

The background of the slide features a series of concentric circles composed of small, light-colored dots, creating a tunnel-like or ripple effect that draws the eye towards the center. The dots are more densely packed in some areas, giving a sense of depth and movement.

∞ Infisical

**Le meilleur ami des
devs pour des secrets
bien gardés !**

Julien Briault (@ju_hnny5)

#3615 Ma vie

Julien Briault

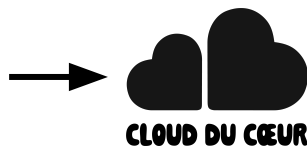
Uptime **26y**

Ingé réseau | SRE @



Auteur @ **Linux Pratique**

Responsable (bénévole) @



X @ju_hnny5



@jbriault.fr





CLOUD DU CŒUR



ceph



openstack®



VICTORIA
METRICS

∞ Infisical



PROXMOX



fluentbit



Canonical
MAAS

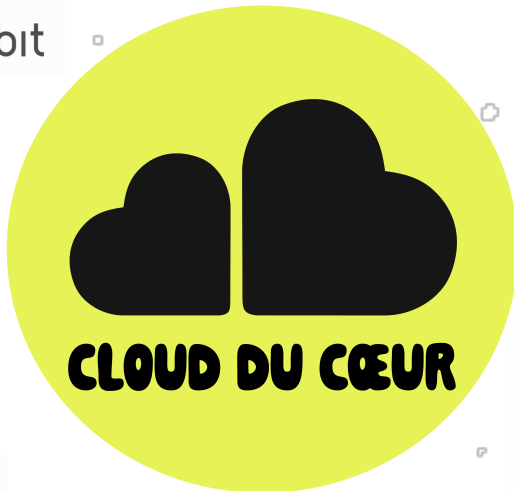
POWERDNS



Pulumi



NGINX



CLOUD DU CŒUR



GitLab



HAPROXY



Grafana



octoDNS



netbox



kubernetes



Consul

passbolt



Rudder



TELEPORT



HashiCorp
Terraform

wazuh.

@ju_hnny5

Nos besoins :

- Des bénévoles (devs, infra, gestion de projet)
- De l'hébergement en DC
(sur **Paris, Marseille** périphérie)
- Du matériel info
(réseau, ordinateurs portables, serveurs, consommable, etc)

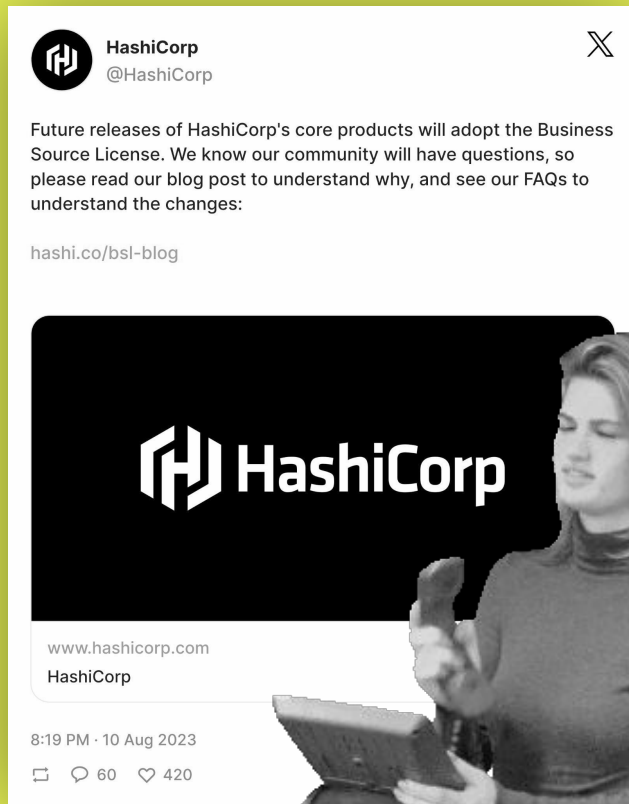


WE NEED YOU!



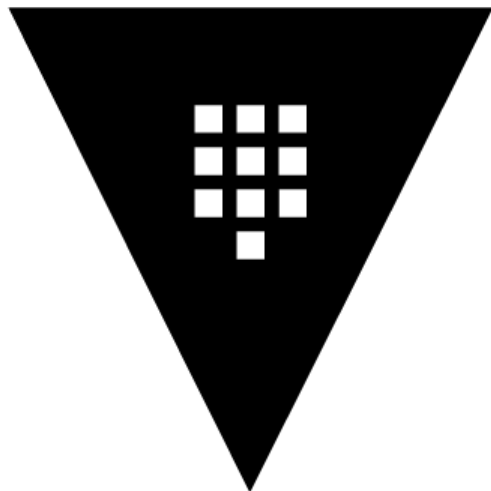
Mais ...
Pourquoi ce talk ?

Un peu de contexte ...



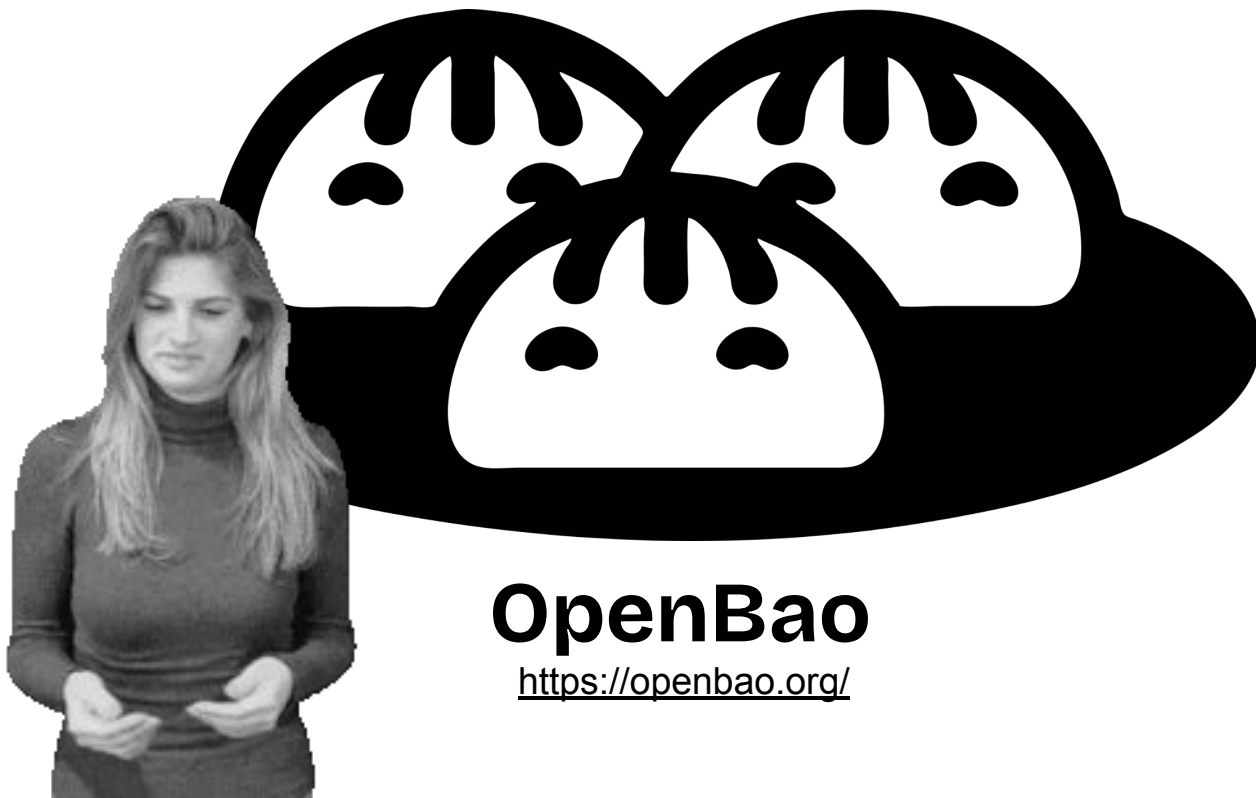
@ju_hnny5

**Un peu de
contexte ...**



HashiCorp
Vault

**Un peu de
contexte ...**



OpenBao

<https://openbao.org/>

@ju_hnny5

DEVOXX FRANCE 2024

12^{ème} EDITION - DU 17 AU 19 AVRIL 2024



Pulumi, ou comment gérer votre infrastructure avec votre langage préféré

<https://www.youtube.com/watch?v=IAwu-WCN6Nw>

@ju_hnny5

Pour des **secrets**
bien gardés ?

explain ?

**Tu entends quoi par
"secrets" ?**



@ju_hnny5



Fait référence à une
info sensible ou confidentielle



**Une info qui doit être protégée
contre tout accès non autorisé**

Un **secret**, qu'est-ce que c'est ?

- Ça peut prendre plusieurs formes :
 - **Mot de passe** (pour authentifier les utilisateurs/apps)
 - **Clés d'API** (pour les services web ou APIs)
 - **Certificats et clés crypto** (chiffrer/déchiffrer des données)
 - On dit ~~crypter~~ chiffrer
 - **Infos de configuration sensibles** (chaînes de connexion à une BDD, un paramètre de serveur)
 - **Données personnelles** (numéro de sécu)

Un peu de
technique ...

Infisical : Késako ?

- Outil **Open Source** de gestion, stockage et sécurisation des secrets* d'un projet, mais pas que !
- Environ **180 contributeurs**
- **Projet jeune** (né en 2022)

Nov 18, 2022

 maidul98

 v0.0.1

 90714dd

Compare ▾

v0.0.1

Changelog

- [bea0ff6](#) Add frontend, backend and CLI
- [90714dd](#) Merge branch 'main' of <https://github.com/Infisical/infisical> into main
- [8d00c5c](#) Start of open source
- [9b017c1](#) Updated Readme
- [a051490](#) remove furry.io and add cloud smith

► Assets 42

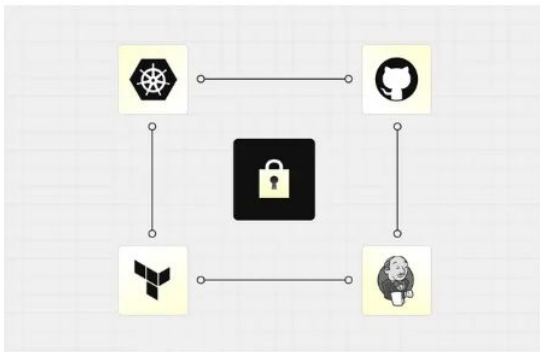


<https://github.com/Infisical/infisical>

@ju_hnny5

Infisical : Késako ?

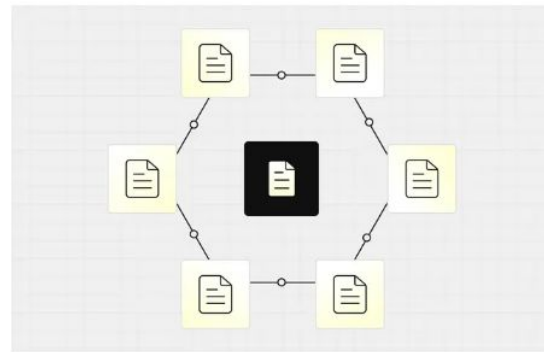
Qu'est-ce que ça fait ?



Secrets Management across Infrastructure



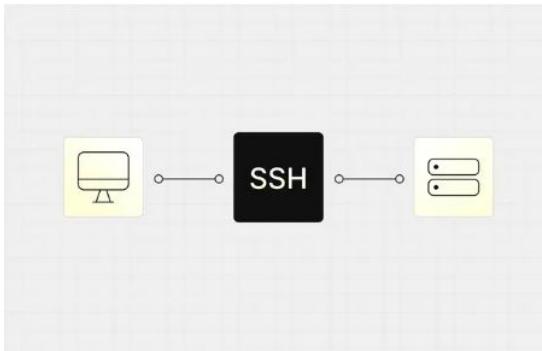
Dynamic Secrets & Secret Rotation



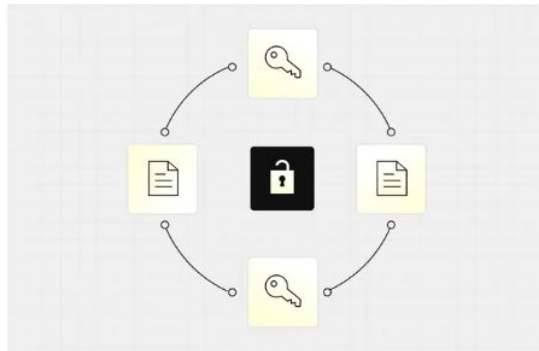
PKI

Infisical : Késako ?

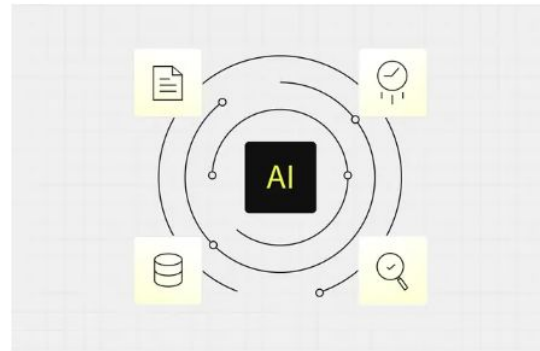
Qu'est-ce que ça fait ?



SSH



KMS



Security Advisor

Infisical : 2 versions



OSS

Enterprise

Infisical : 2 versions



Self-Hosted



SaaS



La gestion des identités

La gestion des identités

2 types :



Les humains



Les machines

La gestion des identités

2 types :

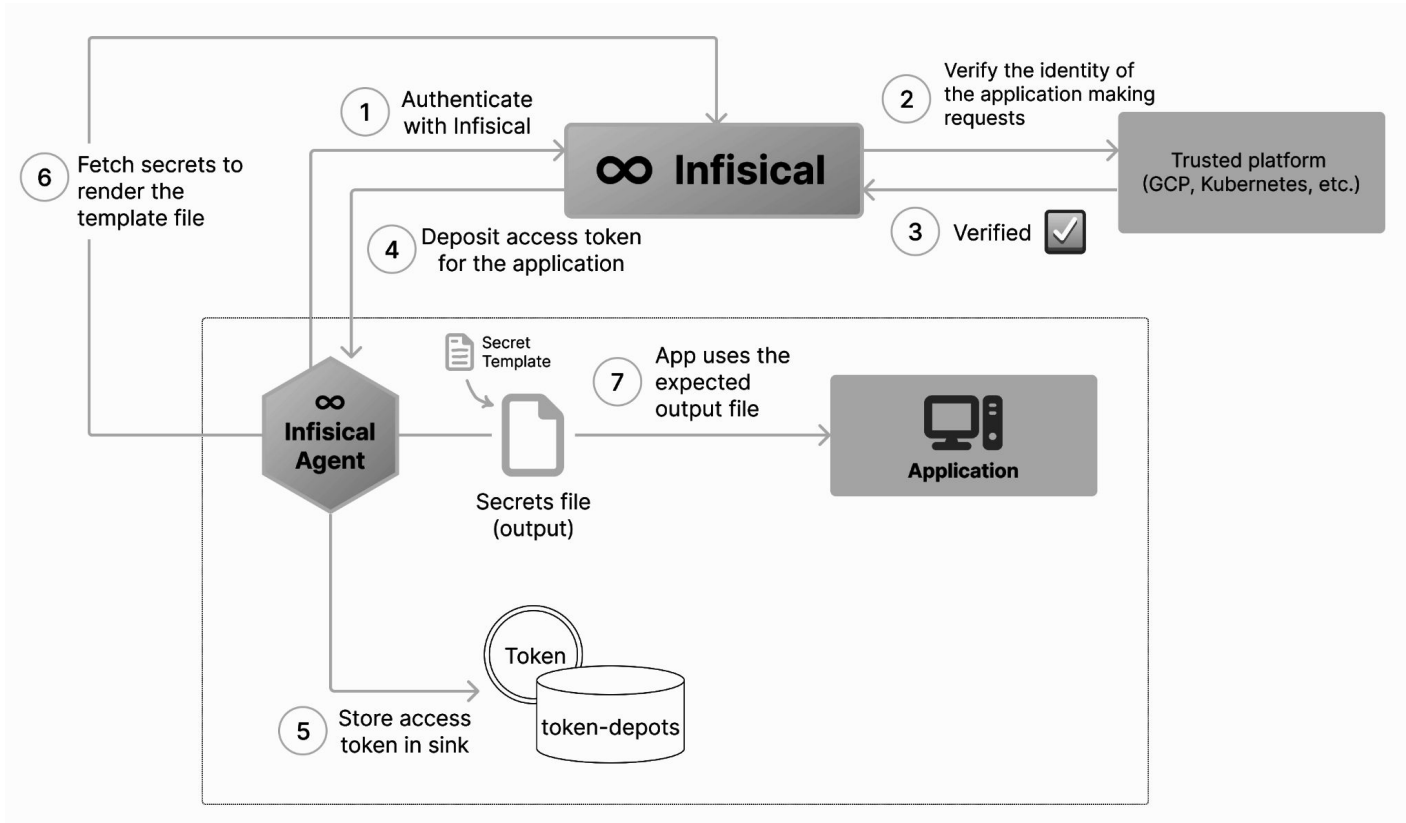
- **Les humains** : les devs, les platforms engineers (former SRE), les admins
- **Les machines** : dans une CI/CD (Gitlab par exemple), par des applications et bien plus !



**Un agent
Secret ?**

@ju_hnny5

Un agent secret ?



<https://infisical.com/docs/integrations/platforms/infisical-agent>

@ju_hnny5

A black and white photograph of a man sitting at a desk in a dimly lit room. He is looking at a computer monitor on the right, with his hand resting on his chin in a thoughtful pose. The desk is cluttered with various items, including a keyboard, a mouse, and some papers. The overall atmosphere is one of concentration and problem-solving.

**Et pour
les devs ?**

La gestion multi-envs

- Isoler pour mieux développer
 - Prod
 - Staging
 - Dev
 - Sandbox
- Fournit nativement par l'outil*
- Out of box



La gestion multi-envs

← **I** Infisical ▾

TD

PROJECT

Example Project ▾

🔒 Secrets

👤 Members

🔗 Integrations

🛡️ IP Allowlist

📋 Audit Logs

⚙️ Project Settings

🔍 ? Help & Support

I Infisical > Example Project > Secrets

Secrets Overview

Inject your secrets using **Infisical CLI** or **Infisical SDKs**

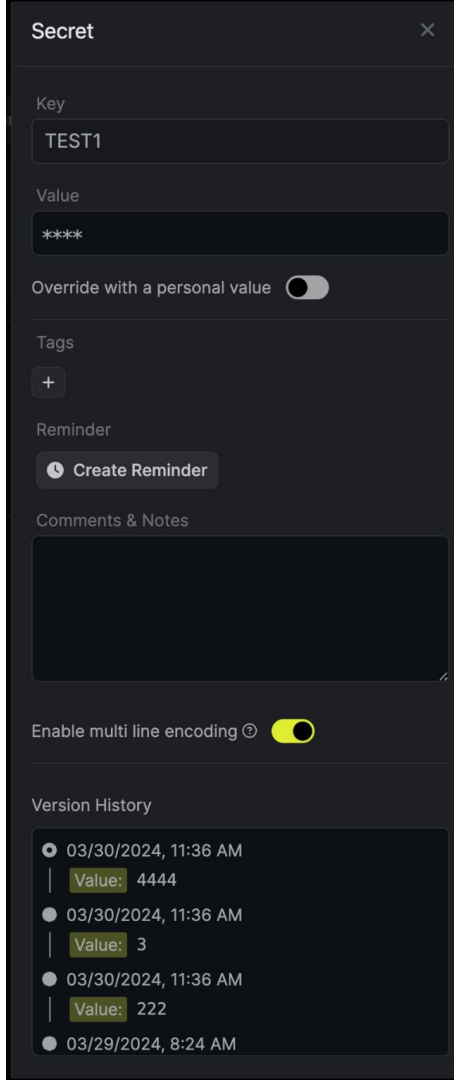
📁 users

🔍 Search by secret/folder name...

NAME ▾	Development	Staging	Production	Testing
📁 user-a	✓	✗	✗	✗
📁 user-b	✓	✗	✗	✗
📁 user-c	✓	✗	✗	✗
📁 user-d	✓	✗	✗	✗
📁 user-e	✓	✗	✗	✗
📁 user-f	✓	✗	✗	✗
	Explore	Explore	Explore	Explore

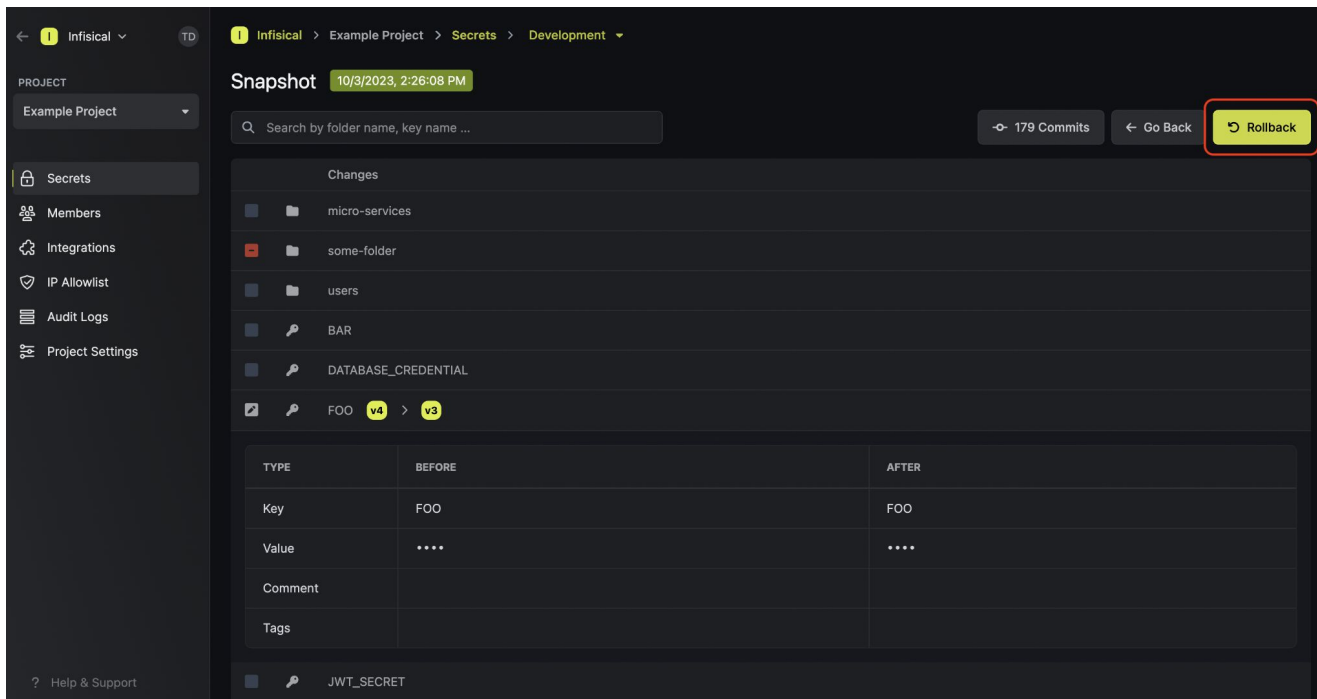
Le versioning

- Pratique en cas d'erreur
- Permet de déboguer plus facilement
 - Exemple : dans le cas d'un secret qui est remplacé automatiquement.



Le Point-in-Time Recovery

- Possibilité de faire :
 - des snapshots de ses secrets
 - des rollbacks



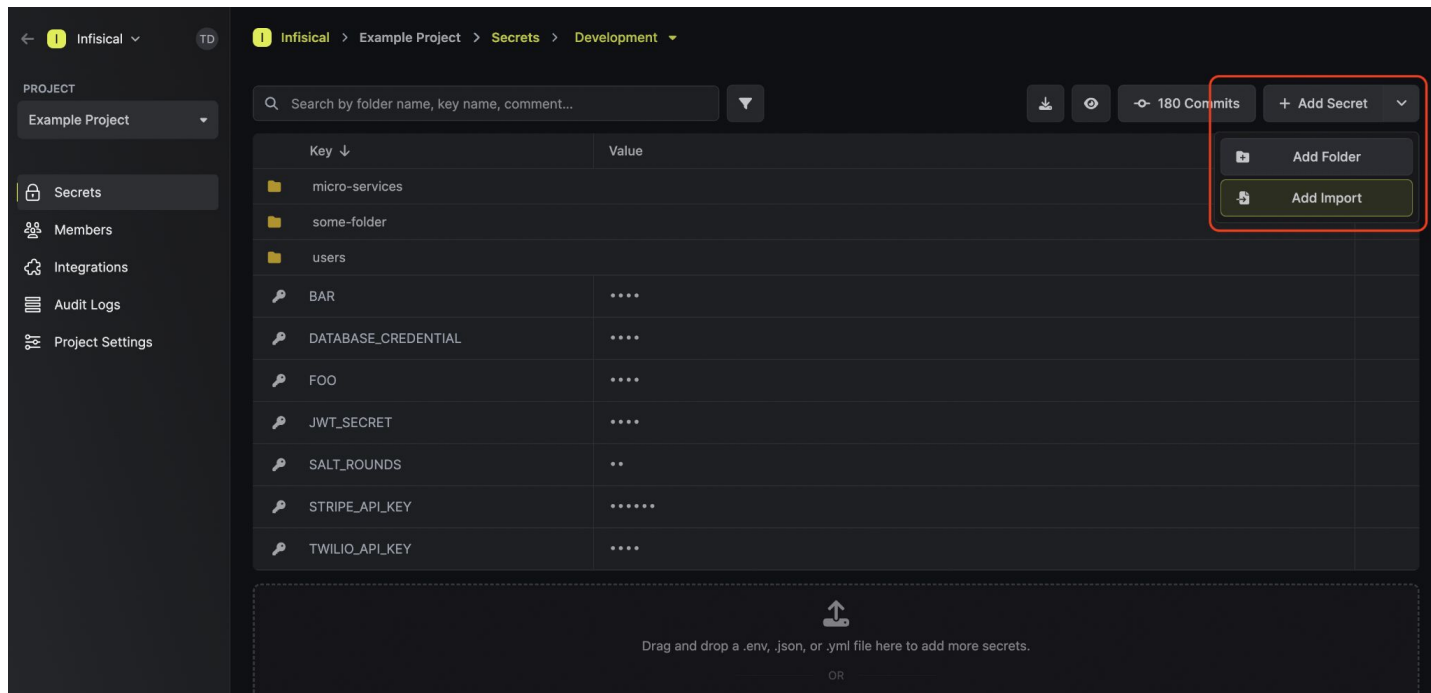
The screenshot displays the Infisical web application interface. The top navigation bar shows the breadcrumb path: **Infisical** > **Example Project** > **Secrets** > **Development**. The left sidebar contains a menu with options: PROJECT (Example Project), Secrets, Members, Integrations, IP Allowlist, Audit Logs, and Project Settings. The main content area is titled "Snapshot" with a timestamp "10/3/2023, 2:26:08 PM". Below the title is a search bar and three buttons: "179 Commits", "Go Back", and a highlighted "Rollback" button. The "Changes" section lists several items: "micro-services", "some-folder", "users", "BAR", "DATABASE_CREDENTIAL", and "FOO". The "FOO" item is expanded, showing a comparison between "v4" and "v3". A table below the comparison shows the "BEFORE" and "AFTER" states for the secret.

TYPE	BEFORE	AFTER
Key	FOO	FOO
Value	****	****
Comment		
Tags		

At the bottom of the interface, a "JWT_SECRET" is partially visible.

Importer des secrets

- Plusieurs méthodes existent :
 - Via la CLI dans un projet donné
 - Via la WebUI



Les intégrations

Don't hurt me no more

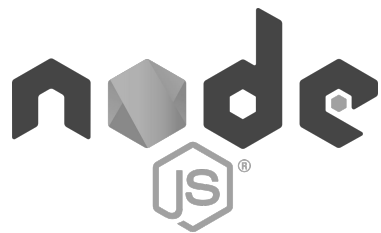
Don't hurt me no more

Les secrets d'un projet

Un **SDK** pour appeler des secrets dans son code

- Ecrit en Rust
- Cross-language

Pour le moment, pour uniquement ces langages/frameworks :



Java™



python™

<https://github.com/Infisical/sdk>

@ju_hnny5

Un provider



README Code of conduct MPL-2.0 license

Infisical Terraform Provider

Usage

```
terraform {
  required_providers {
    infisical = {
      # version = <latest version>
      source = "infisical/infisical"
    }
  }
}

provider "infisical" {
  host      = "https://app.infisical.com" # Only required if using self hosted instance of
  client_id = "<>"
  client_secret = "<>"
}

data "infisical_secrets" "common-secrets" {
  env_slug      = "dev"
  workspace_id = "PROJECT_ID"
  folder_path   = "/some-folder/another-folder"
}

data "infisical_secrets" "backend-secrets" {
  env_slug      = "prod"
  workspace_id = "PROJECT_ID"
}
```

<https://github.com/Infisical/terraform-provider-infisical>

@ju_hnny5



kubernetes

**des secrets pas si
secrets ...**



@ju_hnny5

**Kubernetes : des secrets, pas
très secrets ... Coucou Base64**



Kubernetes : des secrets, pas très secrets ...

- **Accessibles via l'API de Kube**
 - Ça peut être pratique mais pas hyper sécurisé ...
- **Stockage des secrets dans ETCD**
 - Facilement récupérable pour toute personne ayant accès à ETCD
- **Logs et dumps**
 - Peut se retrouver accidentellement dans les logs et dumps ... On a vu mieux !
- **Aucun chiffrement dans les repos**



Kubernetes : des secrets, pas très secrets ... **et avec Infisical ?**

- **Un opérateur**
 - Une helm chart pour installer
- **Les CRDs** (Custom Resource Definitions)
 - InfisicalSecret
 - InfisicalPushSecret
 - InfisicalDynamicSecret



Et via une CSI ?

- Injecter des secrets directement dans un Pod à travers un volume monté.
- A l'inverse de l'opérateur, il permet de synchroniser les secrets dans les pods (sous la forme de fichiers) sans avoir besoin de "Secret resources".

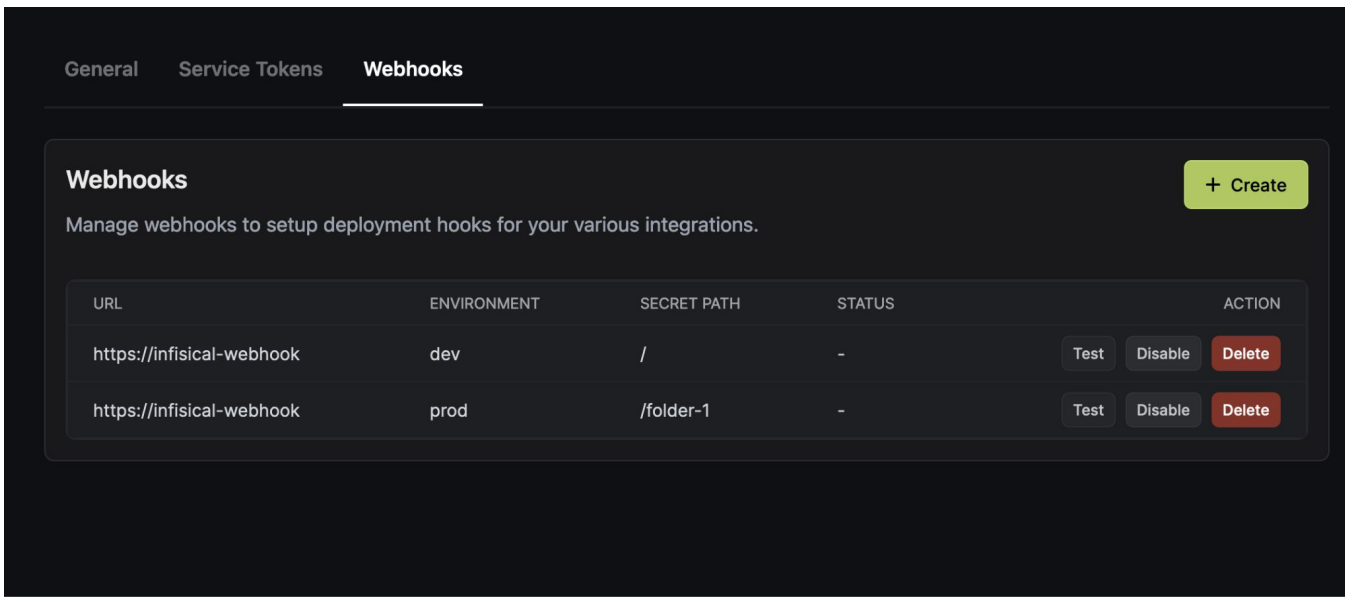


<https://infisical.com/docs/integrations/platforms/kubernetes-csi#kubernetes-csi>

Des notifications sur slack


Être notifié en cas de :

- Modifications
- Expiration d'un secret



The screenshot shows the Slack Webhooks management interface. At the top, there are tabs for 'General', 'Service Tokens', and 'Webhooks'. The 'Webhooks' tab is selected. Below the tabs, there is a section titled 'Webhooks' with a '+ Create' button. A description reads: 'Manage webhooks to setup deployment hooks for your various integrations.' Below this is a table with two rows of webhooks. The table has columns for 'URL', 'ENVIRONMENT', 'SECRET PATH', 'STATUS', and 'ACTION'.

URL	ENVIRONMENT	SECRET PATH	STATUS	ACTION
https://infisical-webhook	dev	/	-	<button>Test</button> <button>Disable</button> <button>Delete</button>
https://infisical-webhook	prod	/folder-1	-	<button>Test</button> <button>Disable</button> <button>Delete</button>



C'est l'heure de
~~tout casser~~
la **démo !**

**On dit “chiffre” et
pas “crypter” !**



Voila`

@ju_hnny5

Merci

DEVOX™ France



Un feedback ?



A black and white photograph of a man in a dark suit, white shirt, and patterned tie. He is looking down and slightly to his left. The background is dark and out of focus, showing some office equipment. Overlaid on the center of the image is the text "Merci pour votre attention !" in a bold, white, sans-serif font.

**Merci pour
votre attention !**

