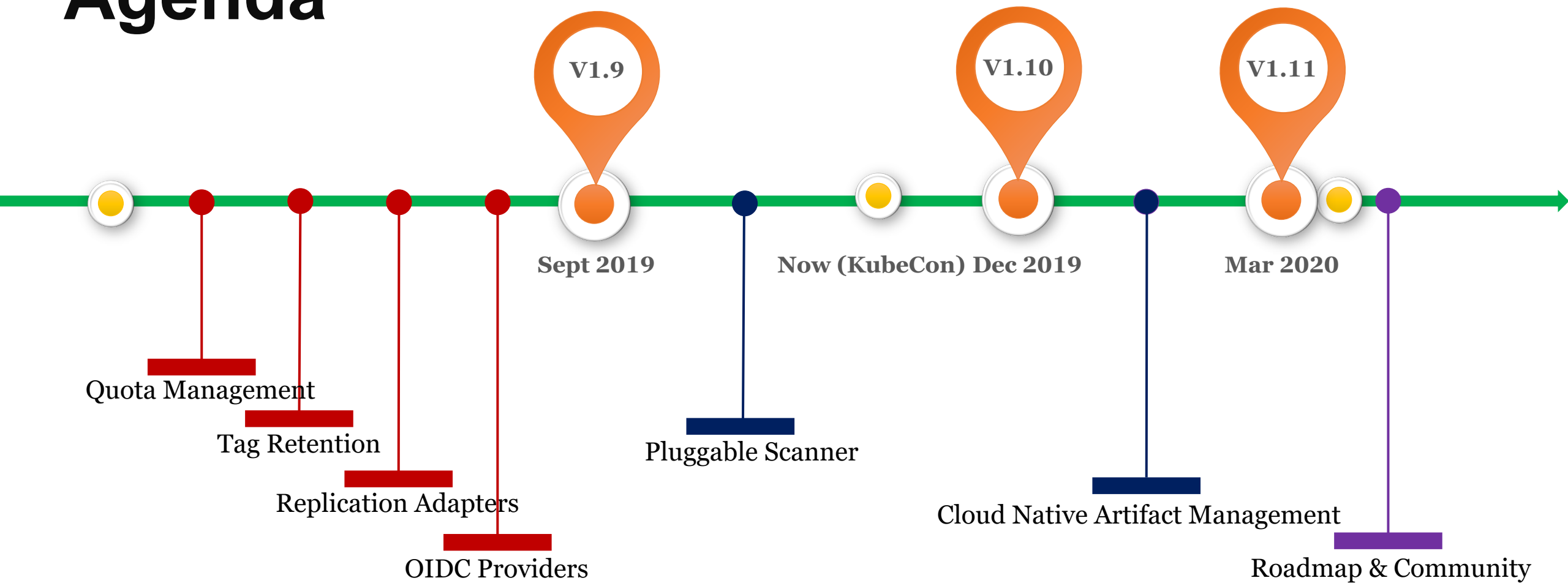

KubeCon
CloudNativeCon
North America 2019

Deep Dive: Harbor

Steven Zou / szou@vmware.com, Staff Engineer at VMware, Harbor Core Maintainer
Daniel Jiang / jiangd@vmware.com, Staff Engineer at VMware, Harbor Core Maintainer

Agenda



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

Latest Features & Updates

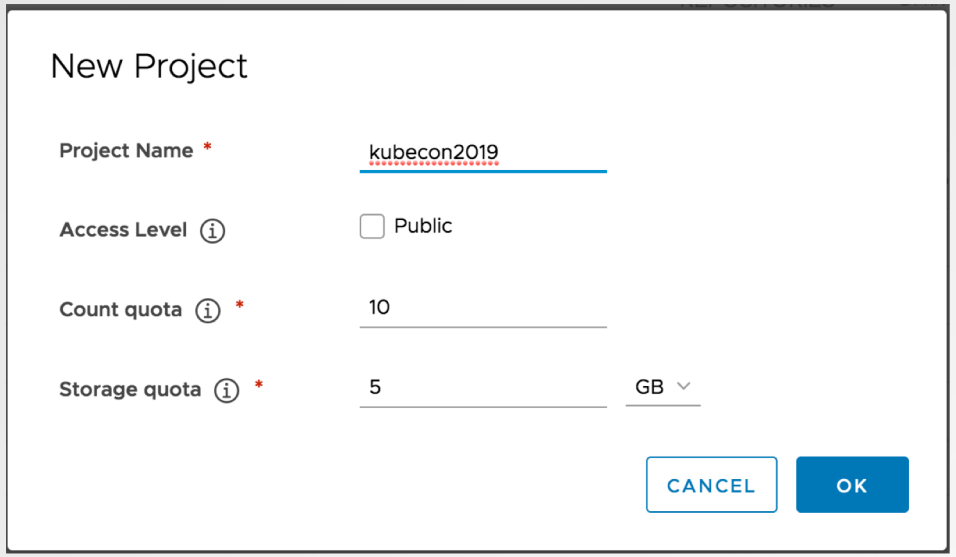
Steven Zou / szou@vmware.com,
Staff Engineer at VMware, Harbor Core Maintainer

Quota Management

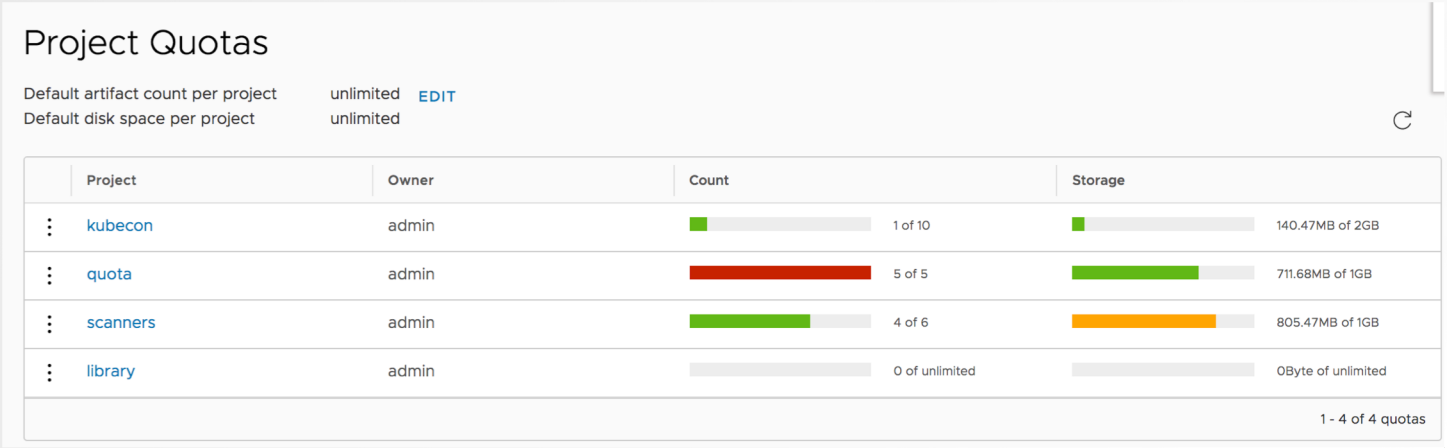
Enhance the regular registry operation capability to improve the efficiencies of resource allocation

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

1.9



Set quota while creating project



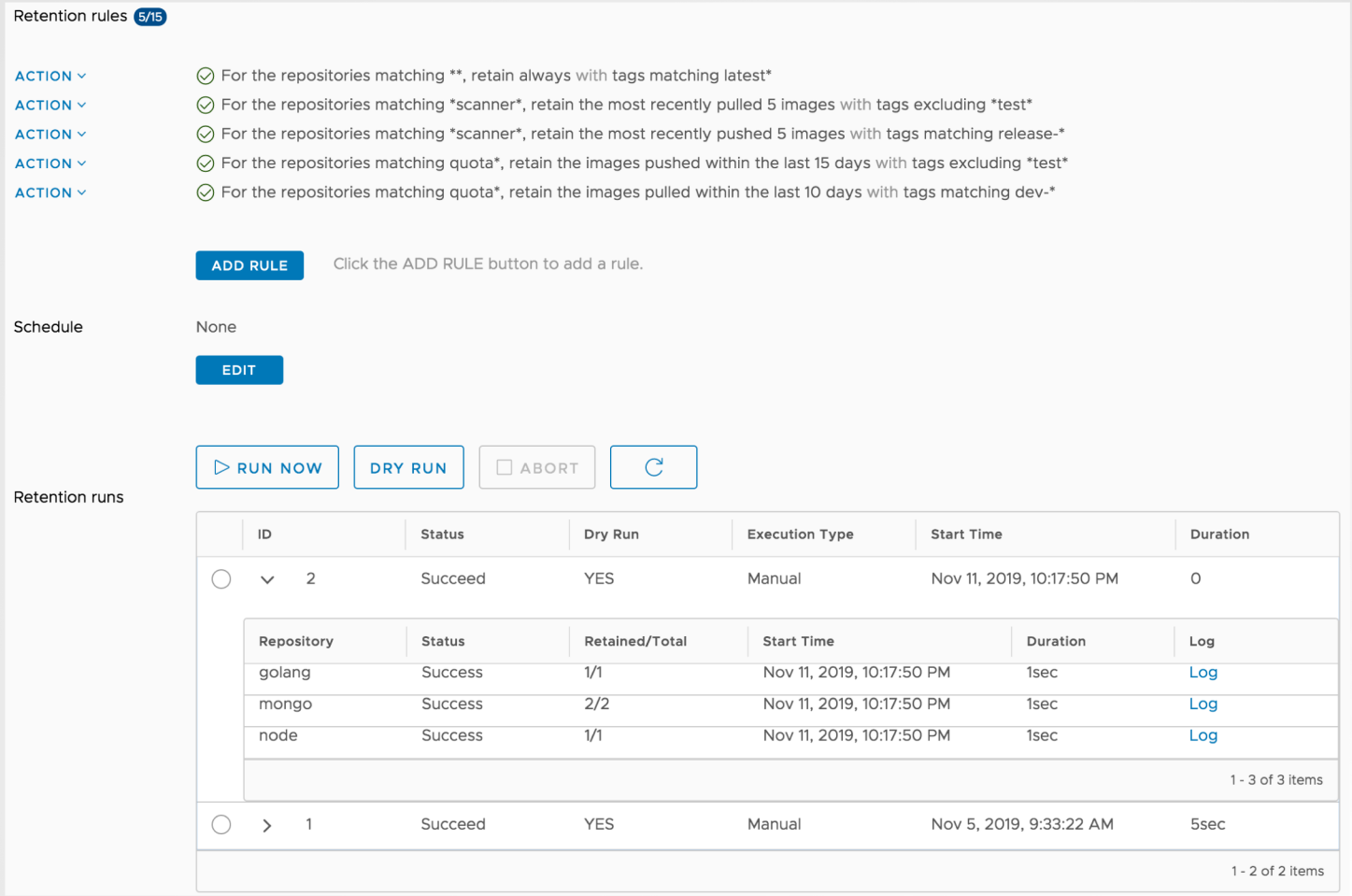
Project quota management

Tag Retention

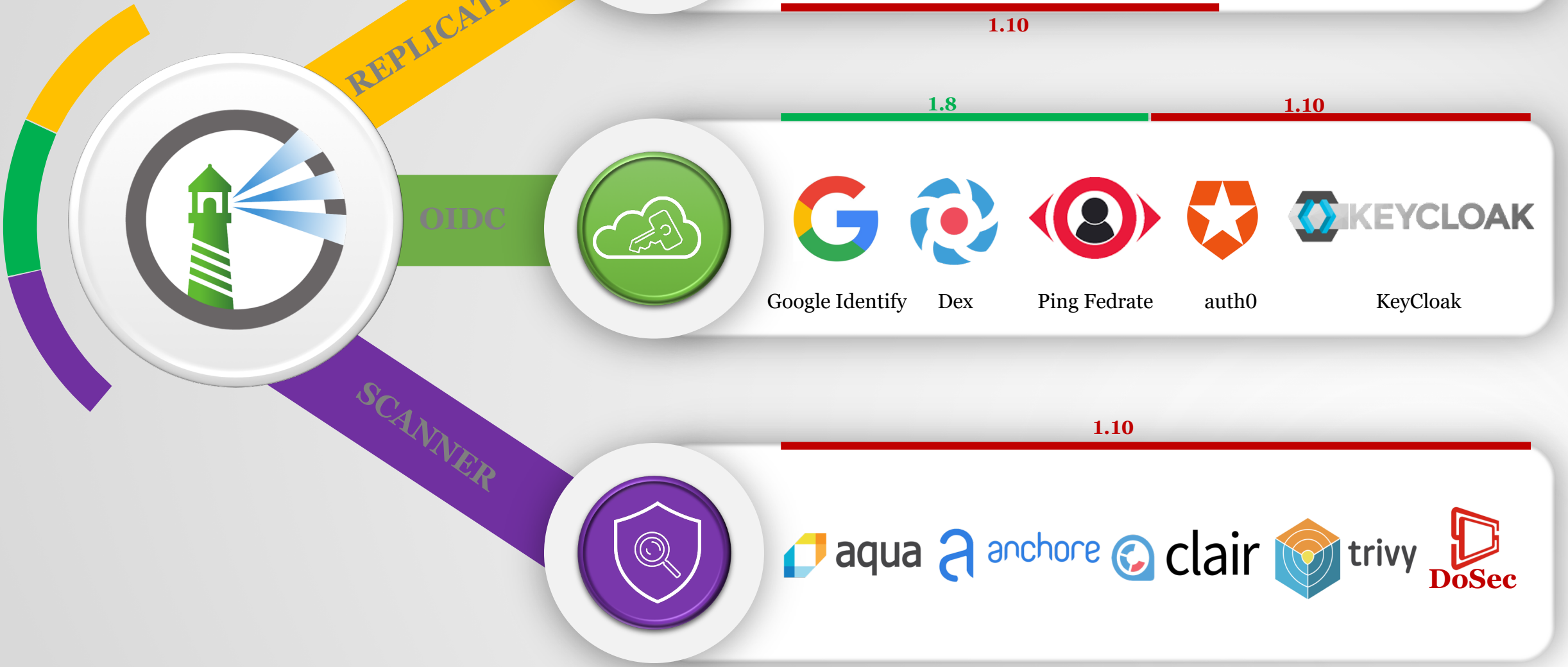
Provide an automated approach of cleaning tags from Harbor based on various rules.

- 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



Extensibility



Highlight: Pluggable Scanner

Daniel Pacak / 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

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

Options

- Open Source
- Free
- Commercial

Support for language packages

Malware scanning

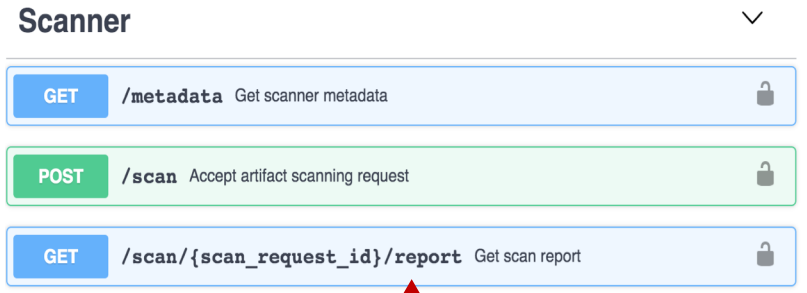
Sensitive data checks

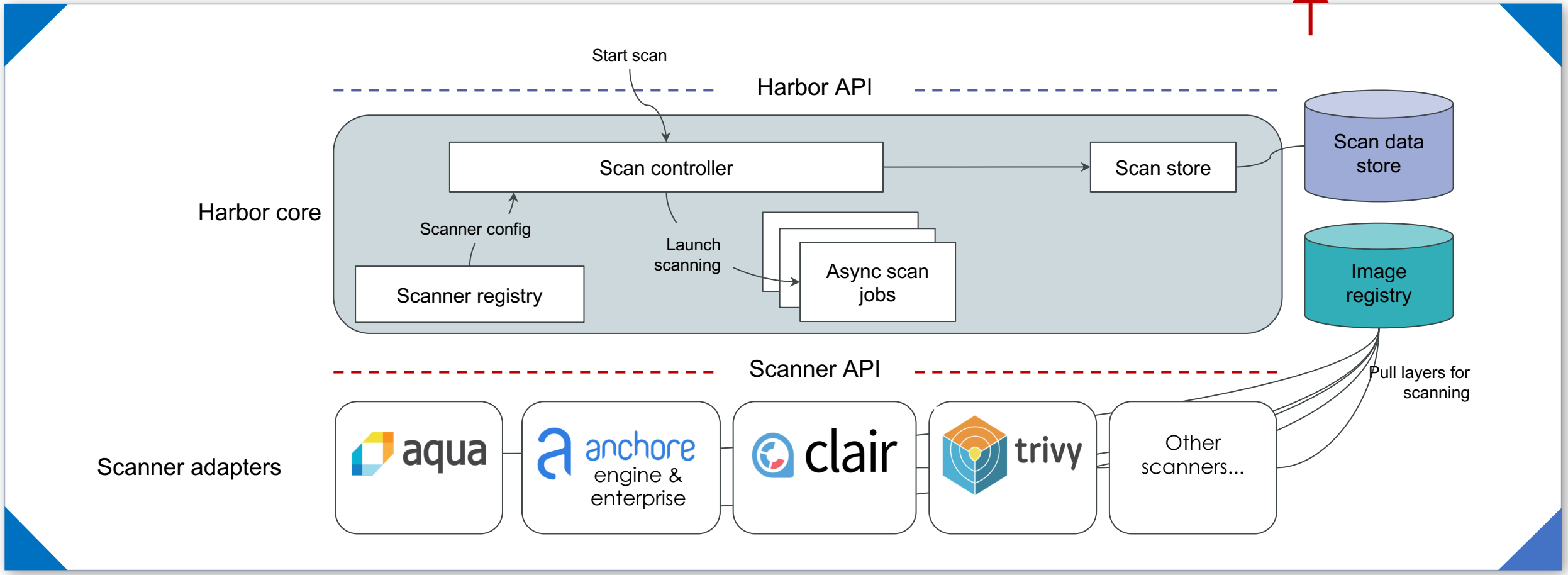
Windows containers

Functionality / Commercial information sources / Support

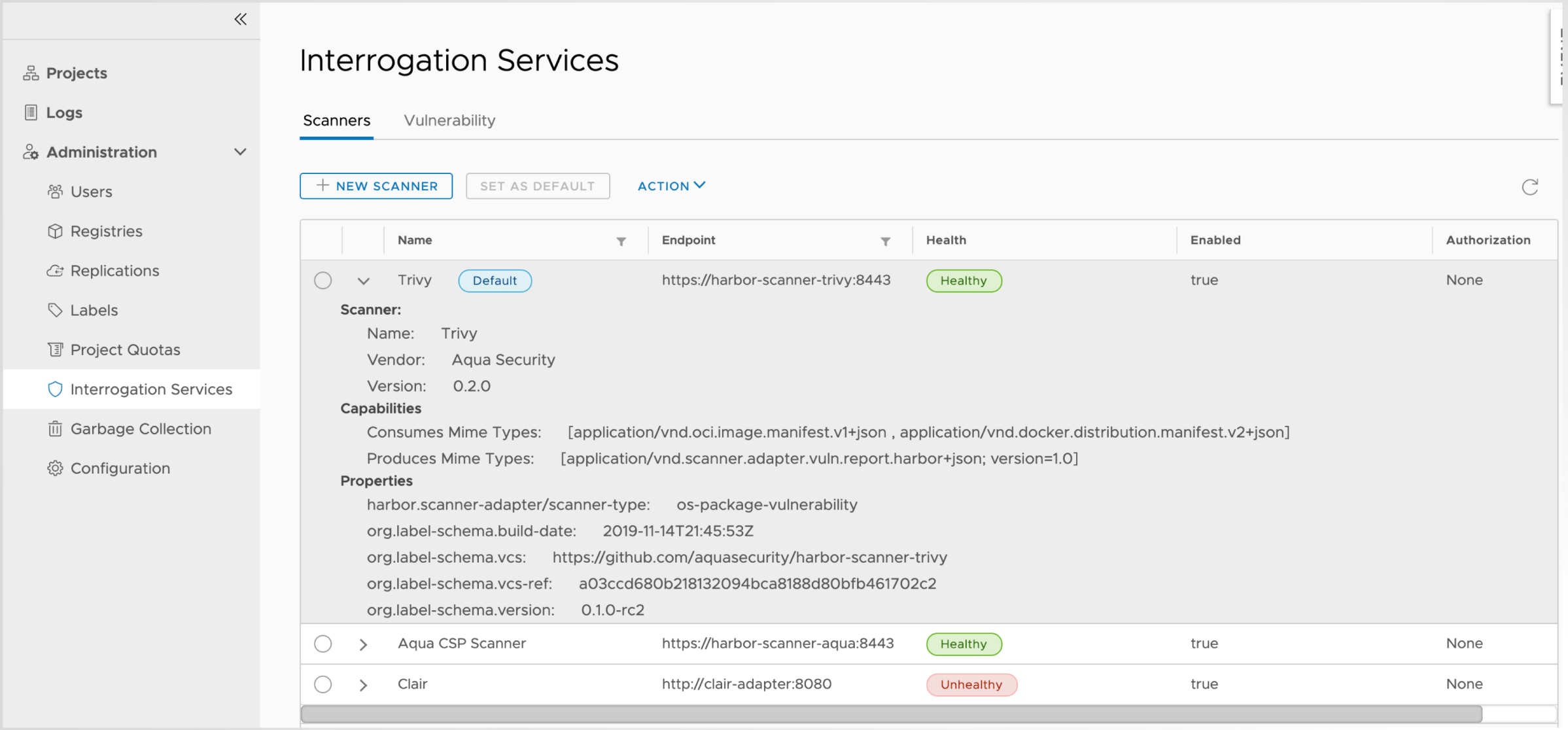
Pluggable Scanner in Harbor

Use your preferred scanner per-project configuration





Scanner Registry



Scan Reports

scan-request.json

```json
{
  "registry": {
    "url": "https://core.harbor.domain",
    "authorization": "Basic "
  },
  "artifact": {
    "mime_type": "application/vnd.docker.distribution.manifest.v2+json",
    "repository": "library/alpine",
    "tag": "3.10.2",
    "digest": "sha256:917..."
  }
}
```

scan-report.json

```json
{
  "generated_at": "2019-08-07T12:17:21.854Z",
  "artifact": {
    "mime_type": "application/vnd.docker.distribution.manifest.v2+json",
    "repository": "library/alpine",
    "tag": "3.10.2",
    "digest": "sha256:917..."
  },
  "scanner": {
    "name": "Trivy",
    "vendor": "Aqua Security",
    "version": "0.2.1"
  },
  "severity": "Medium",
  "vulnerabilities": [
    {
      "id": "CVE-2019-1549",
      "package": "openssl",
      "version": "1.1.1c-r0",
      "fix_version": "1.1.1d-r0",
      "severity": "Medium",
      "description": "...",
      "links": [
      ]
    }
  ]
}
```

Delivered by the Scanning Workgroup

Joint work across multiple organizations in Harbor community

Daniel Pacak

Liz Rice

Steven Zou

Weiwei He

Daniel Jiang

Alex Xu

Zach Hill

Ye Liu

Maggie Ma

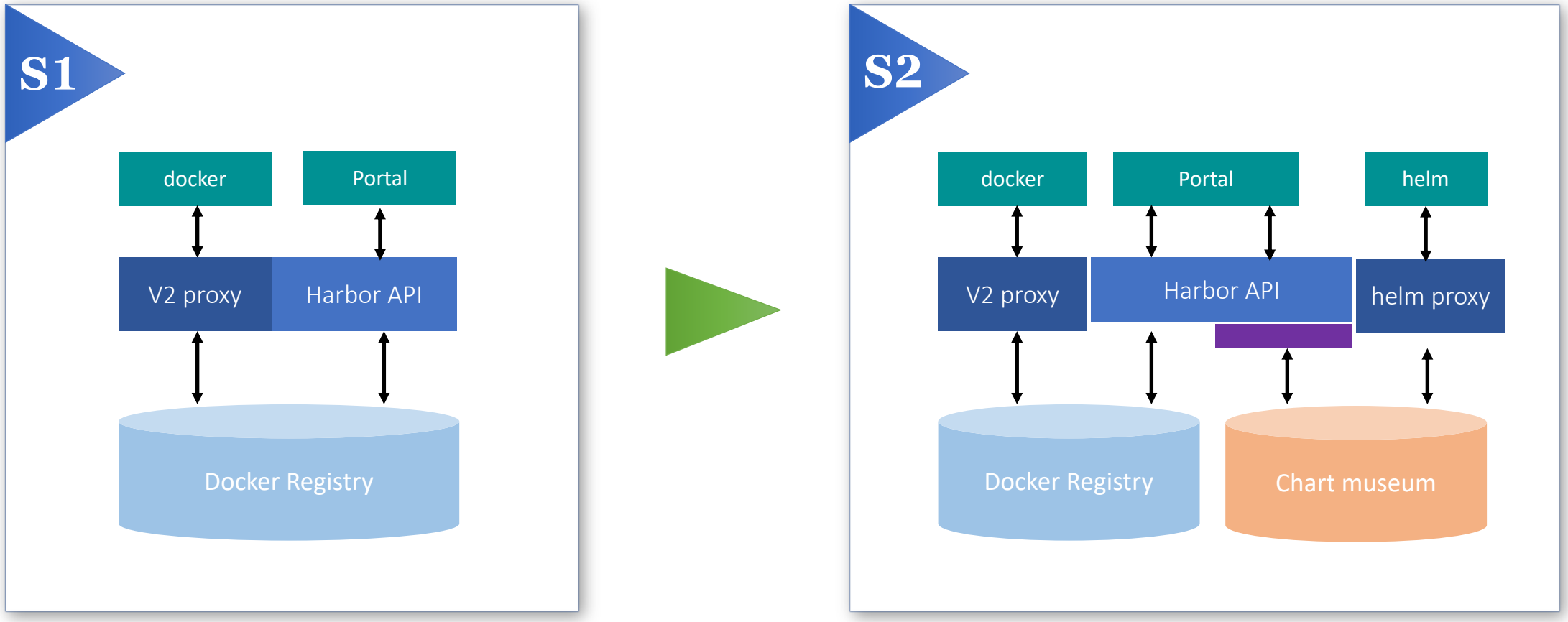
Discussion Notes: https://github.com/goharbor/community/blob/master/workgroups/wg-scanning/README.md

Highlight: Cloud Native Artifact Registry

Daniel (Tan) Jiang / jiangd@vmware.com
Staff Engineer at VMware, Harbor Core Maintainer

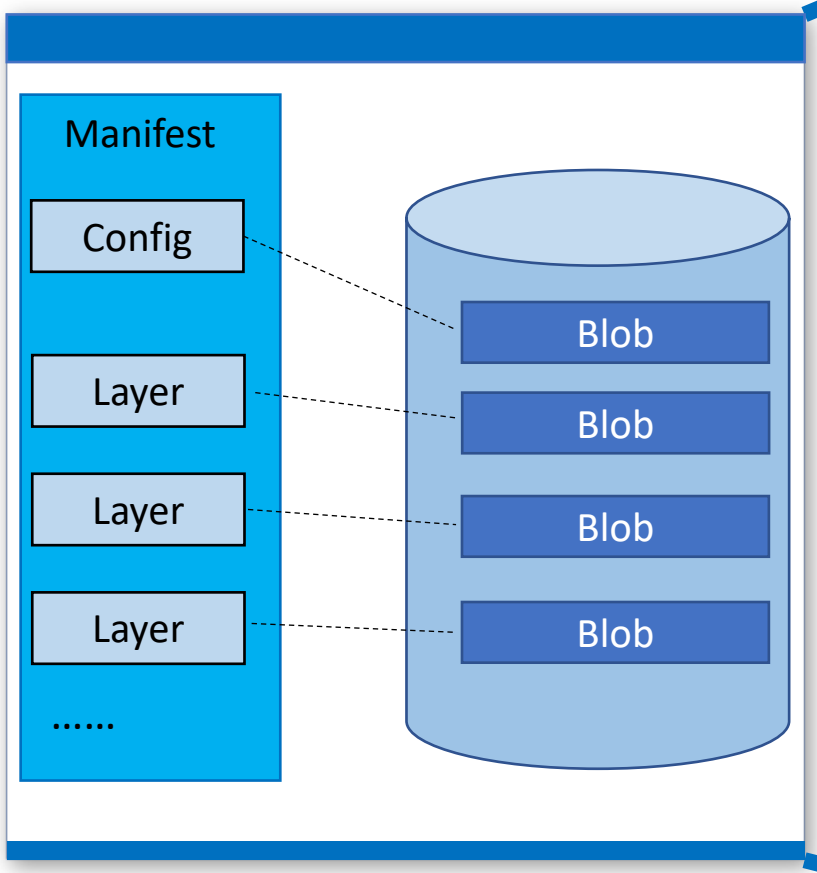
Expansion From an Image Registry

By proxying different servers



This works ...

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

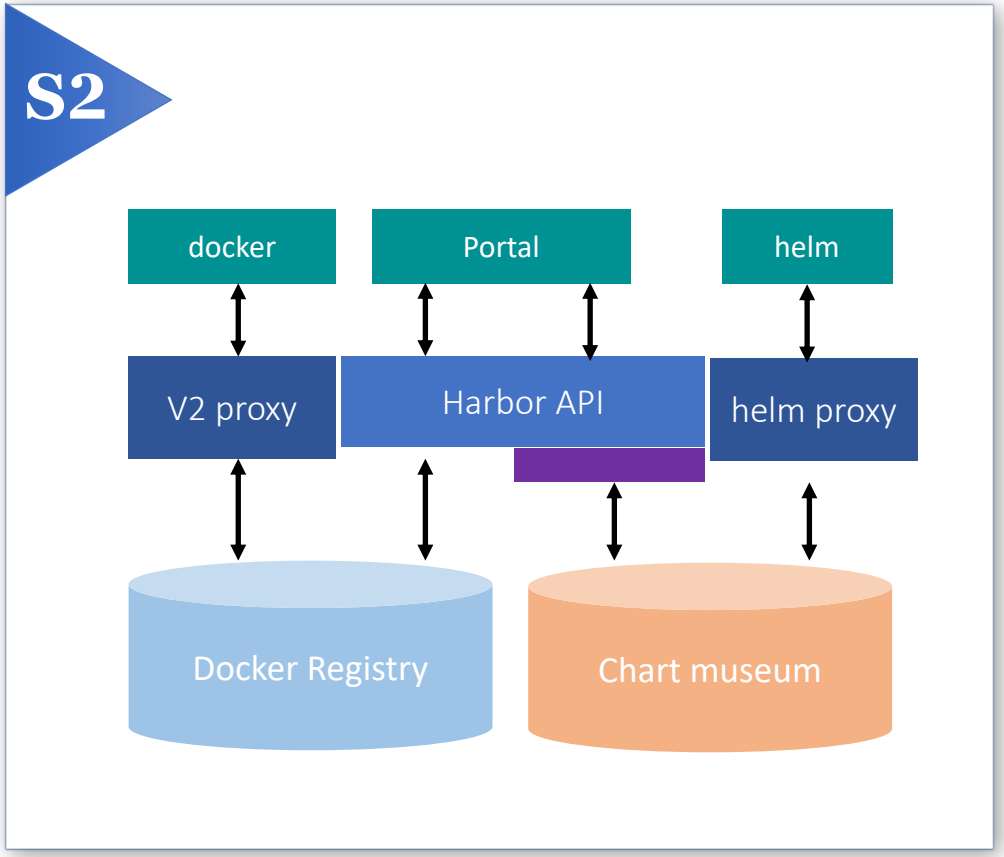
- "oras" for pushing anything to OCI registry:

  https://github.com/deislabs/oras

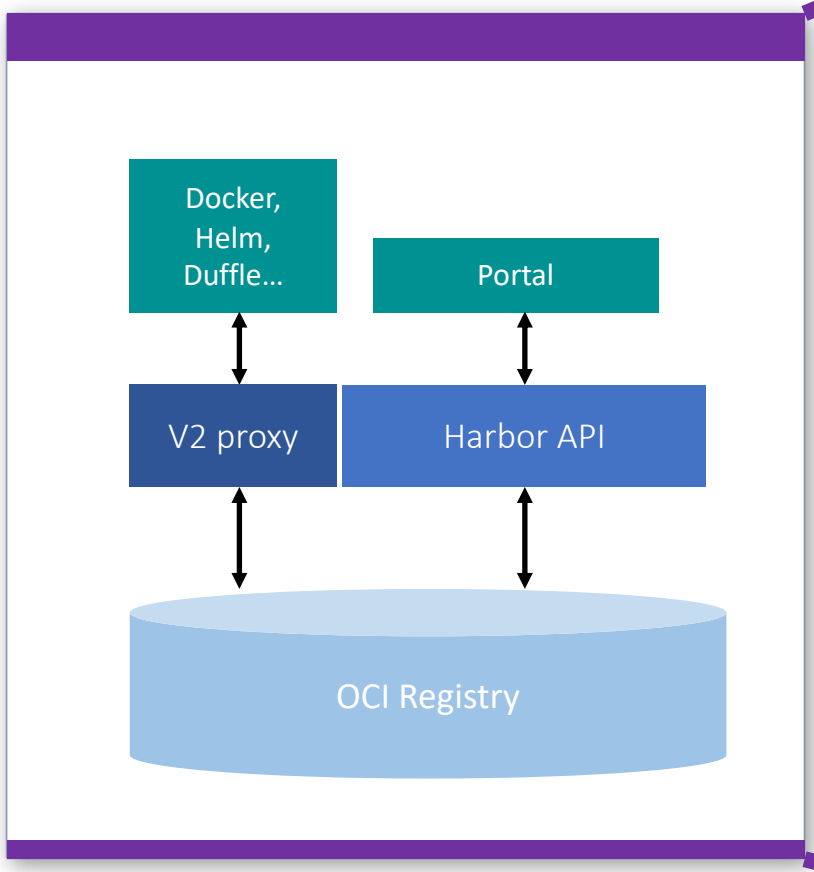
- Repository created for "OCI artifacts"

  https://github.com/opencontainers/artifacts

Expansion From an Image Registry



OCI Registry as a Single Storage Service for All Artifacts



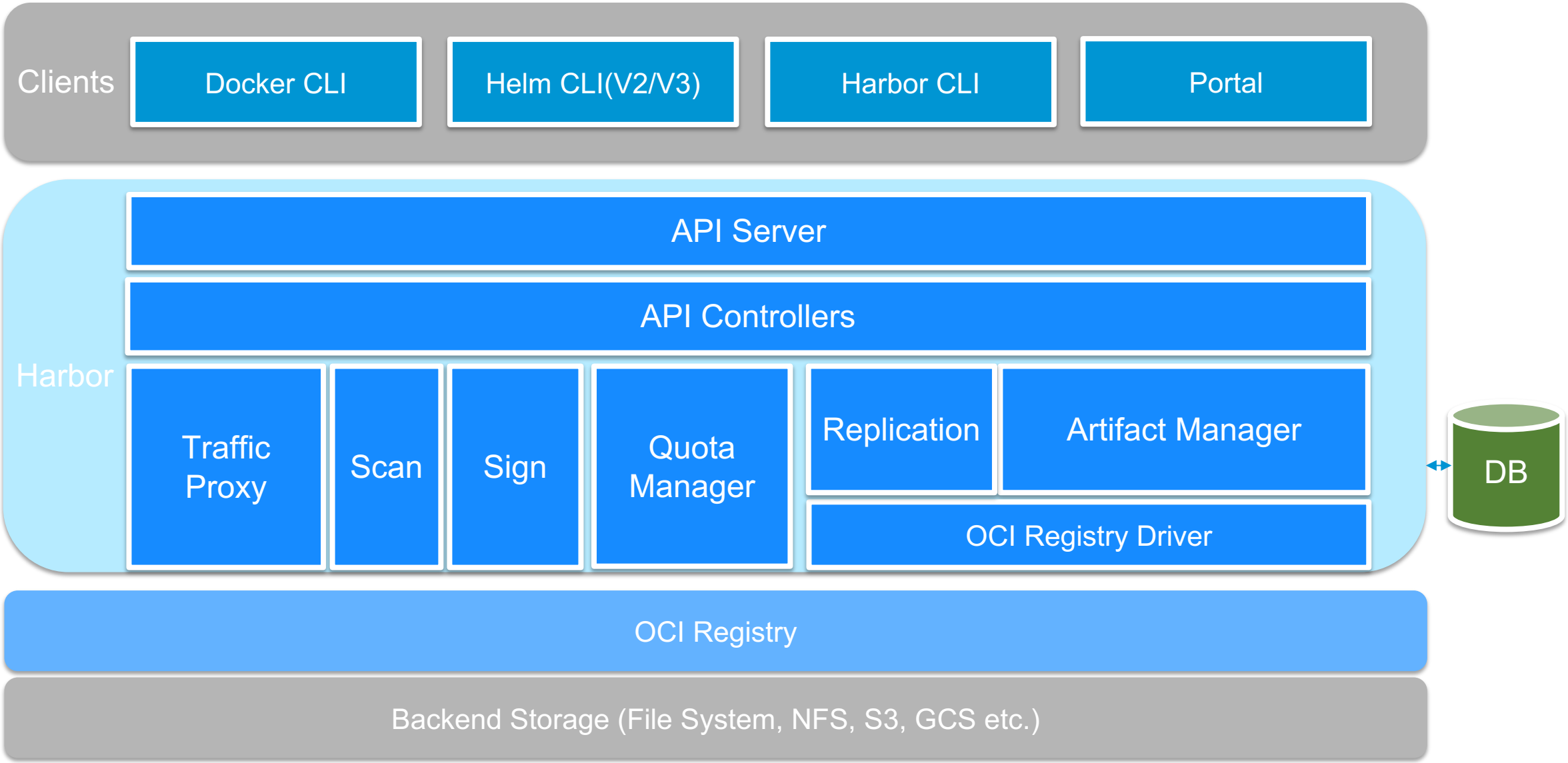
- Simpler deployment, configuration, scaling out
- Provide one set of V2 API to manage ALL artifacts

  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



Roadmap & Harbor Community

Michael Michael / 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

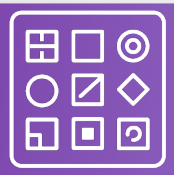
Image Distribution

P2P Distribution

Proxy Cache

3

Extensibility



Cloud Native Artifact Management

Webhook++

Interrogation Service++

The Community is Thriving

GitHub Stars	Contributors
9800+	200+

14 Maintainers across 6 organizations

HARBOR

20+ Product Implementations

vmware caicloud 才云 时速云 RANCHER BingoCloud 品高云 CloudChef ise2c Pivotal

115+ Contributing Organizations

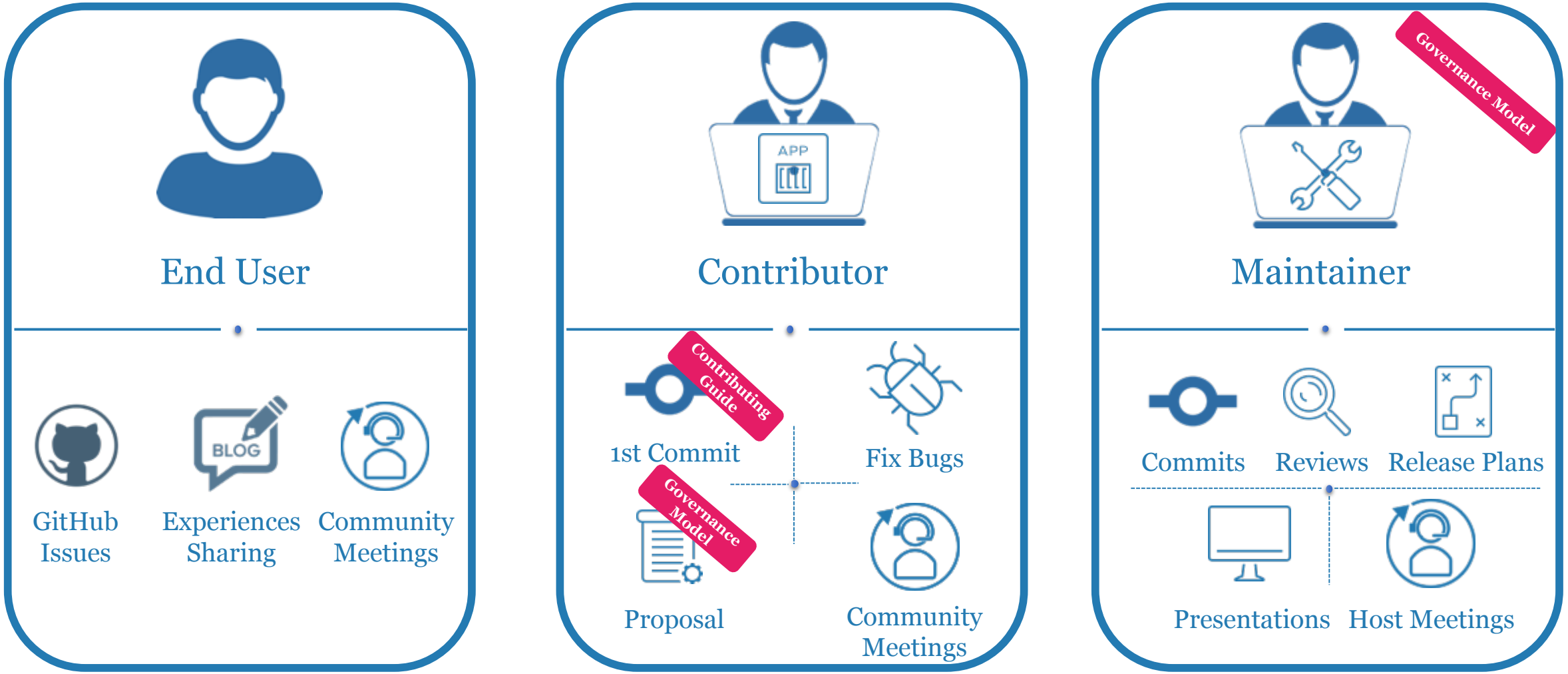
Hyland creator of OnBase DigitalOcean anchore aqua sina 新浪 adorsys GM TVM 天脉

300+ Community Members

NCB NATIONAL COMMERCIAL BANK JAMAICA LIMITED SLAMTEC TREND MICRO 中国移动 China Mobile 360 www.360.cn 腾讯云 京东

Harbor Community

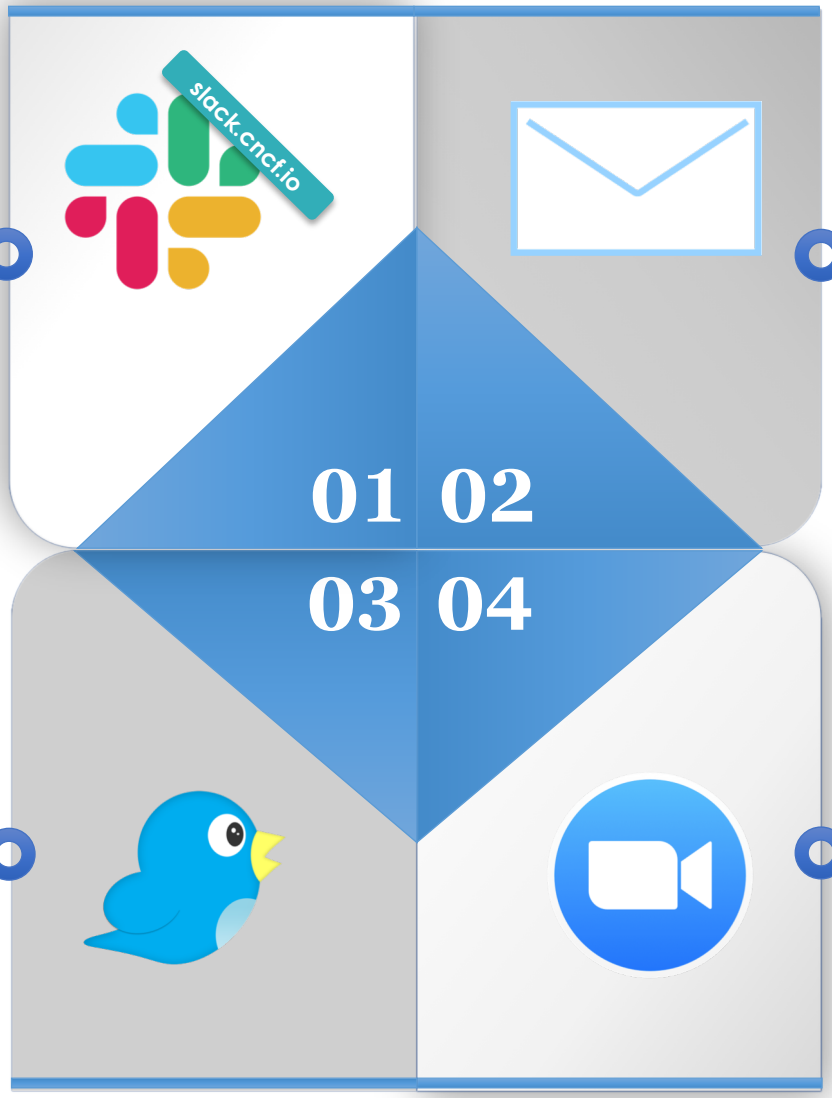
Levels of Participation



Collaborate with the Harbor Team

GoHarbor.io

#harbor
#harbor-dev



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

github.com/goharbor/community/blob/master/MEETING_SCHEDULE.md

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

@project_harbor

Demo ENV

demo.goharbor.io
Sign up for an account

CLOUD NATIVE COMPUTING FOUNDATION