Vault

Implementation Foundations

Module 12: Static Secrets

What You Will Learn

- Secrets Engines Overview
- Static Secrets

Secrets Engines

What Are Secrets Engines

The component of vault responsible for a secret's lifecycle

Secrets are pieces of sensitive information that can be used to access:

- Infrastructure
- Data
- Resources (Databases, Cloud Services)

There are two types of vault secrets engines:

- Static Secrets
- Dynamic Secrets

Static Versus Dynamic

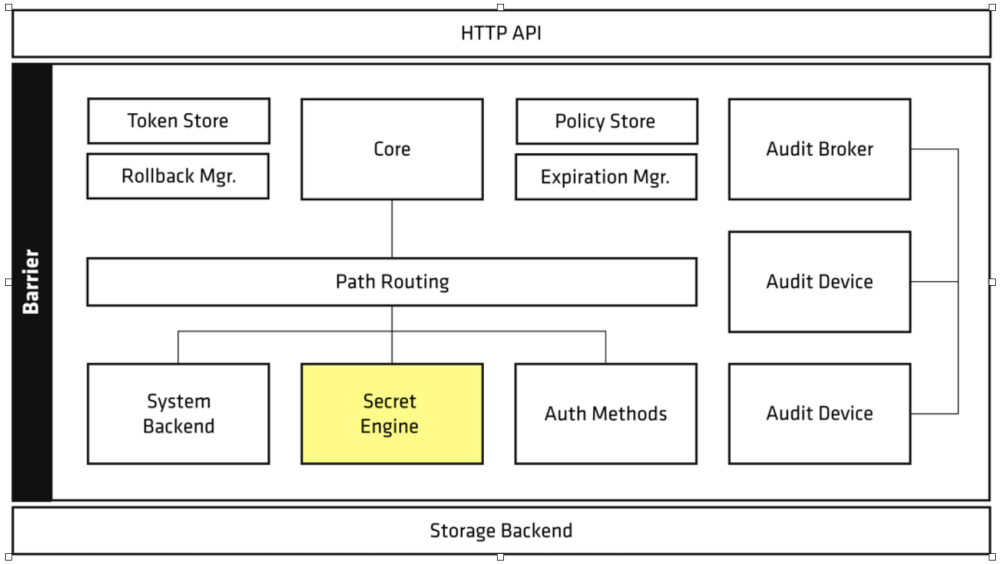
Static Secrets: Secret material that is generated outside of vault

- Username/Password
- PKI
- Encryption Keys

Dynamic Secrets: Just in time generation of secret material

- API Keys
- Database Credentials
- Encryption

How Secrets Engines Work



Secrets Engine Workflow

- When enabled the secret engine is assigned a UUID
- This UUID becomes the root folder at the disk level
- Vault does not support relative pathing
- Creates isolation between secrets engines

Secrets Engine Base Setup

Engines need to be enabled

```
$ vault secrets enable <SECRET_ENGINE>
```

Secrets Engine Base Setup

Engines need to be enabled

```
$ vault secrets enable <SECRET_ENGINE>
```

Using the path options allows for multiple configuration of an engine

```
$ vault secrets enable -path=<END_POINT> <SECRET_ENGINE>
```

Secrets Engine Base Setup

Engines need to be enabled

```
$ vault secrets enable <SECRET_ENGINE>
```

Using the path options allows for multiple configuration of an engine

```
$ vault secrets enable -path=<END_POINT> <SECRET_ENGINE>
```

Using namespaces allows for consistant pathing

```
$ vault secrets enable -namespace=<NAMESPACE> \
        -path=<END_POINT> <SECRET_ENGINE>
```

Things Of Note

- They are disabled by default
- They must be linked to a path
- They are logically isolated from each other
- They cannot be enabled more than once on the same path
- Namespaces allow for multiple implementations of the same secrets engine on the same path (Just different namespaces)

List of Vault Secrets Engines

Secrets Engine	Description
Cubbyhole	Short-term arbitrary secrets scoped to a token
Static Secrets	Stores static secrets
Active Directory	AD password rotation and credential checkout
Cloud Credentials	Create API access keys based on IAM roles
Databases	Generates dynamic database credentials
KMIP	Vault supports the KMIP protocol for key management
Transit	Encryption Services and Key generation
Advanced Data Protection	Format preserving tokenization and data tokenization
PKI	Generates on demand X.509 certificates
SSH	Generates dynamic SSH access for systems

For a complete list of secret engines visit vault.io

Static Secrets

Static Secrets Overview

- Key/Value secrets engine is used to store arbitrary secrets
- There are two versions: v1 (kv), v2 (kv-v2)
- Secrets are accessible via interactive or automated means
- Enforced access control via policies
- Fully audited access
- Encrypted using 256-bits AES in GCM mode with a randomly generated nonce prior to writing them to its storage backend

Static Secrets Overview

- Key/Value secret engine can be enabled at different paths
- Each key/value secret engine is isolated and unique
- Secrets are stored as key-value pairs
- Writing to a key in the key/value secret will replace the old value
- Sub-fields are not merged together
- Can upgrade from v1 to v2 but not the other way

Command Comparison: V1/V2

Operation	CLI command for K/V v1	Endpoint for K/V v2
Write	vault kv put <path> key=data	vault kv put <path> key=data
Read	vault kv get <path>	vault kv get <path> or vault kv get -version=<ver> <path>
Delete	vault kv delete <path>	vault kv delete <path> or vault kv delete -versions=<ver> <path>
List	vault kv list <path>	vault kv list <path>
Undelete	N/A	vault kv undelete -versions=<ver> <path>
Destroy	N/A	vault kv destroy -versions=<ver> <path>
Patch	N/A	vault kv patch <path> key=data
Rollback	N/A	vault kv rollback -version=<ver> <path>

Note: KV2 should be used as the default due to the versioning features.
V1 is discussed only for reference.

Chapter Summary

- Secret Engines are the center of Vault's secret capabilities
- There are two static Engines
  - KVv1
  - KVv2
- Engines have tunable configurations

Reference links

- KV Overview
- KV 1
- KV 2

Vault Static Secrets Module Complete!