Cheat Sheet for HashiCorp Vault

Learn Vault Here → btk.me/btk

Auth Methods

Enable and configure authentication methods, including role-based setups:

`vault auth list`
List enabled auth methods

`vault auth enable <method>`
Enable an auth method (e.g., userpass, approle, oidc)

`vault write auth/<method>/role/<name> ...`
Create or update a role for the auth method

`vault read auth/<method>/role/<name>`
Read role details

`vault login -method=<method> [options]`
Log in using a specific auth method

Tokens

Token lifecycle commands for login, lookup, and revocation:

`vault token create [options]`
Create a new token

`vault login <token>`
Login with a token

`vault token lookup`
Lookup your current token

`vault token lookup <token>`
Lookup a specific token

`vault token revoke <token>`
Revoke a token

Secrets Engines

Work with Vault's Secrets Engines (KV, databases, cloud credentials, etc.):

`vault secrets list`
List enabled secrets engines

`vault secrets list --detailed`
List details about enabled secrets engines

`vault secrets enable <type>`
Enable a secrets engine

`vault secrets enable -path=<path> <type>`
Enable a secrets engine at a specific path

`vault secrets disable <path>`
Disable a secrets engine at the given path

Policies

Create and manage Vault ACL policies:

`vault policy list`
List all policies

`vault policy write <policy_name> <file.hcl>`
Create or update a policy from a file

`vault policy write my-policy -<<EOF <rules> EOF`
Creates a policy directly from inline HCL using heredoc syntax.

`vault policy read <name>`
View a policy's contents

`vault policy delete <name>`
Delete a policy

Day-to-Day Operations

Core operational commands:

`vault status`
Check Vault's current seal and HA status

`vault operator unseal`
Unseal Vault with a key shard

`vault operator members`
List all nodes in the Vault cluster (Raft or HA)

`vault operator raft list-peers`
List Raft cluster peers

`vault operator raft snapshot save <file>`
Save a snapshot of Vault data

`vault operator step-down`
Force the active node to give up leadership

Replication

Enable and manage replication (Vault Enterprise):

`vault read sys/replication/status`
Check the current replication status (enabled, mode, cluster role)

`vault write -f sys/replication/dr/primary/enable`
Enable Disaster Recovery (DR) replication on the primary cluster

`vault write sys/replication/dr/primary/secondary-token id=<name>`
Generate a secondary token for a DR Secondary cluster

`vault write sys/replication/dr/secondary/enable token=<token>`
Enable a node as a DR Secondary using the secondary token

KV Secrets (Key-Value)

Used for storing static secrets manually:

`vault kv put secret/myapp key=value`
Store a secret

`vault kv get secret/myapp`
Read a secret

`vault kv delete secret/myapp`
Delete a secret

`vault kv undelete -versions=1 secret/myapp`
Restore previously deleted secret versions (KV-V2 only)

`vault kv metadata delete secret/myapp`
Permanently remove metadata & versions (KV-V2 only)