**Vault, IaC (Terraform) and Azure**

Injecting Secrets into Terraform Using the Vault Provider

Diagram

Description automatically generated

**Prerequisites:**

1. Terraform installed locally
2. Vault installed locally
3. Azure account and Service Principal / MSI

**Configuration Steps :**

1. Start Vault server

Cmds:

1. vault server -dev
2. export VAULT\_ADDR='http://127.0.0.1:8200'
3. export VAULT\_TOKEN="hvs.xxxxxxxxxxxxxxxxxxxxxx"
4. vault status

**Note**: VAULT\_ADDR and VAULT\_TOKEN values will get when we execute the “vault server -dev” command

Text

Description automatically generated

Text

Description automatically generated

Step 2: The vault server should now be up. Navigate to **127.0.0.1:8200 /** **localhost:8200** and log in with your root token.

Graphical user interface

Description automatically generated

Step 3: We need to set Terraform Variables substituting (Environment variables)

ARM\_ SUBSCRIPTION\_ID = “XXXXXXXXXXXXXXXXXX”

ARM\_TENANT\_ID = “XXXXXXXXXXXXXXXXXX”

ARM\_CLIENT\_ID = “XXXXXXXXXXXXXXXXXX”

ARM\_CLIENT\_SECRET = “XXXXXXXXXXXXXXXXXX”

Step 3: In this configuration, we have two parts 1) Vault Admin 2) Terraform Operator

1. Vault Admin:
2. Provides for azure secrets creation in Vault

A screenshot of a computer

Description automatically generated

1. Azure secret backend and role creation

A screenshot of a computer

Description automatically generated

1. Terraform commands:

terraform init

terraform validate

terraform plan

terraform apply -auto-approve

Text

Description automatically generated

1. Vault server Output



1. Terraform Operator:

Creation of Resources in Azure cloud by using dynamic credential

1. Providers

A screenshot of a computer

Description automatically generated

1. Get dynamic credentials from the state file in vault admin for azure access

A screenshot of a computer

Description automatically generated

Note:

1. CLI command to read azure dynamic credentials

vault read azure/creds/<role-name>

vault read azure/creds/admin

1. Terraform state file stored locally in the above example.