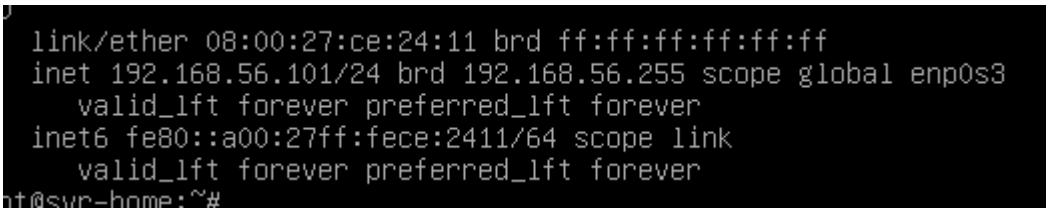
SSH avec échange de clés

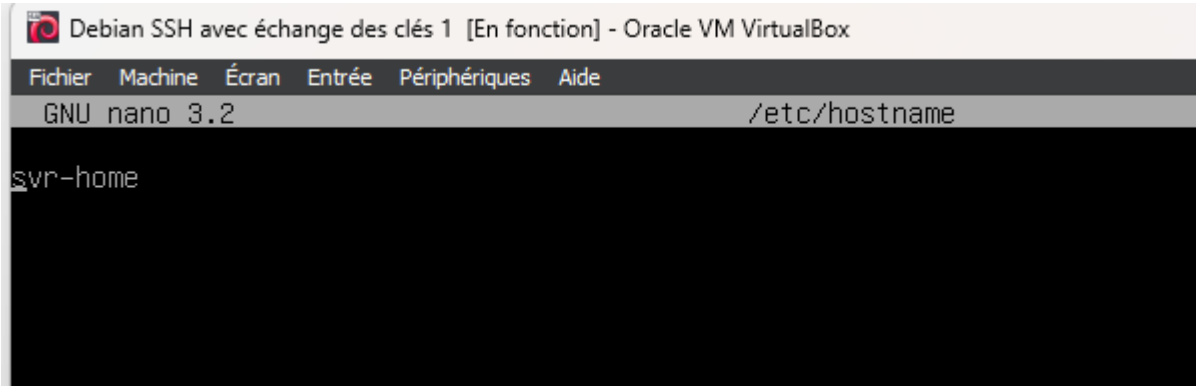
SSH C’est quoi ?

SSH (Secure Shell) est un protocole de communication sécurisé qui permet d'établir une connexion à distance avec un autre ordinateur ou serveur. Il est utilisé pour l'administration des systèmes à distance, la gestion des fichiers et l'exécution de commandes sur des machines distantes. SSH chiffre les données échangées pour garantir la sécurité des informations lors de la transmission. Il est couramment utilisé pour accéder à des serveurs Linux ou Unix.

Dans ce projet, nous allons configurer deux machines virtuelles pour permettre une connexion SSH sécurisée avec échange de clés. Les deux machines sont configurées comme suit :

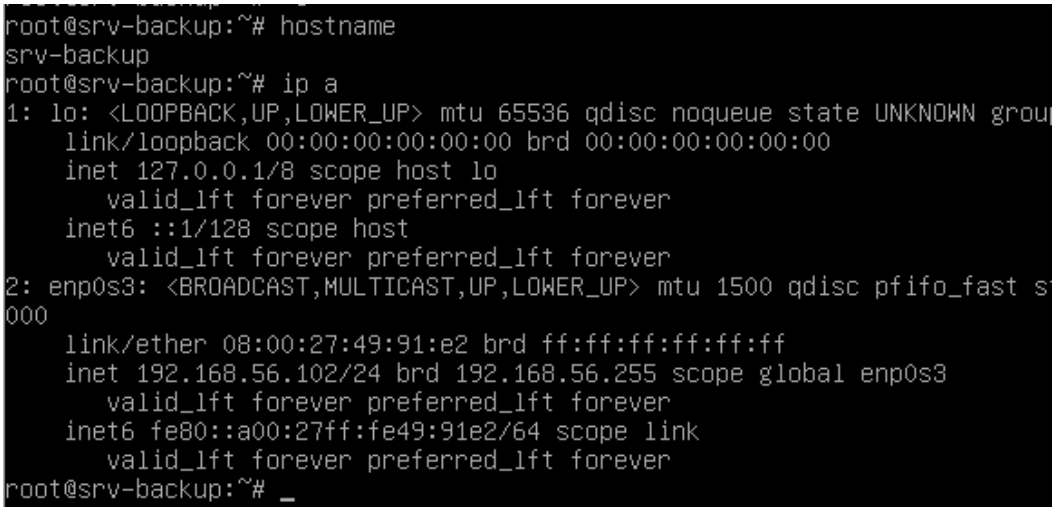
srv-home : cette machine aura l’adresse IP 192.168.56.101.
srv-backup : cette machine sera configurée avec l’adresse IP 192.168.56.102.
Ces configurations permettent de tester l’authentification sans mot de passe entre les deux machines via SSH.





Installation de SSH sur les deux machines

Pour activer le SSH sur les deux machines, installez le serveur OpenSSH en utilisant la commande suivante sur srv-home (192.168.56.101) puis sur srv-backup (192.168.56.102) :



Configuration initiale des machines virtuelles

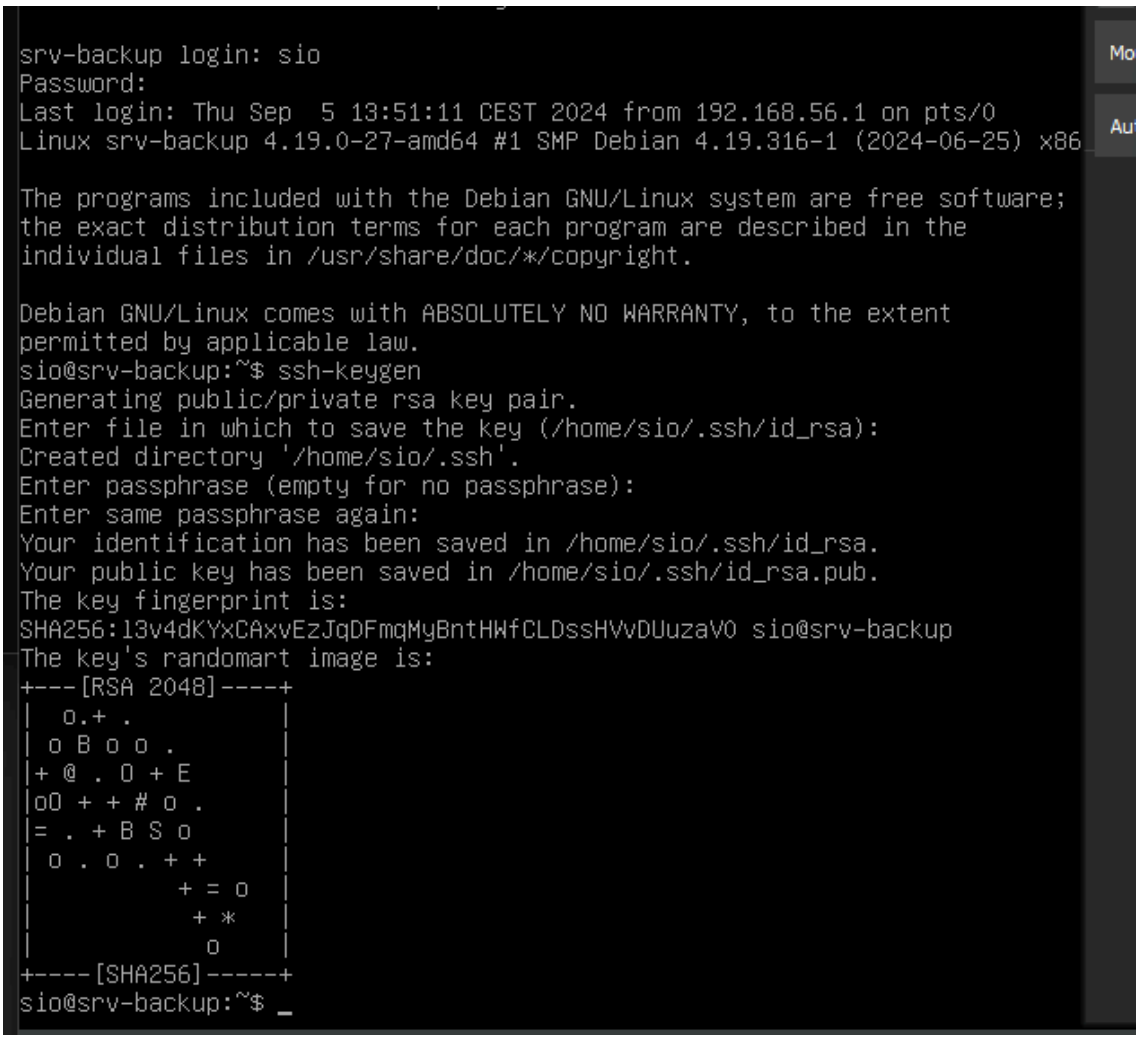
Les deux machines virtuelles, **srv-home** et **srv-backup**, sont maintenant correctement configurées pour démarrer le processus d'authentification SSH par clés.

Génération de la paire de clés SSH

La commande suivante permet de générer une paire de clés SSH (clé publique et clé privée), également appelée **empreinte numérique** ou **fingerprint**, que sera utilisée pour l'authentification sans mot de passe :

ssh-keygen

Cela crée la base de l'authentification sécurisée en utilisant des clés SSH.



Vérification de l'empreinte numérique de la clé SSH

Après avoir généré la paire de clés, vous pouvez afficher l'empreinte numérique (fingerprint) de la clé publique en utilisant la commande suivante :

SSH-keygen -lf .ssh/id_rsa

ssh-copy-id -i sio@192.168.56.101

Cette commande permet de copier la clé publique sur la machine distante afin d'activer l'authentification SSH sans mot de passe.

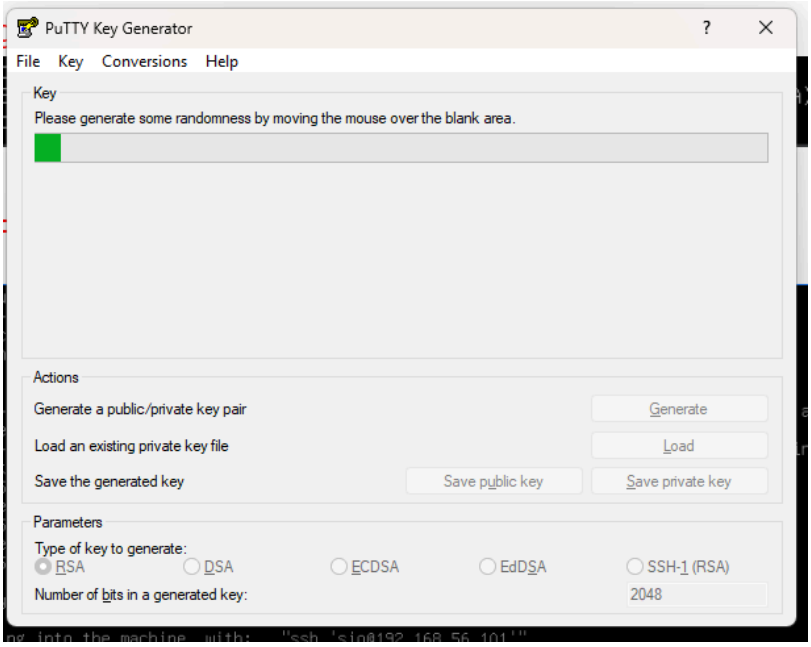
```
sio@srv-backup:~$ ssh-copy-id -i sio@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/sio/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:IADg5f+nBMRFTb8WgL8MscpljKWBH9YkwZbrAWvEquU.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
/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: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
sio@192.168.56.101's password:
Permission denied, please try again.
sio@192.168.56.101's password:
Permission denied, please try again.
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.
```

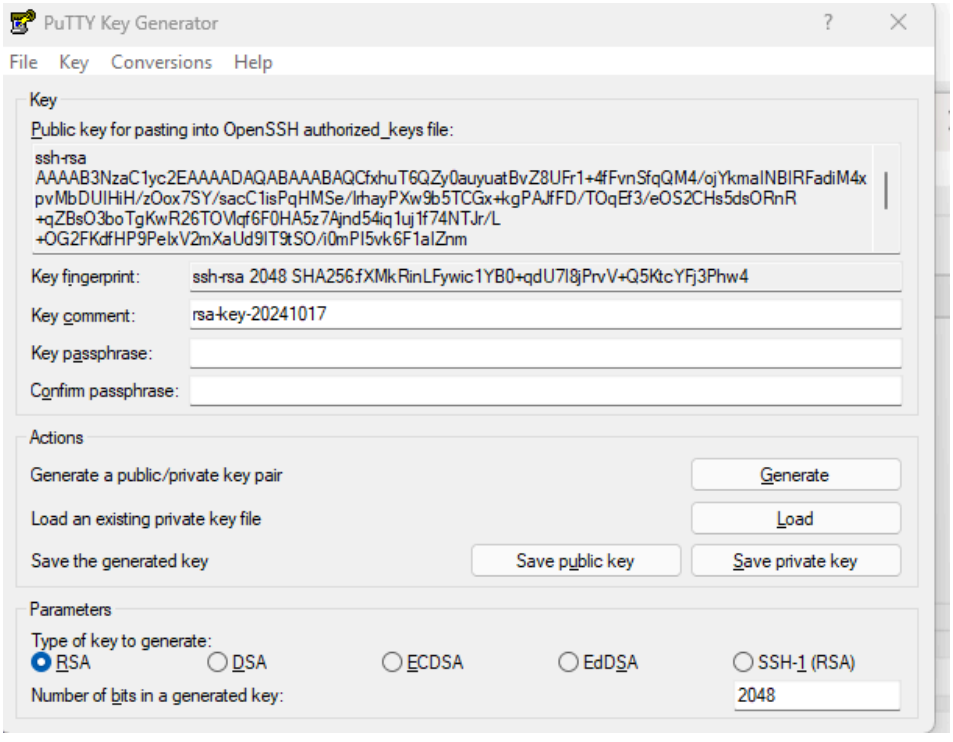
Une fois la clé publique copiée sur **srv-home**, vous pouvez tester la connexion SSH sans mot de passe depuis **srv-backup**
Avec la commande : shh sio@192.168.56.101

```
sio@srv-backup:~$ ssh sio@192.168.56.101
Linux svr-home 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Thu Sep  5 13:51:11 2024 from 192.168.56.1
sio@svr-home:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:ce:24:11 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fece:2411/64 scope link
       valid_lft forever preferred_lft forever
sio@svr-home:~$
```

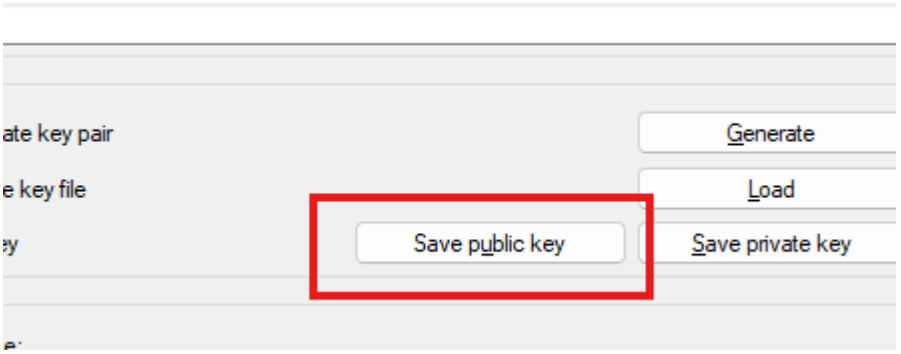
Windows ver Debian

Création d’une paire de clés dans PuTTYgen

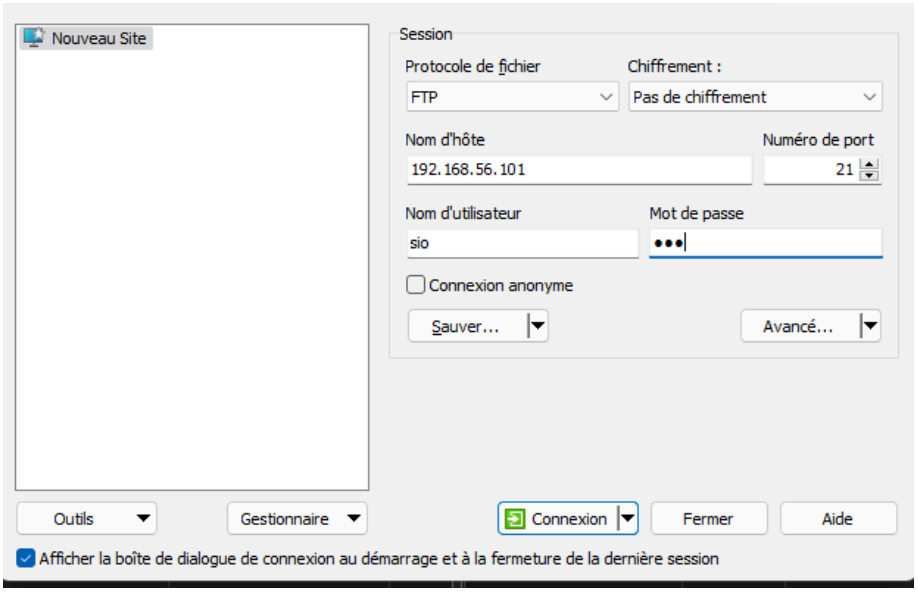


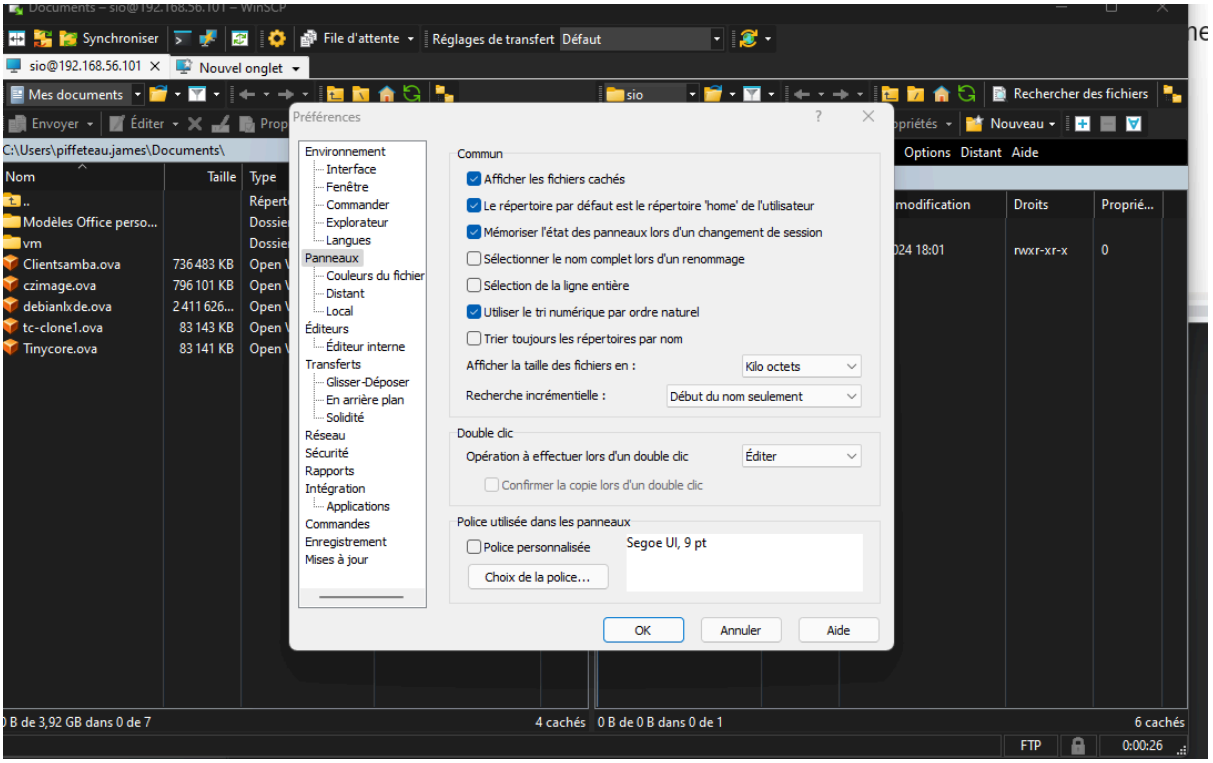


Création de la clé publique



Pour activer les transferts de fichiers FTP entre Windows et **srv-home**, installez **vsftpd** (Very Secure FTP Daemon) sur **srv-home**
avec apt installe vsftpd



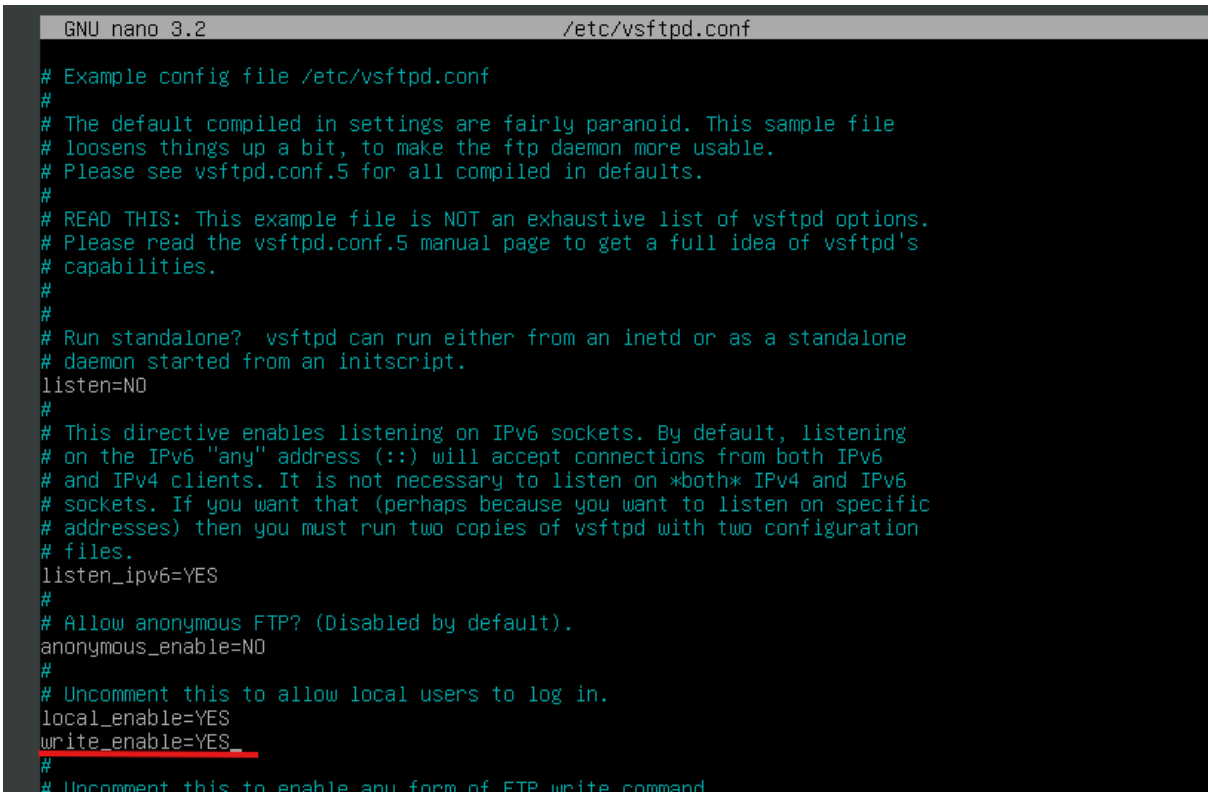


Il faut couche affichage des fichiers cachés

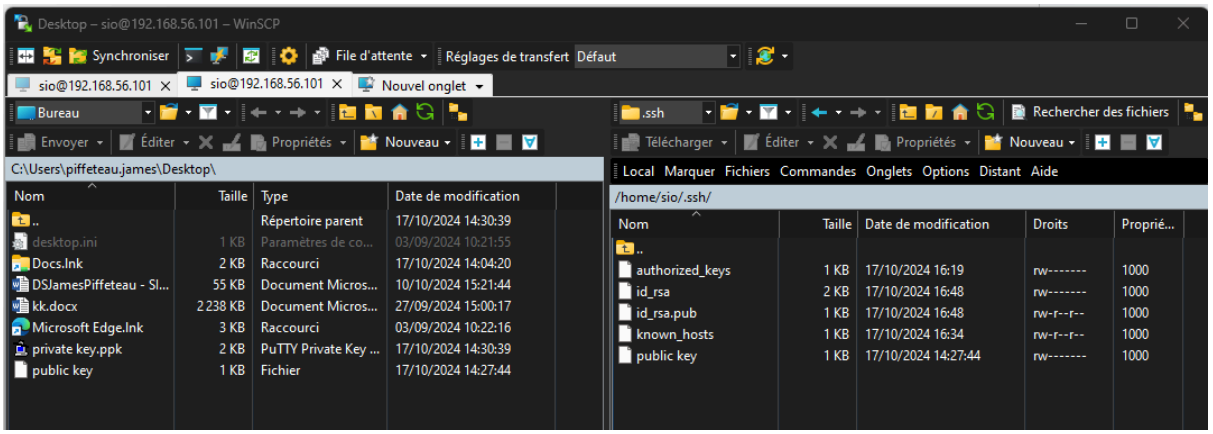
Modification du fichier de configuration vsftpd

Sur le serveur srv-home, ouvrez le fichier de configuration de vsftpd pour ajuster les paramètres FTP

nano /etc/vsftpd.conf



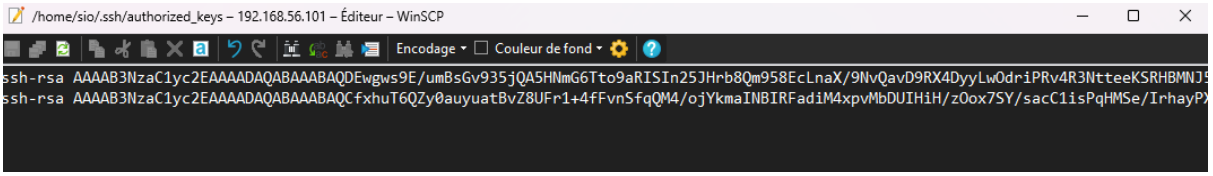
La clé publique de votre machine hôte a été copiée dans le répertoire `/home/sio/.ssh/` de **srv-home**. Ensuite, ajoutez cette clé publique dans le fichier `authorized_keys` pour permettre l'authentification sans mot de passe.




```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20241017"
AAAAB3NzaC1yc2EAAAADAQABAAABAQCfxhuT6QZy0auyuatBvZ8UFr1+4fFvnSfq
QM4/ojYkmaINBIRFadiM4xpvMbDUIHiH/zOox7SY/sacC1isPqHMSe/IrhayPXw9
b5TCGx+kgPAJfFD/TOqEf3/eOS2CHs5dsORnR+qZBsO3boTgKwR26TOV1qf6F0HA
5z7Ajnd54iq1uj1f74NTJr/L+OG2FKdfHP9PeIxV2mXaUd9IT9tSO/i0mPI5vk6F
1aIZnm+DM0tYL3vtLQKD1zcmuMV2gaot9WMBNKI5jRuEopSsTkLMGzmxQbNoxKnm
00j+kPRkGzkH25k8z4SeEJSJYW/85yYN47CFOp712fMIxLFe21tn
---- END SSH2 PUBLIC KEY ----
```

La clé public

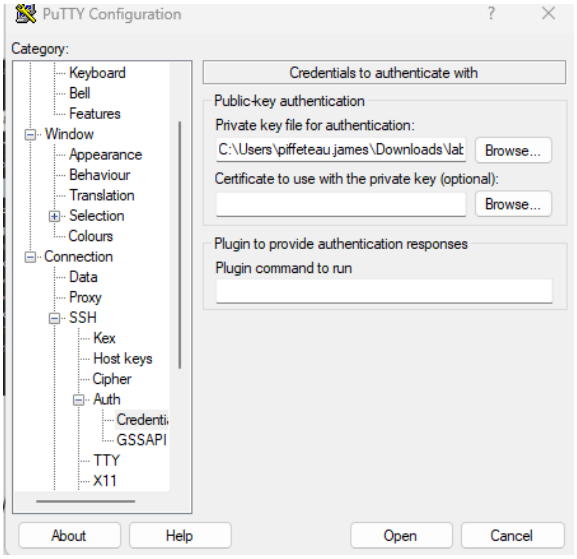
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCfxhuT6QZy0auyuatBvZ8U
Fr1+4fFvnSfqQM4/ojYkmaINBIRFadiM4xpvMbDUIHiH/zOox7SY/sacC1i
sPqHMSe/IrhayPXw9b5TCGx+kgPAJfFD/TOqEf3/eOS2CHs5dsORnR+
qZBsO3boTgKwR26TOVlqf6F0HA5z7Ajnd54iq1uj1f74NTJr/L+OG2FKdf
HP9PeIxV2mXaUd9IT9tSO/i0mPI5vk6F1aIZnm+DM0tYL3vtLQKD1zcm
uMV2gaot9WMBNKI5jRuEopSsTkLMGzmxQbNoxKnm00j+kPRkGzkH2
5k8z4SeEJSJYW/85yYN47CFOp712fMIxLFe21tn sio@srv-home



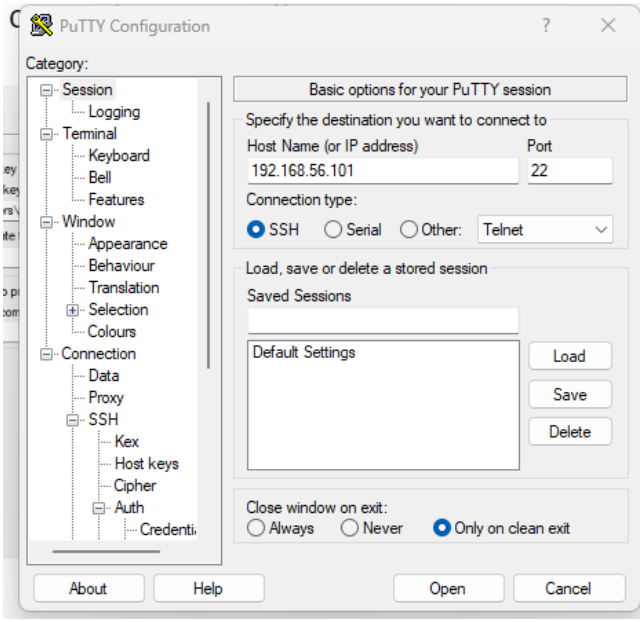
Connexion avec PuTTY

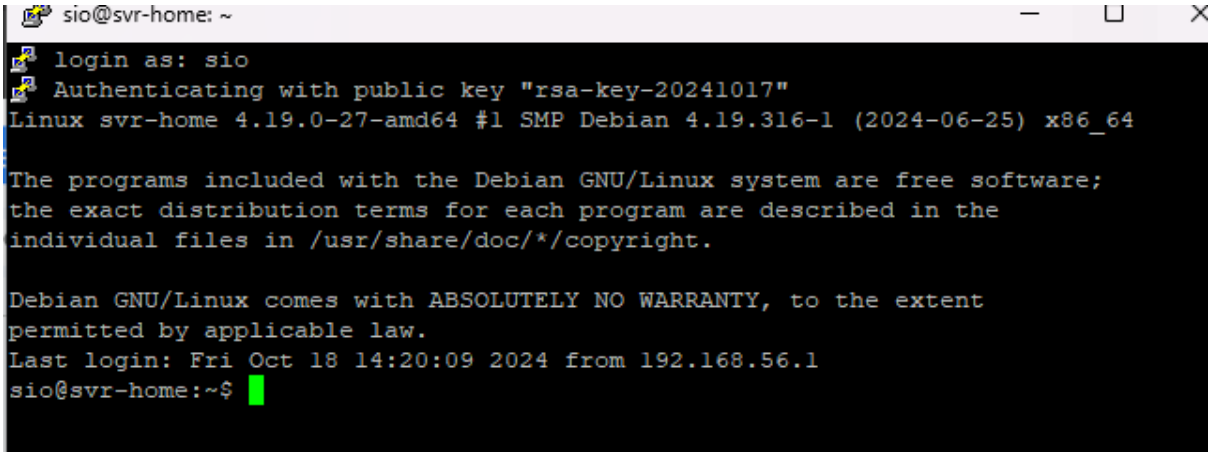
Après avoir configuré l'authentification par clé publique, vous pouvez maintenant vous connecter à srv-home depuis Windows en utilisant PuTTY. Pour l'authentification, assurez-vous d'ajouter votre clé privée dans les paramètres de PuTTY, dans la section SSH / Auth sous Credentials.

I



On met l'adresse IP du Srv-home.




sio@svr-home: ~
login as: sio
Authenticating with public key "rsa-key-20241017"
Linux svr-home 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Fri Oct 18 14:20:09 2024 from 192.168.56.1
sio@svr-home:~$