Managing Secrets on OpenShift

HashiCorp Vault Helm chart has been updated with RedHat OpenShift 4.X support and Officially Certified by Red Hat.

HashiCorp Vault Helm chart has been updated with RedHat OpenShift 4.X support. With the release of OpenShift 4.8, it has also been officially certified by Red Hat. We have extended the existing Helm chart to support installing and running Vault Enterprise on OpenShift. Using the Helm chart, you will be able to use annotations to inject secrets, via sidecar injection, into applications with no native HashiCorp Vault logic built-in to leverage static and dynamic secrets sourced from Vault.

HashiCorp’s Vault Helm chart also supports a Vault Agent, which performs three functions: It authenticates with Vault using a configured authentication method. It stores the Vault token in a sink file like /var/run/secrets/vaultproject.io/token, and keeps it valid by refreshing the token at the appropriate time.

The latest release of HashiCorp’s Vault Helm chart has also been enhanced with the Template functionality, which allows Vault secrets to be rendered to files using Consul Template markup.

Executive summary

Companies are adopting Kubernetes at scale and are using OpenShift, but need to utilize external secrets management. Using the Helm Chart for Vault, you can start a Vault cluster running on Kubernetes in just minutes. The Helm chart allows you to run Vault directly on Kubernetes, so in addition to the native integrations provided by Vault itself, any other tool built for Kubernetes can choose to leverage Vault. HashiCorp together with Red Hat can thus support enterprises running their applications in a secure manner on OpenShift.

Product profile

HashiCorp Vault empowers you to secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.

Product Principles

API Driven: Enable automation and CI/CD use cases while enabling policy to codify, protect, and govern access to secrets.

Secure with any Identity: Leverage any trusted identity provider, such as cloud IAM platforms, Kubernetes, Active Directory, to authenticate into Vault. Identity is scale independent, unlike IP addresses, which require complex firewall rules and frequent updates.

Extend and Integrate: Request secrets for any system through one consistent, audited, and secured workflow. Vault supports public clouds and private datacenters, and a broad range of endpoint systems including databases, cloud platforms, messaging queues, SSH, and more.

The Vault Helm chart is the recommended way to install and configure Vault on OpenShift. In addition to running Vault itself, the Helm chart is the primary method for installing and configuring Vault to integrate with other services such as Consul for High Availability (HA) deployments.
“Developers and architects looking to build new applications in, and for the cloud, or migrate existing applications to a cloud-based infrastructure, partner with Red Hat to develop and deliver more supportable solutions sooner. Red Hat certification assures a supportable platform for all types of customer deployment models. Red Hat is thrilled to work with software partners like, HashiCorp, resulting in the world’s largest open, and commercially supportable application ecosystem.”

Product benefits
The Vault Agent Injector alters pod specifications to include Vault Agent containers that render Vault secrets to a shared memory volume using Vault Agent Templates. By rendering secrets to a shared volume, containers within the pod can consume Vault secrets without being Vault aware.

The Vault Agent performs three functions:

- It authenticates with Vault using a configured authentication method using the Kubernetes authentication method.
- It stores the Vault token in a sink file like /var/run/secrets/vaultproject.io/token, and keeps it valid by refreshing it at the appropriate time.
- The latest feature from Vault Agent is the template, which allows Vault secrets to be rendered to files using Consul Template markup.

Use cases

- Vault helps to manage and standardized control workflows for Red Hat databases:
  - Simplify secrets management. Generate and manage secrets for Red Hat database users and programmatic API keys with HashiCorp Vault.
  - Standardize and control workflows. Manage access to Red Hat databases in the same way as other cloud tools and services with HashiCorp Vault.
  - Cloud-first and platform agnostic. HashiCorp Vault and Red Hat make it easy to programmatically secrets across cloud providers and platforms.

About Partner
HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open-source tools with features that promote collaboration, operations, governance, and multi-data center functionality.

About Red Hat
Red Hat is the world’s leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.