KUBERMATIC

Continuous Deployment: The GitOps, The Pipelines, and The Ugly

DevOps Pro Europe '24 - Vilnius

Who am I?

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

koray@kubermatic.com

@korayoksay

linkedin.com/in/korayoksay/

koksay

Common Release Antipatterns

Manual Deployments

Most modern applications are complex to deploy, involving many moving parts. Deploying them manually is error prune and can lead to different outcomes with changes on the ordering and timing of the steps.

Deploy to prod like env late

The first time the app is deployed to production-like environment (staging) after all the development is done.

Manual Config Management

Configuration changes are performed by the operations team, manually on the production system.

CI / CD

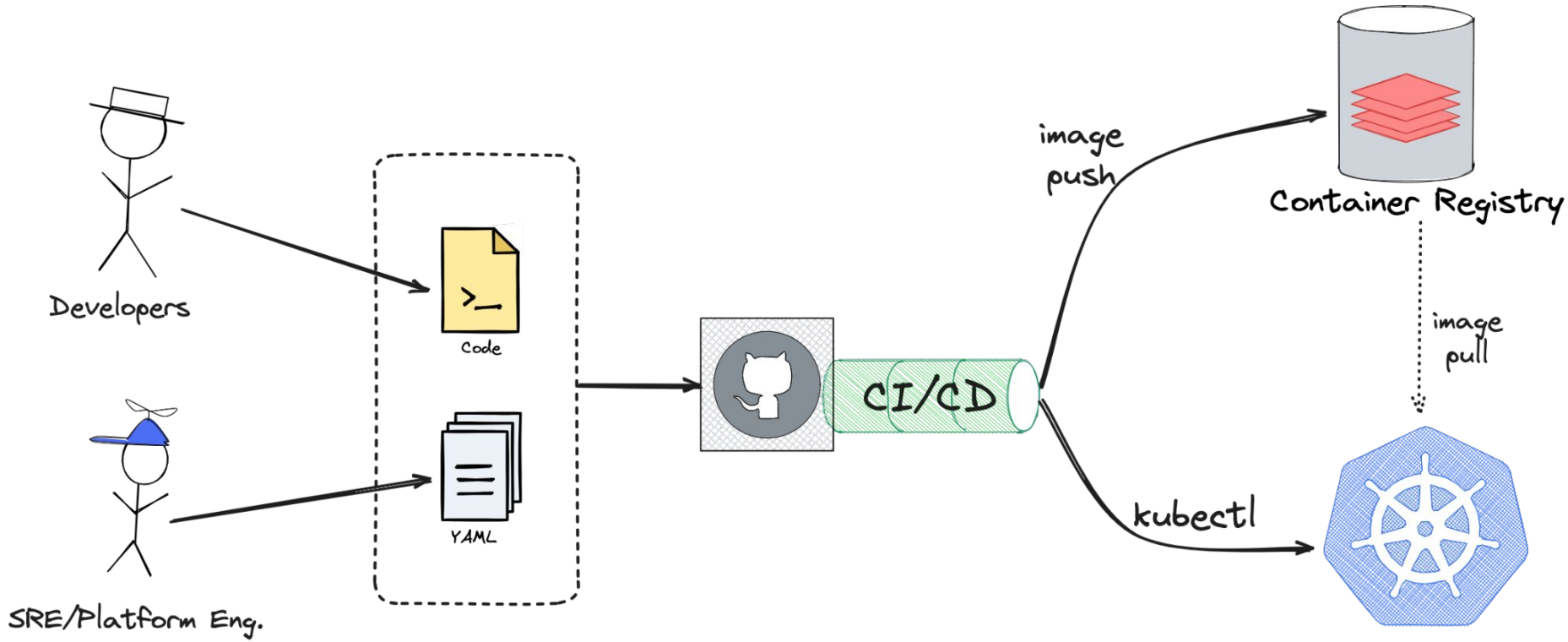
Continuous Integration

Practice of integrating all your code changes into the main branch of a shared source code repository early and often, automatically testing each change when you commit or merge them, and automatically kicking off a build.

Continuous Delivery

Following the automation of builds and unit and integration testing in CI, continuous delivery automates the release of that validated code to a repository.

Pipelines


Developers
SRE/Platform Eng.
Code
YAML
CI/CD
image push
Container Registry
image pull
kubectl

Issues with the Push Model

Correctness

The scripts that are used to deploy the application would not guarantee convergence hence atomic deployments cannot be done.

Security

Credentials are stored on a 3rd party company's infrastructure which we have no influence for it's security.

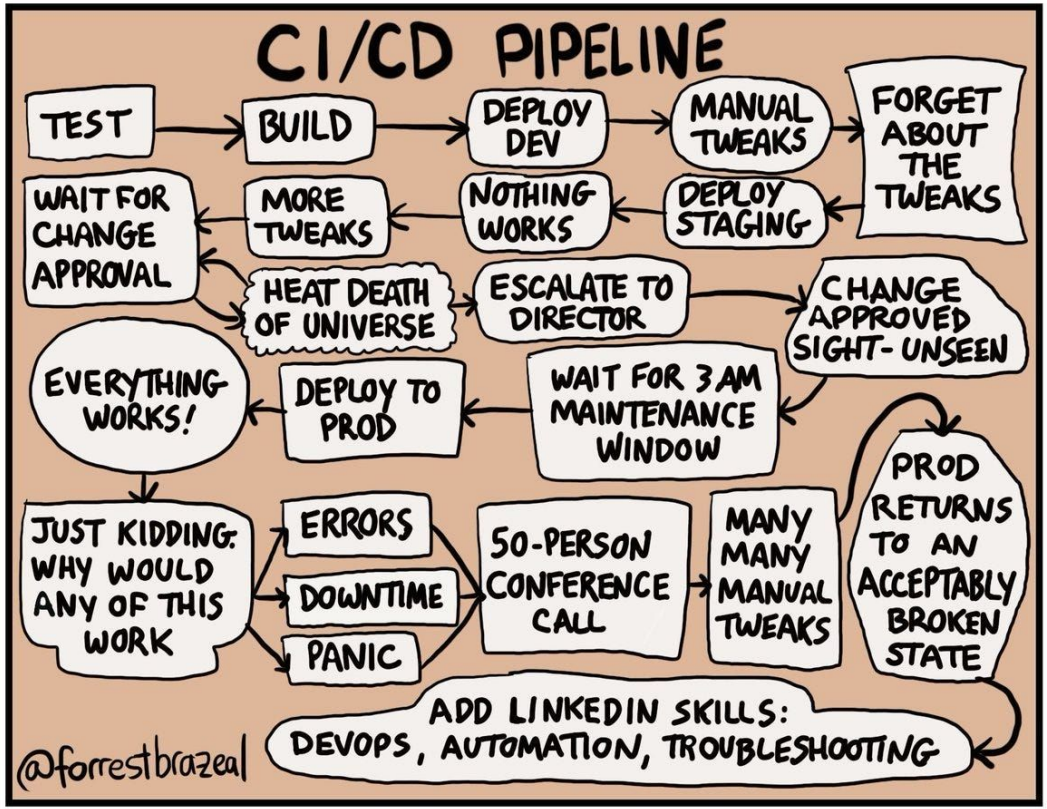
Current State

It's possible that manual updates can be performed on the system and there could be gaps between Git and the Kubernetes cluster.

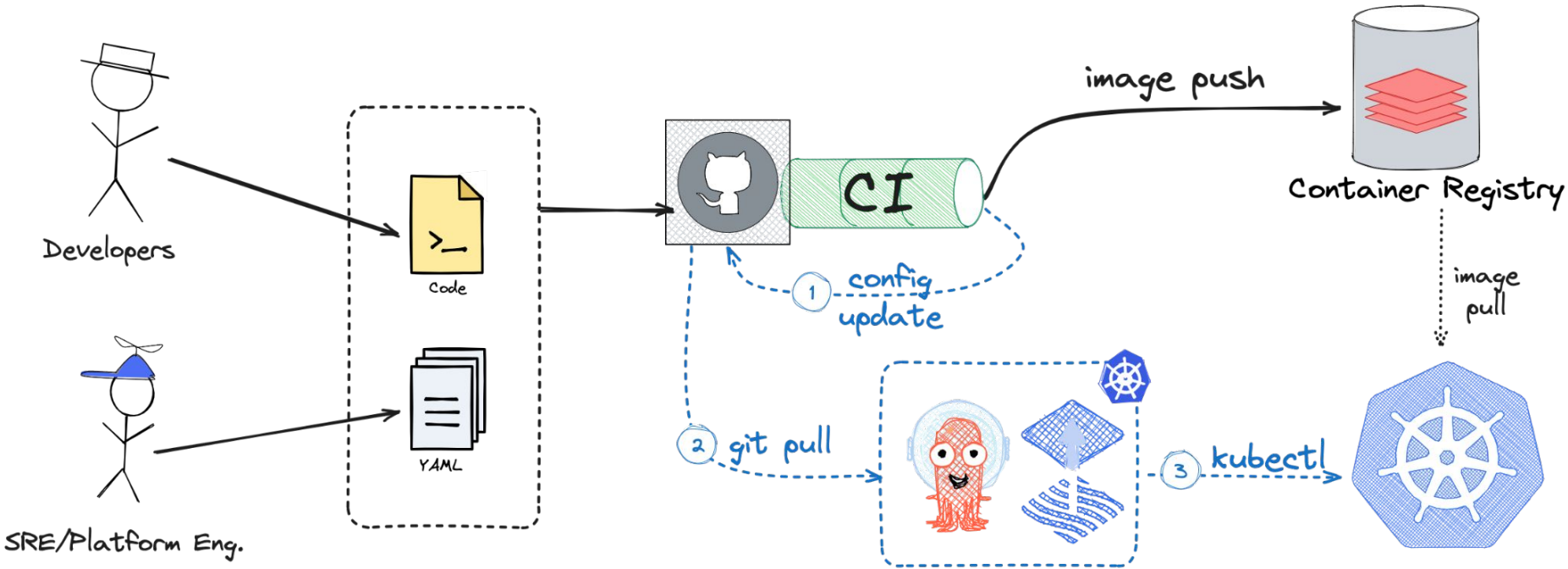
DevEx

Developers need to understand the problems with the deployments scripts and maybe need to fix them. This requires k8s administration knowledge.

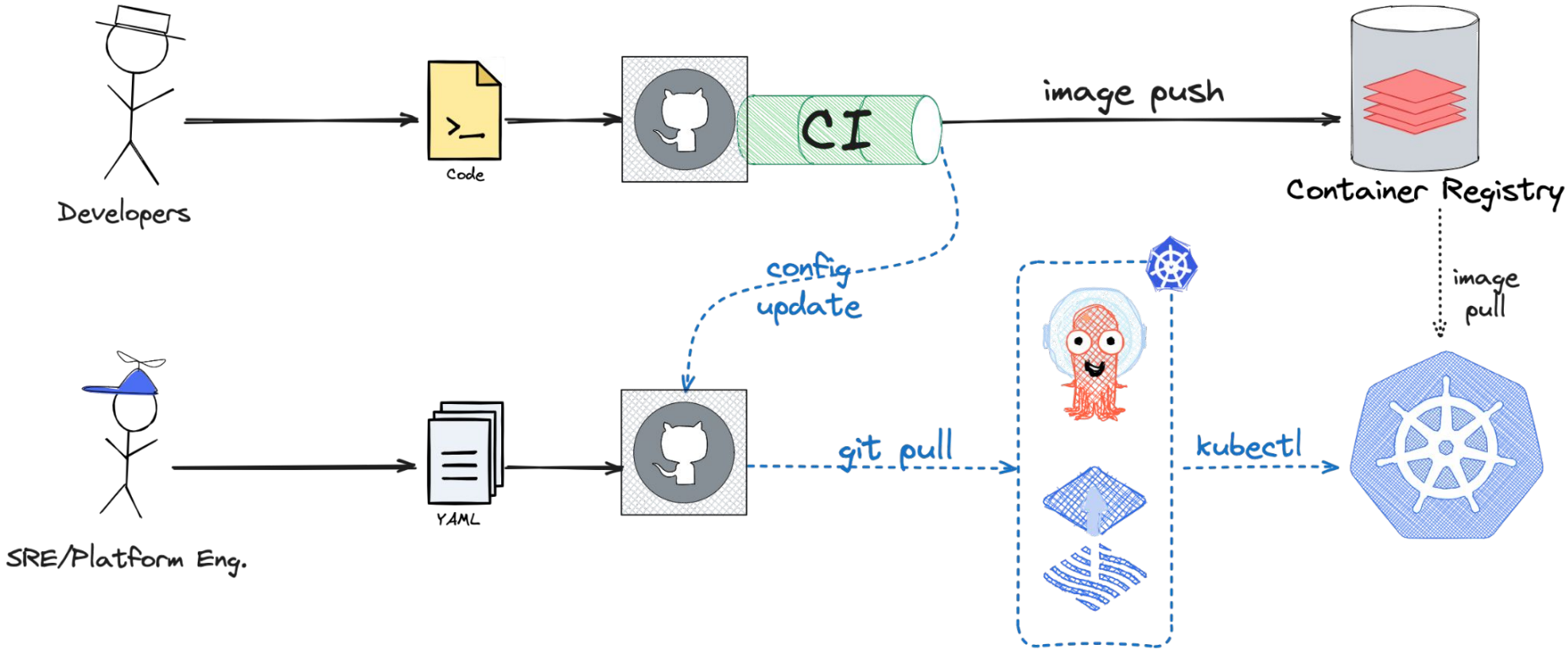
Real World Scenario



GitOps (pull)


Developers
SRE/Platform Eng.
Code
YAML
CI
image push
Container Registry
image pull
1 config update
2 git pull
3 kubectl

Recommended Practise



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.

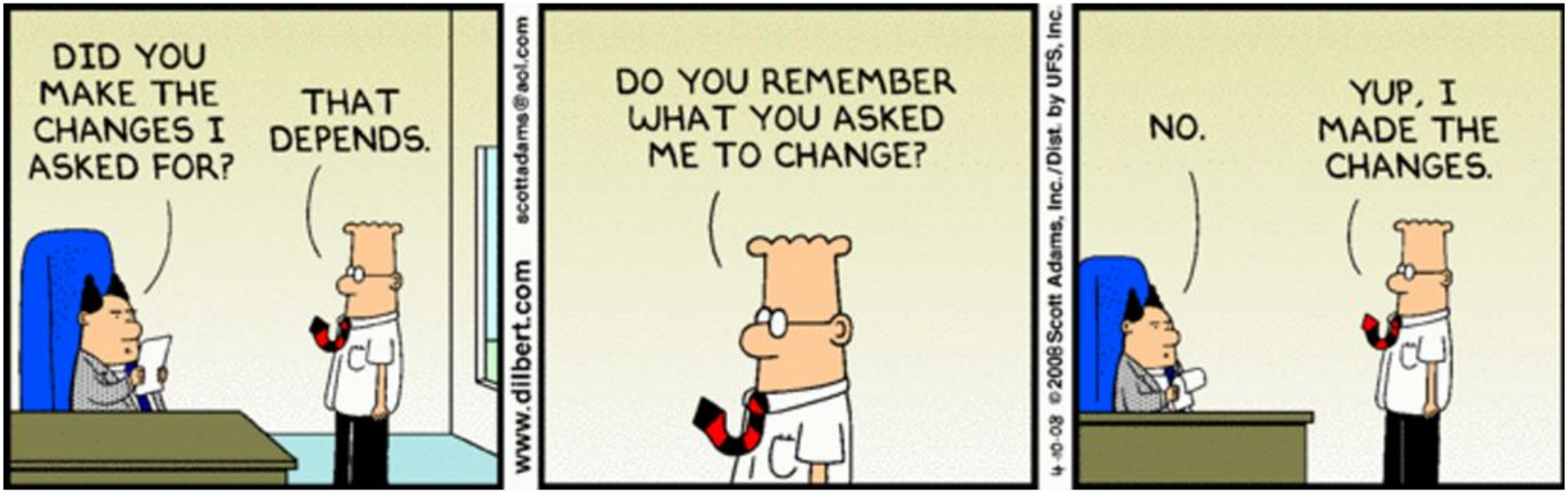
Pulled Automatically

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.

Single Source of Truth



Is it Perfect?

tinyurl.com/k8s-flux-incident

Postmortem of the EKS Prow build cluster outage on 2024-02-21

Authors: Marko Mudrinić, Koray Oksay
Status: Review in progress, action items TBD
Last update: 2024-02-22

Impact: eks-prow-build-cluster being non-operational for almost 2 hours; all monitoring data prior to the incident is lost
Root cause: A broken “kustomization.yaml” file triggered a mass deletion of Flux resources and therefore a mass deletion of all components managed by Flux

Timeline

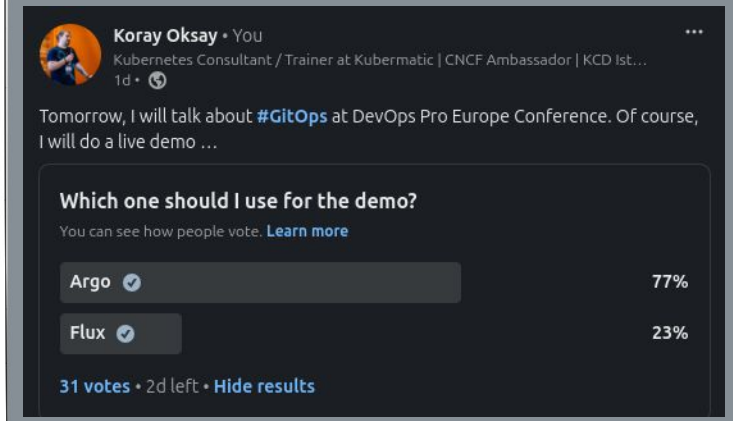
2024-02-14 12:45 UTC: PR #6423 has been created in kubernetes/k8s.io
2024-02-19 13:07 UTC: PR #6423 has been approved for merge and rollout
2024-02-21 12:38 UTC: Additional unrelated changes have been approved
2024-02-21 14:13 UTC: Terraform changes have been applied to eks-prow-build-cluster (prod)
2024-02-21 14:25 UTC: PR #6423 has been merged to kubernetes/k8s.io
2024-02-21 14:30 UTC: Flux automatically applied changes made to the YAML manifests
2024-02-21 14:30-15:00 UTC:

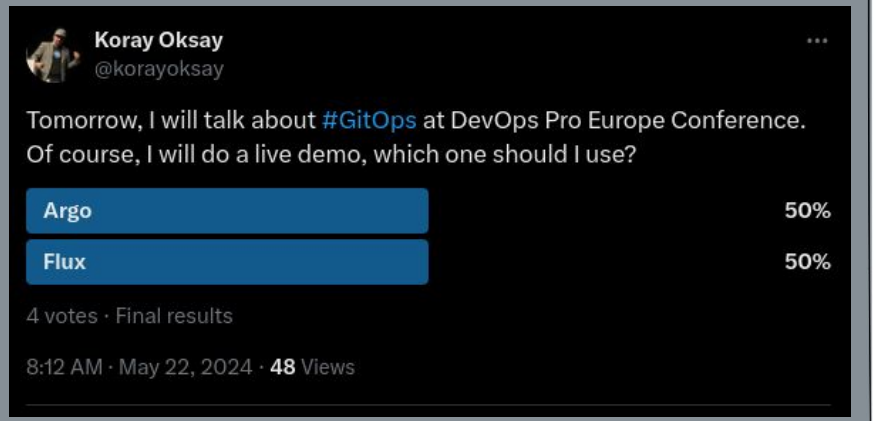
- Using kubectl to do any operation started resulting in RBAC “forbidden” errors
- Prow started reporting inability to run jobs on eks-prow-build-cluster
- Alerts in the #testing-ops Slack channel started reporting unsuccessful heartbeats
- Contributors started reporting that jobs for their PRs are not getting started
- The issue has been confirmed and a message has been posted on #sig-k8s-infra
- PR #6450 has been created as an attempt to mitigate the issue

2024-02-21 15:50 UTC: Authorization/RBAC issues have been resolved, jobs (Pods) were getting created but failed to start due to missing Secrets
2024-02-21 16:12 UTC: Missing Secrets were manually created, jobs started running again
2024-02-21 16:12-17:17 UTC: eks-e2e-boskos AWS accounts were added to boskos again (this required rolling out all access keys)
2024-02-21 17:17 UTC: The incident has been resolved and the cluster was declared to be fully functional

DEMO TIME!

https://killercoda.com/koksay/course/gitops/



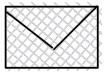


KUBERMATIC

QUESTIONS?

KUBERMATIC

THANK YOU!


koray@kubermatic.com


@korayoksay


linkedin.com/in/korayoksay/


koksay