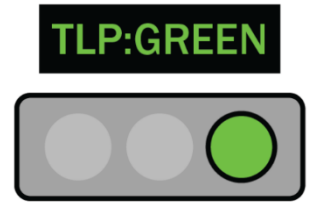


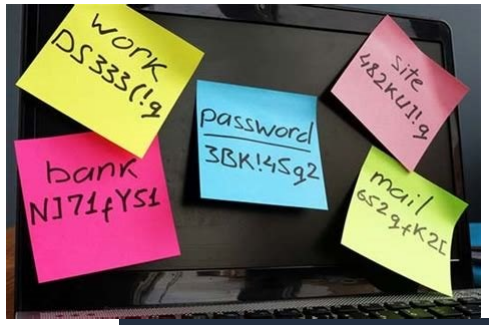
RNEP-GW

MÓDULO COFRES DE PASSWORDS

fct csirt

RNEP-GW

"SOFTWARES" MAIS COMUNS



1Password

Vaultwarden

LastPass

ANSIBLE
Ansible Vault

bitwarden

HashiCorp
Vault

KeePass

Account	Link	Username	Password	Security Question	Answer
Email (Yahoo)	www.yahoo.com/mail	johnsmith@yahoo.com	jelly22fih	What is your mother's middle name?	christianson
Email (Gmail)	www.gmail.com/mail	johnsmith@yahoo.com	1Ki77y	N/A	N/A
Google Drive	www.drive.google.com	jsmilth04312	yknjs:!776	N/A	N/A
Dropbox	www.dropbox.com	john.smith05	m3llycat	N/A	N/A
Instagram	www.instagram.com	johnsmith@yahoo.com	de2la6903	What city where you born?	chicago
Facebook	www.facebook.com	johnsmith@yahoo.com	d3itagarnm	N/A	N/A
Twiter	www.twiter.com	johnsmith@gmail.com	a11Black	N/A	N/A
Skpe	www.skpe.com	johnhsmith	3efBGy&uKlp	Where did you attend your High School?	amundsen

PASSWORD SUGERIDA

Usar um software de gestão de passwords

Letras, números e caracteres especiais

- A Palavra “armadillo” pode ser transformada em ArMad2ll0%

Não usar informação pessoal

- Cert1990

A mesma password para todas as contas

Mnemónicas

- "My first car was a red Toyota in 2005." "MfcwarTi2005."

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

Sugestão: Usar letras minúsculas e maiúsculas, números e carateres especiais, com cerca de 12 carateres

REGRAS DE OURO

Nunca partilhar a sua conta

Nunca dizer a ninguém as suas credenciais de acesso

Nunca usar a mesma password para diferentes ferramentas

Nunca anotar/escrever a sua password em papel

Nunca partilhar por telefone, email ou IM as duas credenciais

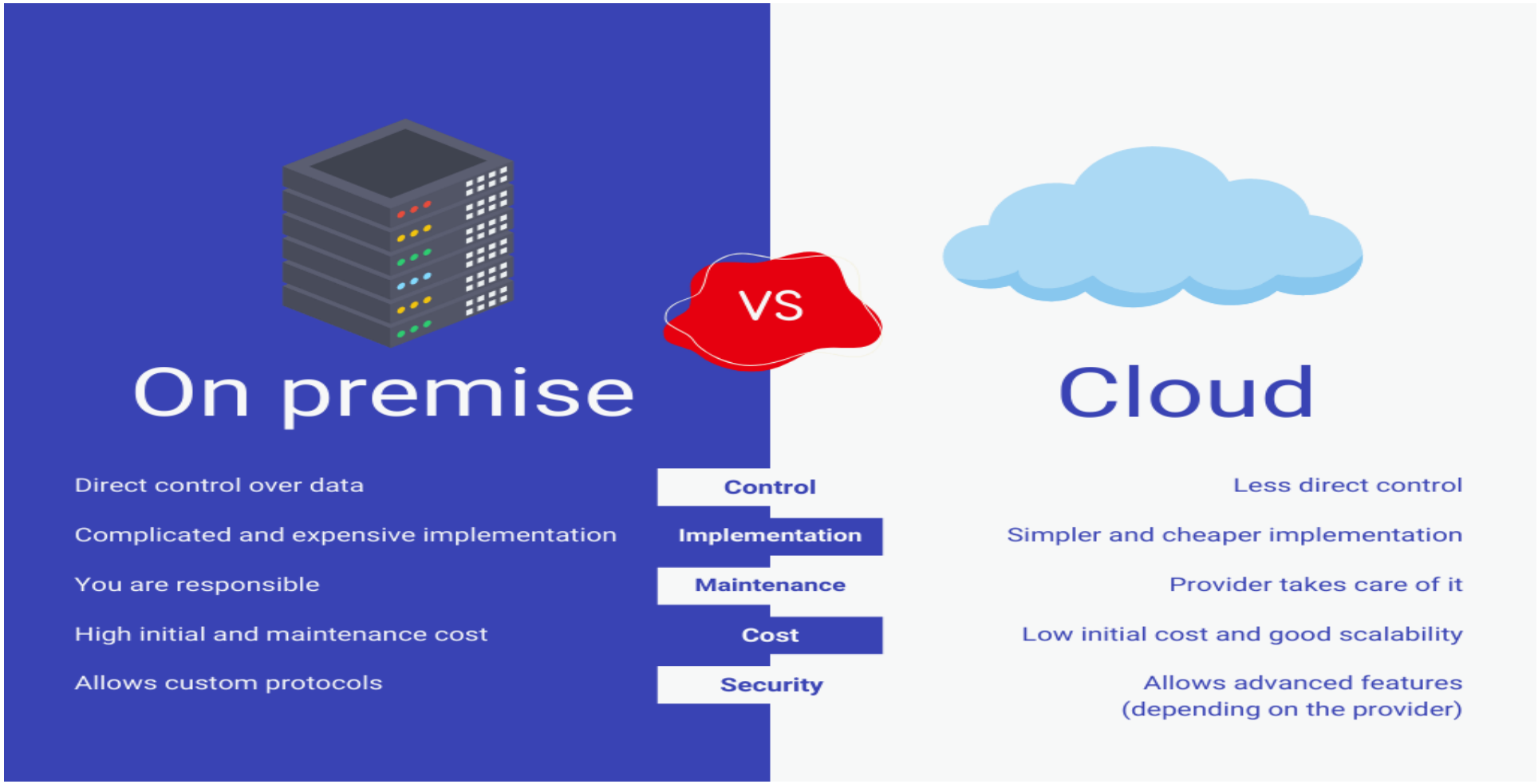
Fazer logout de sessões que não está a usar

Mudar a password com regularidade ou se suspeitar de alguma coisa

Criar password com alguma complexidade.

STORYTIME

DECISÃO INICIAL



MIGRAÇÃO

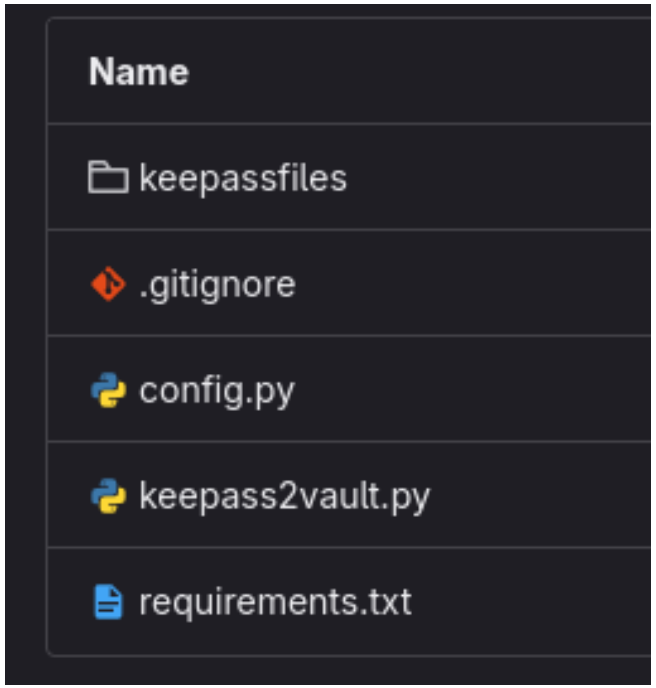
PREMISSAS

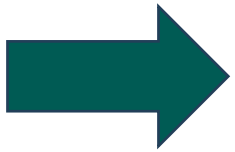
LDAP (organizational)
OpenSource / Gratuito
Certificados SSL

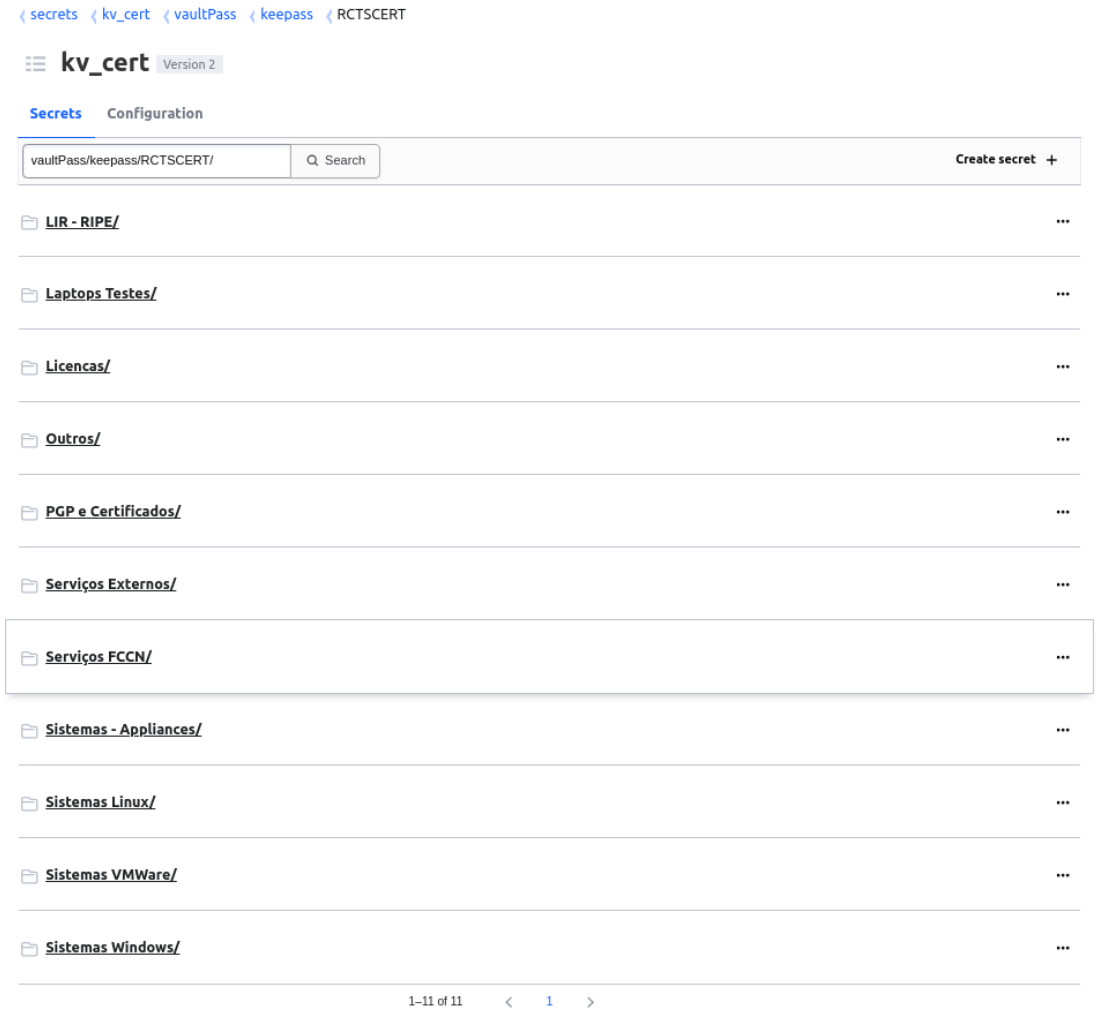
- GET
- SET

Segredos
API
Ansible
Importable
Métricas

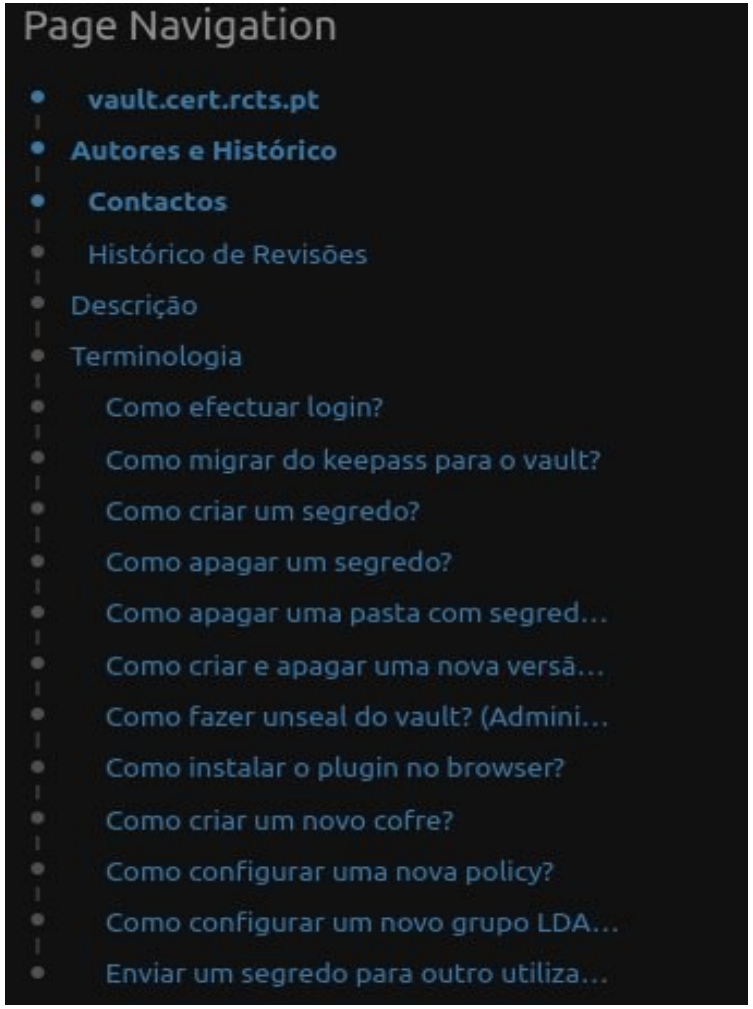
IMPORTABLE

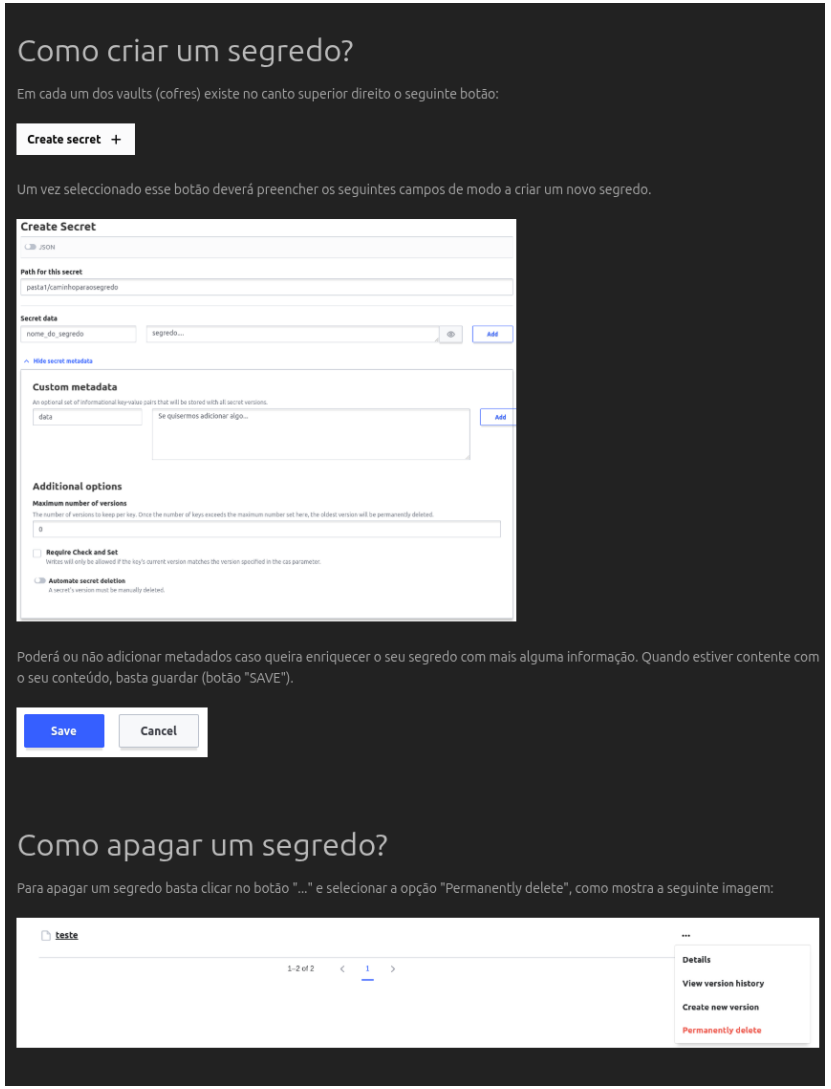

Name
keepassfiles
.gitignore
config.py
keepass2vault.py
requirements.txt



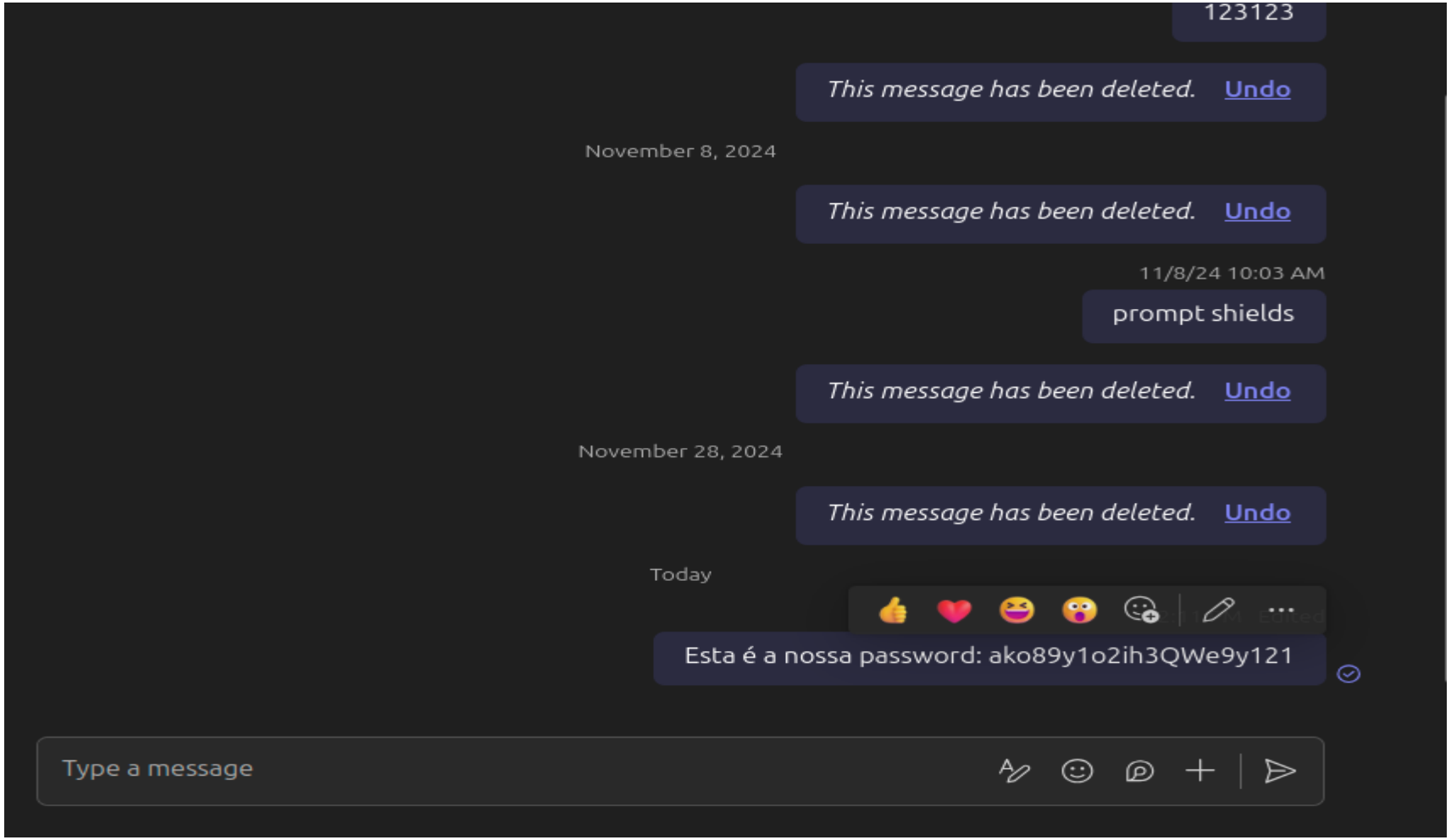

secrets
kv_cert
vaultPass
keepass
RCTSCERT
kv_cert
Version 2
Secrets
Configuration
vaultPass/keepass/RCTSCERT/
Search
Create secret
LIR - RIPE/
Laptops Testes/
Licencas/
Outros/
PGP e Certificados/
Serviços Externos/
Serviços FCCN/
Sistemas - Appliances/
Sistemas Linux/
Sistemas VMWare/
Sistemas Windows/
1–11 of 11
1

DOCUMENTAÇÃO

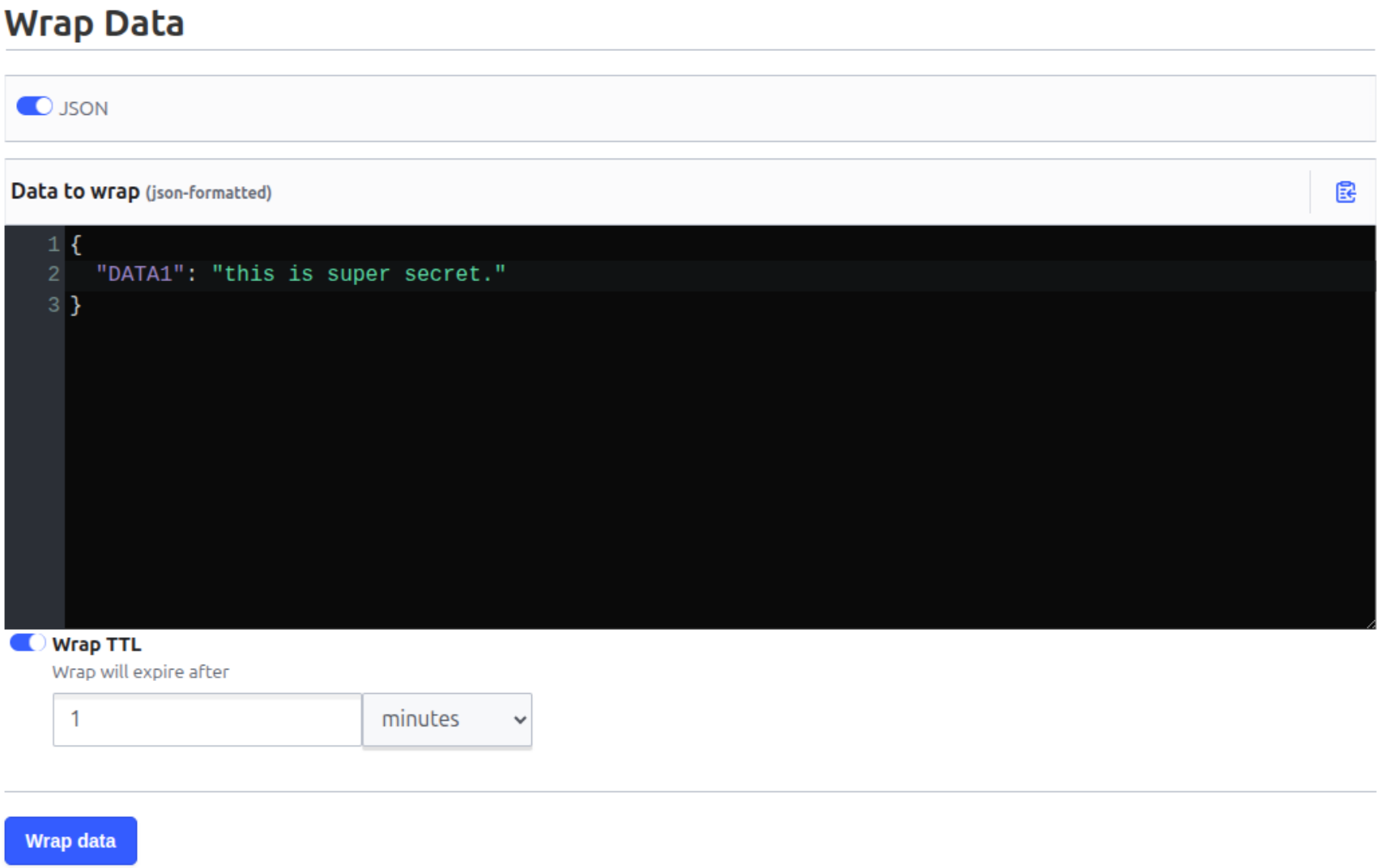




PARTILHA DE INFORMAÇÃO



PARTILHA


Wrap Data
JSON
Data to wrap (json-formatted)
1 {
2 "DATA1": "this is super secret."
3 }
Wrap TTL
Wrap will expire after
1
minutes
Wrap data

PARTILHA

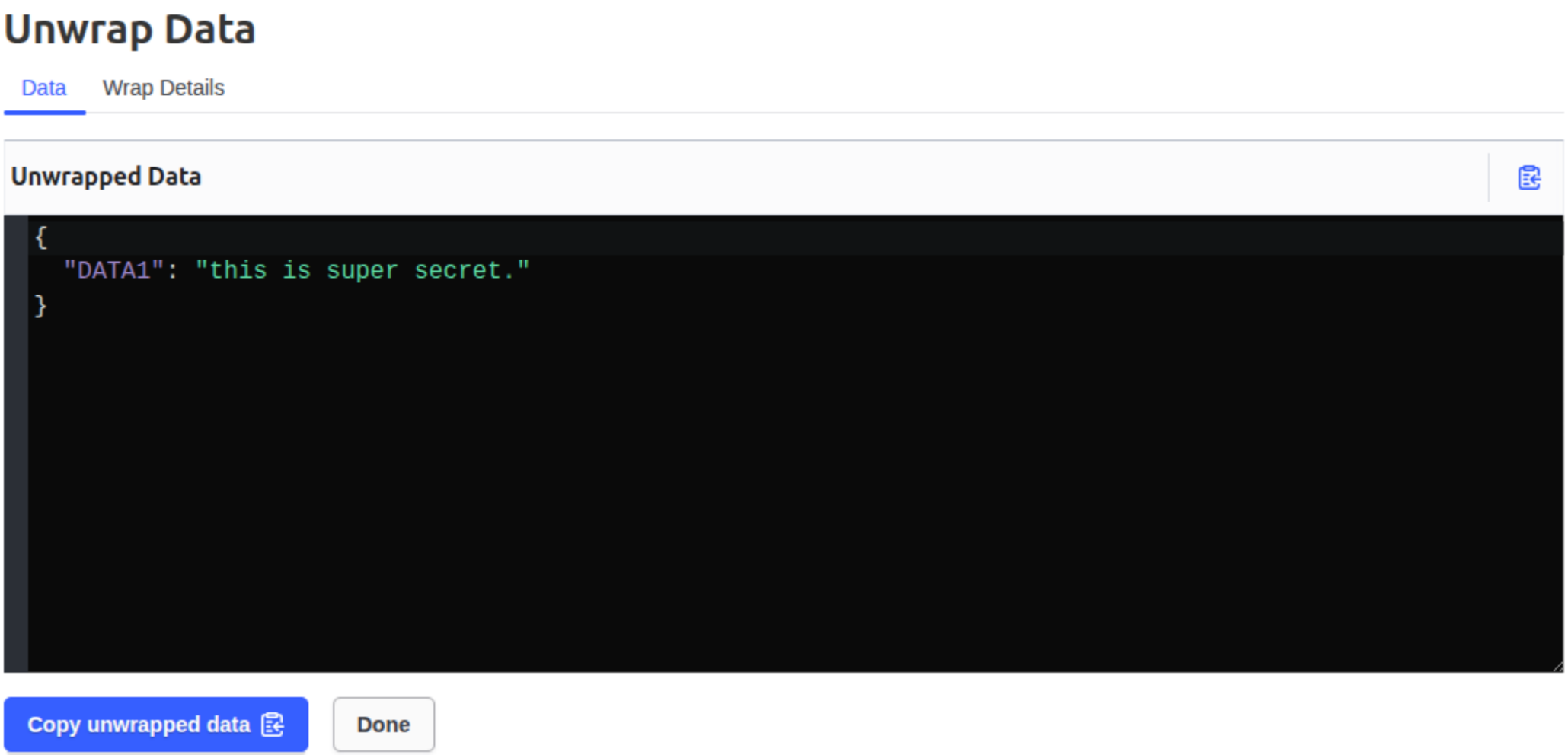
Wrap Data

Wrapped token

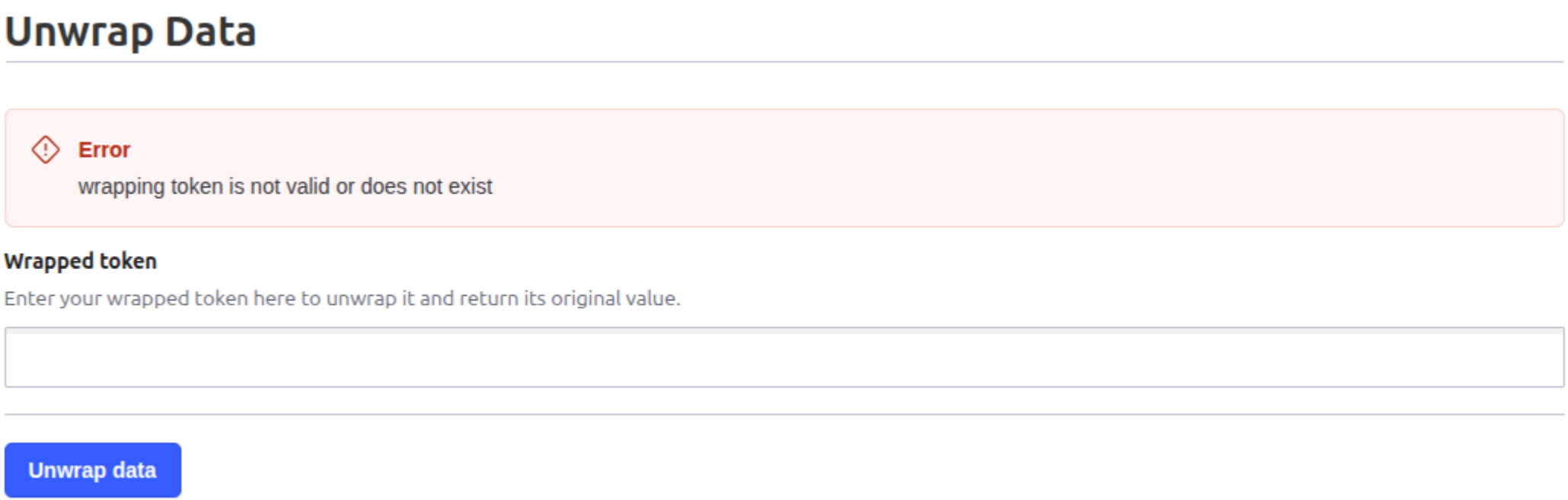
```
hvs.CAESID7san75WB9da2REA-6k3YEBZKdLebyHwA7NECDi18saGh4KHGh2cy5Xek9abXNMOG9BZHFJUndJMzVObElUZmE
```

← Back Done

PARTILHA


Unwrap Data
Data
Wrap Details
Unwrapped Data
{
"DATA1": "this is super secret."
}
Copy unwrapped data
Done

PARTILHA


Unwrap Data
Error
wrapping token is not valid or does not exist
Wrapped token
Enter your wrapped token here to unwrap it and return its original value.
Unwrap data

API

API Explorer

HashiCorp Vault API 1.20.0 OAS 3.0

/v1/sys/internal/specs/openapi

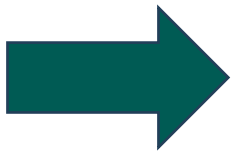
HTTP API that gives you full access to Vault. All API routes are prefixed with `/v1/`.

Mozilla Public License 2.0

Filter by tag

auth

- GET /auth/ldap/config
- POST /auth/ldap/config
- POST /auth/ldap/config/rotate-root
- GET /auth/ldap/groups/ Manage additional groups for users allowed to authenticate.
- GET /auth/ldap/groups/{name} Manage additional groups for users allowed to authenticate.
- POST /auth/ldap/groups/{name} Manage additional groups for users allowed to authenticate.
- DELETE /auth/ldap/groups/{name} Manage additional groups for users allowed to authenticate.



awesome-vault-tools

Awesome tools around HashiCorp Vault

UI

- https://github.com/djenriquez/vault-ui Vault-UI — A beautiful UI to manage your Vault, written in React.
- https://github.com/Caiyeon/goldfish - A HashiCorp Vault UI panel written with VueJS and Vault native Go API.
  - Demo: https://vault-ui.io
- https://github.com/nyxcharon/vault-ui - A webapp for working with Hashicorp's Vault.
- https://github.com/adobe/cryptr - Cryptr is a GUI for Hashicorp's Vault.

Plugins

- https://github.com/nhuff/vault-plugin-auth-chefnode - The "chef-node" auth backend allows Nodes registered with a Chef server to authenticate using their private keys.
- https://github.com/criteo/vault-auth-plugin-chef - Vault Authentication plugin for Chef.
- https://github.com/svagner/vault-auth-chef - Chef authorization plugin for Hashicorp Vault.
- https://github.com/fcantournet/kubernetes-flexvolume-vault-plugin - A kubernetes flexvolume plugin that injects vault tokens at pod creation
- https://github.com/sethvargo/vault-secrets-gen - A Vault secrets plugin for generating high entropy passwords and passphrases.
- https://github.com/sethvargo/vault-auth-slack - The Vault Auth Slack method is a Vault auth method plugin for authenticating users via Slack. The plugin can run in multiple different "modes" depending on your desired user workflow and risk tolerance. This is both a real custom Vault auth method, and an example of how to build, install, and maintain your own Vault auth plugin.
- https://github.com/gites/vault-auth-file - HashiCorp Vault authentication plugin for authenticating via Unix password like file.
- https://github.com/idcmp/vault-plugin-secrets-webhook - Use Vault ACLs to control access to other REST APIs.
- https://github.com/martinbaillie/vault-plugin-secrets-github - A Vault secrets plugin for creating ephemeral, finely-scoped GitHub access tokens.

Ops

- https://github.com/hootsuite/vault-ctrl-tool - Outsource authentication, secrets fetching, and lease management for services.
- https://github.com/starkandwayne/safe - A Vault CLI.
- https://github.com/avantoss/vault-infra - Packer and Terraform to create a fully automated and HA Vault deployment.
- https://github.com/bincyber/pkictl - CLI tool for declaratively configuring and provisioning PKI secrets in HashiCorp Vault via Yaml.
- https://gitlab.com/msvechla/vaultbot - A certbot like tool to provision certificates from a Vault managed CA.
- https://github.com/seatgeek/hashi-helper - A tool meant to enable Disaster Recovery and Configuration Management for Consul and Vault clusters, by exposing configuration via a simple to use and share hcl format.
- https://github.com/UKHomeOffice/vaultctl - Vaultctl is a command line utilty for provisioning a Hashicorp's Vault from configuration files. Essentially it was written so we could source control our users, policies, backends and secrets, synchronize the vault against them and rebuild on-demand if required.
- https://github.com/cloudwatt/vault-sync - Vault-sync is a command line utilty for provisioning a Hashicorp's Vault from configuration files. Essentially it was written so we could source control our users, policies, backends and secrets, synchronize the vault against them and rebuild on-demand if required.
- https://github.com/jaxxstorm/unseal - **[deprecated]** A command line tool to unseal multiple Hashicorp Vault servers quickly.
- https://github.com/jaxxstorm/hookpick - A tool to manage some operational concepts of Hashicorp Vault.
- https://github.com/paywithcurl/vault-update - Tool for updating a single key in vaullt secret.
- https://github.com/martinbaillie/vaultsign - Sign and verify `git` commits and tags using Vault.
- https://github.com/spectralops/teller - secrets management tool for developers, integrate Vault with any other secret and key store

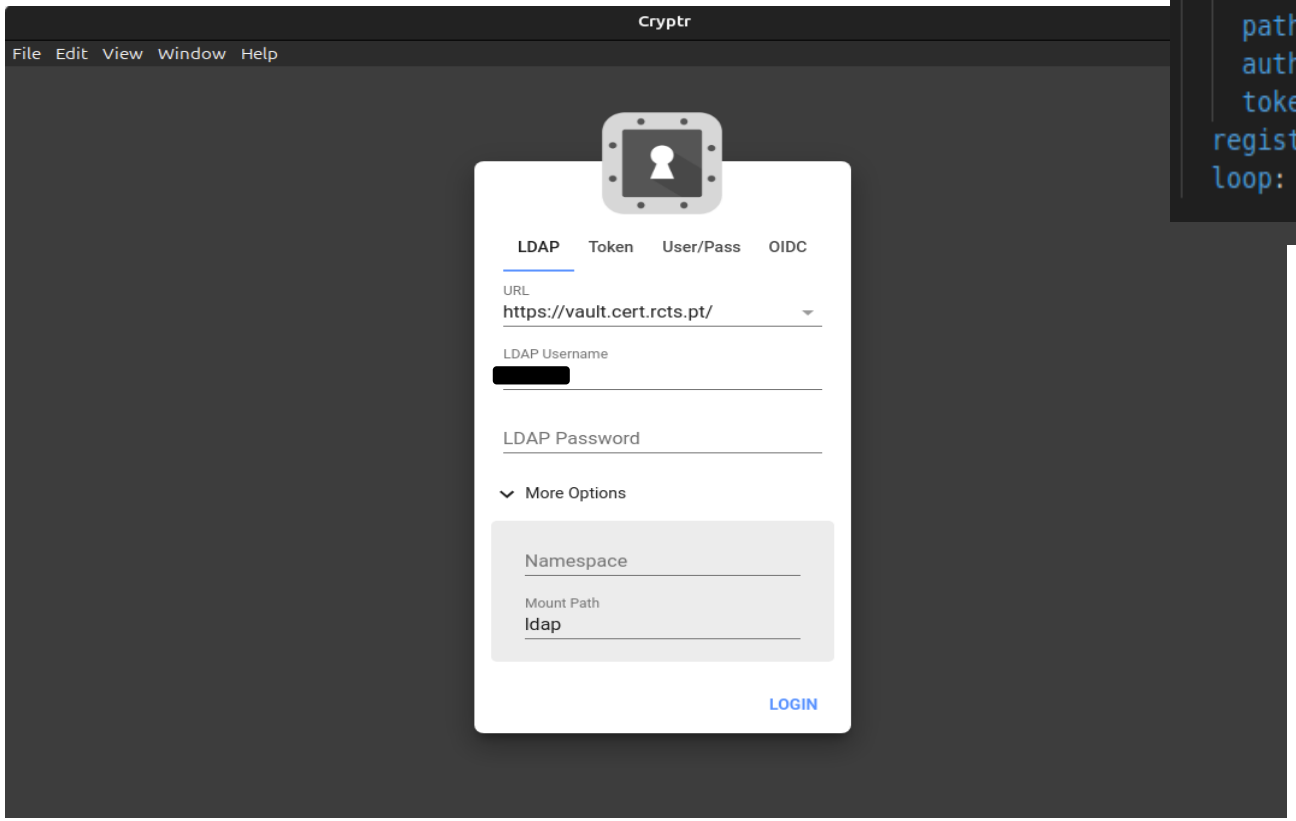
Users

- https://github.com/Lingrino/vaku - Vaku is a CLI and Go API that extends the official Vault CLI and API with useful high-level functions such as the ability to copy, move, and search vault paths and folders.
- https://github.com/Mykolaichenko/vaulter - Vaulter extends default Hashicorp Vault client, implements additional methods like list all backend path, dynamically read value, search in all backend and so on.
- https://github.com/apptio/breakglass - Breakglass is a tool that will make API calls to Hashicorp Vault servers and then retrieve credentials for you. It's designed to ease the process of getting elevated login credentials for a variety of servers. It currently supports MySQL servers and SSH Command line access.

fct csirt

PROJECTOS

```yaml
- name: Read a secrets from Vault
  no_log: true
  vars:
    vault_secret: "{{ mount_point }}/data/vaultPass/ssl_certificates/{{ item }}"
  community.hashi_vault.vault_read:
    url: '{{ vault_url }}'
    path: '{{ vault_secret }}'
    auth_method: token
    token: '{{ vault_token }}'
  register: secrets
  loop: "{{ groups['group_cert_hosts'] }}"
```

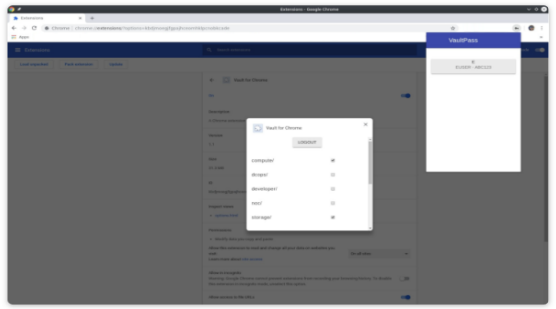


VaultPass

Add to Brave

4.2 ★ (5 ratings) Share

Extension | Workflow and planning | 729 users



Overview

A Chrome extension to leverage Hashicorp Vault as Credential Storage for teams

Think of it like Keepass for Teams where all your secrets are safely stored in Vault.

To use this exention you will need to have a running Vault instance.

IDEIAS CHAVE

- A transmissão de credenciais pode ser realizada através de software de cofres de passwords
- A utilização de cofres de password robustece os mecanismos de autenticação e a segurança em geral
- Existem diversas soluções open-source

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc