



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Harbor Maintainer Track

Yan Wang – Broadcom

Vadim Bauer – 8gears





KubeCon



CloudNativeCon

Europe 2026



Vadim Bauer

8gears Container
Registry



Yan Wang

Staff Engineer
Broadcom





KubeCon



CloudNativeCon

Europe 2026

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.





KubeCon



CloudNativeCon

Europe 2026

Harbor CLI



Harbor CLI



KubeCon



CloudNativeCon

Europe 2026

- Alternative
 - Web UI
 - REST API
- For Workflows in CI/CD
- For AI-agents
- If you haven't tried harbor-cli yet, check it out
- github.com/goharbor/harbor-cli

Demo Time



KubeCon



CloudNativeCon

Europe 2026

Harbor CLI

Thanks to

- People behind Harbor-CLI
- Every Maintainer of Harbor-CLI started as a mentee.
- Special thanks to Lakshit and Patrick, Prasanth



Patrick Eschenbach ✓ · 1.

Kubernetes and HPC DevOps Engineer @ Covestro | Ph.D. in Chemistry



Lakshit Singh ✓ · 2.

LFX'25 @ Harbor | Open Source Contributor | Instrumentalist
Neu-Delhi, Delhi, Indien ·



Prasanth Baskar ✓ · 1.

Open Source Developer | Core-Contributor @CNCF-Harbor |
MLOps | LFX Mentor
Madras, Tamil Nadu, Indien ·

Big Announcement



KubeCon



CloudNativeCon

Europe 2026

- Celebrating 130k+ downloads
- Harbor CLI is **now** out of Sandbox.



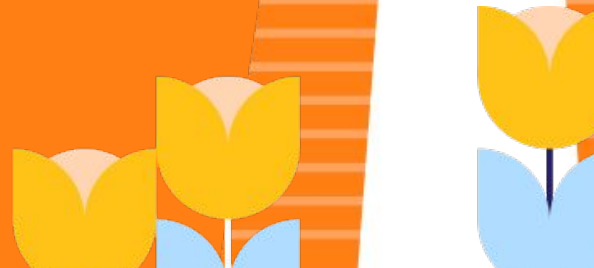
KubeCon



CloudNativeCon

Europe 2026

Harbor Satellite



Harbor Satellite



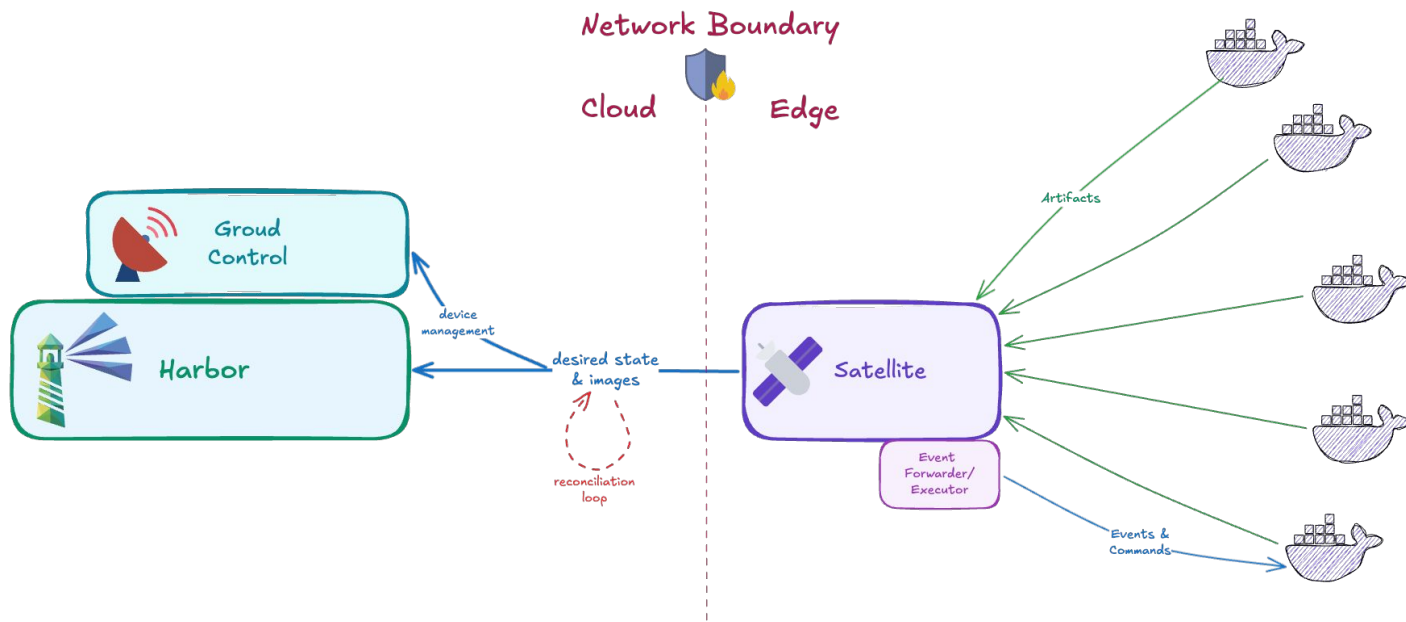
KubeCon



CloudNativeCon

Europe 2026

- Is a stateless, secretless, zero-trust edge registry with a very minimal footprint



What Is Harbor Satellite

- Extension of your container registry to every edge location with reliability, security, and central management.
- Local registry at each edge location
- **Fleet Management**
 - Centrally manage image distribution across hundreds of edge locations
- **Lightweight**
 - Single binary with minimal resource footprint
- satellite.container-registry.com

Recent Changes



KubeCon



CloudNativeCon

Europe 2026

- SPIFEE/SPIRE Integration
 - zero-trust identity with automatic credential rotation. No static secrets shipped to edge devices.
- Satellite can now act as a proxy
- satellite.container-registry.com

- Air-Gap Support
 - What does that even mean?
- Important for Satellite
 - Same process, tools, workflows
 - Fluidity for all types of air-gap definition



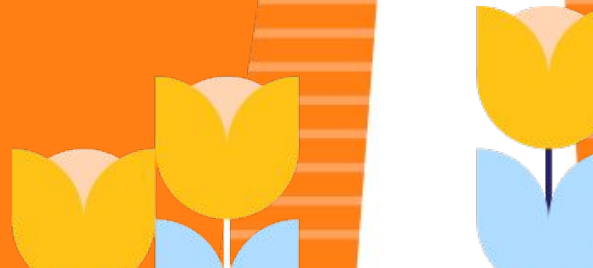
KubeCon



CloudNativeCon

Europe 2026

Harbor



Proxy Cache Enhancements



KubeCon



CloudNativeCon

Europe 2026

What's Shipped

- **Limit Upstream Connections**
 `max_upstream_conn` per project to control upstream pull concurrency
- **Resilient Caching**
 Serve cached images when upstream returns *Not Found*
- **Accurate Tag Retention**
 Correct `LastPullTime` for index/list and child artifacts
- **Updated Support List**
 Refined proxy adapter support

What's Next

- **Proxy Referrer API**
 Enable OCI referrers (SBOMs, signatures) via proxy cache
- **Limiting Proxy Cache Images**
 Cap cached images per project to control storage growth

Harbor GC Performance Enhancement



KubeCon



CloudNativeCon

Europe 2026

Rewrite tag pushes to digest for backend storage, so GC no longer spends time deleting tag-link files.

PUT /v2/<repo>/manifests/<tag>

Client

Harbor Core

Distribution

Storage

Before behavior

Persist tag in DB → Proxy request as-is to distribution

Objects landed in backend storage

Manifest + tag-link file

Extra tag cleanup remains in GC path

GC deletes blobs + manifest + tag link

Tag-link deletion calls Distribution API and is slow on S3/object storage.

After behavior

Persist tag in DB → Rewrite to digest push to distribution

Objects landed in backend storage

Manifest only

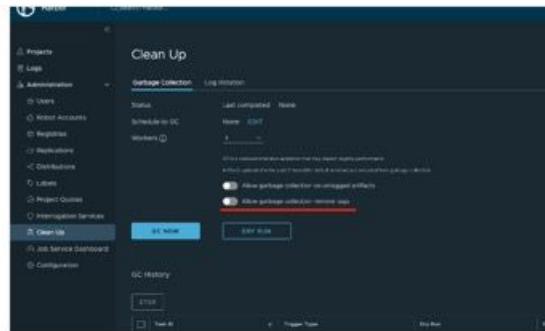
No new tag-link file lands in storage

GC deletes blobs + manifest only

Newly pushed artifacts skip tag deletion, shortening the slow path.

Why it matters

- Removes the tag-file deletion bottleneck that can take multiple seconds per tag in object storage.
- No API/UI break: Harbor still serves pull-by-tag by resolving tag → digest at the Harbor Core layer.
- Optional GC toggle preserves legacy cleanup behavior for older artifacts that already landed tag files.



root@yan-dev:~/harbor_source/put-mainfest/harbor/make# tree /data/registry/

```
/data/registry/  
├── docker  
│   └── registry  
│       └── v2  
│           ├── blobs  
│           │   ├── sha256  
│           │   │   ├── 74  
│           │   │   │   ├── 74cc54e27dc41bb10dc4b2226072d469509f2f22f1a3ce74f4a59661a1d44602  
│           │   │   │   └── data  
│           │   │   ├── 75  
│           │   │   │   ├── 7565f2c7034d87673c5ddc3b1b8e97f8da794c31d9aa73ed26afffa1c8194889  
│           │   │   │   └── data  
│           │   │   └── e6  
│           │   │       ├── e6590344b1a5dc518829d6ea1524fc12f8bcd14ee9a02aa6ad8360cce3a9a9e9  
│           │   │       └── data  
│           └── repositories  
│               └── library  
│                   └── hello-world  
│                       ├── _layers  
│                       │   ├── sha256  
│                       │   │   ├── 74cc54e27dc41bb10dc4b2226072d469509f2f22f1a3ce74f4a59661a1d44602  
│                       │   │   │   ├── link  
│                       │   │   │   └── e6590344b1a5dc518829d6ea1524fc12f8bcd14ee9a02aa6ad8360cce3a9a9e9  
│                       │   │   │       └── link  
│                       ├── _manifests  
│                       │   ├── revisions  
│                       │   │   ├── sha256  
│                       │   │   │   ├── 7565f2c7034d87673c5ddc3b1b8e97f8da794c31d9aa73ed26afffa1c8194889  
│                       │   │   │   └── link  
│                       │   └── tags  
│                       │       ├── latest  
│                       │       │   ├── current  
│                       │       │   │   ├── link  
│                       │       │   │   ├── index  
│                       │       │   │   │   ├── sha256  
│                       │       │   │   │   │   ├── 7565f2c7034d87673c5ddc3b1b8e97f8da794c31d9aa73ed26afffa1c8194889  
│                       │       │   │   │   │   └── link  
│                       └── _uploads
```

root@yan-dev:~/harbor_source/put-mainfest/harbor/make# tree /data/registry/

```
/data/registry/  
├── docker  
│   └── registry  
│       └── v2  
│           ├── blobs  
│           │   ├── sha256  
│           │   │   ├── 74  
│           │   │   │   ├── 74cc54e27dc41bb10dc4b2226072d469509f2f22f1a3ce74f4a59661a1d44602  
│           │   │   │   └── data  
│           │   │   ├── 75  
│           │   │   │   ├── 7565f2c7034d87673c5ddc3b1b8e97f8da794c31d9aa73ed26afffa1c8194889  
│           │   │   │   └── data  
│           │   │   └── e6  
│           │   │       ├── e6590344b1a5dc518829d6ea1524fc12f8bcd14ee9a02aa6ad8360cce3a9a9e9  
│           │   │       └── data  
│           └── repositories  
│               └── library  
│                   └── hello-world  
│                       ├── _layers  
│                       │   ├── sha256  
│                       │   │   ├── 74cc54e27dc41bb10dc4b2226072d469509f2f22f1a3ce74f4a59661a1d44602  
│                       │   │   │   ├── link  
│                       │   │   │   └── e6590344b1a5dc518829d6ea1524fc12f8bcd14ee9a02aa6ad8360cce3a9a9e9  
│                       │   │   │       └── link  
│                       ├── _manifests  
│                       │   └── revisions  
│                       │       ├── sha256  
│                       │       │   ├── 7565f2c7034d87673c5ddc3b1b8e97f8da794c31d9aa73ed26afffa1c8194889  
│                       │       │   └── link  
│                       └── _uploads
```

Model Distribution



KubeCon



CloudNativeCon

Europe 2026

AI models serve as the central artifacts across both training and inference. This part focuses on inference, addressing how to manage and distribute these models within Kubernetes.

Large Size: Model weights have grown from hundreds of megabytes to hundreds of gigabytes, even terabytes, posing significant challenges for model storage and transfer. Leverage Harbor's registry to efficiently manage and transfer large model weights, solving storage challenges.

Immutability: A base model used for inference is a read-only, versioned artifact. Like a container image, it follows a strict build once, distribute everywhere, never mutate in place.

Lack of Model Management Standards: The community is overly focused on distribution throughput while ignoring critical governance primitives, including standardized versioning, metadata schemas, and lifecycle management. These are exactly the prerequisites for promoting models from experimentation to production at scale.

Cloud-Native Gap: AI infrastructure is built on top of cloud-native infrastructure, yet companies widely rely on custom solutions around object storage or Git LFS for model management. This leads to non-standardized artifact management and a lack of cloud-native support.

<https://github.com/modelpack/model-spec>

Integration with ModelPack



KubeCon



CloudNativeCon

Europe 2026

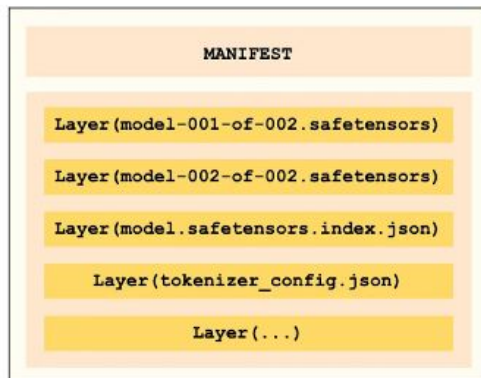
Build

Model Repository

```
/model-001-of-002.safetensors  
/model-002-of-002.safetensors  
/model.safetensors.index.json  
/tokenizer.json  
/tokenizer_config.json  
/vocab.json  
/.gitattributes  
/config.json  
/generation_config.json  
/LICENSE  
/README.md  
/...
```

BUILD →

Model Artifact



→ *PUSH*



```
$ modctl modelfile generate .
```

```
$ modctl login -u username -p password harbor.registry.com
```

```
$ modctl build -t harbor.registry.com/models/qwen2.5-0.5b:v1 -f Modelfile .
```

```
$ modctl push harbor.registry.com/models/qwen2.5-0.5b:v1
```

Model Distribution



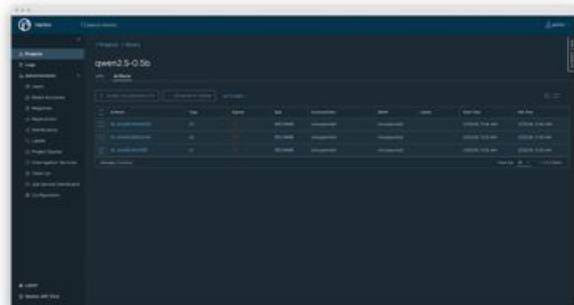
KubeCon



CloudNativeCon

Europe 2026

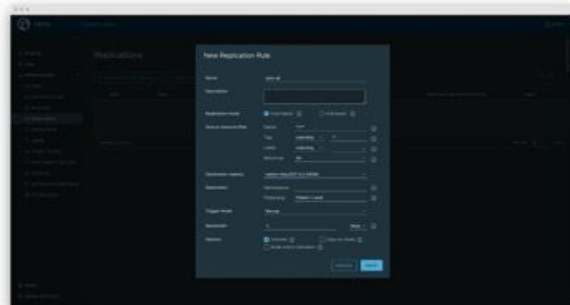
Management



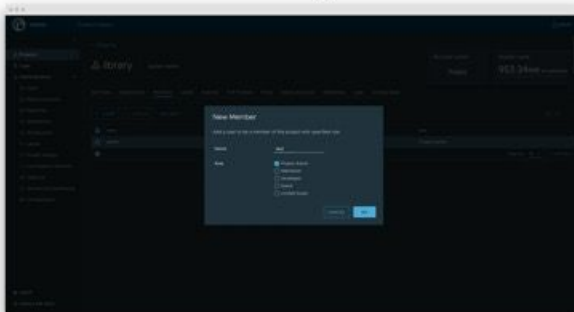
Versioning



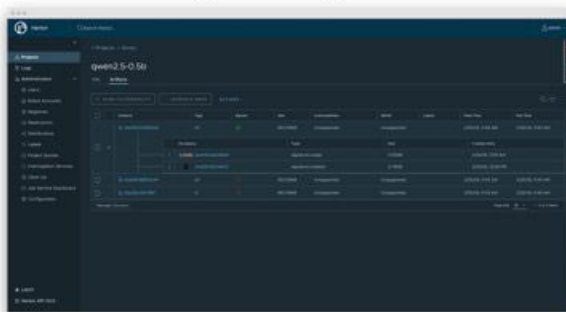
Lifecycle Management



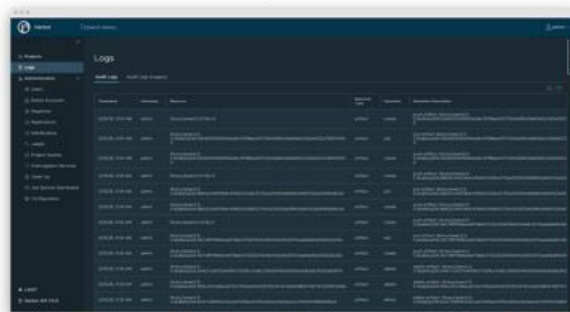
Replication



Access Control



Supply Chain Security



Audit

Demo



KubeCon



CloudNativeCon

Europe 2026

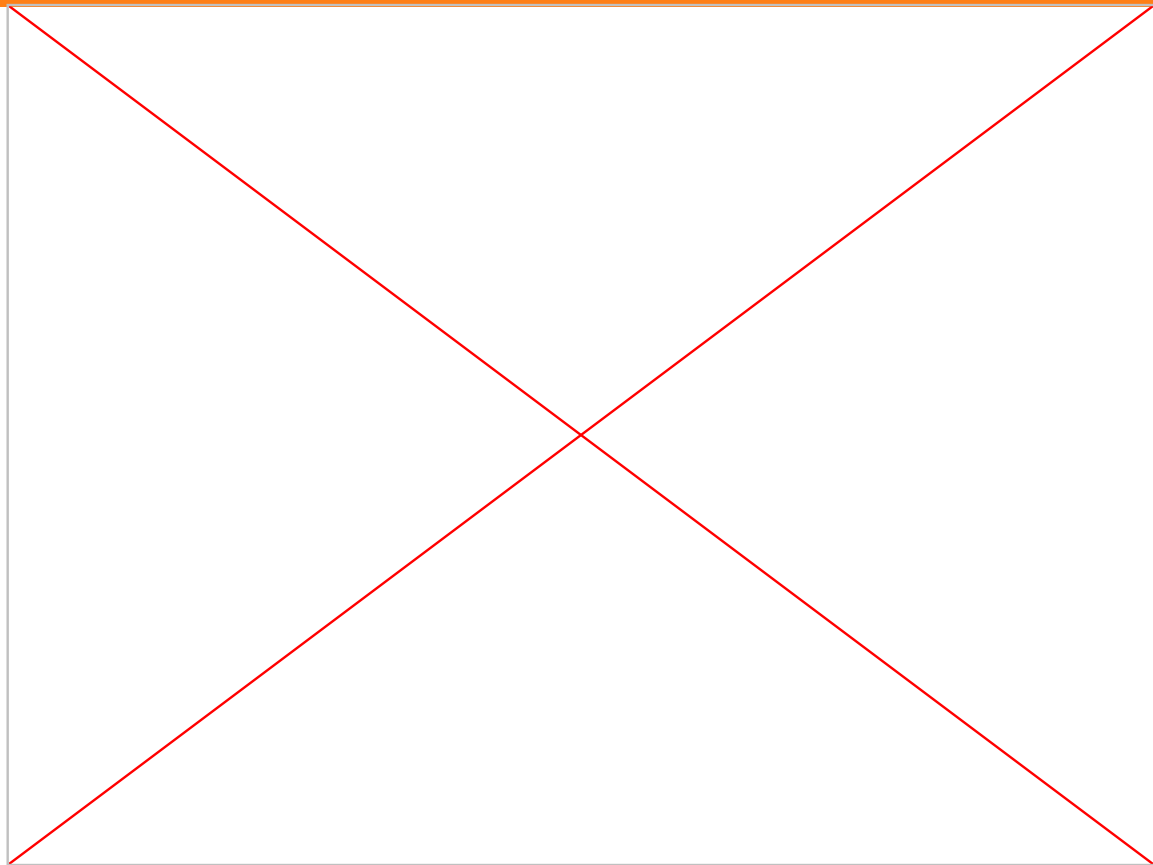
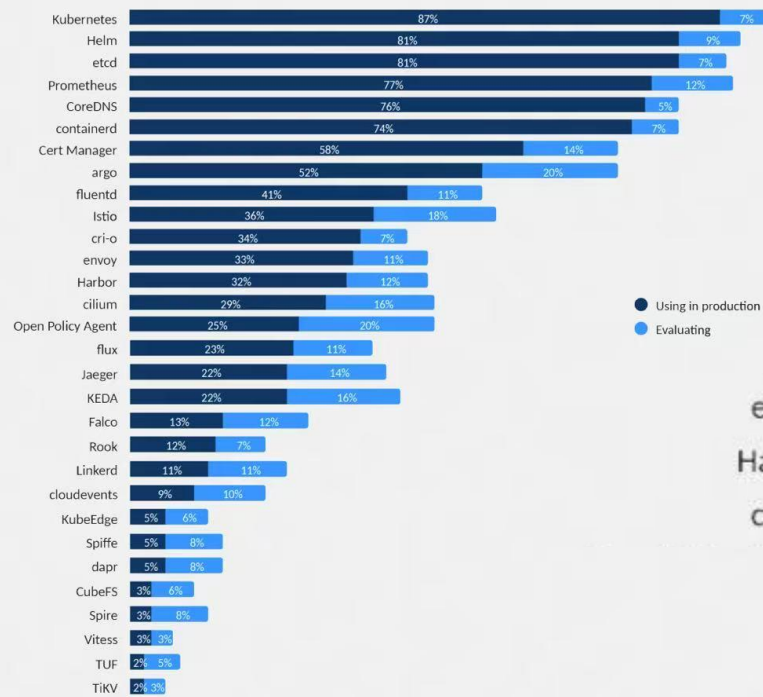


FIGURE 19
CNCF GRADUATED PROJECTS

Which of these graduated CNCF projects is your organization using in production or evaluating? (select one response)



2025 CNCF Annual Survey, Q32, Sample size = 395-596, DKNS excluded





KubeCon



CloudNativeCon

Europe 2026

