**Terraform + Vault Step-by-Step Tutorial**

This tutorial will cover:

1. Setting up Vault
2. Configuring Vault secrets
3. Writing Terraform code to fetch secrets from Vault
4. Running Terraform with Vault integration

**Step 1: Install Prerequisites**

* Install **Terraform** → Download
* Install **Vault** → Download
* Have **Docker** (optional for running Vault quickly)

Check versions:

terraform -v

vault -v

**Step 2: Start Vault (Dev Mode for Lab)**

Run Vault in **dev mode** (easy for learning, not for production):

vault server -dev -dev-root-token-id="root"

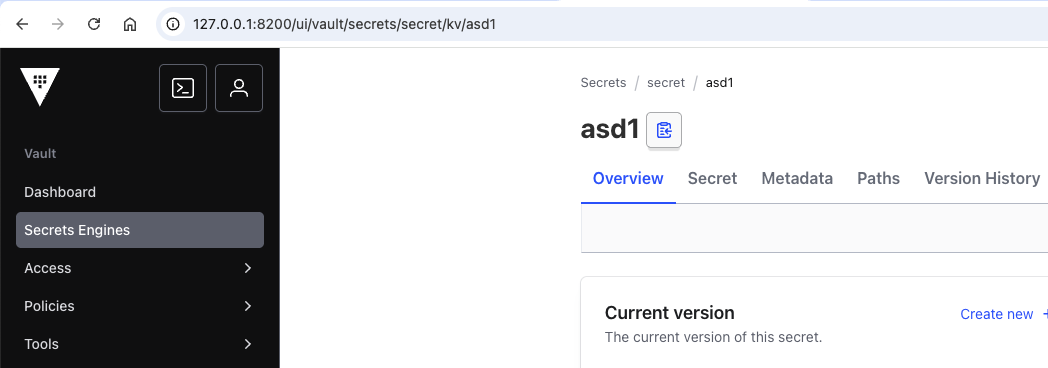
This runs Vault locally at:  
👉 http://127.0.0.1:8200  
with token root.

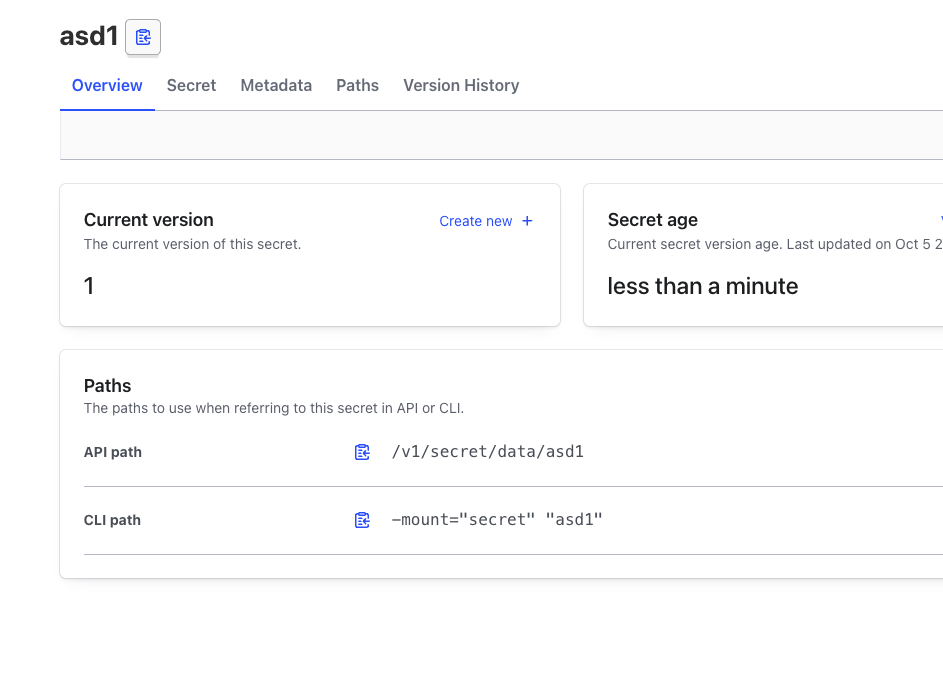
Export environment variables so Terraform can talk to Vault:

export VAULT\_ADDR='http://127.0.0.1:8200'

export VAULT\_TOKEN='root'

**Step 3: Store a Secret in Vault**

****

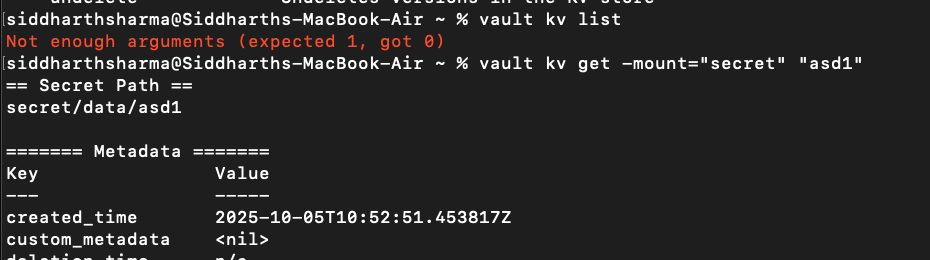
****

Enable kv secrets engine and add a secret:

vault secrets enable -path=secret kv-v2

vault kv put secret/aws access\_key=MYACCESSKEY secret\_key=MYSECRETKEY

Verify:



vault kv get secret/aws

**Step 4: Create Terraform Configuration**

Create a main.tf file:

terraform {

required\_providers {

vault = {

source = "hashicorp/vault"

version = "~> 3.0"

}

}

}

provider "vault" {

address = "http://127.0.0.1:8200"

token = "root"

}

# Read AWS credentials from Vault

data "vault\_kv\_secret\_v2" "aws\_creds" {

mount = "secret"

name = "aws"

}

output "aws\_access\_key" {

value = data.vault\_kv\_secret\_v2.aws\_creds.data["access\_key"]

}

output "aws\_secret\_key" {

value = data.vault\_kv\_secret\_v2.aws\_creds.data["secret\_key"]

sensitive = true

}

**Step 5: Initialize & Apply Terraform**

terraform init

terraform apply

You’ll see:

aws\_access\_key = "MYACCESSKEY"

aws\_secret\_key = (sensitive)

**Step 6: Use Secrets in Terraform Resources**

Example: provision AWS provider using Vault secrets.

provider "aws" {

region = "us-east-1"

access\_key = data.vault\_kv\_secret\_v2.aws\_creds.data["access\_key"]

secret\_key = data.vault\_kv\_secret\_v2.aws\_creds.data["secret\_key"]

}

resource "aws\_s3\_bucket" "example" {

bucket = "my-vault-terraform-demo"

acl = "private"

}

Then:

terraform apply

✅ This will create an S3 bucket using credentials pulled securely from Vault.

**Step 7: Cleanup**

* Destroy resources:
* terraform destroy
* Stop Vault dev server.