Hashicorp Vault

Durée 2 jour(s) (VAULT)

Savoir mettre en place et utiliser le gestionnaire de secret Hashicorp Vault.

Description

HashiCorp Vault est un système de gestion des secrets (clés de chiffrement, mots de passe, certificats) et du chiffrement basé sur l'identité. Vault assure le stockage, l'auditabilité et la tracabilité de vos secrets, et ce de manière sécurisée. Pendant cette formation, vous apprendrez à installer, configurer et utiliser Hashicorp Vault OSS. Nos ateliers pratiques, fournissant des environnements pré-configurés vous permettront de manipuler et de vous familiariser avec l'outillage et l'ecosystème Vault.

Objectifs

- Gérer des identités
- Déployer et configurer Vault
- Gérer les accès aux secrets
- Appréhender et utiliser les moteurs de secrets
- Utiliser le chiffrement "as a service"
- Comprendre l'architecture de Vault
- Interagir avec l'API de Vault avec le client Vault et son interface graphique

Public

- Développeur
- Administrateur système
- Architecte logiciel / système
- DevOps / SRE / Platform Engineer

Prérequis

- Savoir utiliser un outil en ligne de commande (utilisation d'un terminal)
- Comprendre les concepts de base de la cryptographie

Répartition

60% Théorie, 40% Pratique

Evaluations des acquis

L'évaluation des acquis de la formation se fera en séance au travers d'ateliers, d'exercices et/ou de travaux pratiques. Dans le cas d'une formation officielle éditeur, veuillez nous consulter afin que nous vous fassions part des modalités d'évaluation.

A l'issue de la formation, vous sera transmis une évaluation à chaud de l'action de formation qui vous permettra de nous faire part de vos retours quant à votre expérience apprenant avec Zenika.

Ressources pédagogiques

Les ressources pédagogiques proviennent de productions des équipes Zenika et/ou de la documentation éditeur dans le cas d'une formation "Officielle". Les documents sont en français ou en anglais.

RQTH et ma formation Zenika

Si vous êtes sujet à un handicap, prenez contact avec nos équipes pour que nous puissions définir ensemble comment nous pourrons aménager la session afin que vous puissiez vivre une expérience en formation inchangée.

Programme

1. Introduction à Vault
    1. Présentation de Vault
    2. Architecture de Vault
    3. Les cas d'usage (secrets, chiffrement, authentification)
    4. Les concepts de base (secrets, leases, policies)
    5. Les différents modes d'authentification (token, approle, ...)
    6. Les différents moteurs de secrets (kv, transit, ...)
2. Interagir avec Vault
    1. Le client Vault
    2. L'interface graphique
3. La gestion des accès
    1. Les politiques d'accès
    2. Identités: les entités et les groupes
    3. La gestion des tokens
    4. L'Agent Vault et le Vault Proxy
4. Les moteurs de secrets (KV, Azure, Database, SSH,...)
5. Gérer les Vault leases
    1. Qu'est-ce qu'un bail (lease) Vault ?
    2. Gérer la révocation et le renouvellement des baux
6. Le Chiffrement "as a service": Transit