HashiCorp
an IBM Company

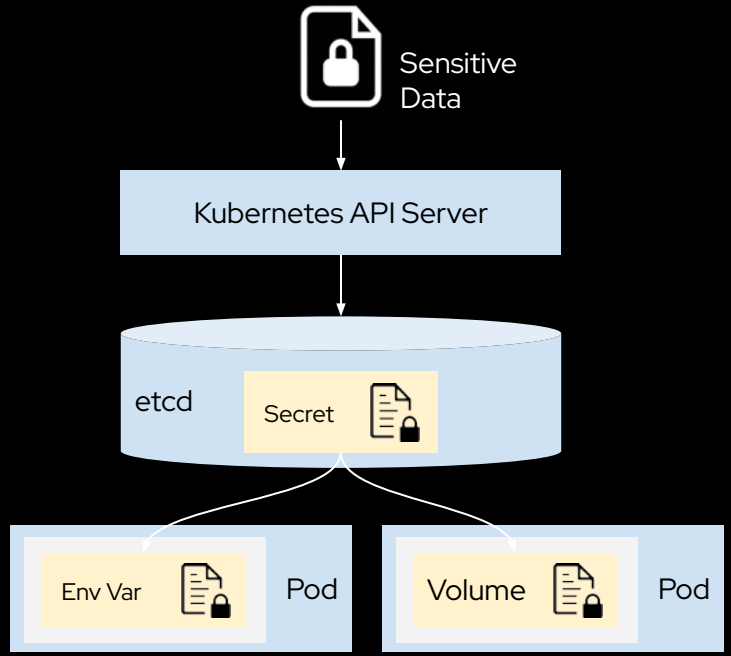
HashiCorp Vault and OpenShift: Discover Security and Speed in Perfect Harmony

Pieter Lewyllie
Senior Solutions Architect
Red Hat

Cojan van Ballegooijen
Solutions Engineer
HashiCorp

Kubernetes Secrets

- Secret is a Kubernetes resource to store confidential data
  - Credentials
  - Certificates
  - API Tokens
  - SSH keys
- Separates confidential data from application code
  - container image does not contain sensitive data

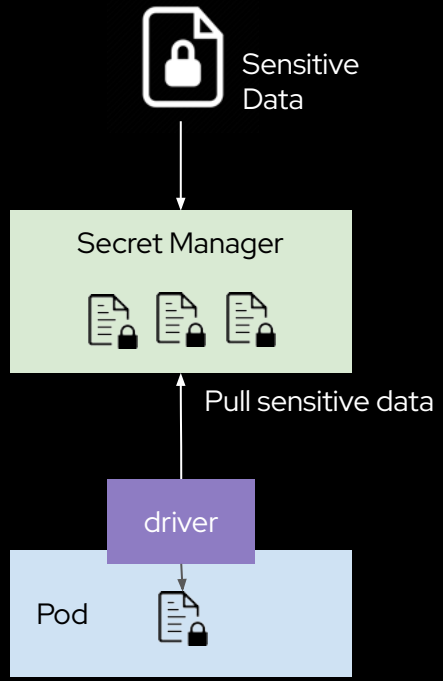


Security Challenges of Kubernetes Secrets

- **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.

The Value of External Secret Management

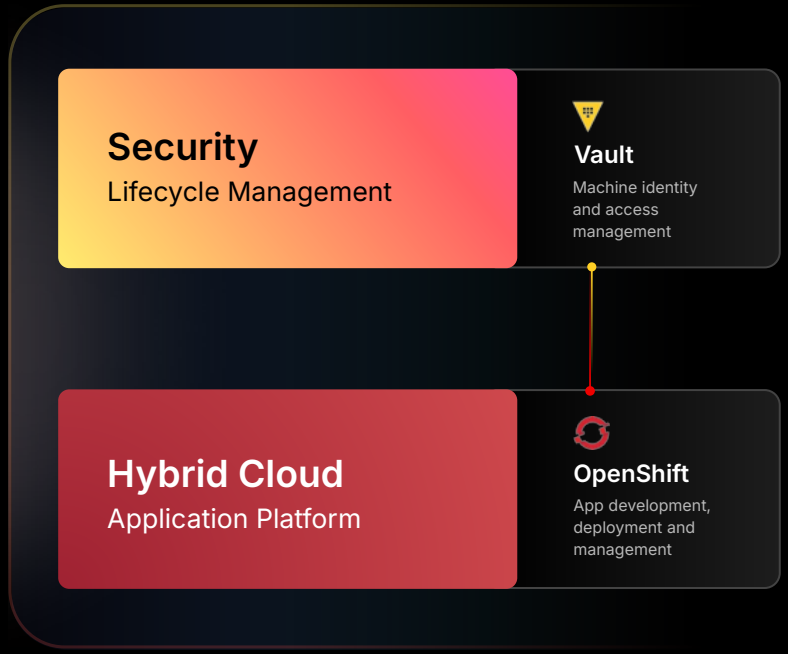
- A dedicated system for managing sensitive data
- Store sensitive data outside Kubernetes
- Protect secrets from admin access
- Fine-grained access control
- Automated secret lifecycle management (e.g. rotation, expiration)



Red Hat

BETTER TOGETHER

Protect hybrid applications from credential theft



Reduce risk and streamline hybrid operations with Vault and OpenShift

Build, manage, and secure hybrid applications on a single platform

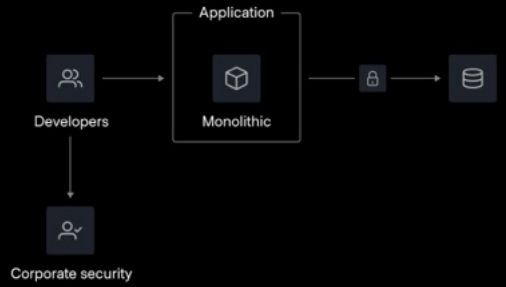
Enforce identity-based authorization and security policies consistently across environments

Encrypt, rotate, and inject credentials into OpenShift containers and CI/CD workflows

Basic secrets management

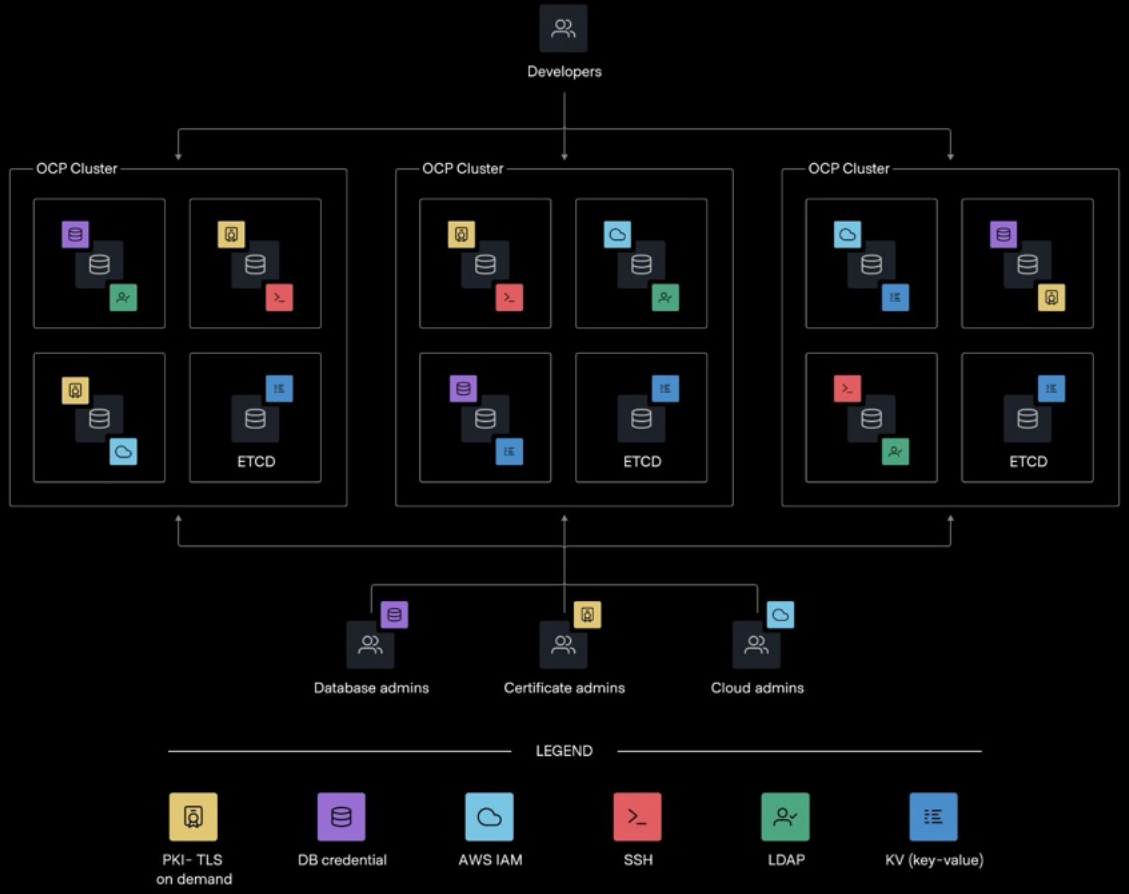
Applications require multiple forms of sensitive material. This could be database credentials for web applications, cloud credentials for access to cloud native services, or even the ability to interact with sensitive data types.

Traditional approaches are manually managed through Identity or Information Security teams to maintain chain of custody of sensitive information.



OpenShift secrets management

- Secret Management not centralized
- Administrative overhead is spread out
- Tracking down sprawl of different secrets...

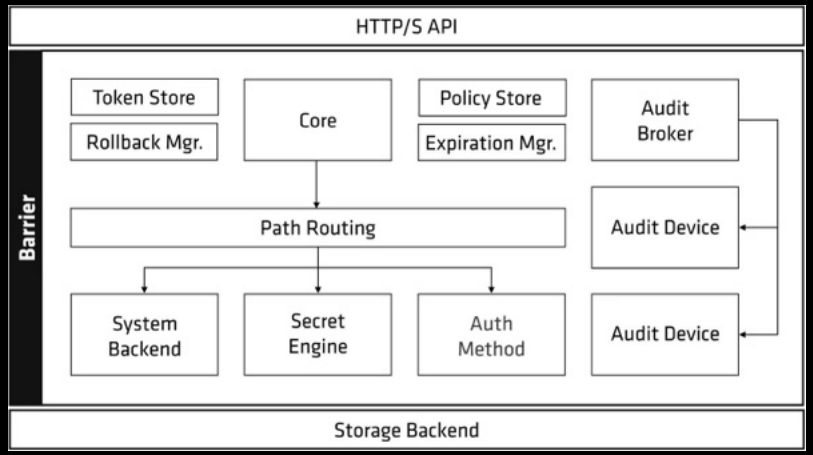


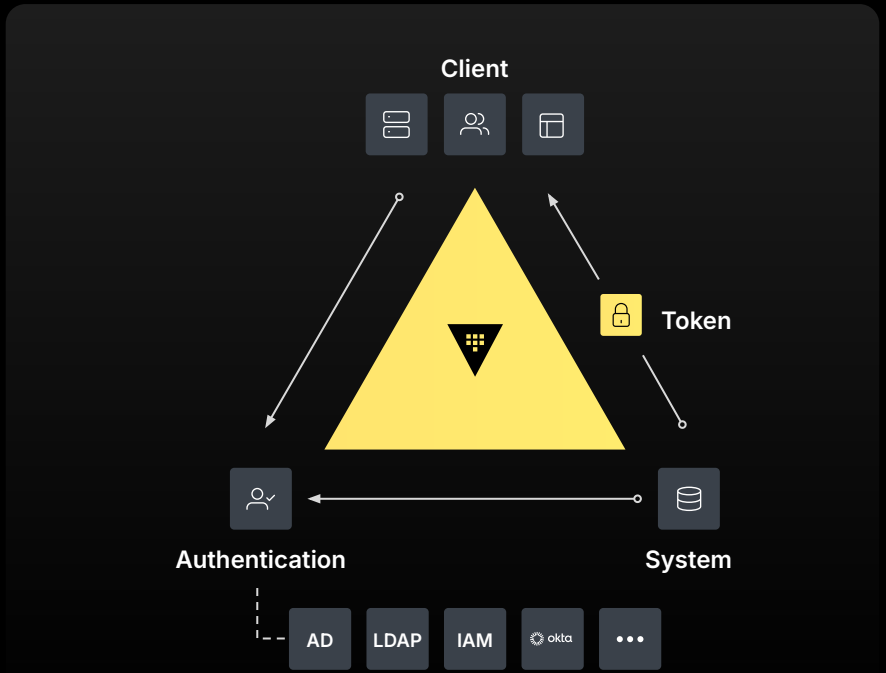
How Vault works

ARCHITECTURE

HashiCorp Vault Components

- Storage backends
- Secrets Engines
- Auth methods
- Audit devices
- HTTP/API





ARCHITECTURE

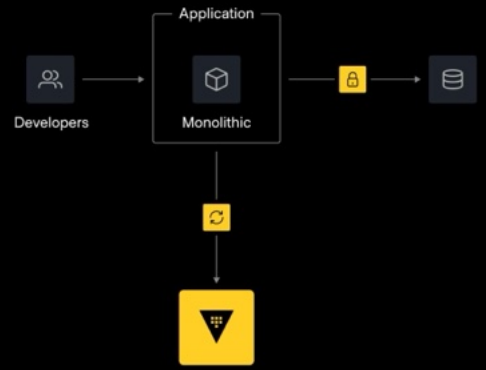
HashiCorp Vault workflow

1. A client provides credentials (ID) to Vault requesting access.
2. Vault uses authentication plugins to validate the client against the appropriate trusted third-party resource, such as GitHub, LDAP, CSP, or others.
3. Vault grants access to secrets and encryption capabilities by issuing a token tied to policies associated with the client's identity.
4. Client uses policy-based access to retrieve secrets, keys, and certificates, and perform other operations like data encryption.
5. Static secrets can be centrally managed and automatically synced to destination sources.
6. Detailed logs retained for monitoring and compliance.

Basic secrets management

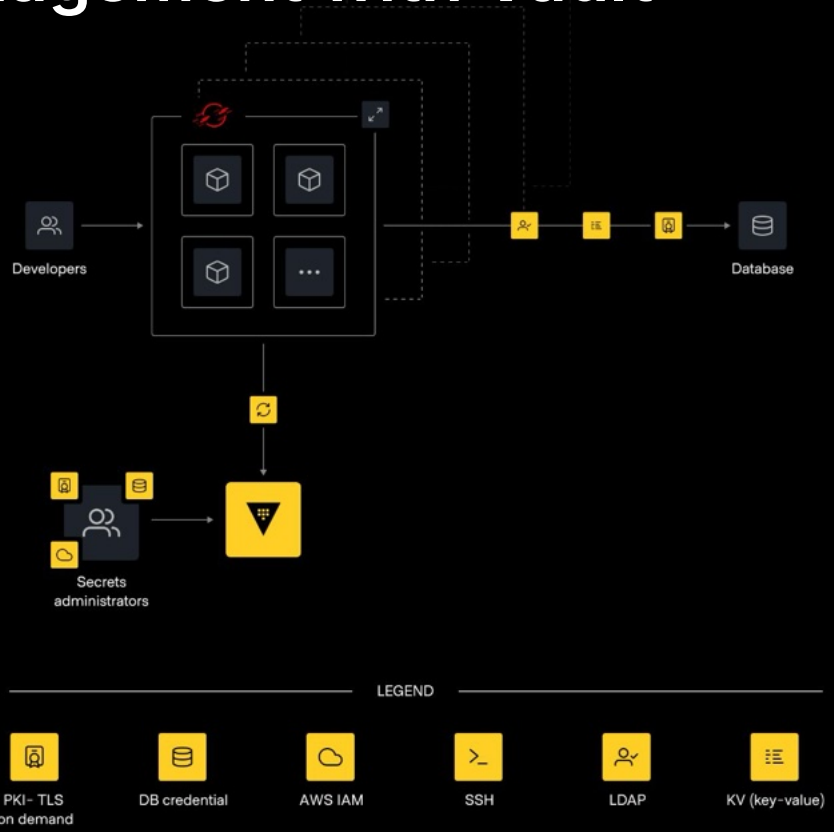
Vault can enable frequent iterative development with self-service while increasing security posture and maintaining your rigorous compliance requirements.

Decoupling the human element and integrating into common workflows reduces friction in the software development lifecycle, increases speed of delivery, and removes operational overhead.



OpenShift secrets management with Vault

- Automated secret injection at runtime
- Centralized identity and access policies
- Consistent secret delivery to all workloads



OpenShift secrets management with Vault

INTEGRATION OPTIONS

Vault Secrets Operator

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

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 Provider

- 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

WHAT IS IT?

- Provides Custom Resource Definitions (CRDs)
  - CRDs extend Kubernetes
- Kubernetes controller manager
  - Each controller is responsible for reconciling one or more Custom Resources
- Syncs Vault data to Kubernetes
- Provides secret transformation support e.g templating
- Caches all Secret data for reliable Pod auto scaling etc.

Vault Secrets Operator

CRDs OVERVIEW

VaultConnection

- Cluster address
- TLS Configuration

VaultAuth

- Vault authentication configuration

Vault*Secret

- Configuration necessary for syncing Vault secret data to K8s Secrets

* KV, PKI, Dynamic

Vault Secrets Operator

CRDs OVERVIEW

Vault*Secret

- Configuration for authenticating to HCP

SecretTransformation

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

K8s Secret

- Rendered/Transformed secret data

Vault Secrets Operator

INSTALLATION

Supported package management tools

- Helm: docs
- Kustomize: docs
- OpenShift: docs

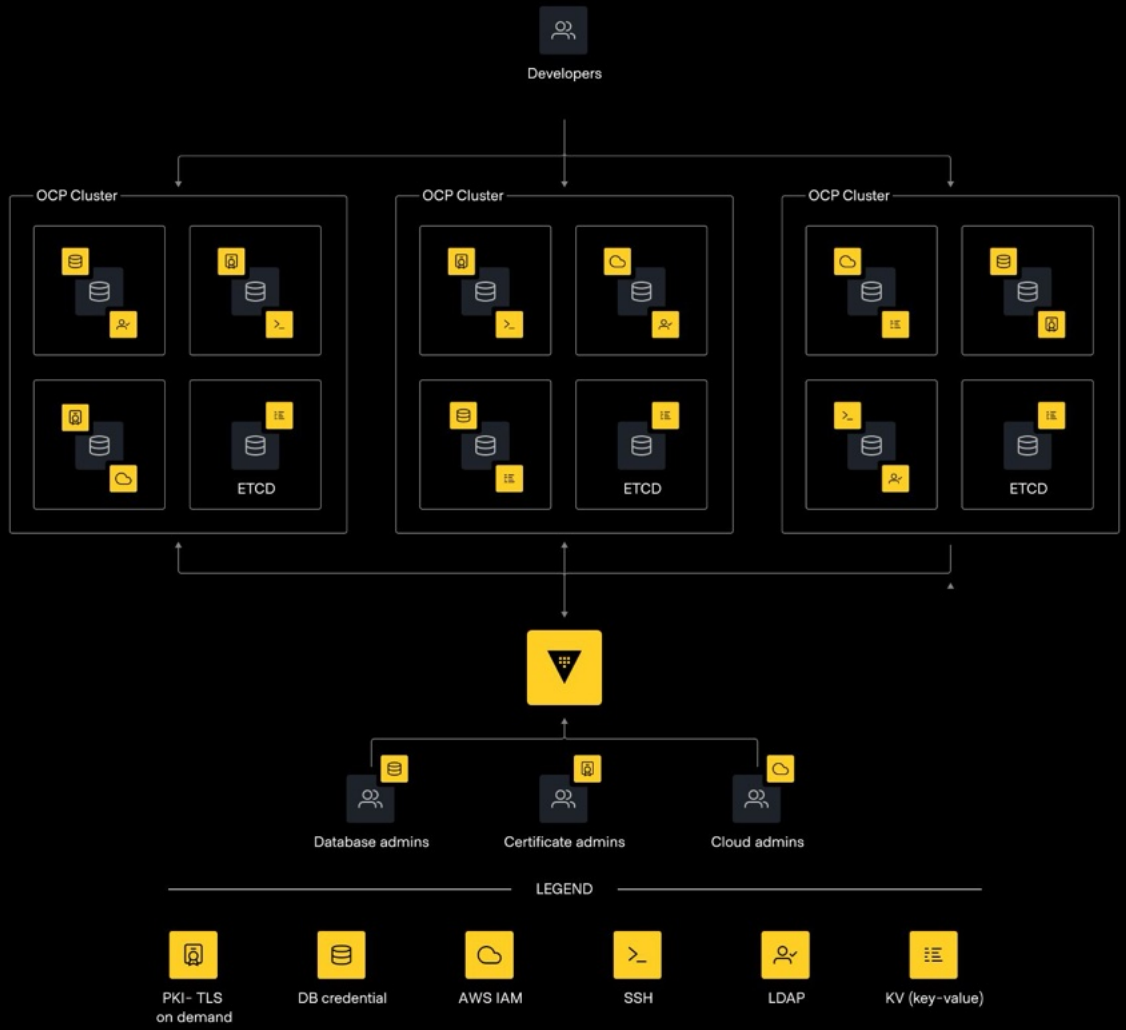
Example installation using Helm:

helm repo add hashicorp https://helm.releases.hashicorp.com

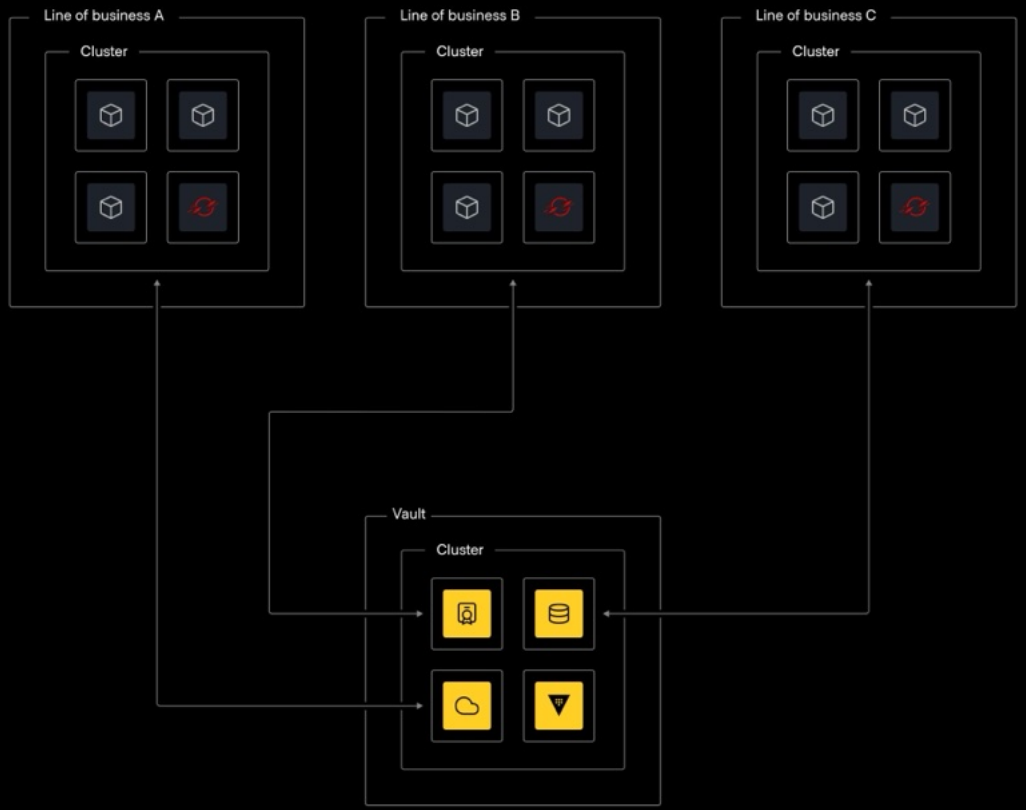
helm install --version 0.10.0 --create-namespace --namespace vault-secrets-operator vault-secrets-operator hashicorp/vault-secrets-operator

OpenShift secrets management with Vault

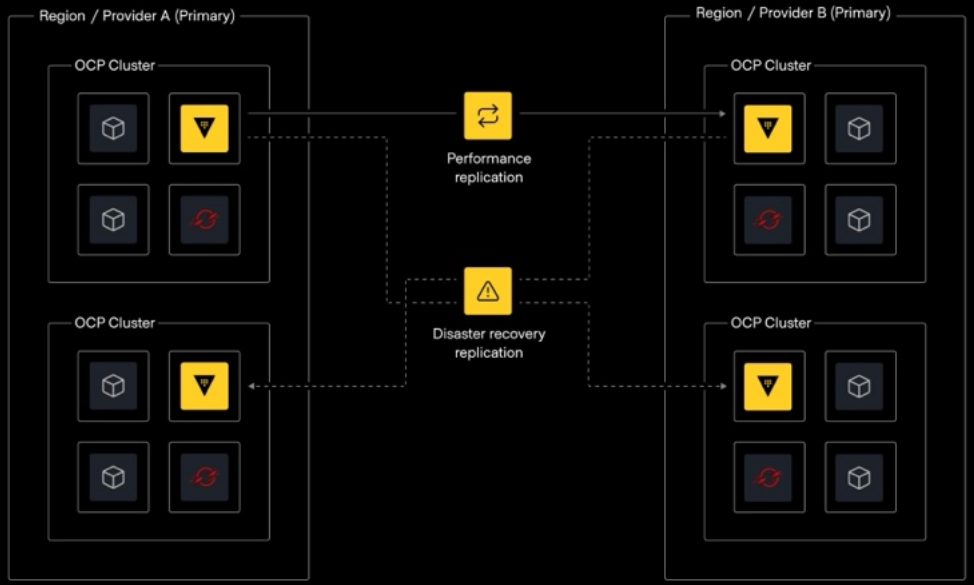
- Centralized management of secret estate
- Developers can focus on their applications
- Standardized deployment of all secrets



Secure multi-tenancy with Vault namespaces



Replication patterns with OpenShift and Vault



HashiCorp Vault

Secrets management
Centrally store, access, and distribute secrets programmatically

Certificate management
Generate, rotate, and revoke certifications on demand

Key management
Distribute, rotate, and disable cryptographic keys from a central location

Data protection
OpenShift KMS API integration to manage etcd encryption keys

Scaled operations
Isolate workloads for security and build for high availability across regions

Red Hat OpenShift

- Runtimes
- CI/CD
- Auth & SSO
- Cloud APIs
- Image build
- GitOps
- Service mesh
- Observability
- Serverless
- Image registry
- CVE scanning
- Enforce policy

Hybrid infrastructure

- Physical
- Virtual
- Private cloud
- Public cloud
- Edge

References

- Vault Documentation
- Vault Secrets Operator
  - API Reference
  - GitHub Project
  - Tutorial
- Vault Config Operator
  - GitHub Project
- Validated Designs
  - Vault Solution Design
  - Vault Operating Guide
    - For Adoption
    - For Standardization
    - For Scale
- Vault Validated Patterns
- Red Hat - The state of Kubernetes security report

Thank you