Managing Vault with Terraform

Jacob Mammoliti

Consultant at Arctiq Inc.

What Are We Trying to Solve Here?

- Deploy full Vault clusters through Terraform
- Make changes to Vault configurations with an infrastructure-as-code mentality
- Replicate an environment to test in a some other “Sandbox” environment
- Store static Vault configurations as code in some SCM tooling

About Me

Jacob Mammoliti
@ArctiqJacob

I’m a consultant at Arctiq Inc. out of Toronto, Canada. I focus on enabling customers with HashiCorp tooling, specifically Terraform, Vault and Consul. I also spend a lot of time in the microservices space working with all things Kubernetes.

Vault Terraform Provider

- Allows Terraform to read from, write to, and configure Vault
- The provider is best used to configure and manage Vault policies and static Secrets Engines
- Provides a way to store basic Vault configuration as code in an SCM repository

Demo Workflow

1. Stand up a GKE cluster and install Vault through the official HashiCorp Helm Chart with Terraform
2. Initialize and Unseal Vault
3. Configure Vault with initial policies, an Auth Method, and KV Secrets Engines with Terraform

Deploy Vault in K8s

Use the official Helm Chart from HashiCorp to deploy a production grade Vault cluster.

TERMINAL

```
$ terraform apply -var-file=main.tfvars
An execution plan has been generated and is shown
below.
...
Apply complete! Resources: 3 added, 0 changed, 0
destroyed.

Outputs:

vault_address = https://vault.domain.local:8200
```

Sample TF Code

Terraform can create policies and enable Secrets Engines in Vault.

CODE SNIPPET

```
resource "vault_auth_backend" "userpass" {
  type = "userpass"
}

resource "vault_policy" "admin_policy" {
  name   = "admins"
  policy = file("policies/admin_policy.hcl")
}

resource "vault_policy" "dev_policy" {
  name   = "developers"
  policy = file("policies/dev_policy.hcl")
}
```

Best Practices to Keep in Mind

- Terraform State should be stored in an encrypted remote storage backend (AWS Encrypted S3 bucket, Google Cloud Storage Bucket, etc.)
- Use caution when using Terraform to write sensitive data such as Cloud or Database credentials

Demo!