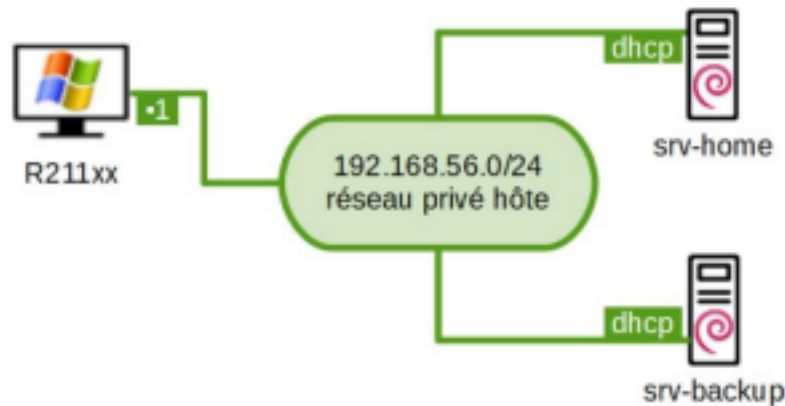


Séance SSH

Schéma :	2
Objectifs :	2
Configuration des VM.....	3
Echange Debian vers Debian.....	4
Echange Windows vers Debian.....	5

Schéma :



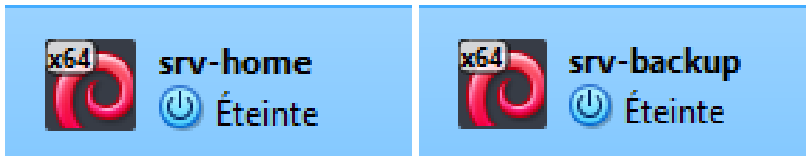
L'échange de clés en SSH permet de *sécuriser la connexion entre un client et un serveur*. Le *client* utilise une *clé publique* pour s'authentifier auprès du *serveur*, qui a la *clé privée correspondante*. Cela permet de chiffrer les données échangées et de protéger la communication contre les interceptions.

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 nommée '**srv-home**' en **192.168.56.101** et l'autre nommée '**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/UF1WC1+opN6HFaqMGSJRuv742Q1L0/An58 root@srv-backup
The key's randomart image is:
+---[RSA 2048]-----+
|      ..0=0 ++.      |
|      00..+0. .      |
|      .+   .0 .      |
|      + B o   + .      |
|      * S o+ o        |
|      o B =*.         |
|      * ++.0         |
|      B0.o.          |
|      .*+E           |
+----[SHA256]-----+
root@srv-backup:~# ssh-keygen -lf .ssh/id_rsa
2048 SHA256:g/SG9Kkc/UF1WC1+opN6HFaqMGSJRuv742Q1L0/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/UF1WC1+opN6HFaqMGSJRuv742Q1L0/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 already 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:Pg9RSHDBR1NwG2DTyf1Z26bb+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



```
root@srv-backup:~# ssh sio@192.168.56.101
Linux srv-home 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) 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  2 11:35:35 2025
```

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

The screenshot shows the PuTTY Key Generator application window. The 'Key' section displays a public key for pasting into an OpenSSH authorized_keys file. The key is an RSA 2048-bit key with a SHA256 fingerprint. The 'Actions' section contains buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows that the 'Type of key to generate' is set to 'RSA' and the 'Number of bits in a generated key' is set to '2048'.

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDU5Pyk9zBmsaOHZRX
+unvGkYsrPpNKEhVAJhldVesJRr7Vvy3SwSK0WuJEEenODObsMyVGAaLv9oo
+UHGZ4wWyVKXXuRFTMEut4nhsT8leUn1HK3JnucCdzyAGNx85oSb8gk6W2qkXtKvQWWojqh/YlgGrfNtoVy2
qnP59ioZV7paYiZKBeOtE776UI797OLNpMUL3qMSQfslxNvzJDUsrPaTOyyhZVWBFVV
+VzPOrs9+iJwLmSXVoXB3sgZ4ZBb
```

Key fingerprint: ssh-rsa 2048 SHA256:6yvlrfXG9DMFoTP3UqjJD55wmPjPODWX0HFG7Xc/Zjw

Key comment: rsa-key-20250923

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

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 générée

```
sio@srv-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:gn1kJP/KICPM+z1Hw/zTBUX/LEeRDgh2Gsue2elkey4 sio@srv-home
The key's randomart image is:
+----[RSA 2048]-----+
|      ..+      ....|
|      0 * + .   .0.|
|      . 0 = * 0.. 0|
|      0      . = B.0 0.|
|    + 0 . S 0 ..0 +|
|      0 0.0 + +   .0|
|      . . .0 0. .  |
|      .....E....|
|      oo  ooo.    |
+----[SHA256]-----+
sio@srv-home:~$ _
```

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_
```

Session

Protocole de fichier : FTP

Chiffrement : Pas de chiffrement

Nom d'hôte : 192.168.56.101

Numéro de port : 21

Nom d'utilisateur :

Mot de passe :

☐ Connexion anonyme

Sauver... Avancé...

Connexion Fermer Aide

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.

Commun

☒ Afficher les fichiers cachés

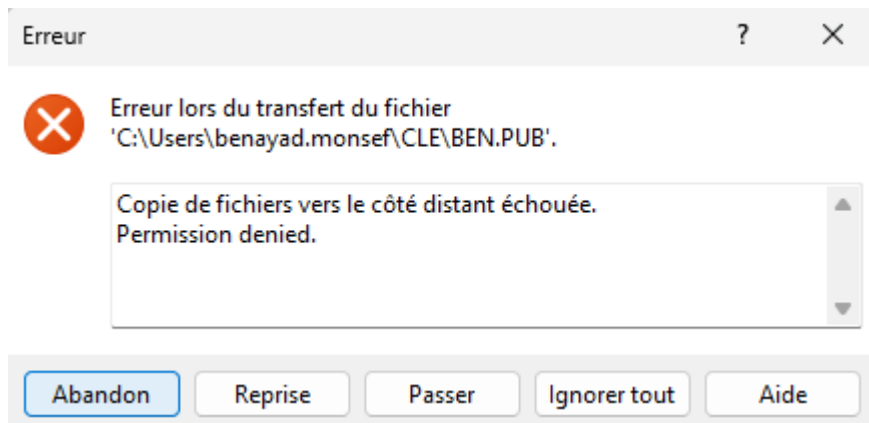
☒ Le répertoire par défaut est le répertoire 'home' de l'utilisateur

☒ Mémoriser l'état des panneaux lors d'un changement de session

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

C:\Users\benayad.monsef\CLE\				/home/sio/.ssh/			
Nom	Taille	Type	Date de mod	Nom	Taille	Date de modification	Droits
..		Répertoire parent	23/09/2025 1	..			
BEN.PRIV.ppk	2 KB	PuTTY Private Key...	23/09/2025 1	authorized_keys	1 KB	23/09/2025 11:08	rw----
BEN.PUB	1 KB	Fichier PUB	23/09/2025 1				

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 **MODe**”

700 → Accorde le droit au propriétaire (sio) : la lecture, l’écriture et l’exécution