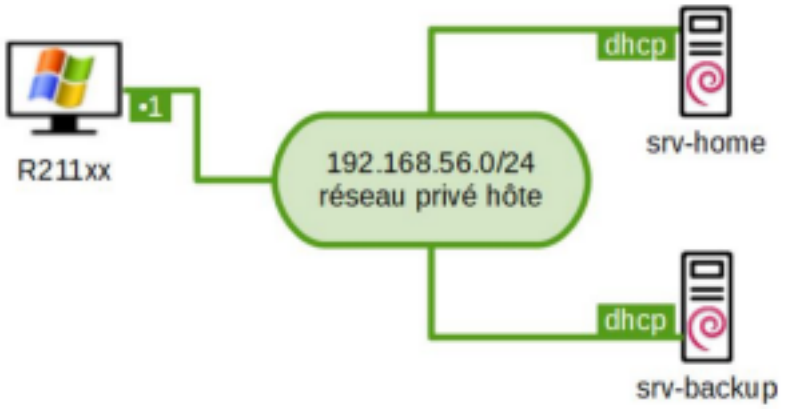
Séance SSH

Schéma :



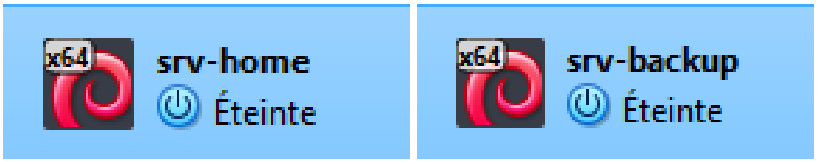
L'échange de clés en SSH permet de *sécuriser la connexion entre un client et un serveur*. *Le client utilise une clé publique pour s'authentifier auprès du serveur*, qui a la *clé privée correspondante*. Cela permet de chiffrer les données échangées et de protéger la communication contre les interceptions.

Objectifs :

- Accéder à srv-home depuis srv-backup
- Générer la paire de clés privées/publiques et vérifier l'empreinte (fingerprint) sur srv-backup - Pas de passphrase
- Pouvoir Se connecter en sio
- Bien renommer les serveurs pour plus de lisibilité

Configuration des VM

Nous créons 2 VM, sur Debian, une nommé ‘**srv-home**’ en **192.168.56.101** et l’autre nommé ’**srv-backup’** en **192.168.56.102**



Premièrement, on installe SSH sur la machine “srv-home”, on utilise la commande “ **apt install open-ssh server**” Ensuite il faut changer le nom de 2 VM, grâce à la commande nano /etc/hostname

Et ensuite la commande nano /etc/hostname

On redémarre les 2 VM avec la commande reboot

Echange Debian vers Debian

- On se rend sur srv-backup qui fait office de « client »

- Il faut se connecter en sio/sio et générer une paire de clé ssh avec la commande : ssh-keygen

- La commande ssh-keygen est un outil qui va générer une paire de clé privée et publique ssh

```
root@srv-backup:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/.ssh/id_rsa
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:g/SG9Kkc/UFlWC1+opN6HFaQMGSJRuv742QlLO/An58 root@srv-backup
The key's randomart image is:
+---[RSA 2048]----+
|      ..o=o ++.   |
|       oo..+o. .  |
|      .+   .o .   |
|      + B o  + .  |
|       * S o+ o   |
|      o B =*.     |
|       * ++.o     |
|        Bo.o.     |
|        .*+E      |
+----[SHA256]-----+
root@srv-backup:~# ssh-keygen -lf .ssh/id_rsa
2048 SHA256:g/SG9Kkc/UFlWC1+opN6HFaQMGSJRuv742QlLO/An58 root@srv-backup (RSA)
```

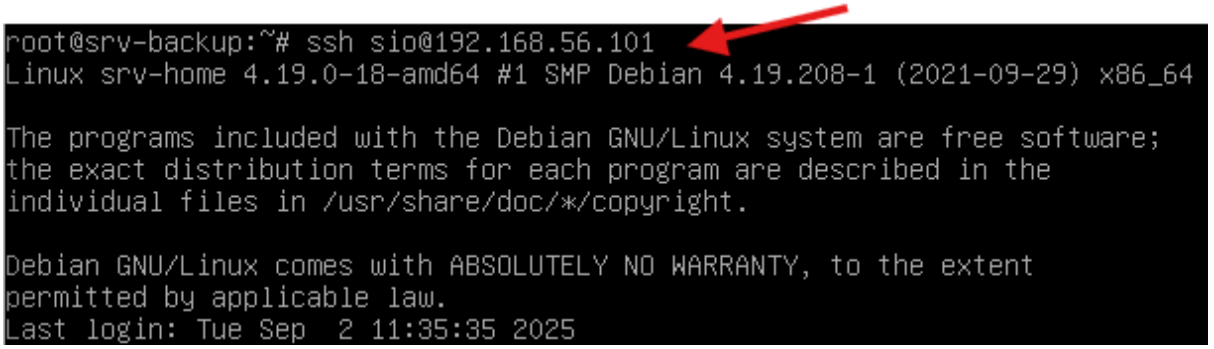
On peut afficher le **fingerprint** avec la commande suivante : **ssh-keygen -lf .ssh/id_rsa**

```
root@srv-backup:~# ssh-keygen -lf .ssh/id_rsa
2048 SHA256:g/SG9Kkc/UFlWC1+opN6HFaQMGSJRuv742QlLO/An58 root@srv-backup (RSA)
root@srv-backup:~# ssh-copy-id -i sio@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed

/usr/bin/ssh-copy-id: ERROR: ssh: connect to host 192.168.56.101 port 22: Connection refused

root@srv-backup:~# ssh-copy-id -i sio@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.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:Pg9RSHDBR1NwG2DTyf1ZZ6bb+4VGbcCJCPhAXGRJATk.
Are you sure you want to continue connecting (yes/no)? yes
```

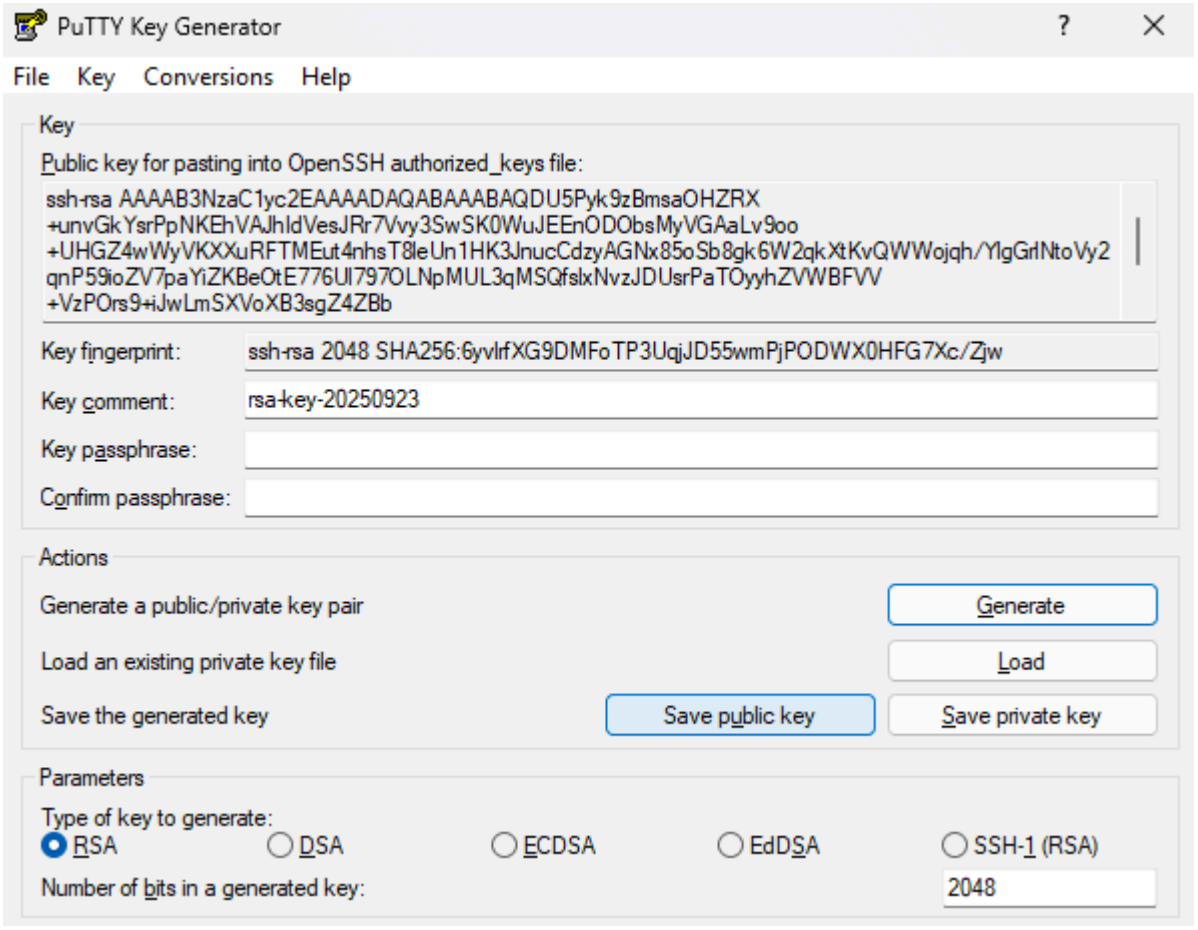
Maintenant que srv-backup est connu par srv-home on peut se connecter en ssh



Nous sommes bien connecté à srv-home en ssh, on peut constater qu'il n'y a pas de mot de passe à rentrer car notre machine est connue par srv-home

Echange Windows vers Debian

Grâce à **PuttyKeyGenerator**, nous allons Générer une clé publique sur le poste Windows, puis il faudra ensuite sauvegarder cette clé



Cliquer sur « generate » puis il faudra bouger la souris pour générer le fingerprint

Il faudra sauvegarder la clé publique au format xxx.pub

Il faut maintenant se connecter sur la machine Debian srv-home

en utilisant le profil ‘sio’

Une fois connecté en sio il faut générer la paire de clé avec la commande

ssh-keygen

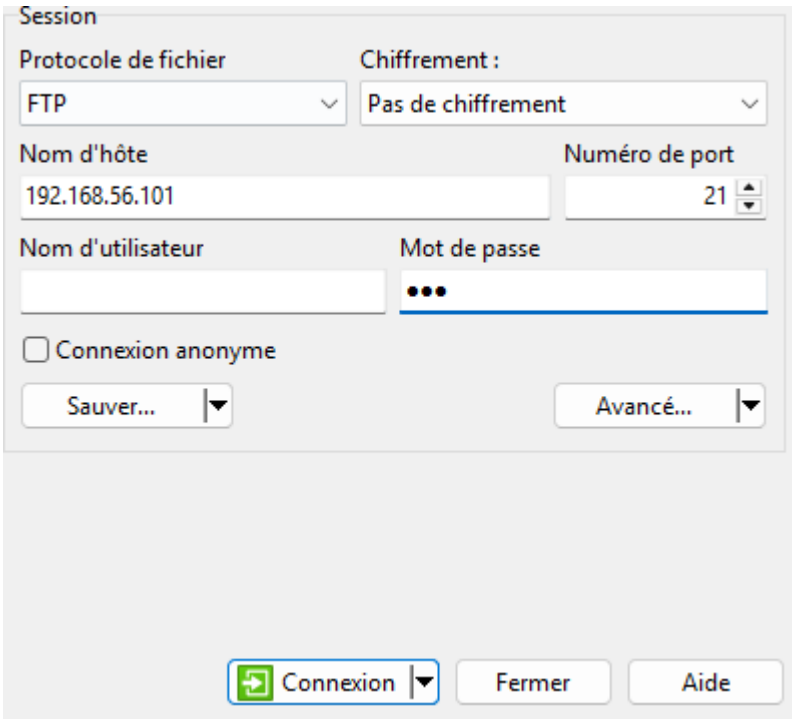
```
sio@srv-home:~$ ssh-keygen
```

La paire de clé a bien été généré

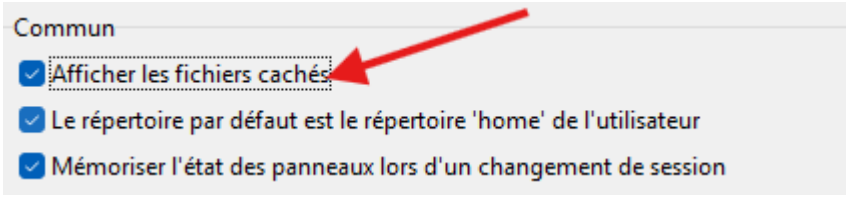
Il faut maintenant lancer **WinSCP** et il faut se connecter à srv-home

Donc il faut installer FTP car il y’a 1 paquet non installé pour la connexion

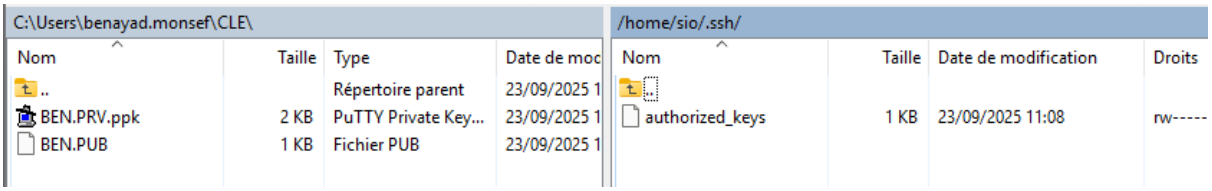
```
root@srv-home:~# apt install vsftpd
```



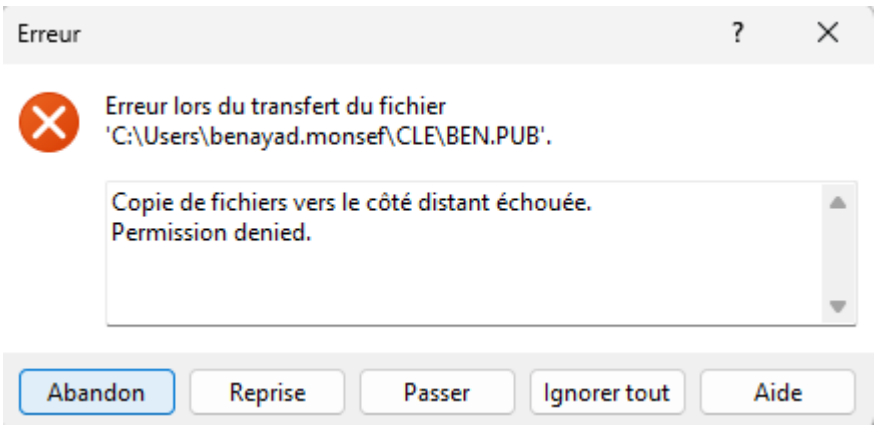
Une fois connecté, on se rend dans les paramètres, panneaux, et on clique sur **afficher les fichiers cachés**, car sans ça nous ne trouvons pas le répertoires SSH.



Il faut maintenant copier la clé publique de notre machine hôte vers srv-home dans le répertoire /home/sio/.ssh



On observe une erreur lorsqu'on essaye de transférer la clé publique vers ce répertoire



Le problème se situe au niveau des permissions donc afin de le résoudre il faut
Il faut se rendre dans le le fichier /etc/vsftpd.conf

Le but va être de modifier le fichier pour pouvoir écrire sur le fichier

On ajoute ces 2 lignes de commande ce qui va autoriser les utilisateurs à se connecter et on
leurs donne également les droits :

```
# Uncomment this to allow local users to log in.
local_enable=YES
write_enable=YES
local_umask=022
```

Il faut également faire des commandes qui vont donner la permission de transférer la clé publique

```
srv-home:~$ chmod 700 /home/sio/.ssh
```

chmod → Nom de la commande “**CH**ange **MOD**e”
700 → Accorde le droit au propriétaire (sio) : la lecture, l’écriture et l'exécution