KubeCon | CloudNativeCon

Europe 2023

Can You Keep A Secret?

Gal Cohen, Liav Yona

Firefly

Gal Cohen

Software Engineer, Firefly

Liav Yona

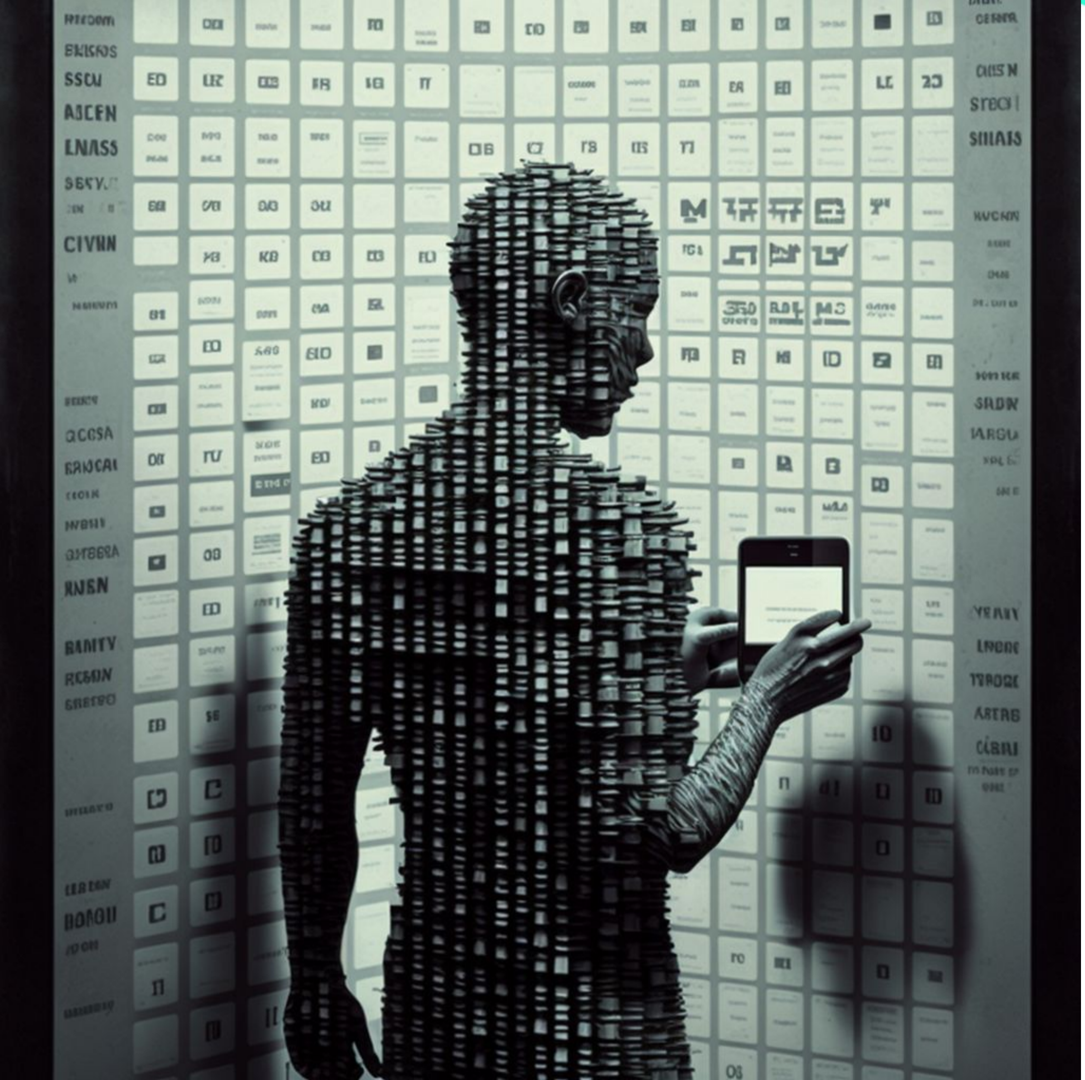
Engineering Team Lead, Firefly

Firefly

K8s secret

What are secrets?

An object that contains sensitive data such as an access key, token, or a password.



Firefly

Applications depend on secrets

However,

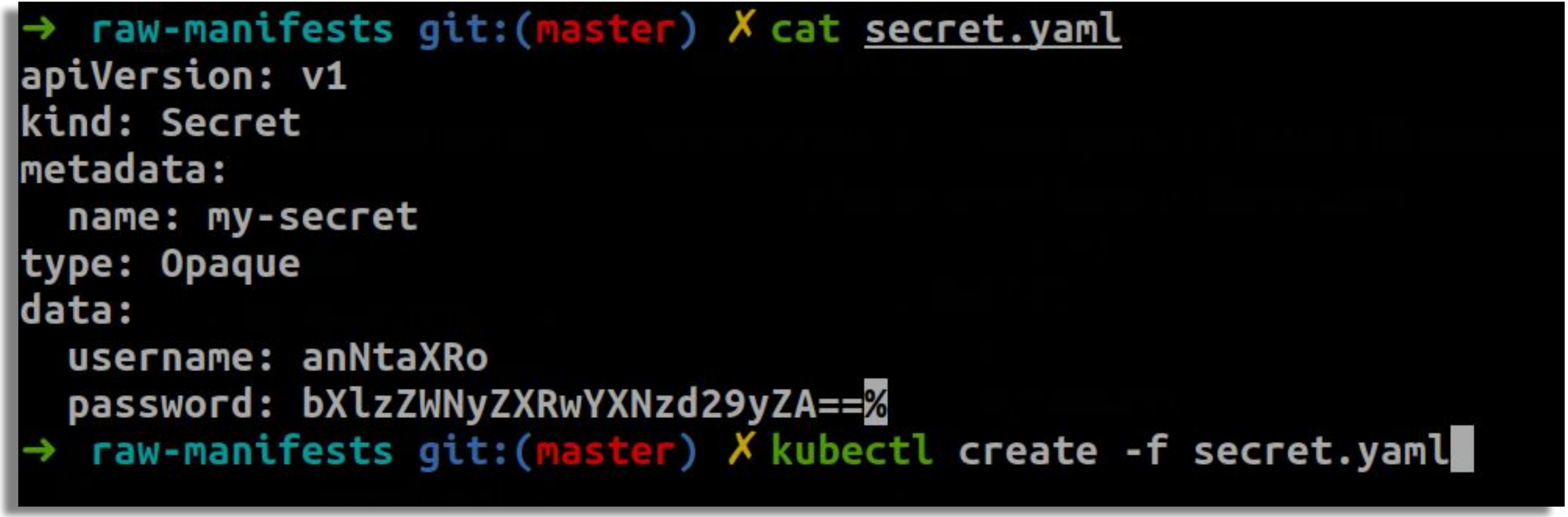
due to security reasons, we can’t store the secrets in our version control system

We have to retrieve them from somewhere else.

Secrets in Kubernetes

Our Kubernetes Application integrates with a Kubernetes Secret using two common ways:

- Data Volumes
- Environment Variables



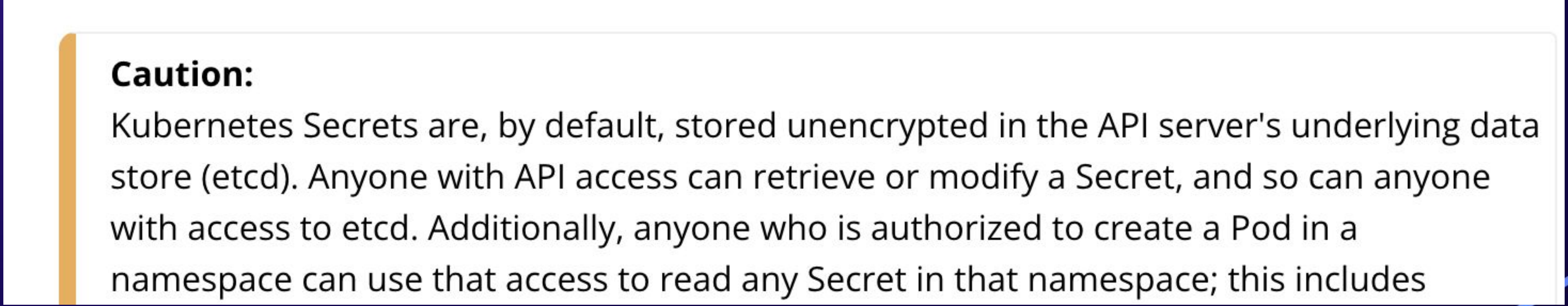
```
→ raw-manifests git:(master) ✗ cat secret.yaml
apiVersion: v1
kind: Secret
metadata:
  name: my-secret
type: Opaque
data:
  username: anNtaXRo
  password: bXlzZWNyZXRwYXNzd29yZA==%
→ raw-manifests git:(master) ✗ kubectl create -f secret.yaml
```

Manage secrets with IaC

Like every other resource and according to the best practice, we would like to manage it with Infrastructure-as-Code.

We can do it easily with any IaC tool like:

- Helm
- Terraform
- Pulumi
- etc..



Caution:
Kubernetes Secrets are, by default, stored unencrypted in the API server's underlying data store (etcd). Anyone with API access can retrieve or modify a Secret, and so can anyone with access to etcd. Additionally, anyone who is authorized to create a Pod in a namespace can use that access to read any Secret in that namespace; this includes

Source: https://kubernetes.io/docs/concepts/configuration/secret/

Firefly

K8S secrets challenges

Unencrypted

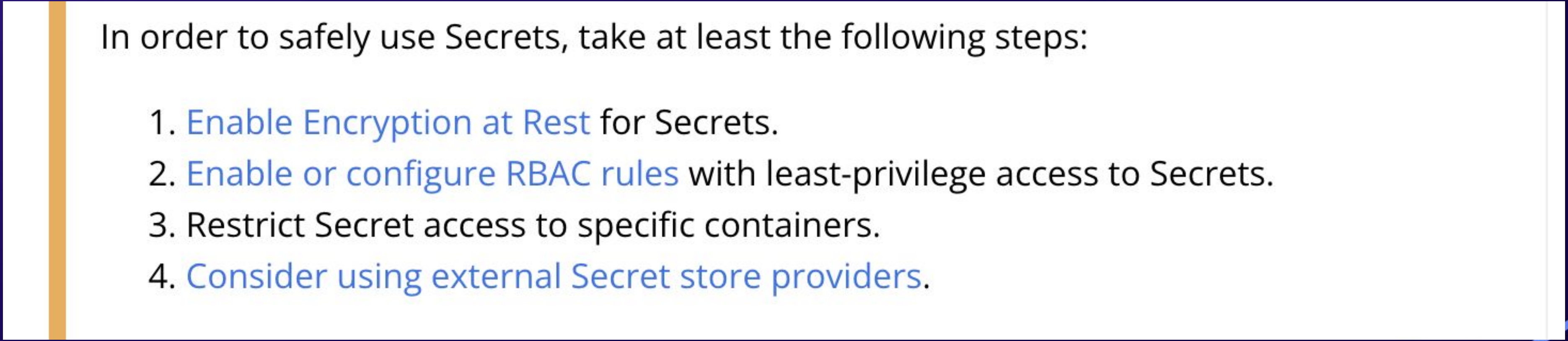
Limited RBAC

Secret Rotation

Scale

No Audit

So How can we safely use secrets?



In order to safely use Secrets, take at least the following steps:

1. Enable Encryption at Rest for Secrets.
2. Enable or configure RBAC rules with least-privilege access to Secrets.
3. Restrict Secret access to specific containers.
4. Consider using external Secret store providers.

Source: https://kubernetes.io/docs/concepts/configuration/secret/

Secrets store providers at the market

- HashiCorp Vault
- AWS Secrets Manager
- Azure key vault
- Google Cloud secret manager
- And etc..

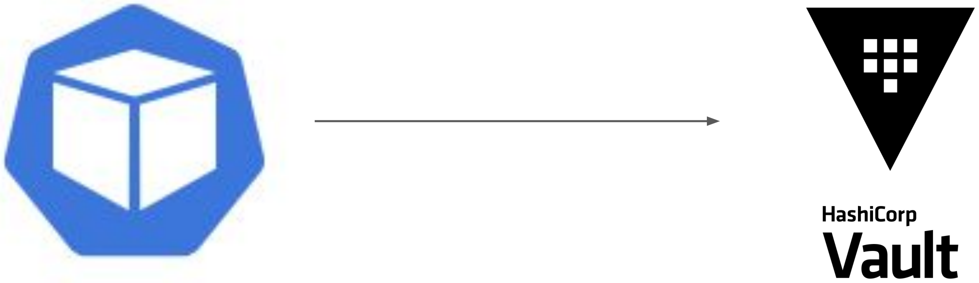
Why do we need external Secrets Store provider?

Single Source of Truth

Secured

Shared

Least Privilege

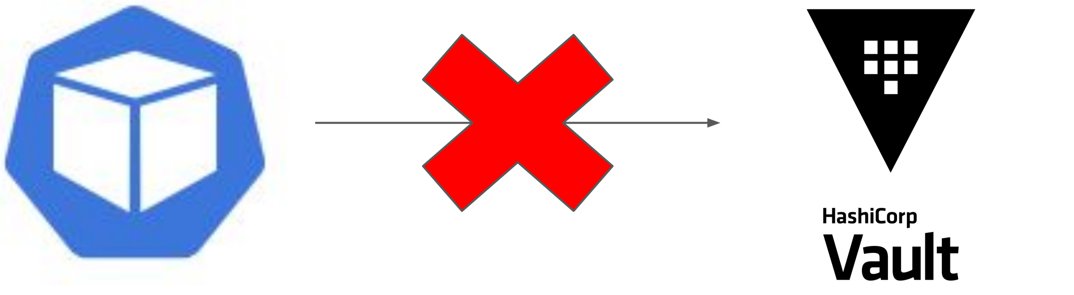


application

Secret store provider

"Applications need only concern themselves with finding a secret at a filesystem path, rather than managing tokens, connecting to an external API, or other mechanisms for direct interaction with Vault."

https://www.hashicorp.com/



application

Secret store provider

Why not just read secrets from a secret store provider ?

- Require code adjustments to call the secret manager API/SDK
- Vendor locked-in.
- Programmatic access to the External Secret Store Provider.

CSI - what is it?

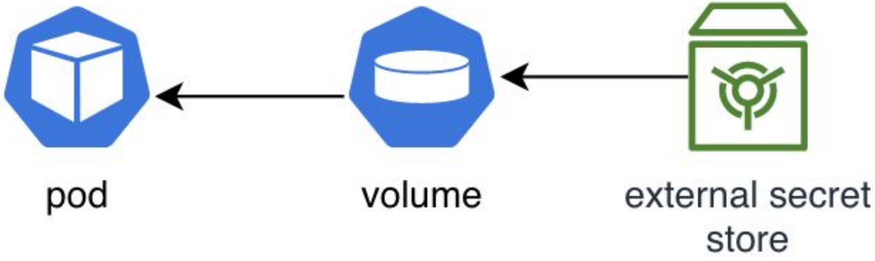
CSI - Container Storage Interface.

Secrets CSI - what is it?

Secrets Store CSI Driver for Kubernetes secrets, integrates secrets stores with Kubernetes via CSI.

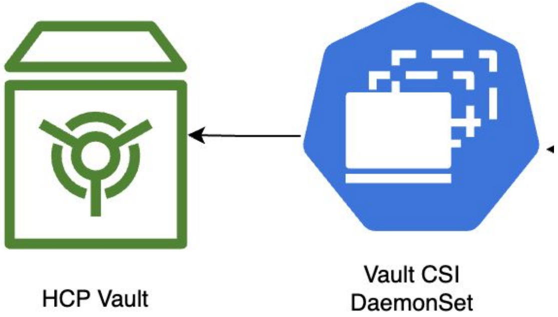
Secrets CSI - How it works?

The CSI Driver allows Kubernetes to mount multiple secrets that stored in external secrets managers into their pods as a volume.

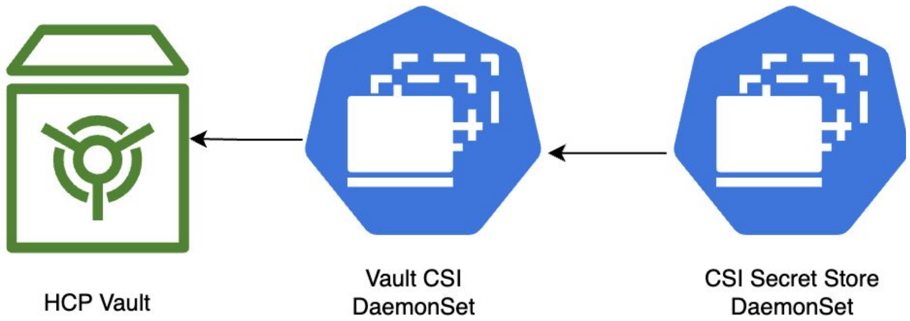


Secret CSI Architecture

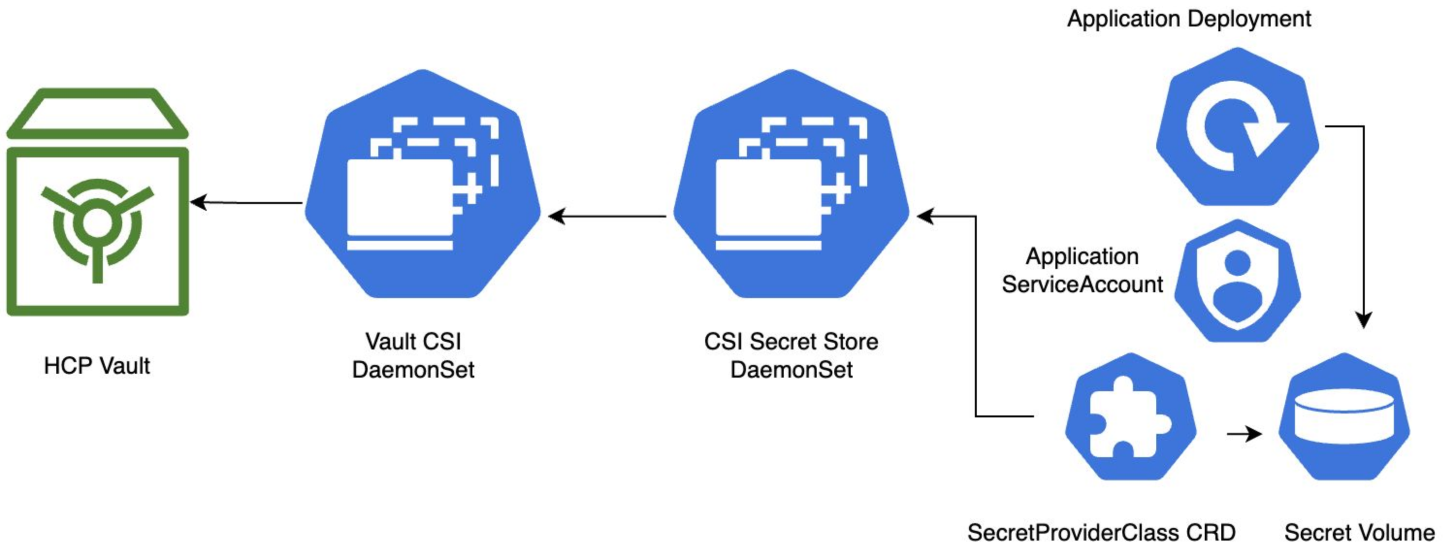
Secret CSI Architecture



Secret CSI Architecture



Secret CSI Architecture



Firefly

Secret CSI Demo

Pain points using secret store CSI

Complexity

Pain points using secret store CSI

Complexity

Performance Overhead

Pain points using secret store CSI

Complexity

Performance Overhead

Auto-Reload

Wrap up

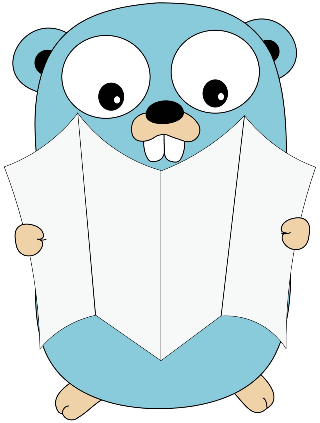
Our applications today need to interface and communicate with many different services, and many times authenticate to these.

Secret store CSI driver is common solution to easily use secrets in a secured way.

Questions?

Useful links

- https://gofirefly.io - Mange cloud complexity using Infrastructure-as-Code at scale.
- https://aiac.dev - Artificial intelligence Infrastructure-as-Code open source generator
- https://www.validiac.com - Open source tool that helps to ensure Infrastructure-as-Code best practices, hygiene and security
- https://www.linkedin.com/company/gofireflyio
- https://www.linkedin.com/in/liavyona
- https://www.linkedin.com/in/galco5/



Firefly

Thank you!