擔心你的***Kubernetes***機密被偷？

整合***Vault***加密資料就安心了

Hello!

I am Evelyn Su

網創資訊 / DevOps Consultant

Agenda

1. About Secret
2. What is Vault
3. Vault Concepts
4. Vault Agent Injector Example

1

About Secret

Let’s start with the first set of slides

What is secret ?

“

Secret is

Anything you deems **sensitive** :

- Username and Passwords
- API Keys
- SSH Keys

- Certificates

- Credential
- Encryption Keys

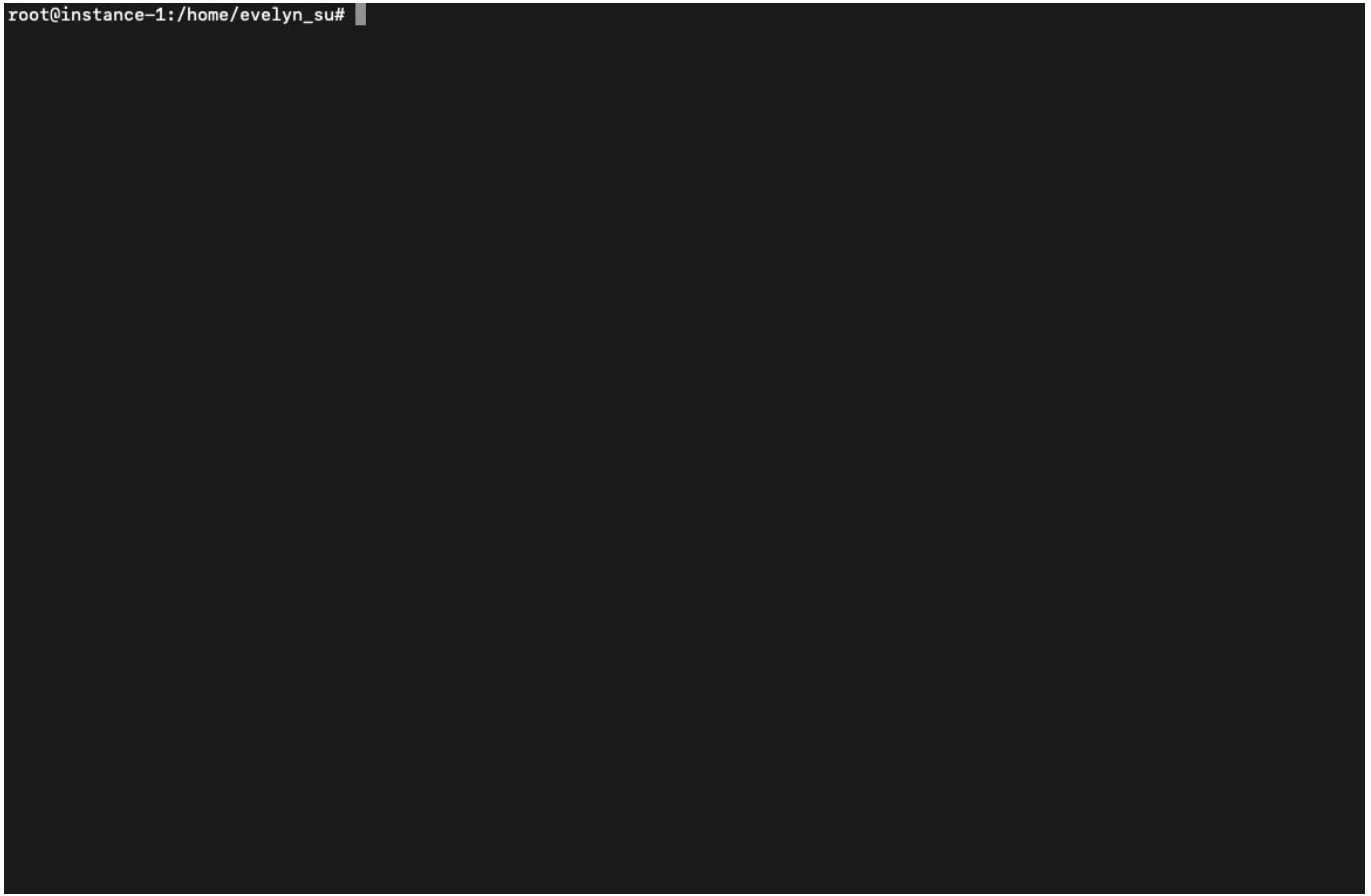
Kubernetes Secret

- 提供開發者一種存放敏感資訊的元件
- 非明碼的方式(opaque) 存放
- Base64編碼

```
$ echo -n "root" | base64
cm9vdA==

$ echo -n "rootpass" | base64
cm9vdHBhc3M=
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: demo-secret-from-yaml
type: Opaque
data:
  username: cm9vdA==
  password: cm9vdHBhc3M=
```


root@instance-1:/home/evelyn_su#

2

What is Vault

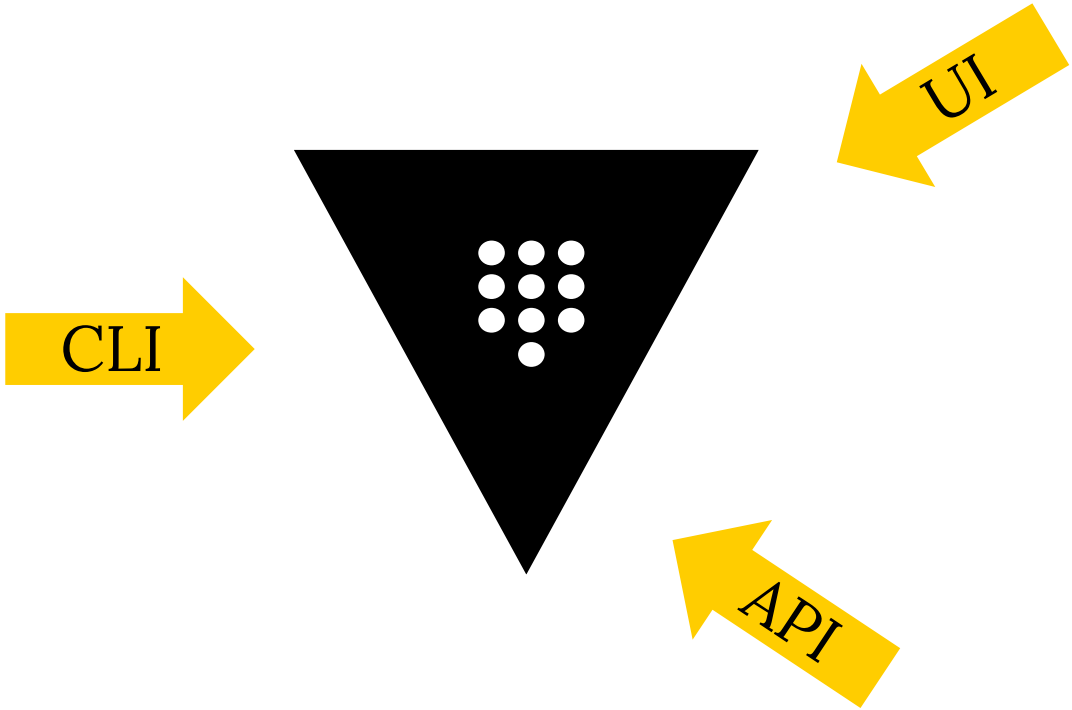
Vault is

- HashiCorp 開發用於**管理機密資料**的開源專案
- 所有儲存在 Vault 的資料都會經過**加密**
- 透過不同的帳號、Token 來限制不同的存取範圍
- 存取紀錄都會透過 Audit 模組記錄下來

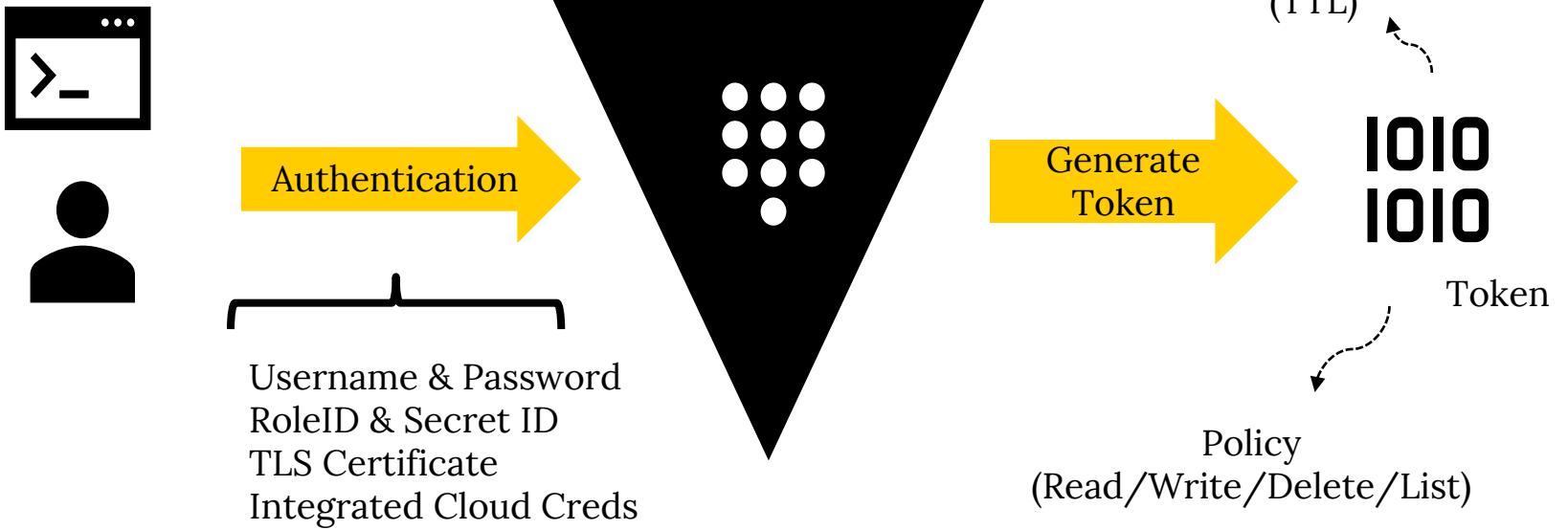
Use Cases of Vault

1. Secrets Management
2. Kubernetes secrets
3. Automated PKI Infrastructure
4. Dynamic secrets
5. Database Credential Rotation
6. Data Encryption

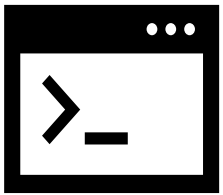
What is Vault



Token Generation



Token Usage

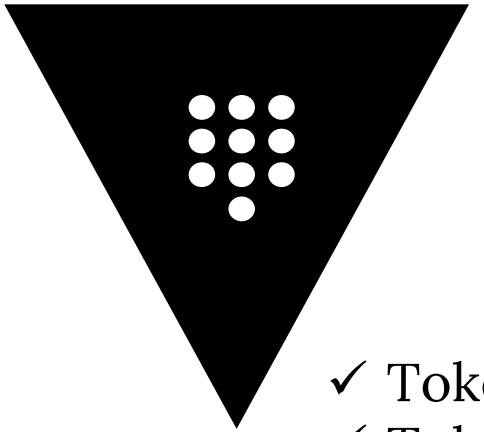


kv/apps/secret

Retrieve Data from a Path

Return Requested Data

Username: evelyn
Password: 123456789



- ✓ Token is valid
- ✓ Token is not Expired
- ✓ Token has Permission

Vault component

Vault is an intricate system with numerous distinct components.

Storage Backend

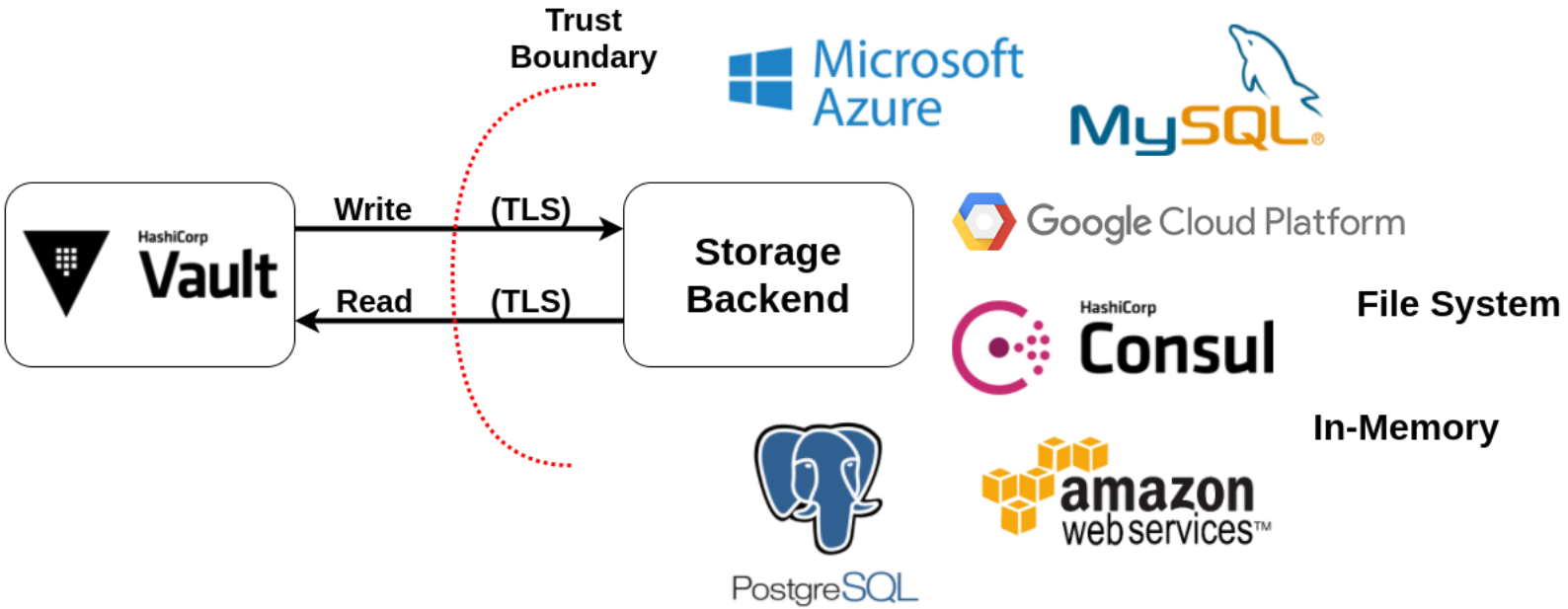
Secrets Engines

Authentication Methods

Audit Devices

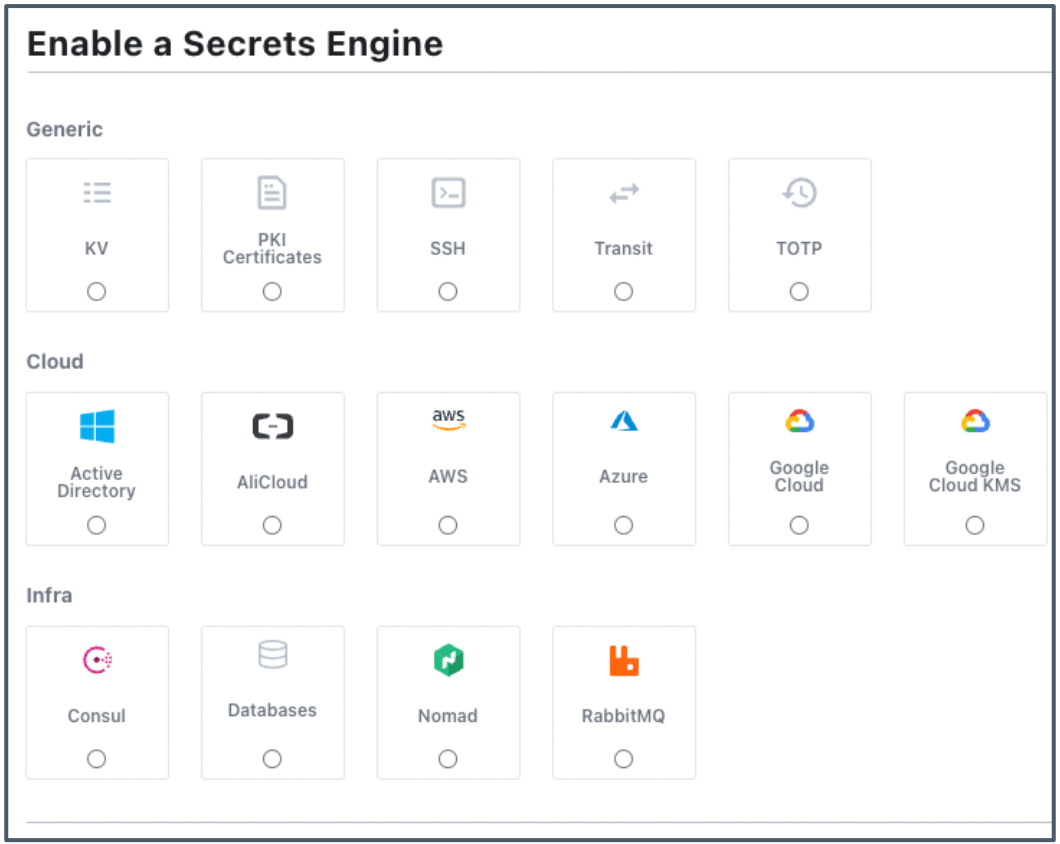
Storage Backend

- 負責**儲存**加密資料
- 所有資料傳輸過程中都使用**TLS**加密
  - 靜態資料使用**AES256**加密
- 每一個Vault Cluster只有一個storage backend
- Storage backend example:
  - Consul, Amazon S3, My SQL, in-memory, etc.


Trust
Boundary
HashiCorp
Vault
Write
(TLS)
Read
(TLS)
Storage
Backend
Microsoft
Azure
MySQL
Google Cloud Platform
HashiCorp
Consul
File System
In-Memory
amazon
web services™
PostgreSQL

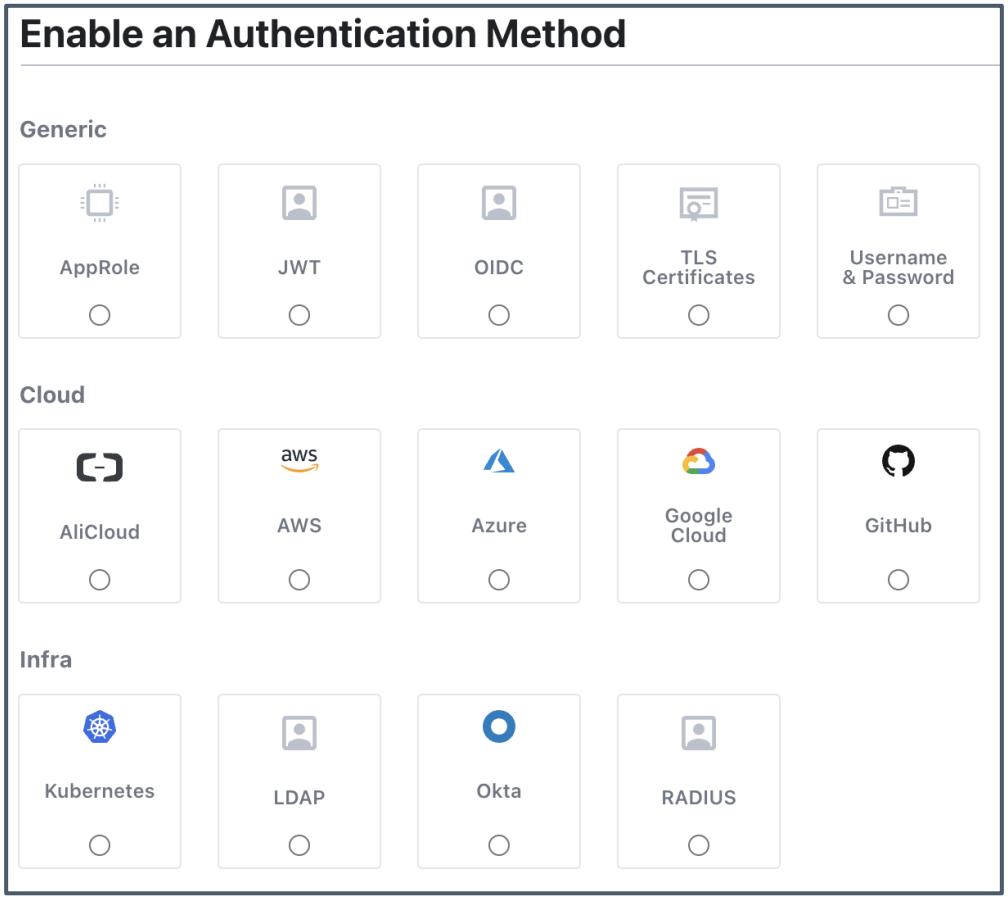
Secrets Engines

- 負責**儲存、建立、管理**Secret或者加密資料
- Secrets engines提供：
  - 儲存和讀取資料
  - 可連接到其他的Service來動態產生憑證
  - 資料加密的服務
  - 建立Certificates
- 相同類型的Secret engine可透過Path啟用或隔離


Enable a Secrets Engine
Generic
KV
PKI Certificates
SSH
Transit
TOTP
Cloud
Active Directory
AliCloud
AWS
Azure
Google Cloud
Google Cloud KMS
Infra
Consul
Databases
Nomad
RabbitMQ

Authentication Methods

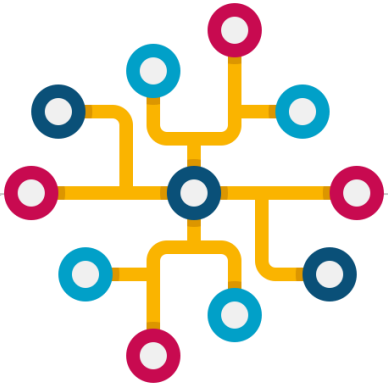
- 執行**身份驗證**及**管理**的元件
- 負責為使用者指派Identity及Policy
- 當通過身份認證，Vault會發出一組Token，用於後續的Requests
- Auth method 最基本的目地是**取得Token**


Enable an Authentication Method
Generic
AppRole
JWT
OIDC
TLS Certificates
Username & Password
Cloud
AliCloud
aws
AWS
Azure
Google Cloud
GitHub
Infra
Kubernetes
LDAP
Okta
RADIUS

Audit Devices

- 紀錄Vault所有Requests和Responses的Log
- 在寫入Log前會經過**Hash**處理
- Format為**JSON**
- 可存放在 system logs 或是其他儲存方式
- 預設 **Disable**

3 Vault Concepts

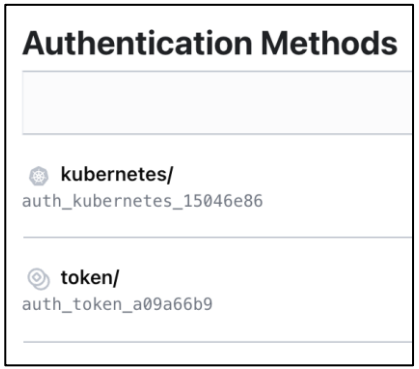


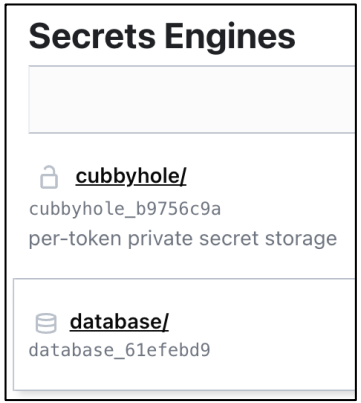
Tokens

- 是Vault進行**身份驗證核心方法**
- 可直接使用Token驗證身份
  - 或是根據外部身份驗證(Github)產生Token
- 所有對 Vault 的Requests都必須有Token
- 每個Token都會有個關聯的**Policy**和**TTL**

Paths

- 在Vault 中的所有動作都是**path-based**
- 有一些無法使用或刪除的系統保留路徑
  - auth/、sys/、secret/、 identity/、 cubbyhole/





Policy

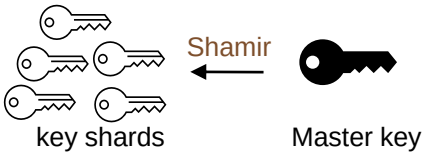
- 設定訪問權限，來管理和限制User行為及RBAC。
- 撰寫的格式是採用 HCL
- 預設為**Deny**，因此不會在系統中授予任何權限。

Policy (hcl format)

```
path "kv/data/k8s/summit" {
  capabilities = ["read"]
}
```

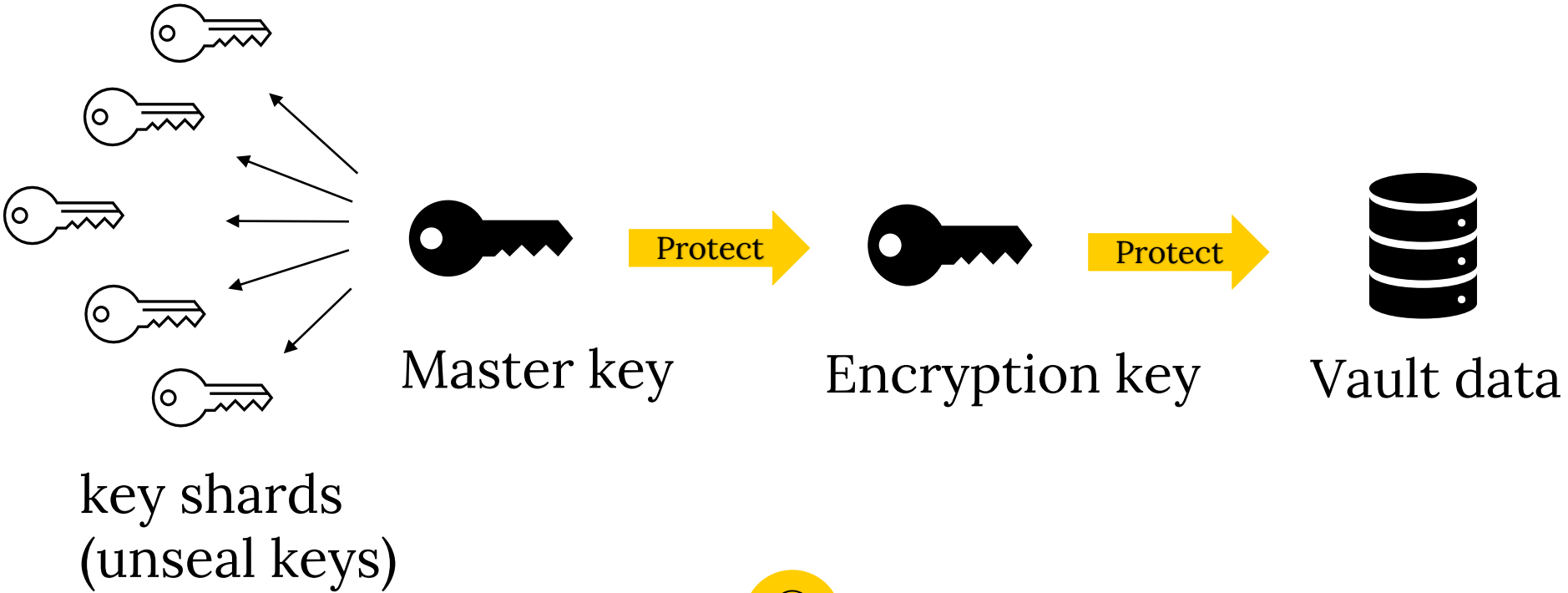
Seal

- Vault server起始狀態為Seal
- 在 Seal 狀態時**不能進行任何操作**
- 預設使用**Shamir's Secret Sharing**
- 什麼情況需要Seal Vault？
  - Key shards遭外洩
  - Vault 節點偵測到不明連線
  - 被植入惡意程式、間諜程式



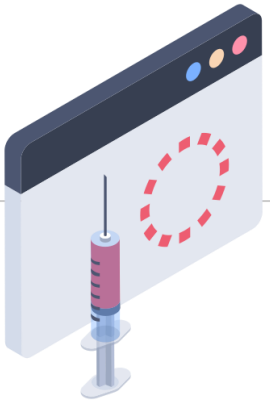
Unseal

- 重構Master key以解密Encryption key的過程。

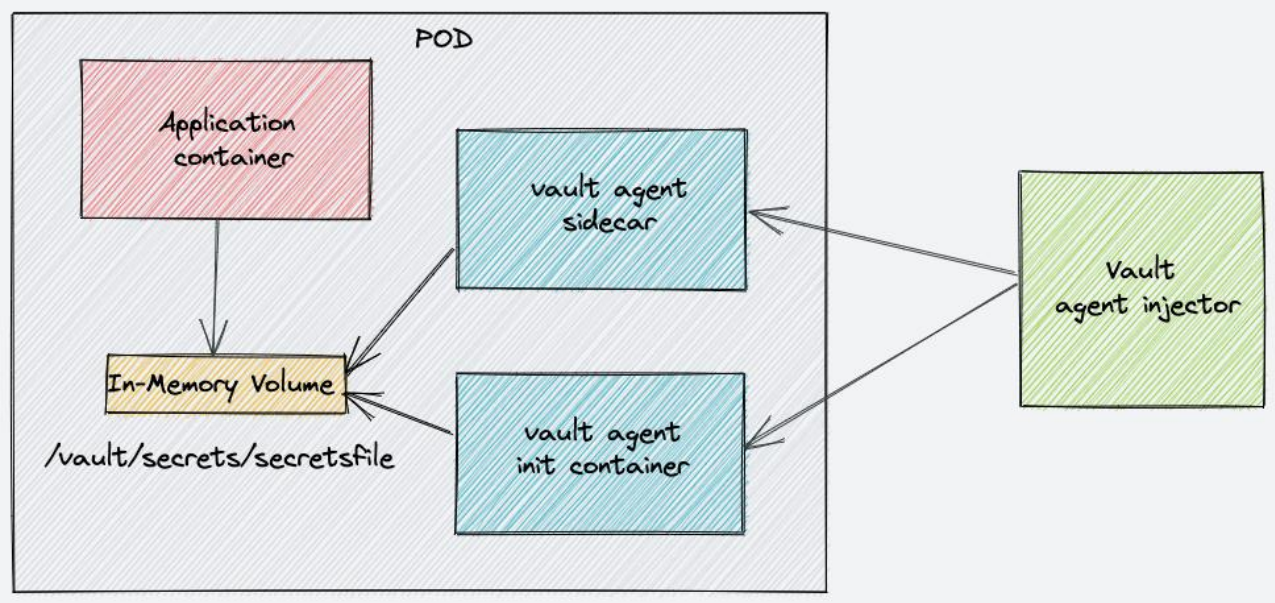

Protect
Protect
Master key
Encryption key
Vault data
key shards
(unseal keys)

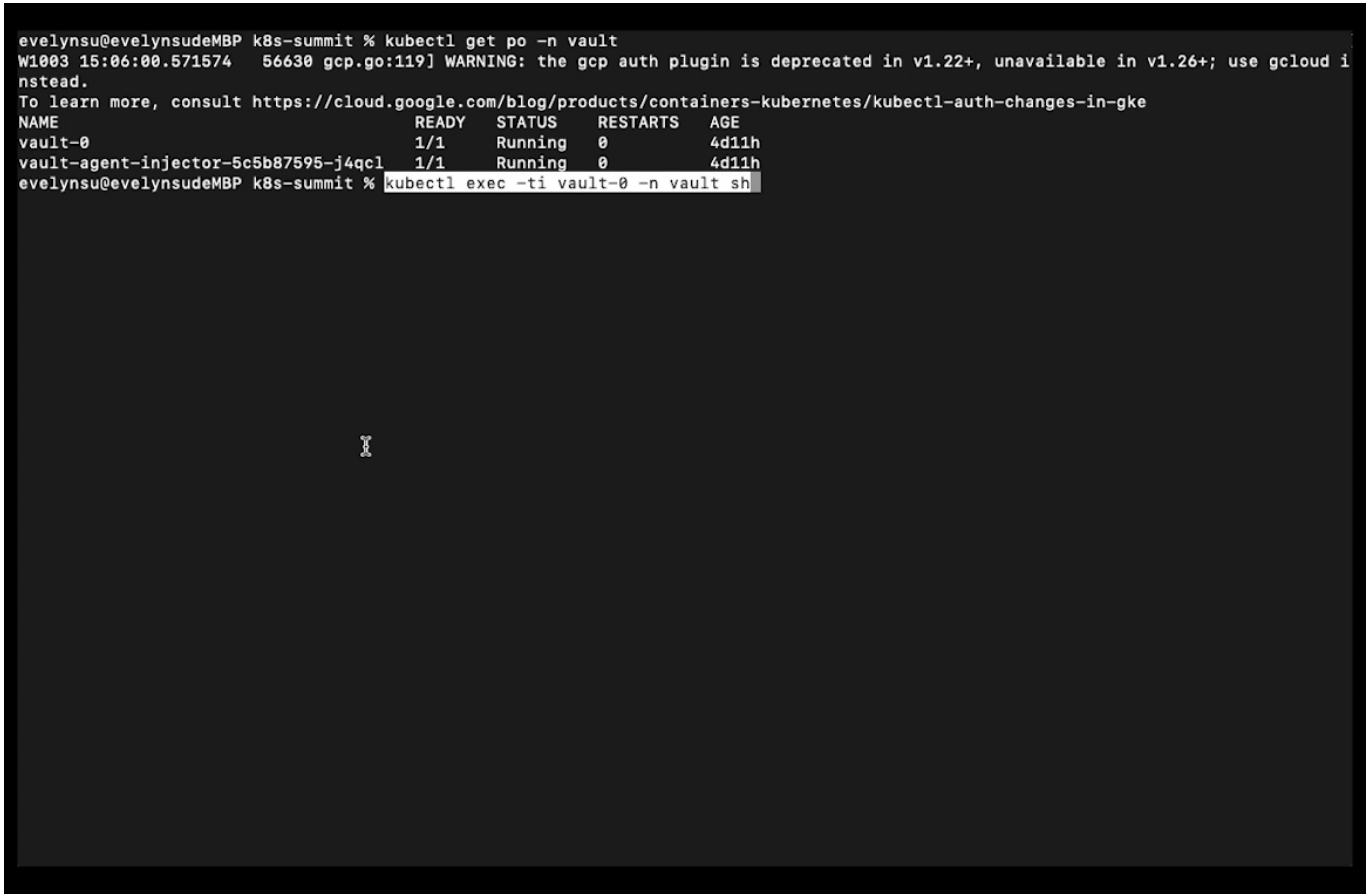
4

Vault agent injector Demo



Vault agent injector




evelynsu@evelynsudeMBP k8s-summit % kubectl get po -n vault
W1003 15:06:00.571574 56630 gcp.go:119] WARNING: the gcp auth plugin is deprecated in v1.22+, unavailable in v1.26+; use gcloud instead.
To learn more, consult https://cloud.google.com/blog/products/containers-kubernetes/kubectl-auth-changes-in-gke
NAME READY STATUS RESTARTS AGE
vault-0 1/1 Running 0 4d11h
vault-agent-injector-5c5b87595-j4qcl 1/1 Running 0 4d11h
evelynsu@evelynsudeMBP k8s-summit % kubectl exec -ti vault-0 -n vault sh

ETCD vs Vault

ETCD	Vault
Base64	 AES256

Thanks!

Any questions ?

You can find me at

- 網創資訊
- evelyn_su@netron.asia

NETRON
網 創 資 訊