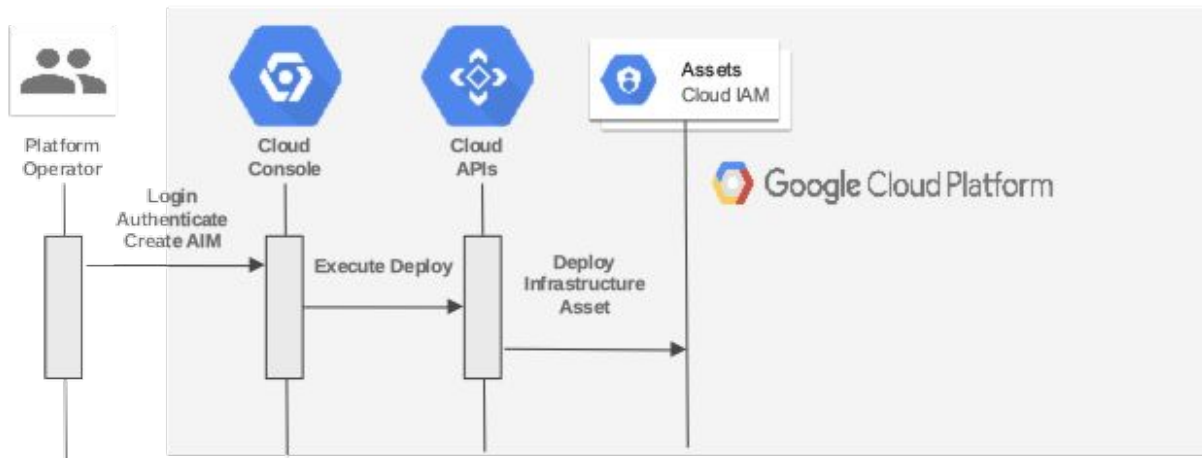# Vault on GKE Demo

victorhdamian@gmail.com 207-712-6330

IAM Infrastructure Development & Deployment Use Case
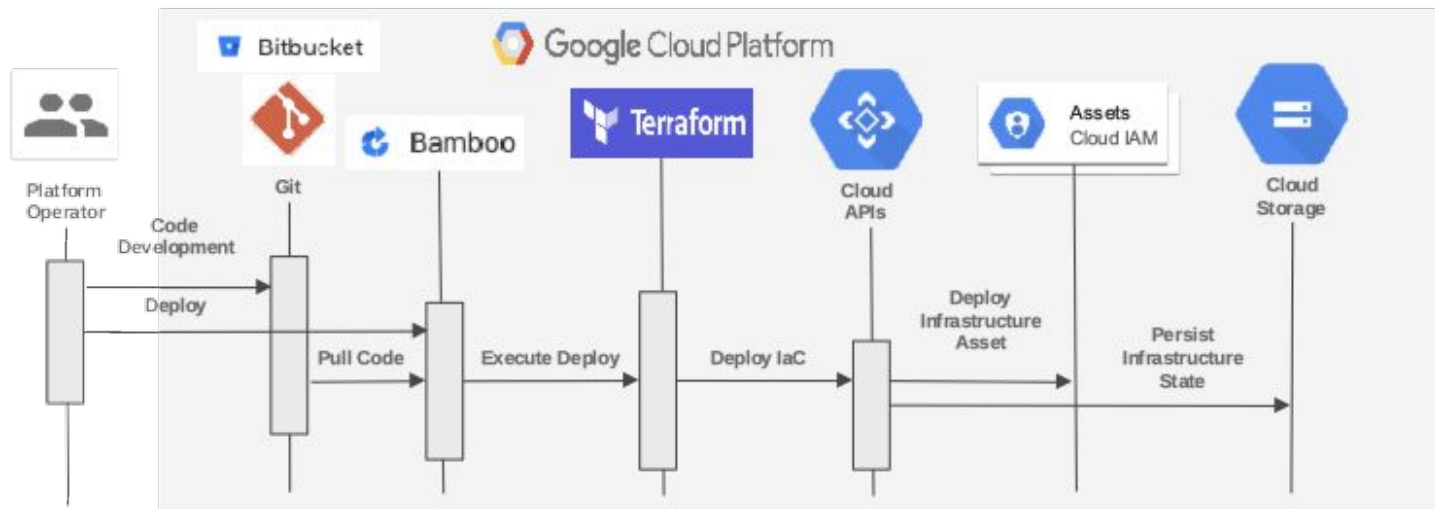
Current State:
UI diven
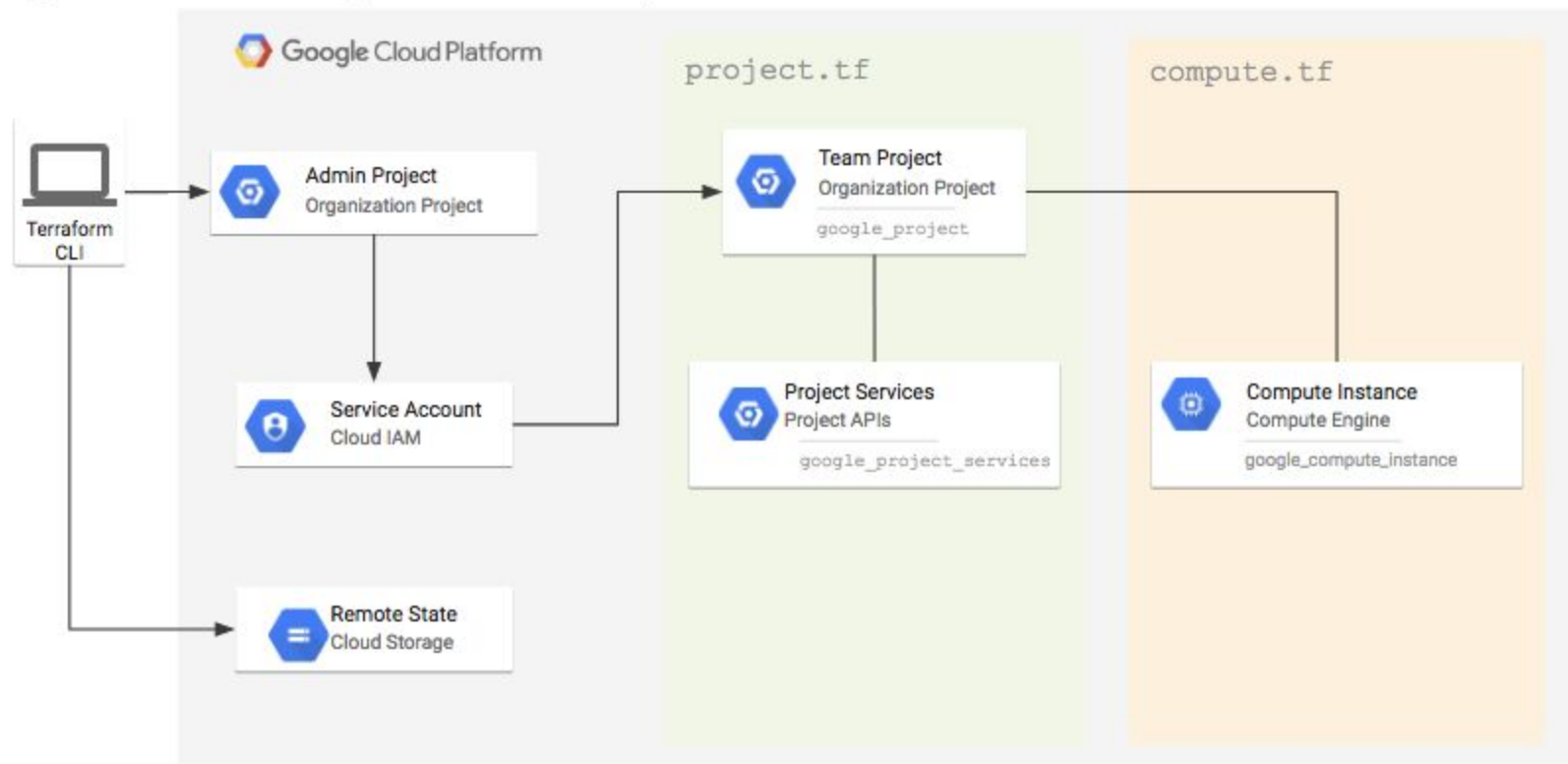Manual
Hard to Scale
Intellectual Property volatility

Future State:
DevOps lifecycle
IaC
State Persistence
Scalable
Reproducible
IP retention

Architecture diagram for tutorial components:

Figure 1. *Architecture diagram for tutorial components*

Vault adoption

The Vault adoption has the following three primary objectives in our technology stack

- CENTRALIZE: SECRET MANAGEMENT
- ENCRYPT: SECRETS AT REST AND IN TRANSIT
- PROVIDE: SECRETS AS A SERVICE
- PROVIDE: ENCRYPTION AS A SERVICE
- Authentication Methods: Auth methods are the components in Vault that perform authentication and are responsible for assigning identity and a set of policies to a user/machine.

Vault Capabilities
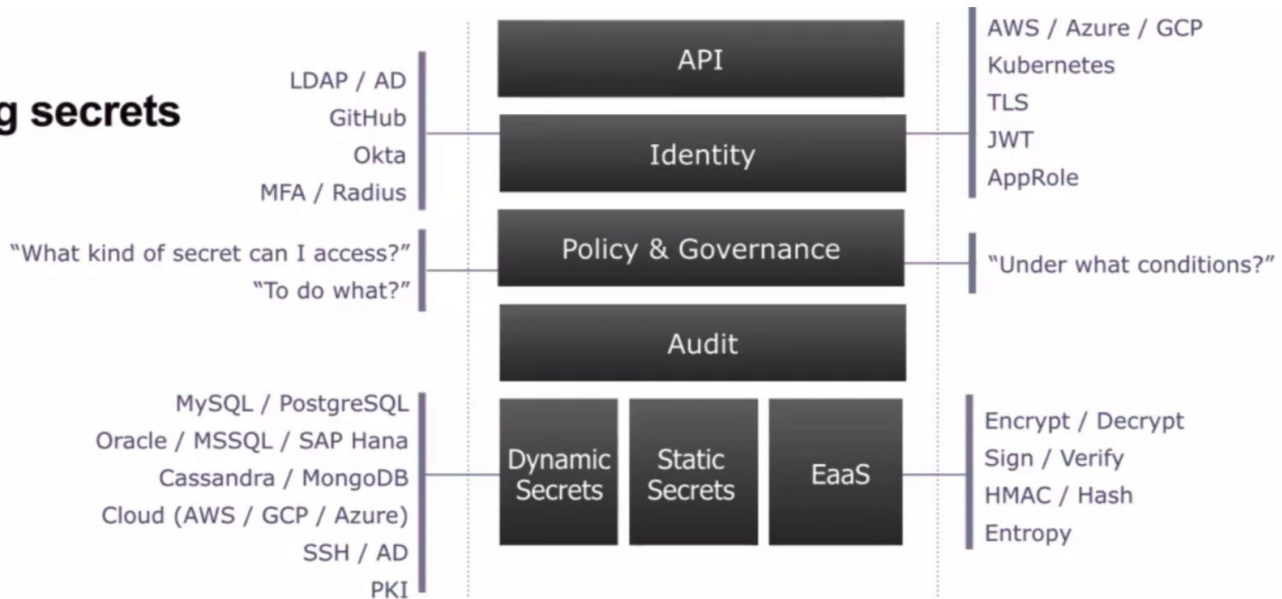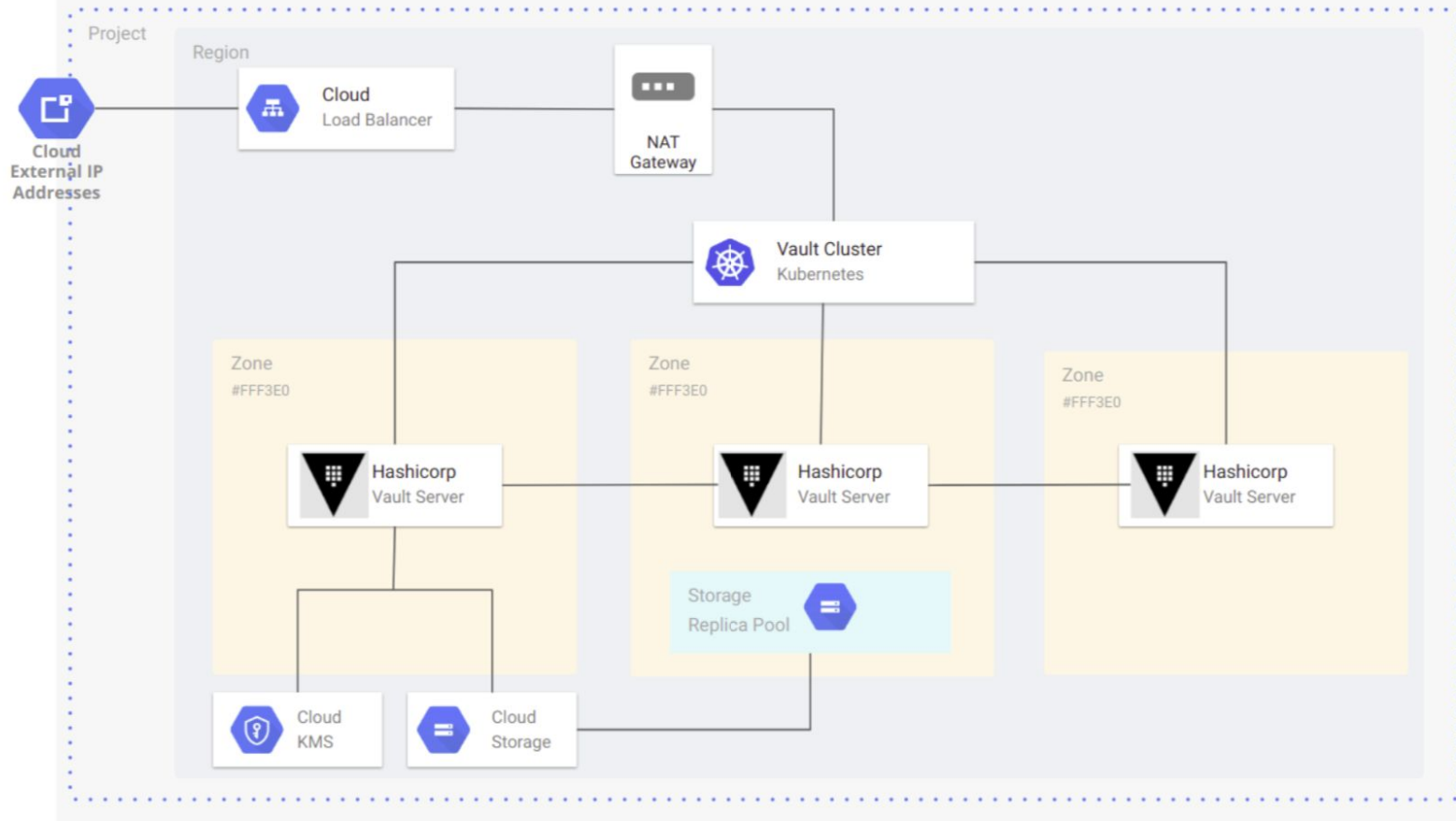
Vault Integration Reference Architecture

Platform Heavy Reference Architecture

- K8s Patters: Sidecar, Init container, JWT secret
- Vault Patterns: Auth Kubernetes, AppRole


```
vault write auth/kubernetes/config \
    kubernetes_host="${K8S_HOST}" \
    kubernetes_ca_cert="${K8S_CACERT}" \
    token_reviewer_jwt="${TR_ACCOUNT_TOKEN}"
```

Vault Client Project

Kubernetes Engine

Token Reviewer

User or Machine

Vault Service Project

Kubernetes Engine

Vault API

Auth Method Kubernetes

Secret Enging

Send JWT token

Verify information

Verify information

Map policy to metadata

Return Vault token

Read secret

```
apiVersion: apps/v1
kind: Deployment
initContainers:
- name: vault-authenticator
spec:
   shareProcessNamespace: true
containers:
- name: app-web
- name: sumologic
- name: fluent
- name: consul-template
```

```
path "secret/policies/policy-guideline_app" {
  capabilities = ["read", "list"]}
path "secret/policies/policy-guideline_app" {
  capabilities = ["read", "list"]}
path "secret/guideline_app/config_loader/btc" {
  capabilities = ["read", "list"]}
```

```
{
  "sftp_host": "prLGcTORpY7gt5yLIN7a8lA91PLT55",
  "sftp_username": "sKUAGfxKCToHeARAaLeXPQ==",
  "sftp_password": "JpCCwu/ovnOUmrRpp9FCzSnU"
}
```