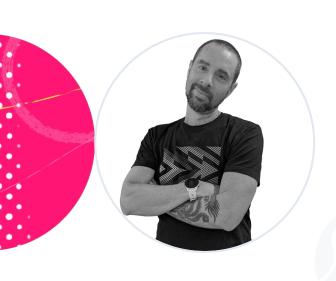
Managing the Vault Seal



Ned Bellavance

HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com



Environment Variables

VAULT_ADDR - Address of the Vault server
VAULT_TOKEN - Token value for requests
VAULT_FORMAT - Specify output format
VAULT_NAMESPACE - Specify namespace

Environment Variables

VAULT_CACERT - Path to CA cert

VAULT_CLIENT_CERT - Path to public cert

VAULT_CLIENT_KEY - Path to private key

VAULT_SKIP_VERIFY - No cert validation

Unseal Vault

```
# Start or continue unseal process
vault operator unseal [options] [KEY]

# Using the API
curl -X POST https://$VAULT_ADDR/v1/sys/unseal \
    --data '{"key": "UNSEAL_KEY"}'
```



Seal Vault

```
# Seal Vault
vault operator seal [options]

# Using the API
curl -X POST https://$VAULT_ADDR/v1/sys/seal \
    --header "X-Vault-Token: $VAULT_TOKEN"
```



Managing Vault Keys

Rotate

Update encryption keys
No downtime
Automatic

Rekey

Create new unseal and root keys

No downtime

Requires threshold

Manage Keys

```
# Start rekey of unseal and root key
vault operator rekey [options] [KEY]
vault operator rekey -init -key-shares=5 -key-threshold=3
# Continue rekey process
vault operator rekey [KEY_SHARE_VALUE]
# Check the encryption key status
vault operator key-status [options]
# Rotate the encryption key
vault operator rotate [options]
```



Seal Migration



No data loss

Requires Vault downtime

Update configuration

Unseal with -migrate flag

Auto-unseal Configuration

```
seal "gcpckms" {
  credentials = "/usr/vault/vault-prod.json"
  project = "vault-prod"
  region = "global"
  key_ring = "vault-prod-keyring"
  crypto_key = "vault-prod-key"
}
```

Auto-unseal with the Transit Engine

