



HashiCorp

**Vault**

Vault

Diego Pacheco

# About Me



- ❑ Cat's Father
- ❑ Principal Software Architect
- ❑ Agile Coach
- ❑ SOA/Microservices Expert
- ❑ DevOps Practitioner
- ❑ Speaker
- ❑ Author



diegopacheco



@diego\_pacheco



<http://diego-pacheco.blogspot.com.br/>



# Manage Secrets | Protect Data



## Secrets Management

Centrally store, access, and distribute dynamic secrets such as tokens, passwords, certificates, and encryption keys



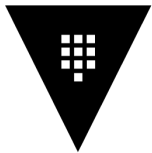
## Data Protection

Keep application data secure with centralized key management and simple APIs for data encryption

# Install Vault

install-vault.sh x

```
1  #!/bin/bash
2
3  wget https://releases.hashicorp.com/vault/1.0.1/vault_1.0.1_linux_amd64.zip
4  unzip vault_1.0.1_linux_amd64.zip
5  chmod +x vault
```



HashiCorp

# Vault

# vault

```
$ vault
```

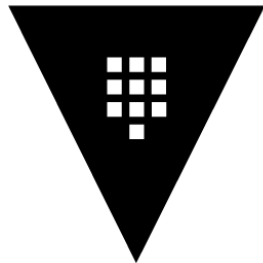
```
Usage: vault <command> [args]
```

## 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
server	Start a Vault server
status	Print seal and HA status
unwrap	Unwrap a wrapped secret

## Other commands:

audit	Interact with audit devices
auth	Interact with auth methods
lease	Interact with leases
operator	Perform operator-specific tasks
path-help	Retrieve API help for paths
policy	Interact with policies
secrets	Interact with secrets engines
ssh	Initiate an SSH session
token	Interact with tokens



HashiCorp  
**Vault**

# vault server -dev

```
vault server -dev

File Edit View Search Terminal Tabs Help

vault server -dev x diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault x

diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault ➤ master ➤ vault server -dev
==> Vault server configuration:

    Api Address: http://127.0.0.1:8200
      Cgo: disabled
  Cluster Address: https://127.0.0.1:8201
    Listener 1: tcp (addr: "127.0.0.1:8200", cluster address: "127.0.0.1:8201", max_request_duration: "1m30s", max_request_size: "33554432", tls: "disabled")
      Log Level: (not set)
        Mlock: supported: true, enabled: false
      Storage: inmem
      Version: Vault v1.0.1
    Version Sha: 08df121c8b9adcc2b8fd55fc8506c3f9714c7e61

WARNING! dev mode is enabled! In this mode, Vault runs entirely in-memory
and starts unsealed with a single unseal key. The root token is already
authenticated to the CLI, so you can immediately begin using Vault.

You may need to set the following environment variable:

$ export VAULT_ADDR='http://127.0.0.1:8200'

The unseal key and root token are displayed below in case you want to
seal/unseal the Vault or re-authenticate.

Unseal Key: dG8Nzxt8UGz8hBs4dMCyT0AZkCPa2A7DQXLyMMC1jPI=
Root Token: s.71IFwn3iXqRTSzh1WcT1ykt
```

# Checking if vault is FINE

```
diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault
File Edit View Search Terminal Tabs Help

diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault vault server -dev
diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master ➤ export VAULT_DEV_ROOT_TOKEN_ID=s.71IFwn3iXgRTSzhjWcIlykLt
diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master ➤ export VAULT_ADDR='http://127.0.0.1:8200'
diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master ➤ vault status
Key      Value
---
Seal Type  shamir
Initialized true
Sealed     false
Total Shares 1
Threshold   1
Version     1.0.1
Cluster Name vault-cluster-96d7f32c
Cluster ID  74a513f7-94c4-c1ec-b714-85f9002b242c
HA Enabled  false
diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master ➤
```

18:13:20 7.49G 0.24

# Write | Read Secrets

```
diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault vault server -dev

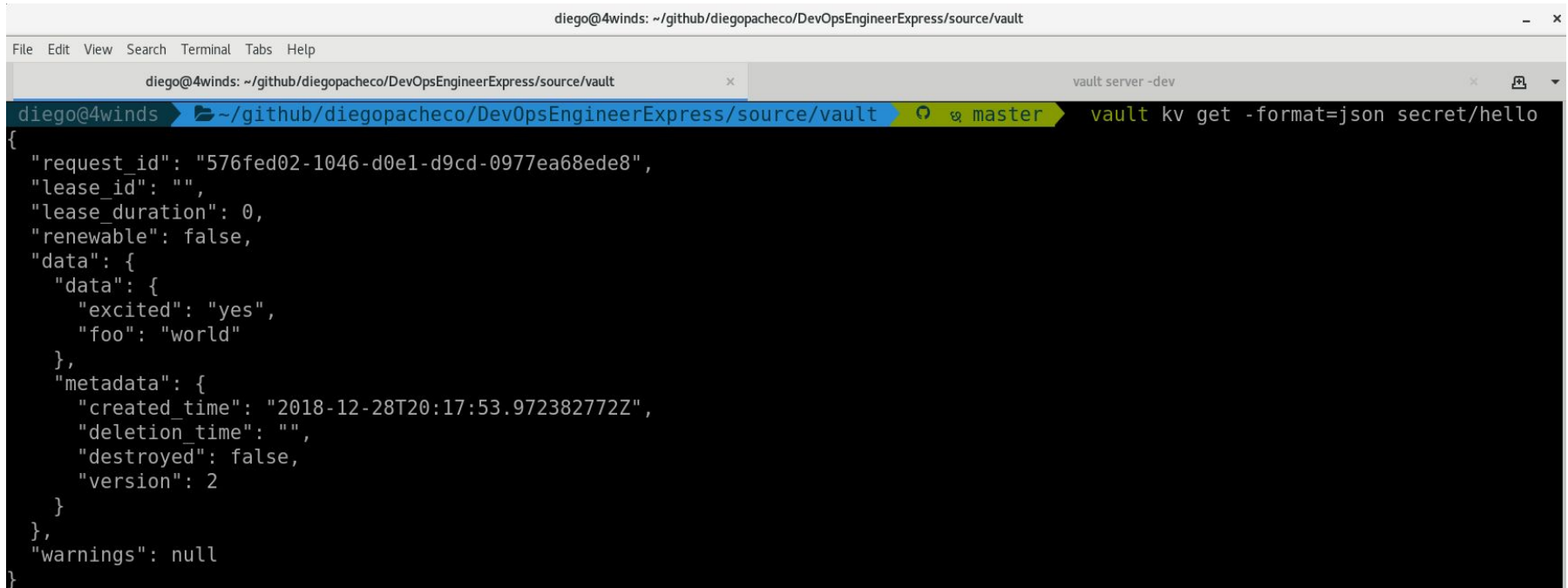
diego@4winds > ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master vault kv put secret/hello foo=world
Key      Value
---
created_time 2018-12-28T20:17:38.473156749Z
deletion_time n/a
destroyed    false
version      1

diego@4winds > ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master vault kv put secret/hello foo=world excit
ed=yes
Key      Value
---
created_time 2018-12-28T20:17:53.972382772Z
deletion_time n/a
destroyed    false
version      2

diego@4winds > ~/github/diegopacheco/DevOpsEngineerExpress/source/vault master vault kv get secret/hello
===== Metadata =====
Key      Value
---
created_time 2018-12-28T20:17:53.972382772Z
deletion_time n/a
destroyed    false
version      2
```



# Get Data as JSON



The screenshot shows a terminal window with a menu bar (File, Edit, View, Search, Terminal, Tabs, Help) and two tabs: 'diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault' and 'vault server -dev'. The active tab is the first one. The terminal prompt is 'diego@4winds' followed by a blue arrow pointing to the directory path. The command 'vault kv get -format=json secret/hello' is entered. The output is a JSON object representing a Vault secret.

```
diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault
vault kv get -format=json secret/hello
{
  "request_id": "576fed02-1046-d0e1-d9cd-0977ea68ede8",
  "lease_id": "",
  "lease_duration": 0,
  "renewable": false,
  "data": {
    "data": {
      "excited": "yes",
      "foo": "world"
    },
    "metadata": {
      "created_time": "2018-12-28T20:17:53.972382772Z",
      "deletion_time": "",
      "destroyed": false,
      "version": 2
    }
  },
  "warnings": null
}
```

# Deleting Secrets

```
diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault
File Edit View Search Terminal Tabs Help

diego@4winds: ~/github/diegopacheco/DevOpsEngineerExpress/source/vault vault server -dev

diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault ➤ master ➤ vault kv delete secret/hello
Success! Data deleted (if it existed) at: secret/hello
diego@4winds ➤ ~/github/diegopacheco/DevOpsEngineerExpress/source/vault ➤ master ➤ vault kv get secret/hello
===== Metadata =====
Key      Value
---      -
created_time 2018-12-28T20:17:53.972382772Z
deletion_time 2018-12-28T20:23:18.411130001Z
destroyed    false
version      2
```

# Vault Web UI

The screenshot displays the Vault Web UI interface in a web browser. The address bar shows the URL `127.0.0.1:8200/ui/vault/secrets/secret/show/hello`. The browser's bookmark bar includes entries like 'Apps', 'Speed Dial 2', 'Engineering', 'Tech', 'default', 'Links', 'Work', 'util', 'CM', 'DevOps.Engineer', and 'DevOpsEngineer'. The Vault Web UI header features a navigation menu with 'Secrets', 'Access', 'Policies', and 'Tools', along with a 'Status' dropdown. The main content area shows the 'hello' secret page, with a breadcrumb trail '< secret < hello' and a 'Delete secret >' link. A table with two columns, 'KEY' and 'VALUE', lists the secret's data. The 'excited' key has a value of '\*\*\*\*\*', and the 'foo' key has a value of '\*\*\*\*\*'. A 'JSON' toggle is visible in the top right of the table area. The footer contains the HashiCorp logo, copyright information for 2018, the version 'Vault 1.0.1', and links for 'Upgrade to Vault Enterprise' and 'Documentation'.

127.0.0.1:8200/ui/vault/secrets/secret/show/hello

Apps Speed Dial 2 Engineering Tech default Links Work util CM DevOps.Engineer DevOpsEngineer Other bookmarks

Secrets Access Policies Tools Status

< secret < hello

hello [Delete secret >](#)

☐ JSON [Copy Secret](#) [Create new version](#) [Version 3 >](#) [History >](#)

KEY	VALUE
excited	*****
foo	*****

© 2018 HashiCorp, Inc. Vault 1.0.1 [Upgrade to Vault Enterprise](#) [Documentation](#)

<http://127.0.0.1:8200/ui/vault>

# ... Much More!

- ❑ Secret Engines
- ❑ Dynamic Secrets
- ❑ Roles
- ❑ Great | Revoke Access Tokens
- ❑ Policies(HCL) Support
- ❑ Consul Integration for Distributed Backend



HashiCorp  
**Vault**



HashiCorp

**Vault**

Vault

Diego Pacheco