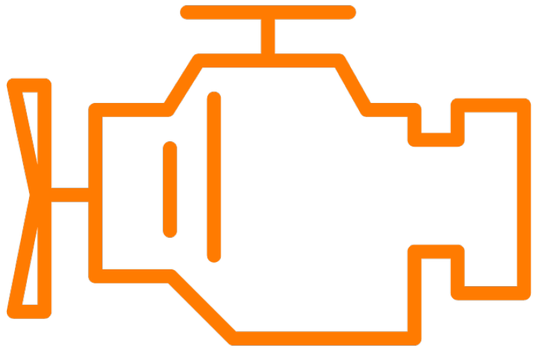
Managing a Secrets Engine

Ned Bellavance

HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

Secrets Engine Lifecycle

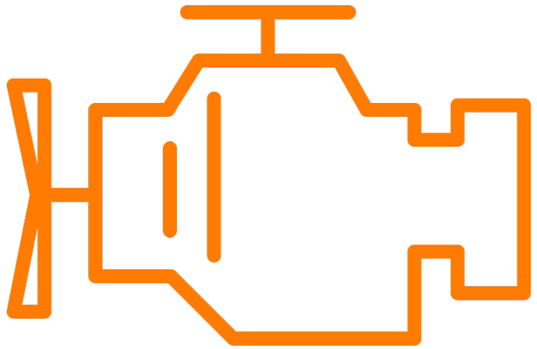


Gather information for engine

Enable engine on a mount path

- Defaults to engine name
- Must be unique in Vault namespace
- Mount can be moved with caveats

Secrets Engine Lifecycle



Tune the engine settings

- Default and max TTL
- Description

Configure the engine specific settings

- Path: mount/config

Disable engine to remove

- Destructive action!

Secrets Commands

```
# List mounted secrets engines
vault secrets list

# Enable a secrets engine
vault secrets enable [options] TYPE
vault secrets enable –path=webapp kv

# Tune a secrets engine
vault secrets tune [options] PATH
vault secrets tune –description="Secrets for Web App" webapp
```

Secrets Commands

```
# Move a secrets engine
vault secrets move [options] SOURCE DESTINATION
vault secrets move "webapp" "trackingapp"

# Disable a secrets engine
vault secrets disable [options] PATH
vault secrets disable "trackingapp"
```

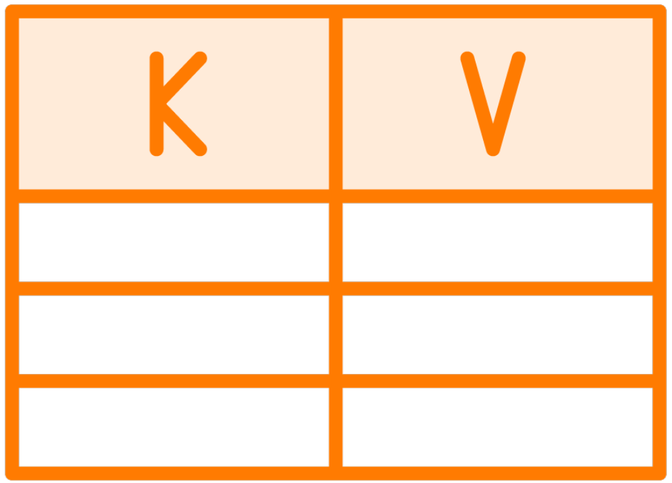
Key Value Secrets Engine

Version 1 Example

```
$ vault kv get kv/webapp/apikeys

==== Data ====
Key     Value
---     -----
key1    abc123
key2    xyz789
```

Version 1 Overview



Keys must be a string

Control parameters with policy

- Version 1 only

Parameters are encrypted

No versioning of values

Deletes are permanent

Version 1 Scenario

Requirements

- High-volume app called Trader
- Store thousands of short-lived tokens
- Tokens purged nightly

Solution

- Version 1 of the KV engine

Vault CLI Basics

```
$ vault -h

Usage: vault <command> [args]

Common commands:
    read        Read data and retrieves secrets
    write       Write data, configuration, and secrets
    delete      Delete secrets and configuration
    list        List data or secrets
    login       Authenticate locally
    agent       Start a Vault agent
    server      Start a Vault server
    status      Print seal and HA status
    unwrap      Unwrap a wrapped secret
```

Environment Variables

```
# Vault Server Address

VAULT_ADDR="https://vault.yolo.local:8200"

# Vault Token

VAULT_TOKEN=hvs.NJI87YHJHY78UHJU87678UJHGY678
```

Key Value Engine Commands

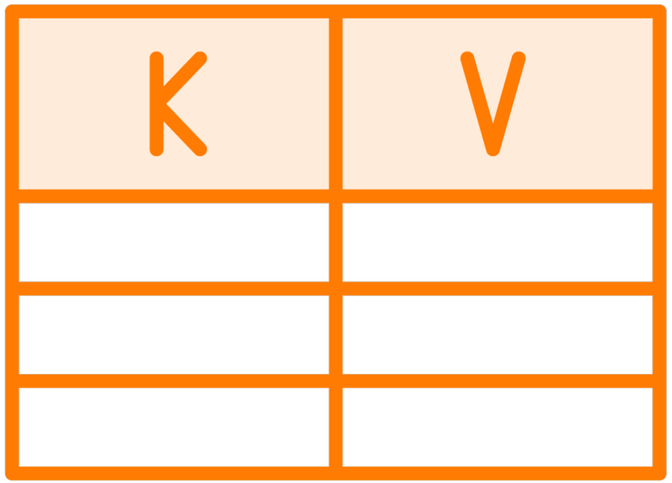
```
# List available keys and segments at a path
vault kv list [options] PATH
vault kv list kv/webapp

# Read the value of a key
vault kv get [options] PATH
vault kv get kv/webapp/apikeys

# Write the value of a key
vault kv put [options] PATH
vault kv put kv/webapp/apikeys "key3=abc123" "key4=xyz789"

# Delete a key and its value
vault kv delete [options] PATH
vault kv delete kv/webapp/apikeys
```

Version 2 Overview



Adds metadata storage

Store multiple versions

- Default of 10

Soft delete and undelete

Custom metadata

Check and set (CAS)

Parameter patching

Parameter Patching

Console command

```
$ vault kv put kv/customers/ned "phone=215-555-5555" "username=nedb"
```

Current value

```
====== Data ======
Key          Value
---          -----
phone        215-555-5555
username     nedb
```

Parameter Patching

Console command

```
$ vault kv put kv/customers/ned "phone=267-555-5555"
```

Current value

```
====== Data ======
Key          Value
---          -----
phone        267-555-5555
```

Parameter Patching

Console command

```
$ vault kv patch kv/customers/ned "phone=267-555-5555"
```

Current value

```
====== Data ======
Key          Value
---          -----
phone        267-555-5555
username     nedb
```

Check and Set

Console command

```
$ vault kv put kv/customers/ned "phone=267-555-5555"
```

Current value

```
======= Metadata =======
Key                Value
---                -----
created_time       2025-03-20T18:06:26.9522926Z
custom_metadata    <nil>
deletion_time      n/a
destroyed          false
version            1
```

Check and Set

Console command

```
$ vault kv put -cas=1 kv/customers/ned "phone=267-555-5555"
```

Current value

```
======= Metadata =======
Key                Value
---                -----
created_time       2025-03-20T18:08:58.1485995Z
custom_metadata    <nil>
deletion_time      n/a
destroyed          false
version            2
```

Version 2 Paths

Purpose	Path
Access key values	`kv/data/key_path`

Version 2 Paths

Purpose	Path
Access key values	`kv/data/key_path`
Access key metadata	`kv/metadata/key_path`

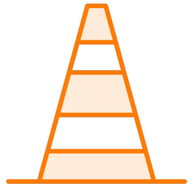
Version 2 Paths

Purpose	Path
Access key values	`kv/data/key_path`
Access key metadata	`kv/metadata/key_path`
Undelete a version	`kv/undelete/key_path`

Version 2 Paths

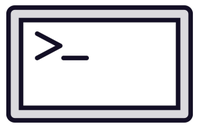
Purpose	Path
Access key values	`kv/data/key_path`
Access key metadata	`kv/metadata/key_path`
Undelete a version	`kv/undelete/key_path`
Destroy a version	`kv/destroy/key_path`

Migration from V1 to V2



Plan for downtime

Update policies for new endpoints



Run vault kv enable-versioning

Comparing Key Value Versions

Version 1	Version 2
Limited functionality	Increased functionality
No metadata	Metadata overheard
More lightweight	Increased resource usage
Specific use cases	Should be the default

Version 2 Scenario

Requirements

- CRM application
- Stores customer data
- Support multiple versions
- Support patching

Solution

- Version 2 of the KV engine

Key Value Engine Commands

```
# Update parameters without overwriting value
vault kv patch [options] PATH [PARAMETERS]
vault kv patch kv/webapp/apikeys "key3=rty465"

# Restore the value of the previous version
vault kv rollback [options] PATH
vault kv rollback -version=2 kv/webapp/apikeys

# Undelete one or more versions
vault kv undelete [options] PATH
vault kv undelete -versions=3 kv/webapp/apikeys

# Permanently destroy one or more versions
vault kv destroy [options] PATH
vault kv destroy -versions=2 kv/webapp/apikeys
```

Key Value Engine Commands

```
# Get metadata about a key
vault kv metadata get [options] PATH
vault kv metadata get kv/webapp/apikeys

# Put information into metadata
vault kv metadata put [options] PATH
vault kv metadata patch [options] PATH [PARAMETERS]
vault kv metadata patch –cas-required kv/webapp/apikeys

# Delete the key and all metadata
vault kv metadata delete [options] PATH
vault kv metadata delete kv/webapp/apikeys
```