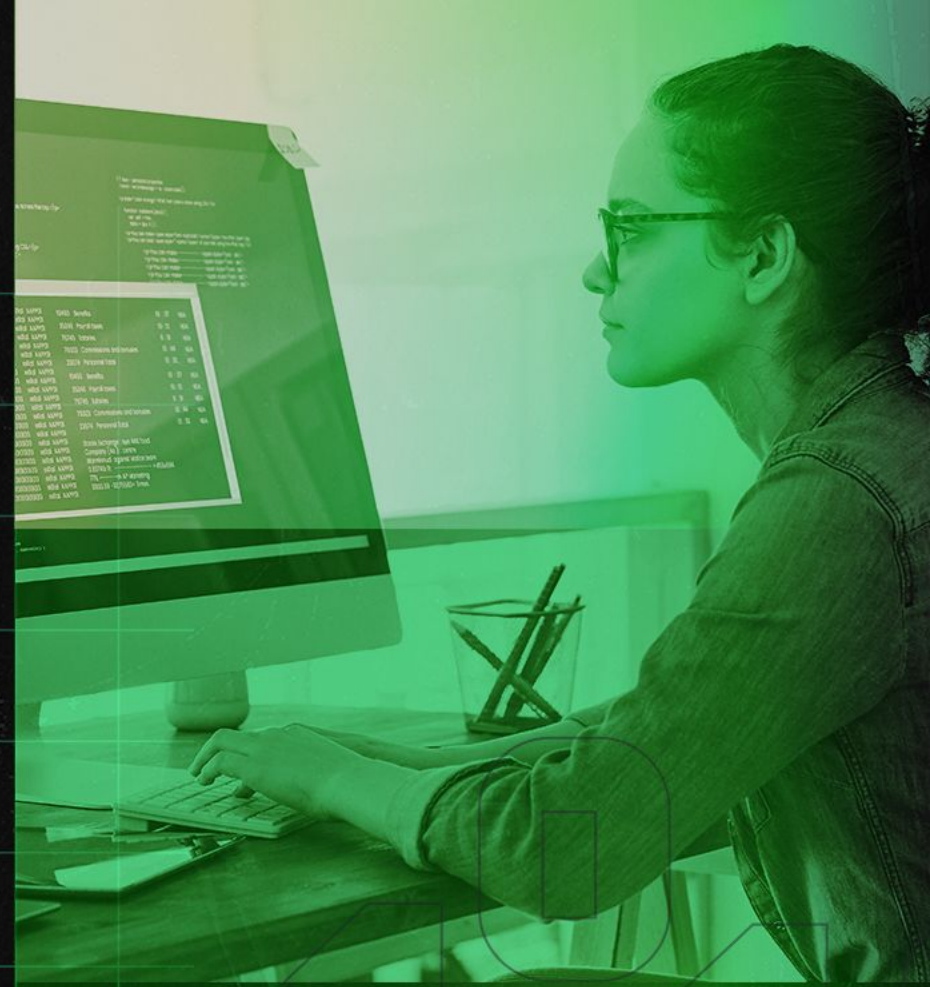
SOMOS

stone tech/



DevOps - Stone

Igor Sousa

Thiago Steiner

Ruan Arcega

Gerson Aquino

Vitor Sandes

stone tech

HashiTalks 2022

Obtendo credenciais de forma dinâmica com Hashicorp Vault & Kubernetes

Como usar o Vault sidecar Injector e Database Secret Engine para renderizar secrets de maneira segura.

stone tech/

Apps modernas e os novos padrões de gerenciamento de secrets

- Desacoplamento das secrets do ciclo de vida da aplicação
- Evitar exposição de secrets nos repositórios (SCM)
- Integração do kubernetes com sistemas externos de gerenciamento de secrets

stone tech

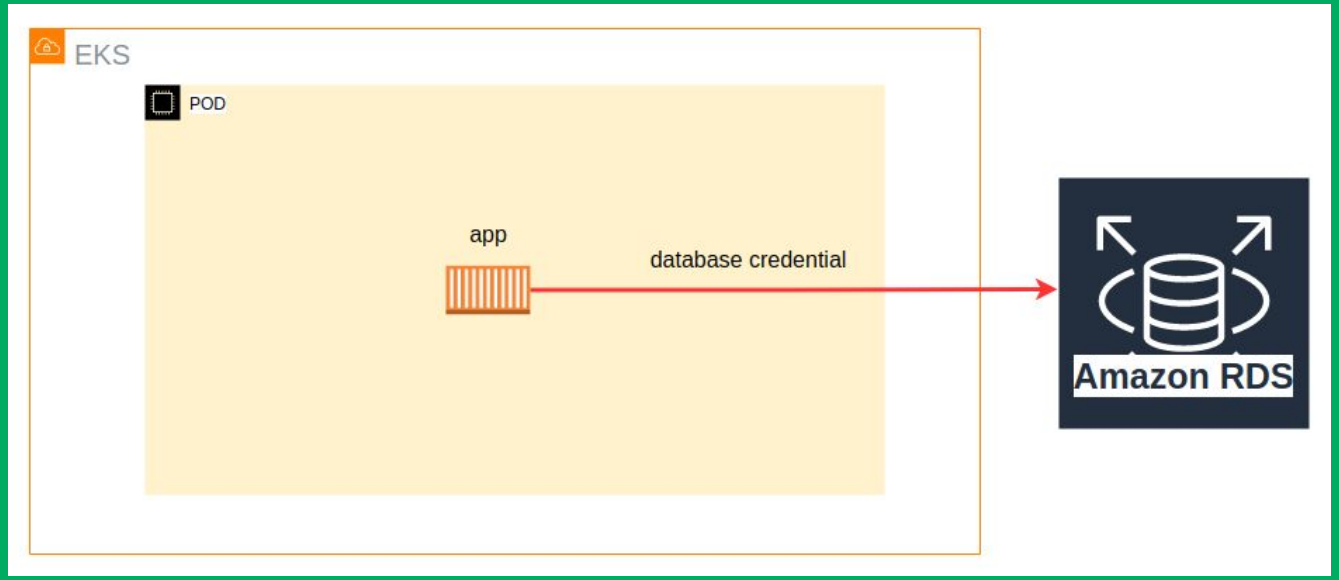
Como as aplicações recebem credenciais?

- Variáveis de ambiente
- Hardcode
- Arquivos

```go
func main() {
    log.Printf("Starting...")
    var cfg DBConfig
    var d DatabaseWrapper
    cfg.dbUser = "admin-db"
    cfg.dbPassword = "StrongPassword123"
    cfg.dbPort = "5432"
    cfg.dbName = "app_db"
    cfg.dbHost = "mydatabase.local"
```

stone tech

Como consumir as credenciais?



APP + EKS + RDS + VAULT

stone tech

Peças do nosso quebra-cabeça...

- **EKS**:
  - Service account
  - Vault Agent Sidecar Injector
  - IAM Roles for Service Account (IRSA)
  - POD annotations
  - Shared memory volume

- **Vault**:
  - Auth Backends: AWS, Kubernetes, App Role
  - Database Secret engines
  - Roles and Policies

- **RDS**
  - Credenciais de acesso
  - Role

- **APP**
  - Renderizar credenciais

stone tech

Database engine

- Criar credenciais dinâmicas
- TTL associado a credencial de acesso
- Renovação automática

stone tech

Sidecar Injector

- Faz alterações nos Pods via mutation webhook controller injeta o vault-agent-sidecar
- Observa k8s pod events de CREATE e UPDATE
- vault.hashicorp.com/agent-inject
- Renderiza as secrets num volume compartilhado

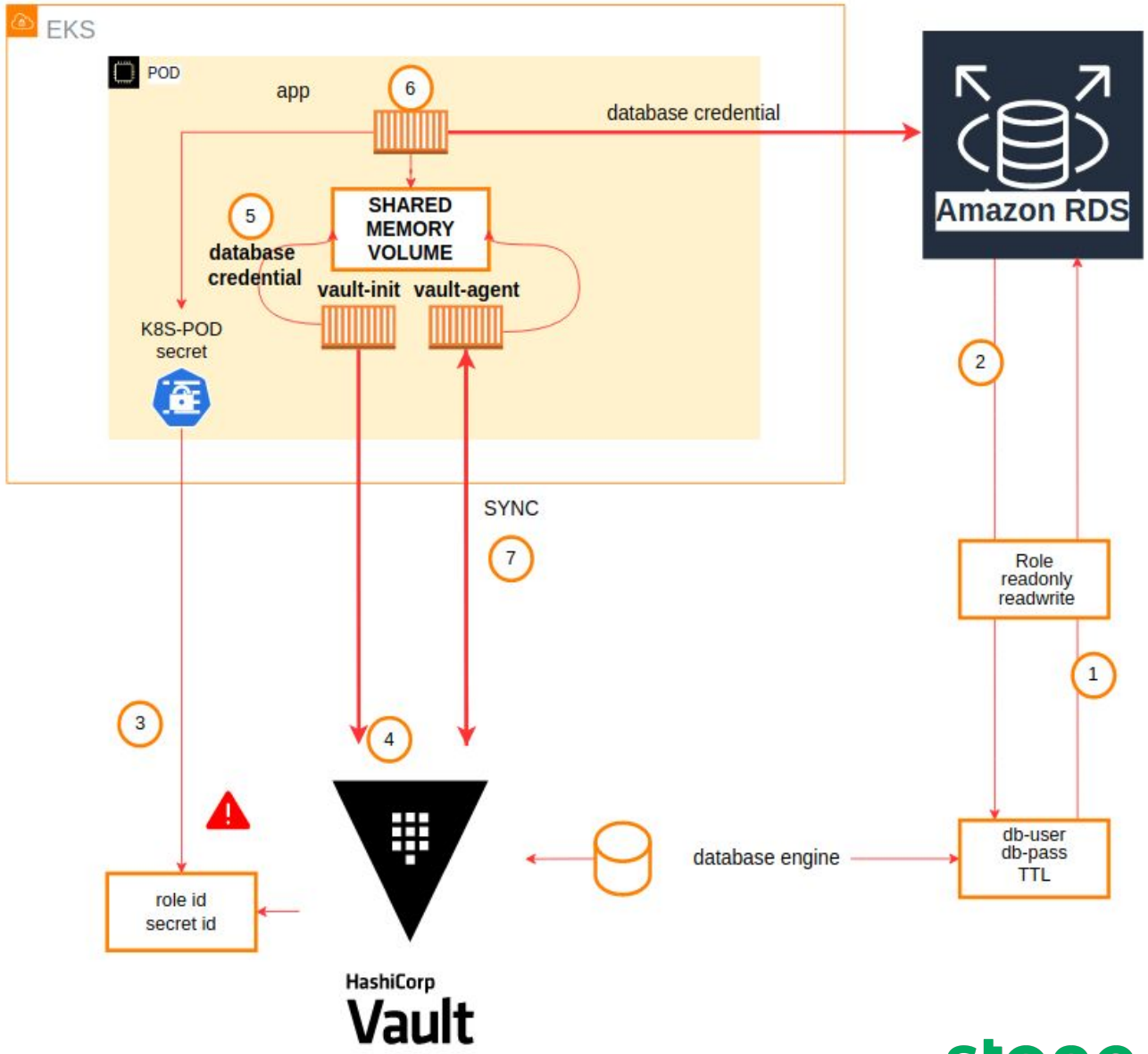
stone tech

Autenticação do Sidecar Injector

- App Role Auth
- Kubernetes Auth
- AWS Auth

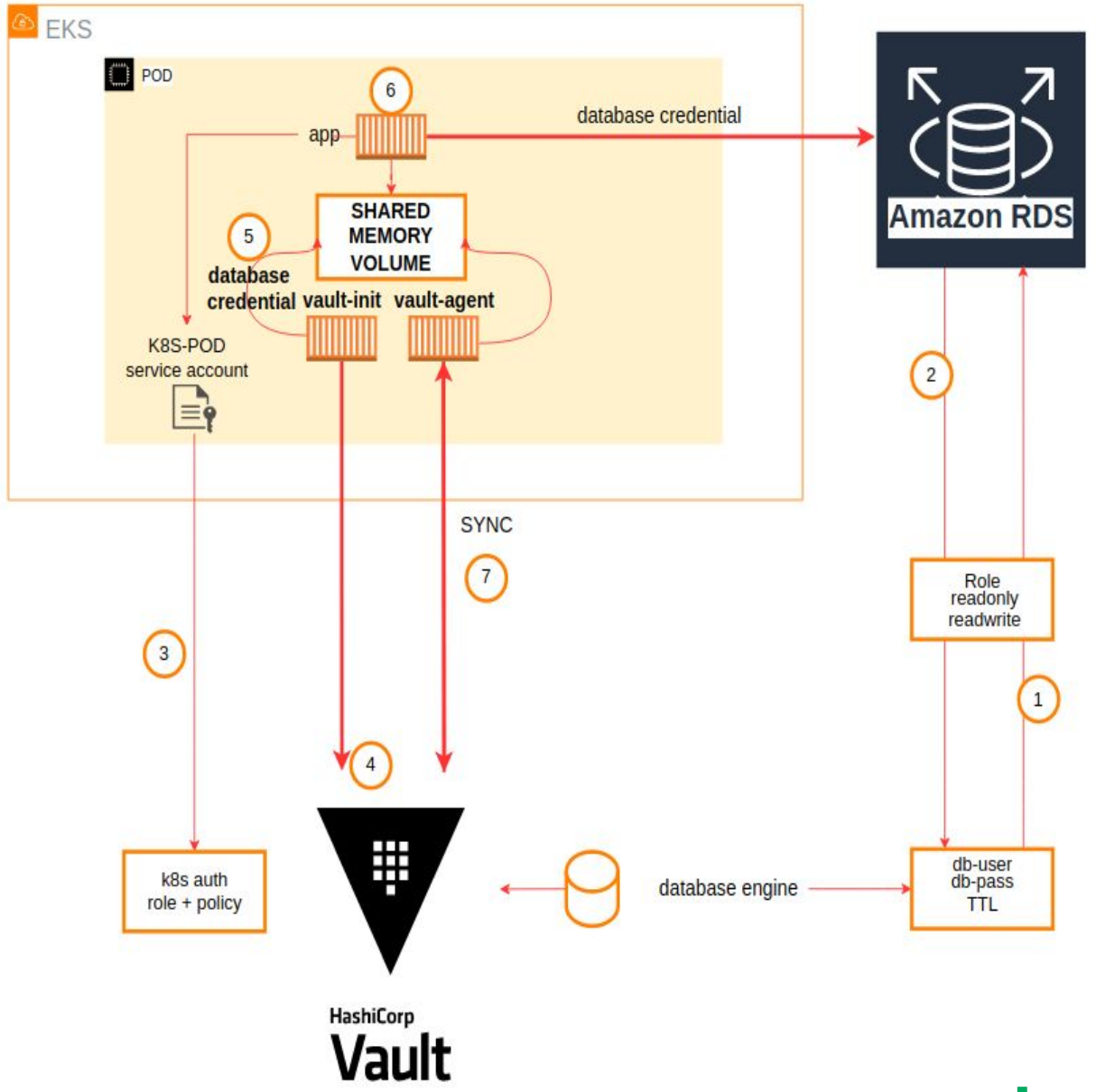
stone tech

Database Engine Sidecar Injector App Role



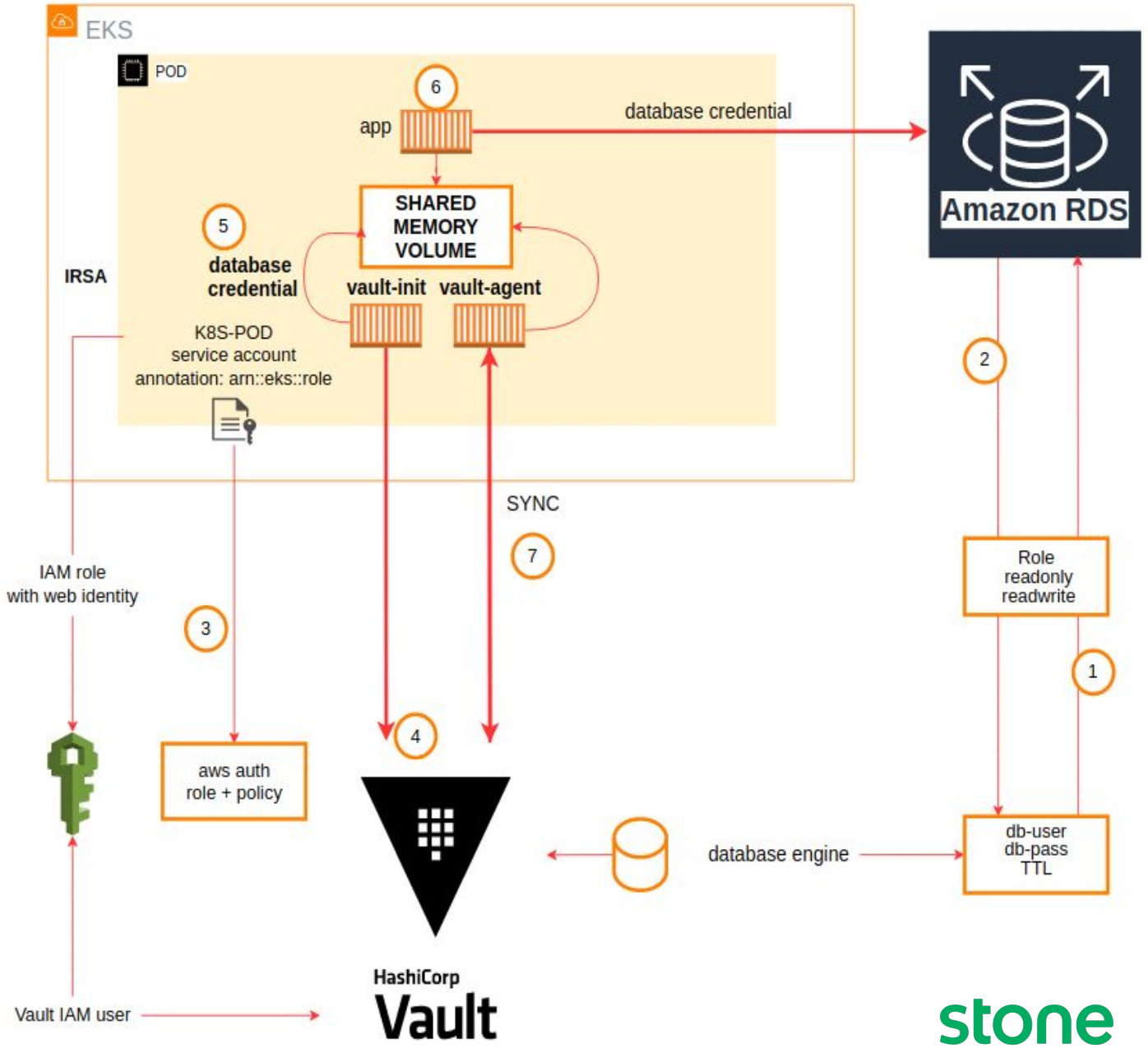
stone tech

Database Engine Sidecar Injector Kubernetes auth



stone tech

Database Engine Sidecar Injector AWS auth



stone tech

Talk is cheap show me the code!

Demo

stone tech

Repositório

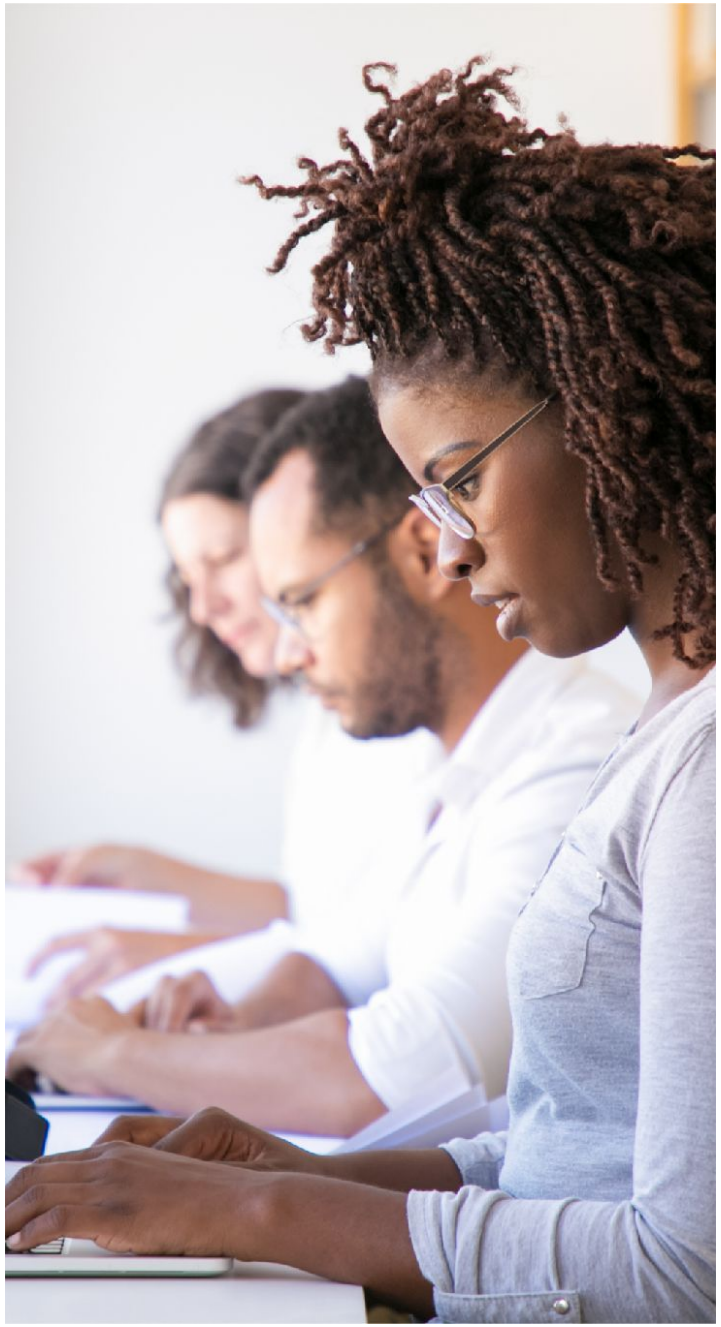
https://github.com/stone-payments/lab-hashicorp-vault-injector

Código com finalidade didática apenas, não utilizar em produção.

stone tech

stone tech/

Venha trabalhar conosco



Obrigado

stone
tech/