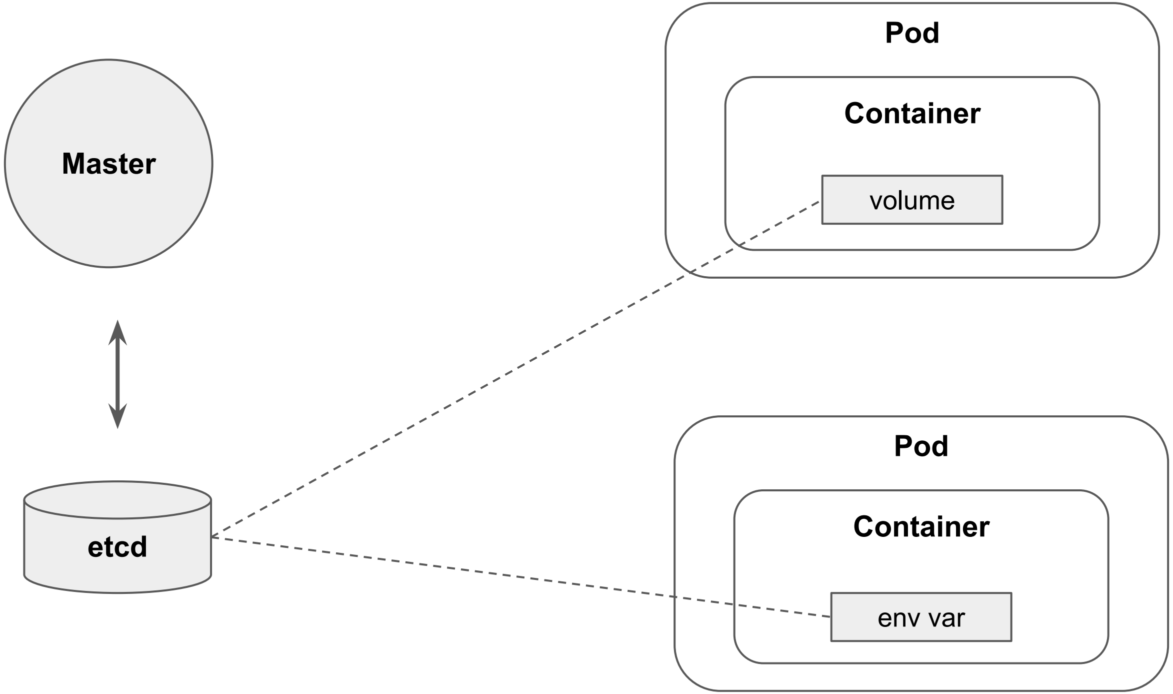
Shhh… It’s a Secret!

Ricardo Rocha

Kubernetes GitOps Workshop - April 27th 2022

https://indico.cern.ch/event/1145174


Master
etcd
Pod
Container
volume
Pod
Container
env var

What’s in a Secret

A core resource in Kubernetes

Values are base64 encoded

Multiple types: opaque, service accounts, basic-auth, tls, token, …

Available through volumes or environment variables

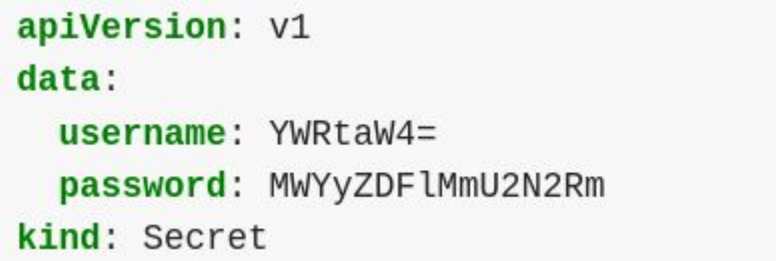
What’s in a Secret

A core resource in Kubernetes

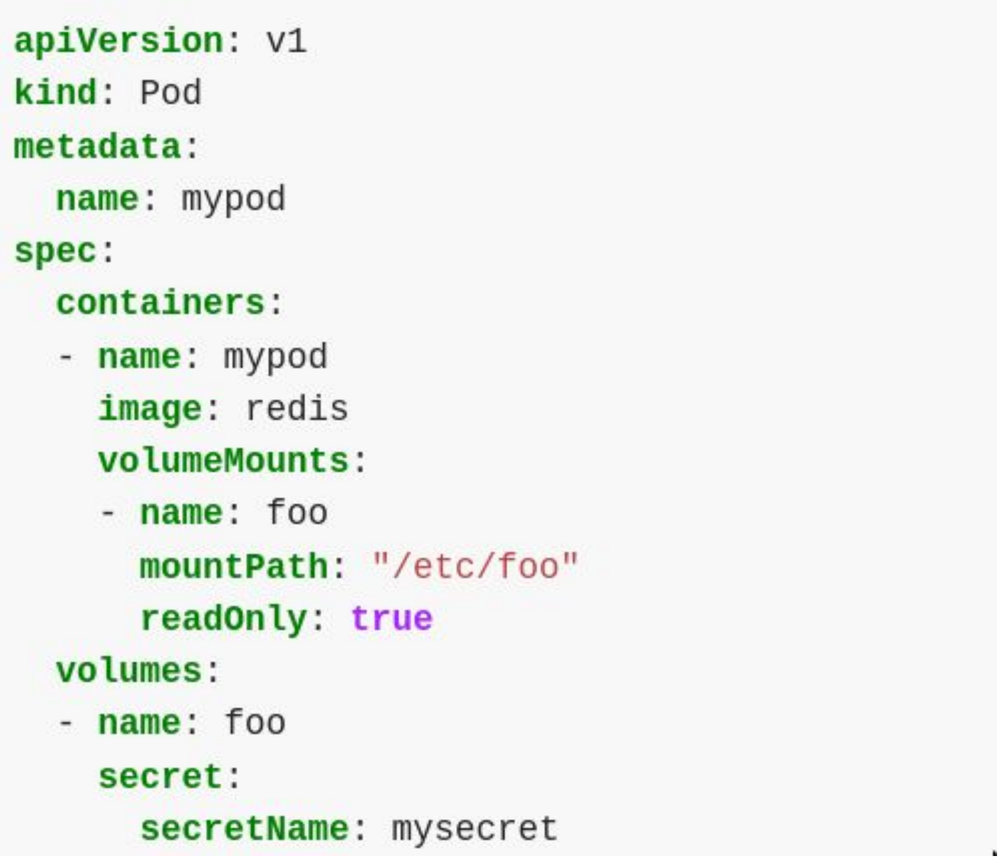
Values are base64 encoded

Multiple types: opaque, service acco

Available through volumes or enviror



```
apiVersion: v1
data:
  username: YWRtaW4=
  password: MWYyZDFlMmU2N2Rm
kind: Secret
```



```
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  containers:
  - name: mypod
    image: redis
    volumeMounts:
    - name: foo
      mountPath: "/etc/foo"
      readOnly: true
  volumes:
  - name: foo
    secret:
      secretName: mysecret
```

What’s in a Secret

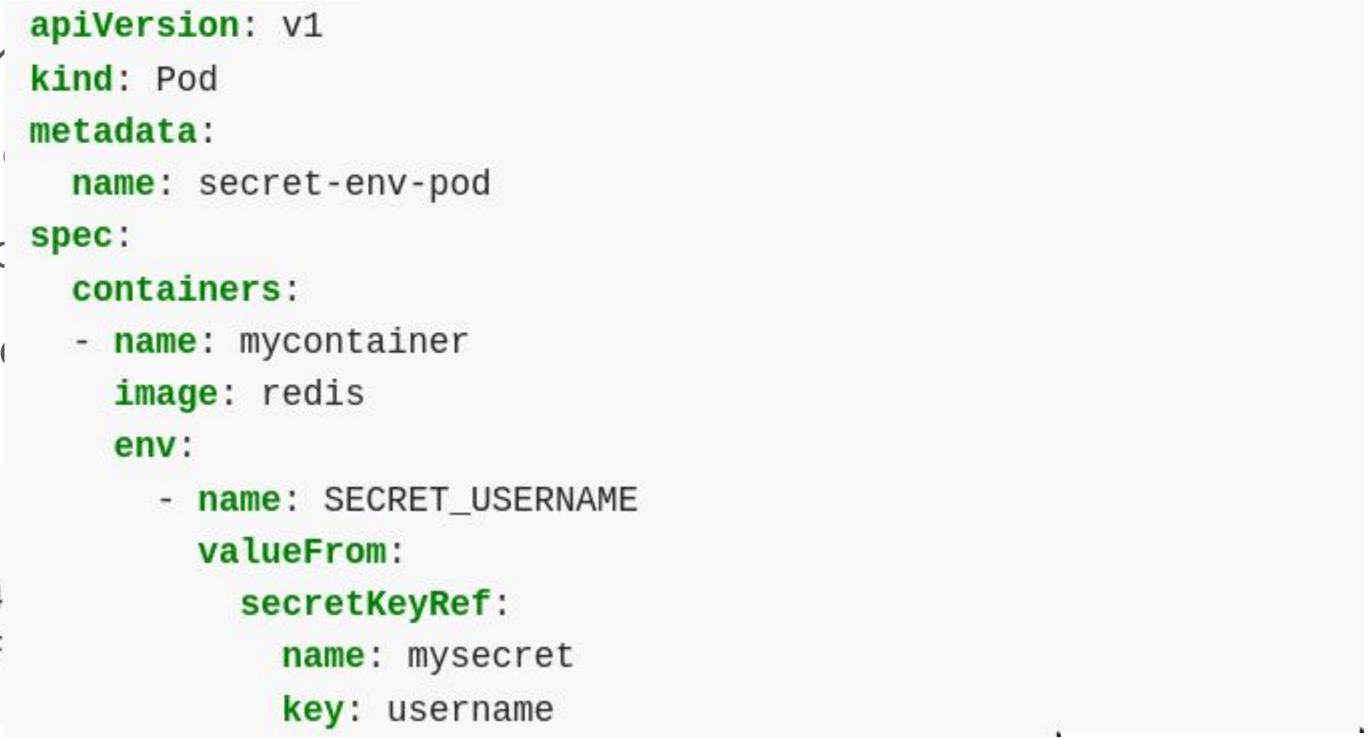
A core resource in k

Values are base64

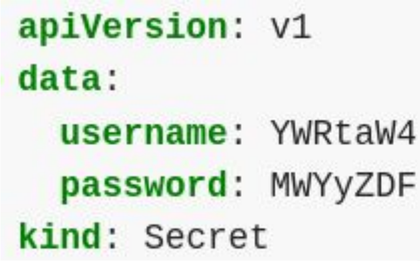
Multiple types: opac

Available through v

```
apiVersion: v1
kind: Pod
```



```
apiVersion: v1
kind: Pod
metadata:
  name: secret-env-pod
spec:
  containers:
  - name: mycontainer
    image: redis
    env:
      - name: SECRET_USERNAME
        valueFrom:
          secretKeyRef:
            name: mysecret
            key: username
```



```
apiVersion: v1
data:
  username: YWRtaW4
  password: MWYyZDF
kind: Secret
```

A word of caution…

Least kept secret…

By default stored unencrypted in etcd

By default accessible by any Pod in a namespace

A word of caution…

Least kept secret…

By default stored unencrypted in etcd - **Encryption at Rest**

By default accessible by any Pod in a namespace - **RBAC Rules**

Secrets and GitOps

It’s not (only) about the Secrets

GitOps main goal is to **version control everything**

Ideally this should also include secrets

An update of a secret, token, … should also trigger reconciliation

Options

1. **Sensitive data in Git** just like all other configuration data (but encrypted)
2. **Sensitive data in an external, secure store**. Git keeps placeholders

1. Sensitive data in Git

Requires a mechanism to encrypt and decrypt the values data

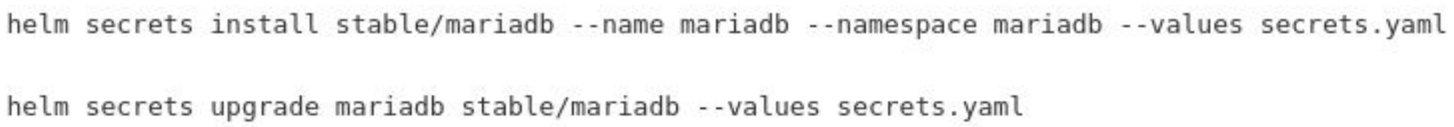
- By the user / client pushing data to the repository
- By the tool or application handling the deployment

1. Sensitive data in Git

Example: **Helm Barbican Plugin**

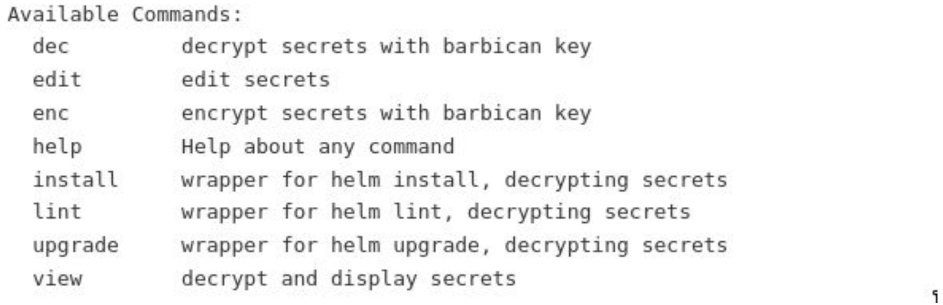
Early attempt of handling secrets at CERN for helm deployments

https://gitlab.cern.ch/helm/plugins/barbican



```
helm secrets install stable/mariadb --name mariadb --namespace mariadb --values secrets.yaml

helm secrets upgrade mariadb stable/mariadb --values secrets.yaml
```



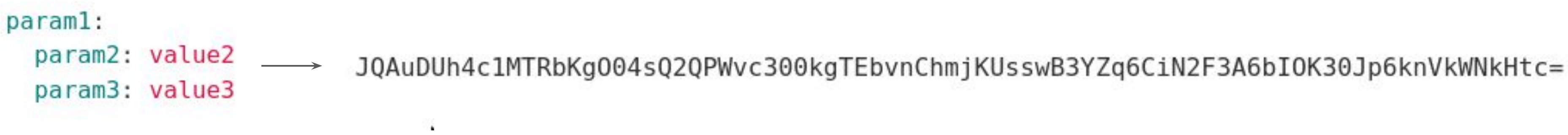
```
Available Commands:
  dec         decrypt secrets with barbican key
  edit        edit secrets
  enc         encrypt secrets with barbican key
  help        Help about any command
  install     wrapper for helm install, decrypting secrets
  lint        wrapper for helm lint, decrypting secrets
  upgrade     wrapper for helm upgrade, decrypting secrets
  view        decrypt and display secrets
```

1. Sensitive data in Git

Example: **Helm Barbican Plugin**

Early attempt of handling secrets at CERN for helm deployments

https://gitlab.cern.ch/helm/plugins/barbican



```
param1:
  param2: value2
  param3: value3
```

→

JQAuDUh4c1MTRbKgO04sQ2QPWvc300kgTEbvnChmjKUsswB3YZq6CiN2F3A6bIOK30Jp6knVkWNkHtc=

1. Sensitive data in Git

Example: **Mozilla SOPS**, supported by Flux, ArgoCD, …

Second attempt at using Barbican as a backend, with a standard tool

https://github.com/mozilla/sops

Support for PGP, age, Azure KeyVault, HC Vault, GCP KMS, AWS KMS, …

> https://github.com/mozilla/sops/pull/683 Barbican PR, Stale

1. Sensitive data in Git

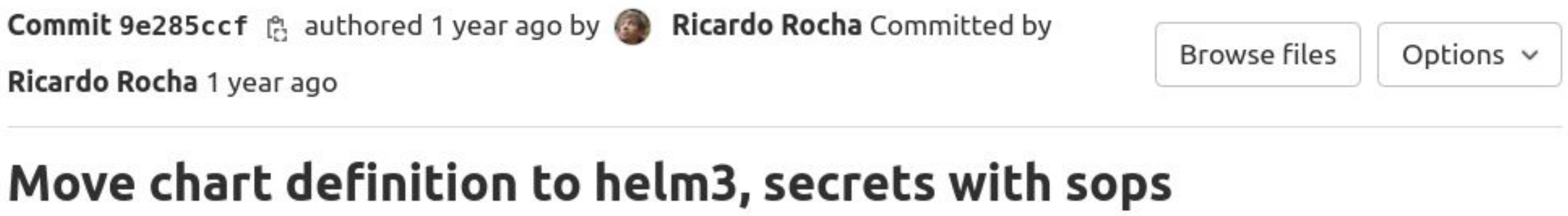
Example: **Mozilla SOPS**, supported by Flux, ArgoCD, …

Second attempt at using Barbican as a backend, with a standard tool

https://github.com/mozilla/sops

Support for PGP, age, Azure KeyVault, HC Vault, GCP KMS, AWS KMS, …

https://github.com/mozilla/sops/pull/683 Barbican PR, stale



Commit 9e285ccf authored 1 year ago by **Ricardo Rocha** Committed by **Ricardo Rocha** 1 year ago

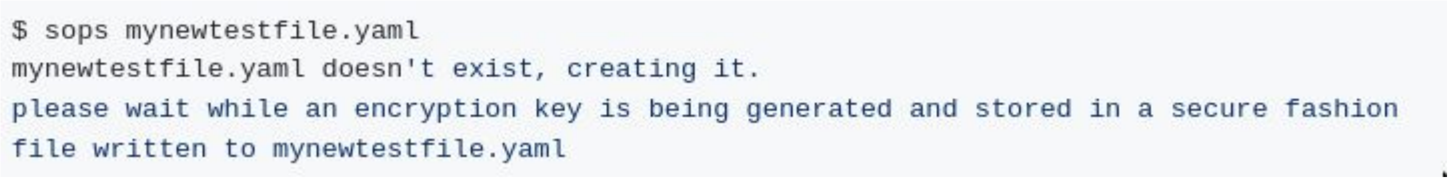
Move chart definition to helm3, secrets with sops

1. Sensitive data in Git

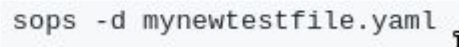
Example: **Mozilla SOPS**, supported by Flux, ArgoCD, …

Second attempt at using Barbican as a backend, with a standard tool

https://github.com/mozilla/sops



```
$ sops mynewtestfile.yaml
mynewtestfile.yaml doesn't exist, creating it.
please wait while an encryption key is being generated and stored in a secure fashion
file written to mynewtestfile.yaml
```



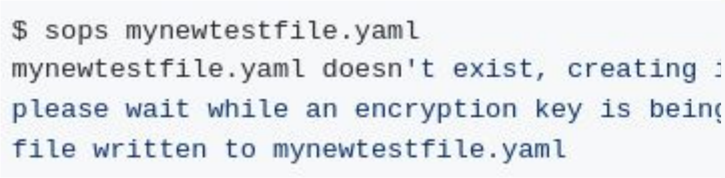
```
sops -d mynewtestfile.yaml
```

1. Sensitive data in Git

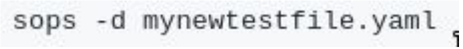
Example: **Mozilla SOPS**, supporte

Second attempt at using Barbican

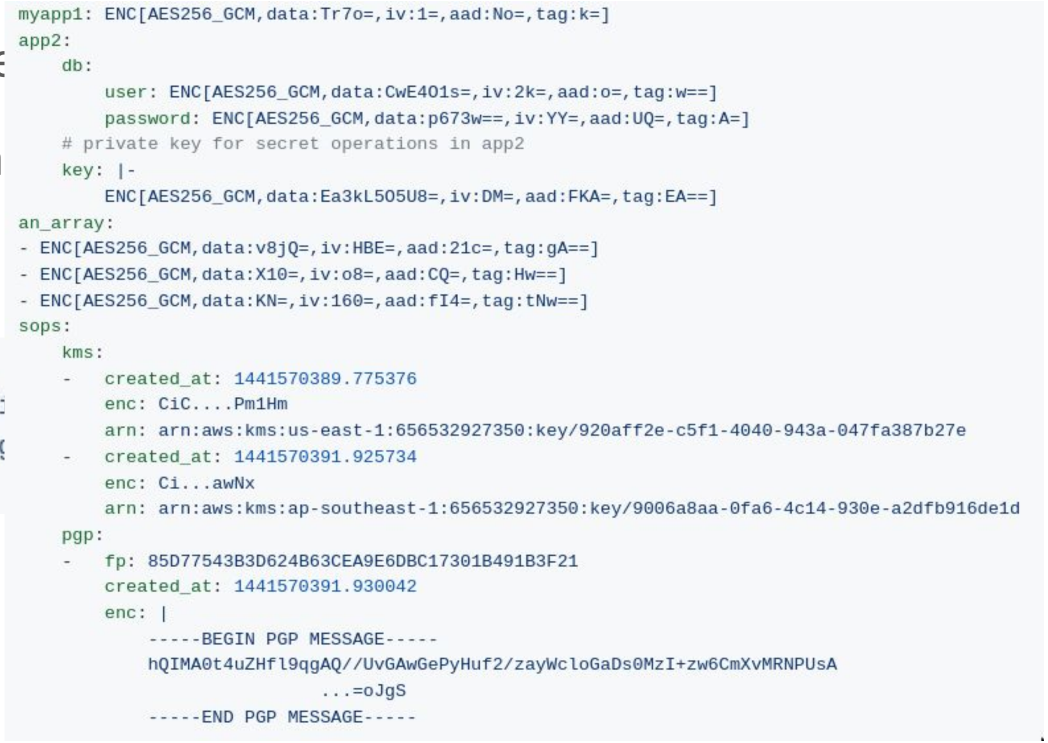
https://github.com/mozilla/sops



```
$ sops mynewtestfile.yaml
mynewtestfile.yaml doesn't exist, creating i
please wait while an encryption key is being
file written to mynewtestfile.yaml
```



```
sops -d mynewtestfile.yaml
```



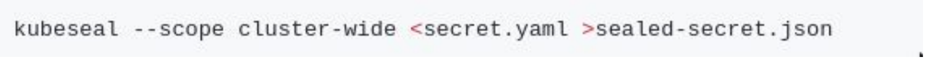
```
myapp1: ENC[AES256_GCM,data:Tr7o=,iv:1=,aad:No=,tag:k=]
app2:
    db:
        user: ENC[AES256_GCM,data:CwE4O1s=,iv:2k=,aad:o=,tag:w==]
        password: ENC[AES256_GCM,data:p673w==,iv:YY=,aad:UQ=,tag:A=]
    # private key for secret operations in app2
    key: |-
        ENC[AES256_GCM,data:Ea3kL5O5U8=,iv:DM=,aad:FKA=,tag:EA==]
an_array:
- ENC[AES256_GCM,data:v8jQ=,iv:HBE=,aad:21c=,tag:gA==]
- ENC[AES256_GCM,data:X10=,iv:o8=,aad:CQ=,tag:Hw==]
- ENC[AES256_GCM,data:KN=,iv:160=,aad:fI4=,tag:tNw==]
sops:
    kms:
    -   created_at: 1441570389.775376
        enc: CiC....Pm1Hm
        arn: arn:aws:kms:us-east-1:656532927350:key/920aff2e-c5f1-4040-943a-047fa387b27e
    -   created_at: 1441570391.925734
        enc: Ci...awNx
        arn: arn:aws:kms:ap-southeast-1:656532927350:key/9006a8aa-0fa6-4c14-930e-a2dfb916de1d
    pgp:
    -   fp: 85D77543B3D624B63CEA9E6DBC17301B491B3F21
        created_at: 1441570391.930042
        enc: |
            -----BEGIN PGP MESSAGE-----
            hQIMA0t4uZHfl9qgAQ//UvGAwGePyHuf2/zayWcloGaDs0MzI+zw6CmXvMRNPUsA
                            ...=oJgS
            -----END PGP MESSAGE-----
```

1. Sensitive data in Git

Example: **Sealed Secrets**

Custom resource, custom controller, compatibility issues

https://github.com/bitnami-labs/sealed-secrets



```
kubeseal --scope cluster-wide <secret.yaml >sealed-secret.json
```

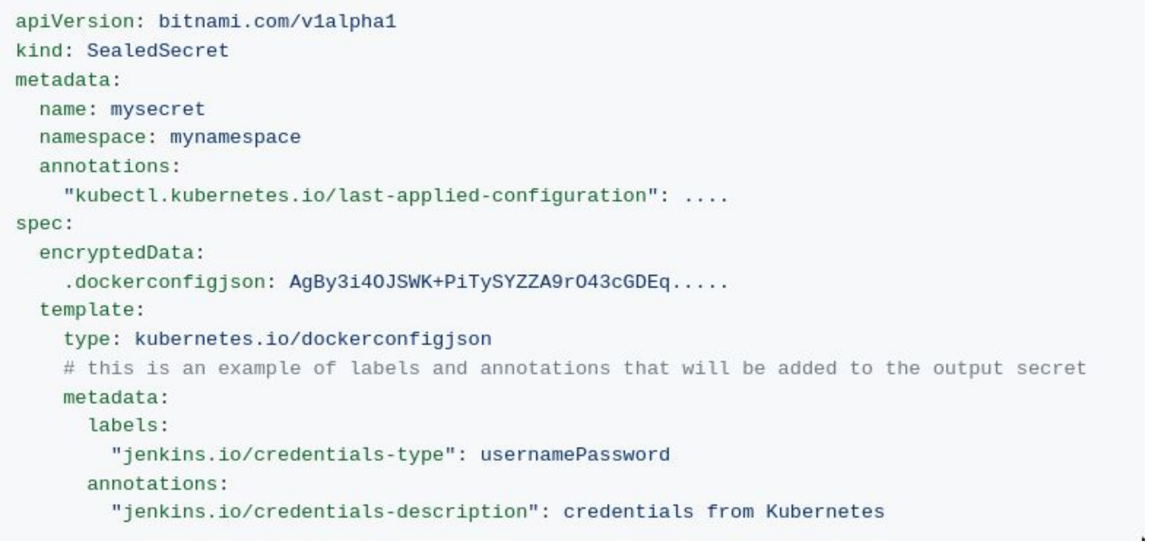
1. Sensitive data in Git

Example: **Sealed Secrets**

Custom resource, custom controller, compatibility issues

https://github.c

```
kubeseal --scope cluste
```



```yaml
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  name: mysecret
  namespace: mynamespace
  annotations:
    "kubectl.kubernetes.io/last-applied-configuration": ....
spec:
  encryptedData:
    .dockerconfigjson: AgBy3i4OJSWK+PiTySYZZA9rO43cGDEq.....
  template:
    type: kubernetes.io/dockerconfigjson
    # this is an example of labels and annotations that will be added to the output secret
    metadata:
      labels:
        "jenkins.io/credentials-type": usernamePassword
      annotations:
        "jenkins.io/credentials-description": credentials from Kubernetes
```

2. Git Placeholders, External Store

Requires a mechanism to trigger reconciliation on secret update

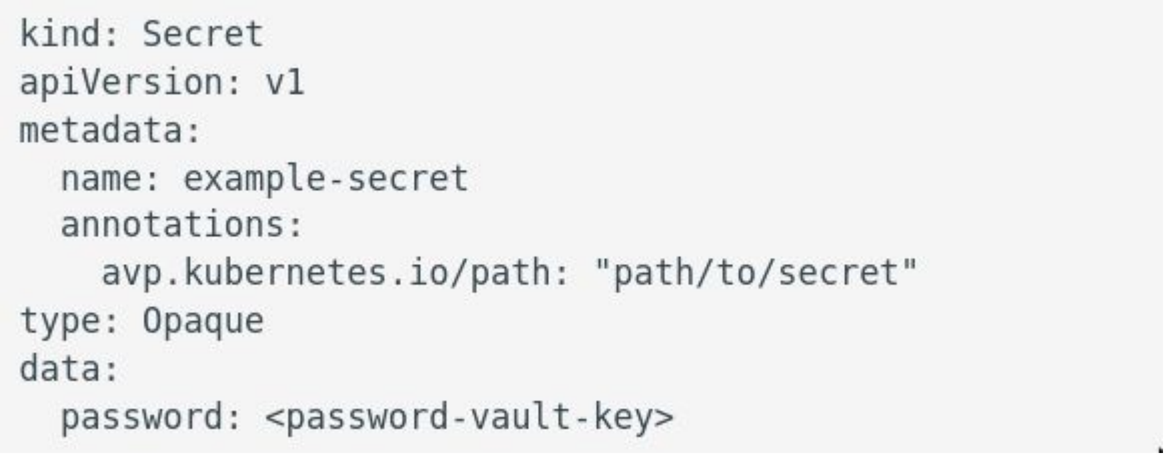
- Git hooks no longer enough
- Hook integration inexistent for some backends

2. Git Placeholders, External Store

Example: **ArgoCD Vault Plugin**

Started but not only about HC Vault: GCP KMS, Azure KeyVault, etc

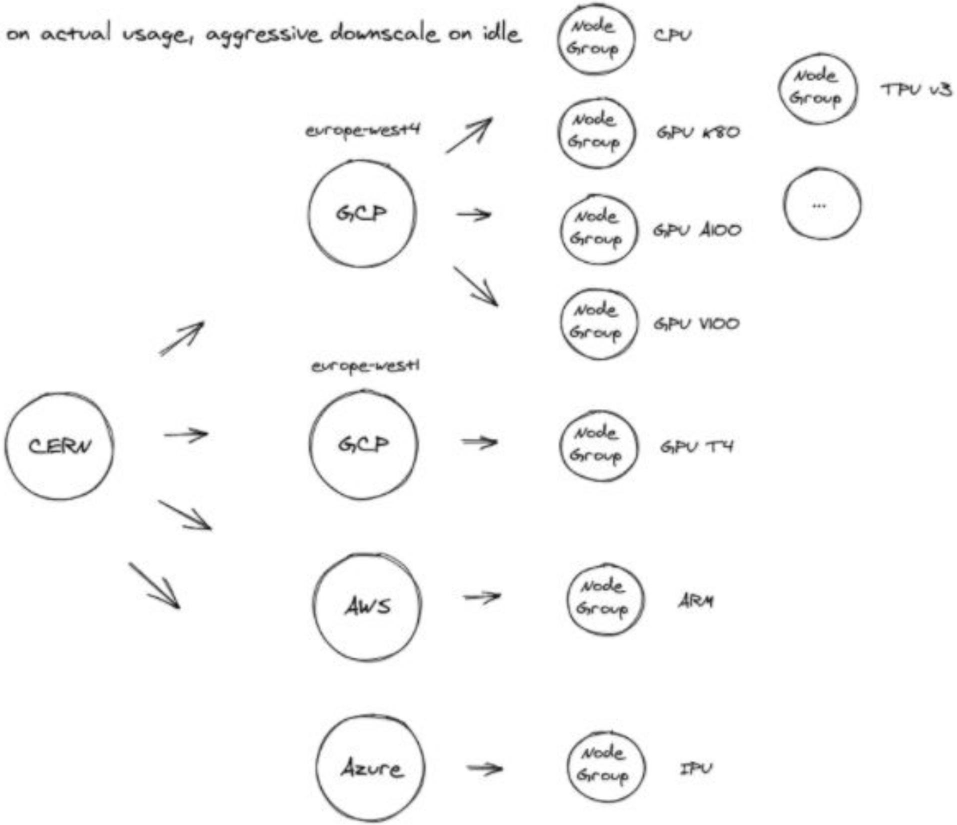
https://github.com/argoproj-labs/argocd-vault-plugin



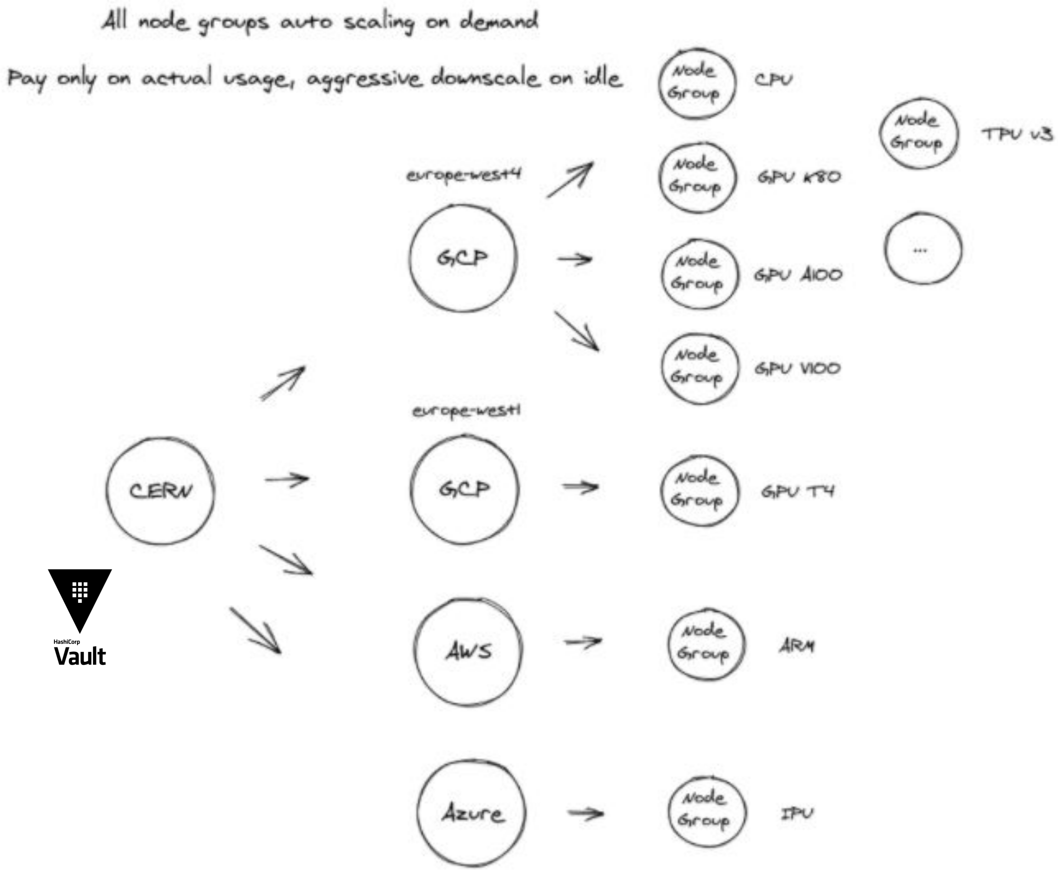
```
kind: Secret
apiVersion: v1
metadata:
  name: example-secret
  annotations:
    avp.kubernetes.io/path: "path/to/secret"
type: Opaque
data:
  password: <password-vault-key>
```

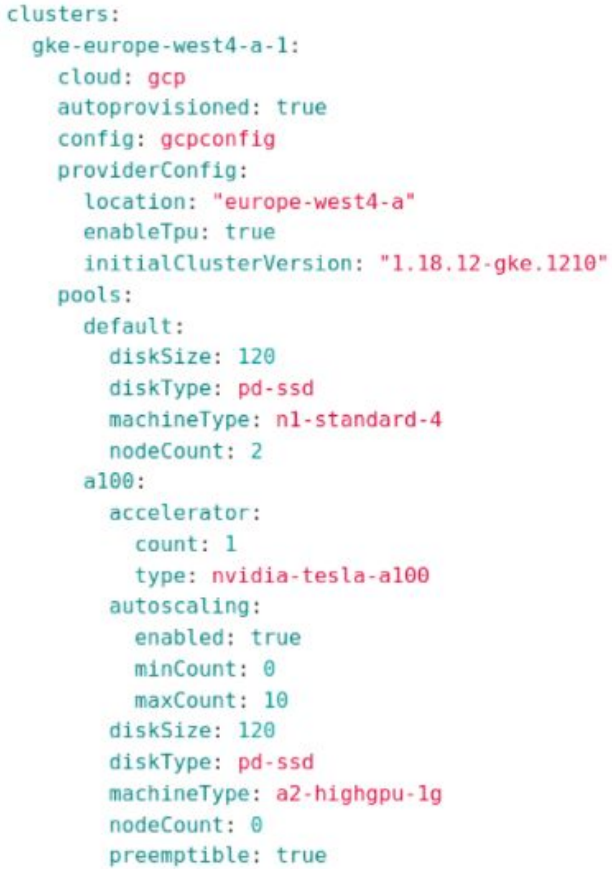
All node groups auto scaling on demand

Pay only on actual usage, aggressive downscale on idle



```yaml
clusters:
  gke-europe-west4-a-1:
    cloud: gcp
    autoprovisioned: true
    config: gcpconfig
    providerConfig:
      location: "europe-west4-a"
      enableTpu: true
      initialClusterVersion: "1.18.12-gke.1210"
    pools:
      default:
        diskSize: 120
        diskType: pd-ssd
        machineType: n1-standard-4
        nodeCount: 2
      a100:
        accelerator:
          count: 1
          type: nvidia-tesla-a100
        autoscaling:
          enabled: true
          minCount: 0
          maxCount: 10
        diskSize: 120
        diskType: pd-ssd
        machineType: a2-highgpu-1g
        nodeCount: 0
        preemptible: true
```





```
clusters:
  gke-europe-west4-a-1:
    cloud: gcp
    autoprovisioned: true
    config: gcpconfig
    providerConfig:
      location: "europe-west4-a"
      enableTpu: true
      initialClusterVersion: "1.18.12-gke.1210"
    pools:
      default:
        diskSize: 120
        diskType: pd-ssd
        machineType: n1-standard-4
        nodeCount: 2
      a100:
        accelerator:
          count: 1
          type: nvidia-tesla-a100
        autoscaling:
          enabled: true
          minCount: 0
          maxCount: 10
        diskSize: 120
        diskType: pd-ssd
        machineType: a2-highgpu-1g
        nodeCount: 0
        preemptible: true
```

2. Git Placeholders, External Store

Example: **Vault Agent Injector**

Annotation based injection with a sidecar or CSI driver

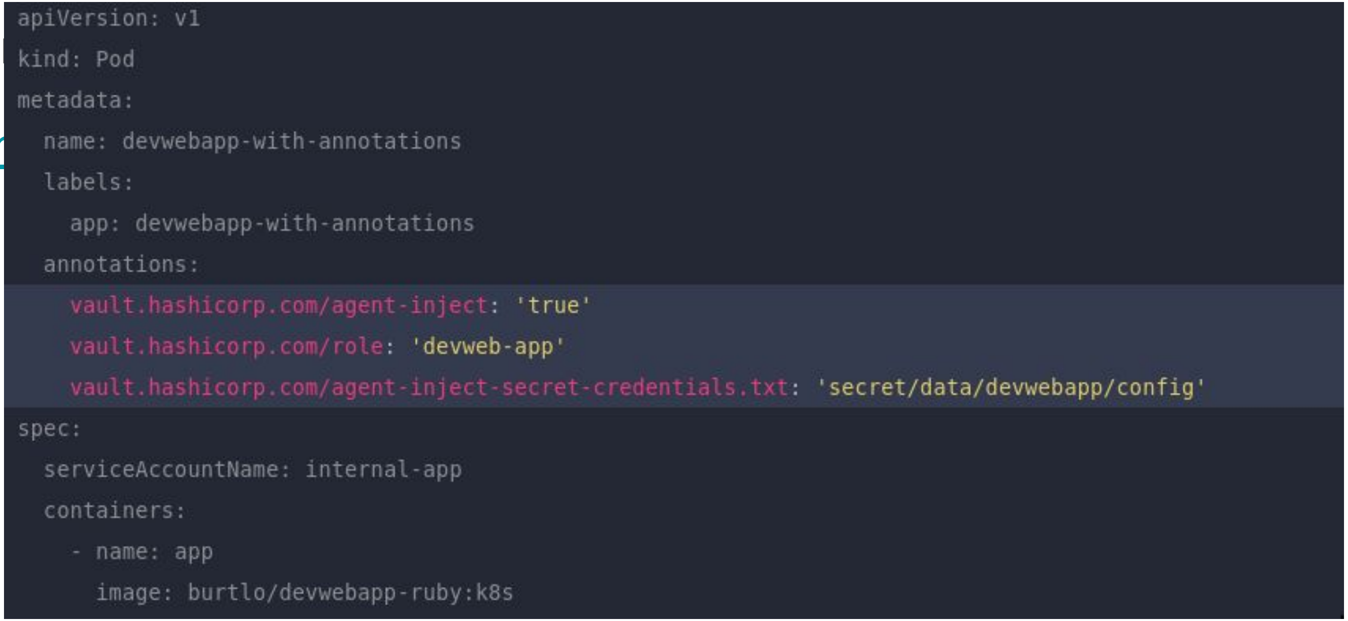
https://github.com/hashicorp/vault-k8s

2. Git Placeholders, External Store

Example: **Vault Agent Injector**

Annotatio

https://gith



```
apiVersion: v1
kind: Pod
metadata:
  name: devwebapp-with-annotations
  labels:
    app: devwebapp-with-annotations
  annotations:
    vault.hashicorp.com/agent-inject: 'true'
    vault.hashicorp.com/role: 'devweb-app'
    vault.hashicorp.com/agent-inject-secret-credentials.txt: 'secret/data/devwebapp/config'
spec:
  serviceAccountName: internal-app
  containers:
    - name: app
      image: burtlo/devwebapp-ruby:k8s
```

Other Tools

CSI Secrets Store, HC Vault, Azure, GCP, AWS

https://secrets-store-csi-driver.sigs.k8s.io/

Teller, similar to SOPS

https://github.com/spectralops/teller

…

Conclusion

Not an area where free choice and experimentation brings great results

Strong motivation for consolidation

- Best practices on handling sensitive data
- Centralized, hardened, properly audited storage for sensitive data

Hopefully we can kickstart an activity to improve this

Questions?