



KubeCon



CloudNativeCon

North America 2023





KubeCon



CloudNativeCon

North America 2023

What's New in Harbor, and How Can You Make Harbor Even Better

Yan Wang, VMWare
Vadim Bauer, 8gears

Agenda



KubeCon



CloudNativeCon

North America 2023

- Introduction
- Harbor Superpowers
- Feature Recap
 - Security Hub
 - OCI Distribution Spec v1.1
 - Robot Full Access
 - Other Enhancements
- Demo
- Future Outlook
- Collaboration and how to make Harbor better

Harbor is a CNCF-graduated open-source container registry to store and manage container images and other OCI artifacts securely with policies, role-based access control, vulnerability analytics and signing.



Introduction

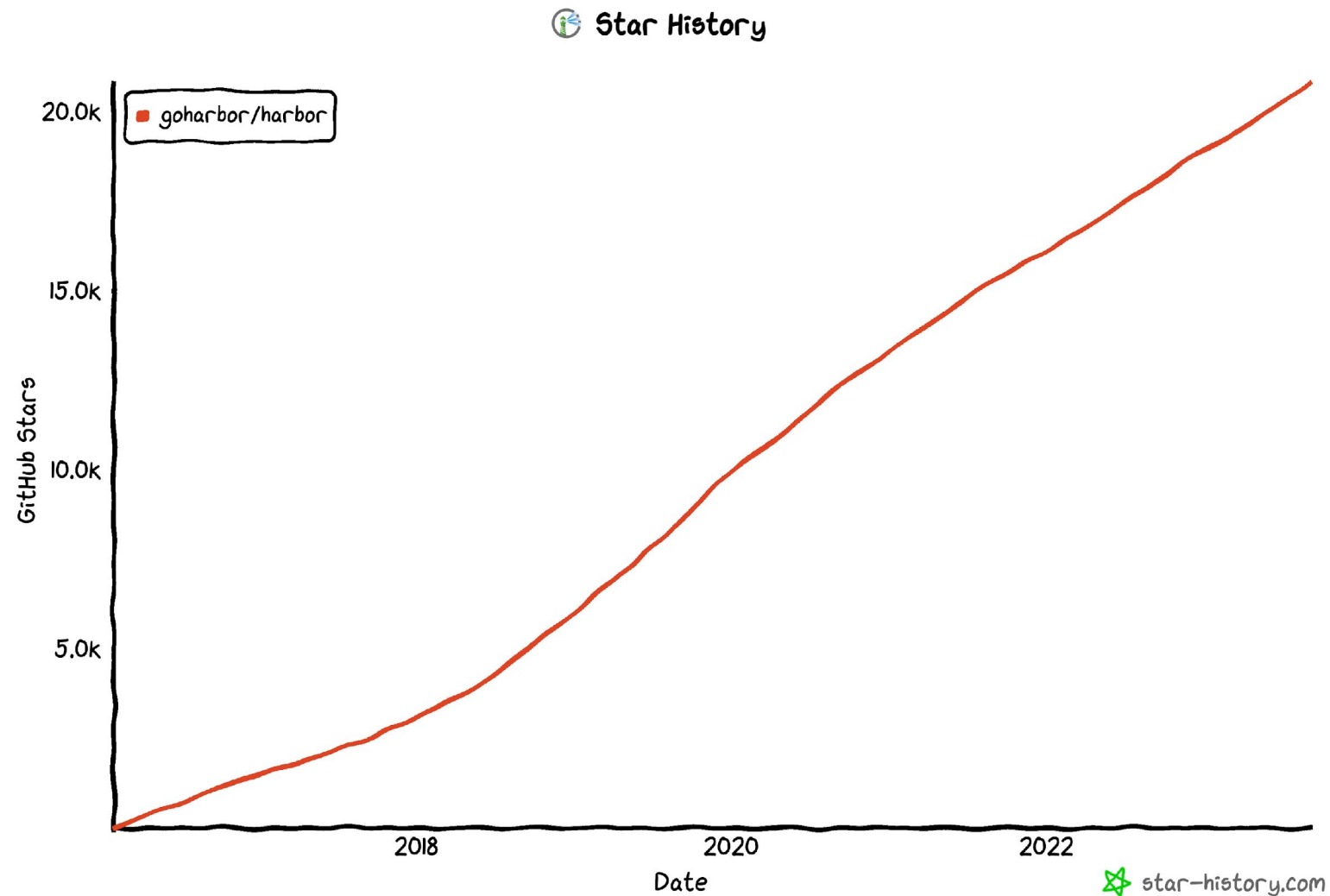


KubeCon



CloudNativeCon

North America 2023





KubeCon

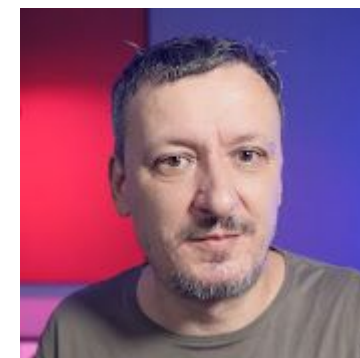


CloudNativeCon

North America 2023

“Harbor is the golden standard when it comes to container registries.”

Victor Farcic



Key Features



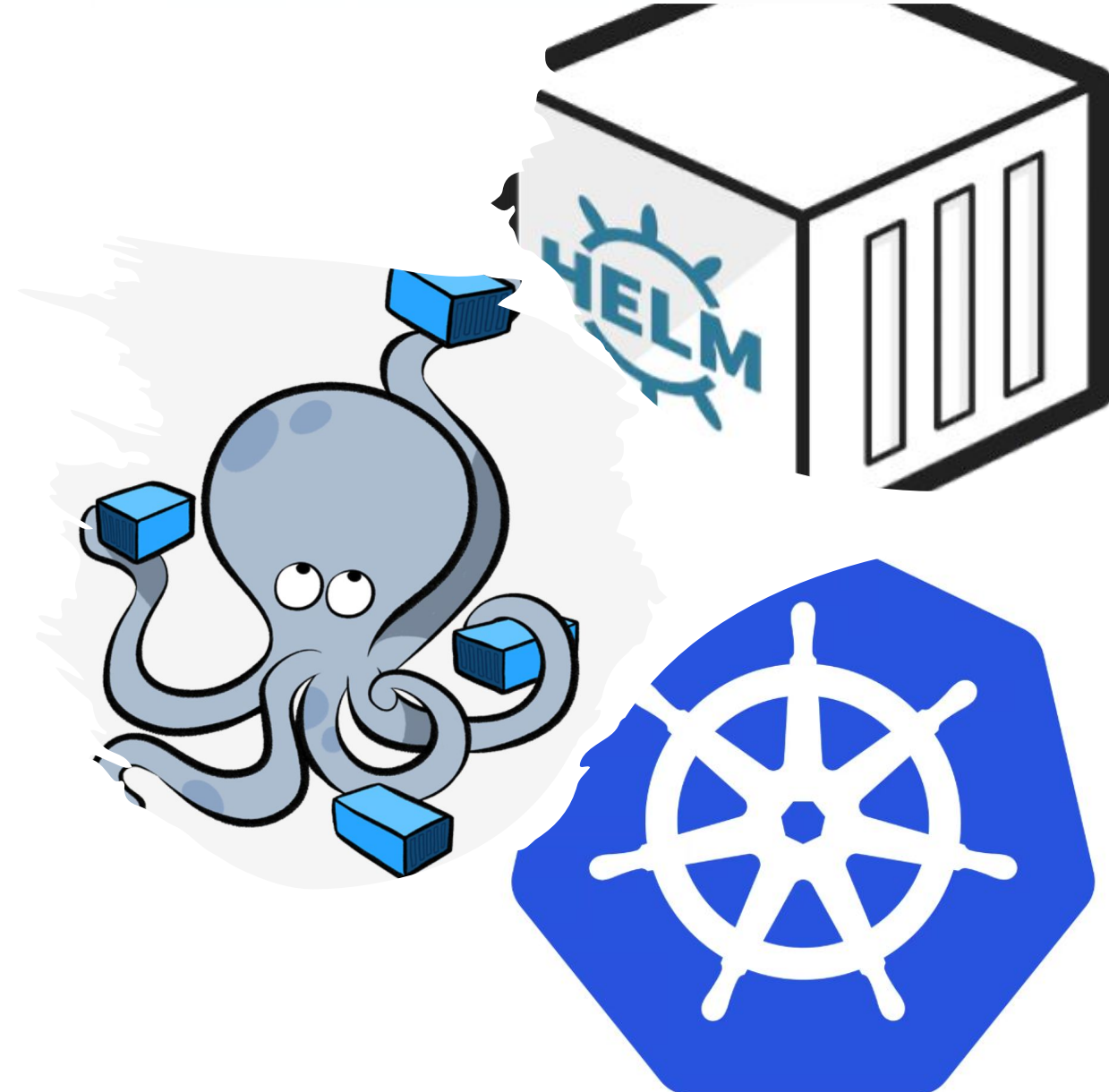
KubeCon



CloudNativeCon

North America 2023

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



1. Works for small Teams and Enterprises

- a. RBAC
- b. IDP and SSO - External identity provider for **authentication** and **authorization**

2. Makes CISOs happy

- a. All your images in one place – Replication, Proxying
- b. Vulnerability overview, audit trails

3. Ops people's darling

- a. Automation & IaC – RESTful API, Terraform, Pulumi
- b. Operational control mechanisms – GC, Quota, Policies

Superpowers



KubeCon



CloudNativeCon

North America 2023

Let me show that ...

Architecture



KubeCon



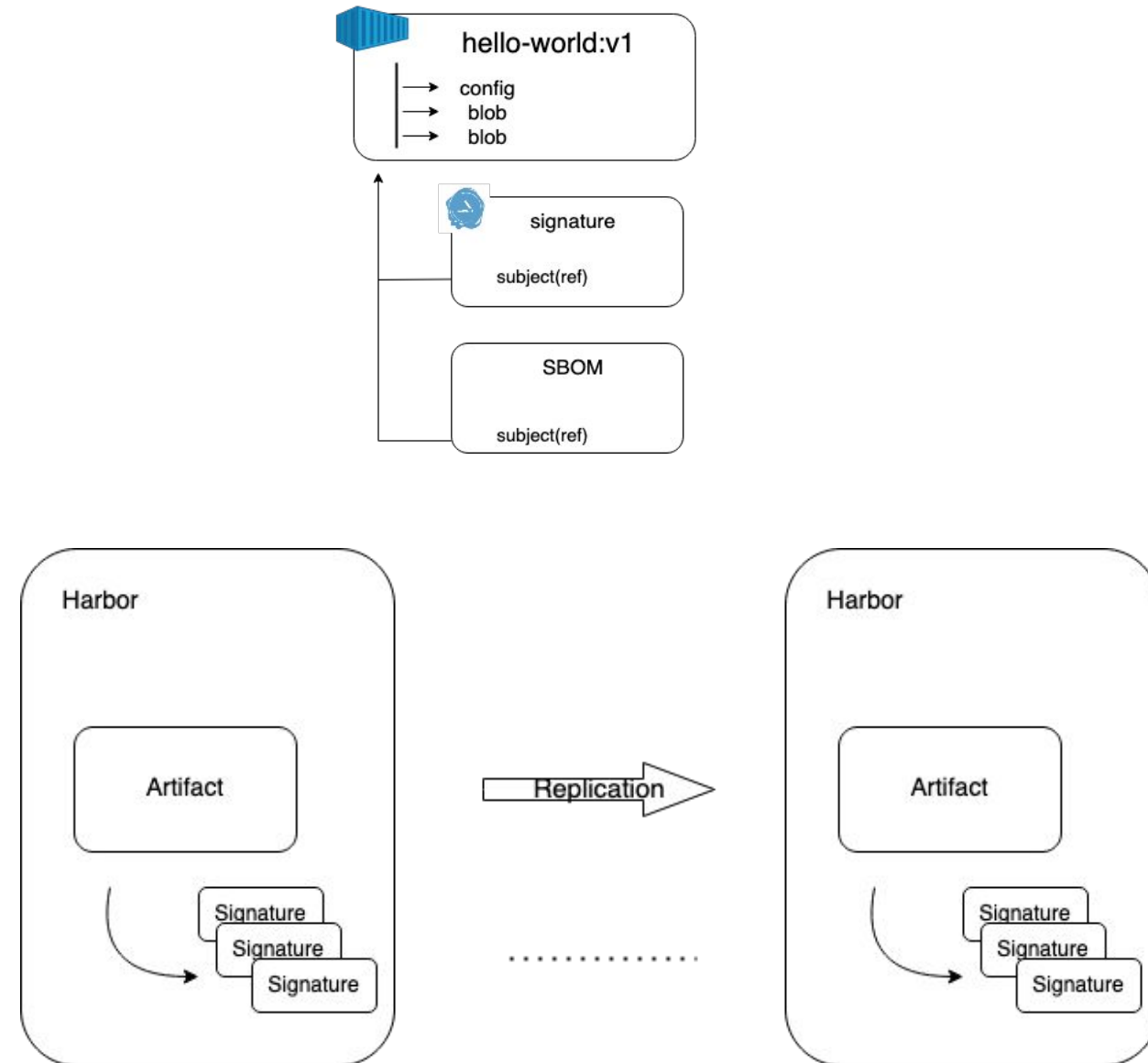
CloudNativeCon

North America 2023



OCI Distribution Spec v1.1.0-rc3

- Establish connections between artifacts by utilizing the subject attribute.
- Enable the storage of Notation signatures and Nydus conversions as referencers.
- Successfully implemented the Referrers API.



Demo -- OCI



KubeCon

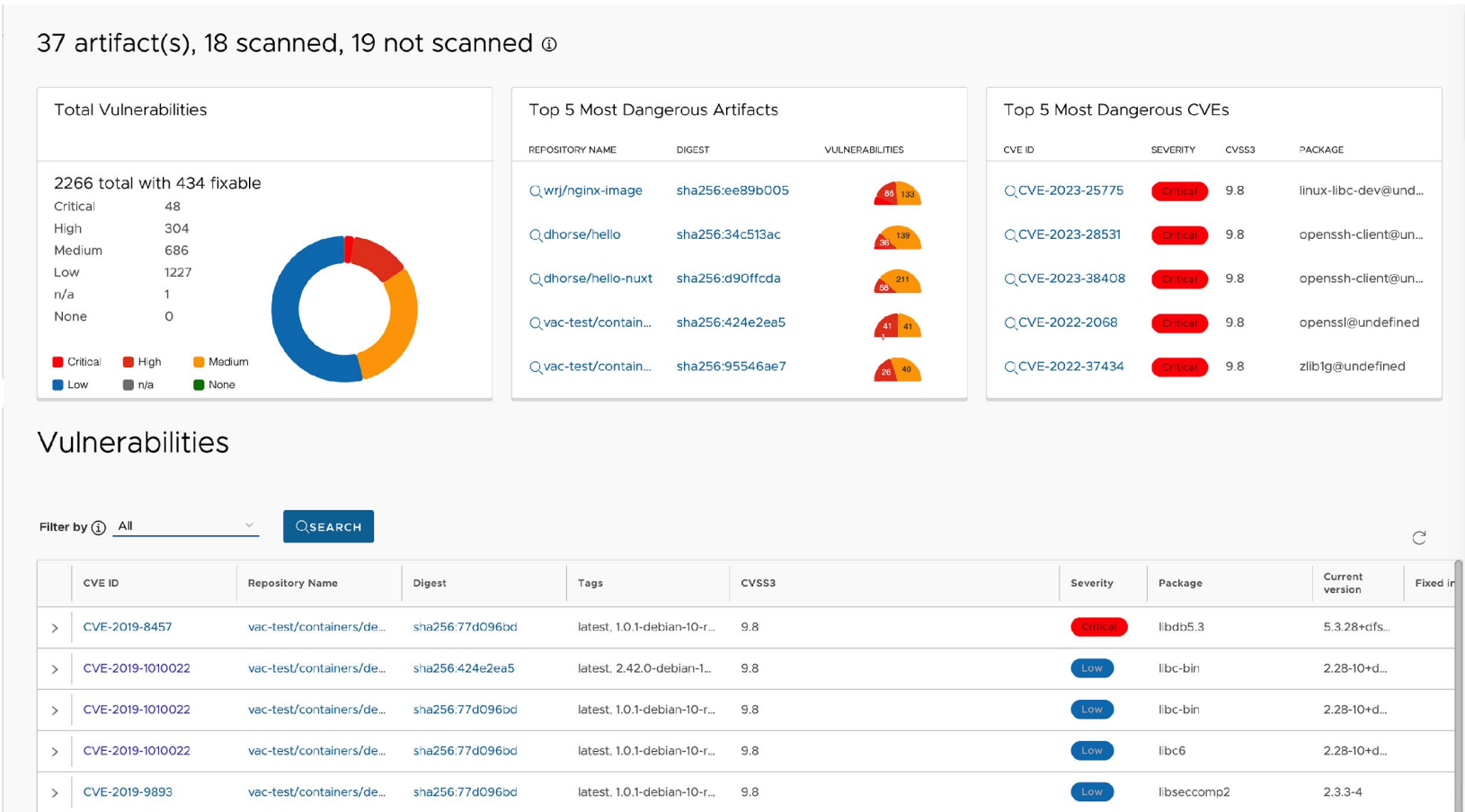


CloudNativeCon

North America 2023



- Offer a comprehensive and centralized overview of the current security status of artifacts stored in Harbor.
- Emphasize the identification of the most critical artifacts and CVEs.
- Enable vulnerability search by attributes, including CVE ID, severity, project, repository, digest, and more.



Enhancements



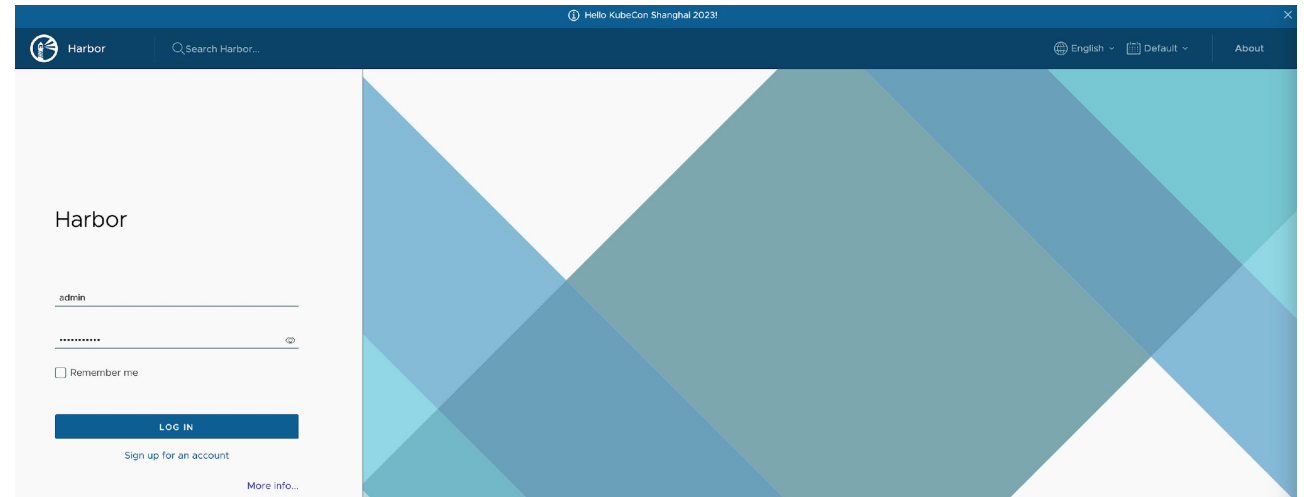
KubeCon



CloudNativeCon

North America 2023

- Introduce a customizable message banner to deliver comprehensive and detailed information about upcoming maintenance or admin activities.
- Enhance visibility by providing a detailed GC execution history and enabling parallel deletion for quicker GC duration.
- Implement a new mechanism that utilizes Redis to optimize quota locks during high-concurrency pushes to the same project.



Clean Up

Garbage Collection

Log Rotation

Status

Last completed Sep 12, 2023, 2:57:57 PM

Schedule to GC

None [EDIT](#)

Workers ①

1

GC is a compute intensive operation that may impact registry performance.
Artifacts uploaded in the past 2 hours(the default window) are excluded from garbage collection.

☒ Allow garbage collection on untagged artifacts

GC NOW

DRY RUN

GC History

STOP

<input type="checkbox"/>	Job ID	Trigger Type	Dry Run	Status	Details	Creation Time	Update Time	Logs
<input type="checkbox"/>	44	Manual	No	SUCCESS	55 blob(s) and 29 manifest(s) deleted, 196.42MiB space freed up	Sep 12, 2023, 2:57:50 PM	Sep 12, 2023, 2:57:57 PM	📄

Page size 5 1 - 1 of 1 items

Demo



KubeCon



CloudNativeCon

North America 2023

Robot Accounts – Full Access



KubeCon



CloudNativeCon

North America 2023

- Provides step-by-step instructions for attaching a robot account to a set of APIs, ensuring clear and straightforward.
- A user-friendly UI that displays the data dictionary, enabling users to make informed choices with ease.

Create System Robot Account

Create a system Robot Account that will cover specific projects. Choose "Cover all projects" to be applied to all existing and future projects

1 Basic Information

2 Select System Permissions

3 Select Project Permissions

Select System Permissions

SELECT ALL

Resource	List	Read	Create	Delete	Update	Stop
Audit Log	<input type="checkbox"/>					
Preheat Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Project	<input type="checkbox"/>		<input type="checkbox"/>			
Replication Policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Replication	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Replication Adapter	<input type="checkbox"/>					
Registry	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Scan All		<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
System Volumes		<input type="checkbox"/>				
Garbage Collection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Purge Audit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Job Service Monitor	<input type="checkbox"/>					<input type="checkbox"/>
Tag Retention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Scanner	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Label	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Export CVE		<input type="checkbox"/>	<input type="checkbox"/>			
Security Hub	<input type="checkbox"/>	<input type="checkbox"/>				
Catalog		<input type="checkbox"/>				

CANCEL

BACK

NEXT

Demo – Robot Accounts Full Access



KubeCon



CloudNativeCon

North America 2023

Pluggable Scanner Spec – v1.2



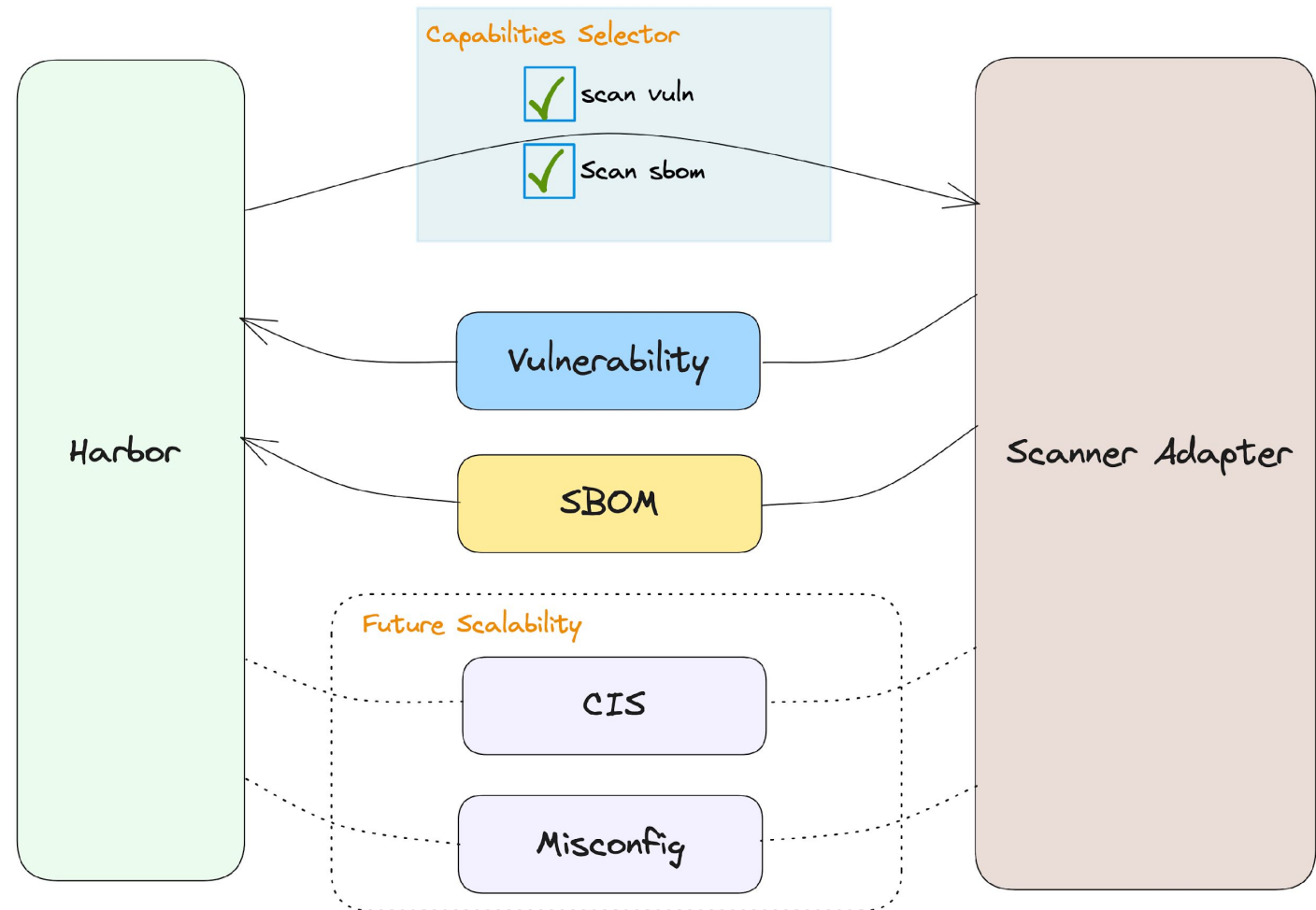
KubeCon



CloudNativeCon

North America 2023

- Enhance the scanner's capabilities and the scan request model to enable the specification of enabled capabilities for Harbor scanning.
- Introduce a new data report model for the Software Bill of Materials (SBOM) and outline the specifications during integration with Harbor.
- This new model will provide greater flexibility and convenience for future expansion of security scanning types, such as CIS and misconfig.
- Update the OpenAPI definitions YAML to version 1.2.



Pluggable Scanner Spec -- Metadata



KubeCon



CloudNativeCon

North America 2023

application/vnd.scanner.adapter.metadata+json;
version=1.0

0 removals

18 lines Copy

```
1 {
2   "scanner": {
3     "name": "Trivy",
4     "vendor": "Aqua Security",
5     "version": "0.4.0"
6   },
7   "capabilities": [
8     {
9       "consumes_mime_types": [
10        "application/vnd.oci.image.manifest.v1+json",
11        "application/vnd.docker.distribution.manifest.v2+json"
12      ],
13      "produces_mime_types": [
14        "application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0"
15      ]
16    }
17  ]
18 }
```

application/vnd.scanner.adapter.metadata+json;
version=1.1

11 additions

29 lines Copy

```
1 {
2   "scanner": {
3     "name": "Trivy",
4     "vendor": "Aqua Security",
5     "version": "0.4.0"
6   },
7   "capabilities": [
8     {
9       "type": "vulnerability",
10      "consumes_mime_types": [
11        "application/vnd.oci.image.manifest.v1+json",
12        "application/vnd.docker.distribution.manifest.v2+json"
13      ],
14      "produces_mime_types": [
15        "application/vnd.scanner.adapter.vuln.report.harbor+json; version=1.0"
16      ]
17    },
18    {
19      "type": "sbom",
20      "consumes_mime_types": [
21        "application/vnd.oci.image.manifest.v1+json",
22        "application/vnd.docker.distribution.manifest.v2+json"
23      ],
24      "produces_mime_types": [
25        "application/vnd.security.sbom.report+json; version=1.0"
26      ]
27    }
28  ]
29 }
```

Pluggable Scanner Spec -- Scan Request



KubeCon



CloudNativeCon

North America 2023

application/vnd.scanner.adapter.scan.request+json;
version=1.0

application/vnd.scanner.adapter.scan.request+json;
version=1.1

1 removal

12 lines Copy

```
1 {
2   "registry": {
3     "url": "https://core.harbor.domain",
4     "authorization": "Basic BASE64_ENCODED_CREDENTIALS"
5   },
6   "artifact": {
7     "repository": "library/mongo",
8     "digest": "sha256:6c3c624b58dbbcd3c0dd82b4c53f04194d1247c6eebdaab7c610cf7d66709b3b",
9     "tag": "3.14-xenial",
10    "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
11  }
```

12 }

15 additions

26 lines Copy

```
1 {
2   "registry": {
3     "url": "https://core.harbor.domain",
4     "authorization": "Basic BASE64_ENCODED_CREDENTIALS"
5   },
6   "artifact": {
7     "repository": "library/mongo",
8     "digest": "sha256:6c3c624b58dbbcd3c0dd82b4c53f04194d1247c6eebdaab7c610cf7d66709b3b",
9     "tag": "3.14-xenial",
10    "mime_type": "application/vnd.docker.distribution.manifest.v2+json"
11  },
12   "enabled_capabilities": [
13     {
14       "type": "vulnerability"
15     },
16     {
17       "type": "sbom",
18       "produces_mime_types": [
19         "application/vnd.security.sbom.report+json; version=1.0"
20       ],
21       "parameters": {
22         "accept_media_type": "application/spdx+json"
23       }
24     }
25  ]
26 }
```

26 }

Software Bill of Materials



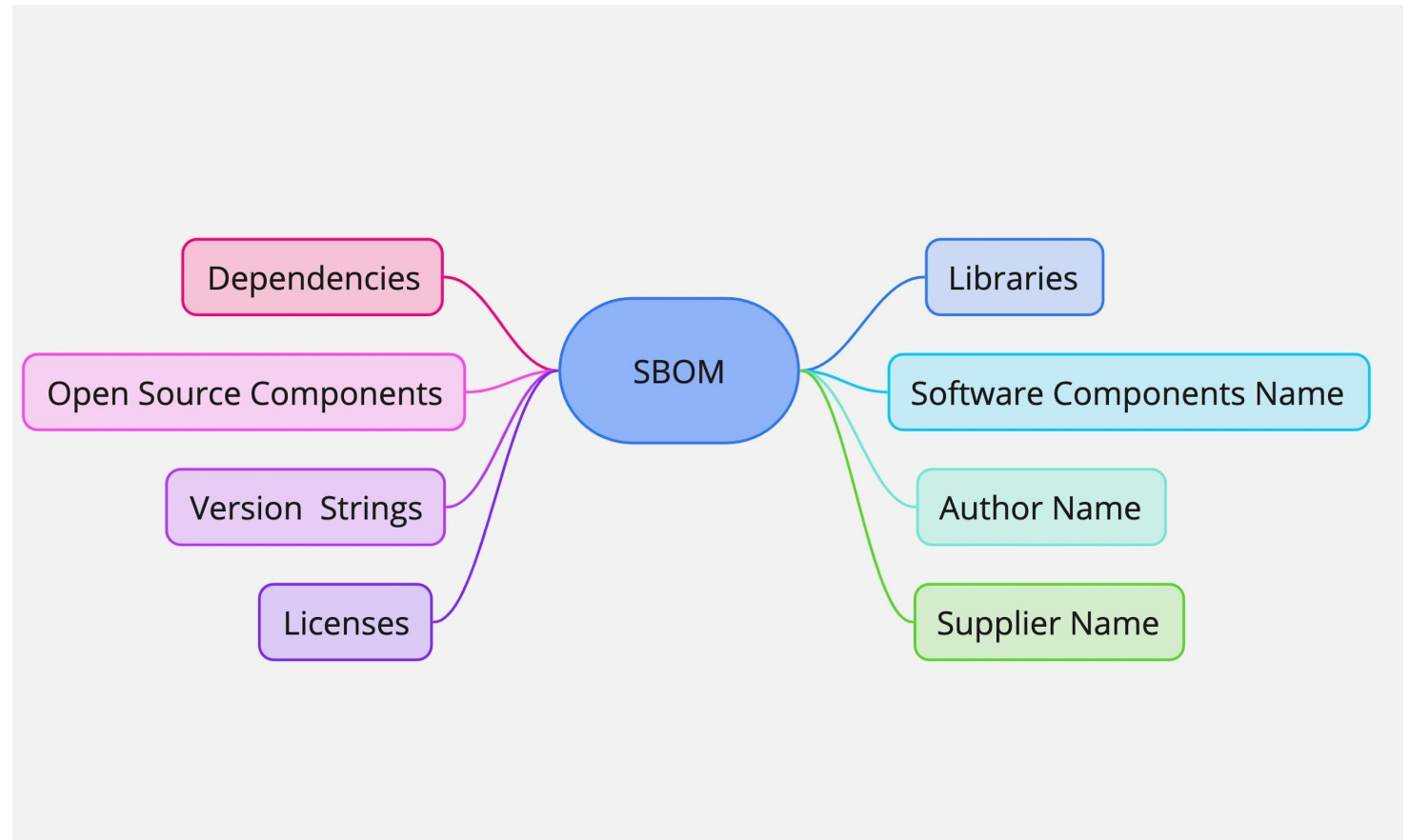
KubeCon



CloudNativeCon

North America 2023

- Automatically generate SBOMs for OCI Artifacts.
- Accelerate the vulnerabilities scan of artifacts by utilizing SBOMs.
- Enable visual management and analysis of SBOMs, including features like export, download, and viewing.
- Integration with Security Hub offers a comprehensive global security overview.



Collaboration

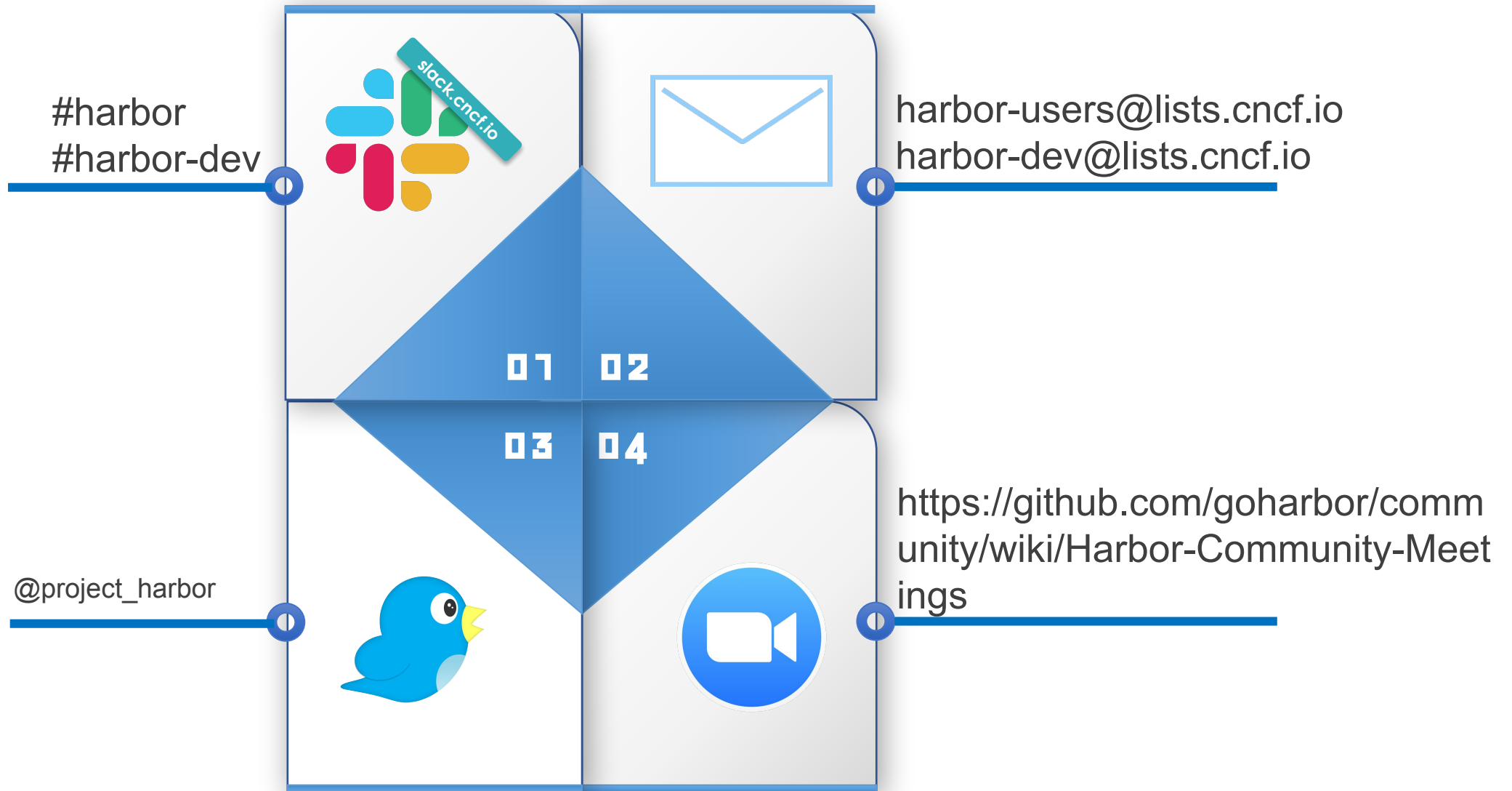


KubeCon



CloudNativeCon

North America 2023



Meet The Team @ Project Kiosk



KubeCon



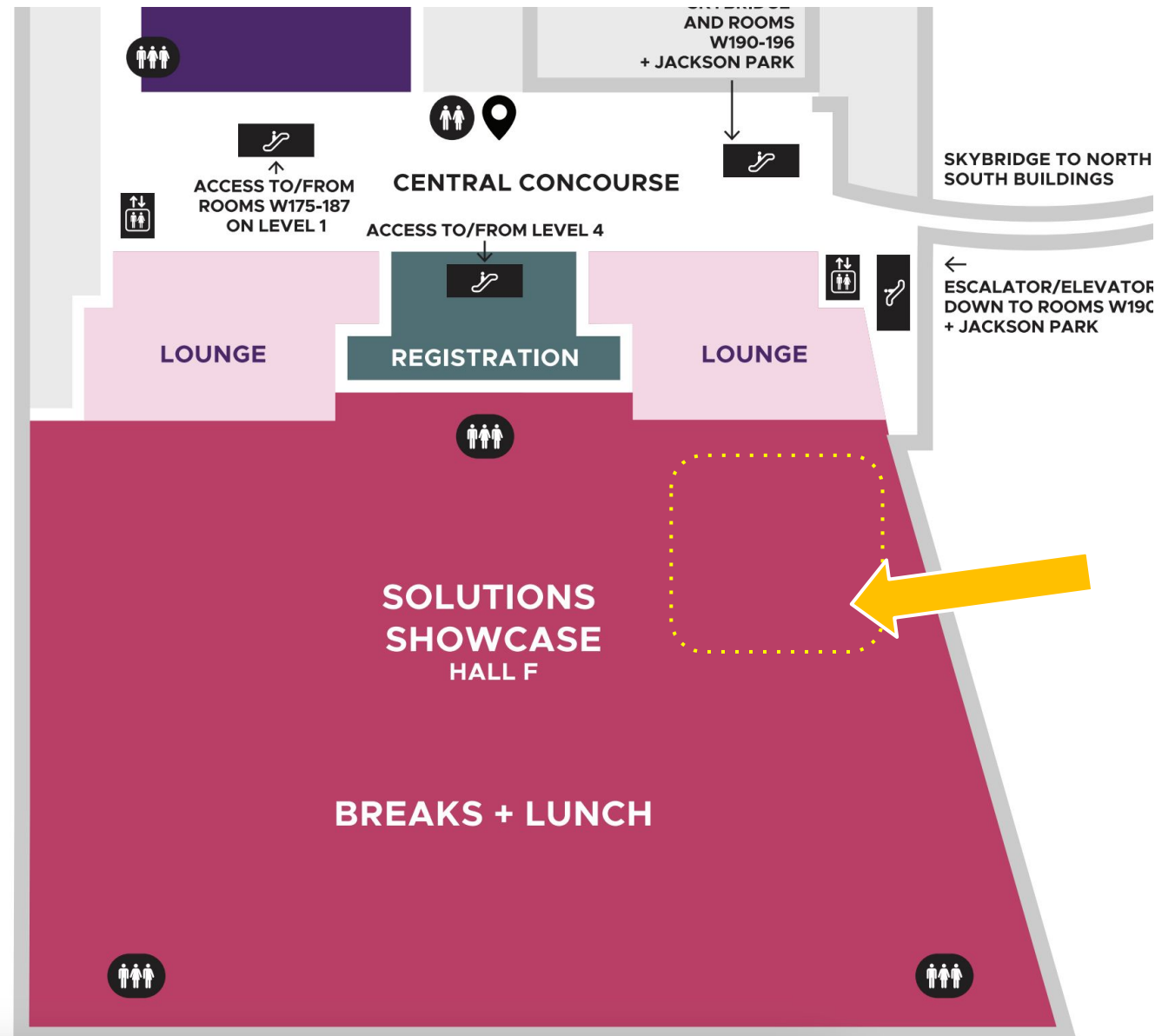
CloudNativeCon

North America 2023

CNCF Project Booth **P2**

Wednesday, **2:00 pm – 5:00 pm**

Thursday, **12:30 pm – 2:30 pm**





PromCon
North America 2021

Session QR Codes will be
sent via email before the event

**Please scan the QR Code above
to leave feedback on this session**