Ubuntu server - authentification SSH par clés

Difficulté : Intermédiaire

Notions : SSH, chiffrement, PKI, clé

I. Introduction

Cette procédure vise à expliquer la mise en place de l'authentification par clé en complément, ou remplacement, de l'authentification par mot de passe.

Celle-ci renforce la sécurité pour l'administration du parc car elle ne nécessite plus d'échange de mot de passe pour l'authentification.

II. Création du couple de clé

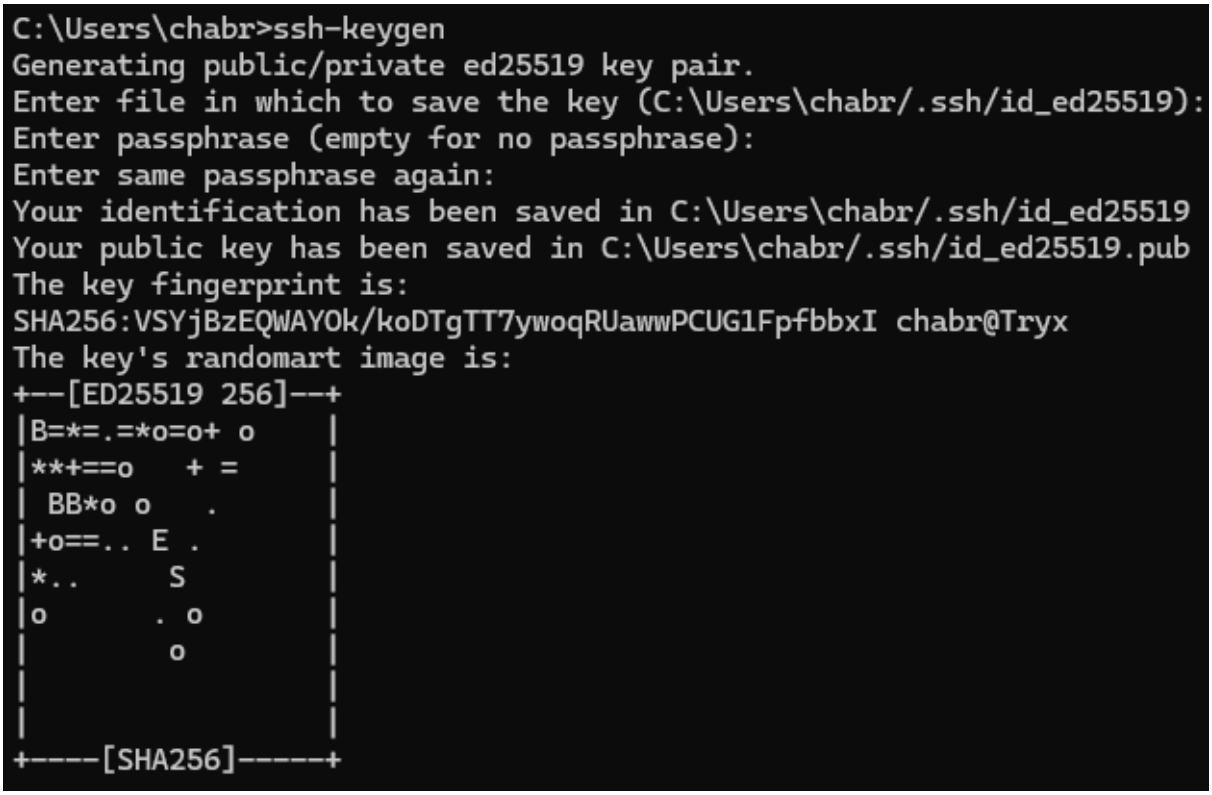
Côté poste d'administration, se connecter avec l'utilisateur qui devra prendre la main sur les machines distante.

Utiliser la commande suivante pour générer un lot de clé :

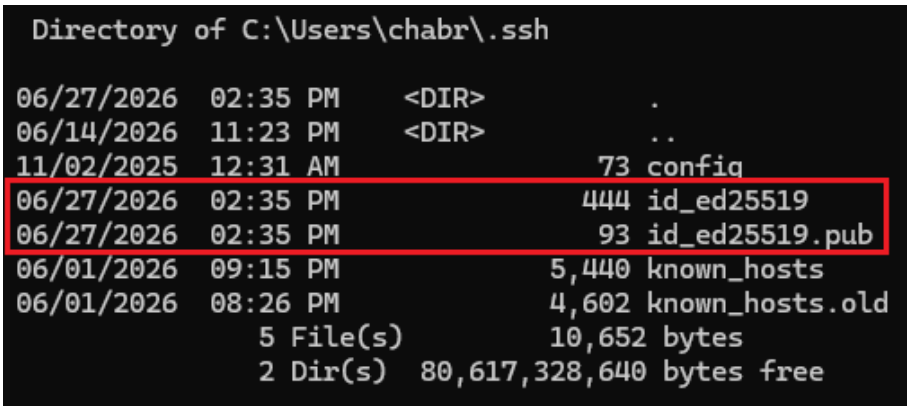
```
ssh-keygen
```

Après le lancement, une série de question seront posées :

- Emplacement des fichiers de clé privée et clé publique.
- Passphrase de la clé.
- (si saisi) Répétition de la passphrase.



Les clés sont alors générées.



II. Installation sur le serveur

Il va ensuite falloir copier la ***clé publique*** (celle finissant pas .pub) sur les machines où il sera nécessaire de se connecter.

2.1 Vérifications préalables

Sur les machines de destinations, il faut s'assurer que le dossier '***.ssh***' existe dans le répertoire '***home***' de l'utilisateur.

Si ce n'est pas le cas, le créer.

> **Info** : Il est important que les droits soient bien définis sur le répertoire .ssh et la clé copiée. Sinon la connexion SSH échouera car le serveur jugera que la clé est mal protégée et a pu être altérée.

```
cd ~
mkdir .ssh && chmod 700 .ssh
```

```
sc4d-@template:~$ mkdir .ssh && chmod 700 .ssh
sc4d-@template:~$ ll
total 32
drwxr-x--- 4 sc4d- sc4d- 4096 Jun 27 12:46 ./
drwxr-xr-x 3 root  root  4096 Mar 20  2025 ../
-rw------- 1 sc4d- sc4d-   16 Mar 20  2025 .bash_history
-rw-r--r-- 1 sc4d- sc4d-  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 sc4d- sc4d- 3771 Mar 31  2024 .bashrc
drwx------ 2 sc4d- sc4d- 4096 Mar 20  2025 .cache/
-rw-r--r-- 1 sc4d- sc4d-  807 Mar 31  2024 .profile
drwx------ 2 sc4d- sc4d- 4096 Jun 27 12:46 .ssh/
-rw-r--r-- 1 sc4d- sc4d-    0 Mar 20  2025 .sudo_as_admin_successful
sc4d-@template:~$
```

Puis créer le fichier '***authorized_keys***' qui contiendra les clé autorisées pour cet utilisateur.

```
touch .ssh/authorized_keys && chmod 600 .ssh/authorized_keys
```

```
sc4d-@template:~$ touch .ssh/authorized_keys && chmod 600 .ssh/authorized_keys
sc4d-@template:~$ ll .ssh/
total 8
drwx------ 2 sc4d- sc4d- 4096 Jun 27 12:49 ./
drwxr-x--- 4 sc4d- sc4d- 4096 Jun 27 12:46 ../
-rw------- 1 sc4d- sc4d-    0 Jun 27 12:49 authorized_keys
```

Il sera également nécessaire de dé-commenter la ligne du fichier '***/etc/ssh/sshd_config***' afin d'autoriser le login par clé :

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes
```

Puis relancer le service avec :

```
service ssh restart
```

2.2 Copier la clé

La méthode varie selon le client.

Depuis un linux

Utiliser la commande suivante pour pousser la clé sur le client :

```
ssh-copy-id <utilisateur>@<ip ou hostname>
```

Si c'est la première connexion, il est demandé si le serveur de destination doit être ajouté aux serveurs connus de confiance.

Répondre '***yes***'.

```
sc4d@template:~$ ssh-copy-id sc4d-@192.168.1.64
The authenticity of host '192.168.1.64 (192.168.1.64)' can't be established.
ED25519 key fingerprint is SHA256:yKSqLCok62ywvhM7Mmrr8cx7v3Q1Yd1zcEpXH4fAM1U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Puis, lorsque demandé, saisir le mot de passe du compte pour se connecter au serveur.

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
sc4d-@192.168.1.64's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'sc4d-@192.168.1.64'"
and check to make sure that only the key(s) you wanted were added.
```

La clé à été normalement ajouté au store du serveur et est visible dans le fichier '***~/.ssh/authorized_keys***'.

```
sc4d-@template:~$ cat .ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKd8Ra7oM9z6ZQ+UHRZrM6AnY71BSowIxJRD7uPuQEo9 sc4d@templat
```

Depuis un windows

Sur windows, la commande '***ssh-copy-id***' n'existe pas. Il faudra donc copier cette clé manuellement sur le serveur.

Pour cela, ouvrir un cmd, puis afficher le contenu du fichier de la clé publique.

```
C:\Users\chabr\.ssh>type id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICnv5OxqDFLD+VV6ZZVfjme71vt44AYVeOg6wZLEV6wz chabr@Tryx
```

Copier le contenu de cette clé dans le presse papier. Puis utiliser la commande suivante pour exécuter une commande distante sur le serveur linux :

```
ssh -t <user>@<ip ou hostname> "(echo '<laclésshh>' >> ~/.ssh/authorized_keys)"
```

```
C:\Users\chabr\.ssh>ssh -t sc4d-@192.168.1.64 "(echo ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICnv5OxqDFLD+VV6ZZVfjme71vt44AY
VeOg6wZLEV6wz chabr@Tryx >> ~/.ssh/authorized_keys)"
sc4d-@192.168.1.64's password:
Connection to 192.168.1.64 closed.
```

Dans les deux cas, il est possible de vérifier l'ajout des clés avec :

```
cat ~/.ssh/authorized_keys
```

```
root@template:/home/sc4d-/.ssh# cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKd8Ra7oM9z6ZQ+UHRZrM6AnY71BSowIxJRD7uPuQEo9 sc4d@template
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICnv5OxqDFLD+VV6ZZVfjme71vt44AYVeOg6wZLEV6wz chabr@Tryx
```

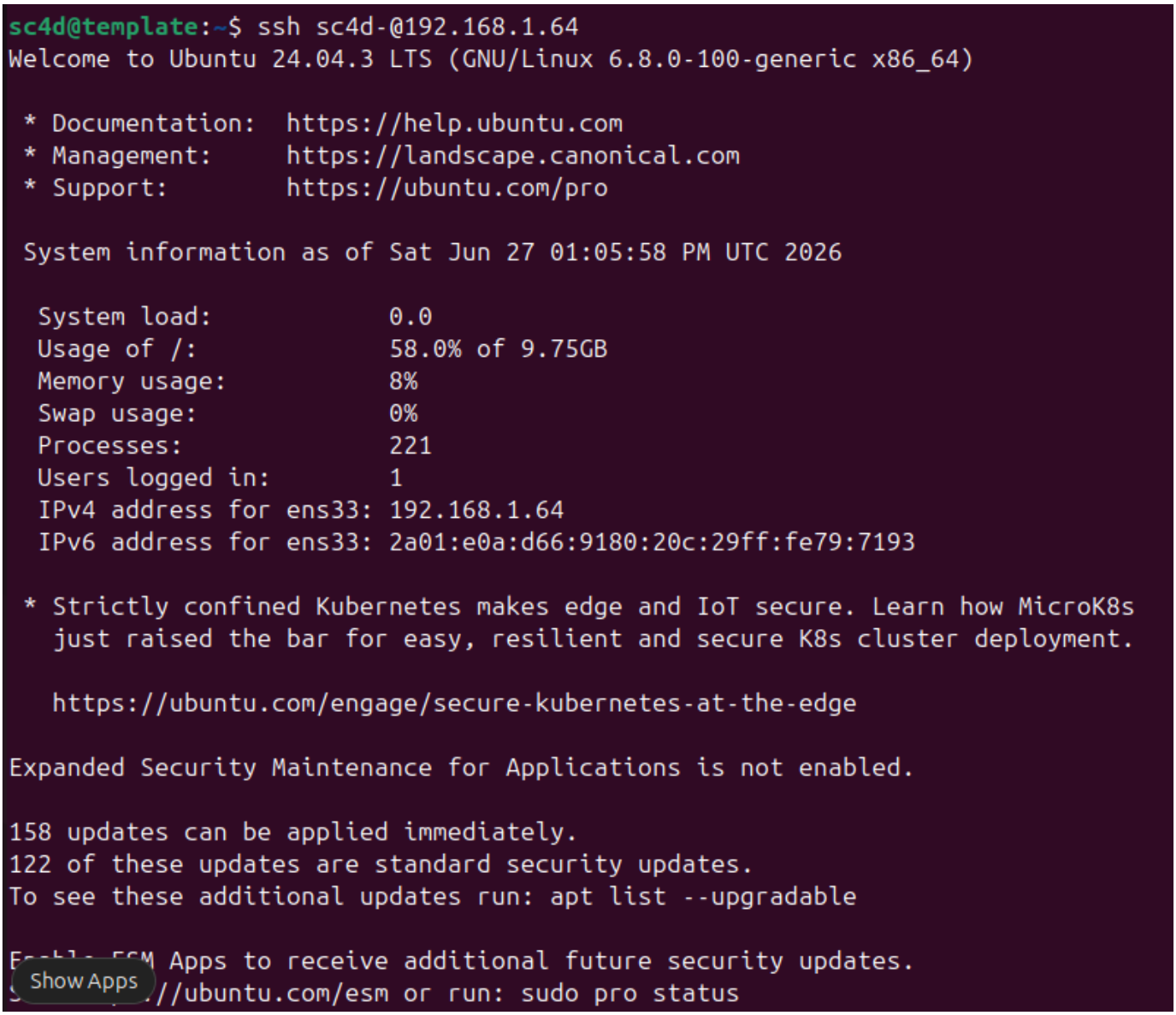
III. Connexion et sécurisation

3.1 Connexion

Se connecter au serveur avec la commande habituelle.

```
ssh <user>@<ip ou hostname>
```

Aucun mot de passe n'a été demandé (sauf si une passphrase a été créée pour la clé, auquel cas c'est elle qui sera demandée).



3.2 Sécurisation

Pour aller plus loin, il est possible de désactiver purement et simplement la connexion par login/mot de passe.

Pour cela, modifier le fichier '***/etc/ssh/sshd_config***'. Et dé-commenter puis changer l'option correspondante comme suit :

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Puis relancer le service avec :

```
service ssh restart
```

Ainsi, seul le login par clé sera autorisé sur le serveur.

Revision #2
Created 2026-07-29 12:10:21 UTC by Olivier
Updated 2026-07-29 13:03:05 UTC by Olivier