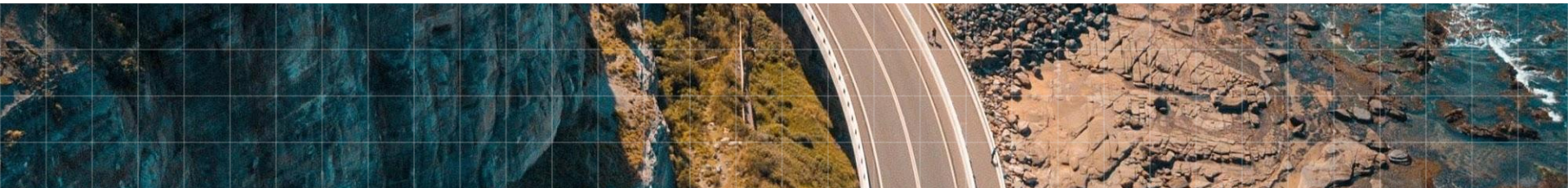


Secret Manager

External Secrets





Hanna Sträng
Platform Engineer

**No secret manager?!
What do we do if all of our secrets
disappears?!**

What we were looking for when choosing a secret manager

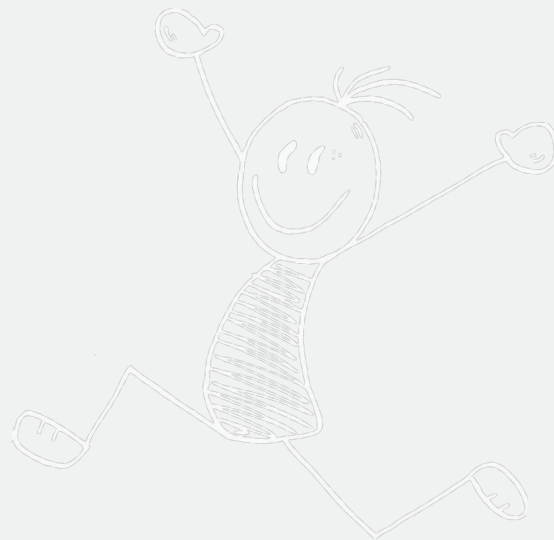
- Easy to restore secrets
- Google Cloud Platform
- Work with Kubernetes
- The teams are themselves responsible for the secrets
- ArgoCD and GitOps
- Already existing secrets running in k8s to migrate



Why External Secrets?

We got what we were looking for, and more

- Easy to restore secrets ✓
- Google Cloud Platform ✓
- Work with Kubernetes ✓
- The teams are themselves responsible for the secrets ✓
- ArgoCD and GitOps ✓
- Already existing secrets running in k8s to migrate ✓
- Create secrets both via terminal or console ✓
- Track the secrets in git without exposing the secret value ✓
- External secrets handles what version is the latest of the secrets ✓



Okay...

**But what does it mean, and how do we
use it at Annotell?**

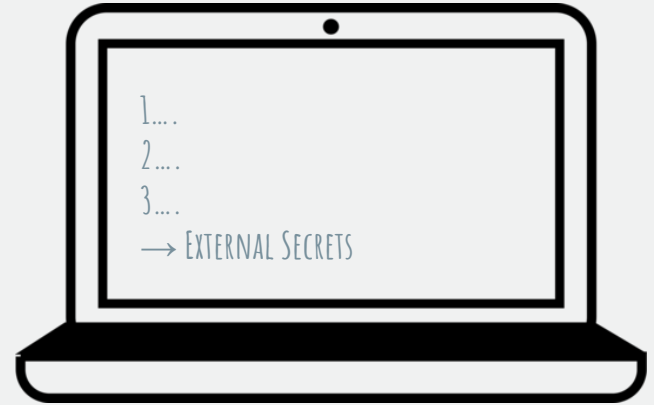
To start

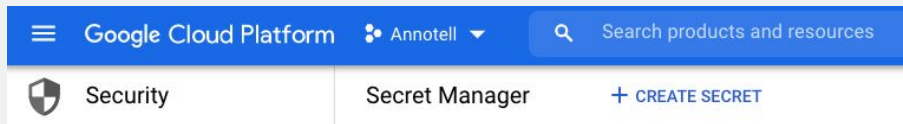
You need to set up...

A custom resource definition for external secrets objects

And

A deployment

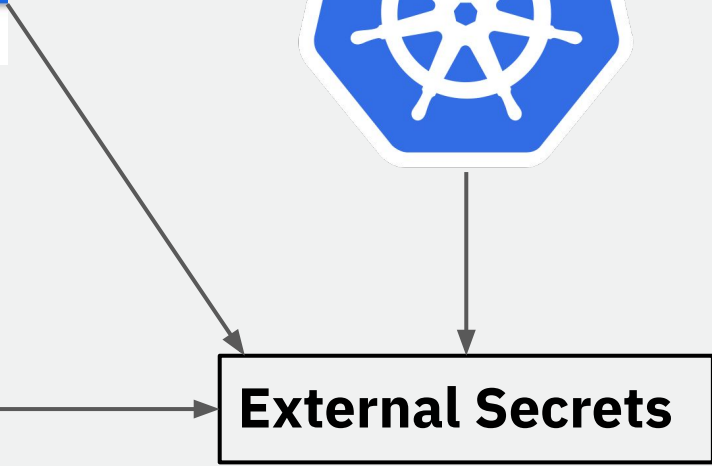




Example deployment yaml

```
1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    namespace: <NAMESPACE>
5    name: example-deployment
6  spec:
7    ...
8    env:
```

External Secrets



How To Create Secrets Before

```
→ ~ kubectl create secret generic secret-example --from-literal=username=hello --from-literal=password=world
```

```
1  apiVersion: v1
2  kind: Secret
3  metadata:
4    name: secret-example
5    namespace: dev
6  data:
7    username: d29ybGQ=
8    password: aGVsbG8=
9  type: Opaque
10
```

Today and Before

External secrets yaml

```
1  apiVersion: kubernetes-client.io/v1
2  kind: ExternalSecret
3  metadata:
4    name: <NAME-OF-SECRET>
5    namespace: <NAMESPACE>
6  spec:
7    backendType: gcpSecretsManager
8    data:
9      - key: <GCP-STORED-USERNAME>
10        name: <KUBERNETES-STORED-USERNAME>
11        version: latest
12      - key: <GCP-STORED-PASSWORD>
13        name: <KUBERNETES-STORED-PASSWORD>
14        version: latest
15
```

Created secret through terminal

```
1  apiVersion: v1
2  kind: Secret
3  metadata:
4    name: secret-example
5    namespace: dev
6  data:
7    username: d29ybGQ=
8    password: aGVsbG8=
9  type: Opaque
10
```

How To Create Secrets Today


```
→ ~ echo -n '<SECRET-VALUE>' | gcloud secrets create <GLOUD-STORED-USERNAME> --replication-policy="automatic" --data-file=
```


☰


Google Cloud Platform


Annotell Test ▼


🔍 Search products and resources


 Security


 Security Command Center


 reCAPTCHA Enterprise

 BeyondCorp Enterprise


 Identity-Aware Proxy


 Access Context Manager

 VPC Service Controls

 Binary Authorization

← Secret details

 EDIT SECRET

 DELETE

Secret: "GOOGLE-STORED-USERNAME"

OVERVIEW

VERSIONS

PERMISSIONS

Versions

[+ NEW VERSION](#)

ENABLE

DISABLE

DESTROY

<input type="checkbox"/>	Version	Status ↑	Encryption	Created on ↓	Actions
<input type="checkbox"/>	1	✓ Enabled	Google-managed	6/28/21, 4:39 PM	⋮

No versions selected

Pros and Cons

Cons:

- Partly unstructured documentation
- Still creating the secrets manually

Pros:

- Easy setup
- Works good with ArgoCD and GitOps
- Store in git
- Easy for everyone
- Migrate seamlessly

SECRETS ARE NOW RESTORABLE!

Thank You!



Search or jump to...



Pull requests

Issues

Marketplace

Explore

external-secrets / **kubernetes-external-secrets**

Watch ▾

38

Star

1.9k

Fork

285

<> Code

Issues 57

Pull requests 3

Discussions

Actions

Projects 1

Security



master ▾

2 branches

40 tags

Go to file

Add file ▾

Code ▾

About

Integrate external secret management systems with Kubernetes

kubernetes

aws

vault

hashicorp

secrets-management

aws-secrets-manager

secrets-manager

kubernetes-external-secrets



Flydiverny chore(release): 8.1.3



2e00799

9 days ago



421 commits

📁 .github	chore(deps): bump crazy-max/ghaction-docker-meta f...	9 days ago
📁 bin	fix: verify CRD is available on startup	21 days ago
📁 charts/kubernetes-externa...	chore(release): 8.1.3	9 days ago
📁 config	feat: Akeyless backend (#767)	21 days ago
📁 docs	chore(release): 8.1.3	9 days ago
📁 e2e	fix!: update crd to apiextensions.k8s.io/v1 (#681)	last month