Comment gérer ses secrets ?

...

Initiation à Vault

Tanguy BERNARD

Quels secrets ?

- Identifiants de connexion à une base de données
- Clés de chiffrement
- Éléments d'infrastructure (Nexus, Jenkins...)
- API tokens d’applications, de services tiers
- Identifiants AWS

Pourquoi ?

Où ? (Pas une si bonne idée)

- Stocker en clair dans le code
- Dans les variables d'environnements
- Dans une base de données
- Stocker chiffré dans le code

```
const my_super_secret="1234";
const database_user="root";
const database_password="root_lol";
```

Source: Photo by Matthew Henry from Burst

Source: http://dracos.deviantart.com/#/d2y5ele

Des secrets un peu partout

Solution: les gestionnaires de secrets

- AWS Secrets Manager
- Google Cloud Secret Manager
- Azure Key Vault
- Hashicorp Vault
- Keywhiz

Hashicorp Vault

Les services

- Secret (Accessible via l'API)
- Audit
- Storage
- Auth Backend

Secrets plugin

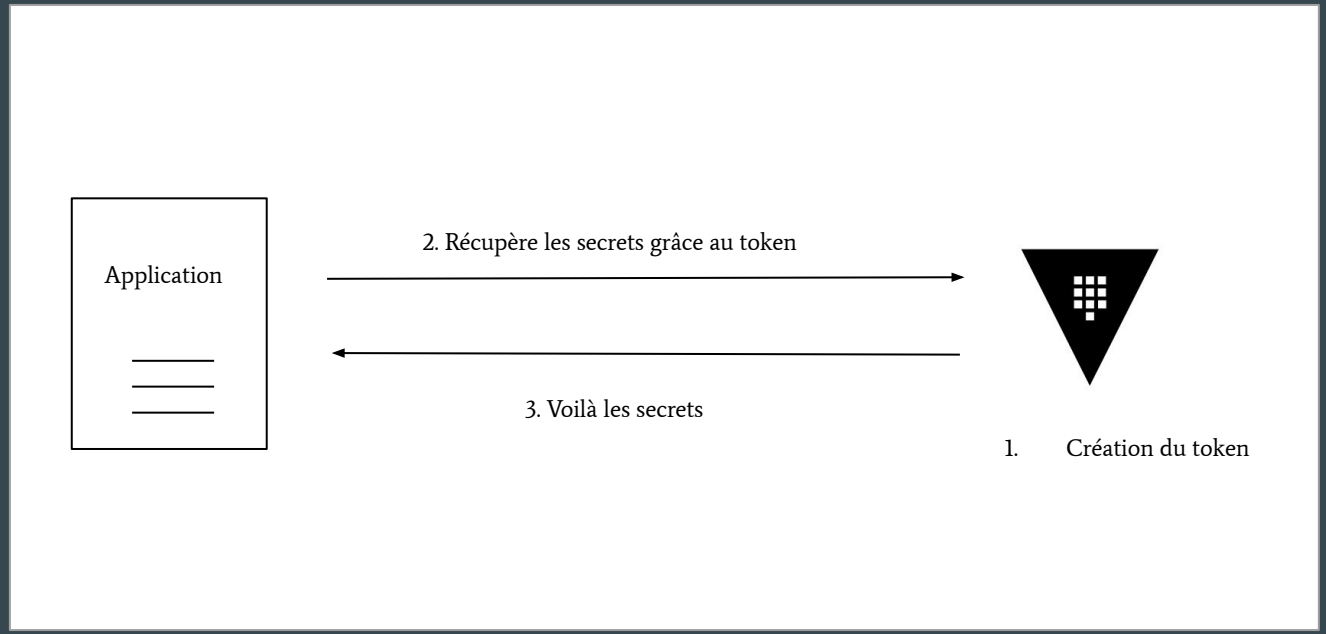
source: http://ippon26.rssing.com/chan-40092195/all_p19.html

Authentification ?

- AppRole
- JWT / OIDC
- LDAP
- AWS
- Github
- Azure
- Google Cloud
- Kubernetes

Source: Photo by Nicole De Khors from Burst

Cas d’utilisation, simple

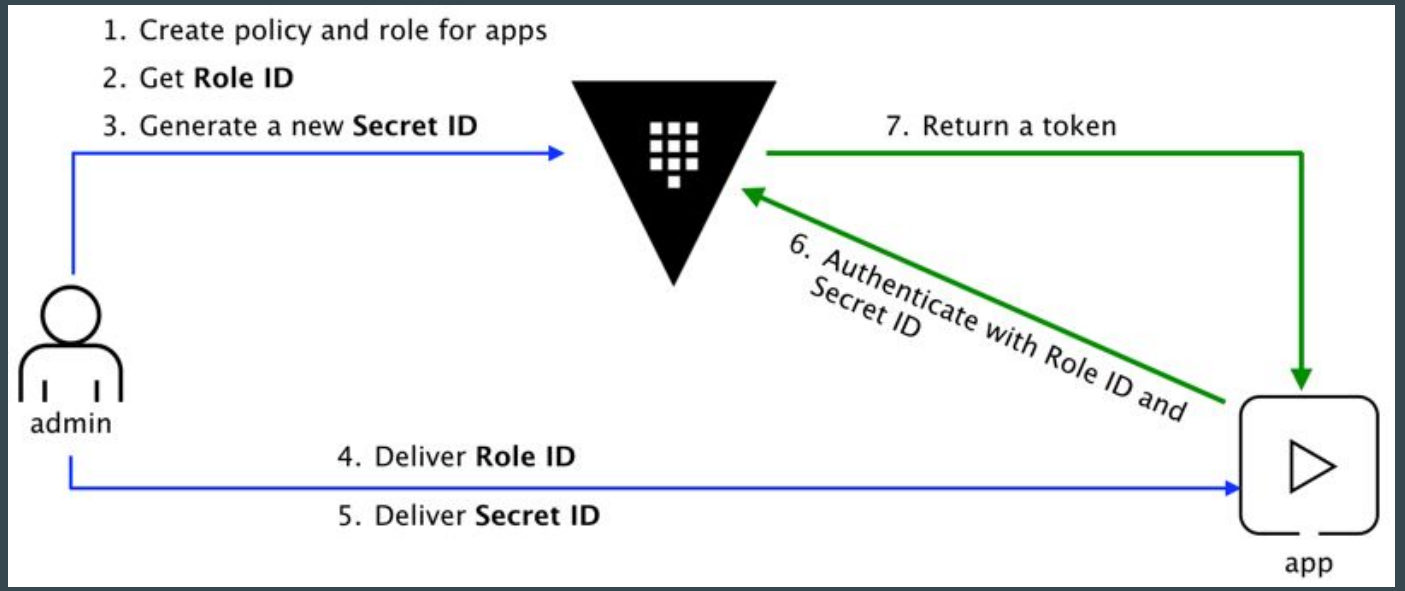


That's the sound of da police!

CRUD... L

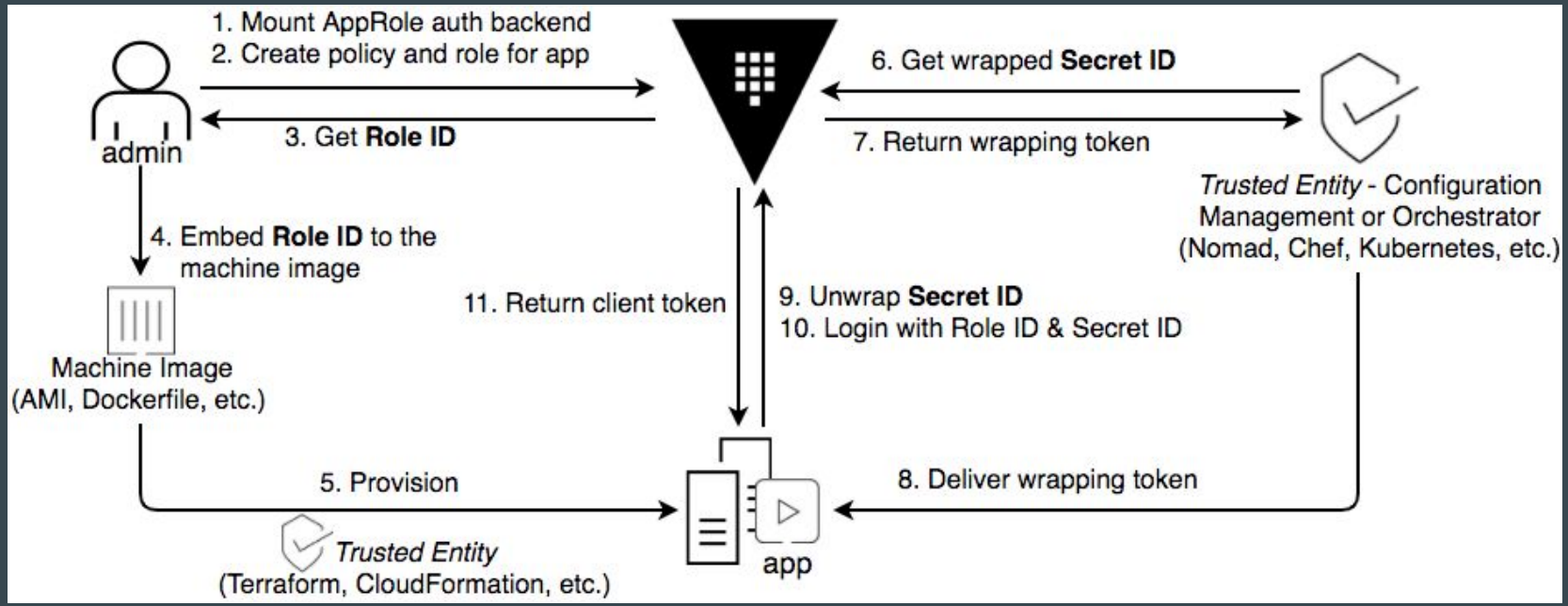
Source: Photo by Shopify Partners from Burst

Approle



source: https://learn.hashicorp.com/vault/identity-access-management/approle

Cas d'utilisation ++



Source: https://www.hashicorp.com/blog/authenticating-applications-with-vault-approle/

DEMO

MERCI