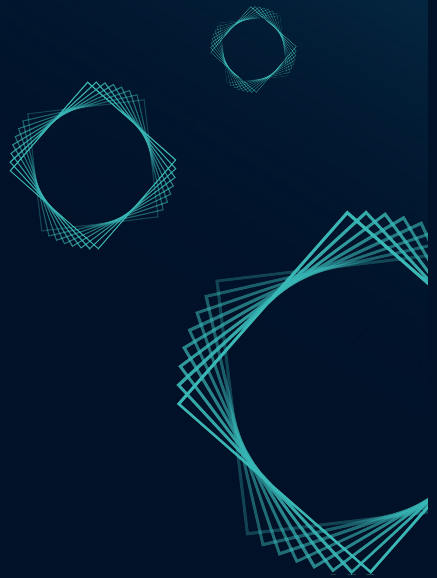
KUBERMATIC



Fast & Secure: Package, Sign, Verify and Deploy

Container Days '24 - Hamburg

Who is Batuhan?

trendyol.com

- Platfrom Engineer @Trendyol
- Best Sigstore Evangelist Award 2022
- CNCF Ambassador
- Kubestronaut
- Docker Captain
- KCD Istanbul Organizer

developerguyn@gmail.com

@developerguyba

linkedin.com/in/bthnapydin

developer-guy

KUBERMATIC

Who am I?

- K8s Consultant & Instructor @Kubermatic
- Working remotely from Istanbul
- CNCF Ambassador | Kubestronaut
- Kubernetes contributor #sig-k8s-infra
- Linux Foundation Instructor for CK.*
- KCD Istanbul Organizer

koray@kubermatic.com

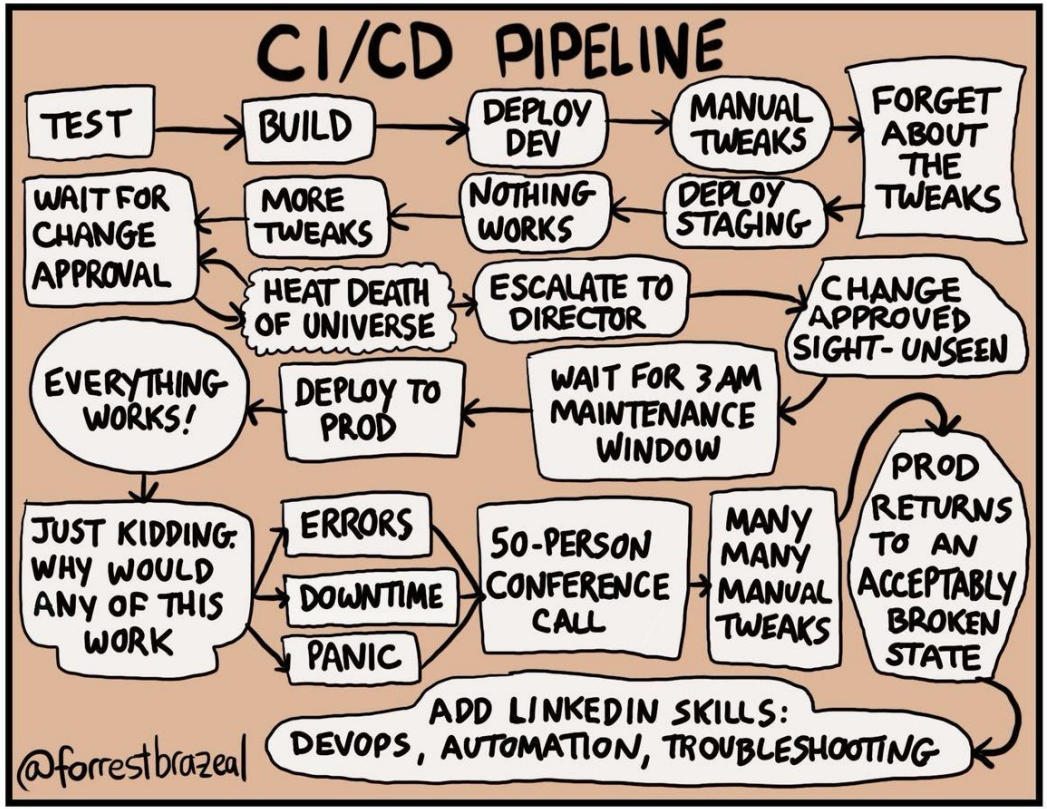
@korayoksay

linkedin.com/in/korayoksay/

koksay

KUBERMATIC

Real World Scenario



KUBERMATIC

GitOps Principles

Declarative

A system managed by GitOps must have its desired state expressed declaratively.

Versioned and Immutable

Desired state is stored in a way that enforces immutability, versioning and retains a complete version history.

Pulled Automatically

Software agents automatically pull the desired state declarations from the source.

Continuously Reconciled

Software agents continuously observe actual system state and attempt to apply the desired state.

Flux

KUBERMATIC

Sources

The origin of a repository containing the desired state of the system and the requirements to obtain it.

Reconciliation

Ensuring that a given state matches a desired state declaratively defined on a Git repository.

Kustomization

A local set of Kubernetes resources (e.g. kustomize overlay) that Flux is supposed to reconcile in the cluster.

Bootstrap

The process of installing the Flux components in a GitOps manner is called a bootstrap.

Continuous Deployment

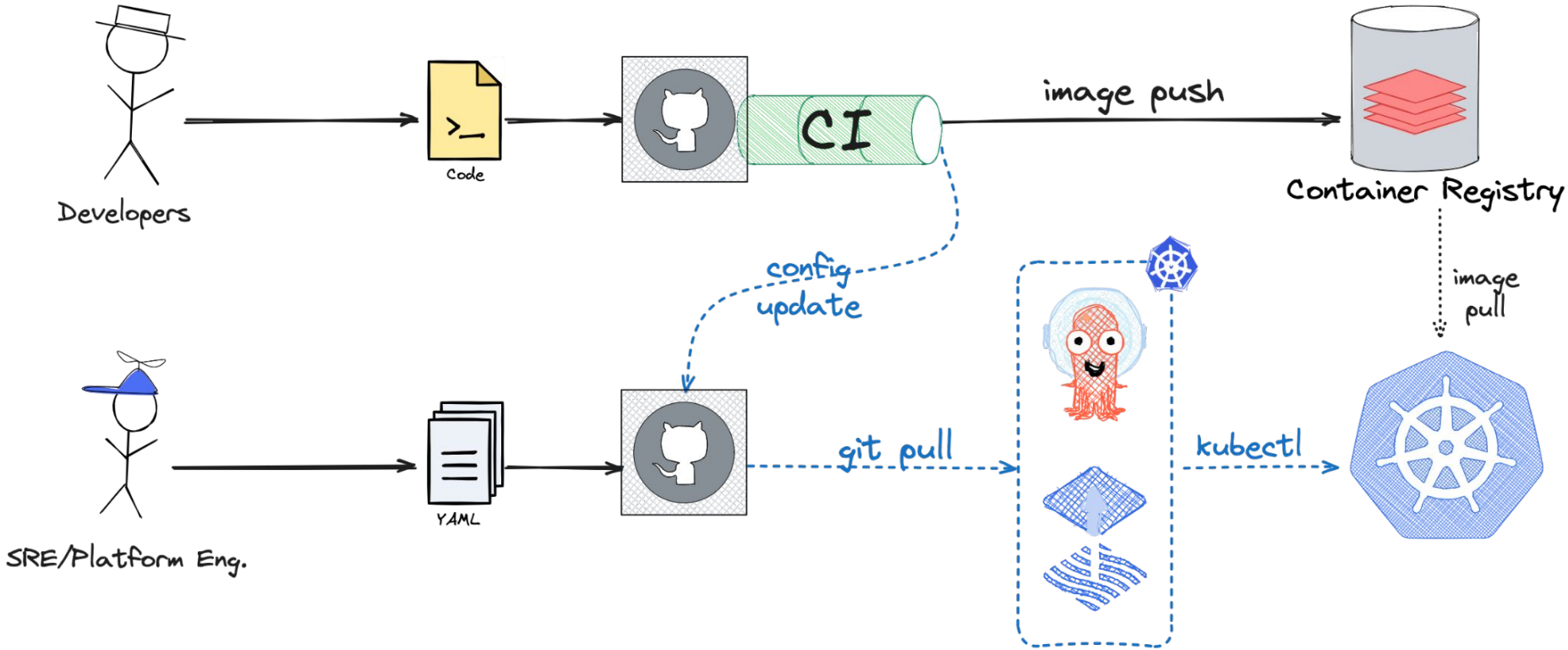
The practice of automatically deploying code changes to production once they have passed through automated testing.

Progressive Delivery

Gradually rolling out new features or updates to a subset of users, allowing to test and monitor the new features in a controlled environment

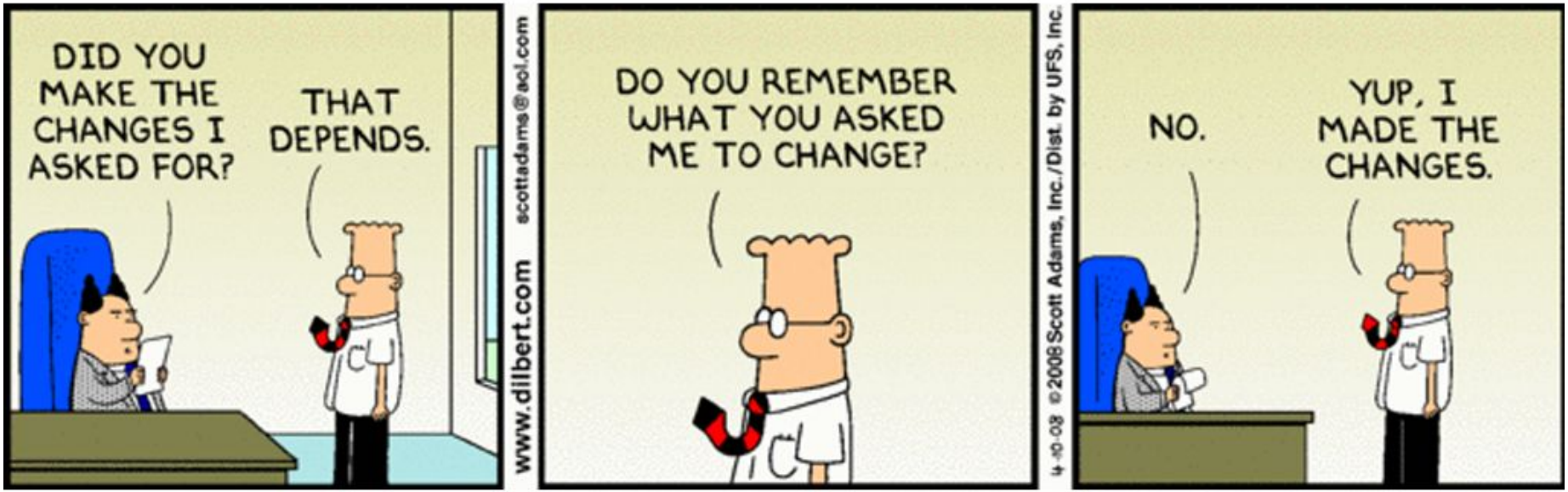
KUBERMATIC

How it works



KUBERMATIC

Single Source of Truth



KUBERMATIC

Sigstore / Cosign

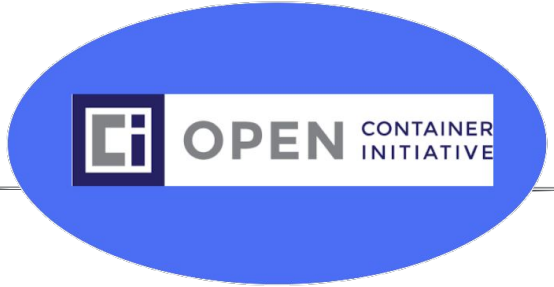
Was founded to address the fundamental challenges preventing wide scale usage of digital signatures within the software supply chain.
It is a set of open source projects and services that dramatically simplify the creation and verification of digital signatures

A tool for signing/verifying containers (and other artifacts) that ties the rest of Sigstore together, making signatures invisible infrastructure.

Includes storage in an Open Container Initiative (OCI) registry.

KUBERMATIC

OCI Artifacts



The Open Container Initiative (OCI) organization has played a crucial role in defining the industry-standard specifications for container formats, runtime, distribution, and artifacts.

https://specs.opencontainers.org

OCI artifacts encompass an extensive variety of content types: signatures, Software Bill of Materials, Helm charts, cat pictures, Tekton Bundles, WASM Modules, Open Policy Agent bundles, ...

https://oras.land/docs/concepts/artifact

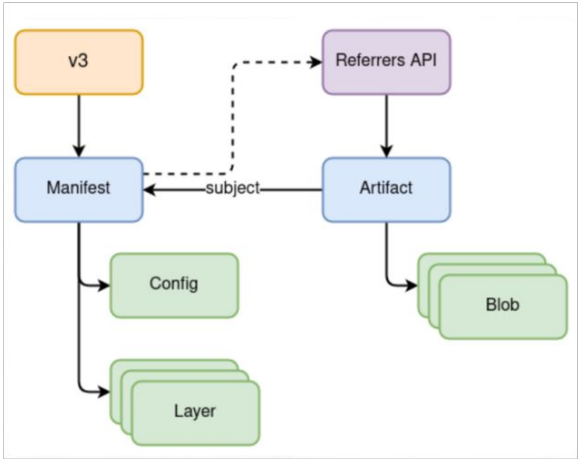
KUBERMATIC

OCI v1.1.0

KUBERMATIC

Changes in OCI Distrubition and Image Specs

v1.1.0 - 15 February 2024



- Storage using Image Manifest metadata
- New field artifactType to get the stored artifact type
- Custom value for config.mediaType field (or empty)
- Establish relationships for linking objects
  - New field subject on manitests for pointing to another object
  - New /v2/<name>/referrers API endpoint for querying the relationships

https://opencontainers.org/posts/blog/2024-03-13-image-and-distribution-1-1/

KUBERMATIC

Support?

Home > Unchained > Engineering Blog

Building towards OCI v1.1 support in cosign

Josh Dolitsky, Software Engineer
February 17, 2023

AWS Open Source Blog

Diving into OCI Image and Distribution 1.1 Support in Amazon ECR

by Jesse Butler and Michael Brown | on 01 AUG 2024 | in Amazon Elastic Container Registry, Announcements, Open Source | Permalink | Comments | Share

Announcing support of OCI v1.1 specification in Azure Container Registry

By Feynman Zhou
Published Jun 27 2024 07:26 PM 4,582 Views

Supporting OCI Distribution Spec v1.1.0 🎉

In this release, Harbor proudly supports OCI Distribution Spec v1.1.0. This update ensures that Harbor stays at the forefront of container image distribution, providing users with the latest standards and functionalities for seamless container management. Read more

KUBERMATIC

Zot: an OCI compliant registry

Zot is a production-ready, open-source, vendor-neutral container image registry server based purely on OCI standards.

It offers features such as minimal deployment using a single binary image, built-in authentication and authorization, and inline garbage collection and storage deduplication.

https://zotregistry.dev/

KUBERMATIC

Image Volumes (Kubernetes v1.31)

https://kubernetes.io/blog/2024/08/13/kubernetes-v1-31-release/#support-for-image-volumes

Support for image volumes

The Kubernetes community is moving towards fulfilling more Artificial Intelligence (AI) and Machine Learning (ML) use cases in the future.

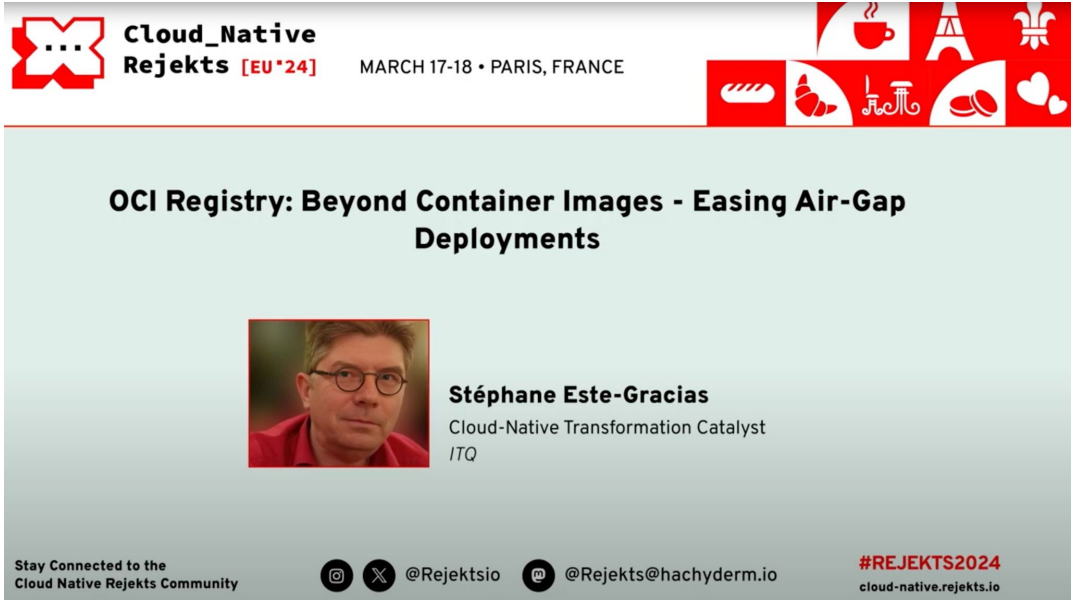
One of the requirements to fulfill these use cases is to support Open Container Initiative (OCI) compatible images and artifacts (referred as OCI objects) directly as a native volume source. This allows users to focus on OCI standards as well as enables them to store and distribute any content using OCI registries.

Given that, v1.31 adds a new alpha feature to allow using an OCI image as a volume in a Pod. This feature allows users to specify an image reference as volume in a pod while reusing it as volume mount within containers. You need to enable the `ImageVolume` feature gate to try this out.

This work was done as part of KEP #4639 by SIG Node and SIG Storage.

KUBERMATIC

More on OCI ...



KUBERMATIC

KUBERMATIC

THANK YOU!


developerguyn@gmail.com


@developerguyba


linkedin.com/in/bthnapydin


developer-guy


koray@kubermatic.com


@korayoksay


linkedin.com/in/korayoksay/


koksay