

# The Seven Deadly Sins *of GitOps*

Cansu Kavili-Örnek

AI Platform Architect @ Red Hat

Koray Oksay

Kubernetes Consultant @ Kubermatic



Platform Architect @ Red Hat



Based in Germany



Platform Engineering Ambassador



Team Topologies Advocate



Huge believer in Open Source



Cansu



Koray



Consultant and Trainer @Kubermatic



Working remotely from Istanbul



CNCF Ambassador and Kubestronaut



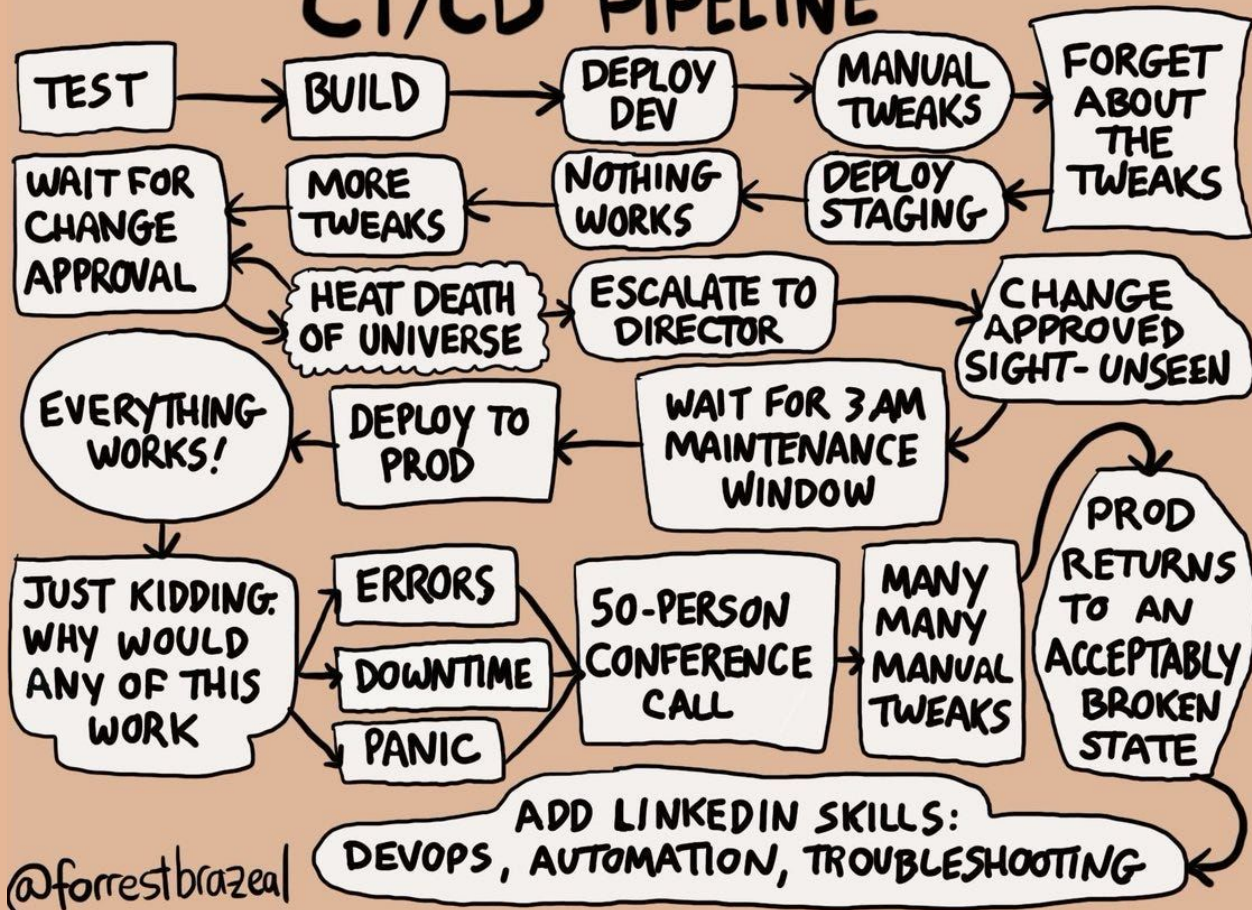
Kubernetes Contributor: SIG K8s Infra  
and K8s conformance testing



KCD and DevOpsDays Istanbul  
Organizer



# CI/CD PIPELINE



@forrestbrazeal



# The Promise of GitOps

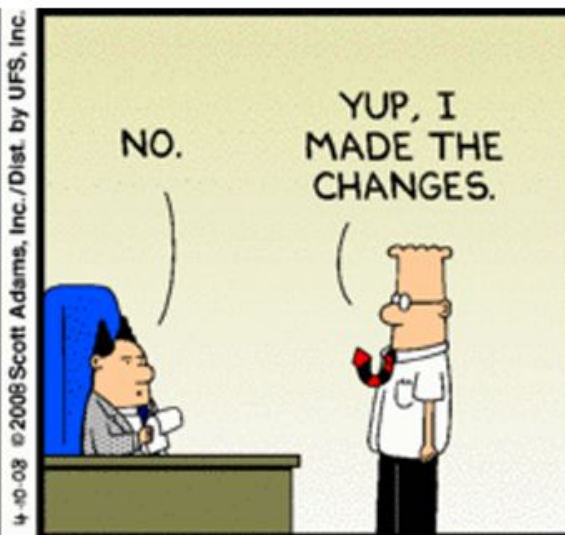
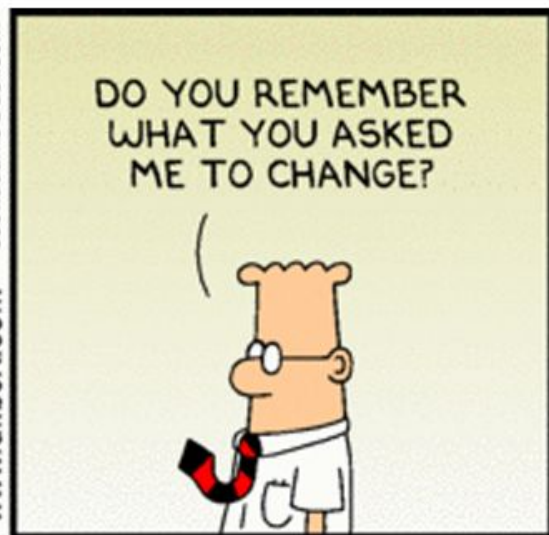
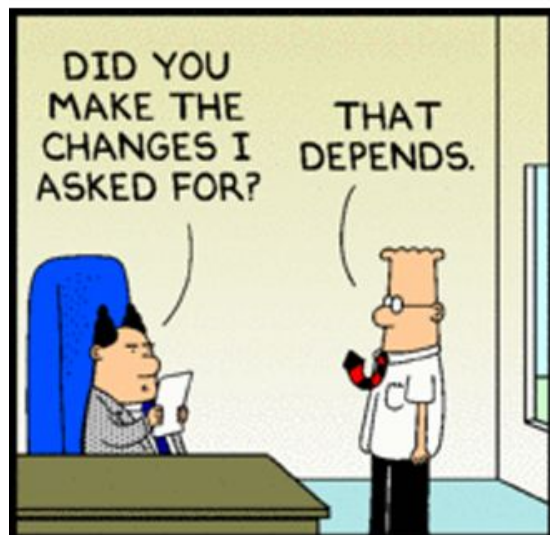
*It's not a 'set it and forget it' solution; it's a living, breathing system.*

GitOps Principles:

1. Declarative
2. Versioned and Immutable
3. Pulled Automatically
4. Continuously Reconciled

..that provides:

- Simplicity
- Consistency
- Automation
- Single Source of Truth






# Sin #1: PRIDE


*or*

*We know better than the system!*



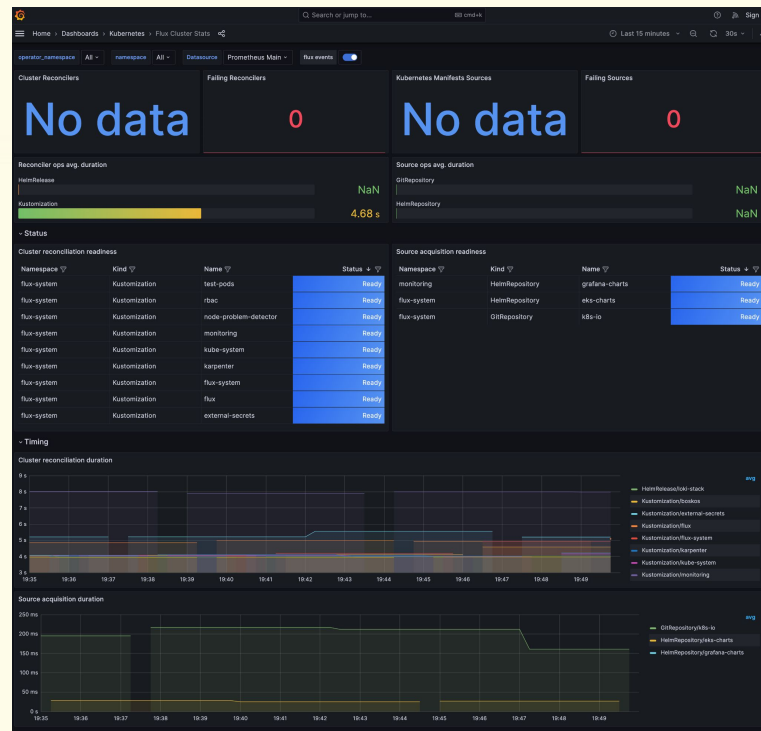


 **Mistake:** The belief that your Git repo always reflects reality, leading to complacency

 **Consequence:** Inconsistency, non-reproducible environments, "works on my machine" for production

 **Redemption:** Monitor for drift, automate reconciliation, process for hotfixes





**ArgoCD APP** 7:38 PM

Application **app-of-apps** is out of sync.  
 Check the details at: <http://localhost:8080/applications/app-of-apps>.

**app-of-apps**

Sync Status: Cluster  
 OutOfSync: gke-test-cluster

Application **app-of-apps** update has started at 2025-04-30T16:38:23Z.  
 Check the details at: <http://localhost:8080/applications/app-of-apps>.

**app-of-apps**

Update Status: Cluster  
 In Progress: gke-test-cluster

Started At: 2025-04-30T16:38:23Z

**source-controller APP** 11:12 AM

**gitrepository/k8s-io.flux-system**

failed to checkout and determine revision: unable to list remote for 'https://github.com/kubernetes/k8s.io': Get "https://github.com/kubernetes/k8s.io/info/refs?service=git-upload-pack": dial tcp 140.82.112.3:443: i/o timeout

summary  
 EKS Prow Build Cluster





# **Sin #2: ENVY**


*or*

*Blindly Copying Other GitOps Setups*



 **Mistake:** Desiring another org's "perfect" GitOps setup without understanding your own context

 **Consequence:** Over-engineering, unnecessary complexity, frustration, slowed adoption

 **Redemption:** Start simple, understand your needs, Adapt instead of just copying



# **Sin #3: SLOTH**

*or*


*Ignoring Reconciliation Errors*





 **Mistake:** Laziness in addressing errors reported by your GitOps engine, letting them pile up

 **Consequence:** Accumulation of technical debt, masked critical issues, eventual system failure

 **Redemption:** Alerting and monitoring, automated remediation where appropriate



# **Sin #4: WRATH**

*or*

*Blaming GitOps for Non-GitOps  
Problems*





 **Mistake:** Expressing frustration at the GitOps system when the root cause lies elsewhere

 **Consequence:** Misdiagnosis, wasted time, undermining trust in the GitOps approach

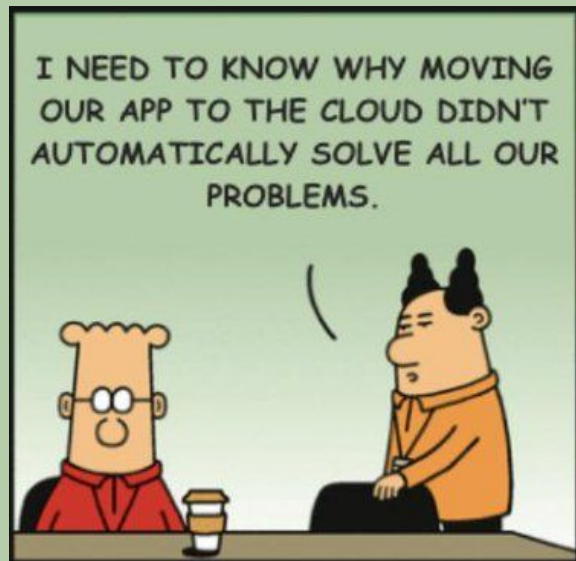
 **Redemption:** Holistic monitoring, structured debugging, collaboration



# Sin #5: LUST

*or*

*Obsessive Feature Chasing*





Dilbert.com @ScottAdamsSays

11-08-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMeel



 **Mistake:** An insatiable desire for the latest tools & features without a clear need

 **Consequence:** Instability, increased complexity, team burnout, lack of consistent understanding

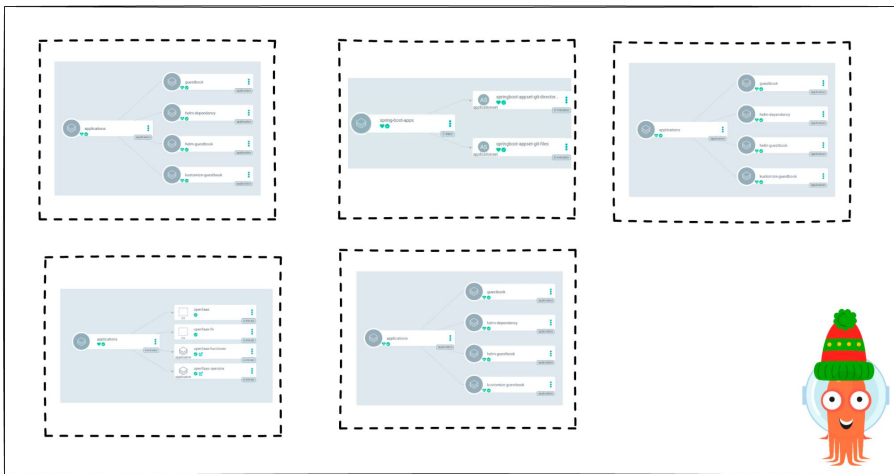
 **Redemption:** Define your reqs, stability over novelty, controlled experimentation



# Sin #6: GLUTTONY

*or*

*One Repo to Rule Them All*





```
EXPLORER  ...
> OPEN EDITORS
  GITOPSCON-ORG
  > docs
  > team-1
  > team-2
  > team-3
  > team-4
  > team-5
  > templates
  ! Chart.yaml
  @ README.md
  {} values.schema.json
  ! values.yaml

! values.yaml  > argocd > [ ] teams > { } 1 > [ ] applications > { } 0 >
1  argocd:
2    enabled: true
3    version: v1.8.2
4    repositories:
5      - "https://charts.bitnami.com/bitnami"
6      - "https://helm.releases.hashicorp.com"
7      - "https://kubecost.github.io/cost-analyzer"
8      - "https://gitlab-ce.apps.emea.rht-labs.com"
9    environments:
10     - test
11     - staging
12   teams:
13     - name: team-1
14       applications:
15         - name: oranges
16       replicate:
17         environments:
18           - performance: # environment name
19             - oranges # service name
20     - name: team-2
21       applications:
22         - name: pomegranate
23         - name: pear
24     - name: team-3
25       applications:
26         - name: cherry
27
28

! pomegranate.yaml  ! pear.yaml
1  deployment:
2    enabled: true
3    revision: 0.0.10
4
```



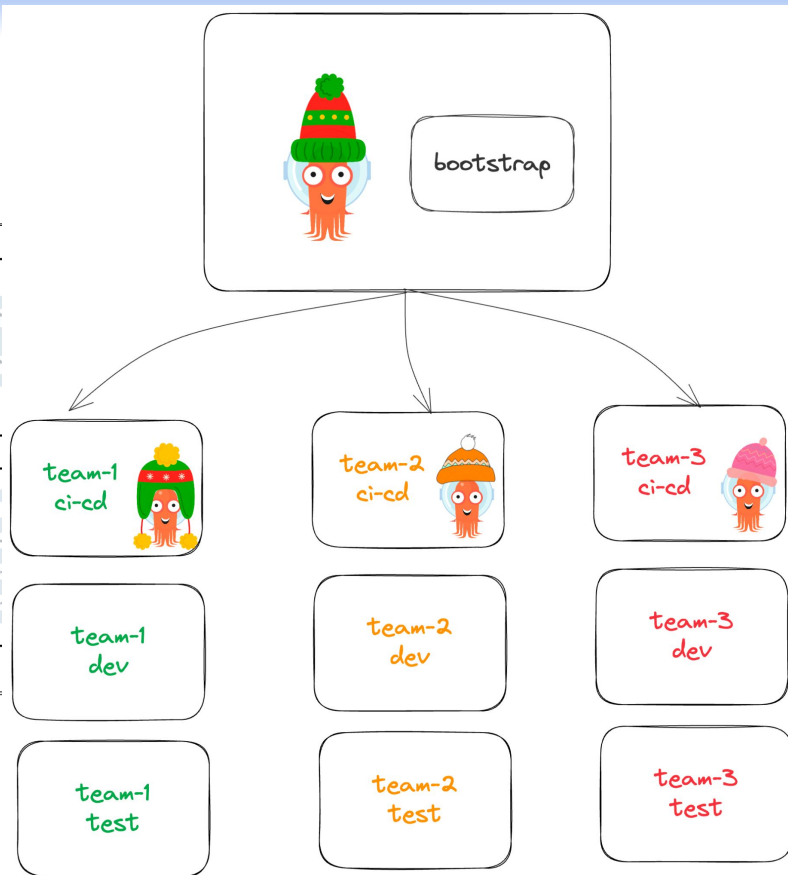
 **Mistake:** Consolidating all app and environment config into a single, monolithic Git repository for perceived simplicity

 **Consequence:** Slow operations, frequent merge conflicts, long sync times, and eroded team autonomy

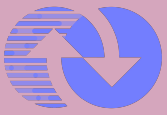
 **Redemption:** A multi-repo strategy; each app has its own repo, enabling isolated deployments and clearer ownership

\* [https://argo-cd.readthedocs.io/en/stable/operator-manual/high\\_availability/#monorepo-scaling-considerations](https://argo-cd.readthedocs.io/en/stable/operator-manual/high_availability/#monorepo-scaling-considerations)





```
oed > [ ] teams > { } 1 > [ ] applications > { } 0 > team-2 > staging > ! pear.yam > { }  
ue  
.8.2  
s:  
//charts.bitnami.com/bitnami"  
//helm.releases.hashicorp.com"  
//kubecost.github.io/cost-analyzer  
//gitlab-ce.apps.emea.rht-labs.com  
s:  
eam-1  
tions:  
e: oranges  
te:  
onments:  
performance: # environment name  
- oranges # service name  
eam-2  
tions:  
e: pomegranate  
e: pear  
eam-3  
tions:  
e: cherry
```





# **Sin #7: GREED**

*or*

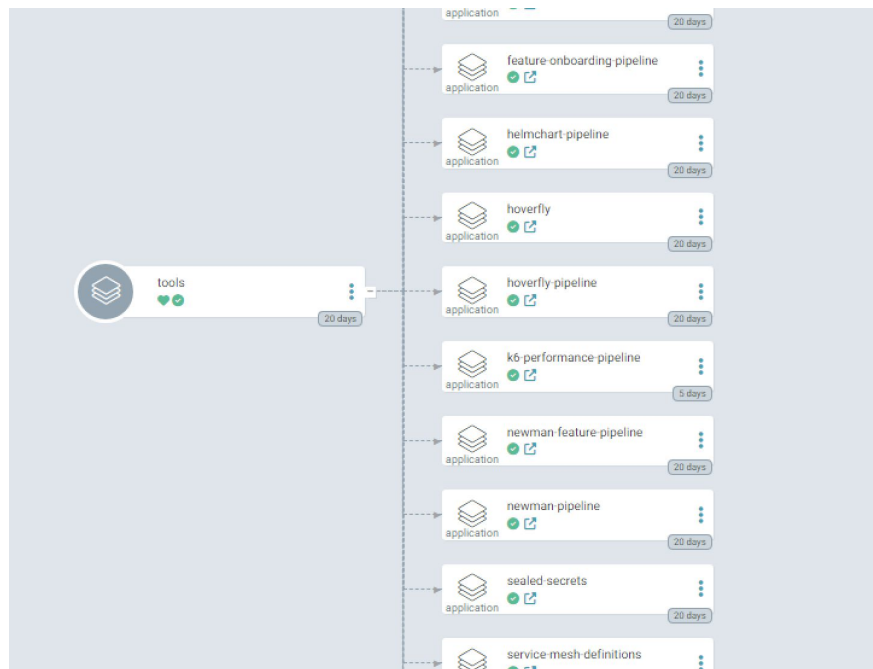
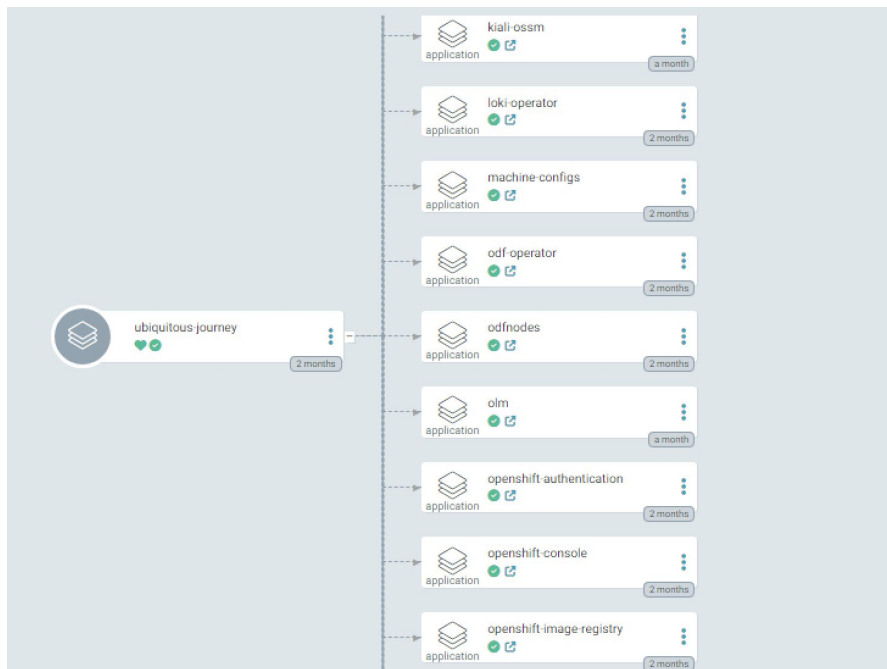
*Hoarding Knowledge*



 **Mistake:** The selfish accumulation of GitOps knowledge by a few individuals, leading a lack of transparency

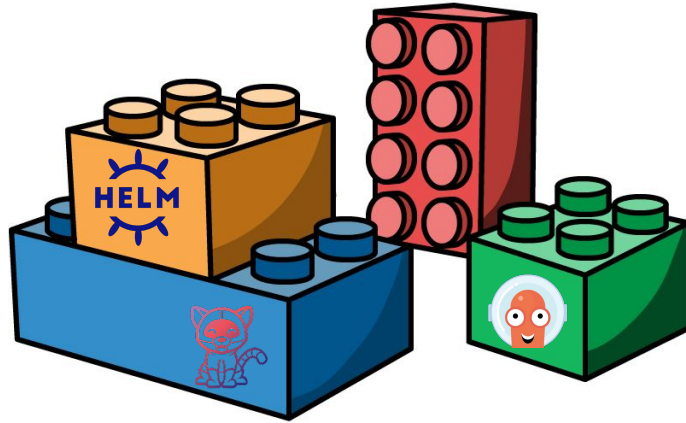
 **Consequence:** Bus factor of one, tribal knowledge, slow onboarding, increased risk of errors

 **Redemption:** Documentation, knowledge sharing sessions, automate setup



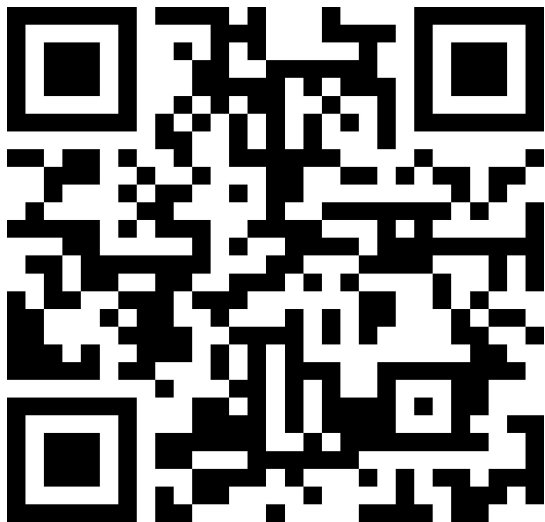


Provide *Lego Bricks* and a way of how to  
*do something.*





# Key Takeaways



*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](#)





- ✓ GitOps is a discipline, not just a tool choice.
- 🚧 Always watch for drift.
- 🪶 Simplicity > complexity.
- 🧭 Don't blindly follow, design what fits your team.
- 📈 Observability is not optional.
- ♻️ Reconciliation is the heartbeat, don't ignore it.



Deadly Sin	GitOps Virtue
<b>Pride</b> – Ignoring drift	<b>Humility</b> – Trust but verify, monitor for drift and reconcile automatically
<b>Greed</b> – Hoarding knowledge	<b>Collaborate</b> – Share the knowledge via documentation and internal workshops
<b>Wrath</b> – Hotfixing under pressure	<b>Patience</b> – Use safe workflows, rollbacks, and reviews
<b>Envy</b> – Blindly copying others' setups	<b>Discernment</b> – Design for your team's needs and maturity
<b>Lust</b> – Chasing every shiny GitOps tool	<b>Discipline</b> – Master fundamentals before scaling complexity
<b>Gluttony</b> – Overconfiguring and overengineering	<b>Simplicity</b> – Keep your manifests minimal, declarative, and understandable
<b>Sloth</b> – Ignoring reconciliation errors	<b>Diligence</b> – Treat reconcilers and alerting as first-class citizens

# Thank you!



[cansu@redhat.com](mailto:cansu@redhat.com)



[linkedin.com/in/ckavili](https://linkedin.com/in/ckavili)



[koray@kubermatic.com](mailto:koray@kubermatic.com)



[linkedin.com/in/korayoksay](https://linkedin.com/in/korayoksay)