Automating secret rotation in Kubernetes

Minimizing mistakes by removing the human element

Márk Sági-Kazár

2023-02-04 @ FOSDEM ’23

`whoami`

Márk Sági-Kazár

Engineering Technical Lead @ Cisco

Help engineering teams run their business on Kubernetes

@sagikazarmark

https://sagikazarmark.hu

Once upon a time..

Why is secret rotation important?

- Maintain security of sensitive information
- Meet compliance requirements
- Reduce the risk of a data breach

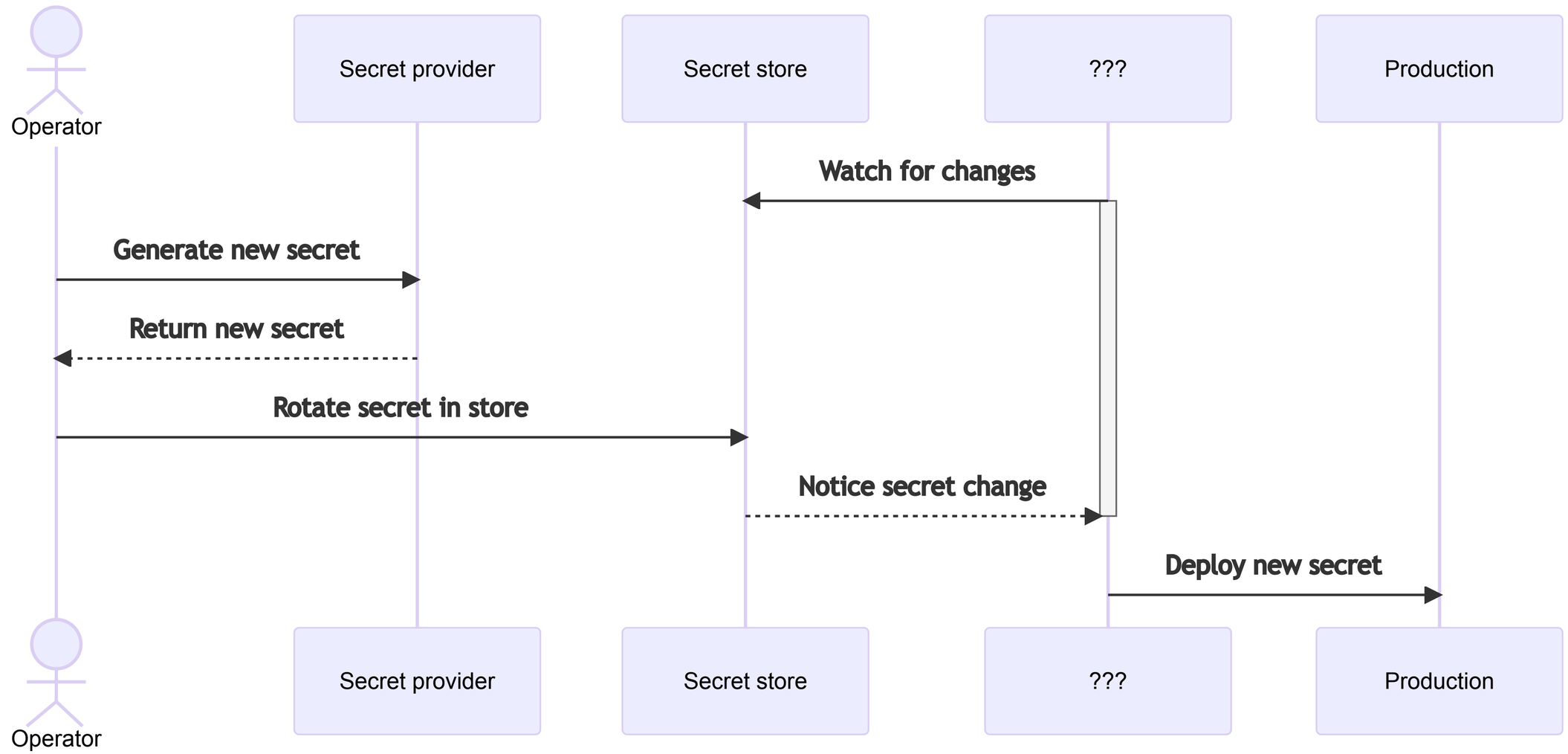
Challenges of secret rotation

- Complexity
- Time-consuming and error prone process
- Disruption of service availability

Secret rotation should be…

- possible
- automated
- periodic

Secret rotation flow



Secret rotation in Kubernetes

Deploying secrets to Kubernetes

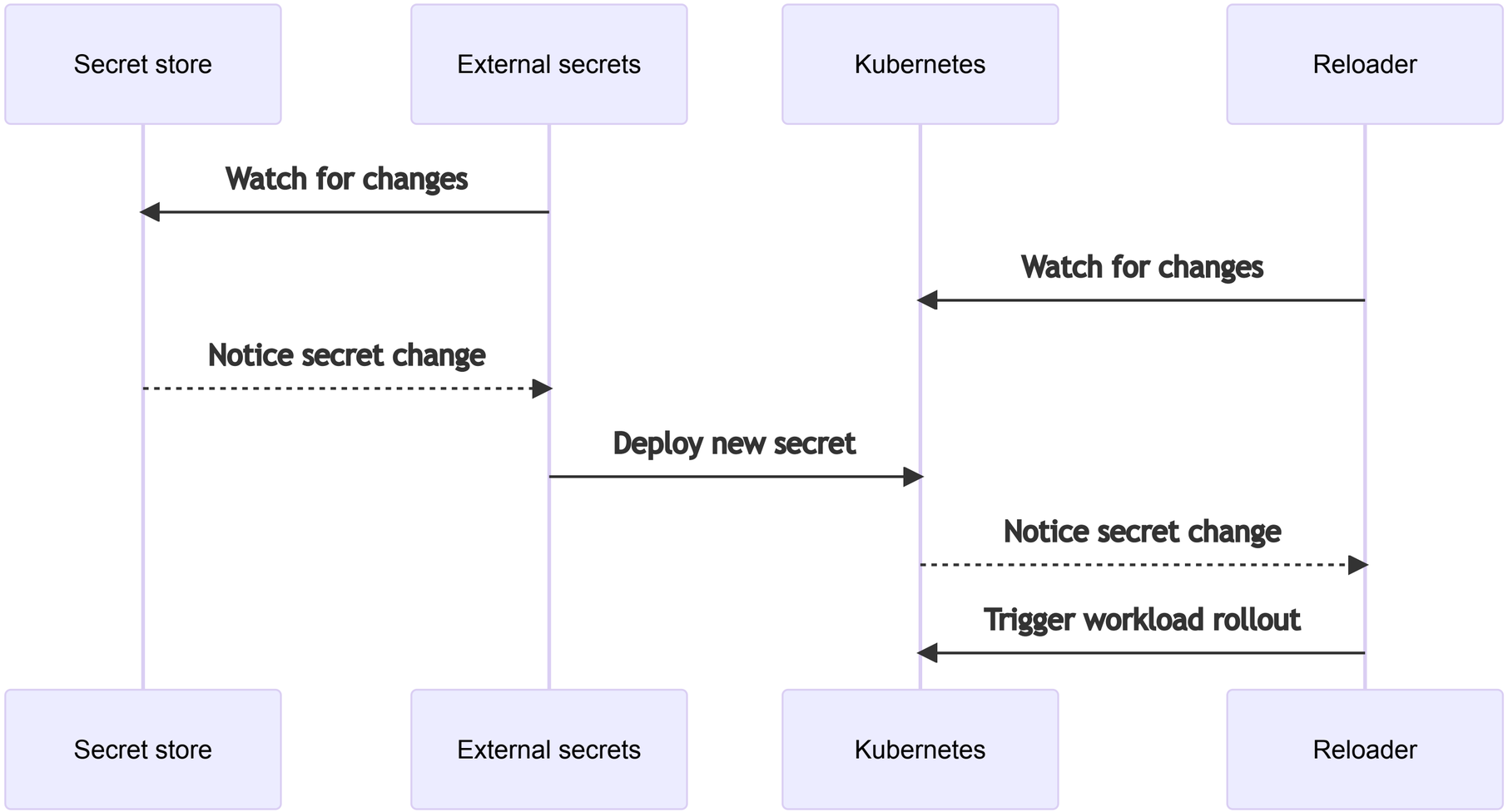
- External Secrets: https://external-secrets.io
- Synchronize secrets from an external store to Kubernetes secrets
- Mount secrets as usual (env var, file)

> **Important**
>
> **Turn on envelope encryption!!!**


SECRET CHANGED
NOW WHAT?

Triggering workload rollout

- Reloader: https://github.com/stakater/Reloader
- Detects secret changes
- Triggers rollout for workloads referencing changed secrets


Secret store
External secrets
Kubernetes
Reloader
Watch for changes
Watch for changes
Notice secret change
Deploy new secret
Notice secret change
Trigger workload rollout
Secret store
External secrets
Kubernetes
Reloader

Demo

https://github.com/sagikazarmark/demo-fosdem23-kube-secret-rotation

Thank you

Any questions?

@sagikazarmark

https://sagikazarmark.hu