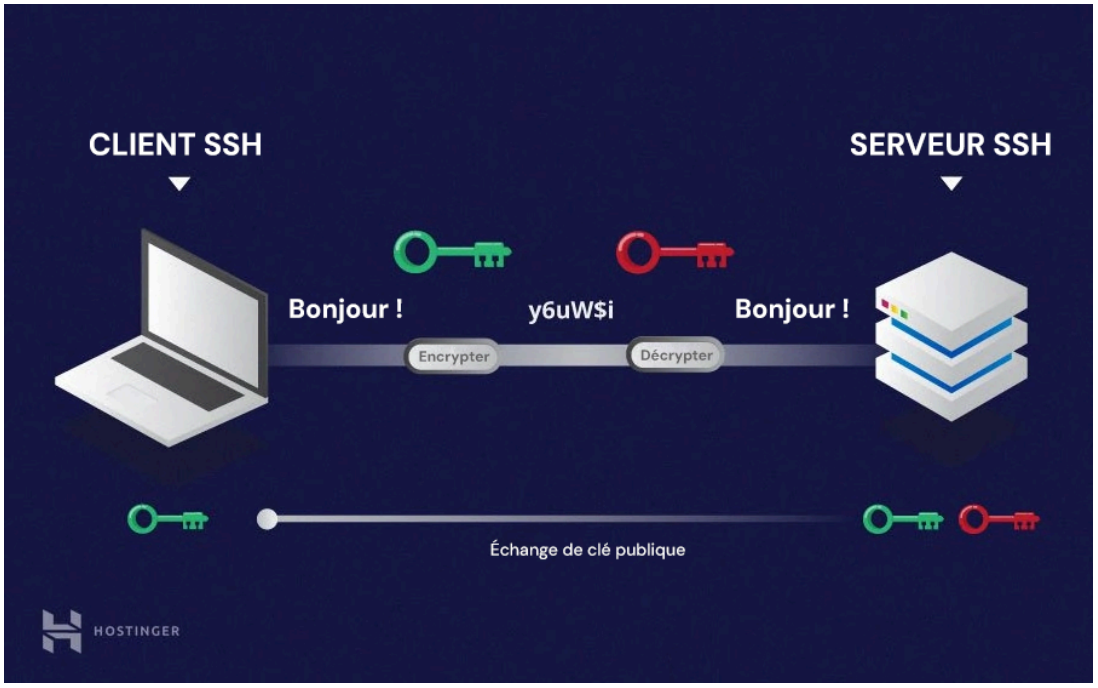
SSH avec échange de clés



SOMMAIRE

Introduction : *3*
Définition de SSH (Secure Shell) 3
Échange de clés SSH (authentification par clé publique) 3
Schéma : **3**
Objectifs : **4**
Création des machines virtuelles : **4**
Echange de clé debian vers debian : **4**
Echange de clé windows vers debian : **5**

Introduction :

Définition de SSH (Secure Shell)

SSH (Secure Shell) est un protocole réseau sécurisé qui permet de se connecter à distance à un ordinateur ou un serveur.
Il chiffre toutes les données échangées entre le client et le serveur, garantissant confidentialité, intégrité et authentification.

Échange de clés SSH (authentification par clé publique)

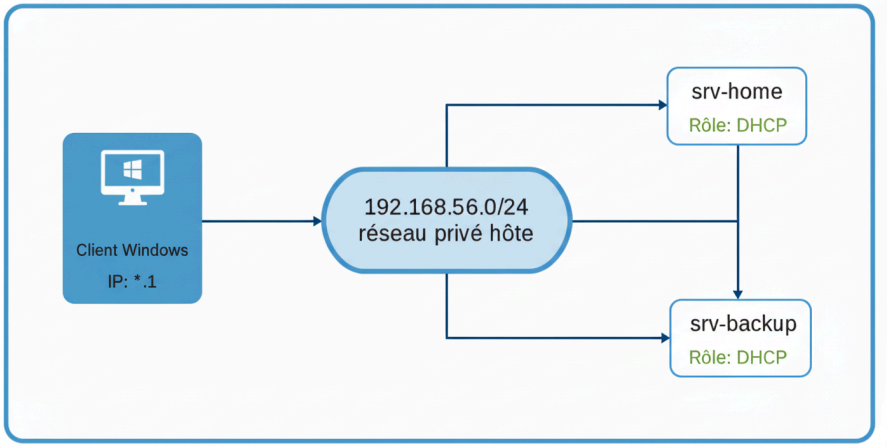
L'authentification par clé SSH repose sur un couple de clés cryptographiques :

- ***Une clé privée (conservée secrètement sur le poste du client).***
- ***Une clé publique (copiée sur le serveur distant).***

Lors de la connexion :

1. ***Le serveur envoie un défi chiffré avec la clé publique.***
2. ***Le client le déchiffre avec sa clé privée.***
3. ***Si le déchiffrement est correct, la connexion est autorisée.***

Schéma :



Objectifs :

- ***Se connecter à distance : permettre l'accès depuis `srv-backup` vers `srv-home`.***
- ***Générer une paire de clés SSH sur `srv-backup` (clé privée/clé publique) et vérifier l'empreinte (fingerprint) de la clé publique.***
- ***Pas de passphrase : la clé privée sera créée sans phrase de passe pour automatiser la connexion.***
- ***Connexion avec l'utilisateur `sio` : pouvoir se connecter en tant que `sio` sur `srv-home`.***

Création des machines virtuelles :

Deux machines ont été créées pour la mise en place de l'environnement SSH :

- ***srv-home →* `192.168.56.101`**
- ***srv-backup →* `192.168.56.102`**

Echange de clé debian vers debian :

Le service SSH a été installé et activé sur la machine `srv-home` afin de permettre les connexions distantes sécurisées.

```
root@backup:~# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssh-server est déjà la version la plus récente (1:8.4p1-5+deb11u3).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 8 non mis à jour.
```

Dans l'exemple suivant, nous montrerons comment générer une clé SSH sur srv-backup.

```
sio@backup:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sio/.ssh/id_rsa):
Created directory '/home/sio/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sio/.ssh/id_rsa
Your public key has been saved in /home/sio/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:dgZSbUx3S9BV6ZtthEj3IjN6lrxgZm/n12gVLDQmRsE sio@backup
The key's randomart image is:
+---[RSA 3072]----+
|        .++o+oo.=|
|       .  +E.*oo |
|      . ....+o=o |
|       . .  =.o+o|
|        S oo =.o=|
|       . o* =  o+|
|         + = . +.|
|            + + o|
|           . +.. |
+----[SHA256]-----+
```

Après avoir généré la clé SSH sur srv-backup, nous affichons l'empreinte de la clé publique.

```
sio@backup:~$ ssh-keygen -lf .ssh/id_rsa
3072 SHA256:dgZSbUx3S9BV6ZtthEj3IjN6lrxgZm/n12gVLDQmRsE sio@backup (RSA)
```

Ici l'empreinte de la clé publique est 3072.

Ici, je vais copier la clé publique générée sur la machine srv-backup vers le serveur srv-home.

```
sio@backup:~$ ssh-copy-id sio@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/sio/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:/9ajSJak5UcNTKXMOIsphnFQZcyPDbkdubZlcqOL36M.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alrea
dy installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to instal
l the new keys
sio@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'sio@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.
```

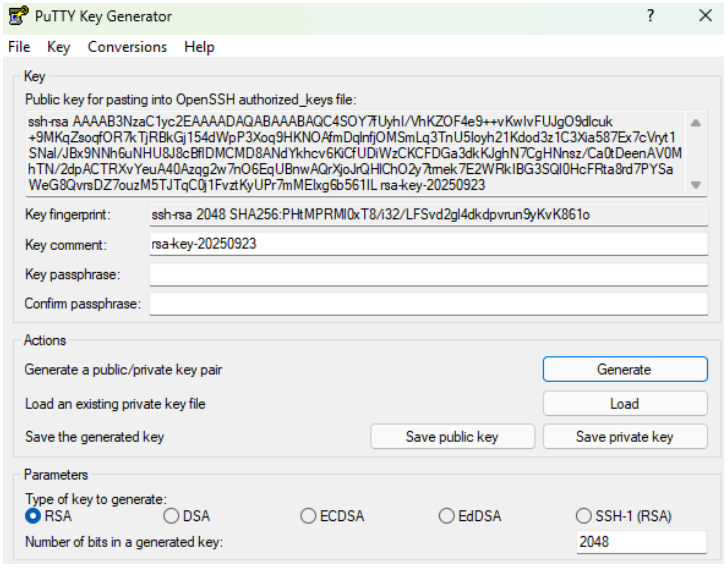
```
sio@backup:~$ ssh sio@192.168.56.101
Linux home 5.10.0-32-amd64 #1 SMP Debian 5.10.223-1 (2024-08-10) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 23 11:00:09 2025 from 192.168.56.1
sio@home:~$
```

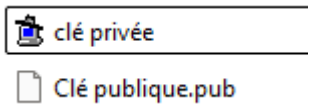
Echange de clé windows vers debian :

Ici, je vais utiliser PuTTYgen sur mon poste Windows afin de générer une paire de clés SSH.



Ici, nous allons sauvegarder les deux clés générées avec PuTTYgen.

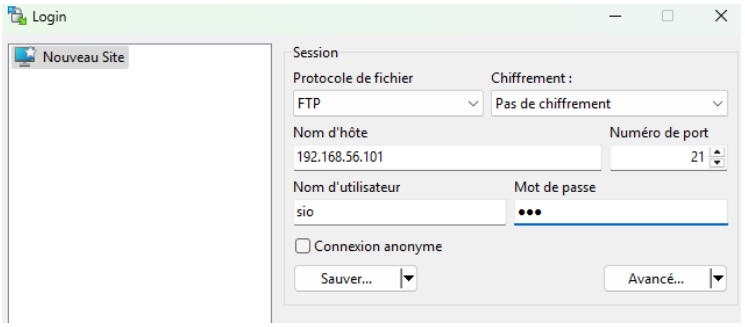
voici les clés générées.



Ici, nous allons générer une paire de clés SSH directement sur le serveur `srv-home`.

```
sio@home:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sio/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sio/.ssh/id_rsa
Your public key has been saved in /home/sio/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:2jfo9IIZQLv4NA7tHc+gaYU3zviE2uGU12IGKUqCN5U sio@home
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|     ..          |
|    .E.          |
|.  .o.           |
|o.+oo+  S        |
|oooo*+B+ .       |
|.  *=@BX= o      |
|   =O***+o .     |
|  ..o.. ...      |
+----[SHA256]-----+
```

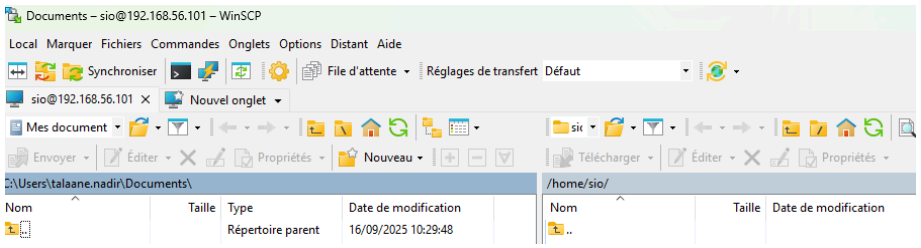
Ici, nous allons nous connecter depuis notre poste Windows au serveur srv-home en utilisant WinSCP.



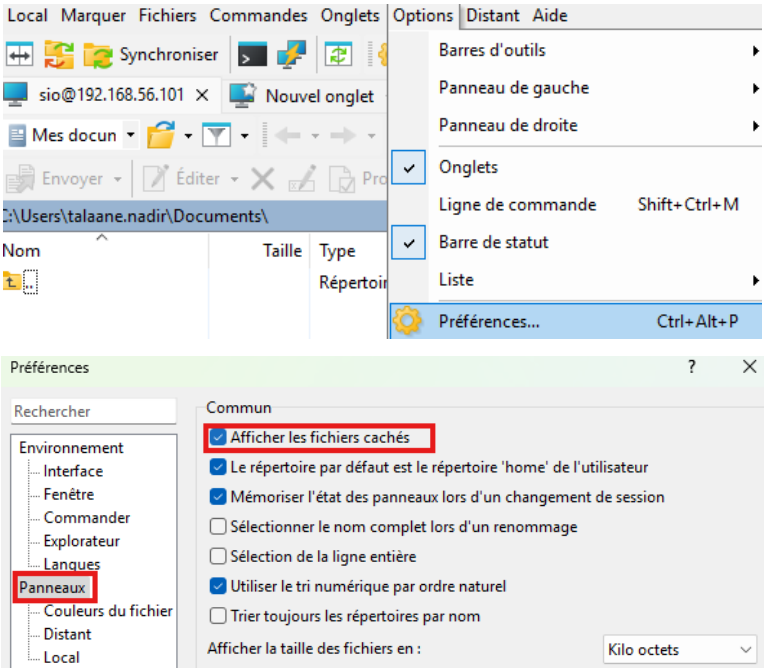
Si la connexion ne fonctionne pas, nous allons exécuter cette commande sur srv-home.

```
root@home:~# apt install vsftpd
```

nous retournons sur WinSCP pour retenter la connexion au serveur srv-home.



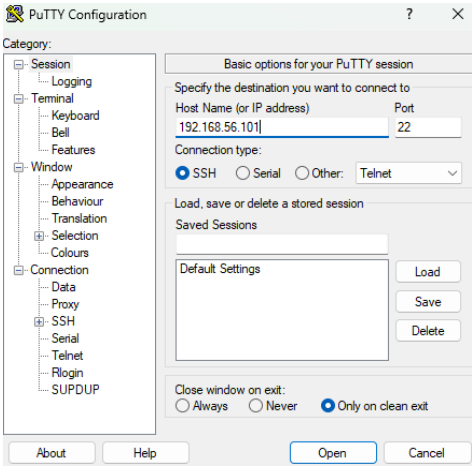
Nous allons aller sur options → préférences → panneaux et cocher la case afficher les fichiers cachés



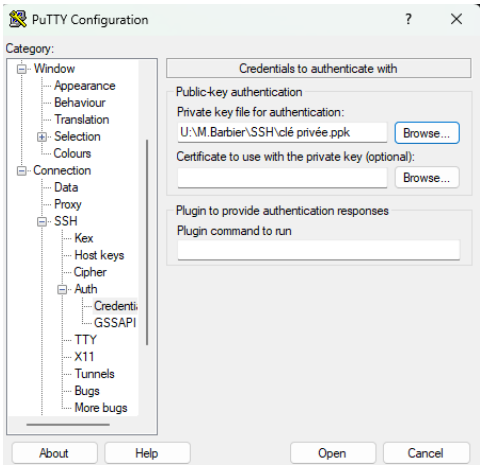
Ici, nous allons copier la clé publique de notre machine hôte vers le serveur srv-home, dans le répertoire /home/sio/.ssh/.

J'ai utilisé Powershell car le transfert du fichier ne marchait pas de mon côté.

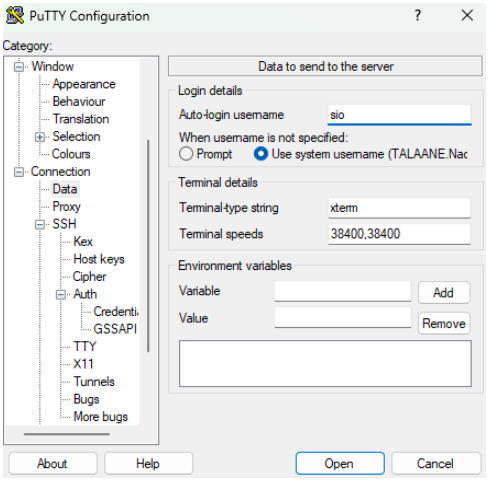
Ensuite, nous allons nous connecter au serveur srv-home en utilisant PuTTY.



Ici, nous allons accéder à la section SSH → Auth → Credentials dans PuTTY pour sélectionner notre clé privée.



Maintenant nous allons dans Data afin de mettre l'authentification directe en sio.



Nous sommes maintenant connectés à srv-home en SSH sans avoir à saisir de mot de passe, grâce à l'authentification par clé SSH.