


Protecting Your Crown Jewels

with External Secrets Operator



Lucas Severo Alves

Software Engineer at  **Red Hat**

github.com/knelasevero




Moritz Johner

Senior Software Engineer at **FORM3**

github.com/moolen



Gustavo Fernandes de Carvalho

Software Engineer at  **Container Solutions**

github.com/gusfcarvalho



Idan Adar

SRE Team Lead at **IBM**

github.com/IdanAdar



Sebastián Gómez

Software Engineer at  **UBISOFT**

github.com/sebagomez

Agenda

- What is Secrets Management?
- External Secrets Operator

What is Secrets Management

...and why should you care?

What attributes do credentials have?

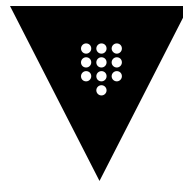
- **Expiry:** eternal vs. ephemeral
- **Creation:** manual vs. automatic
- **Dependency:** external vs. internal vs. none
- **Consumer:** user vs. application

Where do we need Secrets?

- Development Laptops
 - CLIs
 - UI Logins
- CI/CD
 - terraform / ansible / ...
 - deploy keys
 - container registry
- Operational Environment
 - Infrastructure
 - Applications
 - Cloud and on-prem

Centralise and Win 🏆

- Secure Storage
- Auditing
- Authentication & Authorization
- Secret Rotation APIs & Integration



Challenges



Secret Sprawl



Lifecycle Management: rotation & access control



Integration & Tooling



Bad Practices



Secrets Management with External Secrets Operator

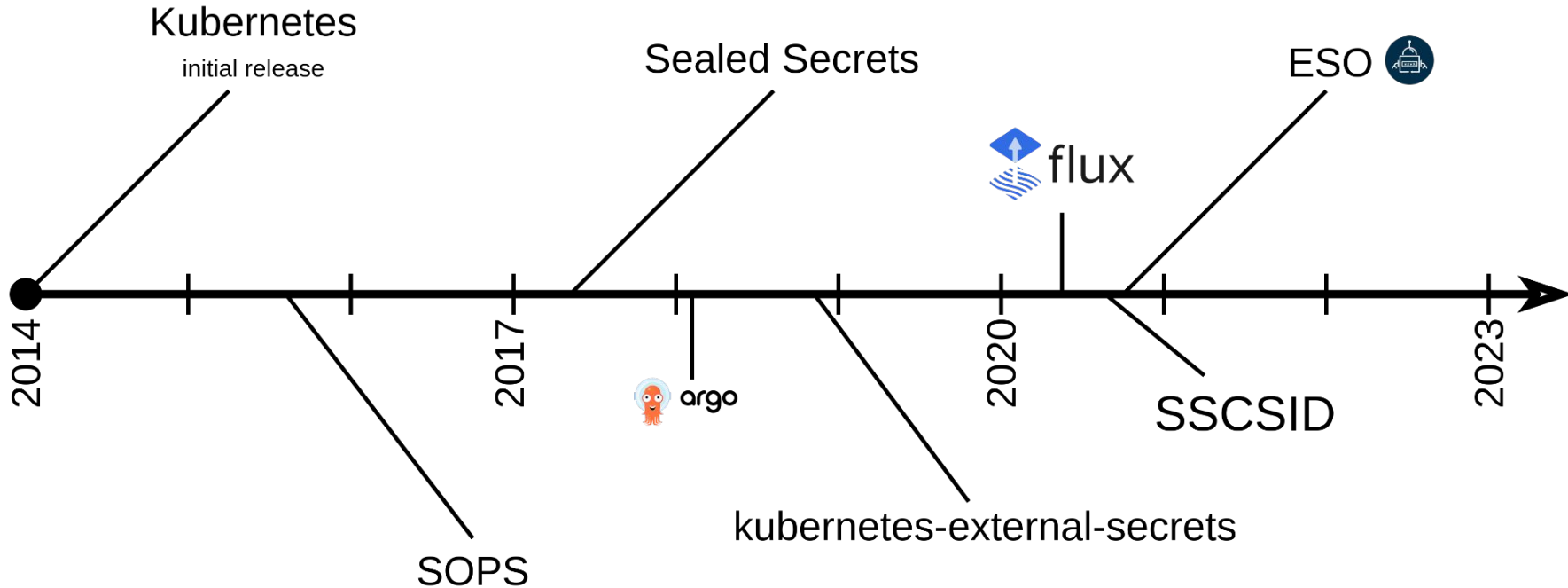


History Time

- Successor of **godaddy/kubernetes-external-secrets**
- Joint Venture of multiple projects, see [#47](#)
- initial commit November 2020
- ~2100 commits / >200 contributors

github.com/external-secrets/external-secrets

external-secrets.io

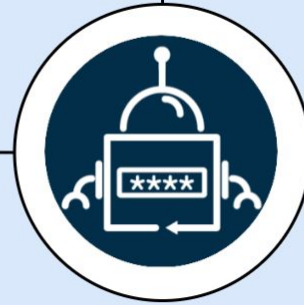


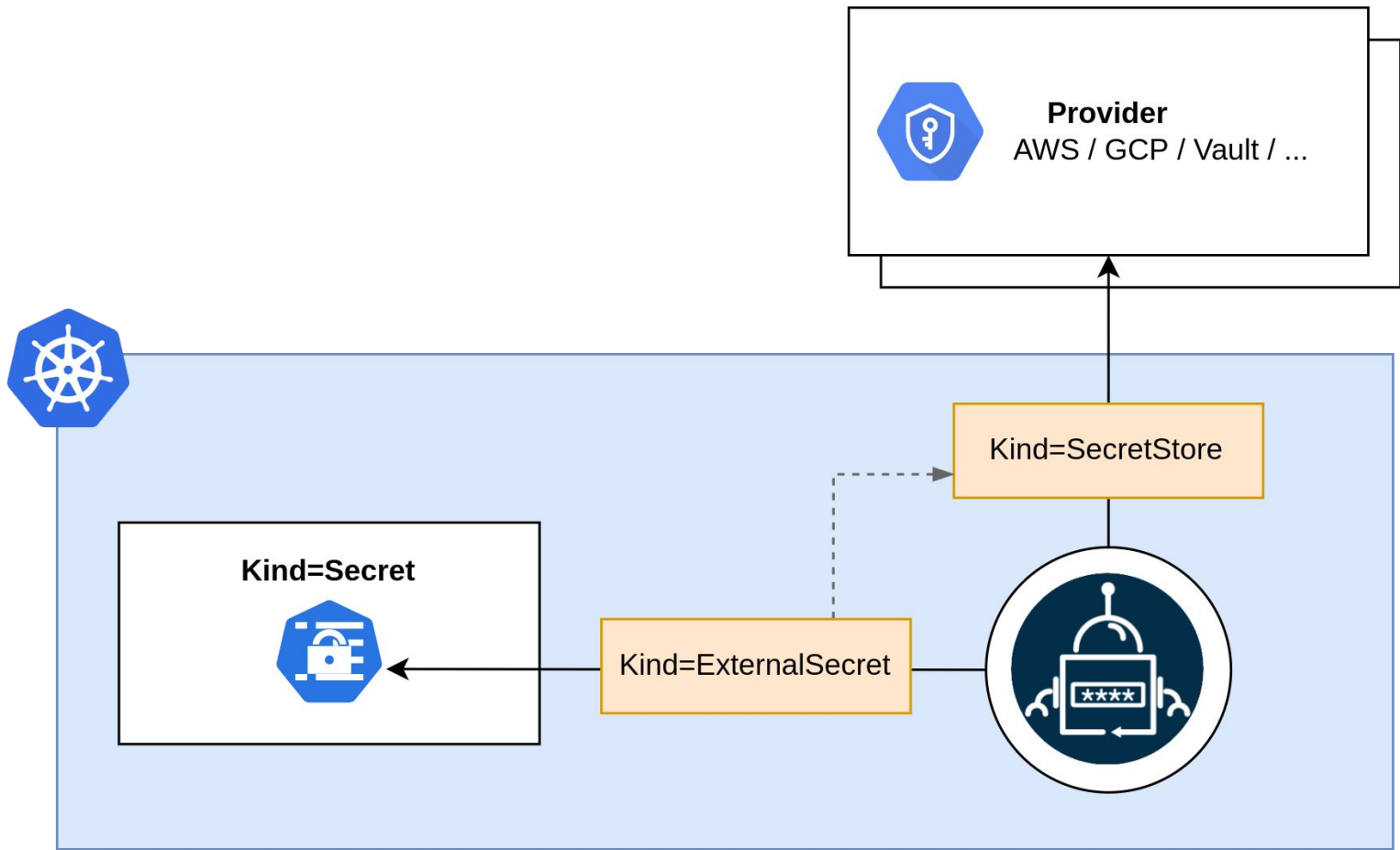


Kind=Secret




Provider
AWS / GCP / Vault / ...



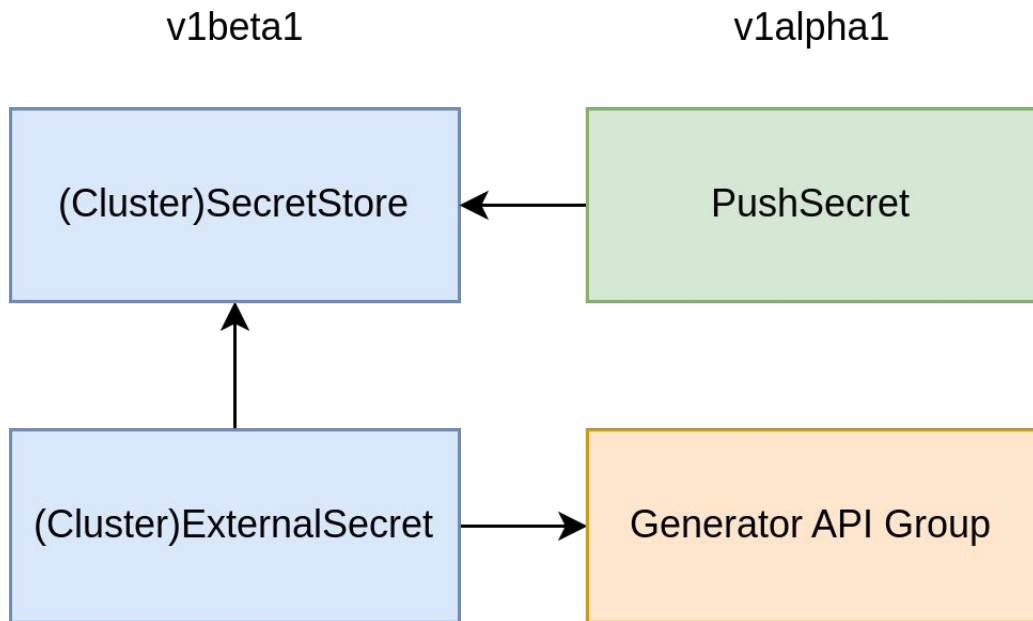


```
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "hello-world"
spec:
  secretStoreRef:
    name: "secret-store-name"
  refreshInterval: "1h"
  target:
    name: "my-api-key"
  data:
    - secretKey: "API_KEY"
      remoteRef:
        key: "/applications/foo/apikey"
```

A horizontal line connects the 'name: "secret-store-name"' field in the 'secretStoreRef' section of the left YAML to the 'name: "secret-store-name"' field in the 'spec' section of the right YAML.

```
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: "secret-store-name"
spec:
  provider:
    aws:
      service: SecretsManager
      region: "eu-central-1"
      auth:
        jwt:
          serviceAccountRef:
            name: "my-serviceaccount"
```

API Surface



Features

- 🔒 zero-configuration authentication: IRSA & Workload Identity
- ↺ lifecycle management: rotation, creationPolicy & deletionPolicy
- 📀 secret distribution across namespaces
- ♻️ cross-cluster synchronization
- 🎨 secret templating
- 🐶 fetch & aggregate multiple secrets
- ⛏️ extract secrets from structured data
- 👤 designed for multi-tenancy purposes


```
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "grafana-config"
spec:
  # ...
  target:
    template:
      data:
        config: |
          datasources:
            - name: Graphite
              type: graphite
              access: proxy
              url: http://localhost:8080
              password: "{{ .password }}"
              user: "{{ .user }}"
    data:
      - secretKey: "user"
        remoteRef:
          key: "/applications/foo/user"
      - secretKey: "password"
        remoteRef:
          key: "/applications/foo/password"
```

define template

define data

Vault Contents

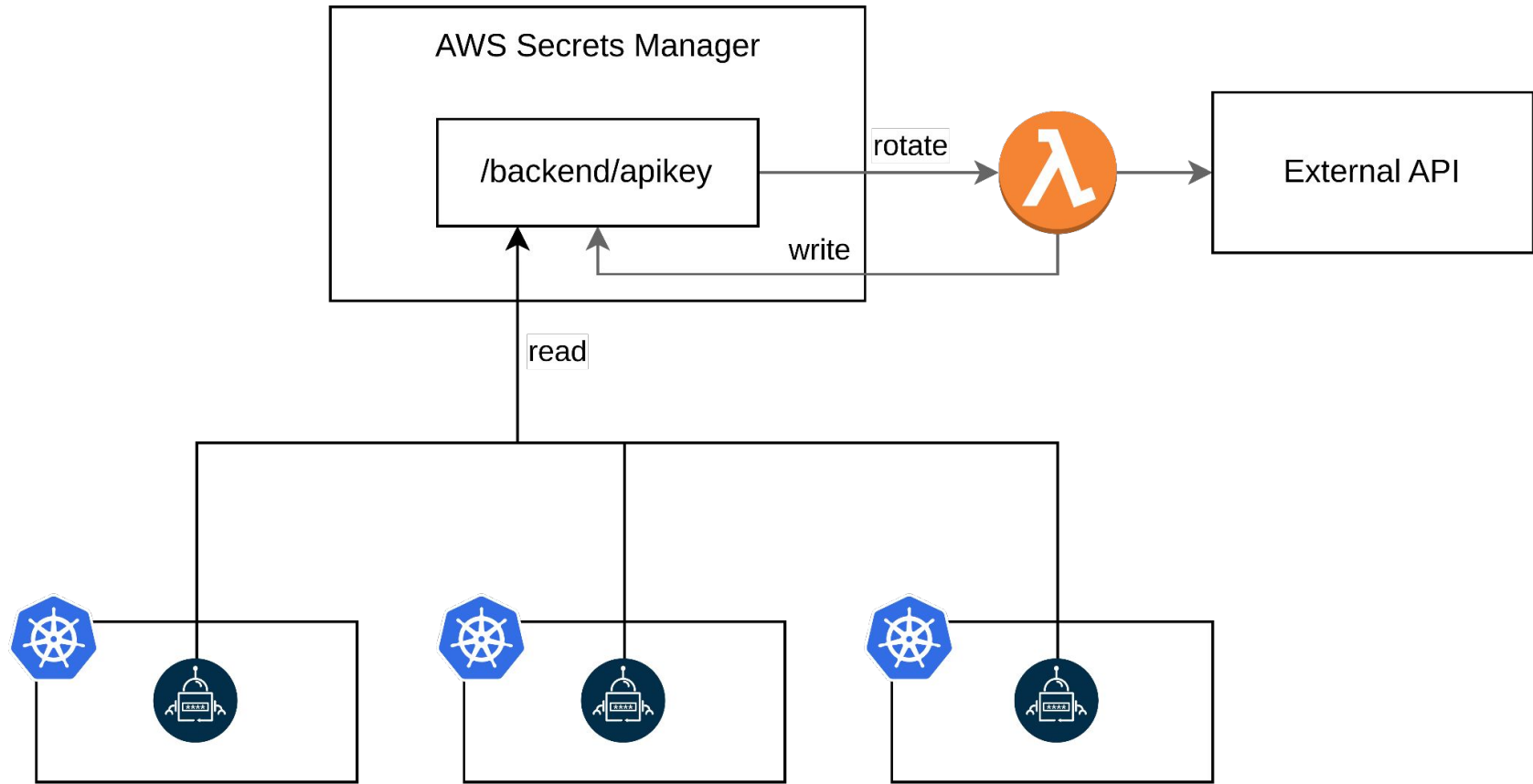
key	value
<i>backend/database/creds</i>	foo:6ZbvugPdhUB9aj5TnPNctQqrF2mVzI
<i>backend/cache/creds</i>	foo:SMZkv1Ht6hSdz7Bddz5vG15qYXsHjB
<i>backend/tls/key</i>	-----BEGIN PRIVATE KEY----- ...
<i>backend/tls/cert</i>	-----BEGIN CERTIFICATE----- ...
...	

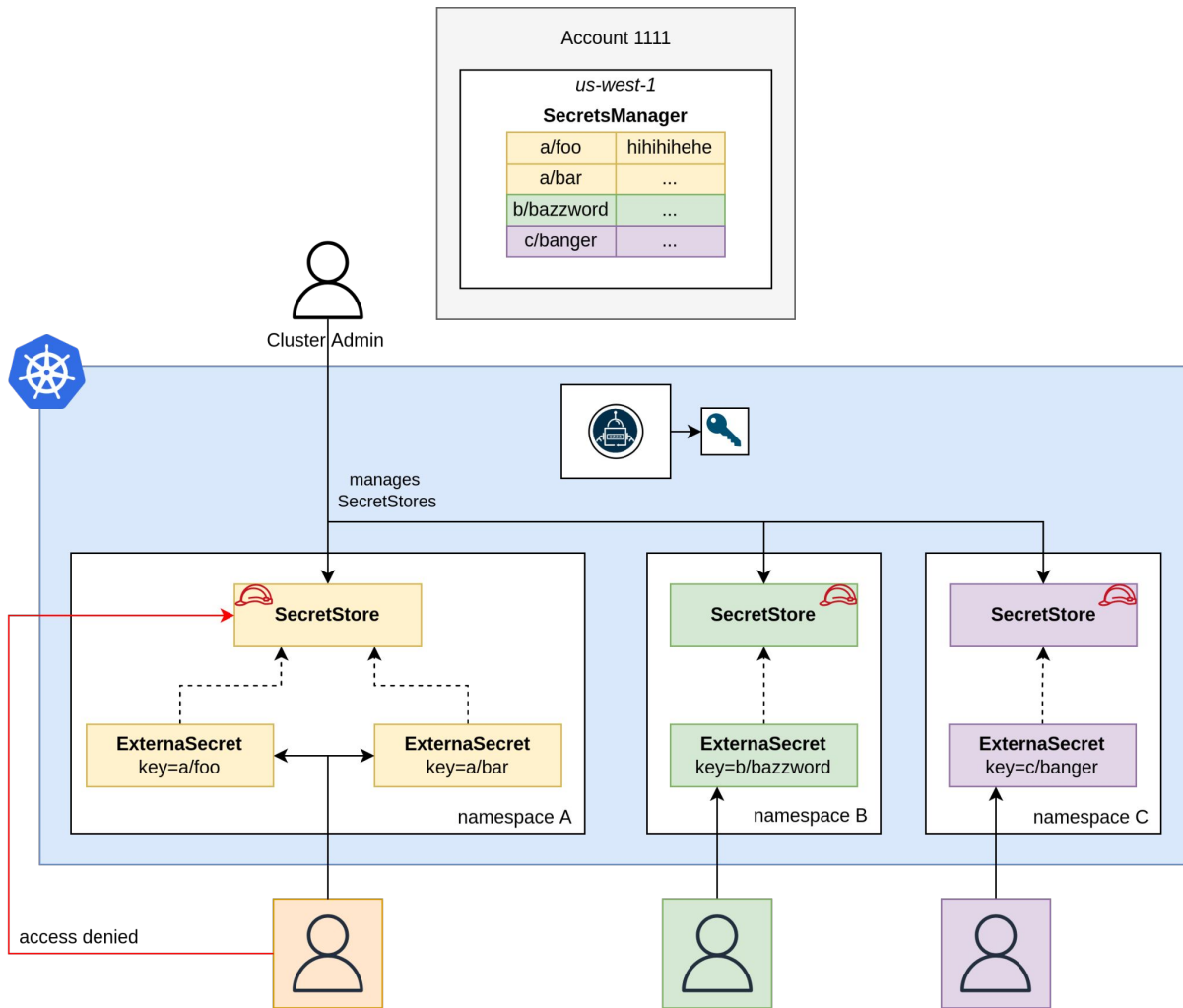
```
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: "database-creds"
spec:
  dataFrom:
    - find:
        name:
          regexp: "^backend\/.+ $"
```

Vault Contents

key	value
<i>/database/creds</i>	<pre>{ "MYSQL_USER": "foo", "MYSQL_PASS": "1234", "MYSQL_HOST": "example.com", "MYSQL_PORT": "3306" }</pre>

```
apiVersion: external-secrets.io/v1beta1  
kind: ExternalSecret  
metadata:  
  name: "database-creds"  
spec:  
  dataFrom:  
    - extract:  
      key: "/database/creds"
```





Lookout

- GA in 2023 🙌
- contributors & maintainers wanted ;)

Reach out

CNCF Project Pavilion in Hall 5

Kubernetes slack **#external-secrets**

<https://external-secrets.io/>

github.com/external-secrets/external-secrets



Thanks!