trousseau.io

Kubernetes key management service provider

FOSDEM 2022

security track

romuald vandepoel (He/Him/His)
aka rom - rom@beezy.sh

who am i?

fair question...

romuald aka rom

redhat.com - transformation leader

ondat.io - open source strategy

secrets?

don't tell anyone secrets!

kubernetes API object encoded in base64 for:

- password, tokens, keys
- configuration files
- tls certs

written in etcd

kubernetes best practices

from kubernetes.io

the minimum:
- encryption at rest for secrets
- enable RBAC to restrict reading data in secrets
- enable RBAC to limit who can create and replace secrets

not enough for most organizations

what else?

open source projects

options seen are:

- cyberark conjur
- external secrets
- hashicorp vault community
- keywhiz
- sealsecrets

challenges

existing solutions

require:
- dedicated cli tool
- application orientation
- skill ramp up
- using an API superset instead of native k8s API

is there a better approach?

project origin

customer + fosdem 2021

GitOps demand native integrations
with kubernetes to reduce friction

what is trousseau

kubernetes native KMS provider plugin

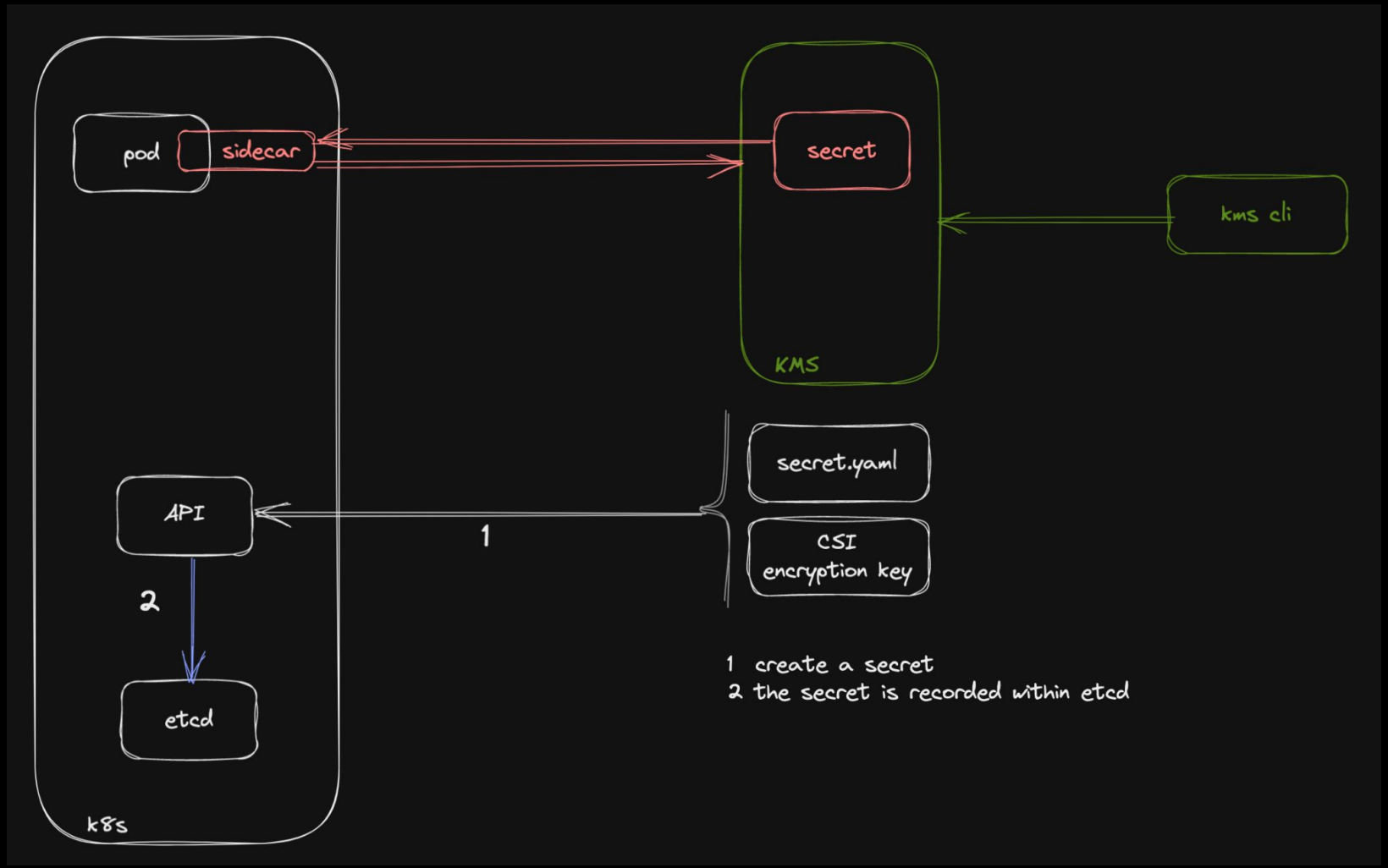
contributors have built a framework called "Key Management Service (KMS) provider and plugin" to integrate with the native kubernetes secret API management and an external KMS.

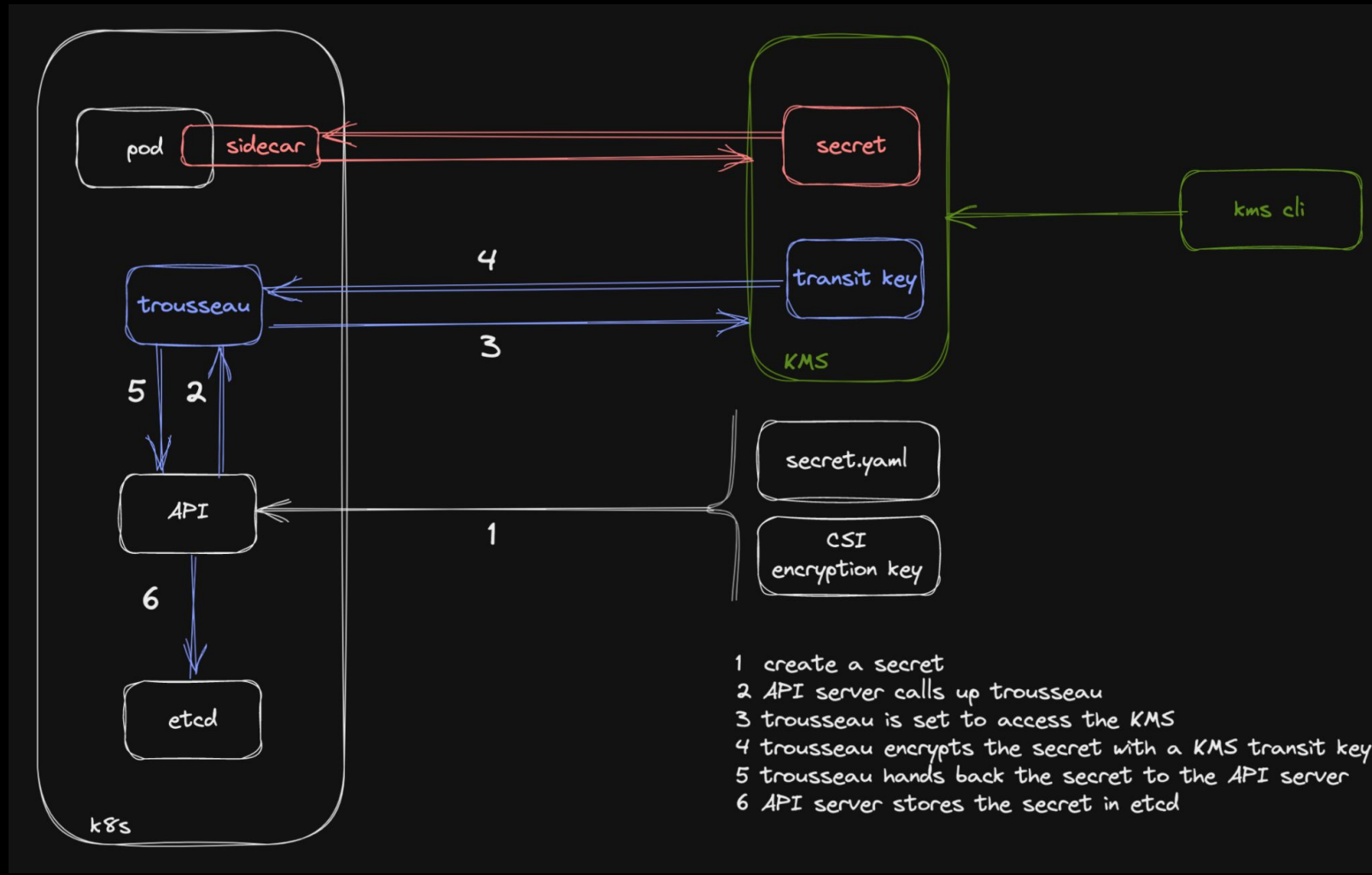
approach

kiss principle

Keep It Short and Simple

- written in Go
- container based
- limited settings
- API Server best buddy
- enjoy native kubernetes API again


pod
sidecar
secret
kms cli
KMS
secret.yaml
API
1
CSI
encryption key
2
etcd
k8s
1 create a secret
2 the secret is recorded within etcd


pod
sidecar
secret
kms cli
4
transit key
trousseau
3
KMS
5
2
secret.yaml
API
1
CSI
encryption key
6
etcd
k8s
1 create a secret
2 API server calls up trousseau
3 trousseau is set to access the KMS
4 trousseau encrypts the secret with a KMS transit key
5 trousseau hands back the secret to the API server
6 API server stores the secret in etcd

words words words

less fluff, show us!

demo setup:

- 2 VMs on DigitalOcean
- centos stream
- rke2
- cloud instance of hashicorp vault

share the love

sponsors and volunteers

ondat.io
- sponsoring!

hashicorp
- providing guidance

what's next

more openness!

two features targeted:

- sidecar implementation with Vault
- build a kms boiler template
- integration with one more kms using the kms boiler template

call to action

join us!
github/ondat/trousseau

stay safe like secrets :)