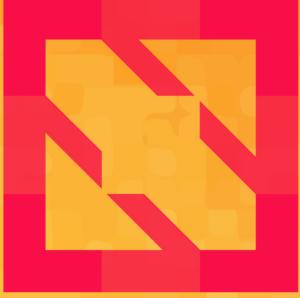




KubeCon



CloudNativeCon

---

North America 2019

---





KubeCon



CloudNativeCon

North America 2019

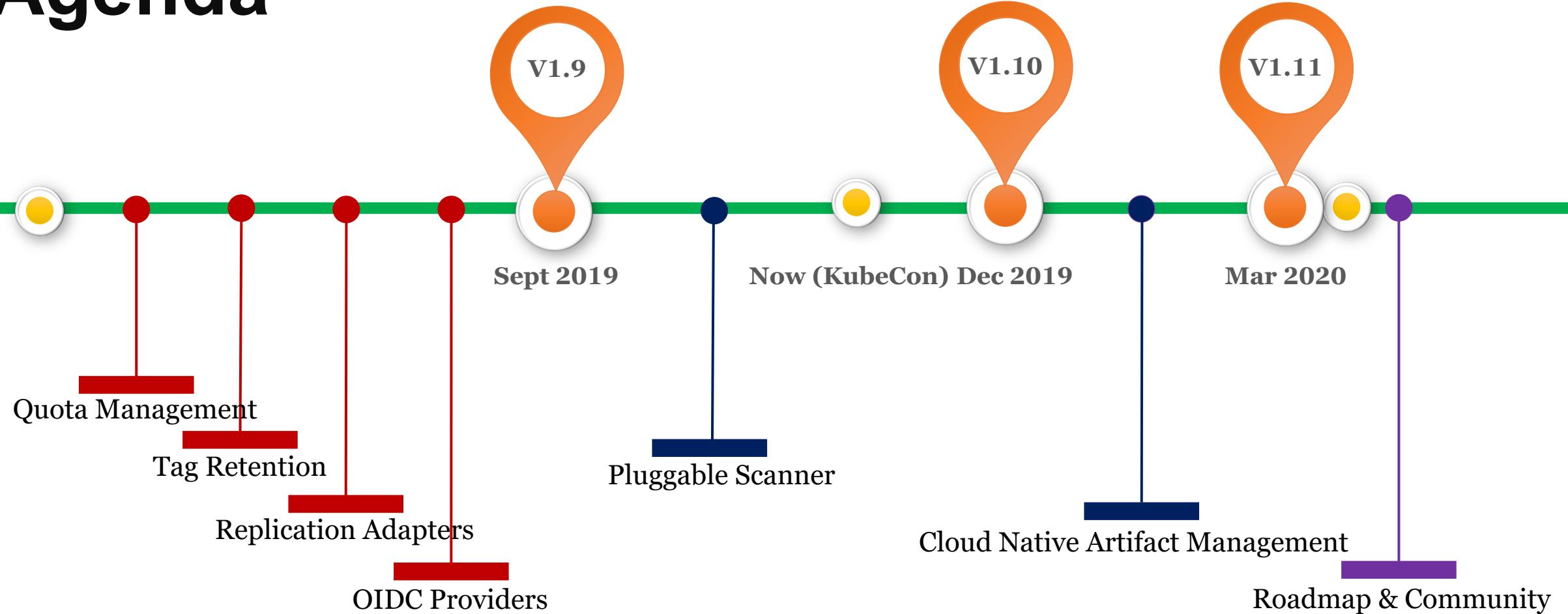
# Deep Dive: Harbor

Steven Zou / [szou@vmware.com](mailto:szou@vmware.com), Staff Engineer at VMware, Harbor Core Maintainer

Daniel Jiang / [jiangd@vmware.com](mailto:jiangd@vmware.com), Staff Engineer at VMware, Harbor Core Maintainer



# Agenda



- Section 1: Latest Features & Updates
- Section 2: Highlights
- Section 3: Roadmap & Community



KubeCon



CloudNativeCon

North America 2019

# Latest Features & Updates

*Steven Zou / [szou@vmware.com](mailto:szou@vmware.com),  
Staff Engineer at VMware, Harbor Core Maintainer*



# Quota Management

Enhance the regular registry operation capability to improve the efficiencies of resource allocation

- Allow system admin to set quota threshold per projects from two factors:
- count of artifacts (images & charts)
  - storage size

1.9 ► Storage size:  
- sum the blob size + manifest size  
- **shared blob in the project scope will be only counted once**

- Push requests:  
- rejected if reaches the pre-defined quota threshold

- Deallocate:  
- allocated quota freed immediately after deletion



New Project

Project Name \*

Access Level  Public

Count quota

Storage quota  GB

Set quota while creating project

## Project Quotas

Default artifact count per project  [EDIT](#)  
Default disk space per project

Project	Owner	Count	Storage
kubecon	admin	<div style="width: 10%;">1 of 10</div>	<div style="width: 10%;">140.47MB of 2GB</div>
quota	admin	<div style="width: 100%;">5 of 5</div>	<div style="width: 100%;">711.68MB of 1GB</div>
scanners	admin	<div style="width: 66.67%;">4 of 6</div>	<div style="width: 66.67%;">805.47MB of 1GB</div>
library	admin	<div style="width: 0%;">0 of unlimited</div>	<div style="width: 0%;">0Byte of unlimited</div>

Project quota management

# Tag Retention

Provide an automated approach of cleaning tags from Harbor based on various rules.

## ► Rule based:

- retain always (retain all)
- based on **pull time**
  - most recently pulled # artifacts (count numbers)
  - pulled within X days (time)
- based on **push time**
  - most recently pushed # artifacts (count numbers)
  - pushed within Y days (time)
- positive calculate approach (get all the retained ones by the rules and clean the left ones)

## ► Filter by tag

## ► Trigger: run now / schedule

- dry run (create result preview, no actual actions taken)

## ► Report:

- execution history recorded
- detailed report in the log text stream (retained/deleted/error)



1.9

Retention rules **5/15**

ACTION **v**  
ACTION **v**  
ACTION **v**  
ACTION **v**  
ACTION **v**

For the repositories matching \*\*, retain always with tags matching latest\*  
For the repositories matching \*scanner\*, retain the most recently pulled 5 images with tags excluding \*test\*  
For the repositories matching \*scanner\*, retain the most recently pushed 5 images with tags matching release.\*  
For the repositories matching quota\*, retain the images pushed within the last 15 days with tags excluding \*test\*  
For the repositories matching quota\*, retain the images pulled within the last 10 days with tags matching dev-\*

**ADD RULE** Click the ADD RULE button to add a rule.

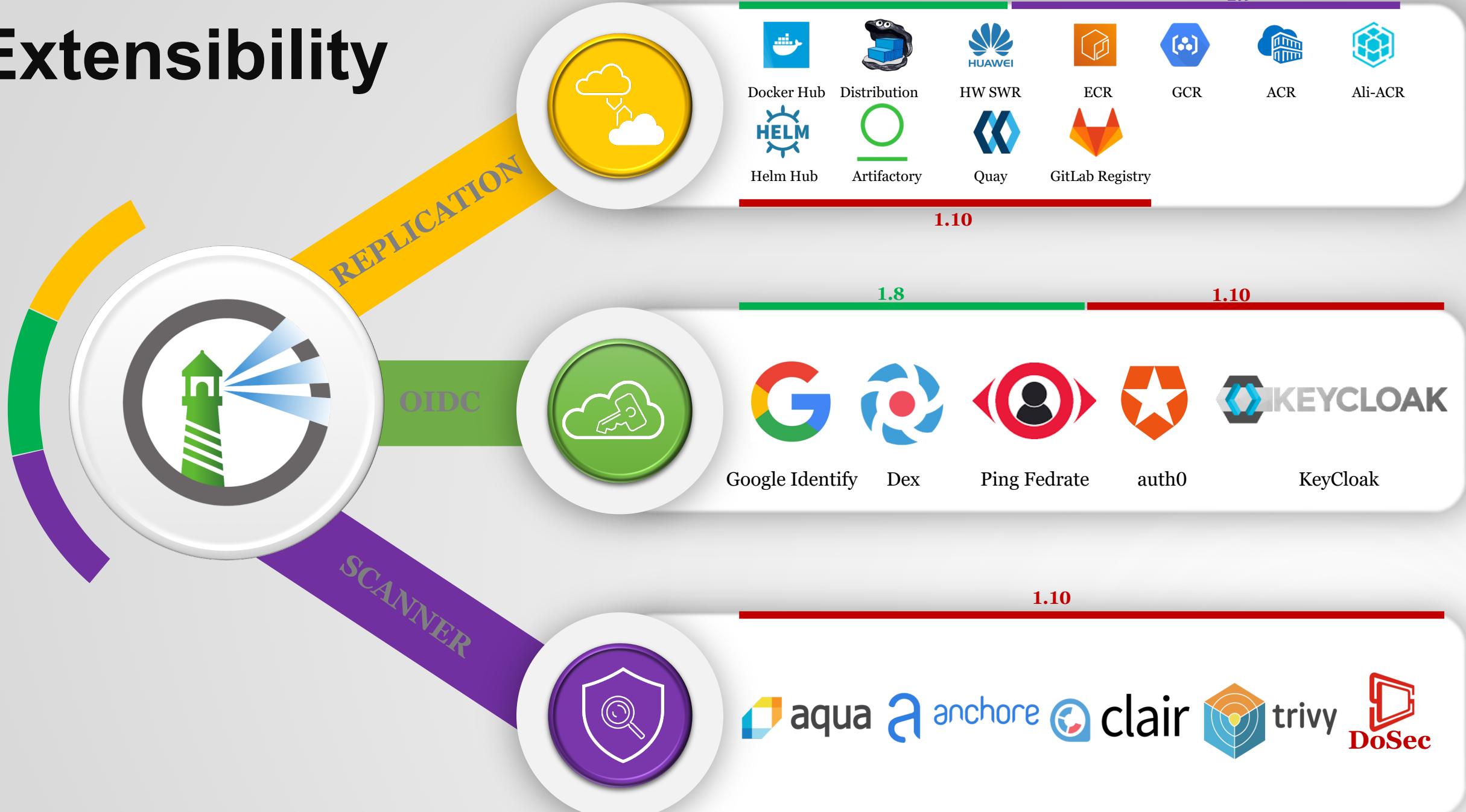
Schedule None **EDIT**

**RUN NOW** **DRY RUN**  **ABORT**

Retention runs

ID	Status	Dry Run	Execution Type	Start Time	Duration
2	Succeed	YES	Manual	Nov 11, 2019, 10:17:50 PM	0
Repository	Status	Retained/Total	Start Time	Duration	Log
golang	Success	1/1	Nov 11, 2019, 10:17:50 PM	1sec	<a href="#">Log</a>
mongo	Success	2/2	Nov 11, 2019, 10:17:50 PM	1sec	<a href="#">Log</a>
node	Success	1/1	Nov 11, 2019, 10:17:50 PM	1sec	<a href="#">Log</a>
					1 - 3 of 3 items
1	Succeed	YES	Manual	Nov 5, 2019, 9:33:22 AM	5sec
					1 - 2 of 2 items

# Extensibility





KubeCon



CloudNativeCon

North America 2019

# Highlight: Pluggable Scanner

*Daniel Pacak / [daniel.pacak@aquasec.com](mailto:daniel.pacak@aquasec.com),  
OSS Engineer at Aqua Security, Harbor Maintainer*



# Not All Scanners Are Created Equal

Which package versions have vulns?

Is package patched for this vuln in this distro?

Additional info from vendor

Additional info from security researchers



## Options

- Open Source
- Free
- Commercial

Relevant, up-to-date information sources /  
Accuracy & rate of false positives

Support for language packages

Malware scanning

Sensitive data checks

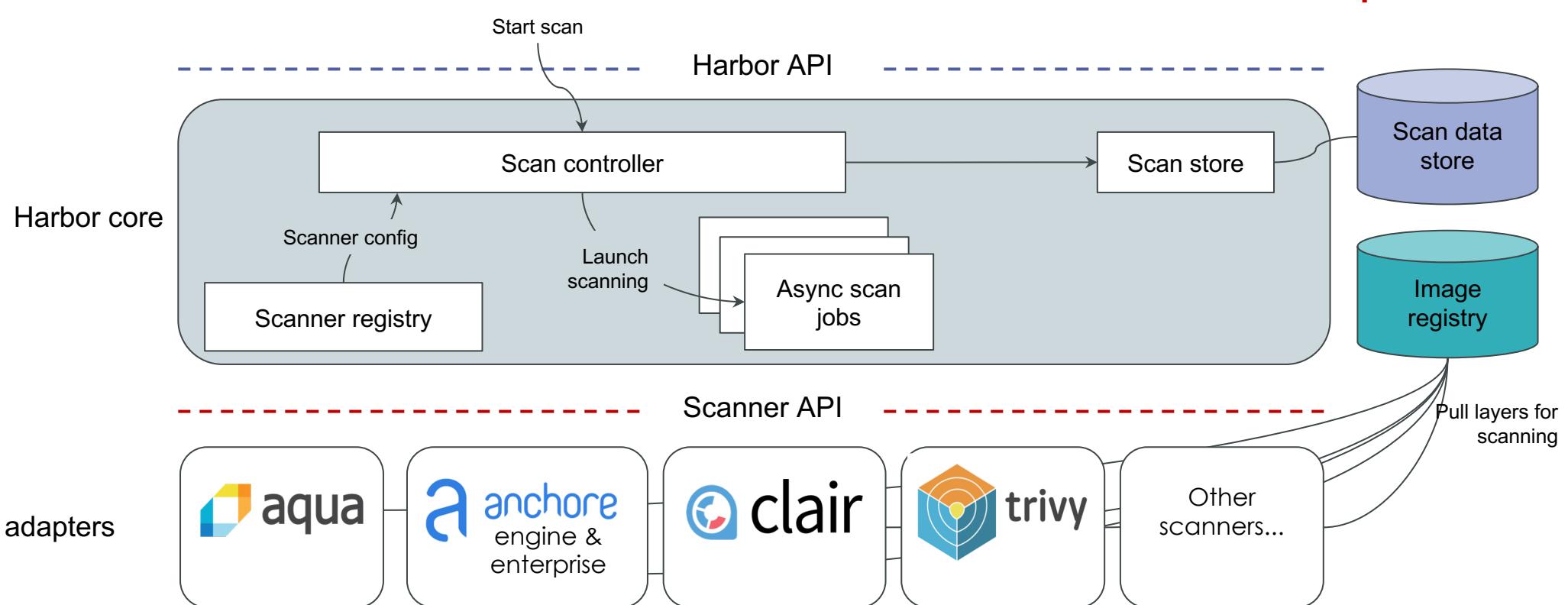
Windows containers

Functionality / Commercial information sources / Support

# Pluggable Scanner in Harbor

► Use your preferred scanner per-project configuration

Scanner	
GET	/metadata Get scanner metadata
POST	/scan Accept artifact scanning request
GET	/scan/{scan_request_id}/report Get scan report



# Scanner Registry

«

- Projects
- Logs
- Administration
  - Users
  - Registries
  - Replications
  - Labels
  - Project Quotas
  - Interrogation Services
  - Garbage Collection
  - Configuration

Interrogation Services

Scanners Vulnerability

+ NEW SCANNER SET AS DEFAULT ACTION ▾

	Name	Endpoint	Health	Enabled	Authorization
○	Trivy	https://harbor-scanner-trivy:8443	Healthy	true	None
<b>Scanner:</b> Name: Trivy Vendor: Aqua Security Version: 0.2.0					
<b>Capabilities</b> 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]					
<b>Properties</b> harbor.scanner-adapter/scanner-type: os-package-vulnerability org.label-schema.build-date: 2019-11-14T21:45:53Z org.label-schema.vcs: https://github.com/aquasecurity/harbor-scanner-trivy org.label-schema.vcs-ref: a03ccd680b218132094bca8188d80bfb461702c2 org.label-schema.version: 0.1.0-rc2					
○	> Aqua CSP Scanner	https://harbor-scanner-aqua:8443	Healthy	true	None
○	> Clair	http://clair-adapter:8080	Unhealthy	true	None

# Scan Reports

The image shows a code editor interface with two tabs: "scan-request.json" and "scan-report.json".

**scan-request.json:**

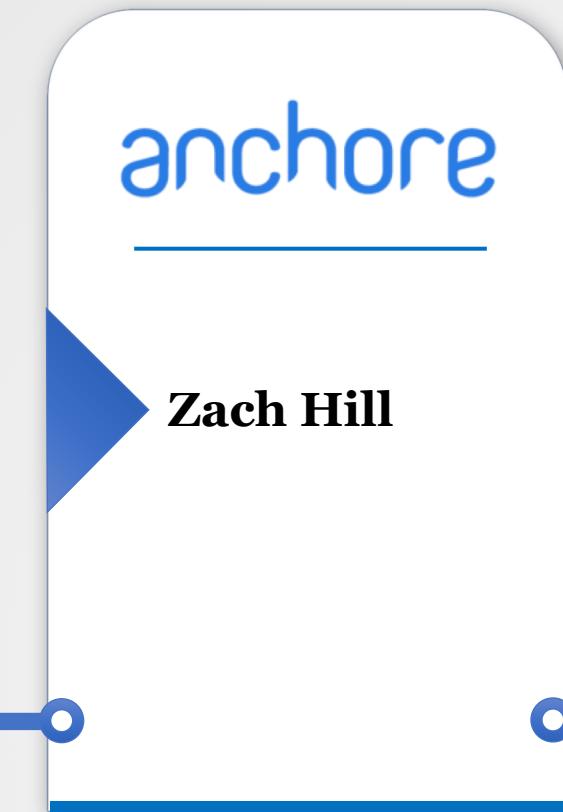
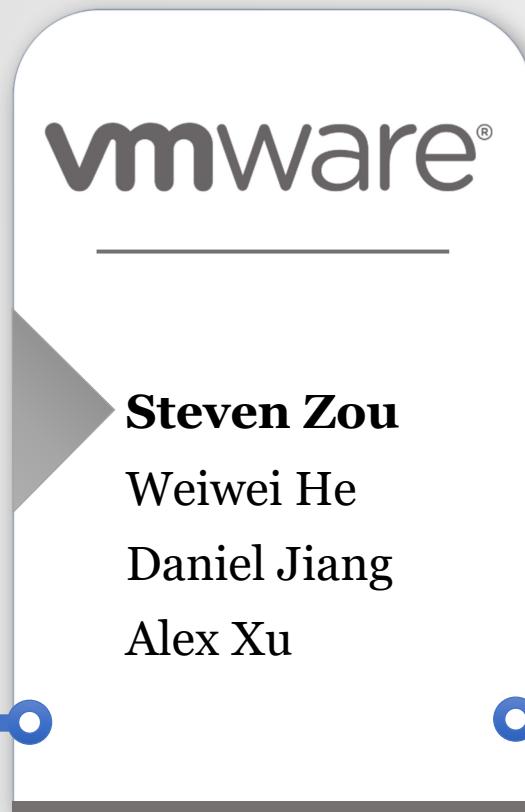
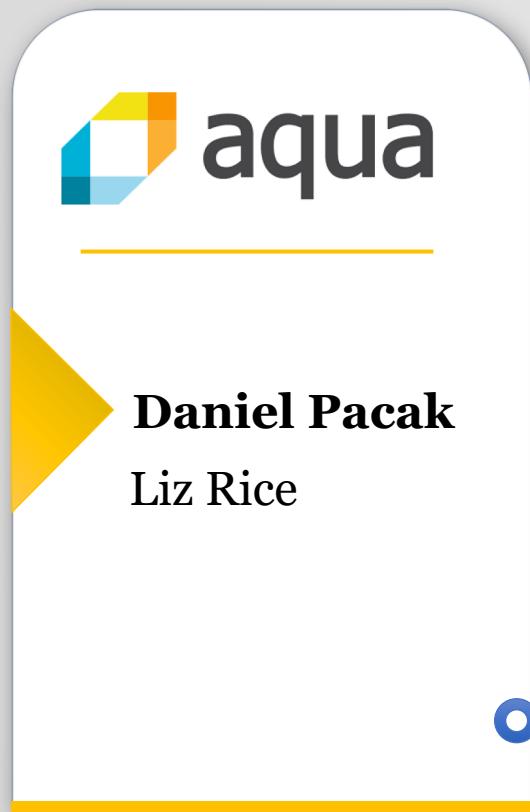
```
1 {  
2   "registry": {  
3     "url": "https://core.harbor.domain",  
4     "authorization": "Basic "  
5   },  
6   "artifact": {  
7     "mime_type": "application/vnd.docker.distribution.manifest.v2+json",  
8     "repository": "library/alpine",  
9     "tag": "3.10.2",  
10    "digest": "sha256:917..."  
11  }  
12}  
13
```

**scan-report.json:**

```
1 {  
2   "generated_at": "2019-08-07T12:17:21.854Z",  
3   "artifact": {  
4     "mime_type": "application/vnd.docker.distribution.manifest.v2+json",  
5     "repository": "library/alpine",  
6     "tag": "3.10.2",  
7     "digest": "sha256:917..."  
8   },  
9   "scanner": {  
10    "name": "Trivy",  
11    "vendor": "Aqua Security",  
12    "version": "0.2.1"  
13  },  
14  "severity": "Medium",  
15  "vulnerabilities": [  
16    {  
17      "id": "CVE-2019-1549",  
18      "package": "openssl",  
19      "version": "1.1.1c-r0",  
20      "fix_version": "1.1.1d-r0",  
21      "severity": "Medium",  
22      "description": "...",  
23      "links": [  
24        {}  
25      ]  
26    }  
27  ]
```

# Delivered by the Scanning Workgroup

Joint work across multiple organizations in Harbor community





KubeCon



CloudNativeCon

North America 2019

# Highlight: Cloud Native Artifact Registry

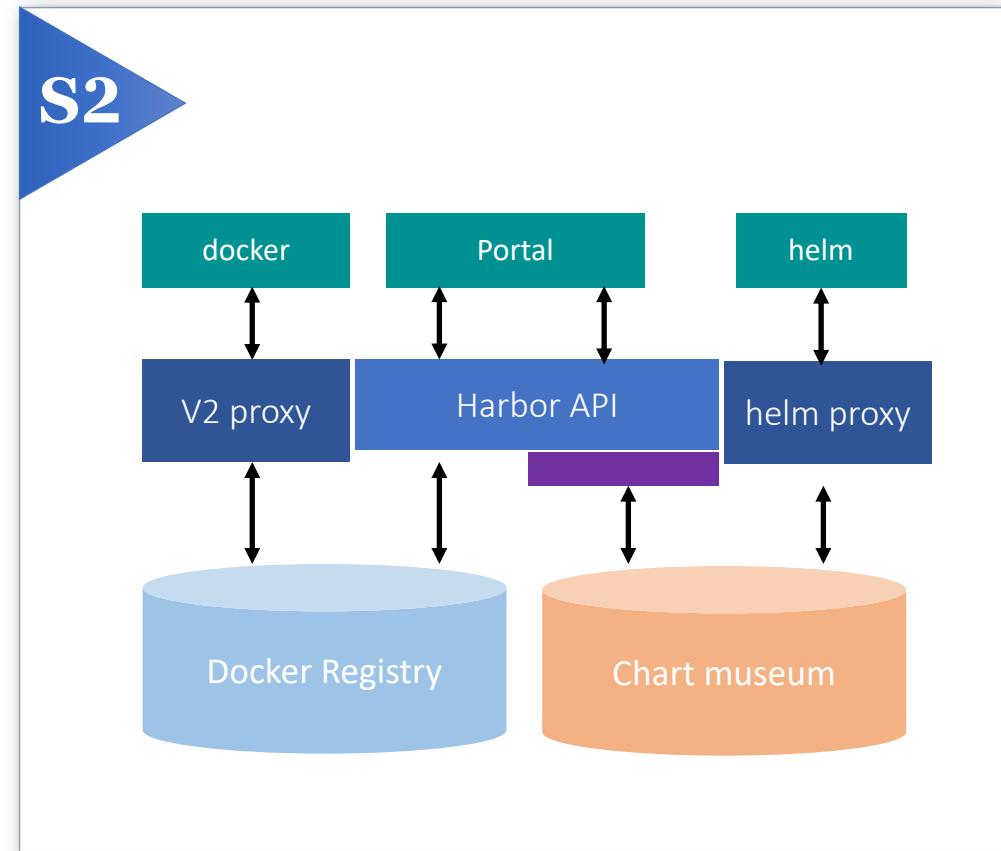
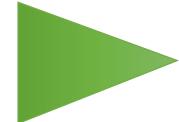
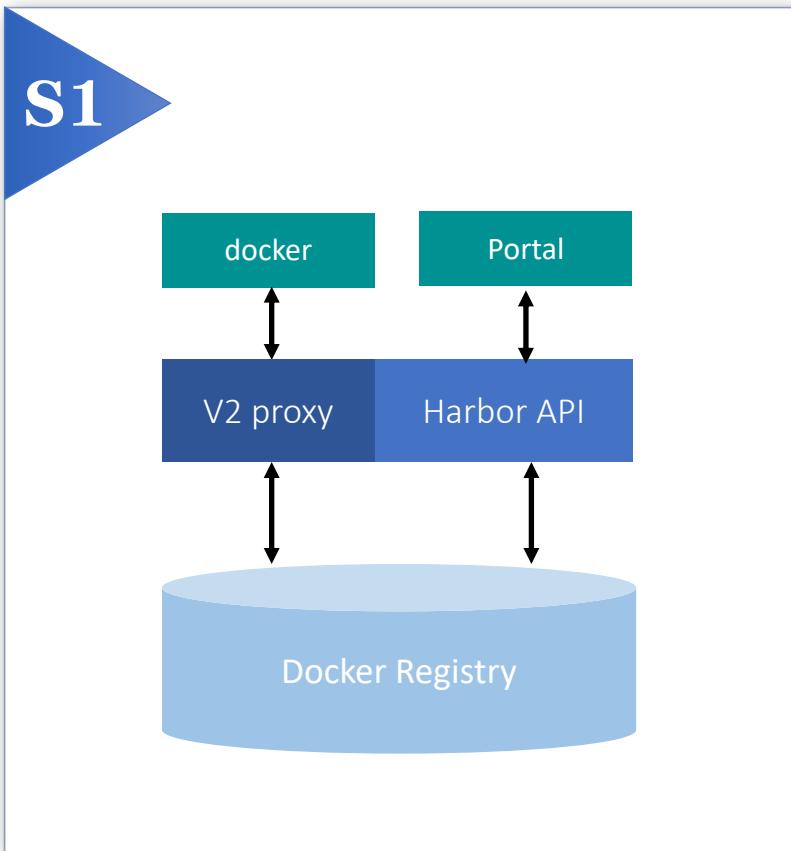
*Daniel (Tan) Jiang / [jiangd@vmware.com](mailto:jiangd@vmware.com)*

*Staff Engineer at VMware, Harbor Core Maintainer*



# Expansion From an Image Registry

By proxying different servers

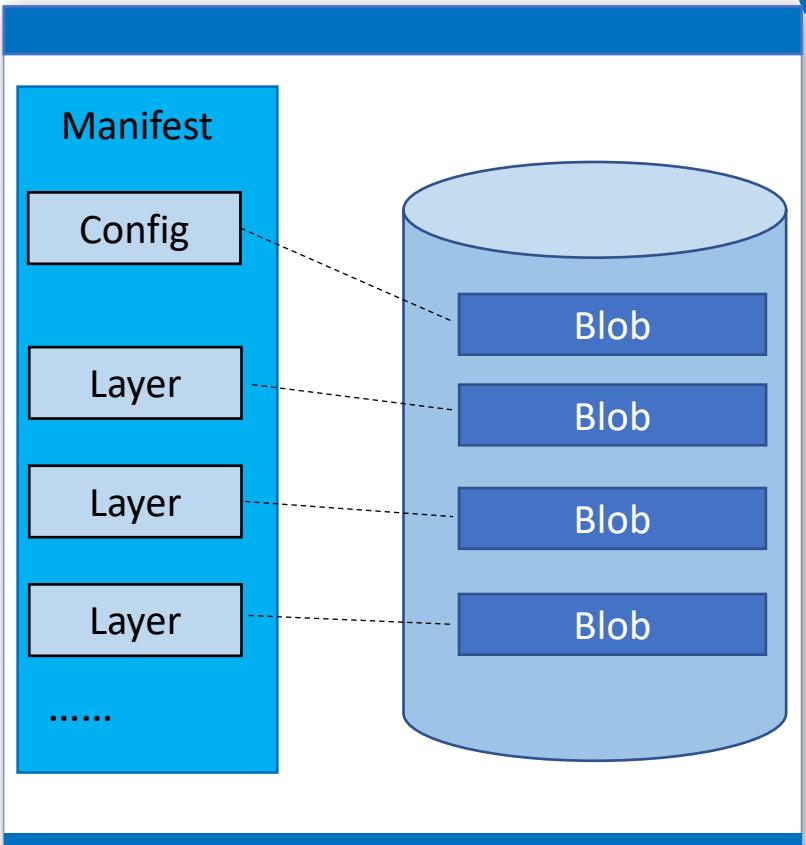


**This works ...**



**BUT ...**

# OCI Artifacts



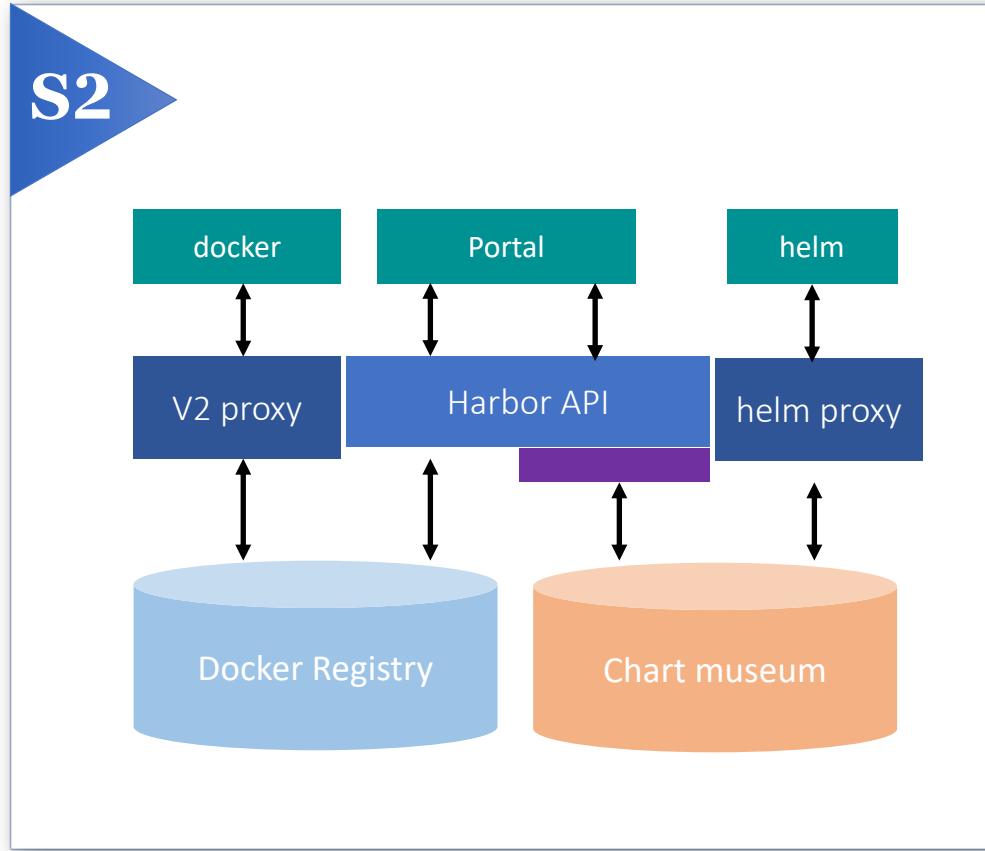
- ... registries were designed to support small to really large “files”, with security and a layered, cross-referenceable file system, that works across the internet and within a datacenter, registries can support just about any artifact type.

Steve Lasker

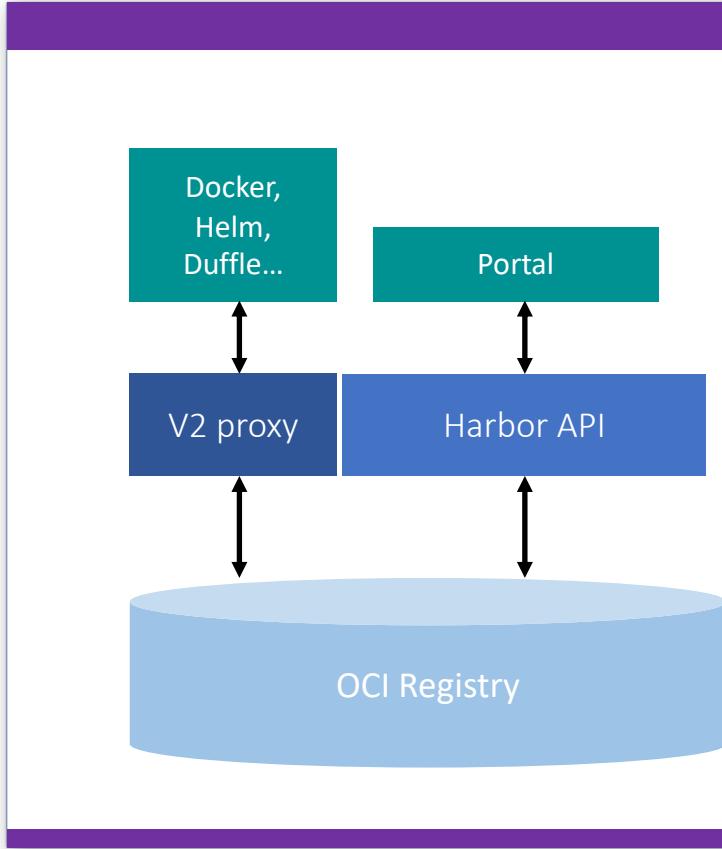
[Cloud native artifact stores evolve from container registries](#)

- “oras” for pushing anything to OCI registry:  
<https://github.com/deislabs/oras>
- Repository created for “OCI artifacts”  
<https://github.com/opencontainers/artifacts>

# Expansion From an Image Registry

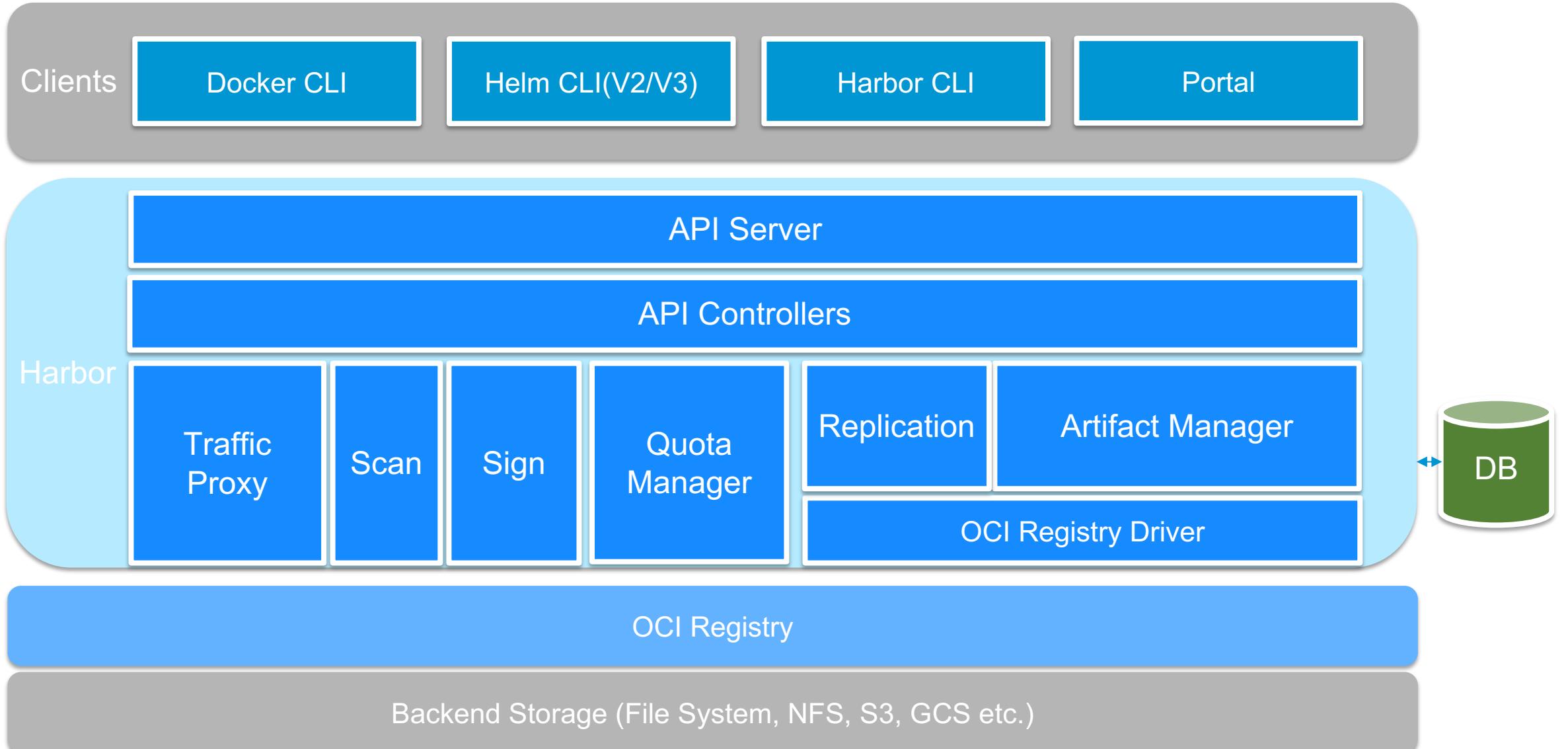


# OCI Registry as a Single Storage Service for All Artifacts



- Simpler deployment, configuration, scaling out
- Provide one set of V2 API to manage ALL artifacts
  - GET /api/repositories/{repo}/tags
  - GET /api/chartrepo/{repo}/charts
  - > GET /api/v2/projects/{p-id}/repositories/{r-id}/artifacts
- Support for index (manifest list)
- Aggregated view for all artifacts under a project/repository
- Consistent management features for all artifact

# Opportunity for Architecture Evolution





KubeCon



CloudNativeCon

North America 2019

# Roadmap & Harbor Community

*Michael Michael / [michaelmi@vmware.com](mailto:michaelmi@vmware.com),  
Director of Product Management at VMware, Harbor Core Maintainer*



# Roadmap

1



Management



Perf & Scale



K8s  
Operator



Signing Policy  
Replication



Metadata  
Management



Observability

2



Image  
Distribution



P2P  
Distribution



Proxy Cache

3



Extensibility



Cloud Native  
Artifact Management



Webhook++

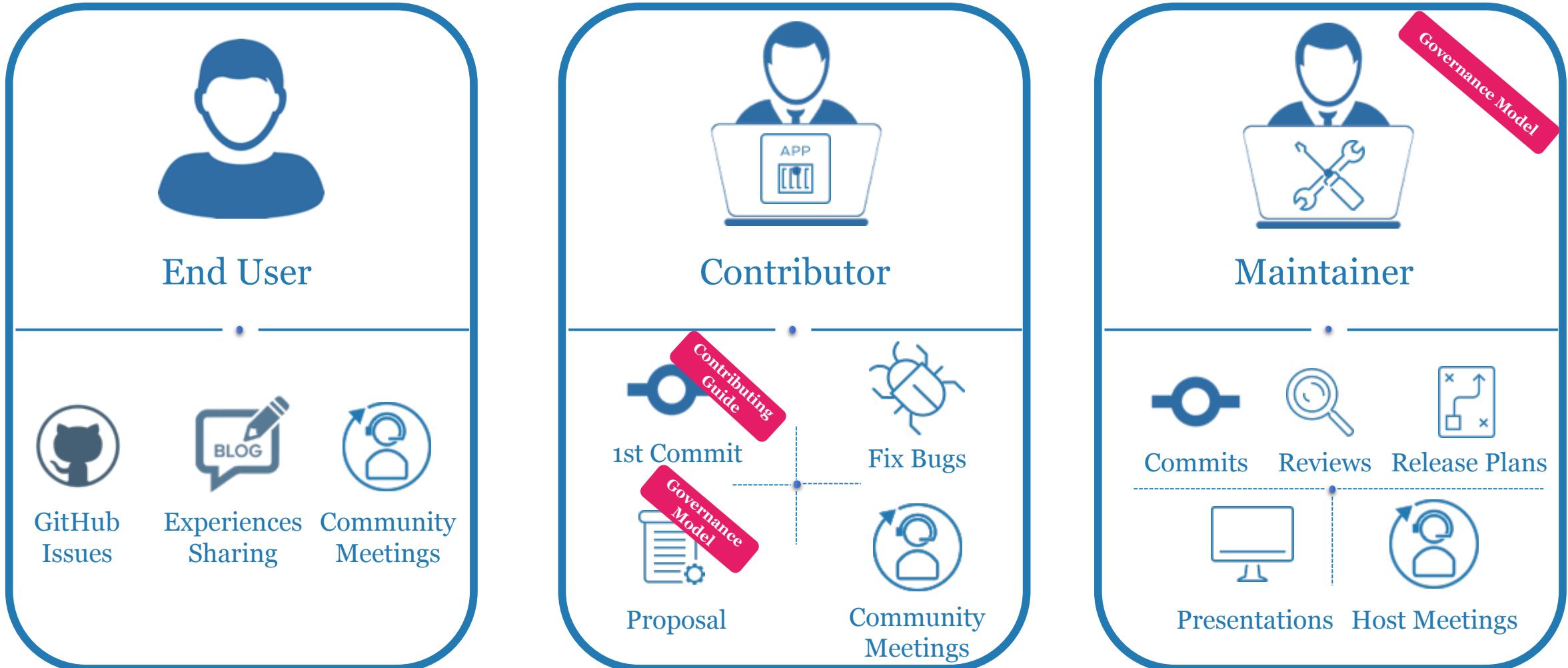


Interrogation  
Service++

# The Community is Thriving

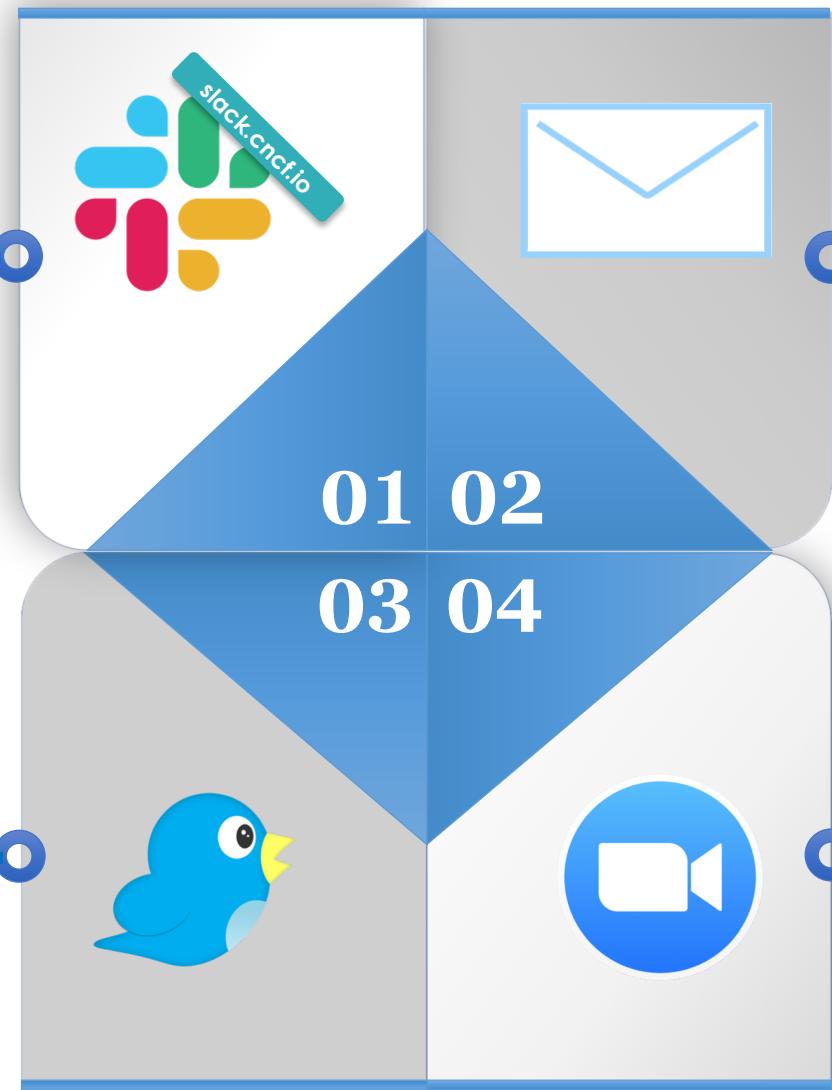


# Levels of Participation



# Collaborate with the Harbor Team

#harbor  
#harbor-dev



lists.cncf.io/g/harbor-users  
lists.cncf.io/g/harbor-dev

@project\_harbor

[github.com/goharbor/community/blob/  
master/MEETING\\_SCHEDULE.md](https://github.com/goharbor/community/blob/master/MEETING_SCHEDULE.md)

APAC + EU zone: **9pm** UTC+8 time zone  
Americas + EU zone: **1pm** Pacific time zone

