Vault Operator

Ned Bellavance

HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

Native Integration

Simplest option

No additional resources

Most difficult to execute

Vault Agent Injector

- Include Vault container in pod
- Init or sidecar container
- Performs authentication and secret retrieval
- Pass secrets with shared volume
- Init for static secrets
- Sidecar for dynamic secrets

Vault CSI Provider

Container storage interface

Secret store volume type

Presentation options

- Volume
- Kubernetes secret
- Environment variable

Runs as a daemonset

Vault Secrets Operator

- Runs as a Kubernetes operator
- Uses custom resource definitions
- Synchronizes to Kubernetes secrets
- Operator handles secret lifecycle

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset
Secrets types	All	All	All

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset
Secrets types	All	All	All
Presentation options	Shared volume or environment variable	Ephemeral disk, environment variable, Kubernetes secret	Kubernetes secret

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset
Secrets types	All	All	All
Presentation options	Shared volume or environment variable	Ephemeral disk, environment variable, Kubernetes secret	Kubernetes secret
Lifecycle management	Secret rotation and caching	None	Secret rotation and caching

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset
Secrets types	All	All	All
Presentation options	Shared volume or environment variable	Ephemeral disk, environment variable, Kubernetes secret	Kubernetes secret
Lifecycle management	Secret rotation and caching	None	Secret rotation and caching
Templates	Supported	None	Data transformation

Kubernetes Integration Selection

Option	Agent Injector	CSI Provider	Secrets Operator
Auth methods	Agent methods	Kubernetes	Special subset
Secrets types	All	All	All
Presentation options	Shared volume or environment variable	Ephemeral disk, environment variable, Kubernetes secret	Kubernetes secret
Lifecycle management	Secret rotation and caching	None	Secret rotation and caching
Templates	Supported	None	Data transformation
Deployment mode	Container per pod	Daemonset	Operator pods

Vault Secrets Operator

VSO Features

- Sync from multiple sources
- Automatic secret drift detection and remediation
- Automatic secret rotation
- Secret data transformation

VaultConnection

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultConnection
metadata:
  namespace: vso-system
  name: vault-prod-connection
spec:
  address: https://vault-prod.vault.svc.cluster.local:8200
  headers:
    X-VSO-Cluster: cluster1
```

VaultAuth

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultAuth
metadata:
  namespace: web-app
  name: web-app-auth
spec:
  vaultConnectionRef: vso-system/vault-prod-connection
  method: kubernetes
  mount: kubernetes
  kubernetes:
    role: web-app
    serviceAccount: web-app-sa
```

VaultAuth

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultAuth
metadata:
  namespace: web-app
  name: web-app-auth
spec:
  vaultConnectionRef: vso-system/vault-prod-connection
  method: kubernetes
  mount: kubernetes
  kubernetes:
    role: web-app
    serviceAccount: web-app-sa
```

VaultStaticSecret

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  namespace: web-app
  name: web-app-api-keys
spec:
  vaultAuthRef: web-app-auth
  type: kv-v2
  mount: secret
  path: web-app/api-keys
  destination:
    name: web-app-api-keys
    create: true
    transformation:
      transformationRefs:
        - name: vso-templates
  refreshAfter: 30s
```

VaultStaticSecret

```
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  namespace: web-app
  name: web-app-api-keys
spec:
  vaultAuthRef: web-app-auth
  type: kv-v2
  mount: secret
  path: web-app/api-keys
  destination:
    name: web-app-api-keys
    create: true
    transformation:
      transformationRefs:
        - name: vso-templates
  refreshAfter: 30s
```

VaultStaticSecret

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  namespace: web-app
  name: web-app-api-keys
spec:
  vaultAuthRef: web-app-auth
  type: kv-v2
  mount: secret
  path: web-app/api-keys
  destination:
    name: web-app-api-keys
    create: true
    transformation:
      transformationRefs:
        - name: vso-templates
  refreshAfter: 30s
```

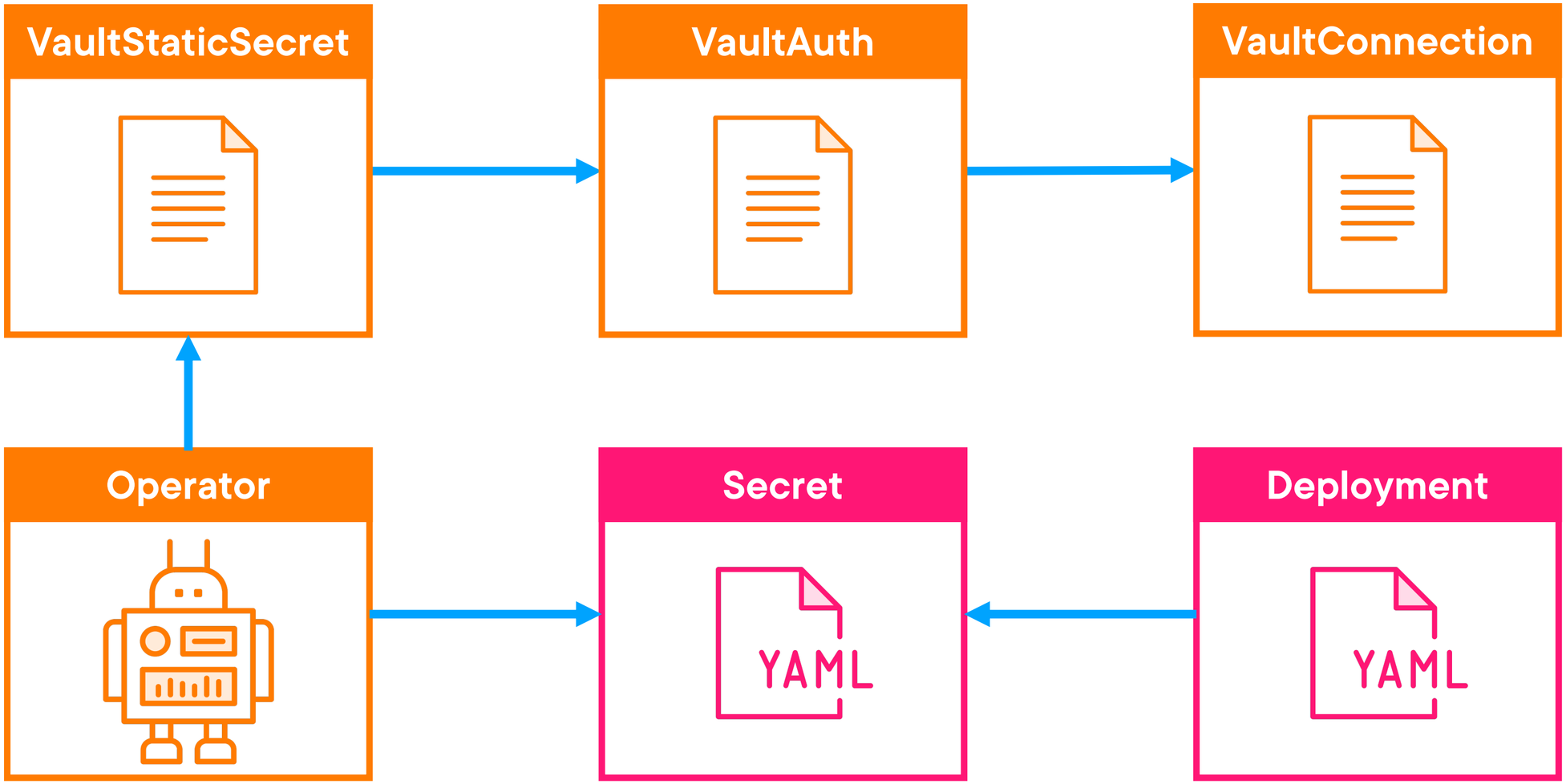
VaultStaticSecret

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  namespace: web-app
  name: web-app-api-keys
spec:
  vaultAuthRef: web-app-auth
  type: kv-v2
  mount: secret
  path: web-app/api-keys
  destination:
    name: web-app-api-keys
    create: true
    transformation:
      transformationRefs:
        - name: vso-templates
  refreshAfter: 30s
```

VaultStaticSecret

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  namespace: web-app
  name: web-app-api-keys
spec:
  vaultAuthRef: web-app-auth
  type: kv-v2
  mount: secret
  path: web-app/api-keys
  destination:
    name: web-app-api-keys
    create: true
    transformation:
      transformationRefs:
        - name: vso-templates
  refreshAfter: 30s
```

Secret Creation



Running the Vault Secrets Operator

Create a Kubernetes cluster with Vault and VSO installed, and then configure the necessary CRDs and Vault settings to retrieve a secret