Be secret like a ninja with Hashicorp Vault
Whoami?

Mehdi LARUELLE
Cloud & Automation
@mehdilaruelle
Github Access
Table of contents

1. Contextualization
2. How does Vault work?
3. Steps to become a ninja
4. Demonstration
// Contextualization
Problem?

Hello,

Here your access to your DB:
- Username: DBuser
- Password:Password

$host = getenv('DB_HOST');
$dbname = getenv('DB_NAME');
$user = getenv('DB_USER');
$pass = "dev";
Vault ? Why ?
How does Vault work?
Methods & Engines

- LDAP
- RADIUS
- OKTA
- JWT
- Github

- Approle (pipeline)
- TLS Certificate
- Kubernetes
- JWT / OIDC
- AliCloud / Azure / AWS / GCP
- LDAP

Users → Auth methods → App
Steps to become a ninja
Steps to be a ninja

1. Find secrets
2. Put secrets in Vault
3. Make secrets dynamics
4. Encrypt sensitive data
Steps to be a ninja

- Find secrets
- Put secrets in Vault
- Make secrets dynamics
- Encrypt sensitive data
How is it working?

1. Send Secret ID
2. Auth with Approle
3. Get Token
4. Get secrets with Vault token
Steps to be a ninja

1. Find secrets
2. Put secrets in Vault
3. Make secrets dynamics
4. Encrypt sensitive data
Secret as a Service

1. Ask DB credentials
2. Vault create credentials into DB and retrieve it
3. Get credentials
4. Application use credentials to authenticate into DB
5. Ask to revoke credentials
6. Revoke credentials
Steps to be a ninja

Find secrets → Put secrets in Vault → Make secrets dynamics → Encrypt data
EaaS: Encryption as a Service

1. Put raw data
2. Get encrypted data
3. Put encrypted data
4. Get encrypted data
5. Put encrypted data
6. Get decrypted data
To infinity... and beyond!

- Vault Agent
- Consul service mesh
- envconsul
- and / or consul-template
- envconsul
- and / or consul-template
The last but not least

Trust nobody, not even yourself