Scaling Secrets in Kubernetes: A Secure Multi-Cluster Approach

Gianluca Mardente

Cisco Systems

What is a secret

- A secret is any piece of information that you want to keep confidential, such as API keys, passwords, certificates, and SSH keys.
- Secret Management systems store your secrets in a secure, encrypted format, and provides you with a simple, secure way to access them.

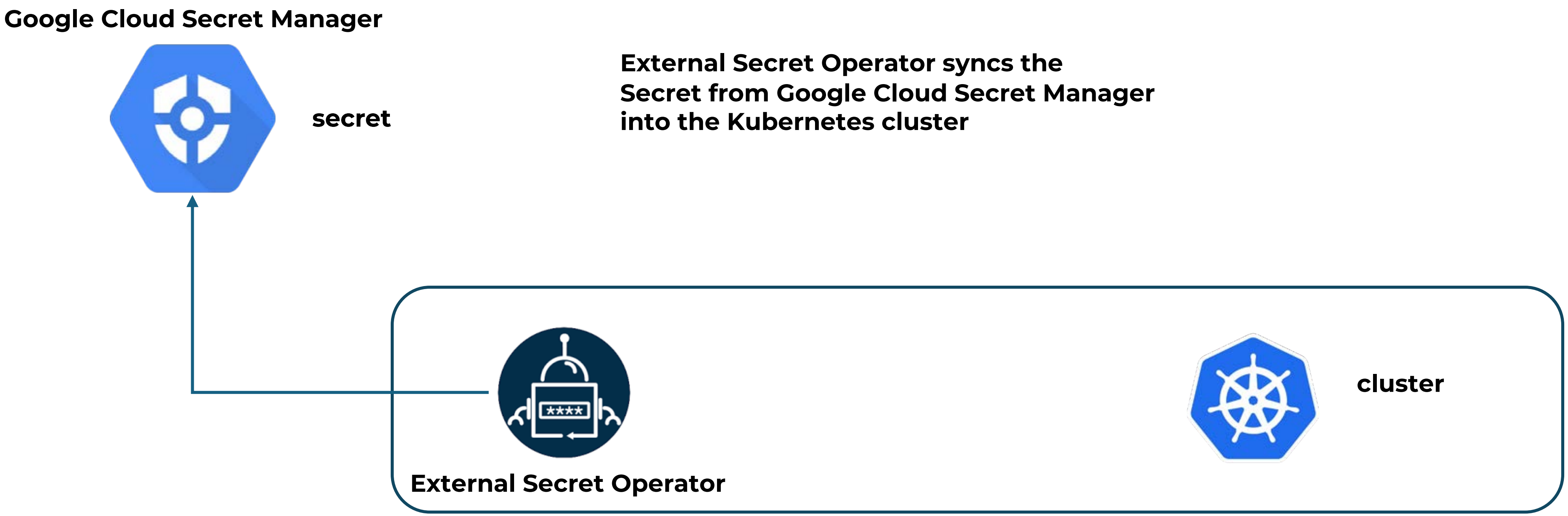
Secret Management System: Benefits

1. **Security:** A Secret Manager uses strong encryption to protect your secrets. Your secrets are never stored in plaintext, and they are only accessible to authorized users only.
2. **Convenience:** A Secret Management System makes it easy to manage the secrets. You can store, access, and rotate your secrets from anywhere.
3. **Auditability:** A Secret Management provides detailed audit logs that track who accessed your secrets and when. This helps you to track down security incidents and to comply with security regulations.

External Secrets Operator

- External Secrets Operator is an open-source Kubernetes operator
- Integrates external secret management systems like AWS Secrets Manager, HashiCorp Vault, Google Secrets Manager, Azure Key Vault, IBM Cloud Secrets Manager, and many more.
- Synchronizes secrets from external APIs into Kubernetes.

External Secret Management Integration



Google Cloud Secret Manager

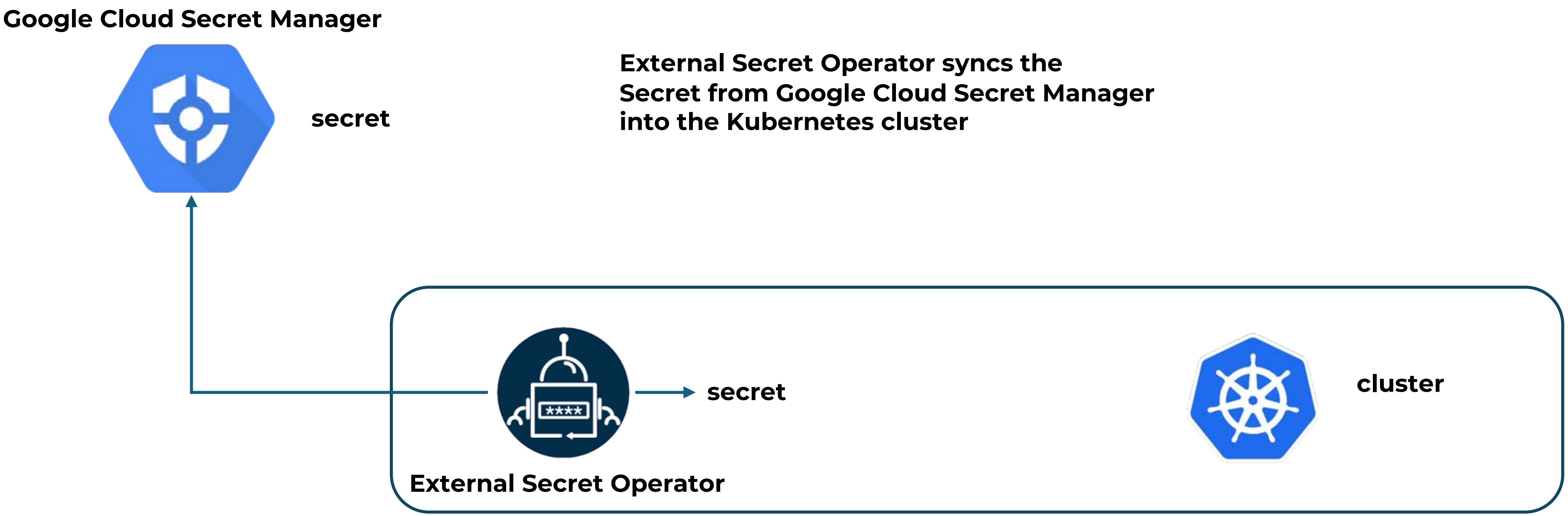
secret

External Secret Operator syncs the Secret from Google Cloud Secret Manager into the Kubernetes cluster

External Secret Operator

cluster

External Secret Management Integration



Google Cloud Secret Manager

secret

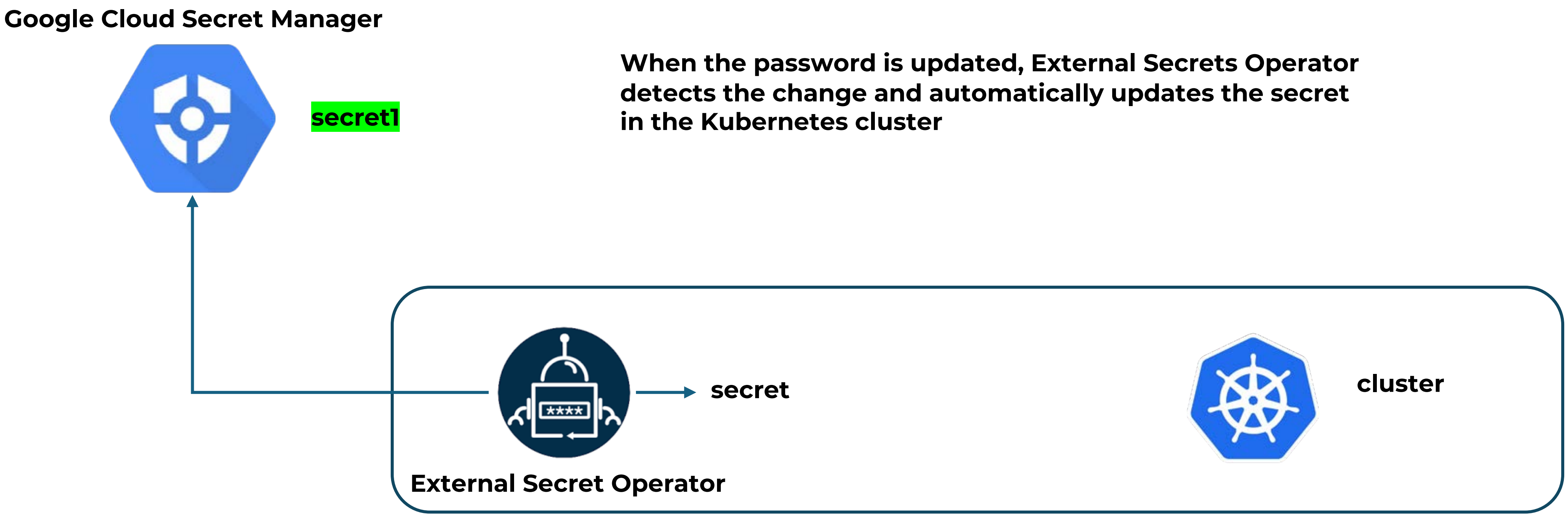
External Secret Operator syncs the
Secret from Google Cloud Secret Manager
into the Kubernetes cluster

secret

cluster

External Secret Operator

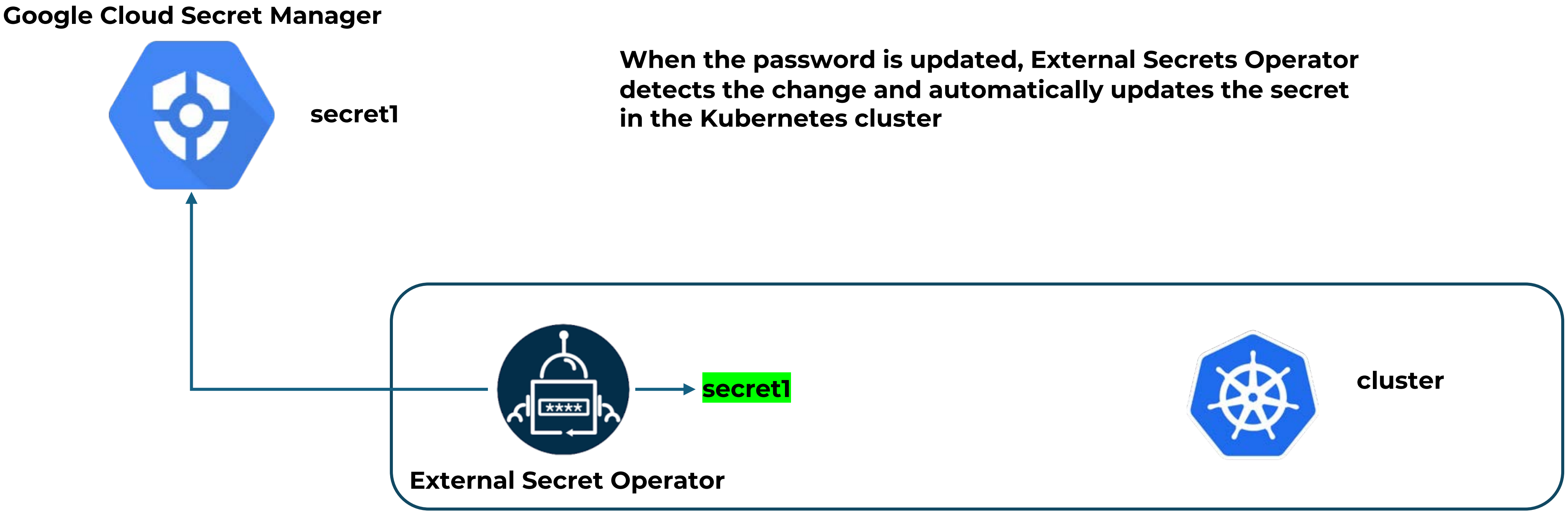
External Secret Management Integration



When the password is updated, External Secrets Operator detects the change and automatically updates the secret in the Kubernetes cluster

External Secret Management Integration

When the password is updated, External Secrets Operator detects the change and automatically updates the secret in the Kubernetes cluster



Google Cloud Secret Manager

secret1

secret1

cluster

External Secret Operator

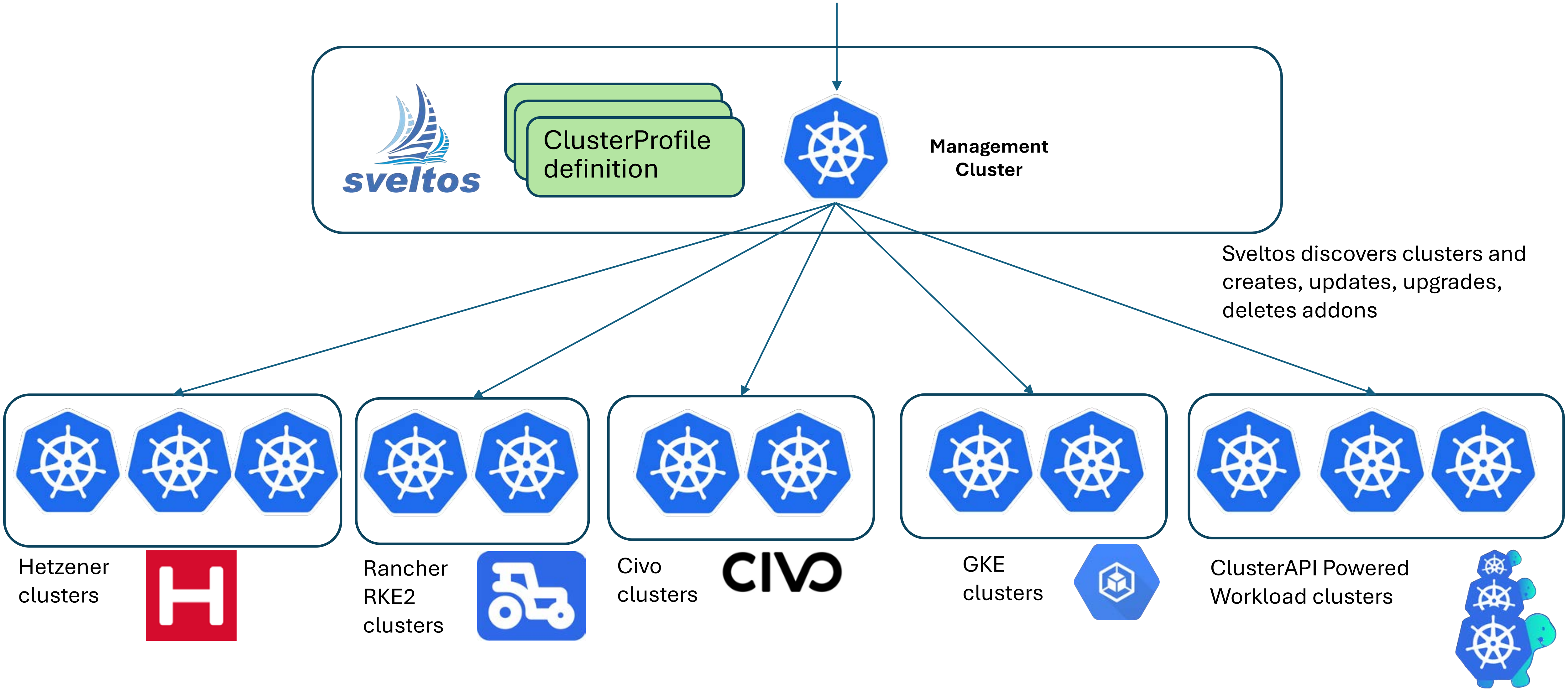
Fleet of Kubernetes clusters

- What if you have a fleet of Kubernetes clusters to manage?

Sveltos

- Sveltos is a Kubernetes add-on controller that simplifies the deployment and management of add-ons and applications across multiple clusters.

Declarative configuration (which addons to deploy and where)



sveltos

ClusterProfile definition

Management Cluster

Sveltos discovers clusters and creates, updates, upgrades, deletes addons

Hetzener clusters

Rancher RKE2 clusters

Civo clusters

GKE clusters

ClusterAPI Powered Workload clusters

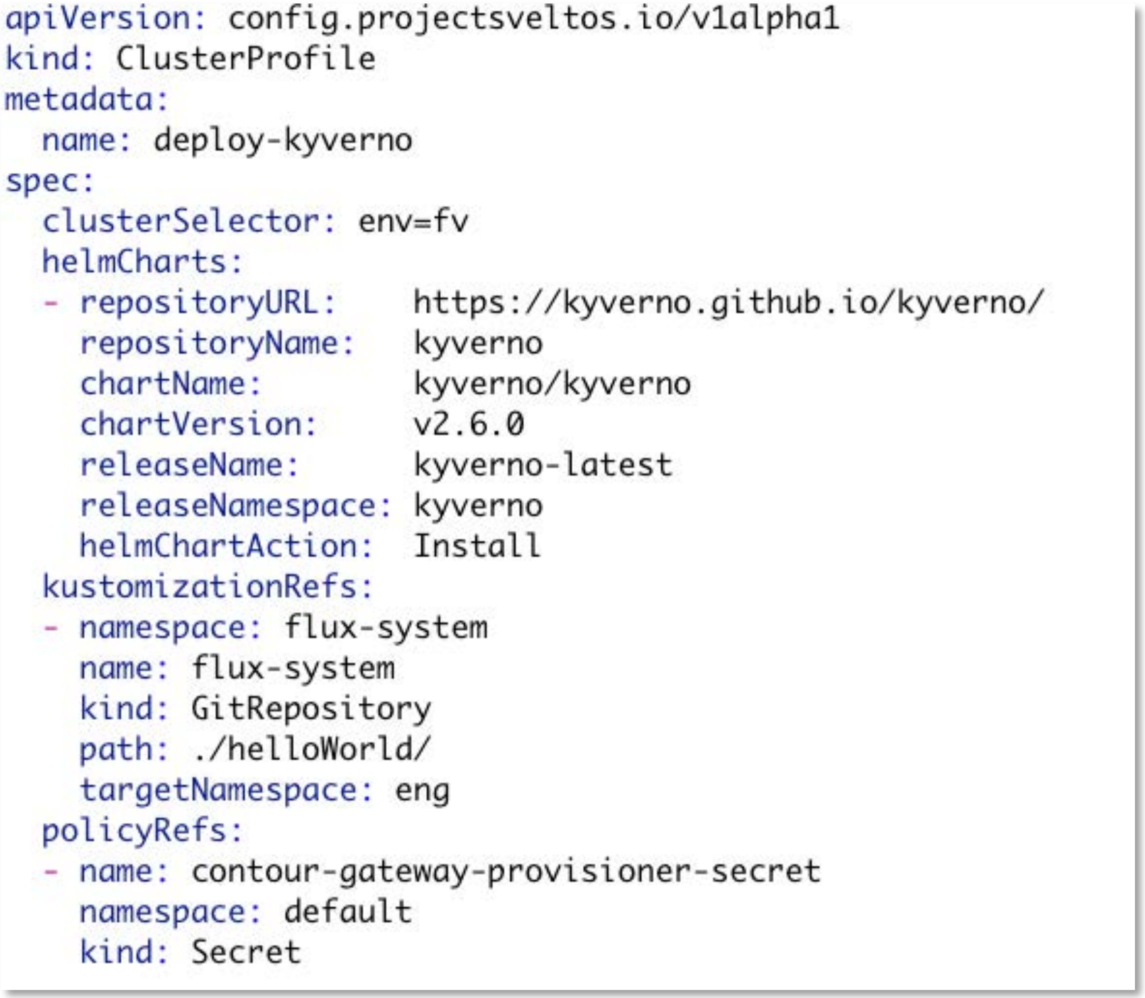
Other clusters can be easily registered with Sveltos

Built in support for ClusterAPI

ClusterProfile

ClusterProfile:

- CRD used to specify which add-ons need to be deployed in which cluster.



```yaml
apiVersion: config.projectsveltos.io/v1alpha1
kind: ClusterProfile
metadata:
  name: deploy-kyverno
spec:
  clusterSelector: env=fv
  helmCharts:
  - repositoryURL:    https://kyverno.github.io/kyverno/
    repositoryName:   kyverno
    chartName:        kyverno/kyverno
    chartVersion:     v2.6.0
    releaseName:      kyverno-latest
    releaseNamespace: kyverno
    helmChartAction:  Install
  kustomizationRefs:
  - namespace: flux-system
    name: flux-system
    kind: GitRepository
    path: ./helloWorld/
    targetNamespace: eng
  policyRefs:
  - name: contour-gateway-provisioner-secret
    namespace: default
    kind: Secret
```

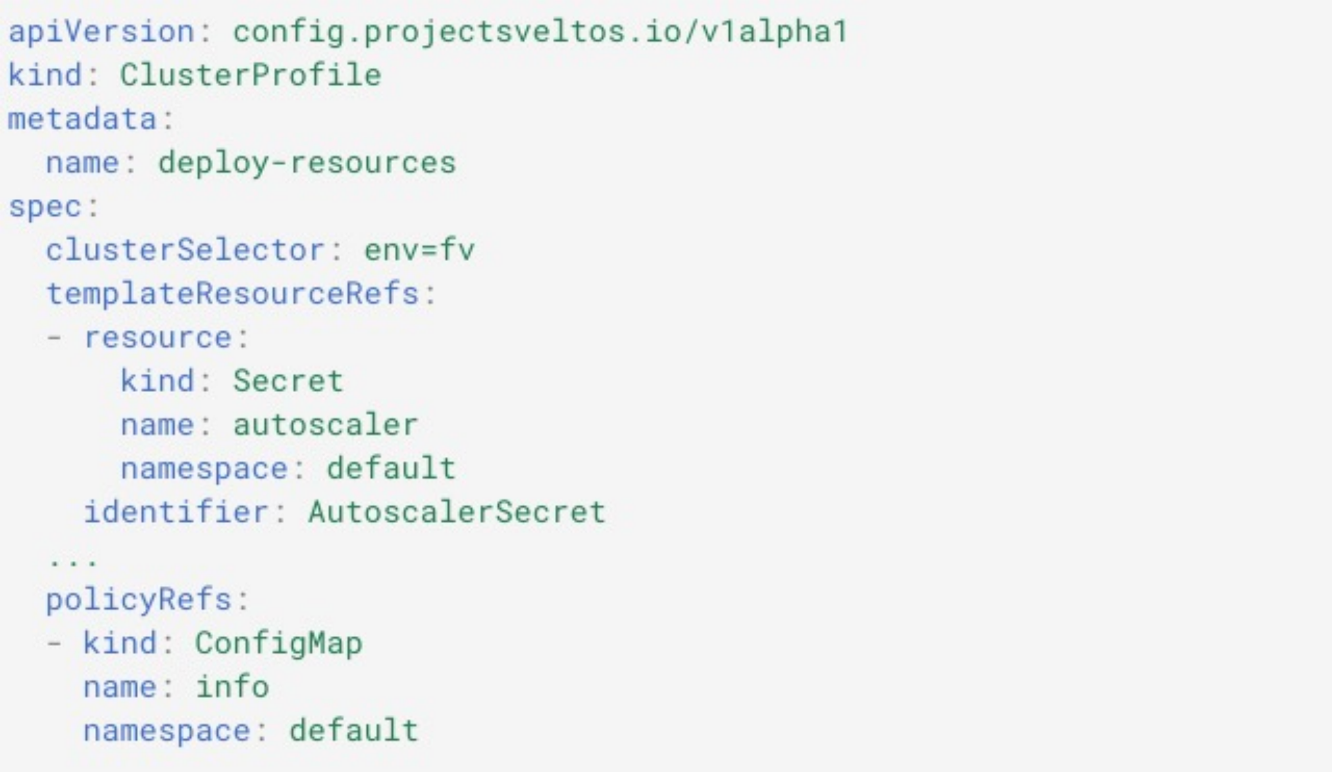
- ***clusterSelector**:* selects set of managed clusters;

- ***helmCharts***: list of helm charts to be deployed in the clusters matching clusterSelector;

- **kustomizationRefs**: : list of sources containing kustomization files. Resources will be deployed in the clusters matching clusterSelector;

- ***policyRefs***: list of ConfigMaps/Secrets containing the Kubernetes resources to be deployed in the clusters matching clusterSelector.

Project Sveltos - Templates



```yaml
apiVersion: config.projectsveltos.io/v1alpha1
kind: ClusterProfile
metadata:
  name: deploy-resources
spec:
  clusterSelector: env=fv
  templateResourceRefs:
  - resource:
      kind: Secret
      name: autoscaler
      namespace: default
    identifier: AutoscalerSecret
  ...
  policyRefs:
  - kind: ConfigMap
    name: info
    namespace: default
```

Sveltos can be instructed to fetch any resource from management cluster

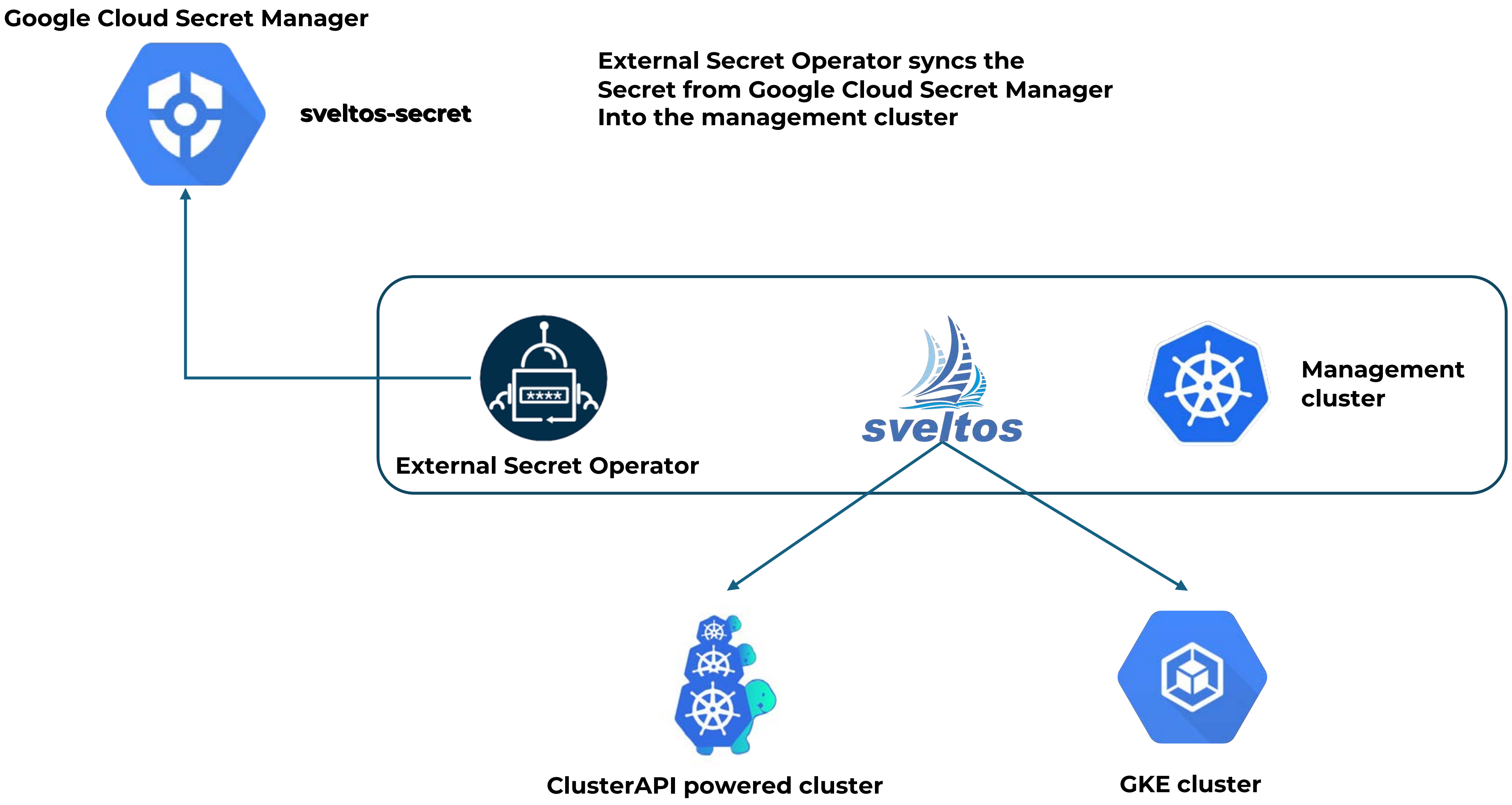
Following YAML instructs Sveltos to fetch the Secret instance *autoscaler* in the namespace *default* and make it available to the template with the keyword AutoscalerSecret

Sveltos does not have all the necessary permissions to fetch resources from the management cluster by default.
Therefore, when using *templateResourceRefs*, you need to provide Sveltos with the correct RBACs.

External Secrets Operator and Sveltos together

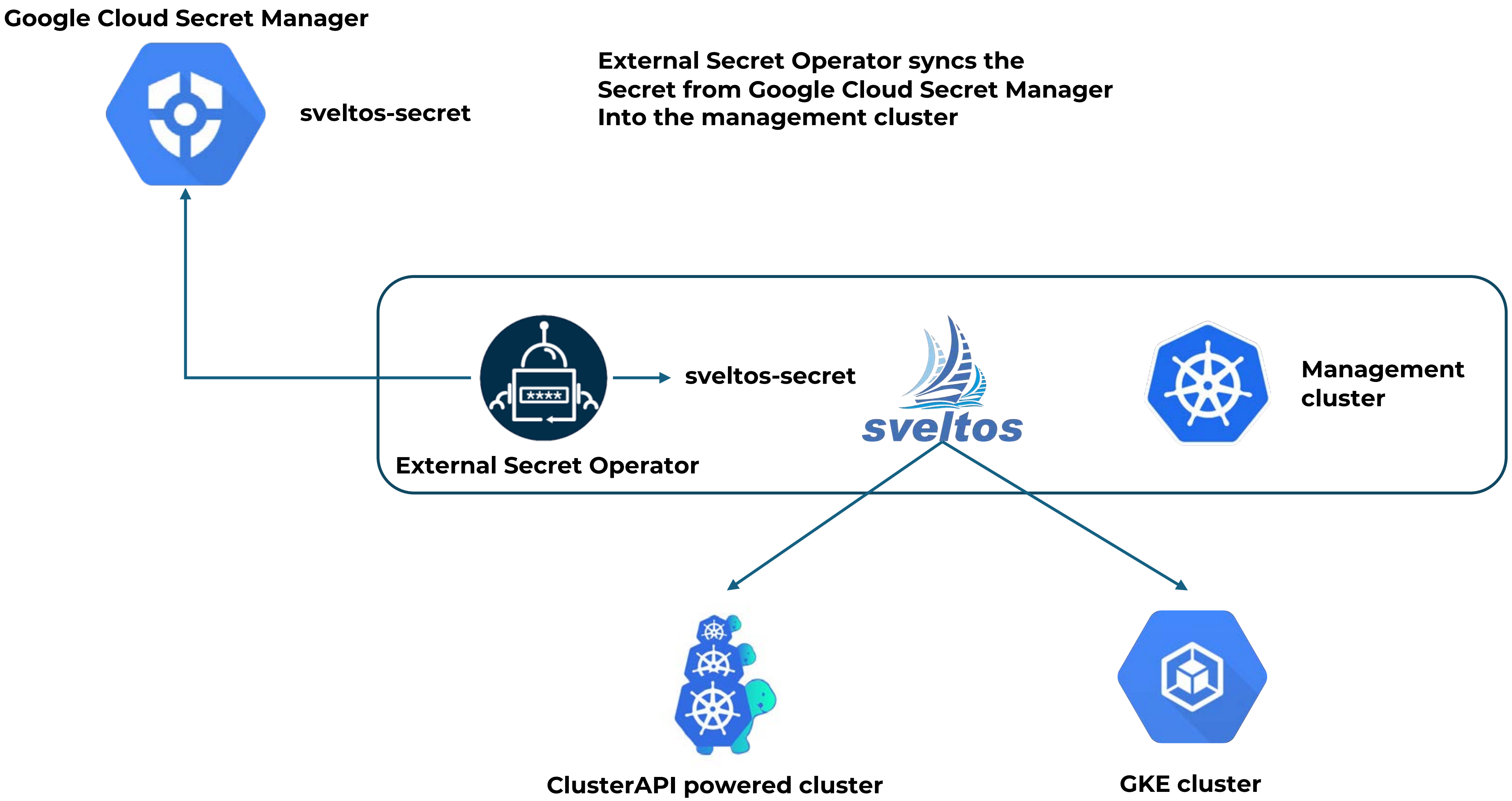
- When managing a multitude of Kubernetes clusters:
  - External Secrets Operator can be deployed in the management cluster;
  - Sveltos can be used to distribute the secrets to the managed clusters.

External Secret Management Integration



External Secret Operator syncs the Secret from Google Cloud Secret Manager Into the management cluster

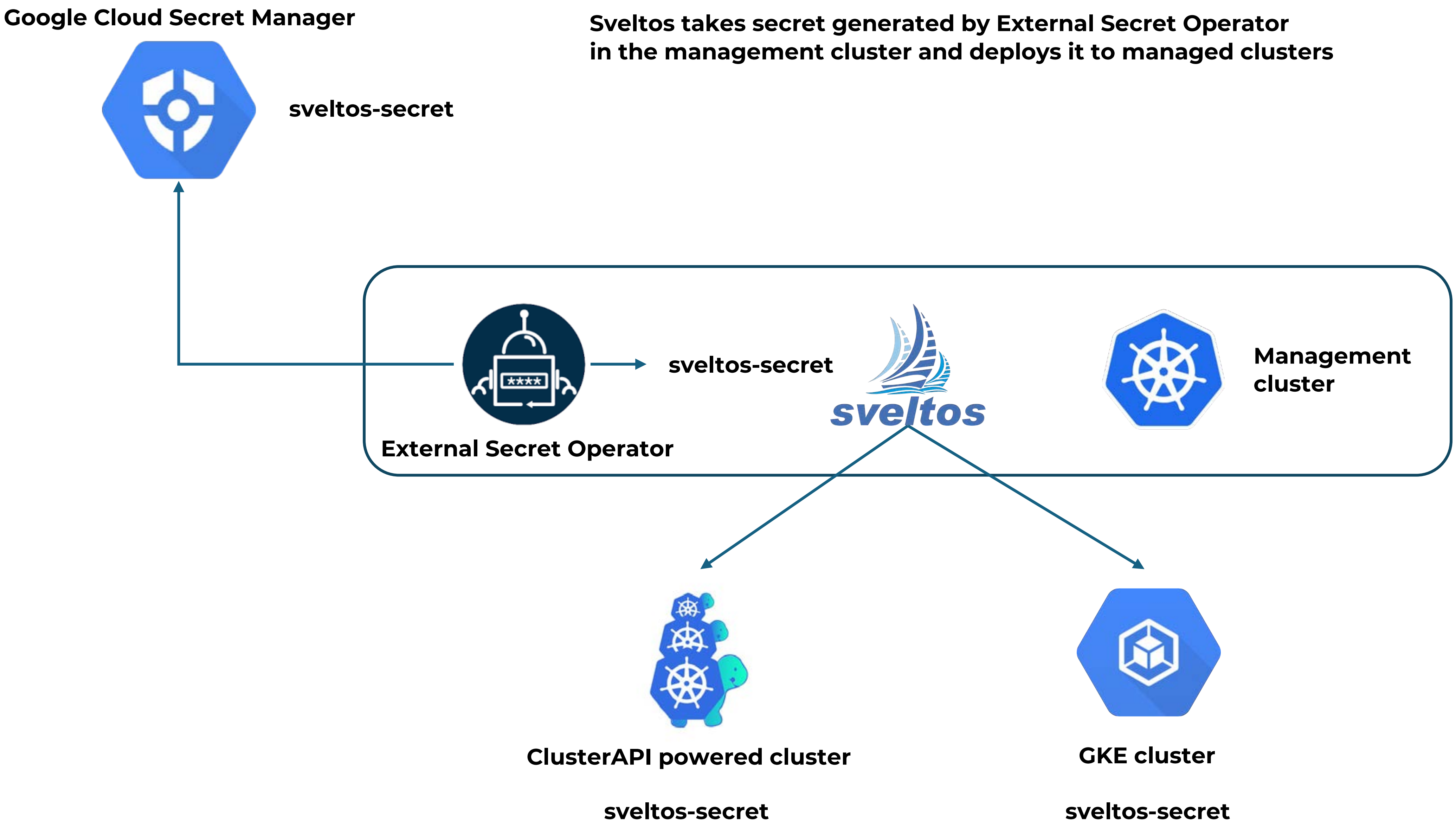
External Secret Management Integration



External Secret Operator syncs the Secret from Google Cloud Secret Manager Into the management cluster

External Secret Management Integration

Sveltos takes secret generated by External Secret Operator
in the management cluster and deploys it to managed clusters



Google Cloud Secret Manager

sveltos-secret

External Secret Operator

sveltos-secret

sveltos

Management cluster

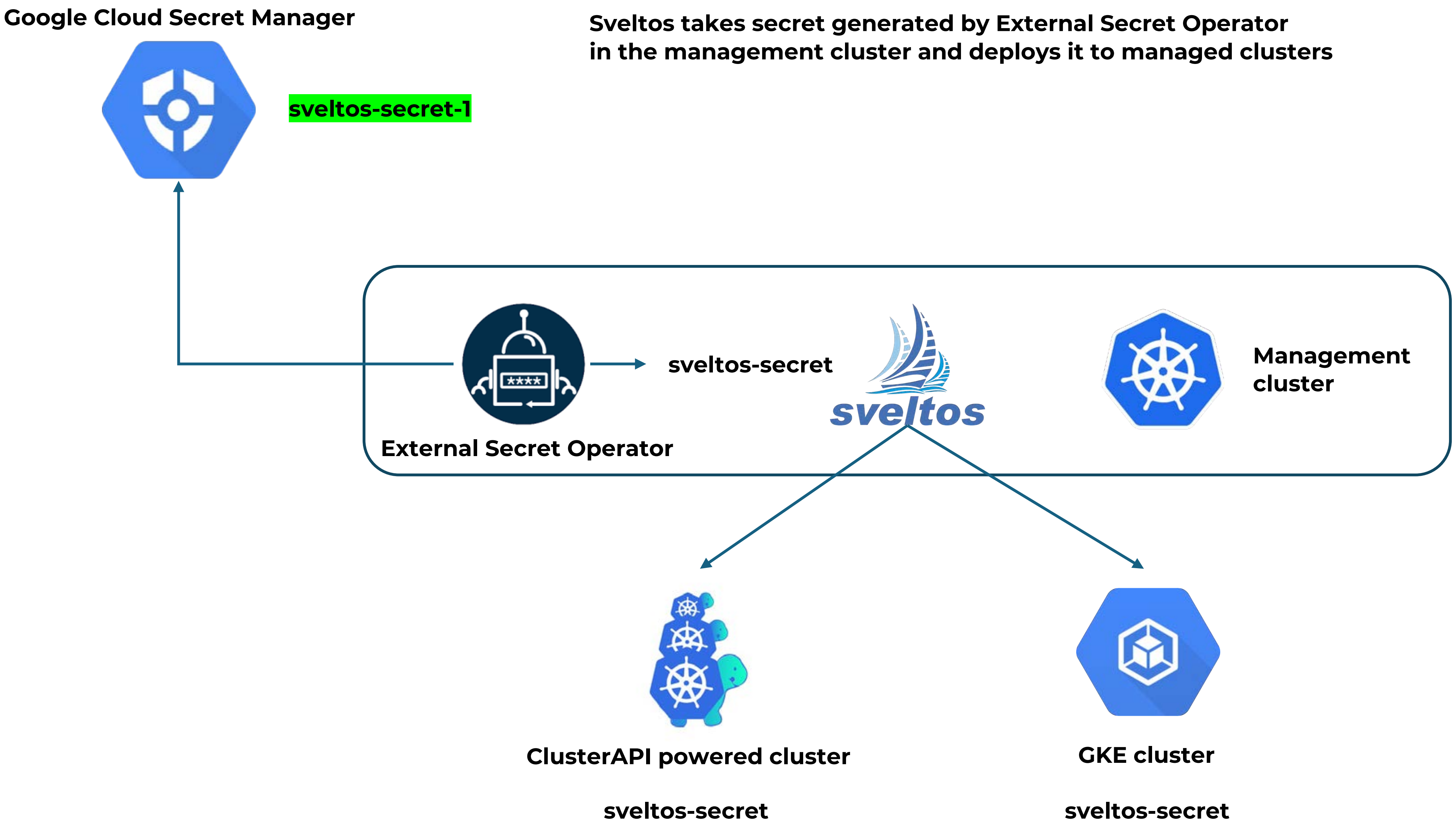
ClusterAPI powered cluster

sveltos-secret

GKE cluster

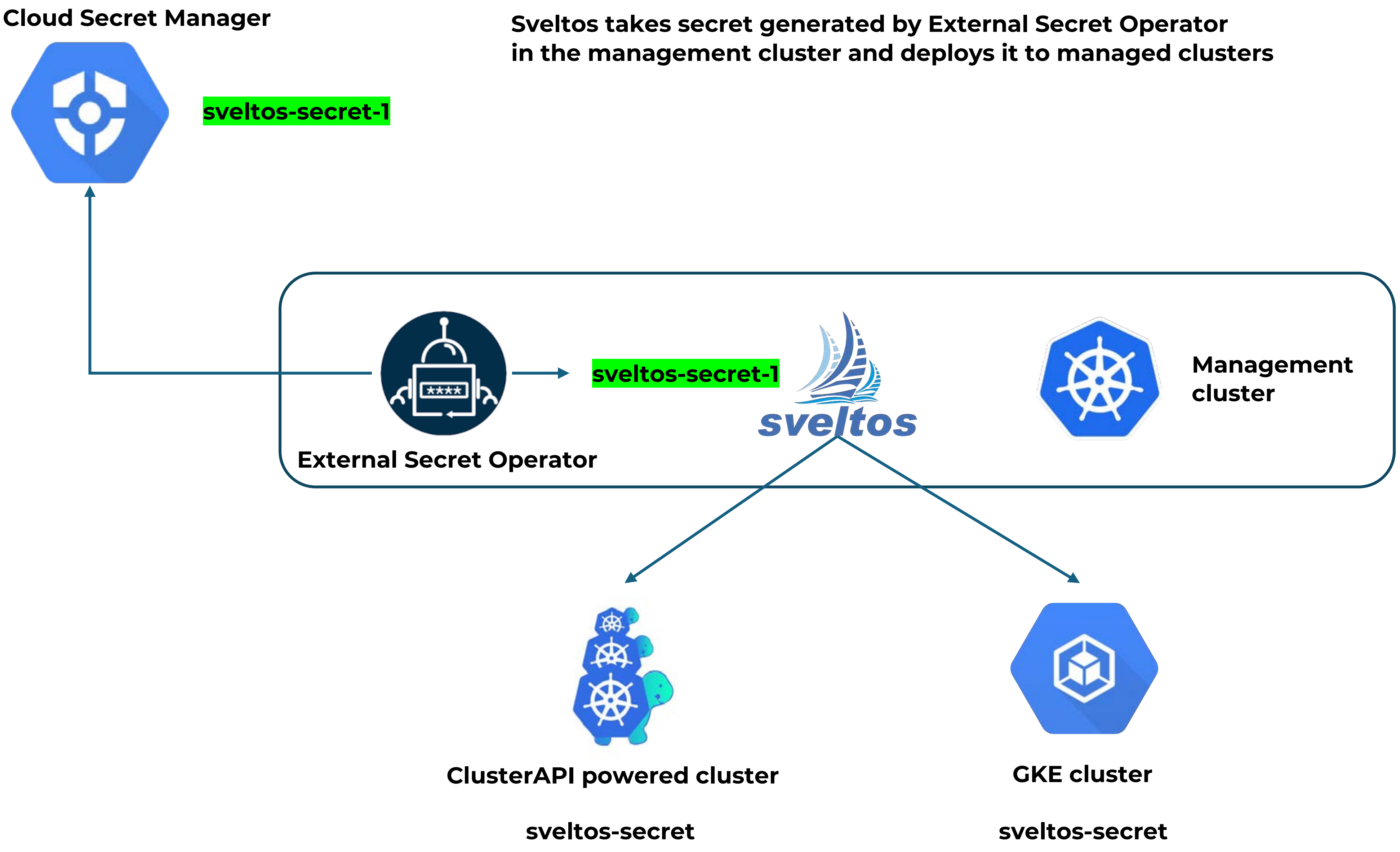
sveltos-secret

External Secret Management Integration



Sveltos takes secret generated by External Secret Operator
in the management cluster and deploys it to managed clusters

External Secret Management Integration



Google Cloud Secret Manager

sveltos-secret-1

Sveltos takes secret generated by External Secret Operator
in the management cluster and deploys it to managed clusters

sveltos-secret-1

External Secret Operator

sveltos

Management cluster

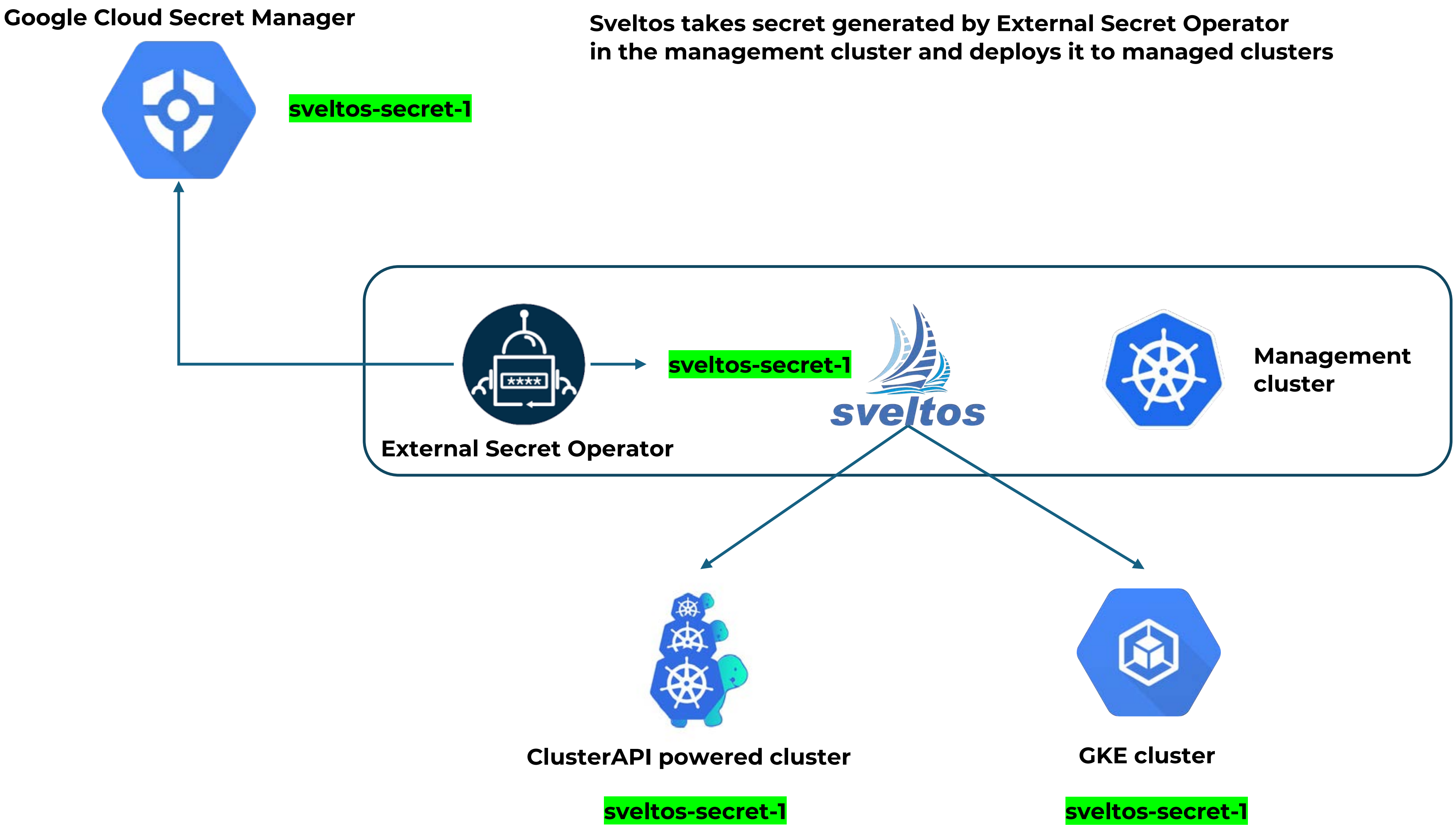
ClusterAPI powered cluster

sveltos-secret

GKE cluster

sveltos-secret

External Secret Management Integration



Sveltos takes secret generated by External Secret Operator in the management cluster and deploys it to managed clusters

Info

Sveltos: https://github.com/projectsveltos

External Secret Operator: https://github.com/external-secrets/external-secrets