aws
COMMUNITY DAY
AOTEAROA

Secure and Unified: Integrating Vault with EKS

Lingxian Kong | 6th Sep, 2023

Lingxian Kong

- Lead Cloud Consultant @ Sourced Group
- Working in cloud space for 11 years
- Open Source project maintainer for 7 years (OpenStack, Kubernetes)

Agenda

- What is a Secret
- Challenges of Managing Secret
- Vault Overview
- AWS Elastic Kubernetes Service (EKS) Overview
- Vault Integration in EKS

aws
COMMUNITY DAY
AOTEAROA

What is a Secret

- Password
- API keys
- Database credentials
- Certificates
- Tokens
- ...

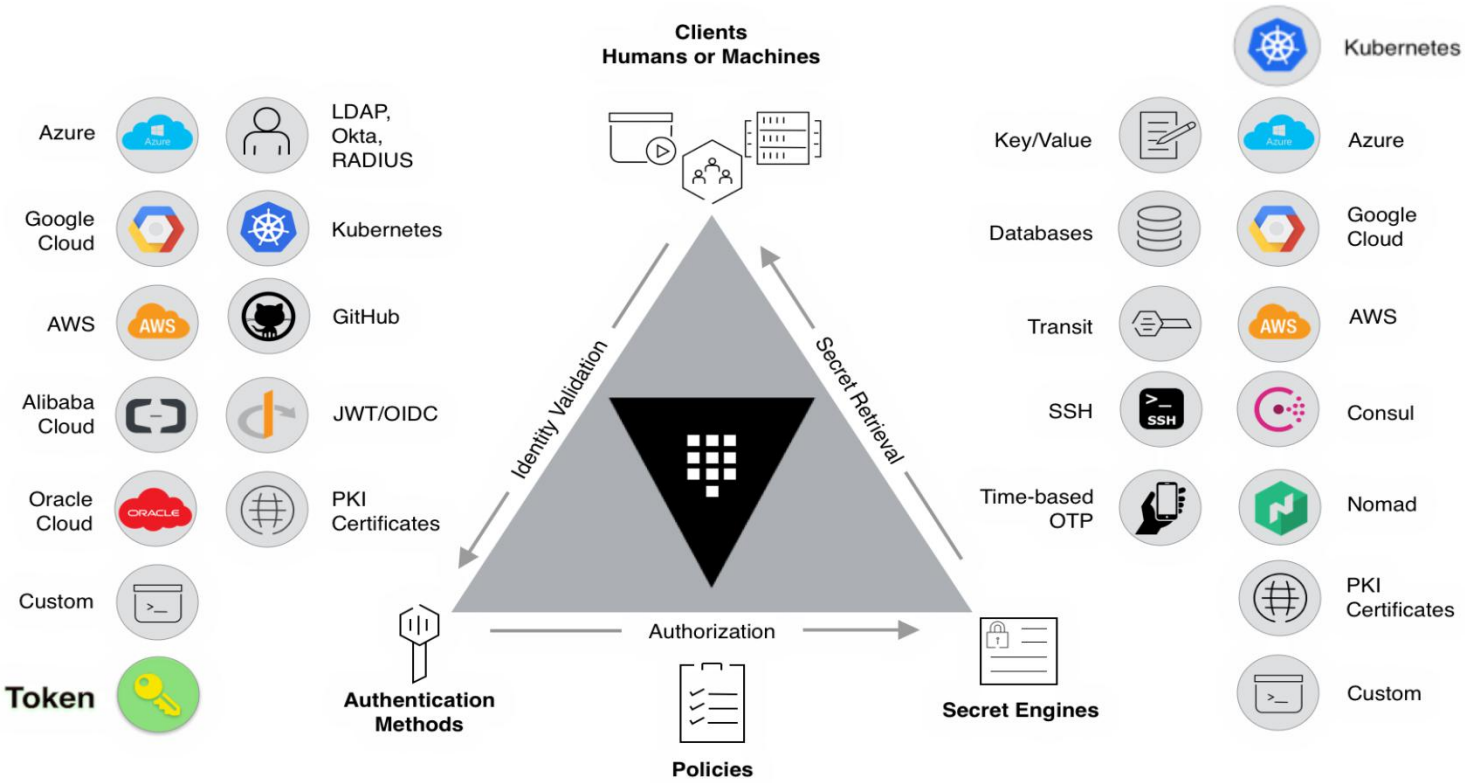
aws
COMMUNITY DAY
AOTEAROA

Challenges of Secret Management

- Secure storage
- Access control
- Auditing and monitoring
- Rotation
- Automation
- Compliance
- Integration
- ...

aws
COMMUNITY DAY
AOTEAROA

Vault Overview


Clients
Humans or Machines
Azure
LDAP, Okta, RADIUS
Google Cloud
Kubernetes
AWS
GitHub
Alibaba Cloud
JWT/OIDC
Oracle Cloud
PKI Certificates
Custom
Token
Identity Validation
Secret Retrieval
Authorization
Authentication Methods
Policies
Secret Engines
Key/Value
Databases
Transit
SSH
Time-based OTP
Kubernetes
Azure
Google Cloud
AWS
Consul
Nomad
PKI Certificates
Custom

aws
COMMUNITY DAY
AOTEAROA

Vault Demo

aws
COMMUNITY DAY
AOTEAROA

AWS Elastic Kubernetes Service (EKS) Overview

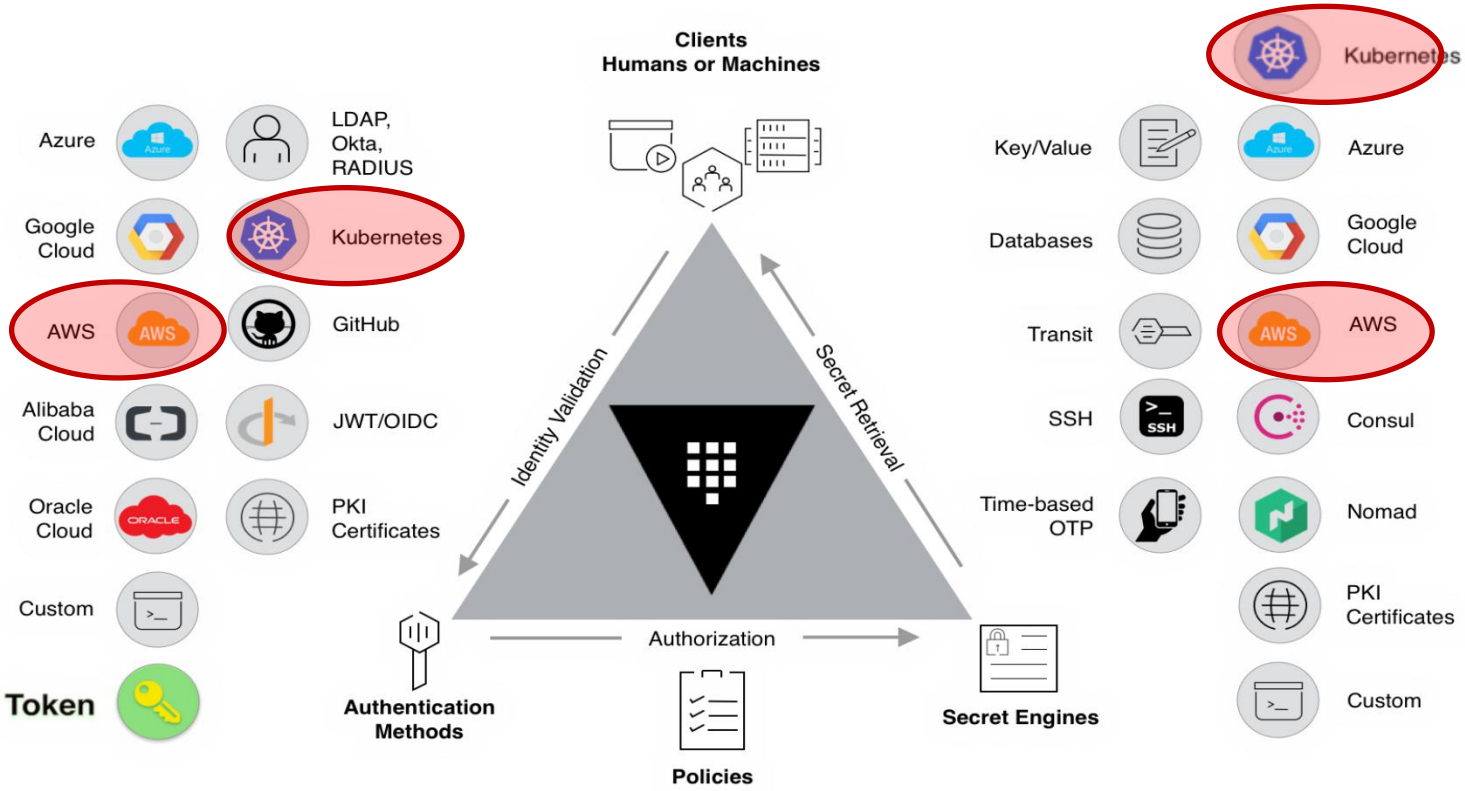
- Fully managed
- VPC networking connection
- AWS integration
- Ecosystem

aws
COMMUNITY DAY
AOTEAROA

EKS cluster demo

aws
COMMUNITY DAY
AOTEAROA

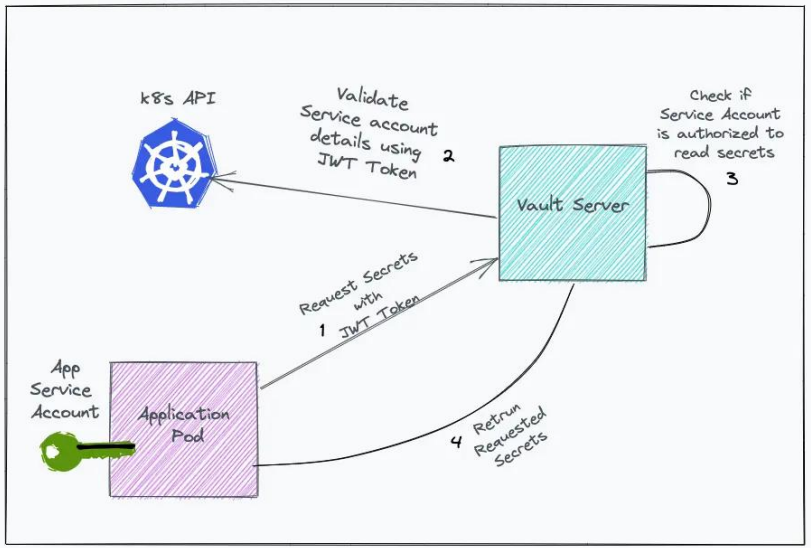
Vault Integration in EKS


Clients
Humans or Machines
Azure
LDAP, Okta, RADIUS
Google Cloud
Kubernetes
AWS
GitHub
Alibaba Cloud
JWT/OIDC
Oracle Cloud
PKI Certificates
Custom
Token
Identity Validation
Secret Retrieval
Authorization
Authentication Methods
Policies
Secret Engines
Key/Value
Azure
Databases
Google Cloud
Transit
AWS
SSH
Consul
Time-based OTP
Nomad
PKI Certificates
Custom
Kubernetes

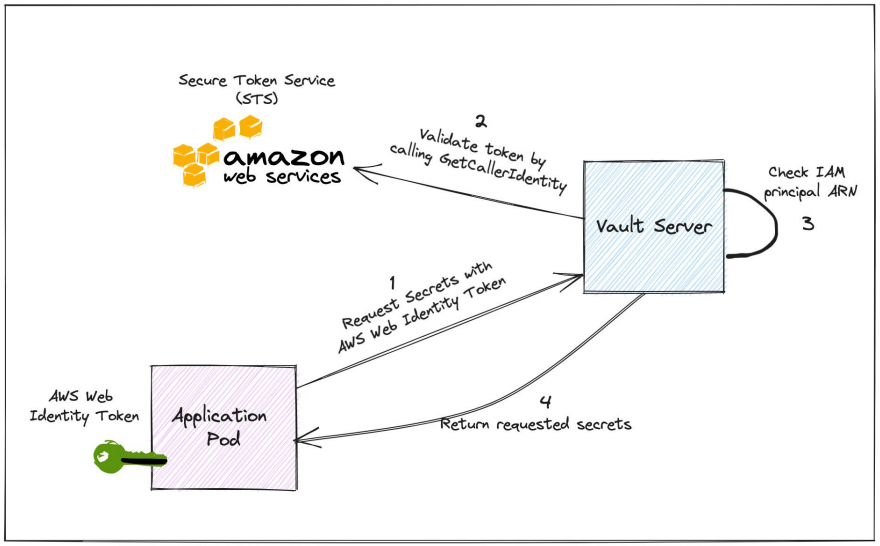
- How does the application log in Vault?
- How does the application access the secrets in the cloud native way?
- How does the application communicate with each other in a secure way?

- How does the application log in Vault?
- How does the application access the secrets in the cloud native way?
- How does the application communicate with each other in a secure way?

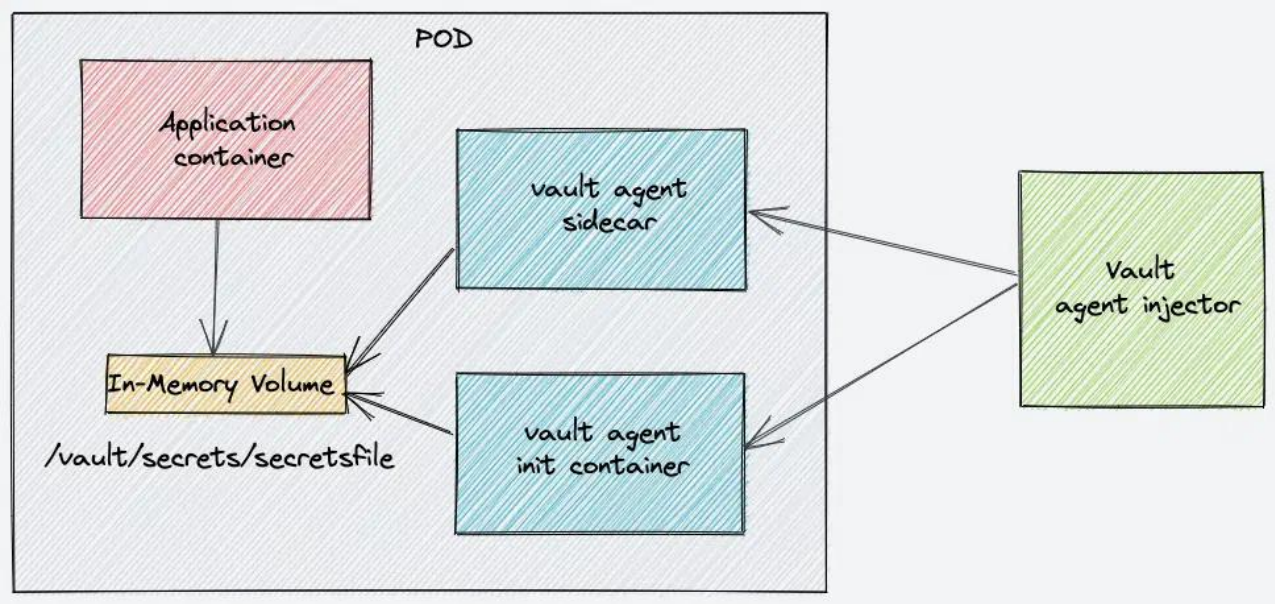
- Kubernetes service account



- AWS IAM roles for service account



- Vault Agent Injector



aws
COMMUNITY DAY
AOTEAROA

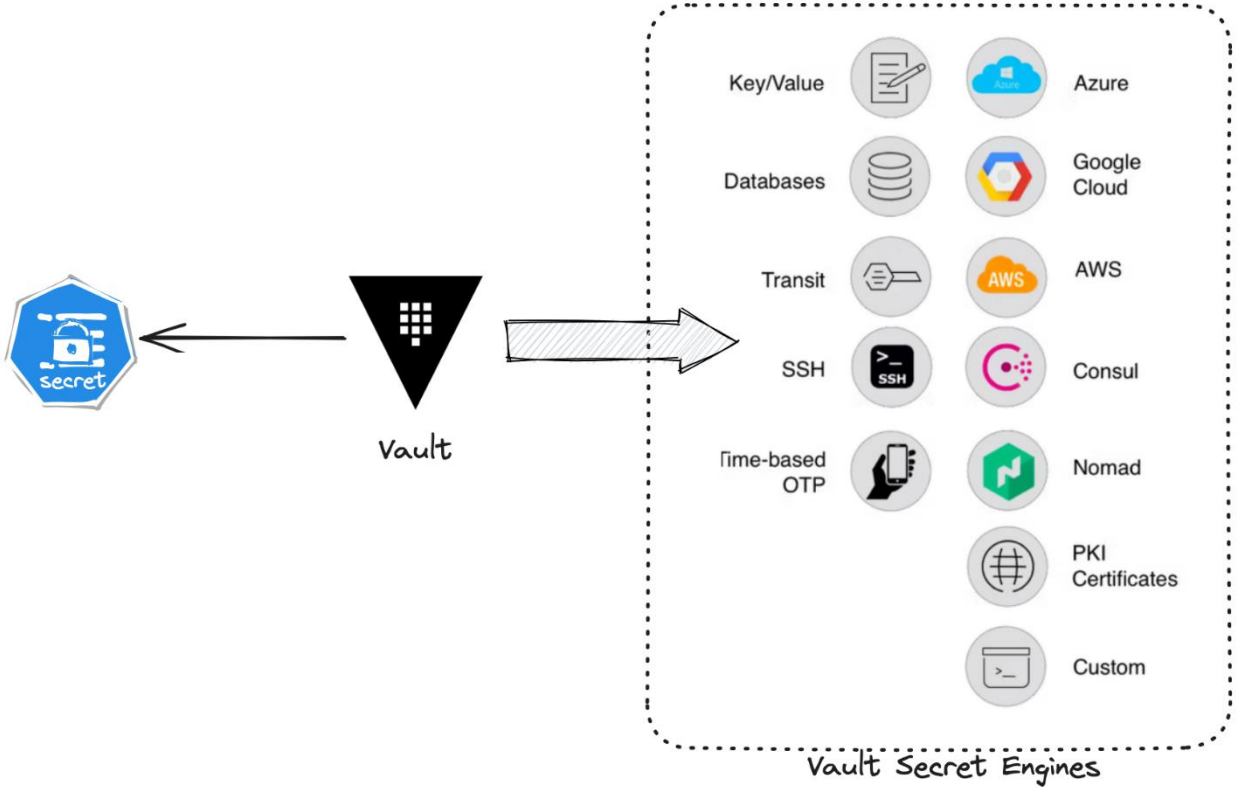
Demo

Vault Agent Injector

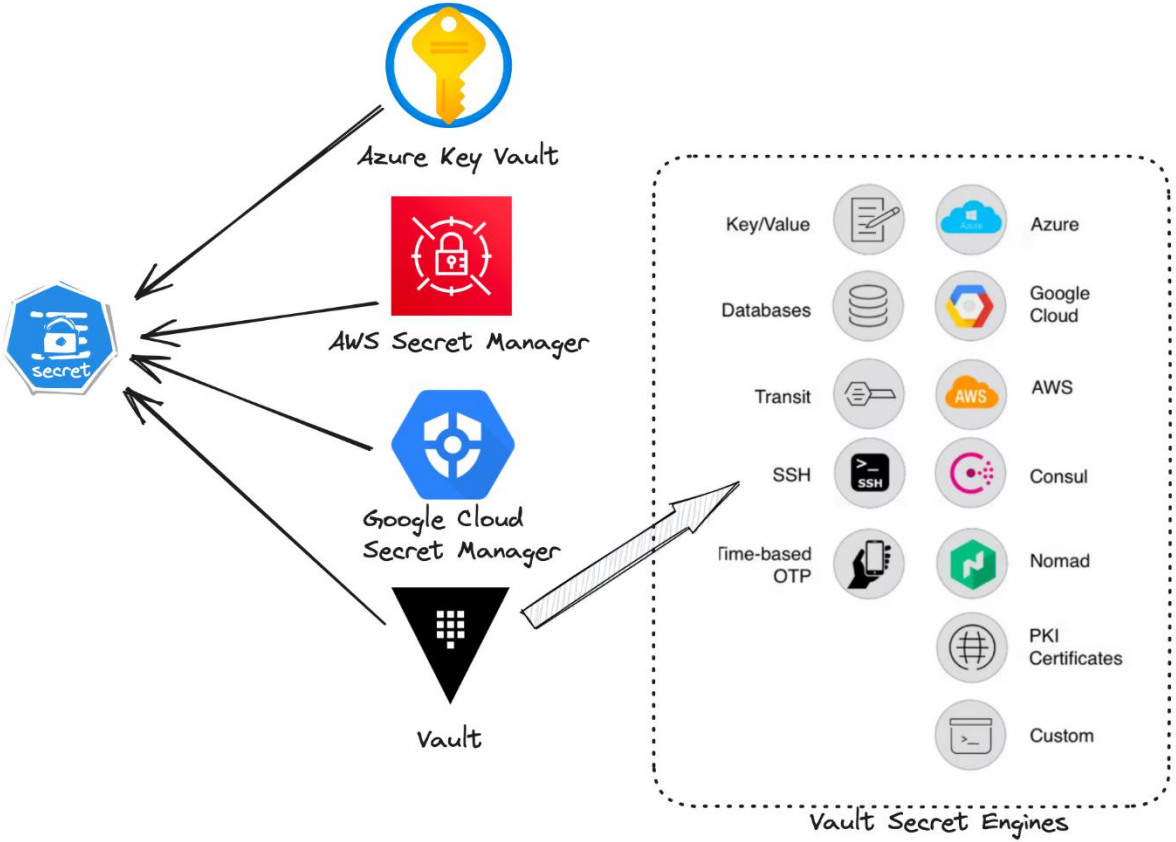
- How does the application log in Vault?
- How does the application access the secrets in the cloud native way?
- How does the application communicate with each other in a secure way?

```
apiVersion: v1
kind: Secret
metadata:
  name: mysecret
type: Opaque
data:
  username: YWRtaW4=
  password: MWYyZDFlMmU2N2Rm
```

Proposal 1


secret
Vault
Key/Value
Databases
Transit
SSH
Time-based OTP
Azure
Google Cloud
AWS
Consul
Nomad
PKI Certificates
Custom
Vault Secret Engines

Proposal 2


Azure Key Vault
AWS Secret Manager
secret
Google Cloud
Secret Manager
Vault
Key/Value
Databases
Transit
SSH
Time-based
OTP
Azure
Google
Cloud
AWS
Consul
Nomad
PKI
Certificates
Custom
Vault Secret Engines

Solution 1 - Vault Secrets Operator

```yaml
---
apiVersion: secrets.hashicorp.com/v1alpha1
kind: VaultStaticSecret
metadata:
  namespace: vso-example
  name: example
spec:
  vaultAuthRef: vault-auth
  mount: kv
  type: kv-v2
  name: secret-in-vault
  refreshAfter: 60s
  destination:
    create: true
    name: secret-in-k8s
```

Solution 2 - External Secrets Operator

```yaml
---
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: vault-example
spec:
  refreshInterval: "5m"
  secretStoreRef:
    name: secretstore-vault
    kind: SecretStore
  target:
    name: test-vault-secret
  data:
  - secretKey: db_pass
    remoteRef:
      key: mysql
      property: MYSQL_PASSWORD
```

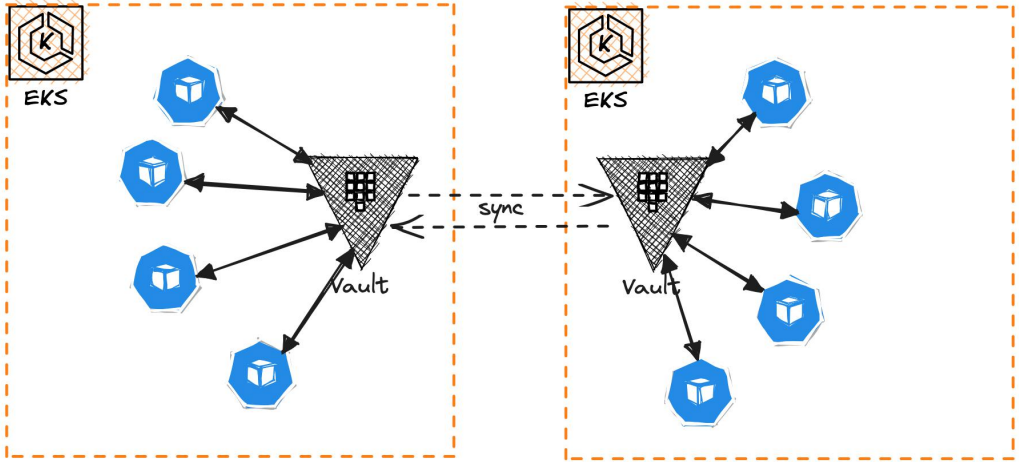
aws
COMMUNITY DAY
AOTEAROA

Demo

External Secrets Operator

- How does the application log in Vault?
- How does the application access the secrets in the cloud native way?
- How does the application communicate with each other in a secure way?

- Zero trust
- Indentity information included
- Support different EKS clusters or different environments
- ...via Vault
- JWT auth method



aws
COMMUNITY DAY
AOTEAROA

Demo

Unified Identity Token

aws
COMMUNITY DAY
AOTEAROA

Q&A