HashiCorp Vault | Red Hat OpenShift

Vault & OpenShift

Protect hybrid applications from credential theft at scale

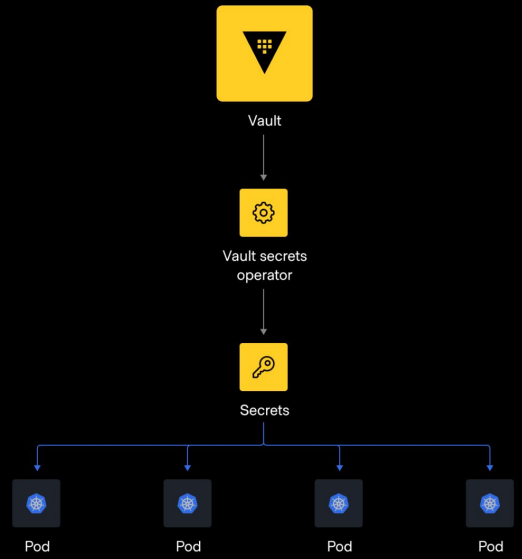
Security Challenges of Kubernetes Secrets

- **No encryption**
  By default, secrets are stored in base64 encoded plain text. Secrets are vulnerable if the etcd database is compromised
- **Access control**
  - misconfigured access control can allow unauthorized entities to access secrets within the namespace
  - cluster-admin can read all the credentials
- **Manual rotation**
  Manual and inconsistent key rotation can lead to stale or compromised credentials across clusters.

Vault Secrets Operator (VSO)

Operator-based approach gives flexibility to application and DevSecOps teams

- Sync Vault secrets into local, native Kubernetes secrets, fully-namespaced
- Full control and management for secrets through Vault
- Rollout restart capabilities roll pods on secret rotation or revocation, when configured
- Accelerates application deployment, once decoupled from secrets management
- Returns control over secrets policies and secrets management to security operations teams



VSO Comparison to Others

Vault Enterprise

Vault Agent Injector

- Stores secrets in ephemeral Volumes
- Depends on Vault being up during Pod scaling
- Utilizes the agent sidecar strategy to inject secrets into Pods

Vault CSI Driver

- Provides secret data to Pods using ephemeral volumes
- Depends on the CSI Secrets driver
- Depends on Vault being up during Pod scaling

Vault Secrets Operator

- Provides secret data to Pods from synced K8s Secrets
- Secret data is cached

VSO CRD Overview - Vault Connection and Authentication

Vault Enterprise

VaultConnection

- Cluster address
- TLS Configuration

VaultAuth

- Vault authentication configuration

Vault*Secret

- Configuration necessary for syncing Vault secret data to K8s Secrets
- KV, PKI, Dynamic

VSO CRD Overview - Transformations

Vault Enterprise

Vault*Secret

- Configuration necessary for syncing Vault secret data to K8s Secrets
- KV, PKI, Dynamic

SecretTransformation

- Provides shared templates and object filters for rendering custom secret data to the K8s secret destination

K8s Secret

- Rendered/Transformed secret data

When to use Vault Secrets Operator

Consider Vault Secrets Operator:

- At the beginning of a new project or re-platforming exercise
- For OpenShift deployments scaling to 1000s of pods, with 1000+ restarting concurrently
- For secrets that are used by multiple pods (not single-use secrets)
- When application development is being slowed down by secrets integration and management
- To help the security operations teams regain control over secrets management
- Alongside other integrations (Agent Sidecar Injector, Secrets Store CSI Provider, Cert-manager)

Thank you