



KubeCon



CloudNativeCon

Europe 2020

Virtual

Deep Dive: Harbor - Enterprise Cloud Native Artifact Registry

Steven Zou, Harbor Maintainer / szou@vmware.com

Daniel Jiang, Harbor Maintainer / jiangd@vmware.com

Agenda

- Harbor community updates
- Key deliverables in the latest V2.0
- Features in the next coming release V2.1
 - None-blocking GC
 - Proxy Cache
 - P2P preheat
 - Extended processor for user-defined OCI artifacts
- Our roadmap

Harbor Graduated!



Virtual

CONGRATS

CLASS OF 2020

Love, CNCF



HARBOR

Harbor Community is Thriving



GitHub Stars

12.3K+

Committers

200+

Contributing Companies

50+

Contributors

3000+

Forks

4000+

Commits

12K+

GitHub Views/Visitors

60K+/11K+

Downloads

5K+

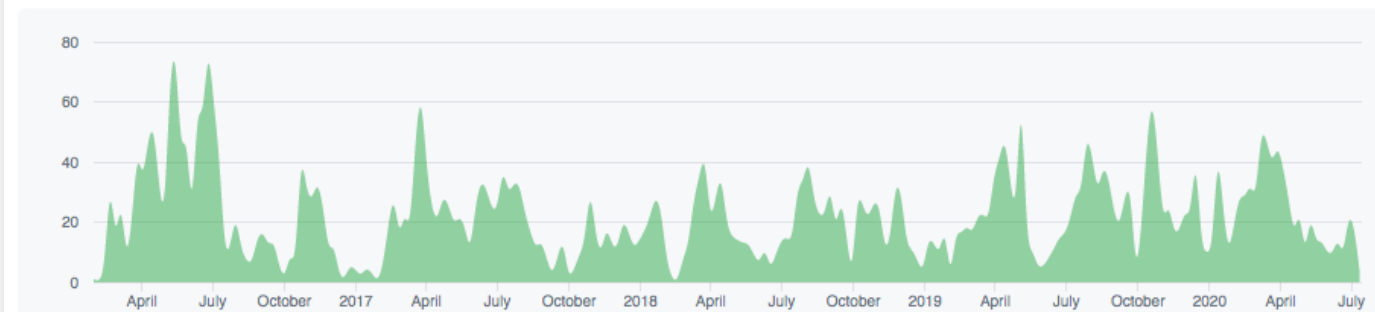
14 Maintainers across 5 companies



Jan 31, 2016 – Jul 15, 2020

Contributions: Commits ▾

Contributions to master, excluding merge commits



Harbor Community

V2.0: Key deliverables

Registry for cloud native artifact:

- Leverage distribution's /v2 API to manage artifacts other than container images (helm charts, OPA bundles, CNAB)
- Aggregated view for different artifacts under a project/repository.
- Consistent management workflow.
- Refined process for managing artifacts' metadata.
- Filled in the gap for manifest list support.

Enhancements:

- Trivy is the default scanner
- Enable TLS communication across internal components.
- Individual expiration for robot accounts

The image shows an architecture diagram of the registry system and a screenshot of the 'hello-world' artifact page. The architecture diagram is divided into several layers:

- Consumers:** Includes Web Portal, kubelet, Helm, docker/notary client, and Oras (OCI compatible clients).
- Fundamental Services:** Includes Proxy (API Routing).
- Core:** Includes Authentication & Authorizations, API Server, Middleware, and API Handlers.
- Configuration:** Includes Configuration Manager, Namespace (project) Manager, Quota Manager, and Chart Control (V2 Ch).
- Controllers:** Includes GC Controller and Chart Museum (3rd party).
- Data Access Layer:** Includes k-v storage.

The screenshot shows the 'hello-world' artifact page with the following table:

Artifacts	Pull Command	Tags	Size
<input type="checkbox"/> sha256:529d87f3		opa-v1	2.69KB
<input type="checkbox"/> sha256:44a99eee		cnab-v1.0	17.21MB
<input type="checkbox"/> sha256:adaf6410		cnab-v1.0-invoc	15.74MB
<input type="checkbox"/> sha256:b699a284		chart-v1	75.29KB

V2.1: New Garbage collector



KubeCon



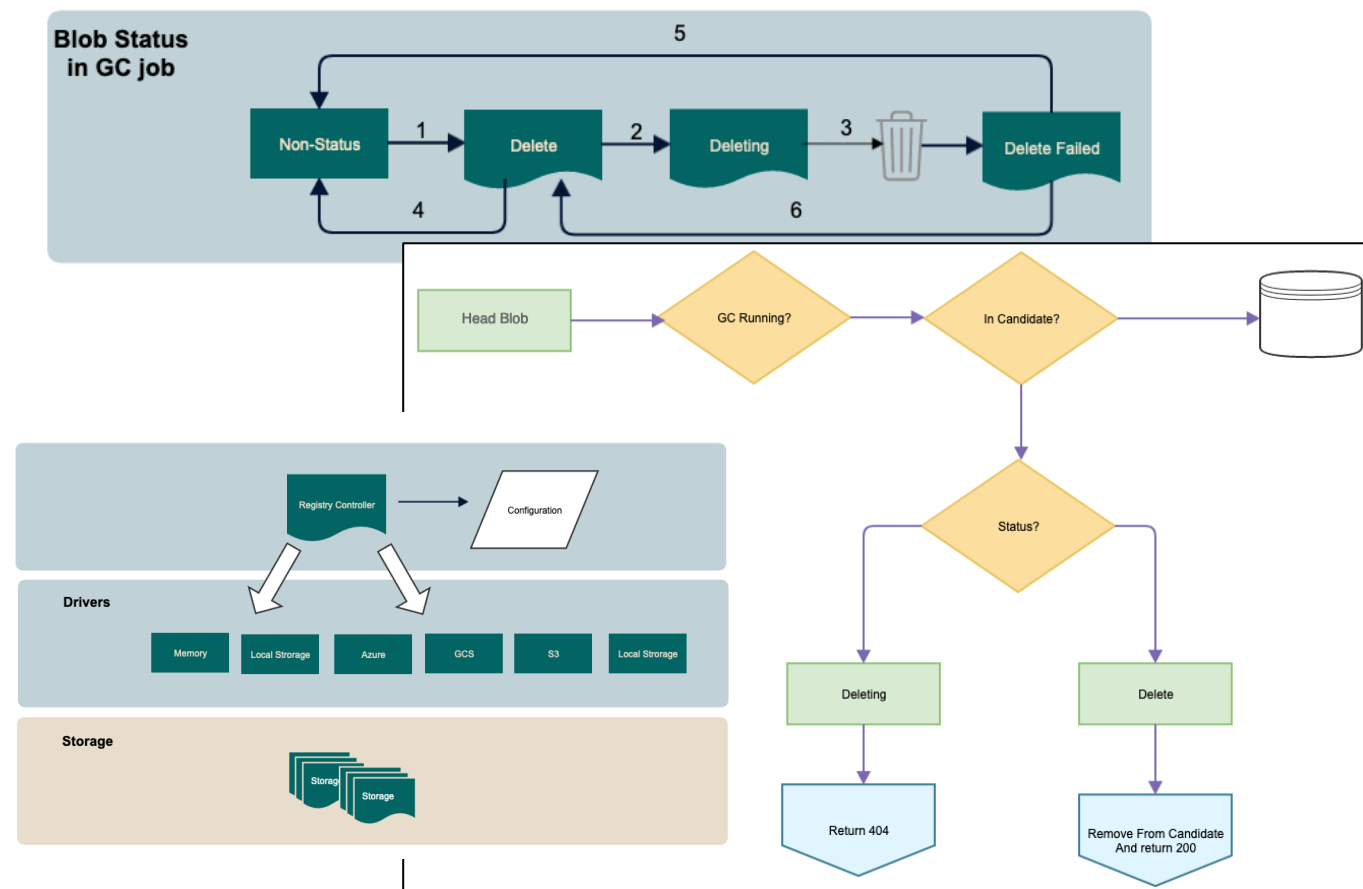
CloudNativeCon

Europe 2020

Virtual

“Non-blocking” Garbage Collector:

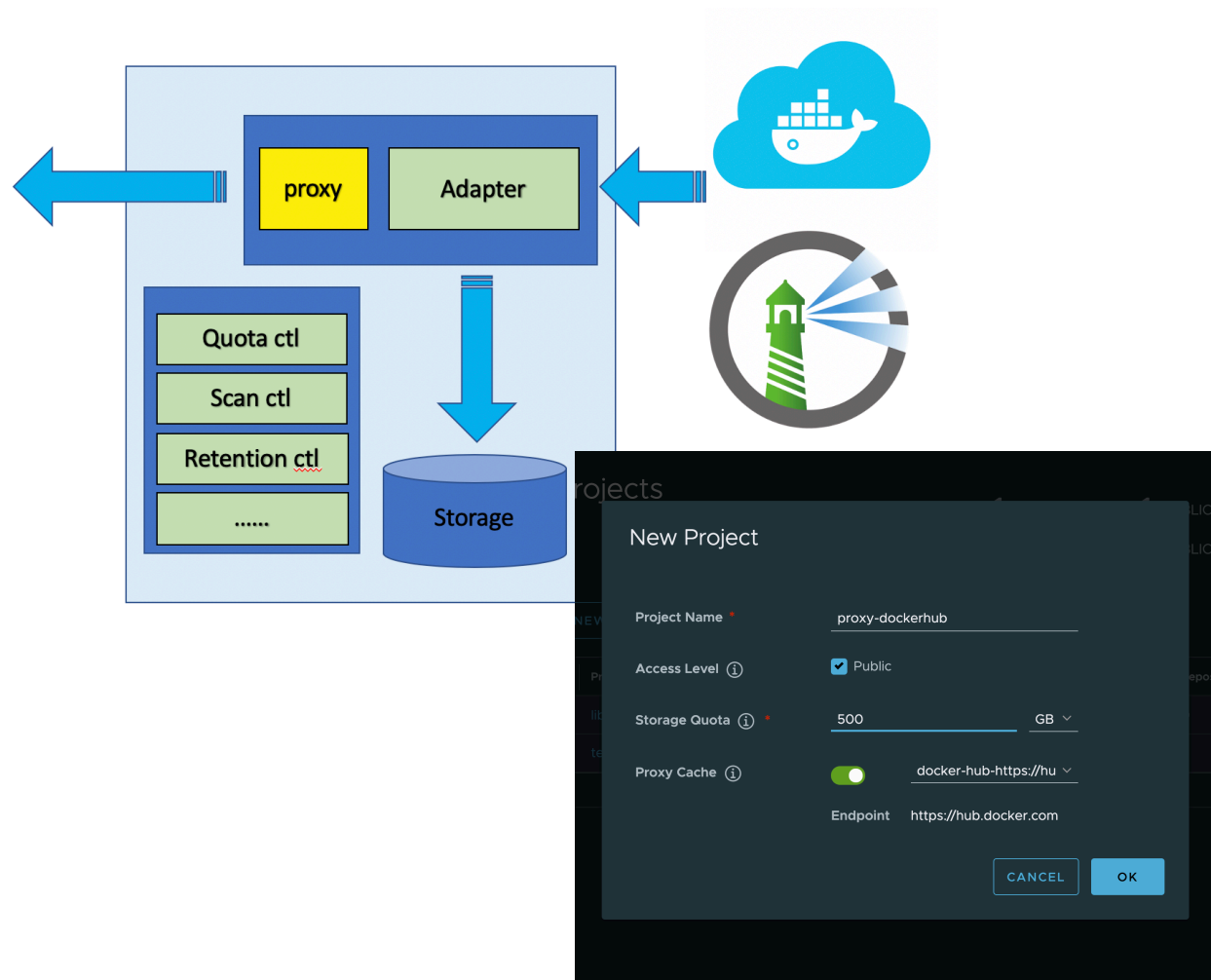
- GC without putting the whole registry to “read-only”.
- GC handler to access storage directly.
- Remove the dependency on distribution binary for deleting blob data.
- “dry-run” a GC job to estimate the space to be released.
- Workflow to trigger and monitor a GC job remain the same in v2.1
- Merged into master branch



V2.1: Proxy cache project

Proxy cache:

- Provide the “proxy” capability at project level.
- Reuse the adapters created for replication, adding the “tee” capability.
- Proxied artifacts are considered “local”
- Management policies can be applied to proxied artifacts, incl. quota, scan ...
- Merged into master branch



V2.1: P2P Preheat

P2P Preheat:

- Define adapter interface to integrate with P2P engines
- Distribute the deploying content to the P2P network(heat the P2P network) in advance
- Policy-based thereby automated
 - Per repos/tags/labels/signatures/vulnerabilities

Engines:

- Dragonfly
- Kraken

Deliver by P2P workgroup

- contributors from VMware, Alauda, Tencent, NetEase, Alibaba and Uber

Create P2P Provider Policy ⓘ

Provider dragonfly harbor - http://47.254.73.172:8002 ▾

Policy name

Description

Filters

Repositories ** ▾
Enter multiple comma separated repos, repo* or **

Tags ** ▾
Enter multiple comma separated tags, tag* or **

Criteria

Only signed images

Preheat on push

No vulnerability severity of Low ▾ and above

Labels matching

Schedule Daily at 10:15 PM [EDIT](#)

[CANCEL](#) [CREATE](#)

V2.1: Extended Artifact Processor



OCI artifacts support:

- Harbor supports managing and distributing the artifacts that following the OCI spec from V2.0
- Extra metadata provided by Harbor via the data processors

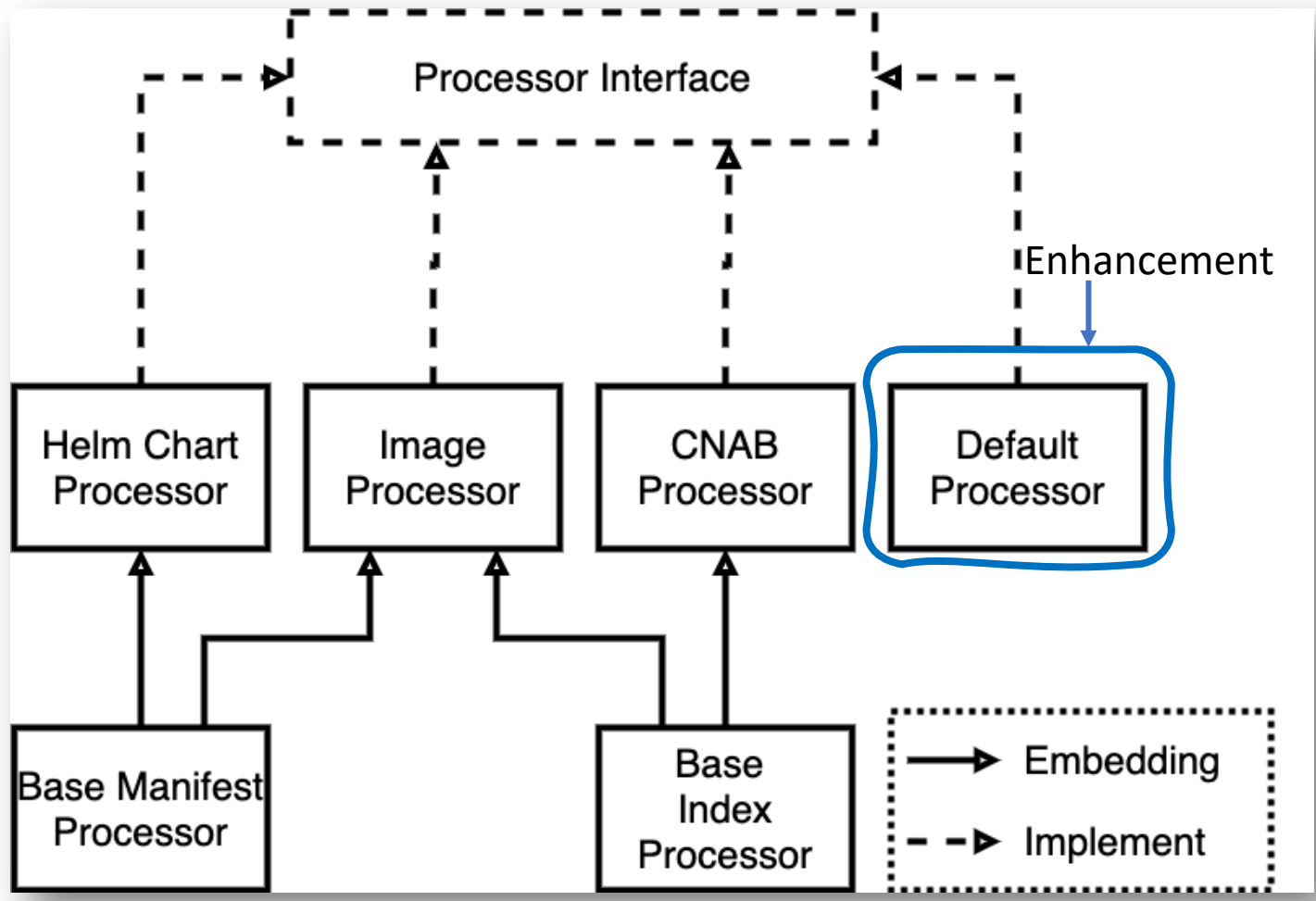
Shortages of current processors:

- Specified processors for the well-known standard artifact kinds (Chart, CNAB etc.)
- No extra metadata provided for the none-standard(user-defined) artifacts by the default processor

Extend the artifact processor:

- Define a simple metadata spec based on the OCI annotations
- Identify and extract the related metadata marked with annotations then returned by API

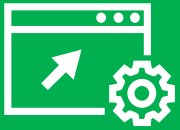
Deliver by CaiCloud team



Our Roadmap



1



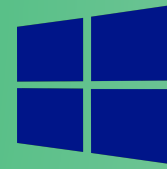
Management



Non-blocking GC



K8s
Operator



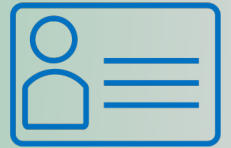
Windows Containers



Observability



Backup & Restore

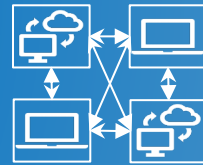


IAM&RBAC

2



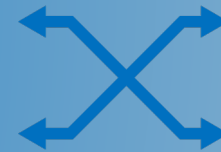
Image Distribution



P2P
Distribution



Proxy Cache

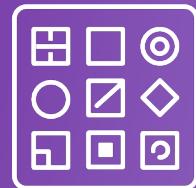


Networking(IPV6)

3



Extensibility



User-defined
Artifact



Interrogation
Service++(Sisdig)

Collaborations



KubeCon



CloudNative

Europe 2020

Demo ENV



demo.goharbor.io
Sign up for an account

#harbor
#harbor-dev



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

01 02
03 04

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

@project_harbor



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



KubeCon



CloudNativeCon

Europe 2020

Virtual

Q&A

Welcome any questions?

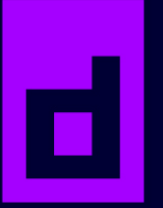
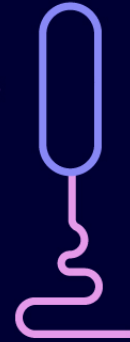
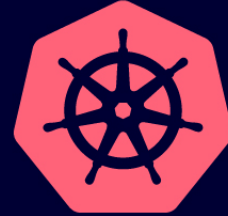


KubeCon



CloudNativeCon

Europe 2020



Virtual



KEEP CLOUD NATIVE

CONNECTED

