Gestion des secrets avec sops-nix & clan

Capitole du Libre 2025 - devroom Guix & Nix

Guilhem Saurel

2025-11-15

LAAS/CNRS

/ Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS

Université de Toulouse

MOTIVATION

Qu’est-ce qu’on veut ?

> Gérer des secrets: clés d’API, clés SSH, tokens, mots de passe
> Gestion d’accès par personne / machine / groupe
> Des rotations triviales
> Une interface simple
> Des configurations **déclaratives** et **reproductibles**
> Éventuellement publiques

Qu’est-ce qu’on ne veut *pas* ?

- De compromission
- De travail supplémentaire
  - au déploiement
  - aux mises à jour
  - aux rotations

SOPS-NIX

SOPS

> https://github.com/getsops/sops
> **SOPS** (Secrets OPerationS) Mozilla -> CNCF
> chiffre et déchiffre des fichiers structurés (YAML, JSON, ENV, INI)
> le fichier reste lisible, mais les valeurs sensibles sont protégées
> clefs age, pgp, aws kms, gcp, azure, vault

sops-nix: configuration

> https://github.com/Mic92/sops-nix
> Gère les secrets chiffrés dans git et dans le store
> Rend les secrets référençable par nix
> Supporte age et GPG (et SSH), un secret par fichier

sops-nix: déchiffrement

> Déchiffre automatiquement à l'activation du système
> avec les clefs SSH de l'hôte
> dans `/run/secrets/my-api-key`
> avec des accès réglables
> qu'on peut mettre dans des `ENV_VARS` via systemd

sops-nix: example

```
$ sudo ls -l /run/secrets/my-ssh-key
-r-------- 1 root root 399 nov.  10 17:05 my-ssh-key
$ sudo head -n1 /run/secrets/my-ssh-key
-----BEGIN OPENSSH PRIVATE KEY-----
```

CLAN

Clan

> https://clan.lol/
> Gestion multi-hôtes
> Configs Backups / VPN / Wifi
> CLI
> Intégrations nixos-anywhere / disko / sops-nix

Gestion des secrets dans Clan

- Définition centralisée des secrets par machine ou groupe
- Chaque utilisateur possède sa clé `age`
- Gestion automatique des clés `age` pour chaque hôte
- Intégration directe avec `sops-nix`
- Gérérateurs pour différents services Clan

DEMO

Chiffrement de disque

Yakafokon !

==> Session Bidouille