

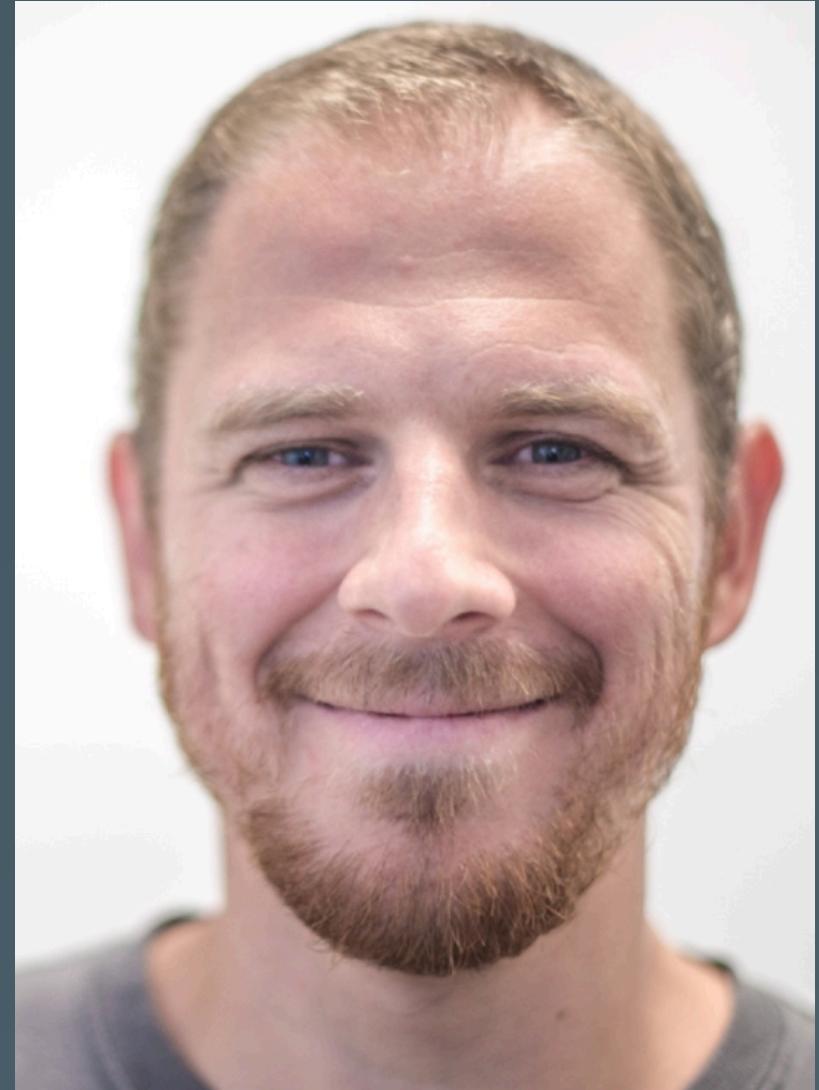
Automatic Secret rotation with ESO

Gergely Brautigam

<https://github.com/Skarlso>

<https://gergelybrautigam.com>

<https://github.com/external-secrets>



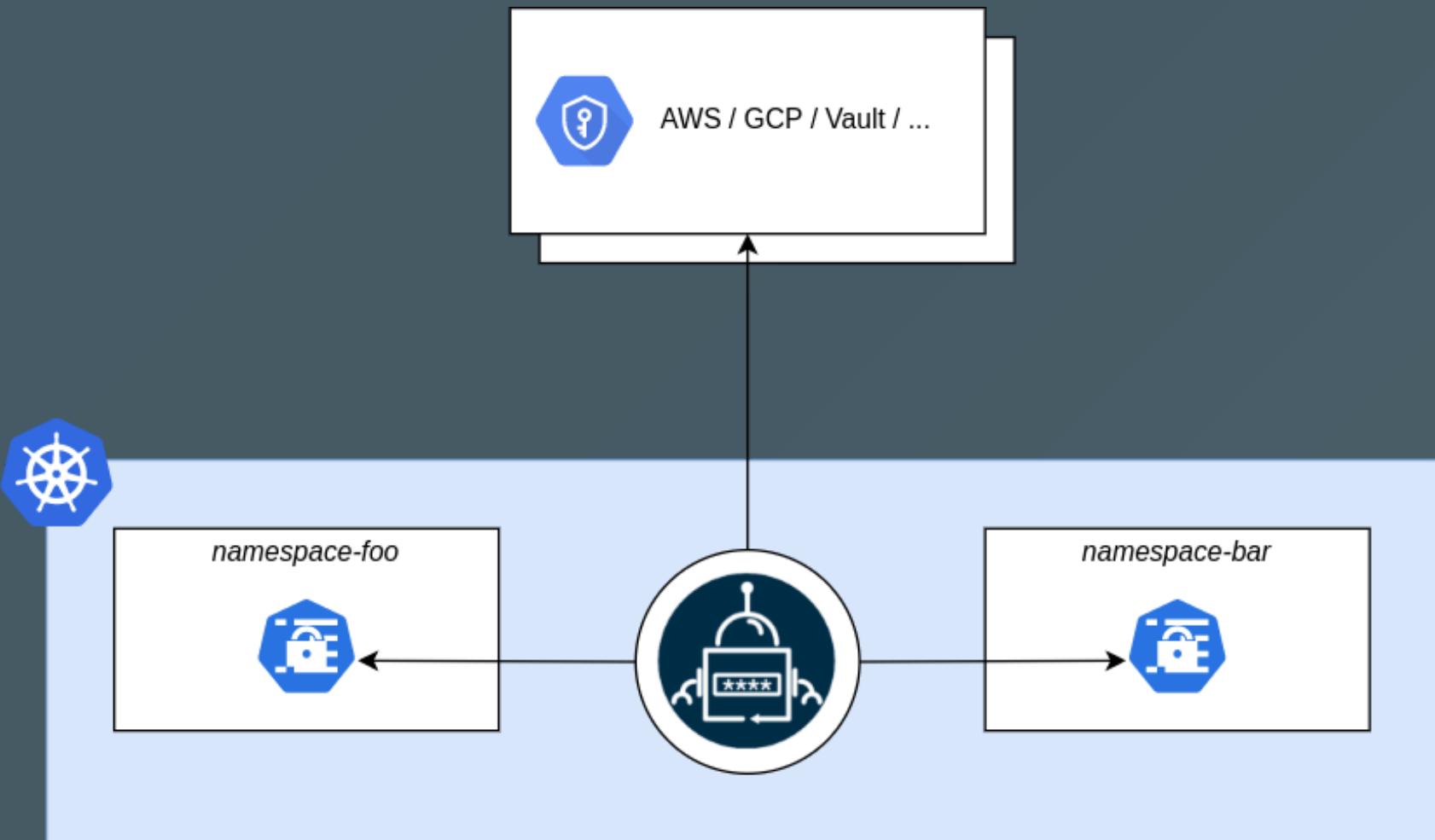
Agenda

- External Secrets intro
- Rotation
- ESO Reloader
- Demo
- Caveats
 - Downtime
 - Race conditions
- Closing words

What is External Secrets Operator



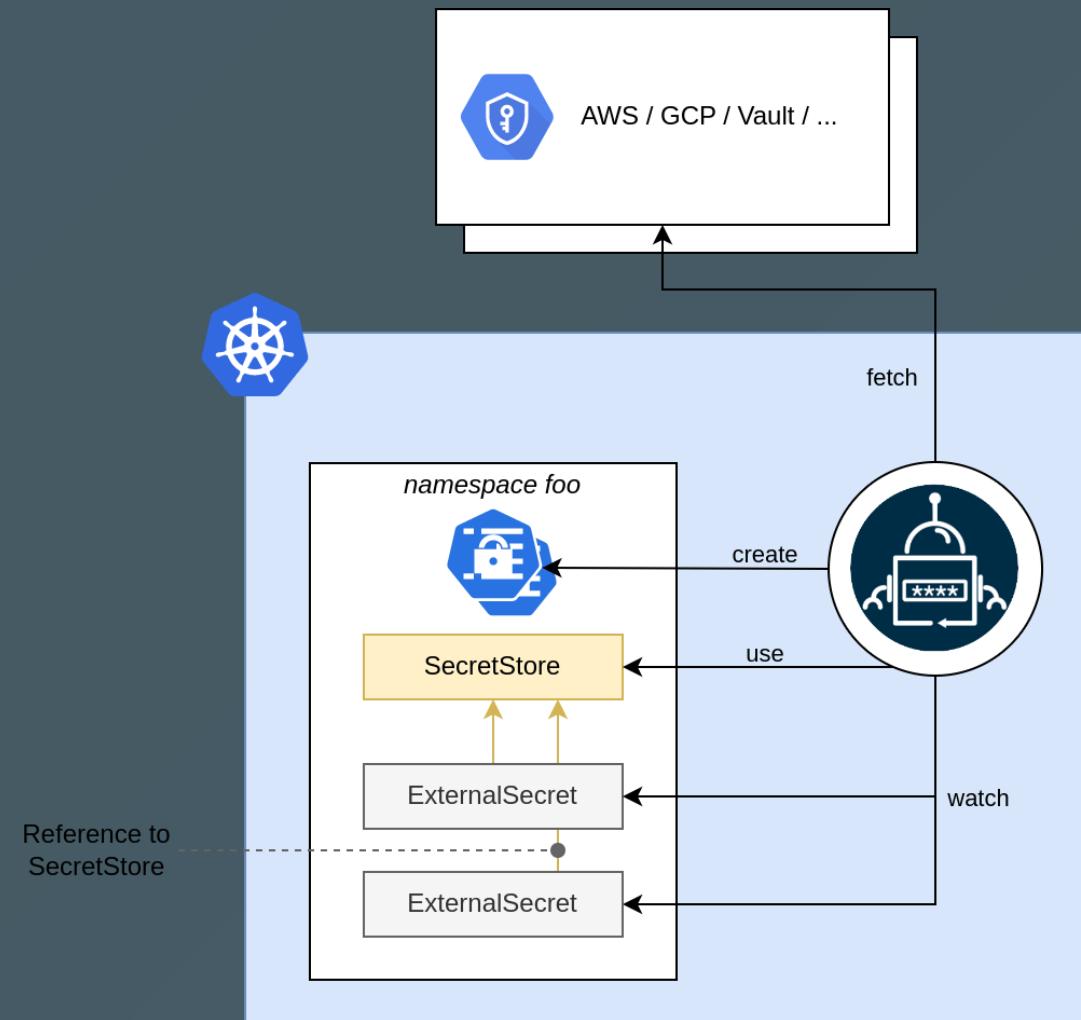
Architecture



Providers

- AWS
 - GCP
 - Vault
 - Kubernetes
- ...

SecretStore architecture



SecretStore

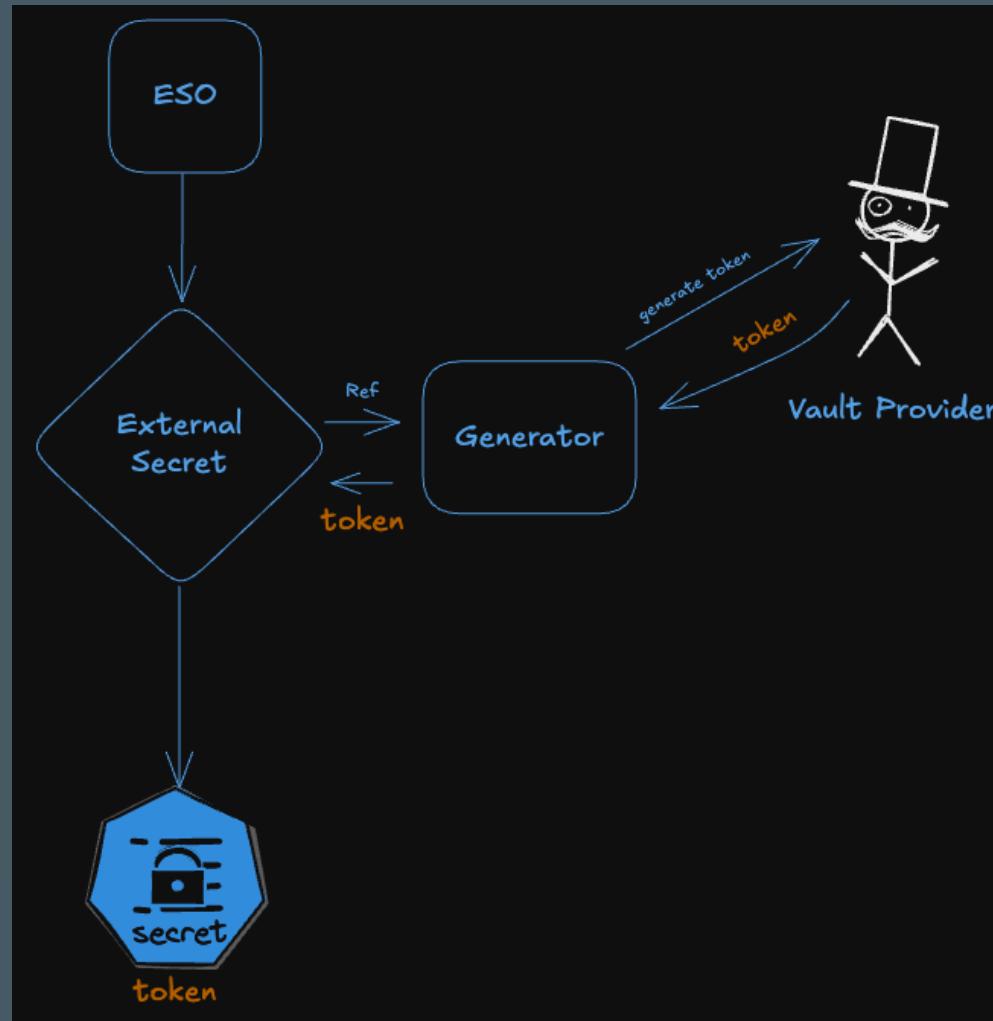
```
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: example
  namespace: example-ns
spec:
  controller: dev
  retrySettings:
    maxRetries: 5
    retryInterval: "10s"
provider:

  # (1): AWS Secrets Manager
  aws: ...
  # (2) Hashicorp Vault
  vault: ...
  # (3): GCP Secret Manager
  gcpsm: ...
```

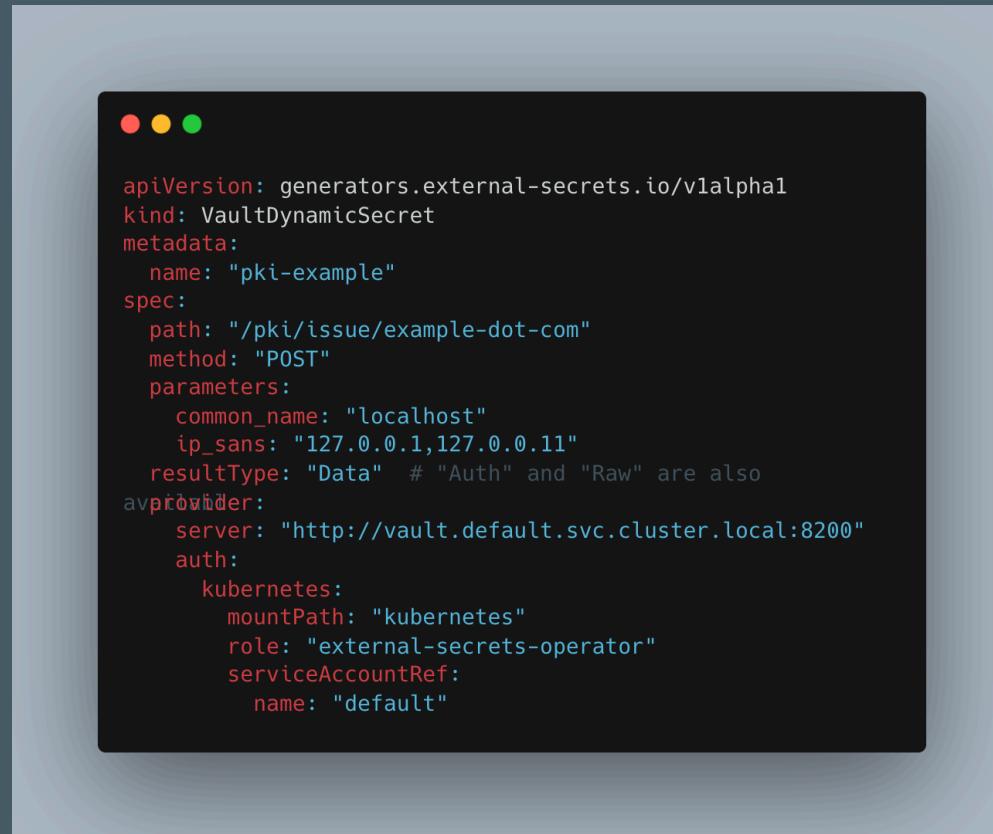
ExternalSecret

```
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "hello-world"
spec:
  secretStoreRef:
    name: aws-store
    kind: SecretStore # or ClusterSecretStore
  refreshPolicy: Periodic
  refreshInterval: "1h"
  target:
    # The secret name of the resource
    # Defaults to .metadata.name of the ExternalSecret
    # It is immutable
    name: application-config
    creationPolicy: Merge
    deletionPolicy: Retain
  data:
    - secretKey: username
      remoteRef:
        key: database-credentials
        version: v1
```

What are generators



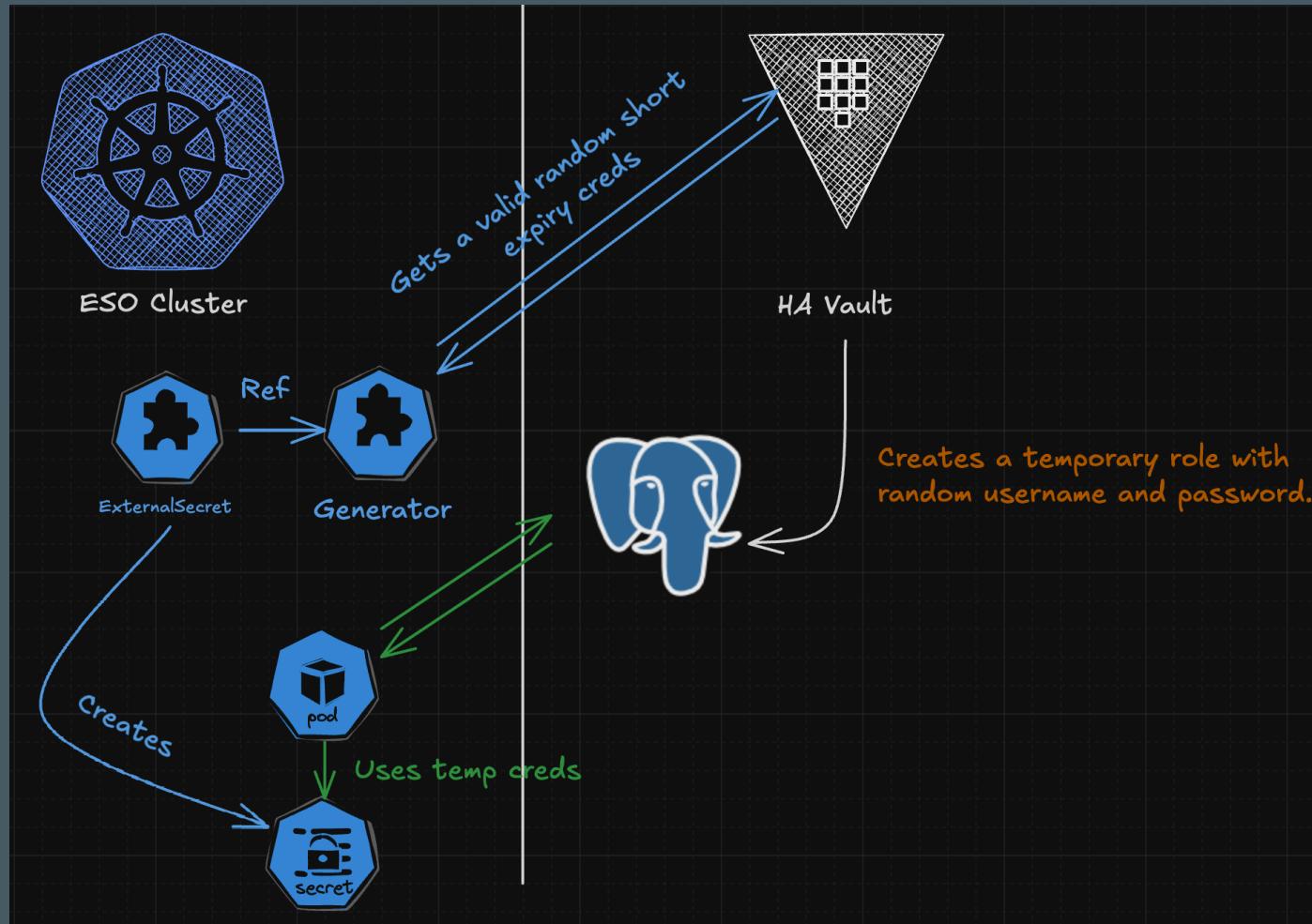
Vault Dynamic Secret Generator



Different Generator Types

- Azure Container Registry
- AWS Elastic Container Registry
- AWS STS Session Token
- Google Container Registry
- Quay
- Vault Dynamic Secret
- Password
- Webhook (*any* type)
- Github
- UUID

What we are trying to achieve



Demo

Conclusion

Thank you for listening!

Gergely.

@Skarlso