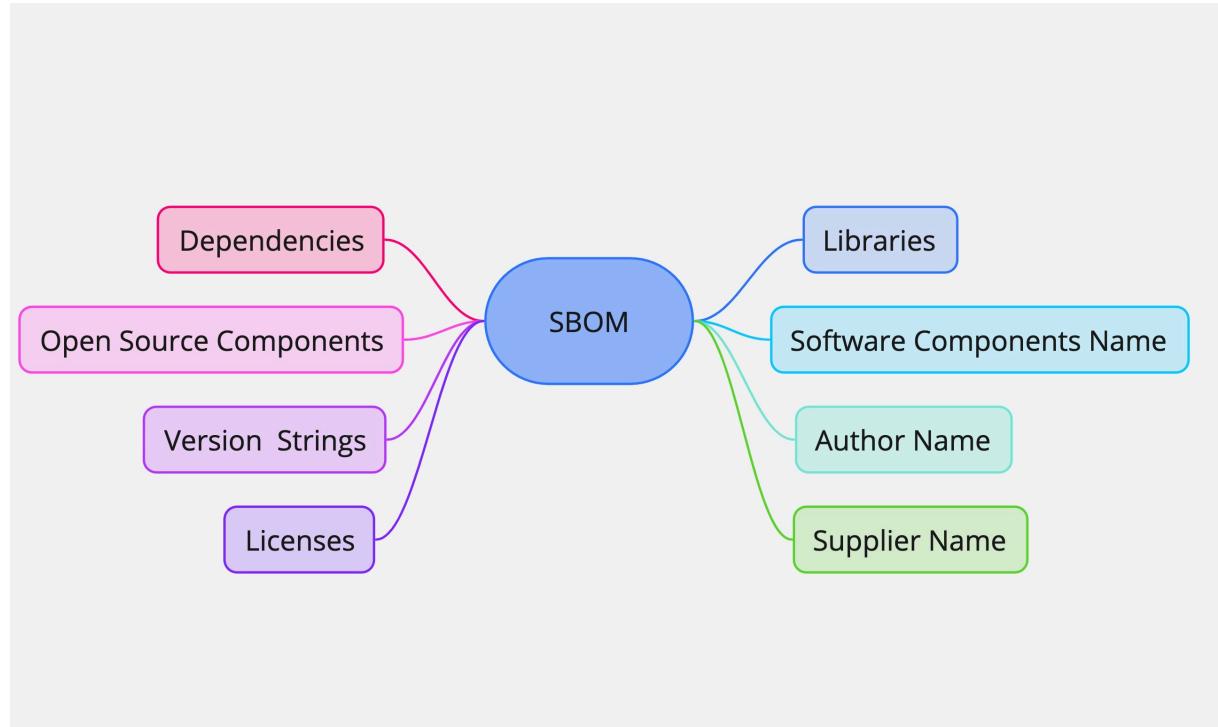
- Guide a new field *artifactType* on the manifest to denote a custom, non-image artifact.
- Introduce the new filed *subject* on the manifest to link the artifact to others.
- Enable the new referrer API to query the relationships between the artifacts.
Optionally support the filter by *artifactType*.

```
● ● ●  
  
// 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"  
      }  
    }  
  ]  
}
```

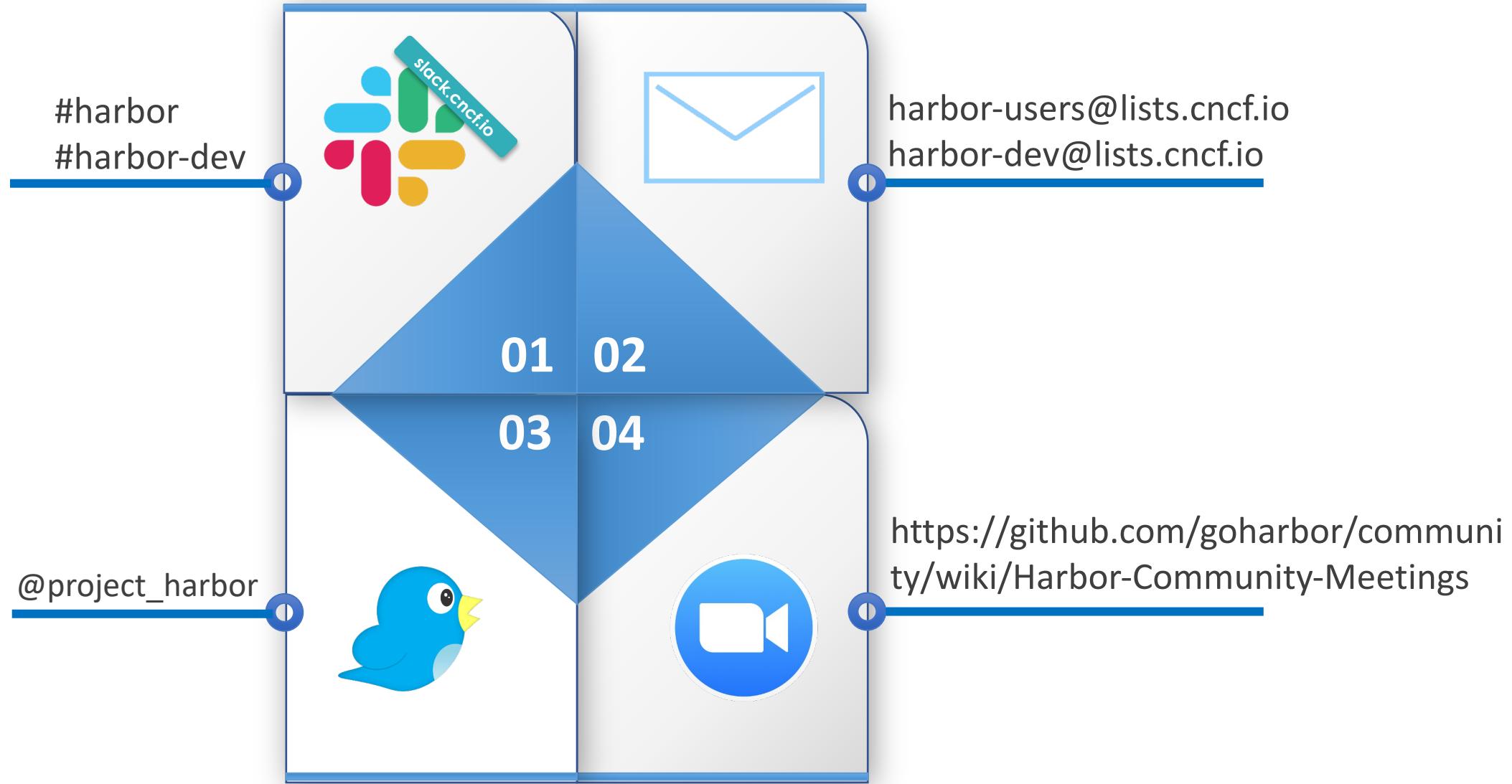
Future Outlook

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!