CSAN: A Secure Container Repository for Research Infrastructure

Ensuring security, provenance, and trust for research

Fabrice Jammes, LPCA
Martin Souchal, INRAE

What is CSAN

CSAN is a centralized, secure platform for the deposit, management and distribution of container images.

Based on Harbor, an Open Source community project.

Objective: federate the creation, storage and distribution of container images within the research ecosystem.

https://csanhub.org

CSAN Key features

Image security :

- Automatic scans to detect vulnerabilities in containers.
- Ability to notify users in real time if an image has a vulnerability.

Traceability:

Each image is signed and logged with its full history to guarantee total transparency.

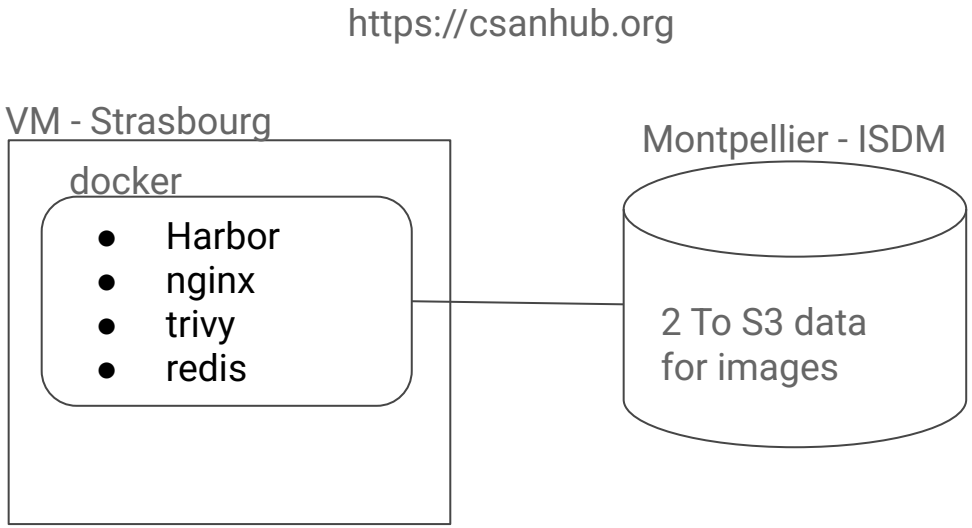
Access control:

Fine-grained rights management: only authorized people can download or modify images.

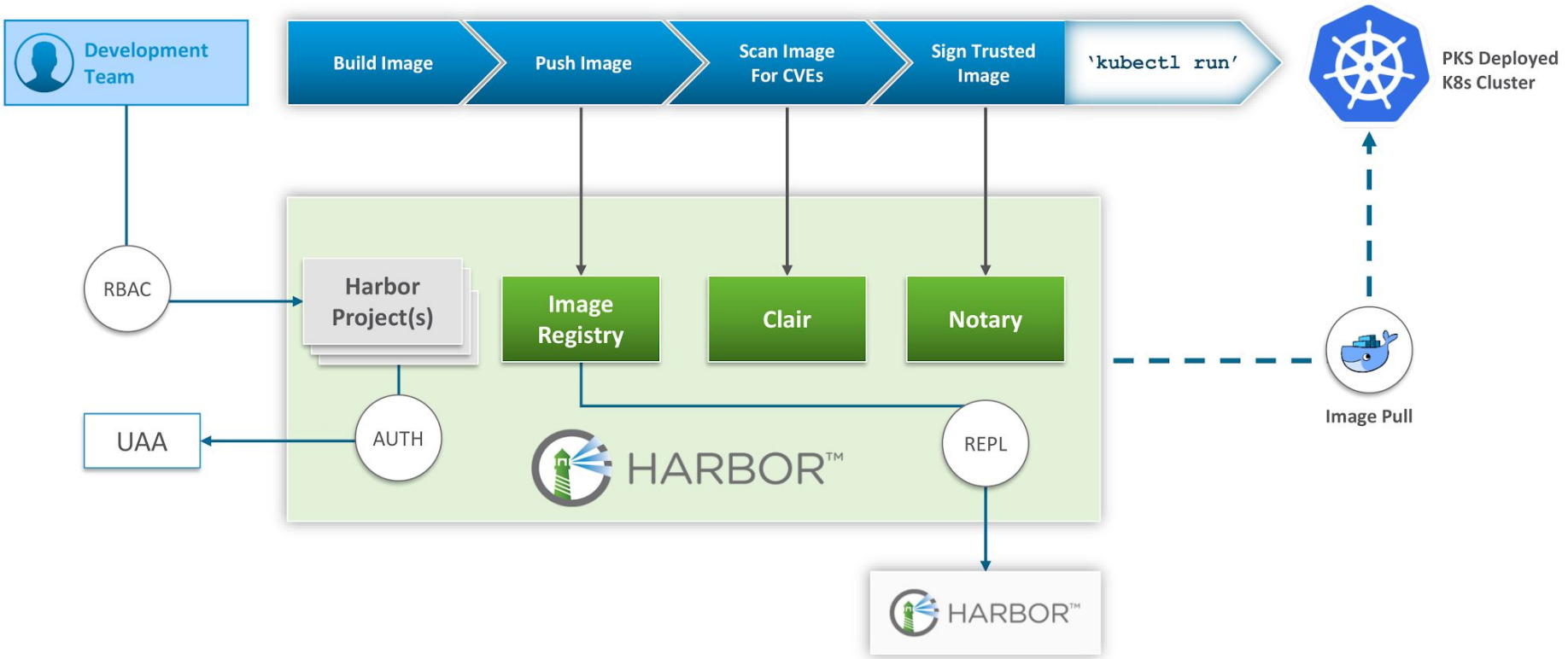
argo CD

HARBOR

Today architecture



CSAN Key features



New in 2025

- Authentication with a European identity provider (IAM)
- Enforce https security (for users and services)
- Monitoring and status page
- Official web site and documentation (https://help.csanhub.org/)

Milestones 2026

- Moving to Kubernetes in production
- Recruitment of a CDD to improve Harbor with our features and CI/CD pipelines
- Improve official web site and documentation (https://help.csanhub.org/)

next steps

- Add features to Harbor :
  - curation
  - automatically compile code for a given hardware (ex : AMD/Intel optimization)
  - display information about builder and maintainer
  - enable computing centers to indicate whether the container is running correctly on their premises, with which library options, and whether they approve its use on their center
  - run containers to analyze active security vulnerabilities in depth
- Providing ready to use gitlab pipelines to build, scan and upload images to CSAN (=> research team write code, then CSAN do the rest)