

Securing your secrets using vault-k8s in Kubernetes — Part 2

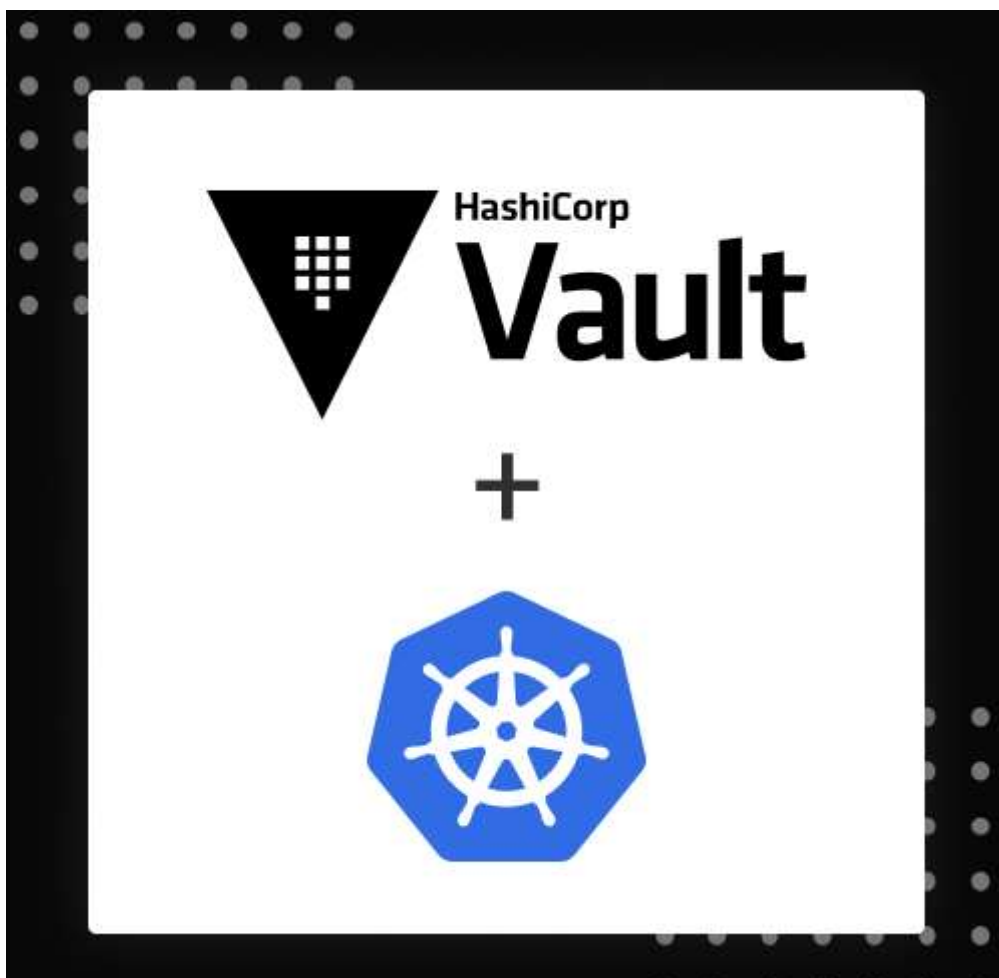


Pavan Kumar

Jul 18, 2020 · 3 min read

In Part 1 of this series, we have learned how to Install Vault-k8s and enable the Kubernetes Auth Mechanism. In this tutorial let's learn how automatically inject these secrets into our Kubernetes Deployments/Pods.

I have used Helm to create the manifests files. Helm charts are easier to create, version, share, and publish. Copying-and-Pasting the same manifests across multiple environments can be avoided and the same charts can be re-used by maintaining a different final overrides file.



Kubernetes and Vault-k8s

1. Clone my git repository that contains all the helm files

```
git clone https://github.com/pavan-kumar-99/vault-secrets-injection-k8s.git
```

2. Now Install the helm chart to see the secrets being populated into the pods

```
helm install vault-generic vault-k8s/generic-secret-injection --dry-run #See if all the values are correct
```

```
helm install vault-generic vault-k8s/generic-secret-injection #This will install your application
```

3. Let us now check if the secrets are present in the pod

```
[root@master helm]# kubectl get pods -l app=vault-deployment
```

NAME	READY	STATUS	RESTARTS	AGE
vault-deployment-6fb7f	2/2	Running	0	111s

```
[root@master helm]# kubectl exec -it vault-deployment-6fb7f -- /bin/bash
```

```
root@vault-deployment-6fb7f5cfc7:/# cat /vault/secrets/prod
Username is pavankumar and Password is Kubeadm
```

Now let us understand how the actual reason behind this magic

```
Open the file :
vim vault-k8s/generic-secret-injection/templates/deployment.yaml
```

Let us understand why these annotations are used:

1. vault.hashicorp.com/agent-inject = true. This parameter specifies If the injection is enabled for a pod.

2. vault.hashicorp.com/agent-inject-<secret-name> = <path where the secret is located>. This parameter configures Vault Agent to retrieve the secrets from Vault required by the container.
3. vault.hashicorp.com/role = <role-name>. This parameter configures the Vault role used by the Vault Agent
4. vault.hashicorp.com/agent-inject-template-<secret-name> = This parameter configures the template Vault Agent should use for rendering a secret.

Hurrah !! We successfully injected a generic secret into our pod from vault-k8's. In my next article, we will learn how to secure our Tls certificates using vault-k8s.

References Used:

Agent Sidecar Injector Annotations | Vault by Hashicorp

The following are the available annotations for the injector. These annotations are organized into two sections: agent...


www.vaultproject.io

Injecting Vault Secrets Into Kubernetes Pods via a Sidecar

We are excited to announce a new Kubernetes integration that enables applications with no native HashiCorp Vault logic...

www.hashicorp.com

 **Join FAUN today and receive similar stories each week in your inbox!** Get your weekly dose of the must-read tech stories, news, and tutorials.

Follow us on [Twitter](#)  and [Facebook](#)  and [Instagram](#)  and join our [Facebook](#) and [Linkedin](#) Groups 



If this post was helpful, please click the clap 🖐️ button below a few times to show your support for the author! ↓

[Kubernetes](#)[Vault](#)[Hashicorp Vault](#)[Vault K8s](#)[Kubernetes Secret](#)[About](#) [Help](#) [Legal](#)

Get the Medium app

