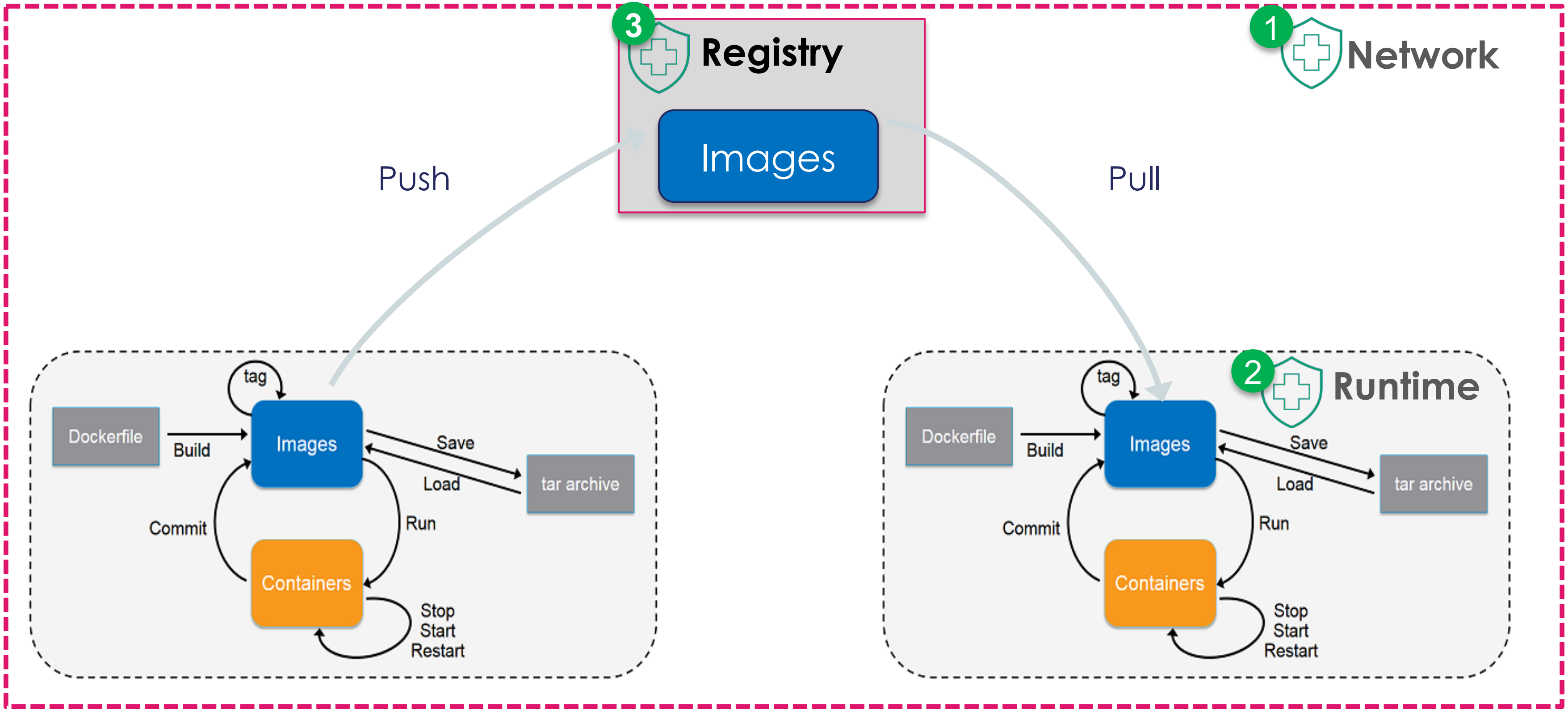
Gain Confidence in Compliance

Advanced Image Scanning with Harbor

Steven Zou@steven-zou / szou@vmware.com
Harbor Core Maintainer / Staff Engineer, VMware

CLOUD NATIVE
COMPUTING FOUNDATION

Registry - Compliance



Open source container image registry that secures images with role-based access control, scans images for vulnerabilities, and signs images as trusted

- Security & Compliance
- Performance
- Interoperability
- Consistent image management for Kubernetes

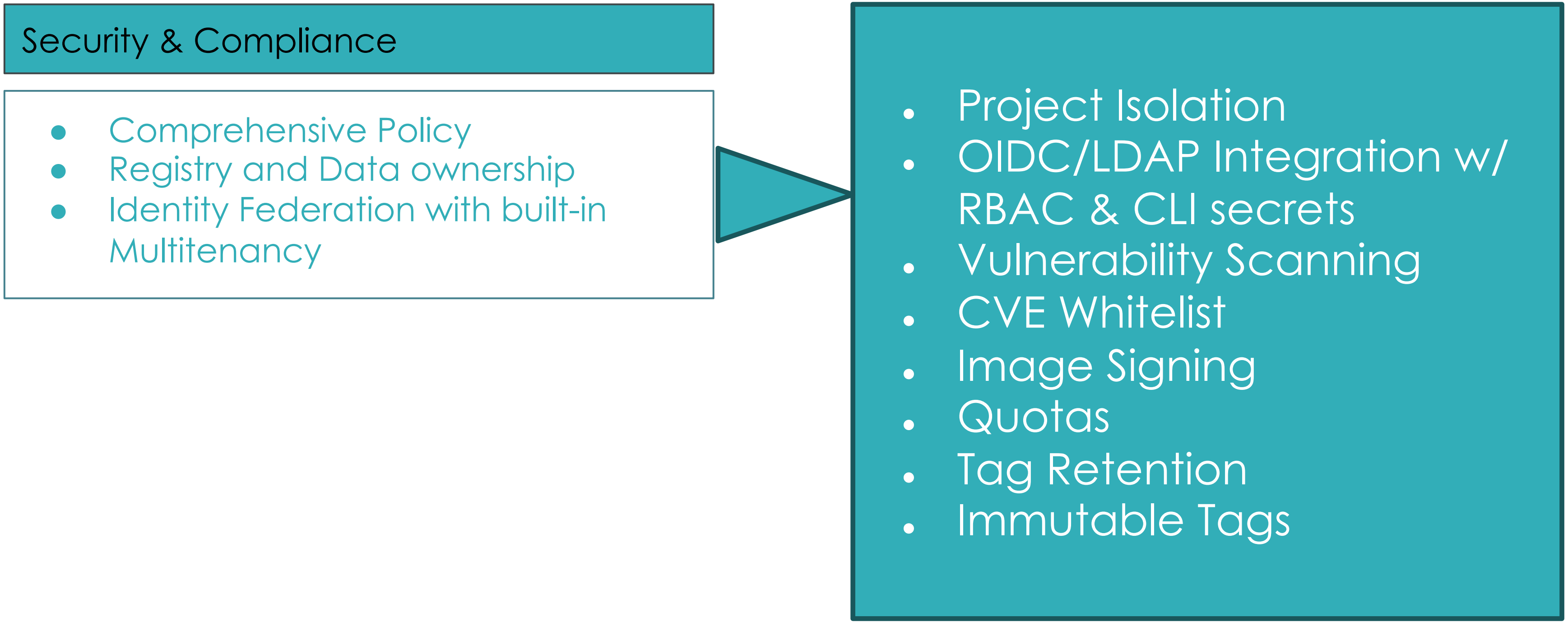
A Cloud Native Computing Foundation Incubating project

goharbor.io

10000+ Stars

CLOUD NATIVE
COMPUTING FOUNDATION

Why run your own registry?



Security & Compliance

- Comprehensive Policy
- Registry and Data ownership
- Identity Federation with built-in Multitenancy

- Project Isolation
- OIDC/LDAP Integration w/ RBAC & CLI secrets
- Vulnerability Scanning
- CVE Whitelist
- Image Signing
- Quotas
- Tag Retention
- Immutable Tags

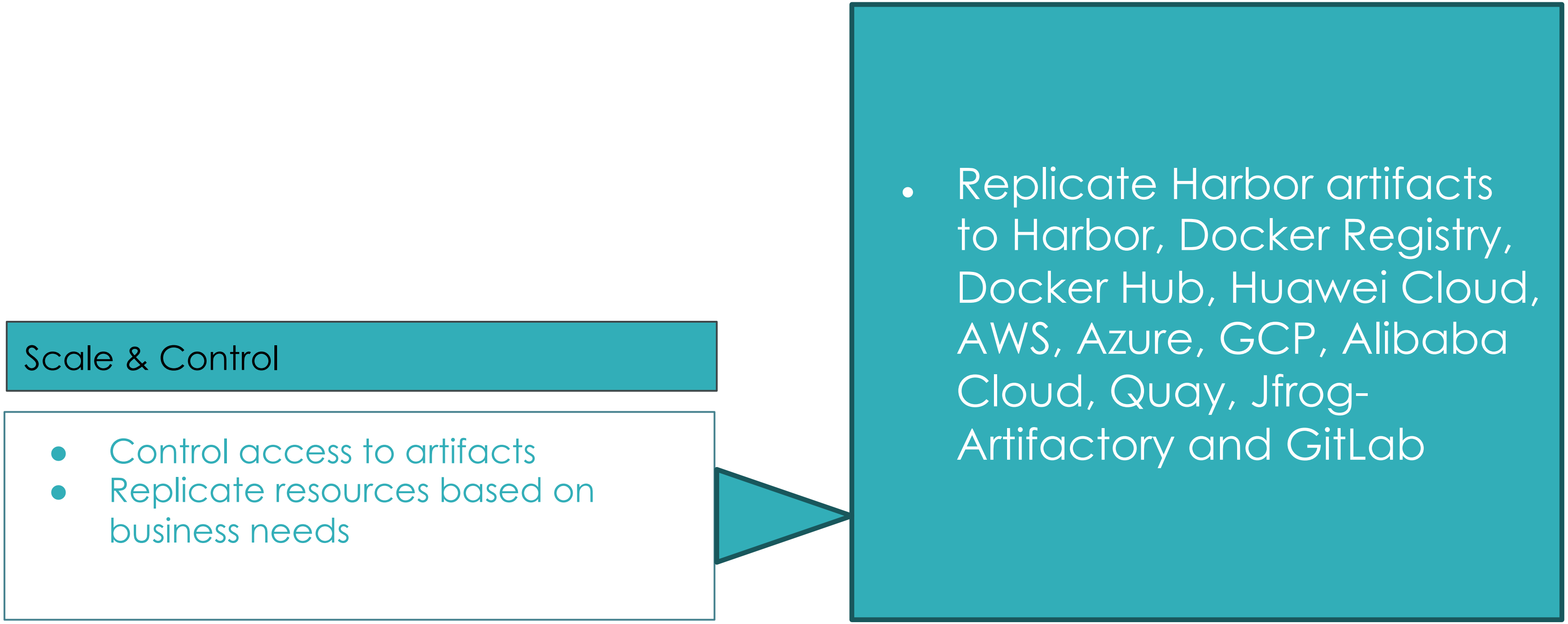
Why run your own registry?

- Online/Offline installer (docker-compose)
- Harbor Helm Chart (K8s)
- Harbor Tile (CF, Products)

Infrastructure

- Deploy on any infrastructure (private, public, hosted, edge)
- Data locality
- Kubernetes and Docker compliant

Why run your own registry?



Scale & Control

- Control access to artifacts
- Replicate resources based on business needs

- Replicate Harbor artifacts to Harbor, Docker Registry, Docker Hub, Huawei Cloud, AWS, Azure, GCP, Alibaba Cloud, Quay, Jfrog-Artifactory and GitLab

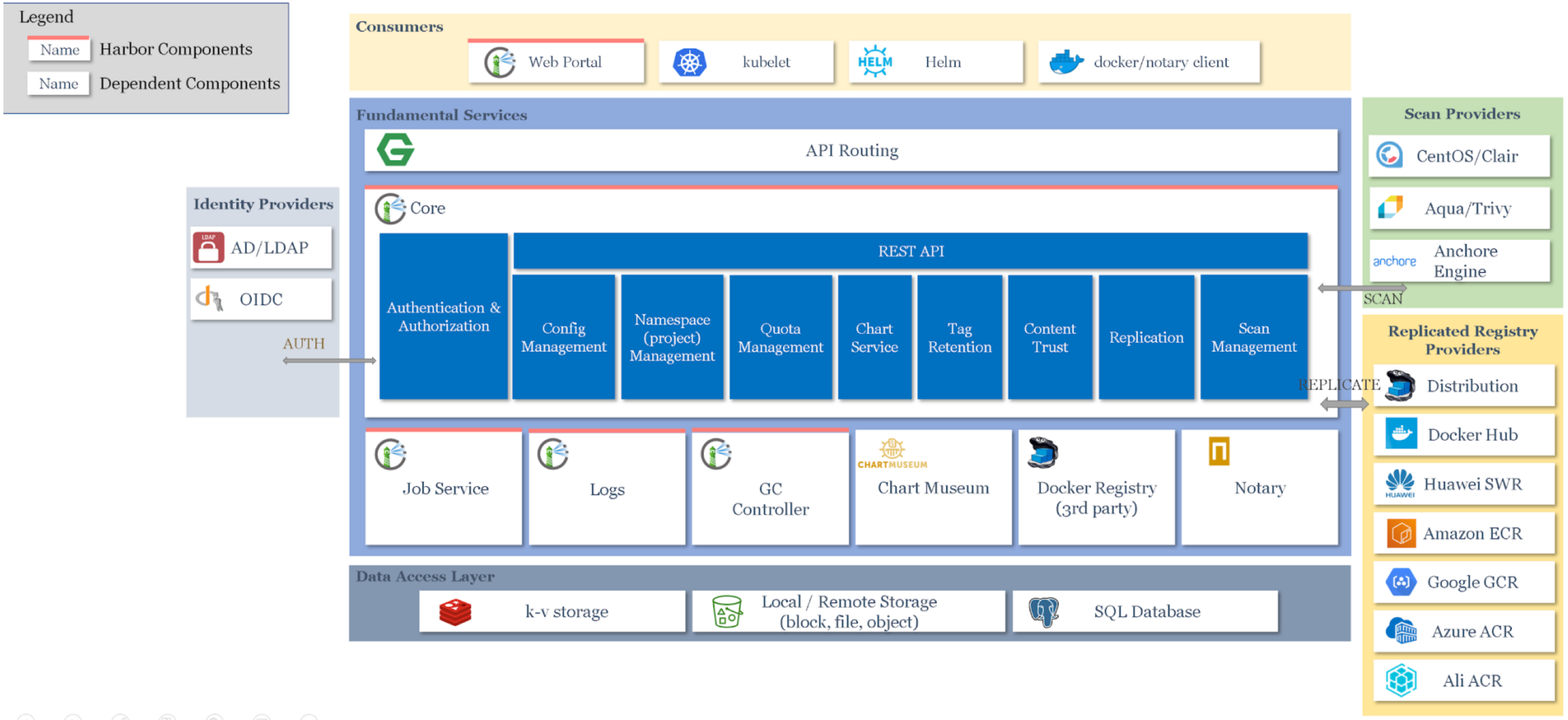
Why run your own registry?

- Syslog integration
- Webhooks
- REST API
- Robot Accounts

Automation & Extensibility

- Plug-n-Play with existing investments in infrastructure and services

Architecture

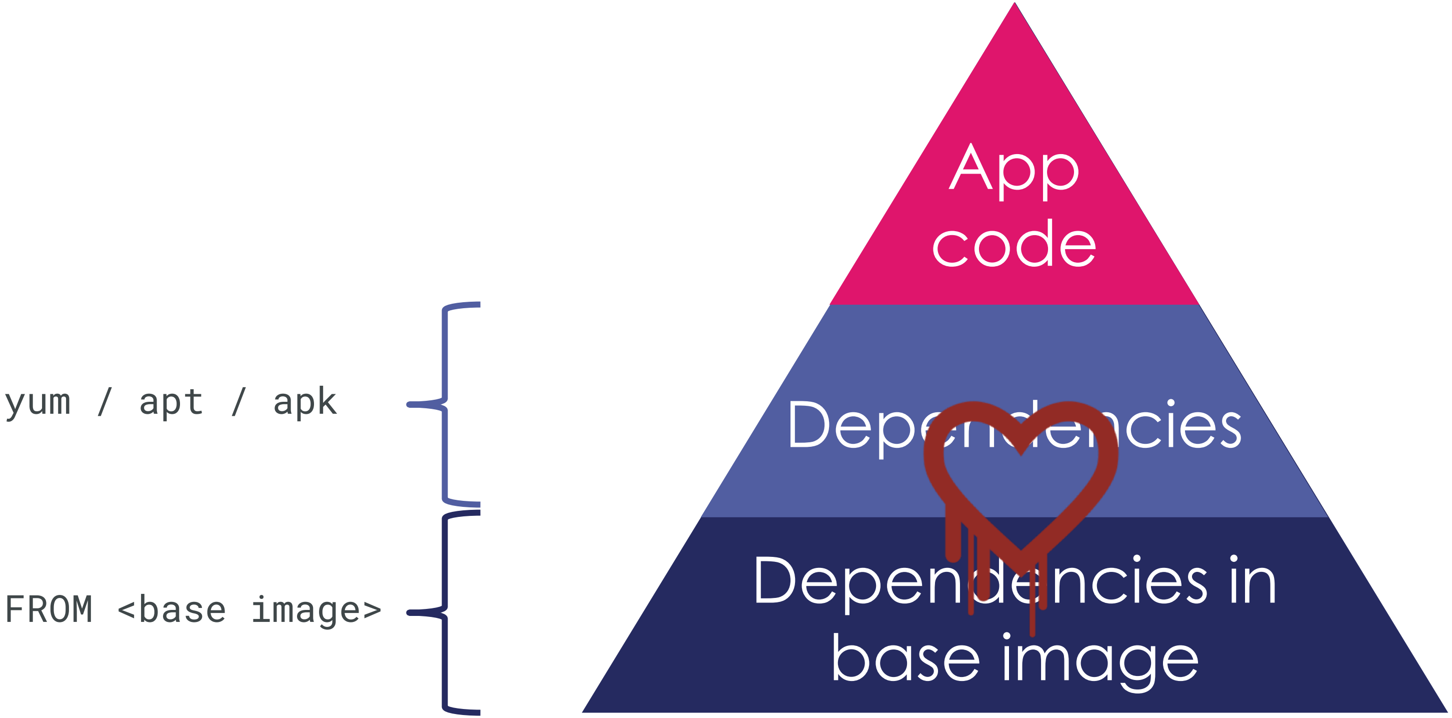


Harbor 1.10 (GA in this week)

Security & Compliance Theme

1. Immutable Images and Repositories
2. OIDC Group Support
3. Limited Guest Role
4. CLI Secret and Robot account enhancements
5. **Interrogation Service**
    a. Pluggable out-of-tree scanners

Container image vulnerability scanning



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

NVD

debian · ubuntu · alpine Linux · CentOS · redhat LINUX

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

Options

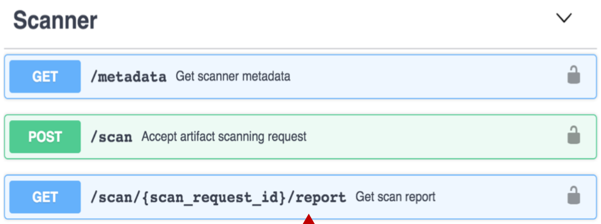
- Open Source
- Free
- Commercial

- 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

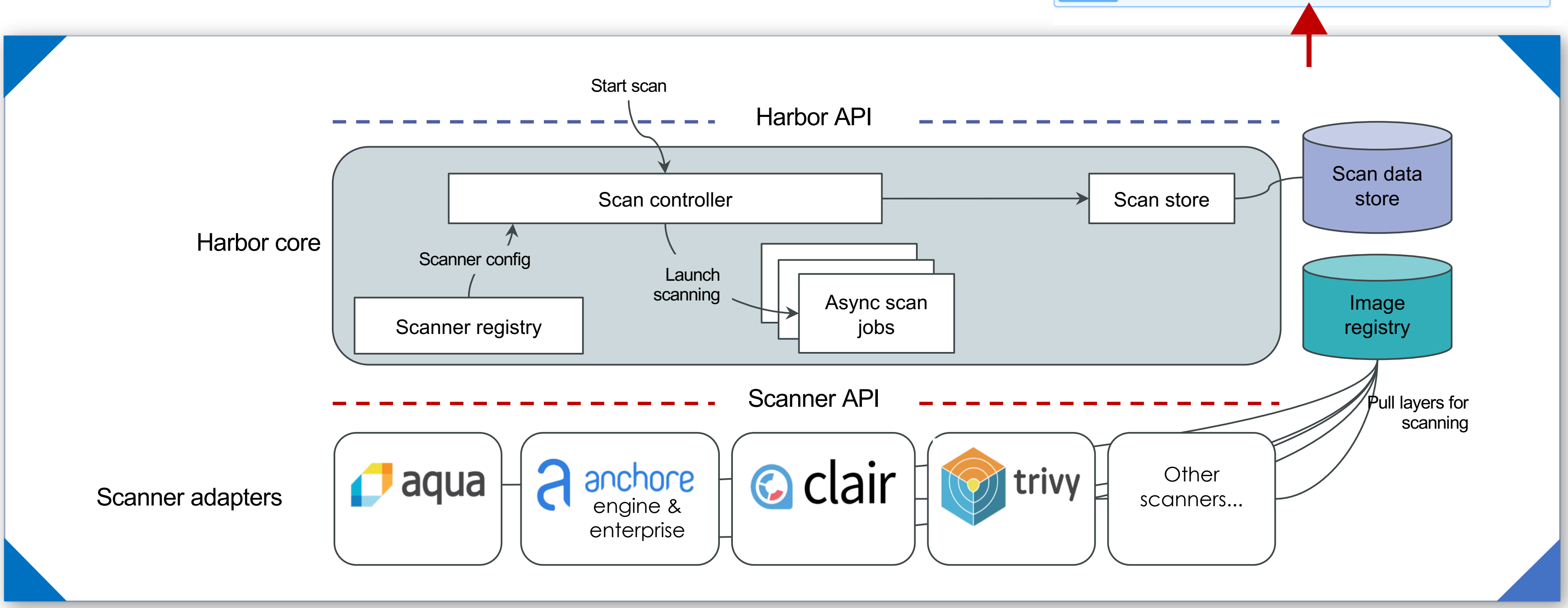


Scanner

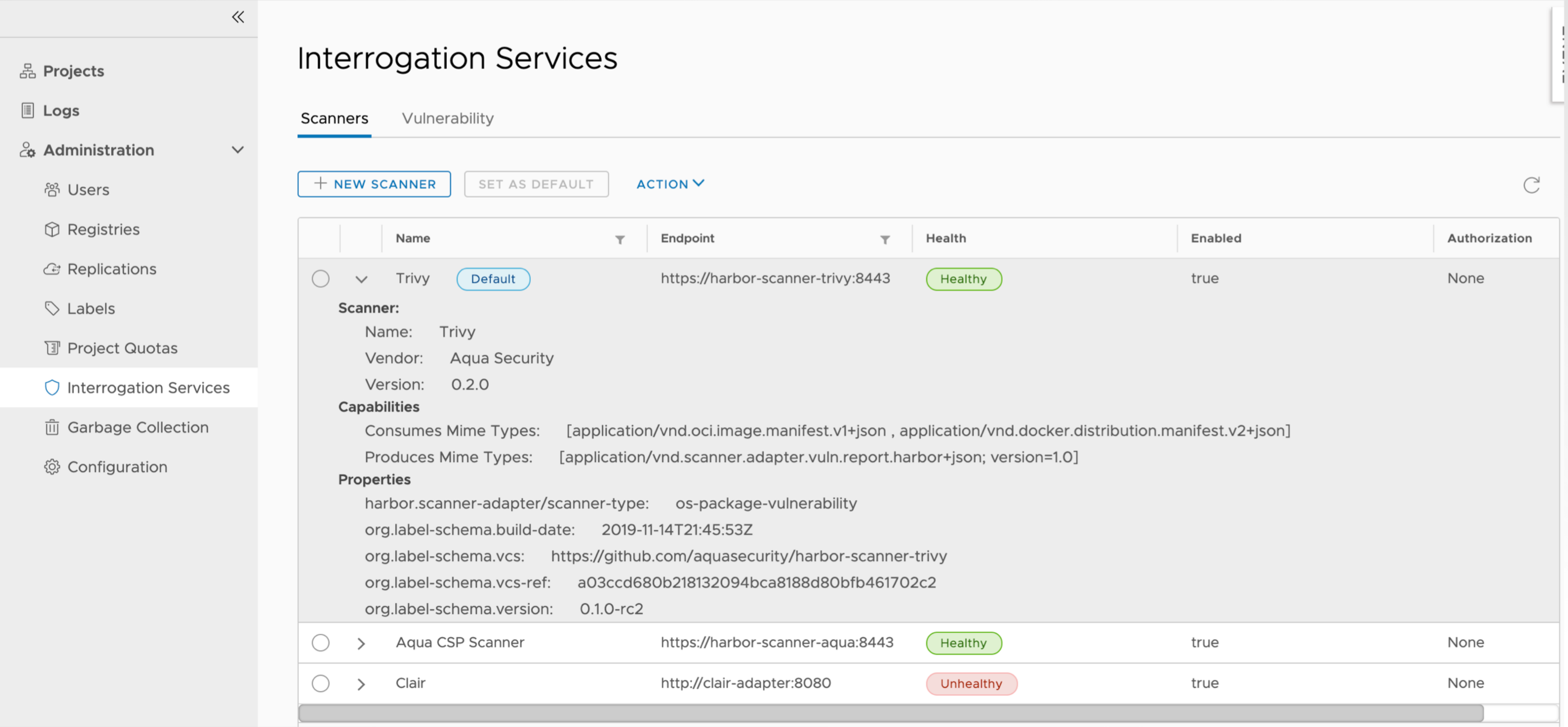
GET /metadata Get scanner metadata

POST /scan Accept artifact scanning request

GET /scan/{scan_request_id}/report Get scan report



Scanner Registry



Interrogation Services

	Name	Endpoint	Health	Enabled	Authorization
○	Trivy Default	https://harbor-scanner-trivy:8443	Healthy	true	None

Scanner:

Name: Trivy

Vendor: Aqua Security

Version: 0.2.0

Capabilities

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]

Properties

harbor.scanner-adapter/scanner-type: os-package-vulnerability

org.label-schema.build-date: 2019-11-14T21:45:53Z

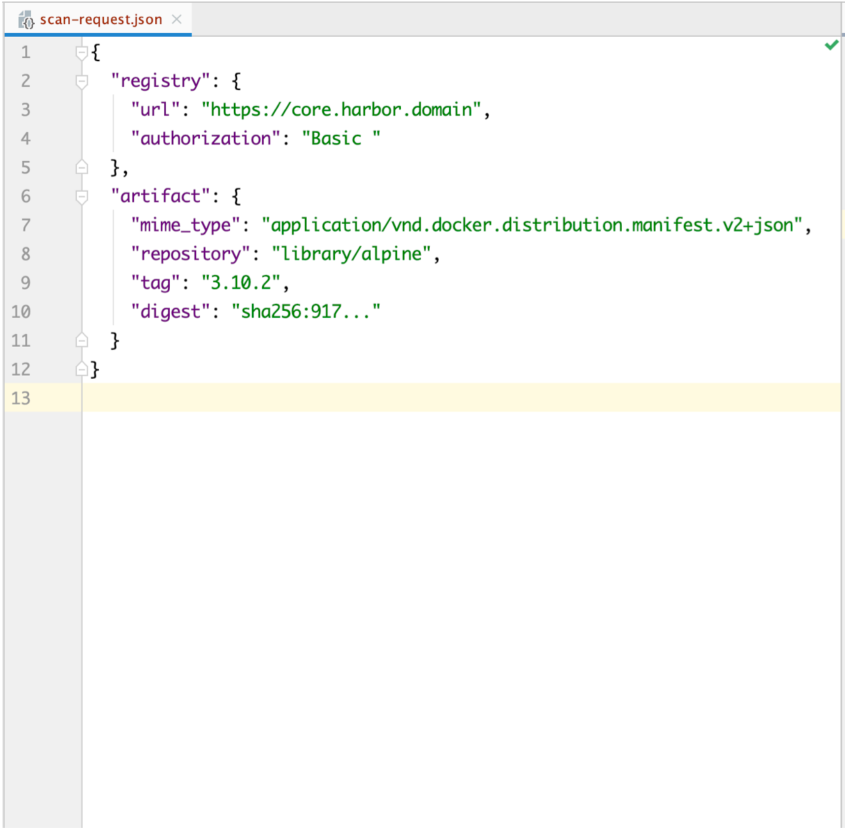
org.label-schema.vcs: https://github.com/aquasecurity/harbor-scanner-trivy

org.label-schema.vcs-ref: a03ccd680b218132094bca8188d80bfb461702c2

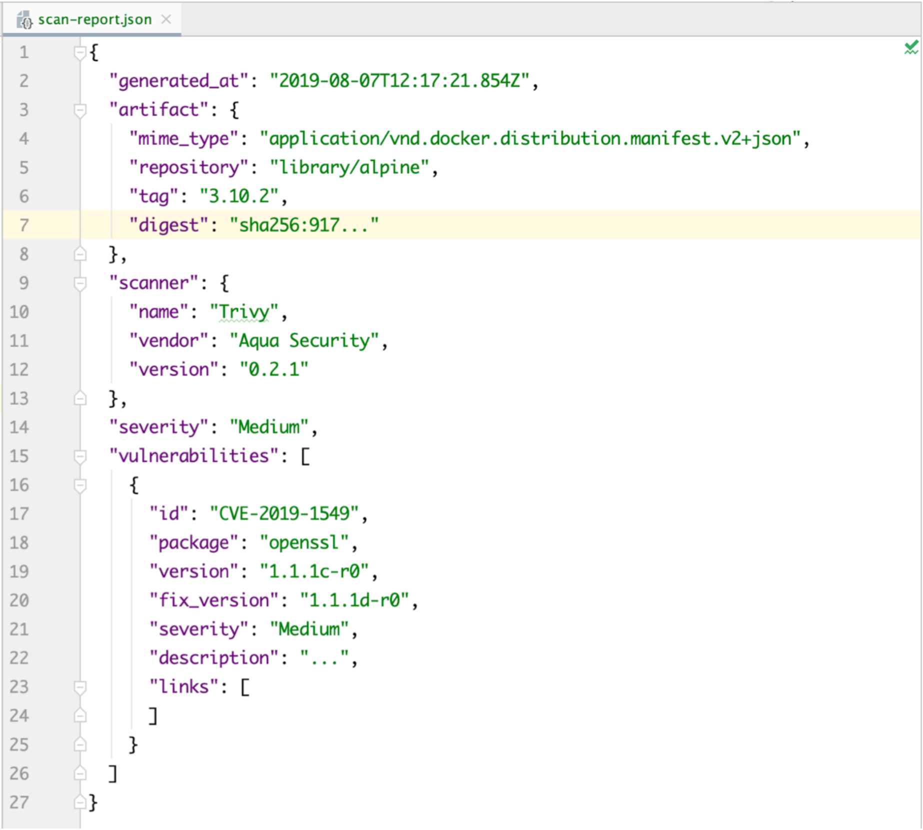
org.label-schema.version: 0.1.0-rc2

	Name	Endpoint	Health	Enabled	Authorization
○	Aqua CSP Scanner	https://harbor-scanner-aqua:8443	Healthy	true	None
○	Clair	http://clair-adapter:8080	Unhealthy	true	None

Scan Reports



```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..."
  }
}
```



```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": [
      ]
    }
  ]
}
```

Supported Scanners

aqua

CSP

trivy

Trivy

anchore

anchore engine & enterprise

clair

Clair

DoSec

https://github.com/goharbor/pluggable-scanner-spec

Delivered by the Scanning Workgroup

Joint work across multiple organizations in Harbor community

aqua

Daniel Pacak
Liz Rice

vmware

Steven Zou
Weiwei He
Daniel Jiang
Alex Xu

anchore

Zach Hill

hp

Ye Liu
Maggie Ma

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

Demo!

Roadmap

1

Management

- Perf & Scale
- K8s Operator
- Signing Policy Replication
- Metadata Management
- Observability

2

Image Distribution

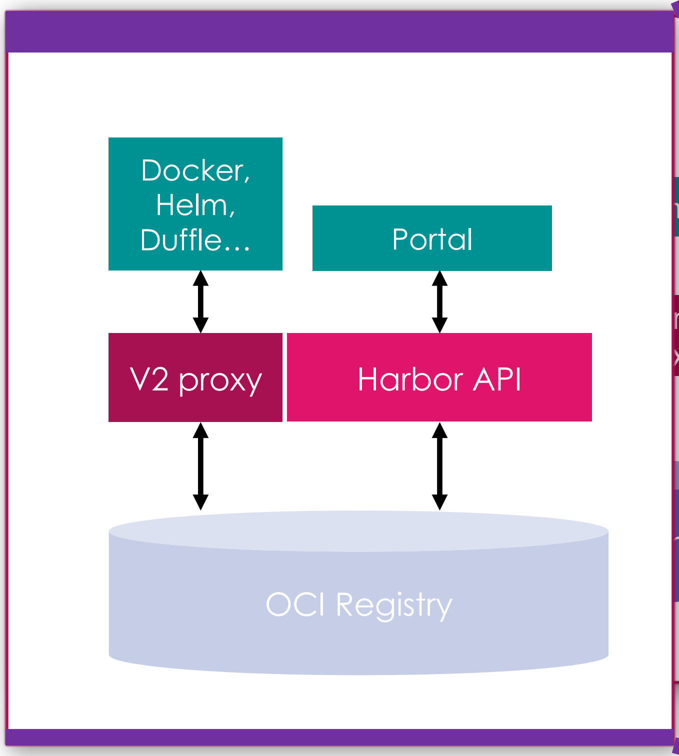
- P2P Distribution
- Proxy Cache

3

Extensibility

- Cloud Native Artifact Management
- Webhook++
- Interrogation Service++

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

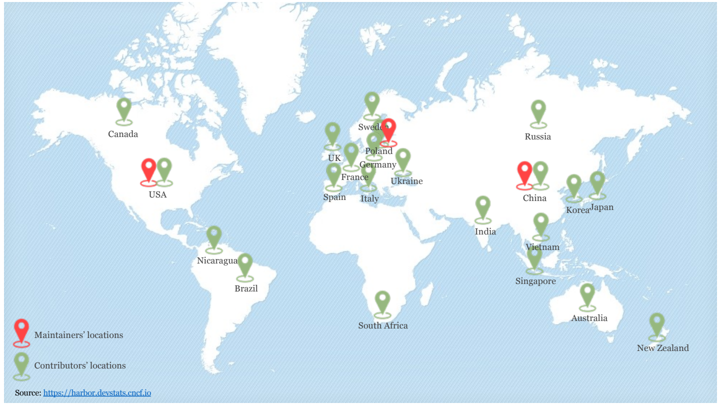
-> GET /api/v2/projects/{p-id}/repositories/{r-id}/artifacts

- Support for index (manifest list)
- Aggregated view for all artifacts under a project/repository
- Consistent management features for all artifact

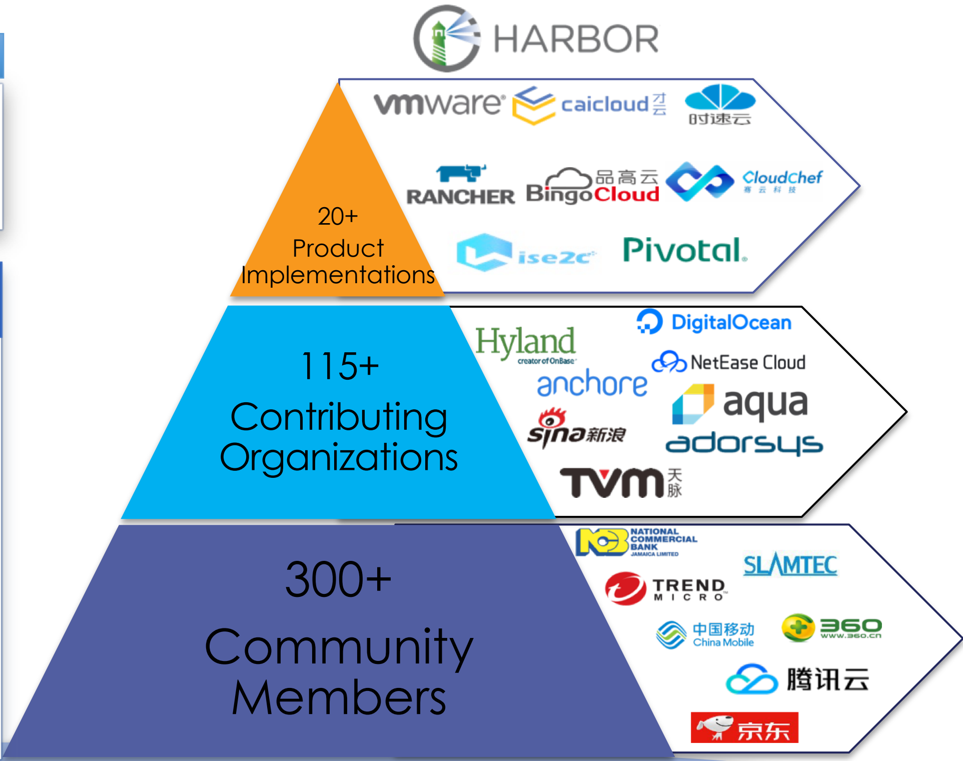
The Community is Thriving

GitHub Stars	Contributors
10000+	200+

14 Maintainers across 6 organizations



Source: https://harbor.devstats.cncf.io



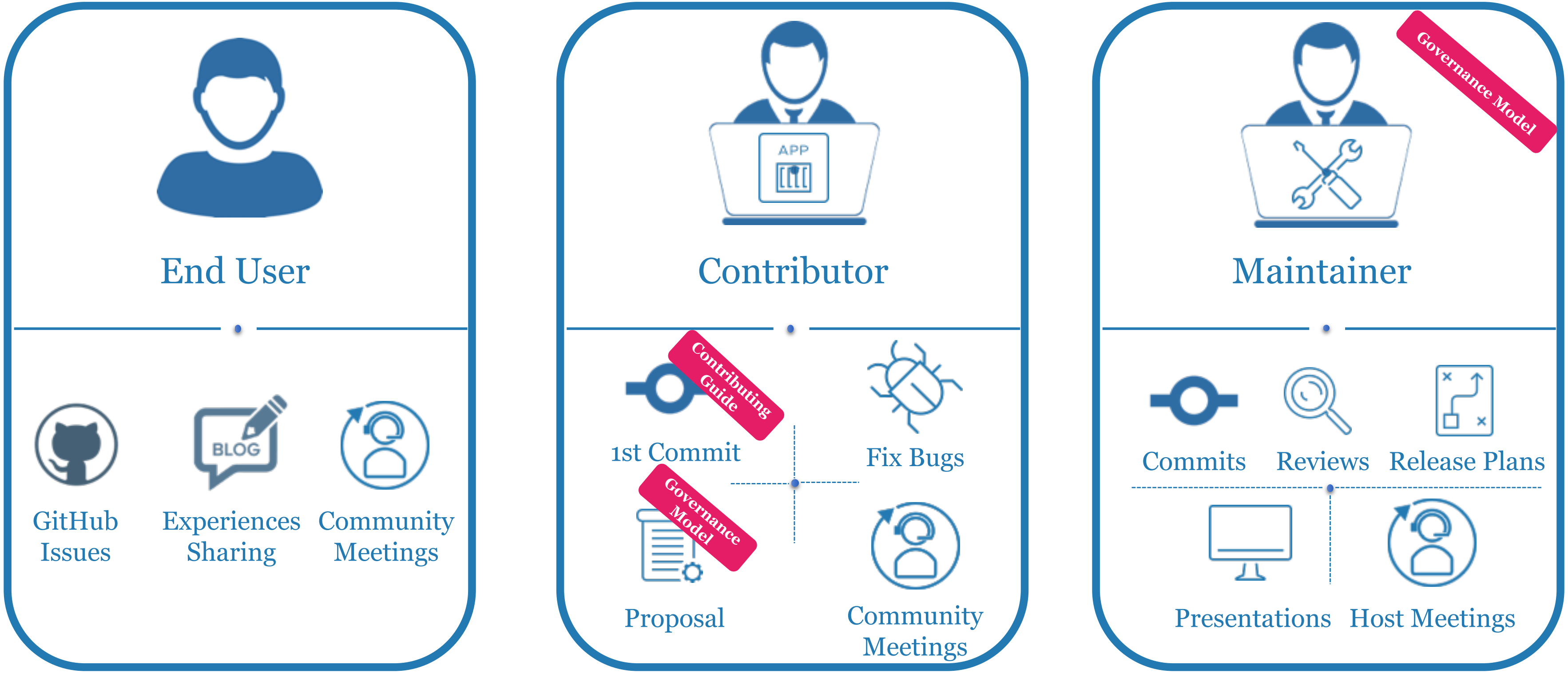
20+ Product Implementations

115+ Contributing Organizations

300+ Community Members

Harbor Community

Levels of Participation



End User

GitHub Issues

Experiences Sharing

Community Meetings

Contributor

Contributing Guide

1st Commit

Fix Bugs

Governance Model

Proposal

Community Meetings

Maintainer

Governance Model

Commits

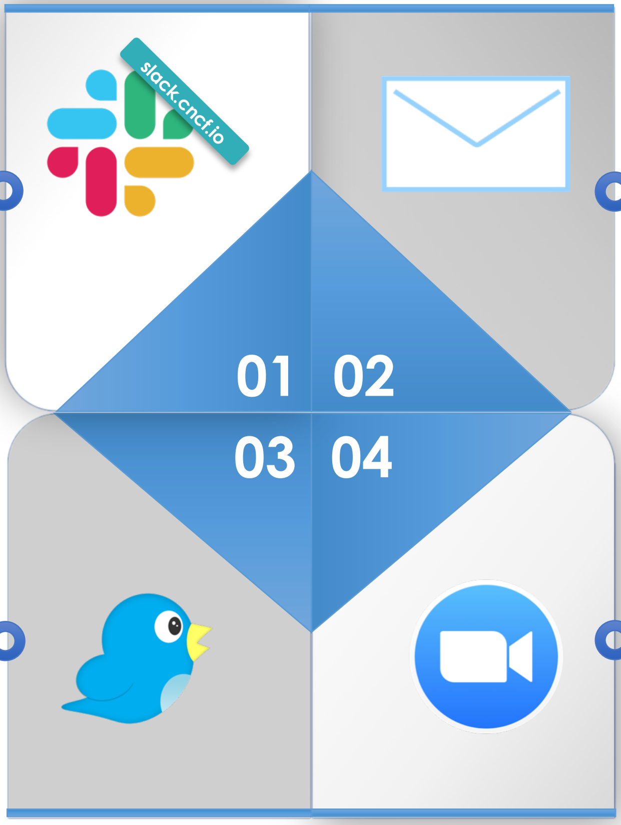
Reviews

Release Plans

Presentations

Host Meetings

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

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

Demo ENV

demo.goharbor.io
Sign up for an account

CLOUD NATIVE
COMPUTING FOUNDATION