

SSH avec échange de clés

- [SSH avec échange de clés](#)

SSH avec échangees de clés

Nous allons crée un serveur Linux puis nous allons config l'ip

pour le SRV-home 192.168.56.101

pour le SRV-backup 192.168.56.102

SRV-Backup :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static

address 192.168.56.101/24
gateway 192.168.56.254
```

Puis nous allons installer openssh-server

```
root@srv-home:~# apt install openssh-server
```

Objectifs : Accéder a srv-home depuis srv-backup

On se connecte au serveur de Backup (serveur linux vierge sans rien)

on écrit

ssh-keygen

```
sio@srv-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:tkvZF5ew7WljtY4WdEqkXUB4o72o/auCvAfZ/wd80jg sio@srv-backup
The key's randomart image is:
+---[RSA 2048]-----+
|      .oo.      |
|     .+.      |
|    .o.o      |
|   .o.o.o     |
|  S  B B .    |
| + = . X +.   |
| . * = o @.   |
| + = E *oo    |
| .+ ..*=+.   |
+-----[SHA256]-----+
sio@srv-backup:~$ _
```

On fais la commande ci dessous afin de voir la clé ssh

```
ssh-keygen -lf .ssh/id_rsa
```

Maintenant on va la copier

ssh

```
ssh-copy-id -i sio@192.168.56.101
```

puis

ssh sio@192.168.56.101

```
ssh sio@192.168.56.101
```

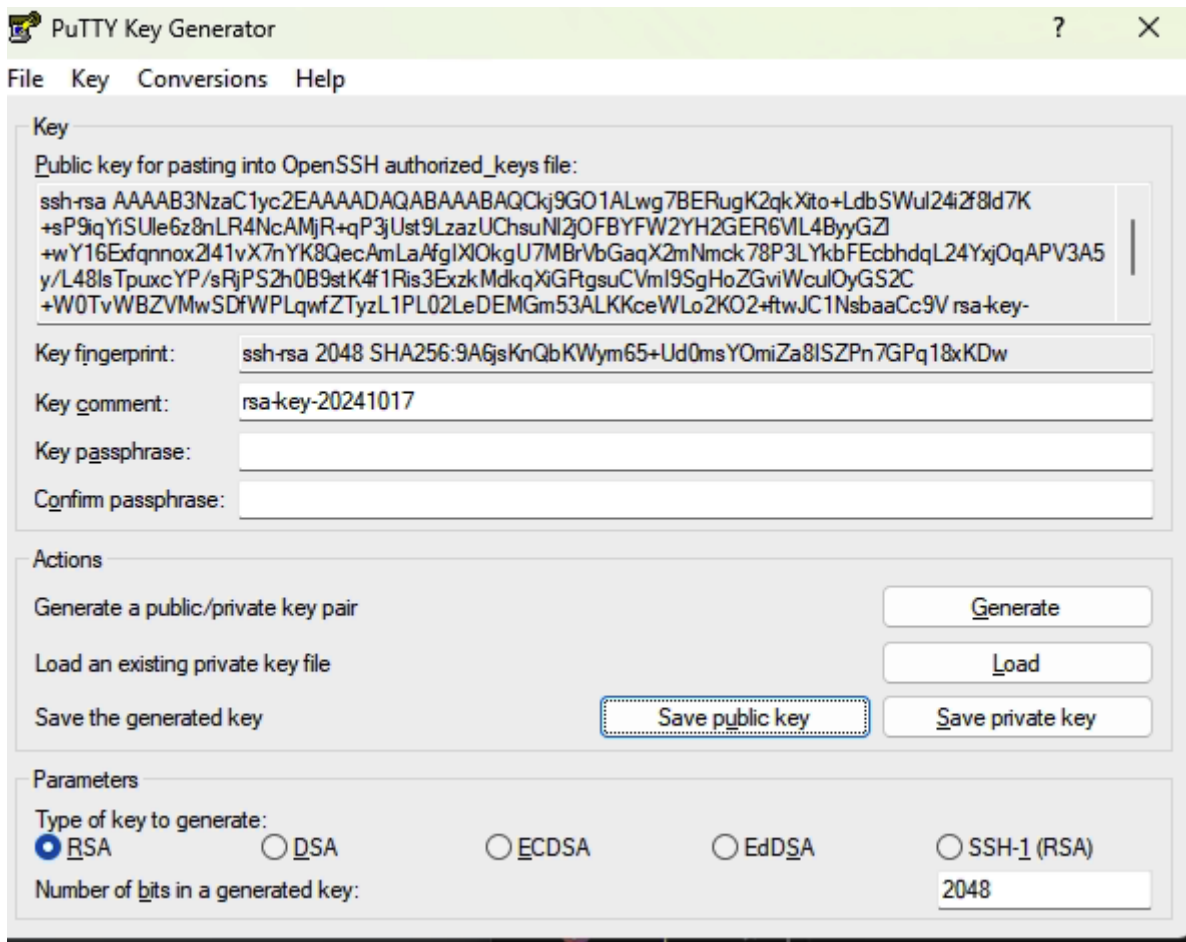
et nous pouvons voir que nous sommes connecté au srv-home a l'aide du srv backup

```
sio@srv-backup:~$ ssh sio@192.168.56.101
Linux srv-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: Tue Jan  7 14:13:42 2020
sio@srv-home:~$ _
```

On va généré une clé public a l'aide de Putty Key Generator



On se connecte sur SRV-home est on genere une paire de clé

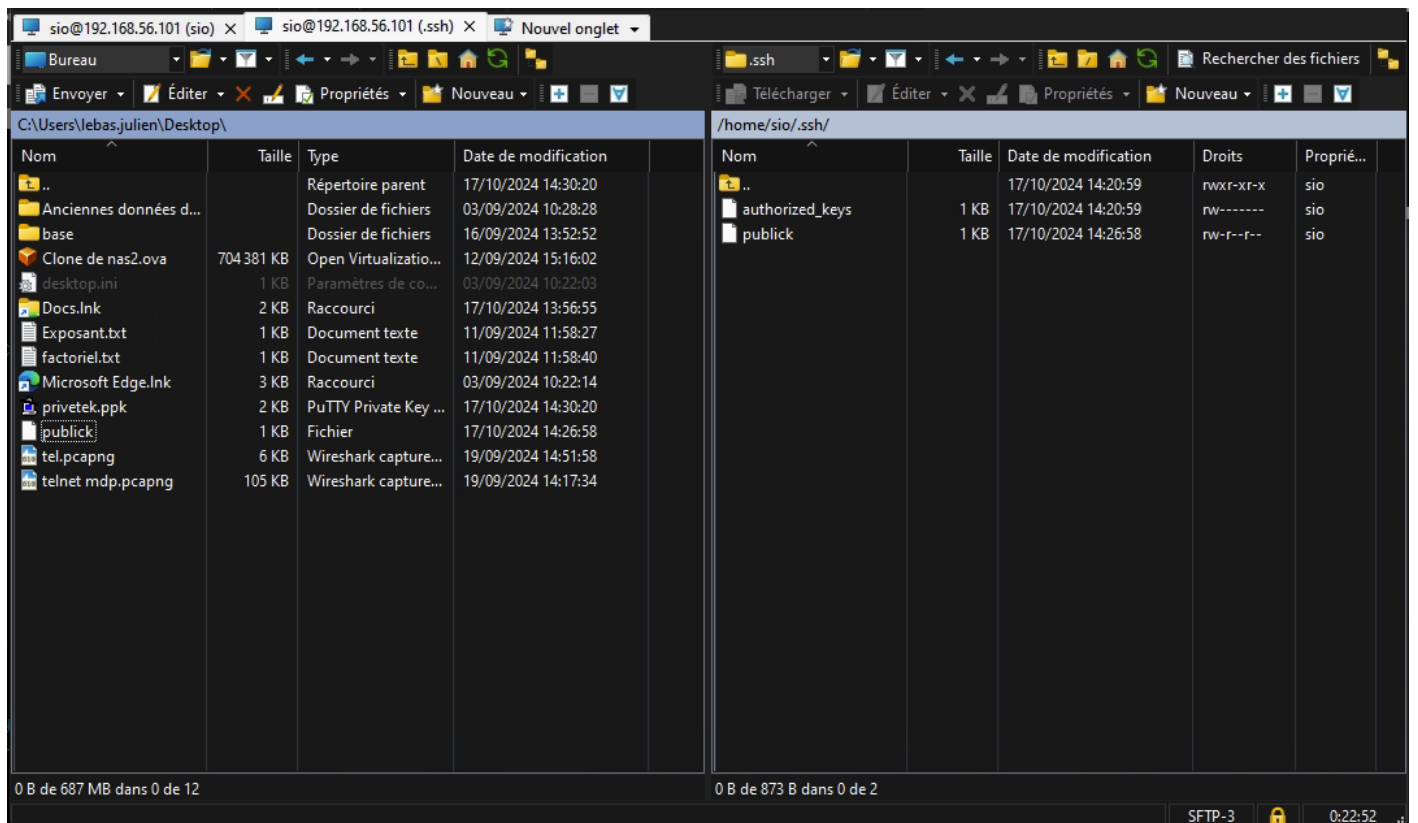
ssh

```
ssh-keygen
```

On install vsftpd

```
apt install vsftpd
```

On se connecte avec WinSCP puis on transfere la clés public qu'on a crée sur le .ssh de l'utilisateur



Modification du fichier de configuration de vsftpd :

- Sur le serveur **srv-home**, éditez le fichier de configuration avec :

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
write_enable=YES
#
```

Ajout de la clé publique pour une authentification sans mot de passe :

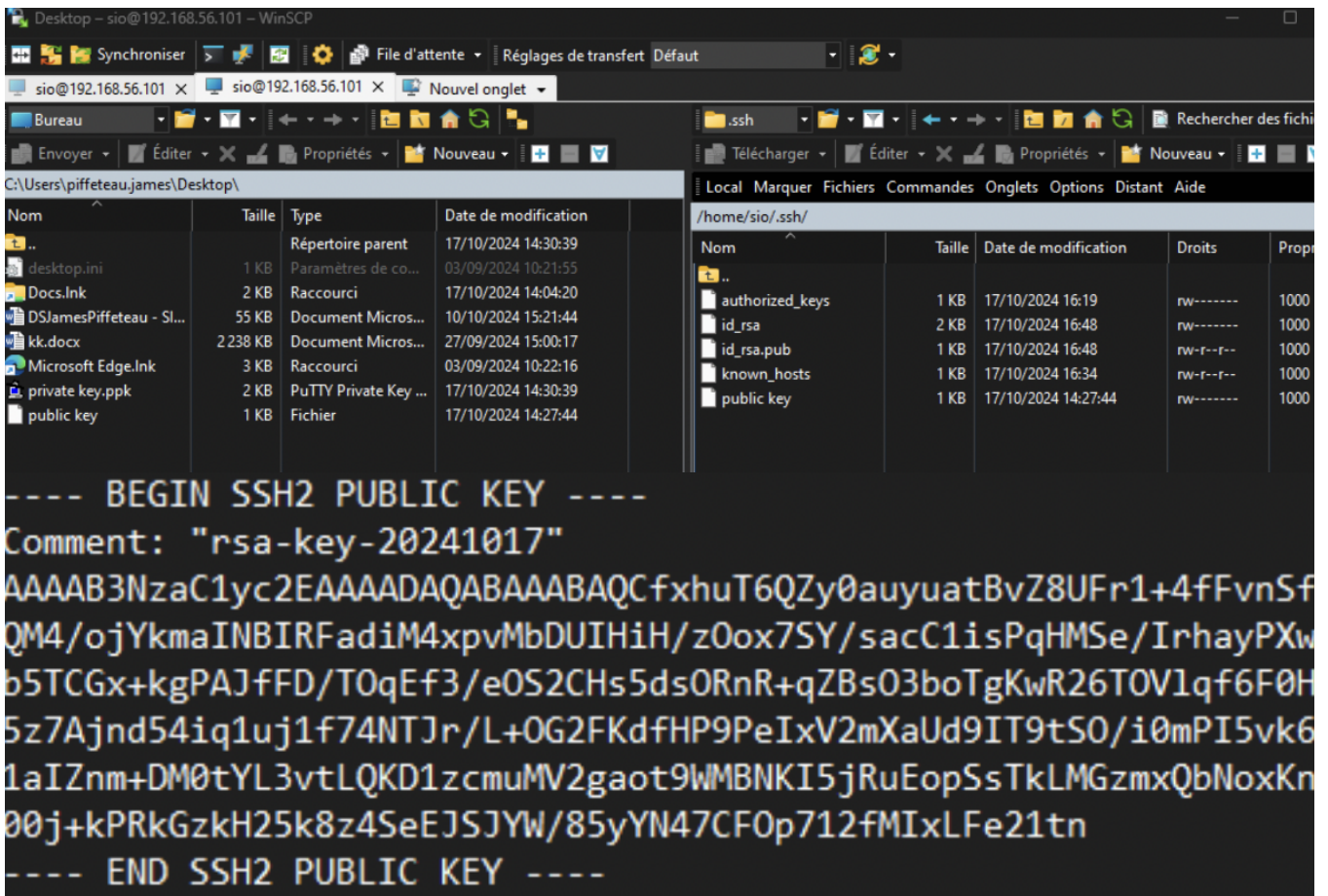
1. **Vérifiez que la clé publique est copiée** dans le répertoire `/home/sio/.ssh/` de **srv-home**.
2. **Ajoutez la clé au fichier** `authorized_keys` :

```
cat /home/sio/.ssh/id_rsa.pub >> /home/sio/.ssh/authorized_keys
```

3. **Vérifiez les permissions :**

Assurez-vous que le fichier et le dossier ont les bonnes permissions :

```
chmod 600 /home/sio/.ssh/authorized_keys
chmod 700 /home/sio/.ssh
```



Et on l'ajoute a notre authorized_keys.

