**HashiCorp Vault Installation and Configuration**

Vault secures, stores, and tightly controls access to tokens, passwords, certificates, API keys, and other secrets in modern computing.

Vault comes with various pluggable components called secrets engines and authentication methods allowing you to integrate with external systems. The purpose of those components is to manage and protect your secrets in dynamic infrastructure (e.g., database credentials, passwords, API keys).

**Step 1: Installation**

1. Windows Installation:

By using Chocolatey, we can install Vault

Cmd: choco install vault

vault –version

vault -help

1. Linux (Ubuntu/Debian):

Cmd:

1. curl -fsSL https://apt.releases.hashicorp.com/gpg | sudo apt-key add –
2. sudo apt-add-repository "deb [arch=amd64] https://apt.releases.hashicorp.com $(lsb\_release -cs) main"
3. sudo apt-get update && sudo apt-get install vault
4. vault –version
5. vault -help
6. For other OS, follow the below URL instructions

<https://learn.hashicorp.com/tutorials/vault/getting-started-install?in=vault/getting-started>

Text

Description automatically generated with low confidence

Graphical user interface, text

Description automatically generated

**Step 2: Starting the Server (development mode)**

1. vault server -dev
2. export VAULT\_ADDR='http://127.0.0.1:8200'
3. export VAULT\_TOKEN="hvs.xxxxxxxxxxxxxxxxxxxxxx"
4. vault status

Note: VAULT\_ADDR and VAULT\_TOKEN values will get when we execute the “vault server -dev” commandText

Description automatically generated

Text

Description automatically generated

**Step 3: Key/Value secret engine**

Cmd: vault kv -help

vault kv <subcommand> <options> <args>

vault kv put secret/hello foo=world

vault kv put secret/hello foo=world excited=yes (multiple values)

vault kv get secret/hello

vault kv delete secret/hello

**Step 4: Secrets Engine**

Cmd: vault secrets list

**Step 5: Dynamic Secrets**

Cmd: i. vault secrets enable -path=aws aws

Success! Enabled the aws secrets engine at: aws/

ii. export AWS\_ACCESS\_KEY\_ID=<aws\_access\_key\_id>

1. export AWS\_SECRET\_ACCESS\_KEY=<aws\_secret\_key>
2. vault write aws/config/root \

access\_key=$AWS\_ACCESS\_KEY\_ID \

secret\_key=$AWS\_SECRET\_ACCESS\_KEY \

region=us-east-1

1. Role Creation:

vault write aws/roles/my-role \

credential\_type=iam\_user \

policy\_document=-<<EOF

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Stmt1426528957000",

"Effect": "Allow",

"Action": [

"ec2:\*"

],

"Resource": [

"\*"

]

}

]

}

EOF

1. Generate Secrets

vault read aws/creds/my-role

**vault common commands:**

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

**Note**: Vault installation and Configuration details available in following URL

https://learn.hashicorp.com/tutorials/vault/getting-started-intro?in=vault/getting-started