Kubernetes Managing Secrets

2023.01
v1.0

kubernetes

- Native :
  - Kind: Secret
- Encrypt secrets before delivery :
  - Sealed Secret (Bitnami)
  - Sops (Mozilla)
- Deliver reference to secrets :
  - ~~Hashicorp Vault Injector~~
  - External Secret Operator (CNCF)
  - Secrets Store CSI Driver (by Kubernetes-SIGS)

kubernetes

Native Kubernetes secrets

Kubernetes secrets

- Base 64
  - Aka … “en clair”

kubernetes

Sealed Secrets

(Bitnami)

Description

- A Kubernetes controller that has knowledge about the private & public key used to decrypt and encrypt encrypted secrets and is responsible for reconciliation

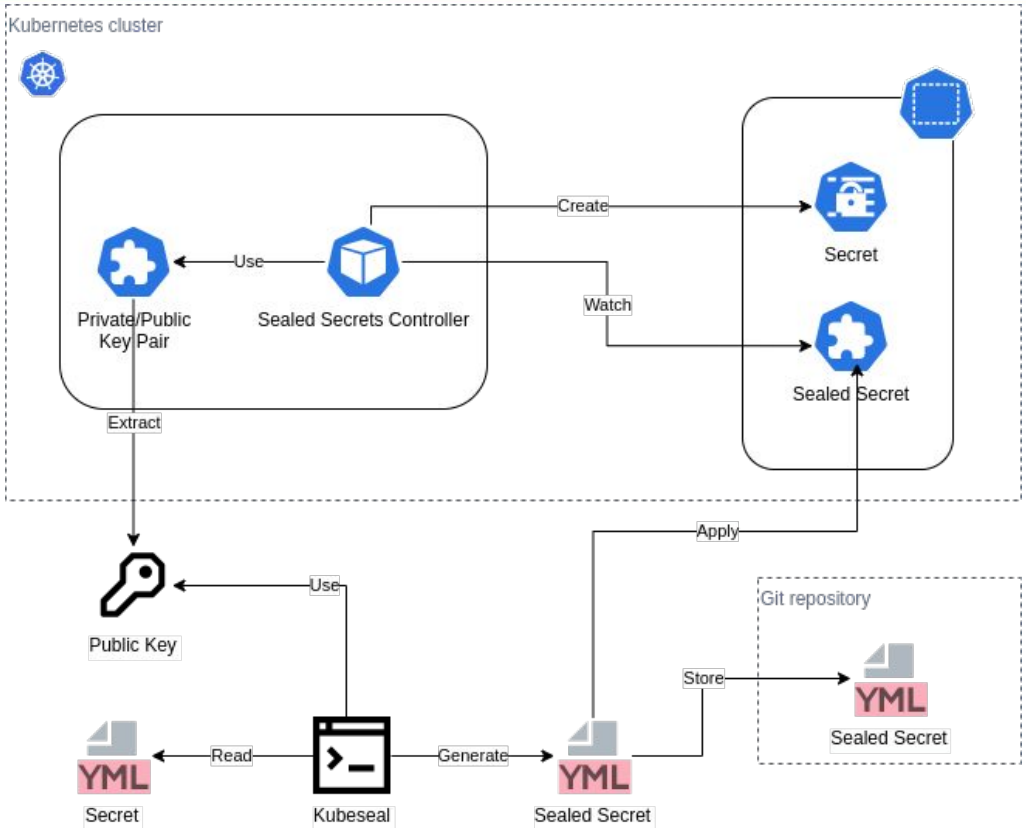
- A CLI (kubeseal) that is used by developers to encrypt their secrets before committing them to a Git repository.

CRD:

- SealedSecret

```
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  name: database-credentials
  namespace: my-namespace
spec:
  encryptedData:
    password: xxxxx==
    username: xxxxx==
  template:
    metadata:
      name: database-credentials
      namespace: my-namespace
    type: Opaque
status: {}
```

SealedSecrets



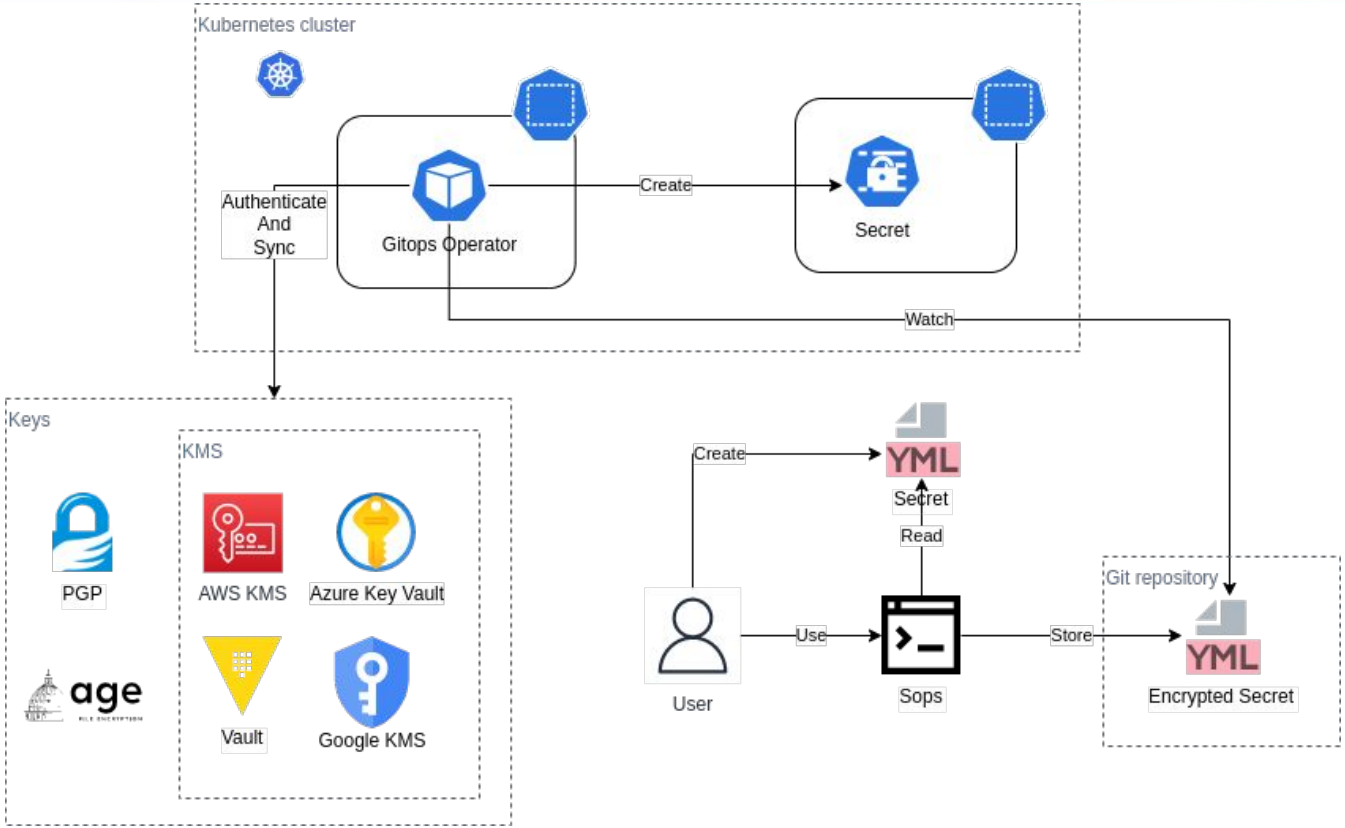
kubernetes

SOPS
Secrets OPerationS
(Mozilla)

Description

- Supports the integration with Key Management Systems (KMS) : AWS KMS, GCP KMS, Azure Key Vault and Hashicorp's Vault.
- PGP, Age for development environment
- Multiple input formats are supported including YAML, JSON, ENV, INI and BINARY formats
- CLI
- Helm plugin, Flux v2, Argo-CD plugin, ...

SOPS



kubernetes

```
apiVersion: v1
kind: Secret
metadata:
 name: mysecret
 Namespace: mynamespace
type: Opaque
data:
 key: xxxxxxx= # "value" in base64
```

```
apiVersion: v1
data:
 key:
ENC[AES256_GCM,data:xxxxxxxxxxxxxxxxxxx,iv:VnCo/PrlsHncu0N1tk2iVPAaVG7wi6imsHE4uD
4yFxI=,tag:bCX5q6tvc7eCyto+6ivsGg==,type:str]
kind: Secret
metadata:
 name: mysecret
 namespace: mynamespace
sops:
 kms: []
 gcp_kms: []
 azure_kv: []
 hc_vault: []
 age:
 - recipient: age133ly60ep0tp9vm4t95a6c6wgvv9uqtpzsgwkw8wfneshvank79ysmew3wl
   enc: |
     -----BEGIN AGE ENCRYPTED FILE-----
     YWdlLWVuY3J5cHRpb24ub3JnL3YxCi0+IFgyNTUxOSArT1B2WUoxUWVlZUptbk1W
     NXpJNTZ4YlR0RUJicVp5SU9CcWxXVkM5MVhvCkV1QWo3eGtkSjFWeHV4cTRma2l0
     VVkyckV0SXVlZjFjYnlwSVpyUE1IdmMKLS0tIHdqUXRCbTVIUG8vOEtXVmxQd2U5
     Y3FMMDF2SndreGZXd0l5UDNnQUh6OW8KR6KawAEz9UEn9TGsFKBaTInZ8jiQCvxk
     vHhhQkxwi8DuYLRg+2O0FlnsukKC5N4wfqDapBoAAHJ4NOI7Ym3DeQ==
     -----END AGE ENCRYPTED FILE-----
 lastmodified: "2021-10-08T15:31:12Z"
 mac:
ENC[AES256_GCM,data:xxxxxxxxxx,iv:8QmFNMe9MV0yfLxZpKcPEXX0vvKEPamB0PF1YBHxEtE=,ta
g:tVm+mXuuSZOyzgwru9N7AA==,type:str]
 pgp: []
 encrypted_regex: ^(data|stringData)
 version: 3.7.1
```

External Secrets Operator

(CNCF)

Description

- CNCF Sandbox (2022/07)
- Reads information from a third-party service
- Automatically injects the values as Kubernetes Secrets

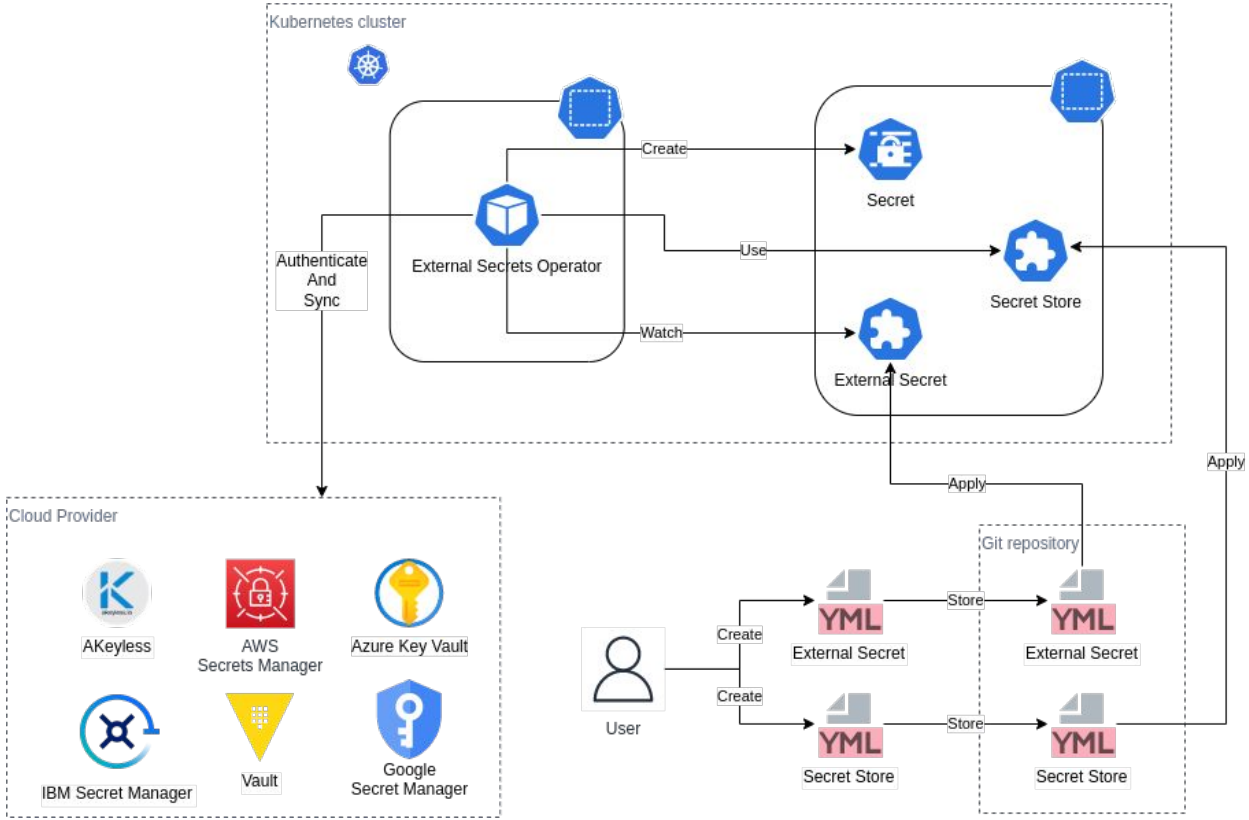
Providers:

- AWS Secrets Manager
- Google Secrets Manager
- Azure Key Vault
- IBM Cloud Secrets Manager
- HashiCorp Vault
- Akeyless
- ...

CRD

- SecretStore and ClusterSecretStore : define the connection details to the external secret stores
- ExternalSecret and ClusterExternalSecret : define what data needs to be fetched and how it should be transformed.

ESO



kubernetes

```yaml
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: aws-secretsmanager
  Namespace: my-namespace
spec:
  provider:
    aws:
      service: SecretsManager
      role: arn:aws:iam::123456789012:role/external-secrets
      region: eu-central-1
      auth:
        secretRef:
          accessKeyIDSecretRef:
            name: awssm-secret
            key: access-key
          secretAccessKeySecretRef:
            name: awssm-secret
            key: secret-access-key
```

```yaml
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: versioned-api-key
  Namespace: my-namespace
spec:
  refreshInterval: 1h
  secretStoreRef:
    name: aws-secretsmanager
    kind: SecretStore
  target:
    name: versioned-api-key
    creationPolicy: Owner
  data:
  - secretKey: previous-api-key
    remoteRef:
      key: "production/api-key"
      version: "AWSPREVIOUS"
  - secretKey: current-api-key
    remoteRef:
      key: "production/api-key"
      version: "AWSCURRENT"
```

Secrets Store CSI Driver

(Kubernetes-SIGS)

Description

Kubernetes API:

- File and block storage : Container Storage Interface (CSI)
- [WIP] Object storage: COSI (Container Object Storage Interface)
- Secrets: Secrets Store CSI Driver

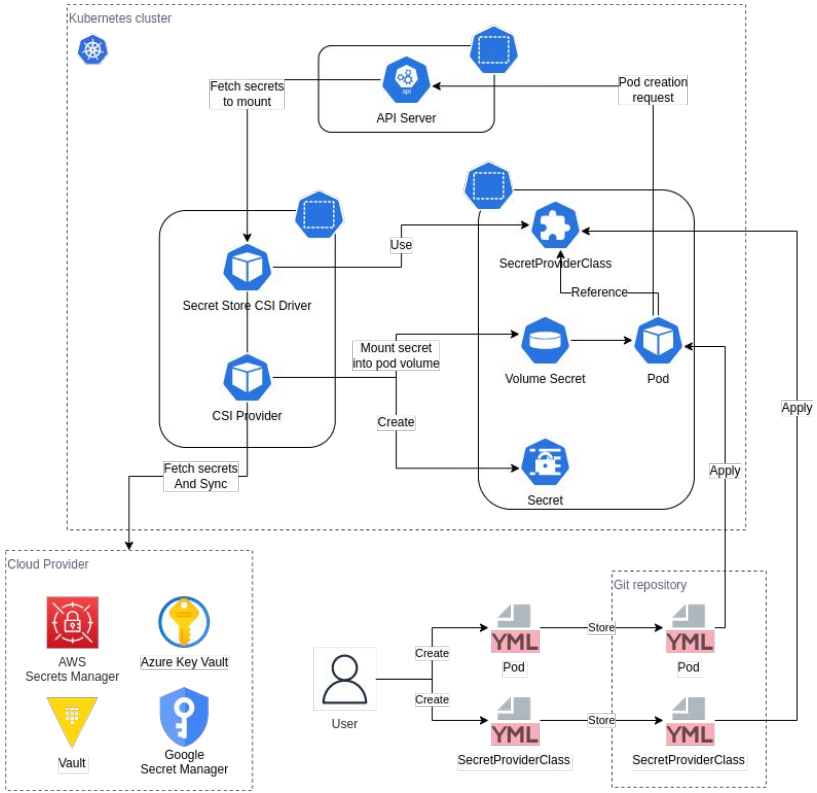
Secrets Store CSI Driver:

- the Secrets Store CSI driver communicates with the provider using gRPC to retrieve the secret content from the external Secrets Store (SecretProviderClass CRD)
- the volume is mounted in the pod as tmpfs and the secret contents are written to the volume
- Create a Kubernetes secret (optional)

Providers

- AWS Provider (AWS Secrets Manager and AWS Systems Manager Parameter Store)
- Azure Provider (Azure Key Vault)
- GCP Provider (Secret Manager)
- Vault Provider (Vault)

Secrets Store CSI Driver



kubernetes

```yaml
---
apiVersion: secrets-store.csi.x-k8s.io/v1alpha1
kind: SecretProviderClass
metadata:
  name: aws-secret-application
spec:
  provider: aws
  secretObjects:
    - secretName: application-api-key  # the k8s secret name
      type: Opaque
      data:
        - objectName: secret-api-key  # reference the corresponding parameter
          key: api_key
  parameters:
    objects: |
      - objectName: "secret-api-key"  # the AWS secret
        objectType: "secretsmanager"  # secretsmanager or ssmparameter
        # jmesPath:
        #  - path: "username"
        #    objectAlias: "MySecretUsername"
        #  - path: "password"
        #    objectAlias: "MySecretPassword"
```

```yaml
---
apiVersion: v1
kind: Pod
metadata:
  name: application
spec:
  serviceAccountName: service-api-key-sa
  volumes:
    - name: api-secret
      csi:
        driver: secrets-store.csi.k8s.io
        readOnly: true
        volumeAttributes:
          secretProviderClass: "aws-secret-application"
  containers:
    - name: application
      image: busybox
      command:
        - "sleep"
        - "3600"
      env:
        - name: API_KEY
          valueFrom:
            secretKeyRef:
              name: application-api-key
              key: api_key
      volumeMounts:
        - name: api-secret
          mountPath: "/mnt/secrets-store"
          readOnly: true
```

Questions