SSH-Agent && Keychain

GESTION DES IDENTITÉS & AUTOMATISATION SSH

Dans une infrastructure sécurisée, les clés SSH sont protégées par des **Passphrases** complexes (ex: 45+ caractères). Cependant, l'administration quotidienne (Git, Ansible, Rsync, SSH multi-bonds) rend la saisie répétitive de ces mots de passe contre-productive, voire insupportable ("Fatigue de sécurité").

L'objectif est de mettre en place un système de **Single Sign-On (SSO) local** pour le terminal : l'administrateur déverrouille ses clés une seule fois au démarrage de la session, et le système les garde en mémoire vive pour toutes les fenêtres et processus ultérieurs.

Le Duo Technique

Pour réaliser cela sous Debian, nous utilisons deux composants qui travaillent en tandem :

SSH-Agent (Le Moteur)

C'est un démon natif d'OpenSSH. Il stocke les clés déchiffrées en mémoire (RAM) et répond aux défis cryptographiques sans jamais écrire la clé privée sur le disque ni la montrer à l'utilisateur.

Problème : Il est volatil. Si on ferme le terminal, l'agent meurt. Si on en ouvre un deuxième, un nouvel agent (vide) démarre.

Keychain (Le Gestionnaire)

C'est une surcouche (wrapper). Au lancement d'un terminal, il vérifie si un ssh-agent tourne déjà pour l'utilisateur.

- *Si OUI :* Il connecte le nouveau terminal à l'agent existant (héritage des clés).
- *Si NON :* Il lance l'agent et demande les passphrases.

Installer le trousseau (Keychain)

L'outil keychain est disponible dans les dépôts officiels Debian. Il est léger et ne tourne qu'à l'initialisation du shell.

C'est un petit paquet magique qui gère ssh-agent pour toi. Il est bien plus malin que l'agent par défaut car il peut partager les clés entre plusieurs terminaux.

Mise à jour et installation

```
admin@laptop:~$ sudo apt update && sudo apt install keychain
```

Configuration (Persistance Shell)

La configuration se fait au niveau du fichier de profil de l'utilisateur (.bashrc pour Bash ou .zshrc pour Zsh). Nous allons instruire le shell de charger keychain à chaque ouverture de session.

```
admin@laptop:~$ nano ~/.bashrc
```

Ajouter le bloc suivant à la fin du fichier.

Il est impératif de déclarer explicitement les noms des clés privées à charger.

Syntaxe : keychain --eval --agents ssh [liste_des_clés_privées]

```
# --- SSH AGENT (KEYCHAIN) ---
if [ -x /usr/bin/keychain ]; then
    eval $(keychain --eval --agents ssh id_ed25519-lab-unsafe.lan)
fi
```

--eval	Génère les lignes de commande nécessaires pour exporter les variables d'environnement (SSH_AUTH_SOCK, etc.) que le shell actuel doit exécuter.
--agents ssh	Spécifie qu'on travaille avec le protocole SSH (Keychain gère aussi GPG).
id_rsa ...	La liste des fichiers présents dans ~/.ssh/ qu'on souhaite charger.

L'Activation

```
admin@laptop:~$ source ~/.bashrc

 * keychain 2.8.5 ~ http://www.funtoo.org
 * Inheriting ssh-agent (1974)
 * Adding 1 ssh key(s): /home/admin/.ssh/id_ed25519-lab-unsafe.lan
Enter passphrase for /home/admin/.ssh/id_ed25519-lab-unsafe.lan:     <-- Une Derniere Fois !
 * ssh-add: Identities added: /home/admin/.ssh/id_ed25519-lab-unsafe.lan
```

Validation & Utilisation

Pour appliquer les changements sans redémarrer (on est sous Debian, ont ne reboot jamais !)

```
admin@laptop:~$ source ~/.bashrc

 * keychain 2.8.5 ~ http://www.funtoo.org
 * Inheriting ssh-agent (1974)
 * Adding 1 ssh key(s): /home/admin/.ssh/id_ed25519-lab-unsafe.lan
Enter passphrase for /home/admin/.ssh/id_ed25519-lab-unsafe.lan:     <-- Une Derniere Fois !
 * ssh-add: Identities added: /home/admin/.ssh/id_ed25519-lab-unsafe.lan
```

Comportement attendu

- **Premier Terminal (Boot) :** Le système affiche :

  Found existing ssh-agent: 12345 Adding 2 keys: /home/admin/.ssh/id_rsa, ... Enter passphrase for /home/admin/.ssh/id_rsa: Une fois le mot de passe saisi, le prompt apparaît.

- **Deuxième Terminal (Multitâche) :** Le système affiche :

  Found existing ssh-agent: 12345 Known ssh key: /home/seed/.ssh/id_rsa **Aucun mot de passe n'est demandé.** L'accès aux serveurs distants est instantané.

- **Vérification de l'Agent :** Pour voir quelles clés sont actuellement actives en mémoire :

```
admin@laptop:~$ ssh-add -l
256 SHA256:zOxxSNAMBSsw5d8ZwPOuyiH+yWEiwU/kXuC1zc6FodY backup_server (ED25519)
```

Avertissement de Sécurité (Security Warning)

ATTENTION : RISQUE D'USURPATION PHYSIQUE

L'utilisation de Keychain crée une **persistance de l'identité**. Tant que la session de l'utilisateur admin est ouverte (ou que le serveur n'a pas redémarré), les clés sont utilisables sans mot de passe.

- **Vecteur d'attaque :** Si un attaquant obtient un accès physique au clavier de laptop (ou un shell distant sur la session admin), il peut se connecter à toute l'infrastructure (rsync, Git, etc.) sans connaître la passphrase.

- **Contre-mesure :**

  1. Verrouillage systématique de la session de travail (Lock Screen) en cas d'absence.
  2. Ne JAMAIS installer Keychain sur un serveur exposé (VPS/DMZ). Cet outil est réservé aux **Zones de Confiance (LAN Management)**.