NULLCON

Secrets Management using Hashicorp Vault

By Rohit Salecha

#whoami

NULLCON

Rohit Salecha

- Associate Director @ **NotSoSecure**
- 9+ years of experience in Information Security
- Featured in ‘50 Influential DevSecOps Professionals in 2019’ - Peerlyst
- Has expertise in Pentesting (Web, Mobile, Infra) and Application Development in Java,Python,PHP
- Certifications: CISSP,OSCP
- Trainer/Speaker : BlackHat (BWH),Nullcon,Global OWASP APPSEC
- https://rohitsalecha.com (@salecharohit on social platforms)

Agenda

- Why Secrets Management ?
- Introduction to Hashicorp Vault(Vault)
- Setting Up Vault – Installation and Configuration
- Adding and Reading Credentials
- Creating Policies
- Rotating Credentials
- Vault Conceptual Architecture

Why Secrets Management ?

- DevOps automation requires storage of sensitive information like passwords, ssh keys, auth tokens, certificates etc…
- Generally this information is available in clear-text stored in files on developer machines, environment variables, configuration files etc...
- Owing to the open nature of DevOps this information may be accessible to a good majority of people

Introduction to Hashicorp Vault

- Open Source tool for managing secrets and applying access control access control rules on who can access them
- Uses a token based approach to fetch secrets
- Dynamic Secret generation

HashiCorp Vault

Setting Up Vault – Installation

- Vagrant 2.2.6 +
- VirtualBox 6.0 +
- `vagrant up`

```
➜  Secrets_Management_Vault vagrant up
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'ubuntu/bionic64'...
==> default: Matching MAC address for NAT networking...
==> default: Checking if box 'ubuntu/bionic64' version '20191218.0.0' is up to date...
==> default: Setting the name of the VM: hashvault
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
    default: Adapter 2: hostonly
==> default: Forwarding ports...
    default: 22 (guest) => 2222 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
==> default: Booting VM...
==> default: Waiting for machine to boot. This may take a few minutes...
    default: SSH address: 127.0.0.1:2222
    default: SSH username: vagrant
    default: SSH auth method: private key
```

Setting Up Vault – Configuration

- `vault status`
- `vault operator init`
- `vault operator unseal`
- `vault login`
- http://192.168.30.110:8200/ui/vault/secrets

Adding and Reading Credentials

- `vault secrets enable kv`
- `vault kv put kv/database/mysql username=root password=toor`
- `vault kv get kv/database/mysql`
- `VAULT_TOKEN=s.WlaFHAyExaM4s5M30PNqZ652`
- `curl -X GET -H "X-Vault-Token:$VAULT_TOKEN" http://192.168.30.110:8200/v1/kv/database/mysql`
- https://www.vaultproject.io/api/libraries.html

Creating Policies

- echo 'path " kv/database/mysql" { capabilities = ["read","list"] }' | vault policy write mysqldb -
- vault token create -policy=mysqldb -format=json | jq -r '.auth.client_token'

```
vagrant@vault:~$ vault token create -policy=mysqldb -format=json
{
  "request_id": "13b0d100-2501-f200-ee79-c1488f07dbfd",
  "lease_id": "",
  "lease_duration": 0,
  "renewable": false,
  "data": null,
  "warnings": null,
  "auth": {
    "client_token": "s.oIcURVWo1OlIyHwL91SLBQ3h",
    "accessor": "b1GfnbFGwPwNwP0MKKlAay9H",
    "policies": [
      "default",
      "mysqldb"
    ],
    "token_policies": [
      "default",
      "mysqldb"
    ],
    "identity_policies": null,
    "metadata": null,
    "orphan": false,
    "entity_id": "",
    "lease_duration": 15,
    "renewable": true
  }
}
```

Renewing Tokens

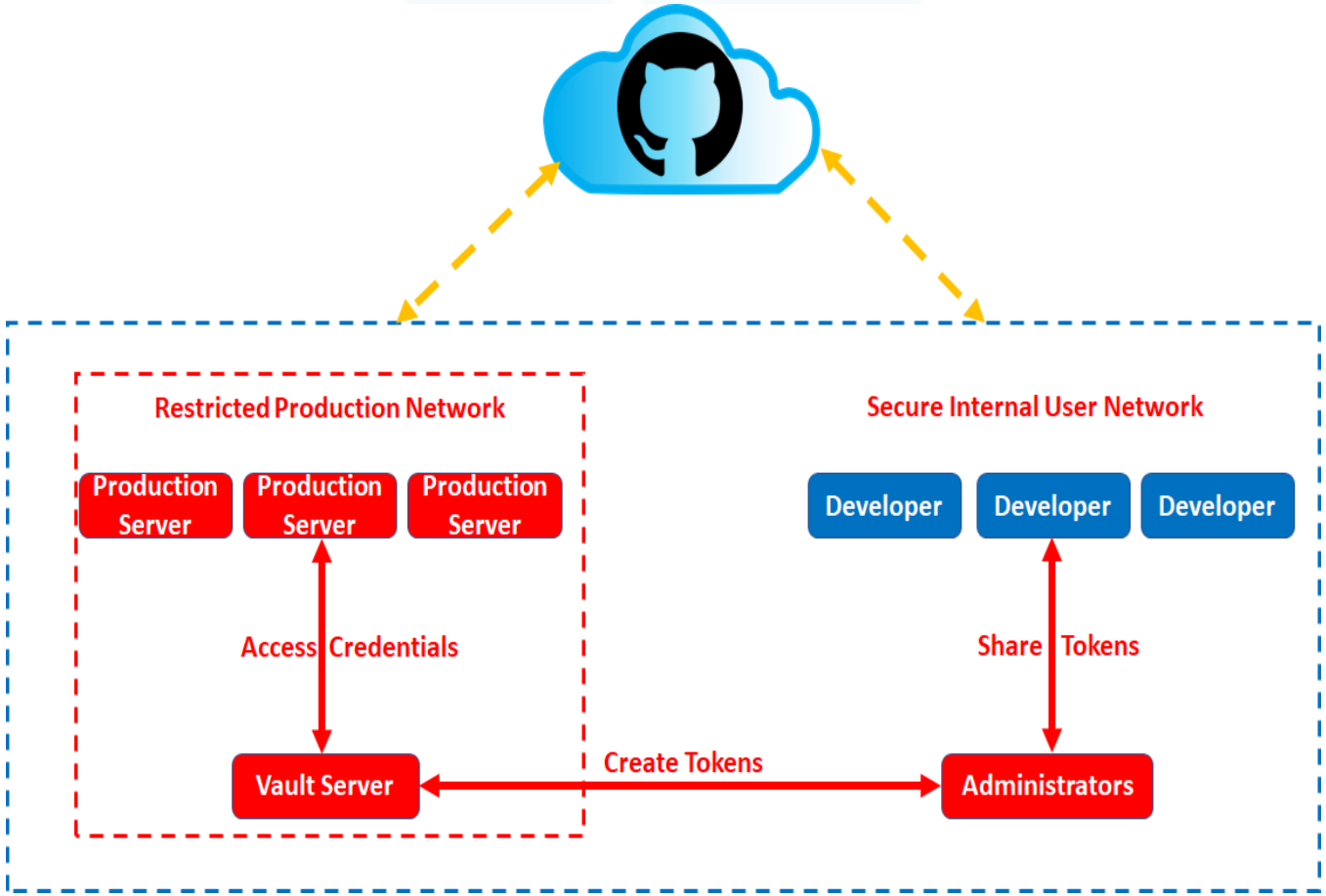
- `vault token create -policy=mysqldb -format=json -ttl=15s`
- `vault token renew <token>`
- `vault token renew -accessor <access_token>`
- Cannot Renew once token is expired

```
vagrant@vault:~$ vault token renew -accessor b1GfnbFGwPwNwP0MKKlAay9H
Error renewing token: Error making API request.

URL: POST http://127.0.0.1:8200/v1/auth/token/renew-accessor
Code: 400. Errors:

* 1 error occurred:
        * invalid accessor
```

Vault Conceptual Architecture



Thank you

@salecharohit