Contents

[Installing Vault 1](#_Toc118951372)

[P1. Installing and Running Vault Server 1](#_Toc118951373)

[P4. Run vault dev server 1](#_Toc118951374)

[P5. Run vault prod server 1](#_Toc118951375)

[P6. Init vault 3](#_Toc118951376)

[P7. Config storage and join cluster 3](#_Toc118951377)

# Installing Vault

### P1. Installing and Running Vault Server

Cài đặt > tạo config file > khởi tạo vault > unseal vault

Cách 1: <https://developer.hashicorp.com/vault/downloads>

# sudo yum install -y yum-utils

# sudo yum-config-manager --add-repo https://rpm.releases.hashicorp.com/RHEL/hashicorp.repo

# sudo yum -y install vault

Cách 2: Dùng helm

# helm repo add hashicorp <https://helm.releases.hashicorp.com>

# helm search repo vault

# helm -n my-vault install --create-namespace -g hashicorp/vault

Cách 3: Binary file:

# curl -O <https://releases.hashicorp.com/vault/1.12.1/vault_1.12.1_linux_amd64.zip>

# unzip vault\_1.12.1\_linux\_amd64.zip

# mv vault /usr/local/bin/

### P4. Run vault dev server

Lệnh chạy:

# export VAULT\_ADDR='http://192.168.88.12:8200'

# vault server -dev

# vault status

# vault secrets list

# vault kv put secret/vaultcourse/bryan bryan=bryan

# vault kv get secret/vaultcourse/bryan

### P5. Run vault prod server

 The HashiCorp vault binary at path /usr/bin

 Directory for storing raft data at path /opt/vault/data

 The Vault configuration file at /etc/vault.d/vault.hcl

 The systemd service file at /lib/systemd/system/vault.service

# cat /etc/vault.d/vault.hcl

storage "raft" {

    path    = "/opt/vault"

    node\_id = "vault-node-a"

  }

  listener "tcp" {

   address = "0.0.0.0:8200"

   cluster\_address = "0.0.0.0:8201"

   tls\_disable = true

  }

  api\_addr = "http://192.168.88.12:8200"

  cluster\_addr = "http://192.168.88.12:8201"

  cluster\_name = "my-vault-cluster"

  ui = true

  log\_level = "ERROR"

  disable\_mlock = true

# cat /lib/systemd/system/vault.service

[Unit]

Description="HashiCorp Vault - A tool for managing secrets"

Documentation=https://www.vaultproject.io/docs/

Requires=network-online.target

After=network-online.target

ConditionFileNotEmpty=/etc/vault.d/vault.hcl

StartLimitIntervalSec=60

StartLimitBurst=3

[Service]

Type=notify

EnvironmentFile=/etc/vault.d/vault.env

User=vault

Group=vault

ProtectSystem=full

ProtectHome=read-only

PrivateTmp=yes

PrivateDevices=yes

SecureBits=keep-caps

AmbientCapabilities=CAP\_IPC\_LOCK

CapabilityBoundingSet=CAP\_SYSLOG CAP\_IPC\_LOCK

NoNewPrivileges=yes

ExecStart=/usr/bin/vault server -config=/etc/vault.d/vault.hcl

ExecReload=/bin/kill --signal HUP

KillMode=process

KillSignal=SIGINT

Restart=on-failure

RestartSec=5

TimeoutStopSec=30

LimitNOFILE=65536

LimitMEMLOCK=infinity

[Install]

WantedBy=multi-user.target

### P6. Init vault

# vault operator init

(chú ý lưu các key này lại)

### P7. Config storage and join cluster

# vault login hvs.SXrTNf3xzC5uRaX3NdDM901q

# vault operator raft list-peers

Thực hiện join **node2 join vào node1**

# vault operator raft join <http://node-1:8200>

# vault status (có kết quả unseal progres 0/3)

# vault operator unseal VtVxv0ycNH740nbA72bWFgTHhjI9Dgnz5NAxkGSyQxvc

# vault operator unseal Ce25VdVF7R5WFm4+Eu0JyUq4pUfj7cEJVlrCjzpui5U3

# vault operator unseal XhlP2TVu7uwv0L/r+HrxJNdIg0cmI4XLRp5QdLTae9CM

Thực hiện join **node3 join vào node1 (tương tự command ở node2)**

Đây là cấu hình của node 1- 2 và 3

root@node-1 ~ ➜ cat /etc/vault.d/vault.hcl

storage "raft" {

path = "/opt/vault/data"

node\_id = "node-1"

}

listener "tcp" {

address = "node-1:8200"

cluster\_address = "node-1:8201"

tls\_disable = true

}

api\_addr = "http://vault-production:8200"

cluster\_addr = "http://node-1:8201"

cluster\_name = "vault-ha-cluster"

ui = true

log\_level = "INFO"

disable\_mlock = true

root@node-2:~# cat /etc/vault.d/vault.hcl

storage "raft" {

path = "/opt/vault/data"

node\_id = "node-2"

}

listener "tcp" {

address = "node-2:8200"

cluster\_address = "node-2:8201"

tls\_disable = true

}

api\_addr = "http://vault-production:8200"

cluster\_addr = "http://node-2:8201"

cluster\_name = "vault-ha-cluster"

ui = true

log\_level = "INFO"

disable\_mlock = true

root@node-3d# cat /etc/vault.d/vault.hcl

storage "raft" {

path = "/opt/vault/data"

node\_id = "node-3"

}

listener "tcp" {

address = "node-3:8200"

cluster\_address = "node-3:8201"

tls\_disable = true

}

api\_addr = "http://vault-production:8200"

cluster\_addr = "http://node-3:8201"

cluster\_name = "vault-ha-cluster"

ui = true

log\_level = "INFO"

disable\_mlock = true

bob@node-1 ~ ➜ vault operator raft list-peers

Node Address State Voter

---- ------- ----- -----

node-1 node-1:8201 leader true

node-2 node-2:8201 follower true

node-3 node-3:8201 follower true

bob@node-1 ~ vault operator step-down (ta force down node 1 xuống, để xem node 2 nhẩy lên làm leader)

B2. Ta thử kiểm tra đồng bộ dữ liệu giữa node 2-3 khi node 1 đã tắt

bob@node-3 ~ ➜ vault secrets enable aws

bob@node-2 ~ ➜ vault secrets list (sang node 2 thấy có path aws vừa được tạo)

B3. Stop luôn node2 leader. Sang node 3 get secret list sẽ bị lỗi (bởi vì 2 node, quorum phải bằng 2)

bob@node-3 ~ ➜ vault secrets list

Error listing secrets engines: Get "http://vault-production:8200/v1/sys/mounts": dial tcp 10.69.109.2:8200: connect: connection refused

B4. Start lại node1 và 2. Chú ý phải unseal node 1-2 . Sau đó làm lại B3, node 3 đã hiện ra secret.

bob@node-3 ~ ➜ vault operator raft list-peers (node 3 làm leader)

bob@node-3 ~ ➜ vault secrets list (có ra dữ liệu)

### P8. Auto unseal