

DONMEZ

Documentation Samba, NFS, CloneZilla et SSH avec échange de clés

Okan

SI02



Table des matières

1) Qu'est-ce que Samba ?	3
1.1) Installation de Samba	4
1.2) Mise en pratique de Samba	4
2) Qu'est-ce que NFS ?	9
2.1) Installation de NFS	10
2.2) Mise en pratique d'NFS	11
3) Qu'est-ce que CloneZilla ?	13
3.1) Installation de CloneZilla	14
3.2) Mise en pratique de CloneZilla	14
4) Qu'est-ce que SSH avec échange de clés ?	18
4.1) Installation de SSH avec échange de clés	19
4.2) Mise en pratique de SSH avec échange de clés	19

1) Qu'est-ce que Samba ?

Samba est une suite de logiciels open source qui permet de partager des fichiers et des imprimantes entre des ordinateurs fonctionnant sous des systèmes d'exploitation différents sur un réseau local. Le nom "Samba" est en réalité un jeu de mots basé sur le protocole SMB (Server Message Block), qui est utilisé pour le partage de fichiers et d'imprimantes dans les environnements Windows. Samba permet aux ordinateurs Linux, Unix et d'autres systèmes d'exploitation compatibles de se comporter comme des serveurs de fichiers Windows, ce qui signifie qu'ils peuvent partager des fichiers et des imprimantes de manière transparente avec des ordinateurs Windows.

Les principales fonctionnalités de Samba incluent :

Partage de fichiers : Samba permet de partager des répertoires et des fichiers entre des ordinateurs Windows, Linux, MacOS et d'autres systèmes d'exploitation compatibles avec le protocole SMB/CIFS.

Impression : Samba permet de configurer des imprimantes partagées sur un réseau, ce qui permet aux utilisateurs d'imprimer des documents sur des imprimantes connectées à des ordinateurs Linux ou Unix via le protocole SMB/CIFS.

Authentification : Samba prend en charge l'authentification des utilisateurs, ce qui signifie qu'il peut être configuré pour contrôler l'accès aux ressources partagées en vérifiant les noms d'utilisateur et les mots de passe.

Intégration avec Active Directory : Samba peut être utilisé pour intégrer des systèmes Linux et Unix dans un domaine Windows Active Directory, ce qui permet une gestion centralisée des utilisateurs et des groupes.

1.1) Installation de Samba

Sur la machine serveur qui est ici cz image, nous allons installer le serveur Samba, mais avant toute installation de paquet, nous allons exécuter la commande : `apt update` pour mettre à jour les paquets.

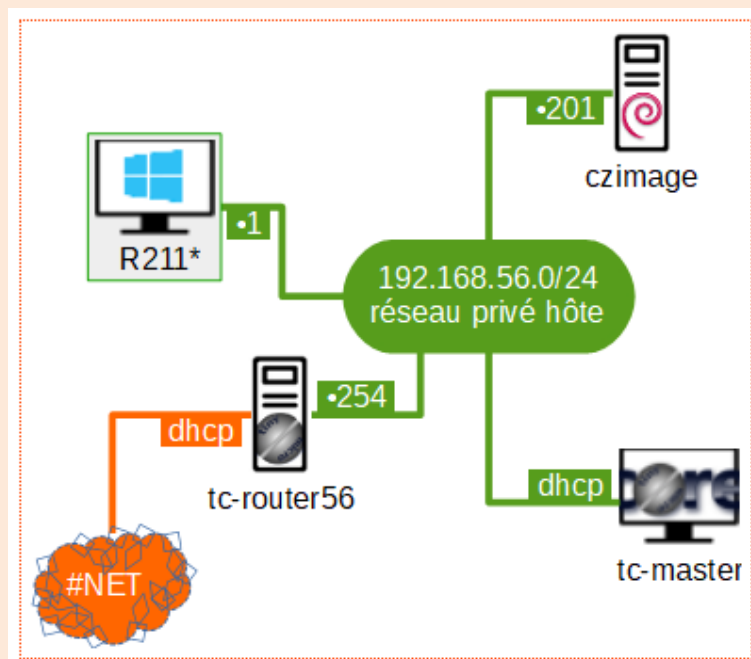
Nous pouvons maintenant exécuter la commande suivante : `apt install samba`

Nous pouvons éventuellement vérifier que le serveur est bien installé en exécutant la commande :

```
systemctl status samba
```

1.2) Mise en pratique de Samba

Schéma de notre réseau :



DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

Puis, nous allons aller dans le fichier de configuration de samba (après avoir vérifié que le serveur est bien actif) soit, en exécutant la commande :

mousepad /etc/samba/smb.conf

Nous allons rajouter le répertoire partagé « partimag » tout à la fin du fichier de configuration « smb.conf ».

```
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin
...
[partimag]
    path = /home/partimag
    guest ok = yes
    read only = yes
    testparm
```

Après avoir modifier le fichier de configuration on peut exécuter la commande :

testparm

Cette commande va nous permettre de valider la configuration de ce dernier.

Passons maintenant au client samba où vous pouvez installer une vm debian 11 Bullseye qui fonctionnera très bien.

DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SI02

Maintenant qu'on est sur notre machine cliente sur LXDE, nous pouvons y installer le client samba via la commande :

apt install smbclient

Après avoir installé le client samba, nous pouvons créer un utilisateur qu'on va nommer « odo ».

```
root@cz-image:~# adduser odo
Ajout de l'utilisateur « odo » ...
Ajout du nouveau groupe « odo » (1002) ...
Ajout du nouvel utilisateur « odo » (1002) avec le groupe « odo » ...
Création du répertoire personnel « /home/odo »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for odo
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Cette information est-elle correcte ? [0/n]o
root@cz-image:~# _
```

Lors de la création de l'utilisateur, il nous demande plusieurs informations, en tapant simplement sur entrée, nous pouvons ignorer cela et passer directement à la création du mot de passe.

Après cela, nous allons lui mettre les droits sur le partage effectué.

```
root@cz-image:~# chown smbuser:smbuser /home/partimag_
```

DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SI02

Il faut maintenant rajouter l'utilisateur dans le fichier de configuration smb.conf sur le serveur samba :

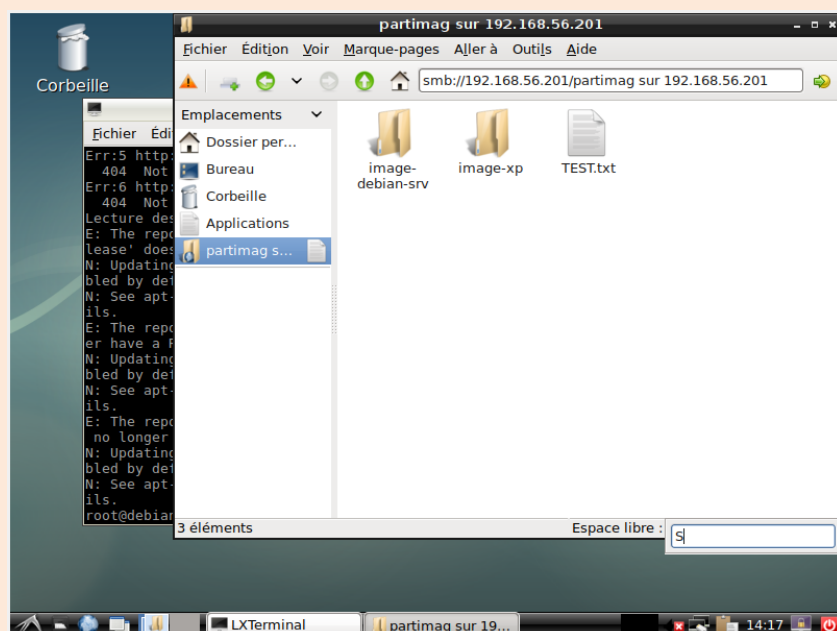
```
root@cz-image:~# nano /etc/samba/smb.conf
```

```
[partimag]
    path = /home/partimag
    guest ok = no
    read only = yes
    valid users = smbuser
```

Nous pouvons valider le fichier de configuration.

```
root@cz-image:~# testparm_
```

Nous allons vérifier qu'on accède bien au partage via LXDE :

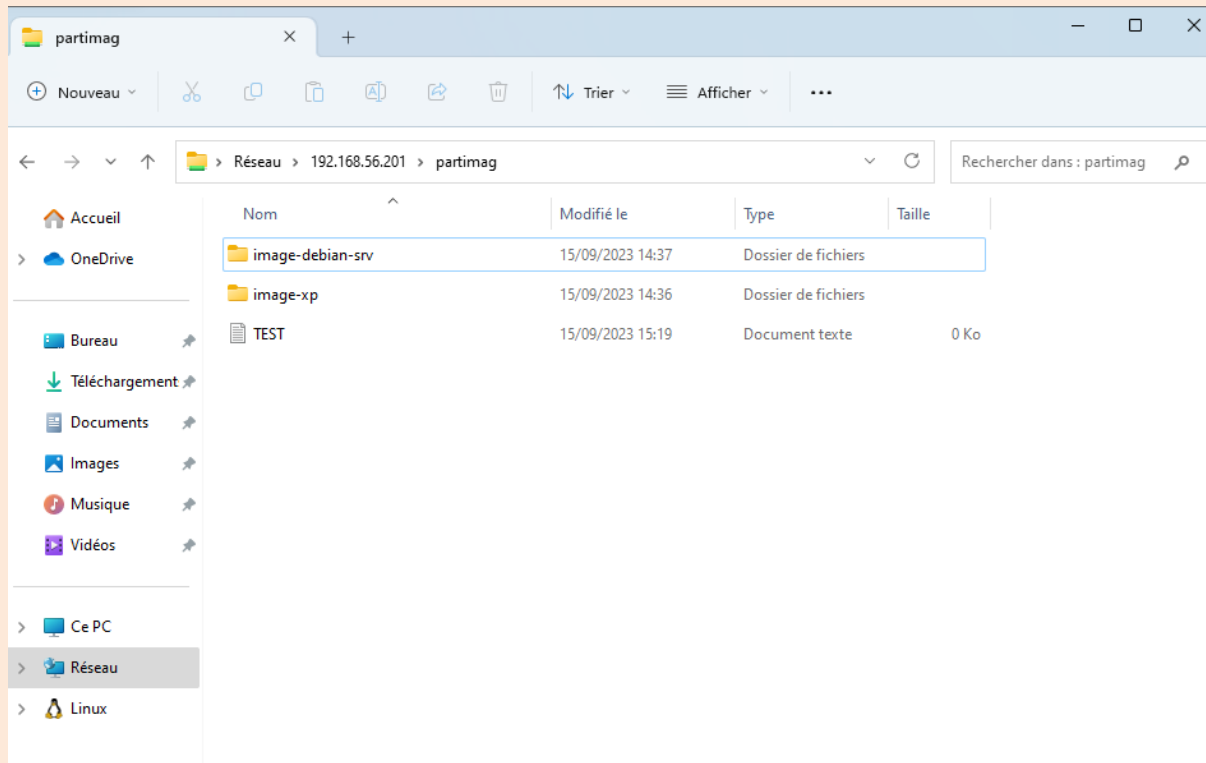


DONMEZ [**Documentation Samba, NFS, CloneZilla et SSH avec échange de clés**](#)

Okan

SI02

Nous allons vérifier qu'on accède bien au partage via la machine hôte Windows :



Nous allons nous connecter au partage via la machine Debian cliente : (-U : User)

Attention de bien rentrer le mot de passe configuré lors de la création de l'utilisateur.

```
root@buster:~# smbclient //192.168.56.201/partimag -U smbuser
Enter WORKGROUP\smbuser's password:
Try "help" to get a list of possible commands.
smb: \>
```


2) Qu'est-ce que NFS ?

NFS, ou Network File System, est un protocole de partage de fichiers qui permet à des ordinateurs de partager des fichiers et des répertoires sur un réseau. NFS a été développé par Sun Microsystems (aujourd'hui une partie d'Oracle) dans les années 1980 et est souvent associé aux systèmes d'exploitation Unix et Unix-like, bien qu'il puisse également être utilisé dans d'autres environnements.

Voici quelques caractéristiques clés de NFS :

Partage de fichiers : NFS permet à un ordinateur de partager des fichiers et des répertoires avec d'autres ordinateurs du réseau, ce qui permet un accès transparent aux données stockées sur des serveurs NFS à partir de clients NFS.

Systèmes d'exploitation compatibles : NFS est couramment utilisé avec des systèmes d'exploitation Unix et Unix-like, tels que Linux, FreeBSD, macOS, et diverses versions d'Unix. Il existe des implémentations de NFS pour d'autres systèmes d'exploitation, notamment Windows.

Montage de répertoires distants : Dans un environnement NFS, les clients peuvent monter (ou "monter en réseau") des répertoires distants partagés par des serveurs NFS, ce qui les rend accessibles comme s'ils étaient locaux.

Protocole réseau : NFS fonctionne sur le réseau en utilisant le protocole RPC (Remote Procedure Call) pour les opérations de partage de fichiers. Il existe plusieurs versions du protocole NFS, telles que NFSv2, NFSv3 et NFSv4, chacune avec ses propres améliorations et fonctionnalités.

Authentification et sécurité : NFS inclut des mécanismes d'authentification et de contrôle d'accès pour protéger les données partagées et limiter l'accès aux utilisateurs autorisés.

DONMEZ [Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

2.1) Installation de NFS

Nous allons installer le serveur NFS côté serveur en exécutant la commande (après un apt update bien sûr) :

```
root@buster:~# apt install nfs-kernel-server
```

Nous nous dirigeons vers le fichier de configuration de ce dernier, en tapant la commande suivante :

mousepad /etc/exports

Une fois arrivé dans le fichier de configuration, nous allons ajouter le dossier partagé tout à la fin :

/home/partimag 192.168.56.0/255.255.255.0(ro,all_squash)

Il faut maintenant relancer le service en exécutant la commande :

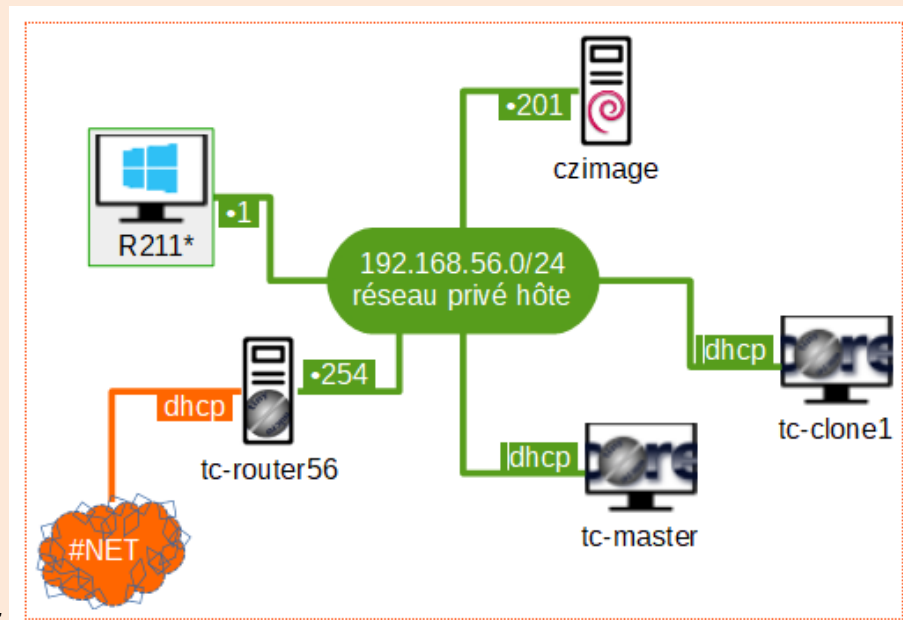
```
root@buster:~# service nfs-kernel-server restart_
```

Okan

SI02

2.2) Mise en pratique d’NFS

Schéma de notre réseau :



Il faut maintenant monter la ressource distante côté client avec la commande :

```
root@buster:~# showmount -e 192.168.56.201
Export list for 192.168.56.201:
/home/partimag 192.168.56.0/255.255.255.0
root@buster:~#
```

Le répertoire est bien monté !

Si la commande est introuvable, il faut installer le paquet nfs-common côté client :

```
root@buster:~# apt install nfs-kernel-server nfs-common
```

DONNEZ *Documentation Samba, NFS, CloneZilla et SSH avec échange de clés*

Okan

SIO2

On va maintenant monter le répertoire /home/partimag dans le répertoire /media/NFS du client.

```
root@buster:~# mkdir /media/NFS
root@buster:~# mount 192.168.56.201.:/home/partimag /media/nfs
mount.nfs: mount point /media/nfs does not exist
root@buster:~# mount 192.168.56.201.:/home/partimag /media/NFS
```

On peut maintenant vérifier en faisant un « ls -la » dans /media/nfs que le répertoire est bien présent.

3) Qu'est-ce que CloneZilla ?

Clonezilla est un logiciel open source de clonage de disque dur et de création d'images système. Il est conçu pour permettre aux utilisateurs de créer des copies exactes de disques durs, de partitions ou de systèmes d'exploitation complets, ce qui peut être extrêmement utile dans divers scénarios, notamment la sauvegarde, la récupération de données, le déploiement de systèmes d'exploitation et la migration vers de nouveaux disques.

Voici quelques caractéristiques principales de Clonezilla :

Clonage de disque dur : Clonezilla permet de créer une copie exacte d'un disque dur, y compris toutes les partitions, le système d'exploitation et les données. Cela peut être utile pour effectuer des sauvegardes complètes de systèmes, des migrations de disque dur ou des mises à niveau matérielles.

Clonage de partition : Il est également possible de cloner des partitions individuelles plutôt que des disques entiers. Cela peut être utile lorsque vous souhaitez dupliquer uniquement une partie spécifique de votre système.

Création d'images système : Clonezilla permet de créer des images système de disques ou de partitions. Ces images peuvent être stockées sur un support externe ou sur un serveur distant, puis restaurées ultérieurement pour récupérer le système dans son état précédent.

Prise en charge de divers systèmes de fichiers : Clonezilla prend en charge de nombreux systèmes de fichiers courants, ce qui le rend compatible avec une large gamme de configurations de disques durs.

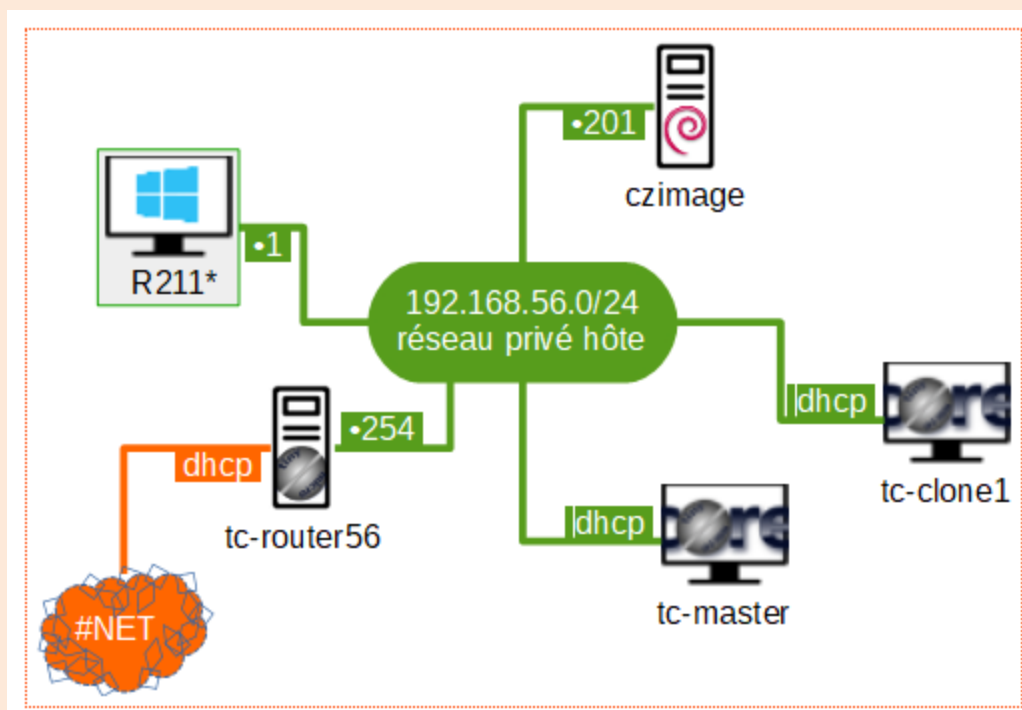
Interface utilisateur en ligne de commande et en mode graphique : Clonezilla est disponible en deux versions, l'une avec une interface en ligne de commande pour les utilisateurs avancés et l'autre avec une interface graphique pour les utilisateurs moins expérimentés.

3.1) Installation de CloneZilla

Tout d'abord, il faut créer une machine virtuelle vide puis mettre une image sur tc master pour faire en sorte de démarrer en bootant sur clonezilla.

3.2) Mise en pratique de CloneZilla

Schéma de notre réseau :

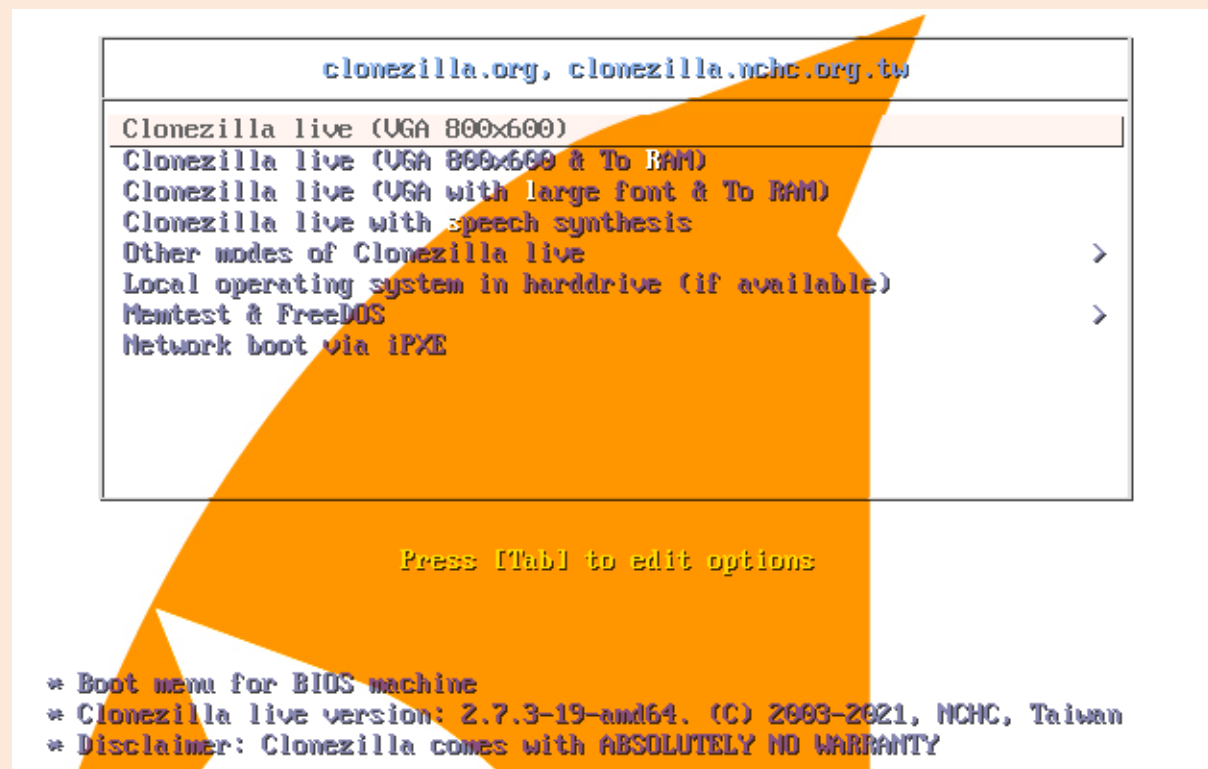


Une fois la machine démarrée, nous allons procéder à la création d'image pour cela il faudra répondre aux différentes questions.

Okan

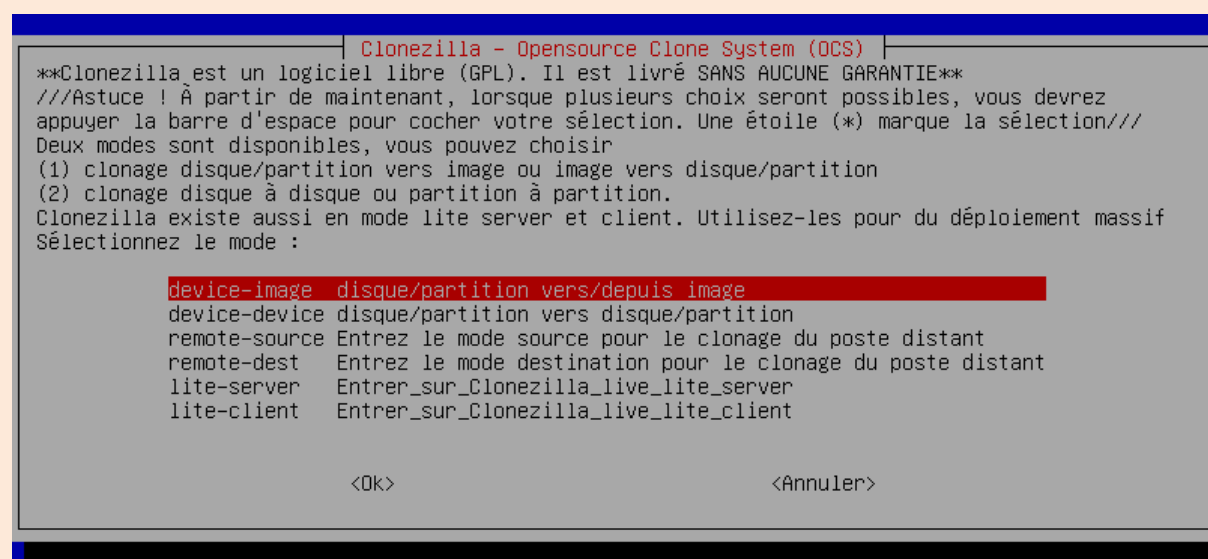
SI02

Cliquons sur le premier choix.



Par la suite, nous choisissons le français et lançons clonezilla.

Ici, nous allons choisir le premier choix, soit « device-image »



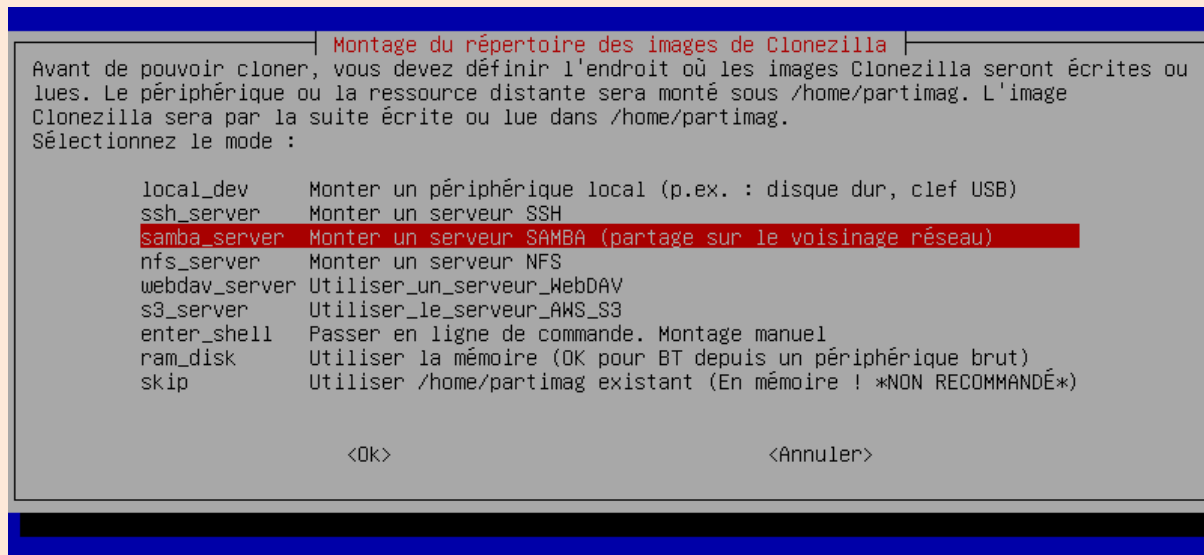
DONNEZ

Documentation Samba, NFS, CloneZilla et SSH avec échange de clés

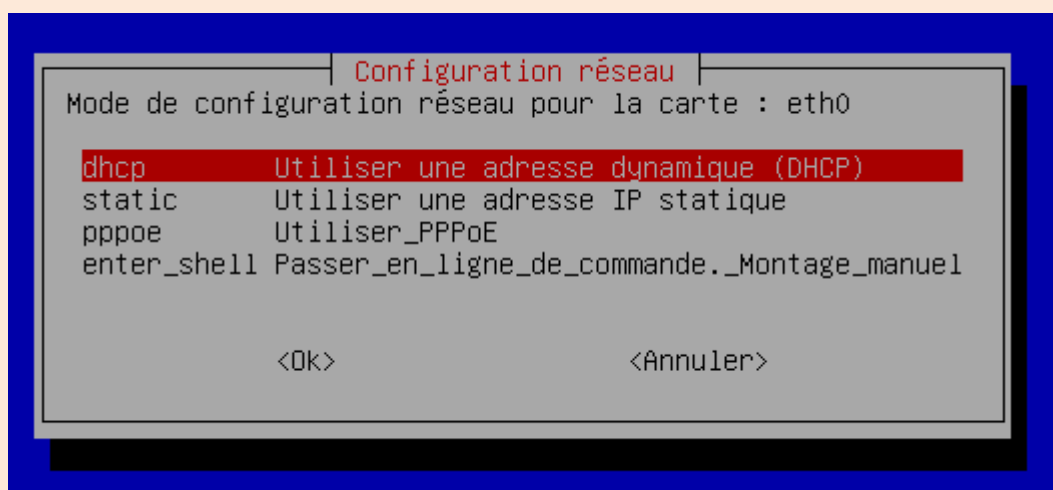
Okan

SI02

Ensuite, nous allons donc créer l'image à partir du serveur samba, pour cela nous choisissons le serveur samba parmi les choix :



Si le serveur DHCP est activé sur virtual box, nous pouvons choisir le premier choix.



Nous renseignons l'ip de notre serveur.

Juste après nous devons renseigner le répertoire dans lequel l'image clonezilla sera écrite soit le répertoire partimag donc on y tape : /partimag.

DONNEZ [Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

Attention de mettre les droits sur le répertoire partimag avec la commande :

Chmod 777 /home/partimag

Dés à présent, nous allons créer un nouvel utilisateur, et modifier le fichier de configuration smb.conf afin de donner que les droits à ce nouvel utilisateur en rajoutant une ligne telle que : valid users = [nouvel utilisateur].

Pour créer ce nouvel utilisateur, on va exécuter la commande :

useradd

Nous allons maintenant booter sur la machine virtuelle que nous avons créer tout au début soit tc avec l'ISO clonezilla.

4) Qu'est-ce que SSH avec échange de clés ?

SSH, ou Secure Shell, est un protocole de communication sécurisé largement utilisé pour accéder à distance à des systèmes informatiques et pour transférer des données de manière sécurisée sur un réseau. Lorsqu'on parle de "SSH avec échange de clés", cela fait référence à une méthode d'authentification et de chiffrement spécifique utilisée dans le protocole SSH pour sécuriser les communications.

Voici comment fonctionne SSH avec échange de clés :

Génération des paires de clés : Dans un système SSH avec échange de clés, deux clés cryptographiques sont générées, une clé privée et une clé publique, pour chaque utilisateur ou entité (par exemple, un serveur). La clé privée doit être conservée de manière sécurisée, tandis que la clé publique peut être partagée librement.

Distribution de la clé publique : La clé publique est distribuée aux systèmes avec lesquels l'utilisateur souhaite se connecter de manière sécurisée. Par exemple, un utilisateur peut copier sa clé publique sur un serveur distant.

Authentification : Lorsqu'un utilisateur tente de se connecter à un système distant via SSH, le système distant demande à l'utilisateur de prouver son identité en utilisant sa clé privée correspondant à la clé publique stockée sur le serveur. Pour cela, l'utilisateur doit présenter sa clé privée au client SSH.

Vérification de l'authenticité : Le serveur distant vérifie que la clé privée présentée par l'utilisateur correspond à la clé publique stockée sur le serveur. Si la vérification est réussie, l'utilisateur est authentifié et la communication continue de manière sécurisée.

Chiffrement de la communication : Une fois l'authentification réussie, SSH chiffre toutes les données échangées entre le client et le serveur, ce qui garantit la confidentialité et l'intégrité des données pendant la session.

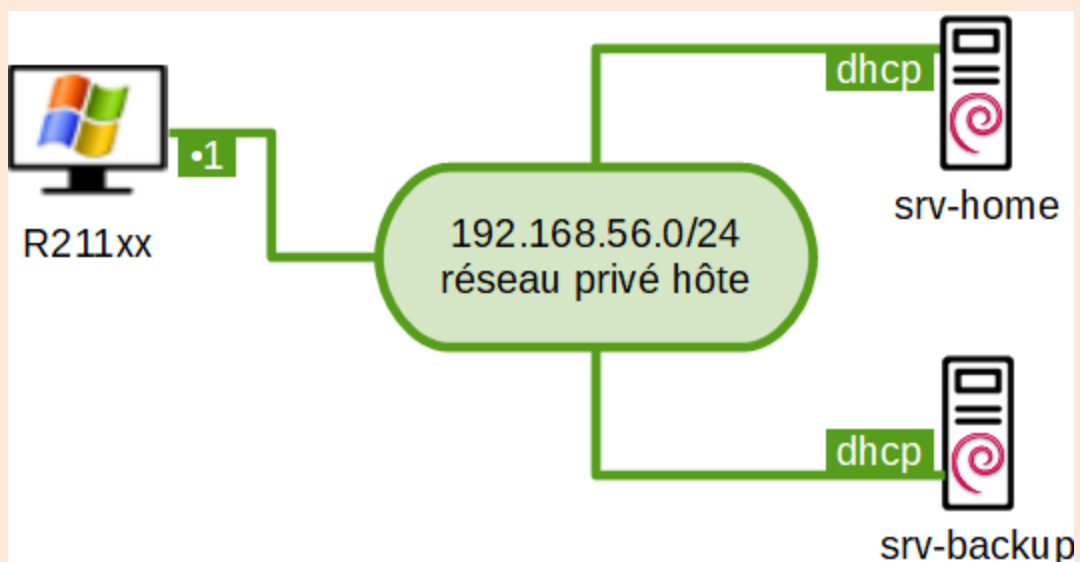
4.1) Installation de SSH avec échange de clés

Tout d'abord, nous allons installer ssh sur srv-home en exécutant la commande :

```
apt install openssh-server
```

4.2) Mise en pratique de SSH avec échange de clés

Schéma de notre réseau :



Srv-home : 192.168.58.101

Srv-backup : 192.168.56.102

Sur srv-backup : On exécute la commande : `ssh-keygen`, qui va nous générer une clé ssh.

DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

On veut connaître la clé publique associée à la paire de clé, pour cela on exécute la commande :

ssh-keygen -lf .ssh/id_rsa

```
root@buster:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/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:CXHEnEsgqcPMcUpXSP/+gd63r2MSP5+ZtD6ftnCw92I root@buster
The key's randomart image is:
+---[RSA 2048]---+
| .ooo.o=o.      |
| +oo. o=       |
| = =. . . .    |
| B . . . .     |
| . . S         |
| . . . . .     |
|   o .+o + .   |
| . ooo=o.oE.   |
| . o*xO=o ..   |
+----[SHA256]-----+
root@buster:~# ssh-keygen -lf .ssh/id_rsa
2048 SHA256:CXHEnEsgqcPMcUpXSP/+gd63r2MSP5+ZtD6ftnCw92I root@buster (RSA)
```

Ici, le « -lf » signifie lister fichier.

On va maintenant copier la clé publique sur srv-home.

```
root@buster:~# 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 SHA256:1a1SF7cp1rfDvnKihS6paTIEVrhkBevuGL+x/NhG38k.
Are you sure you want to continue connecting (yes/no)? yes
/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: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to i
all 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.

root@buster:~#
```

DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

Puis, on se connecte en exécutant la commande :

```
ssh sio@192.168.56.101
```

```
root@buster:~# ssh sio@192.168.56.101
Linux buster 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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.

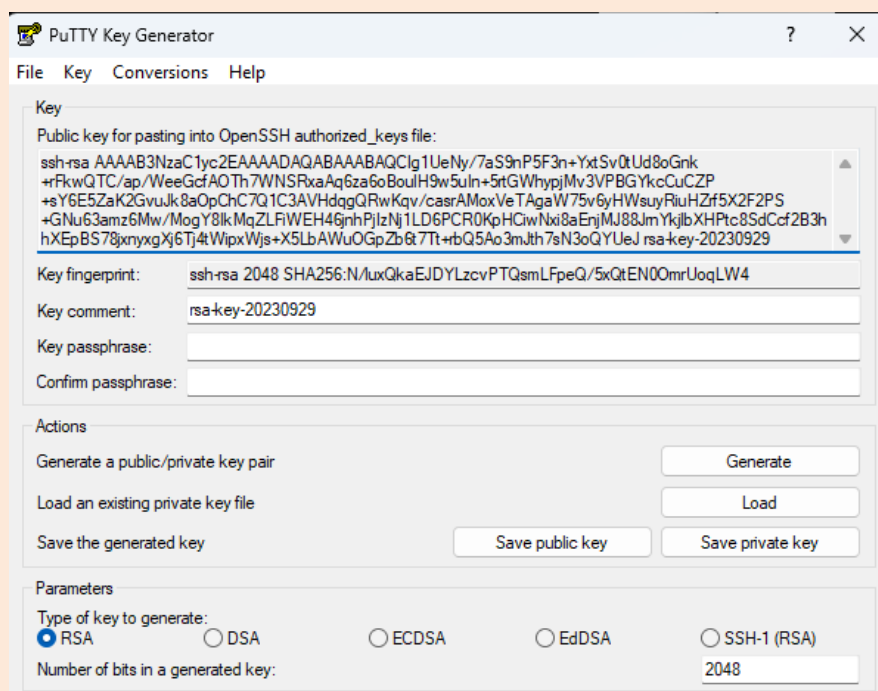
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  7 14:13:42 2020
sio@buster:~$
```

Nous voilà connecté en ssh avec échange de clé sur srv-home à partir de srv-backup sans mot de passe.

Nous allons générer des clés pour se connecter via Putty avec SSH.

Pour cela, il faut tout d'abord aller sur « Putty Key Generator ».

Puis, on génère une clé publique ainsi qu'une clé privée qu'on enregistre sur notre poste.



DONNEZ [Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

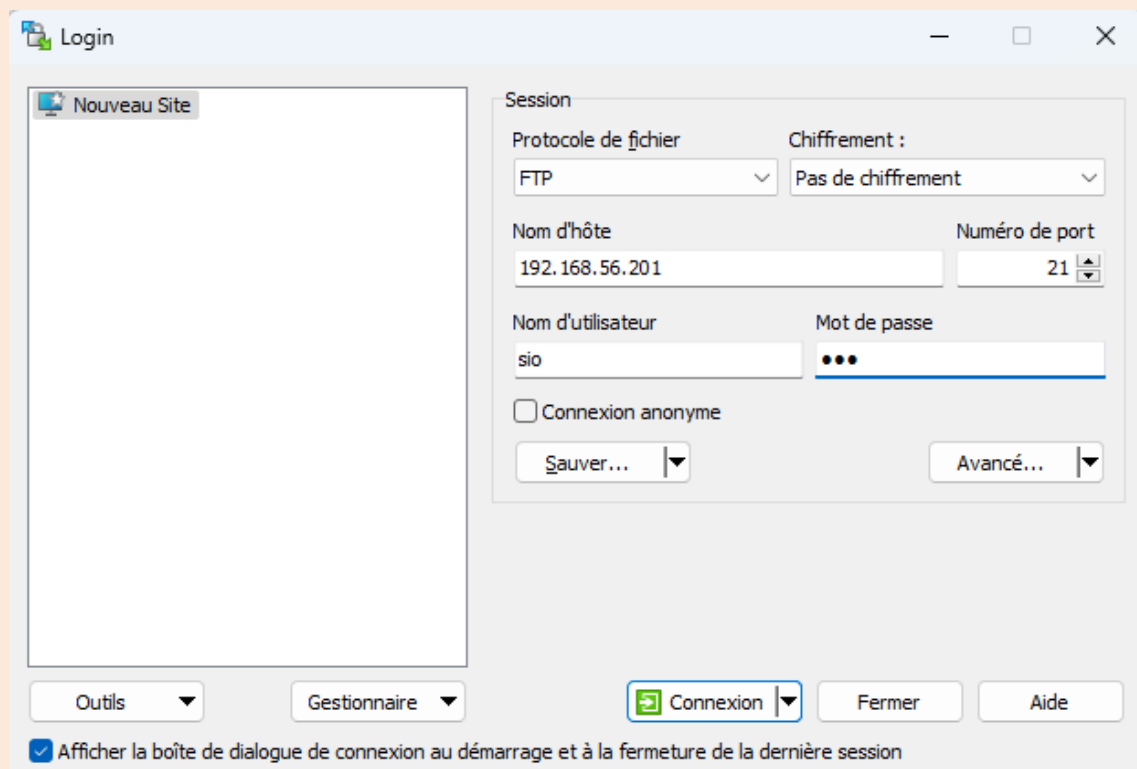
SIO2

On va maintenant se connecter en sio/sio sur srv-home.

Et nous allons exécuter la commande ssh-keygen.

```
sio@buster:/$ 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:pQHRV46gFrg/Ix3SD+JQ2Vs4VashFEfNeju7kPTGAzI sio@buster
The key's randomart image is:
+----[RSA 2048]-----+
|  .*=++...          |
| .. =0.++          |
|  =+000+ .         |
|  =.*.0*.          |
| . +E*S. .         |
| . o 0+ =0         |
|  o o +0 =0        |
|   . 0..          |
| ..               |
+----[SHA256]-----+
sio@buster:/$
```

Nous allons nous connecter en FTP via WinSCP sur srv-home.



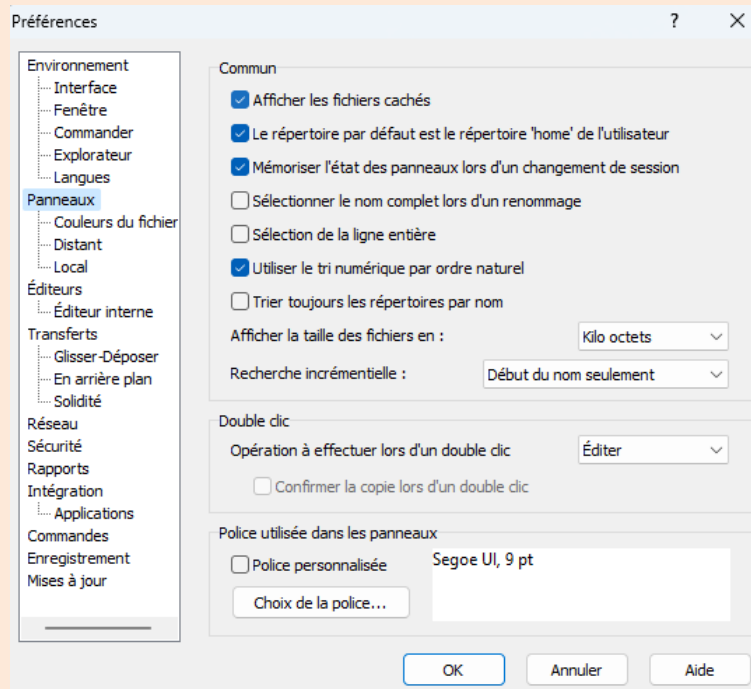
DONMEZ

[Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

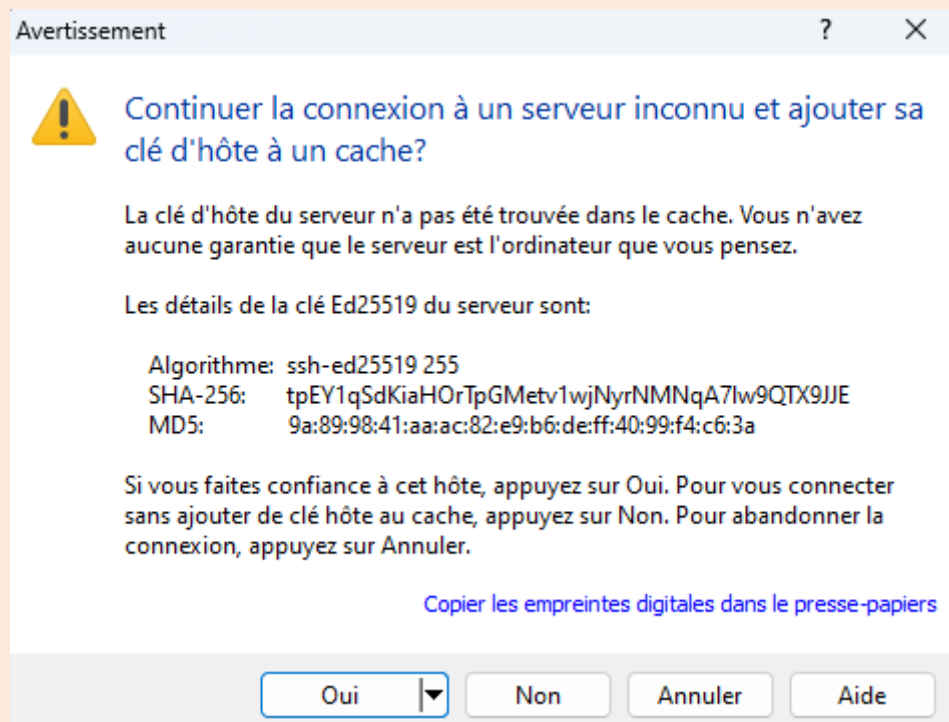
Okan

SI02

En allant dans outils nous allons cocher « Afficher les fichiers cachés ».



Nous allons pouvoir nous connecter.



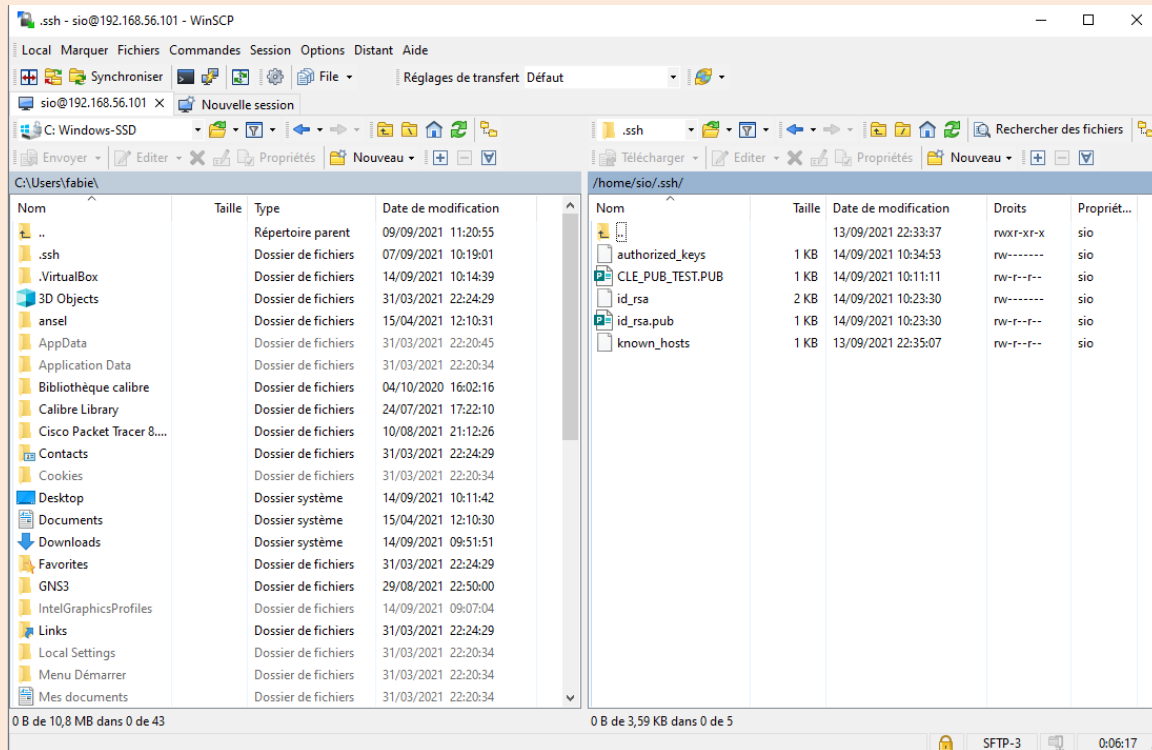
DONMEZ

Documentation Samba, NFS, CloneZilla et SSH avec échange de clés

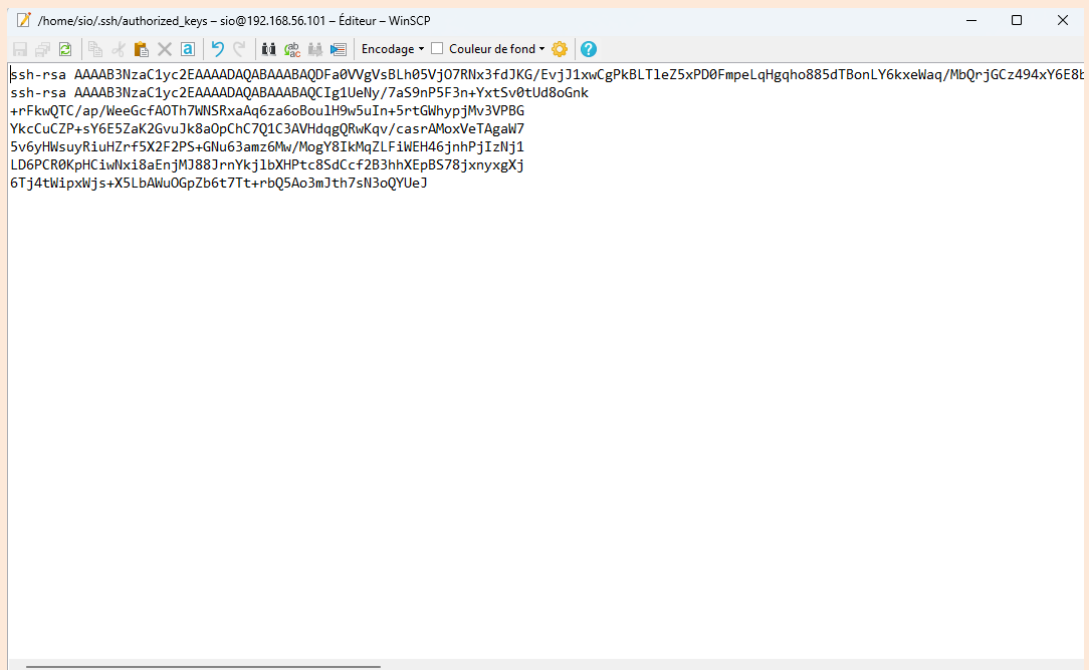
Okan

SIO2

Il faut copier la clé publique de la machine Windows pour la coller dans srv-home dans le répertoire /home/sio/.ssh.



Nous allons copier la clé publique de la machine Windows dans le fichier authorization key :



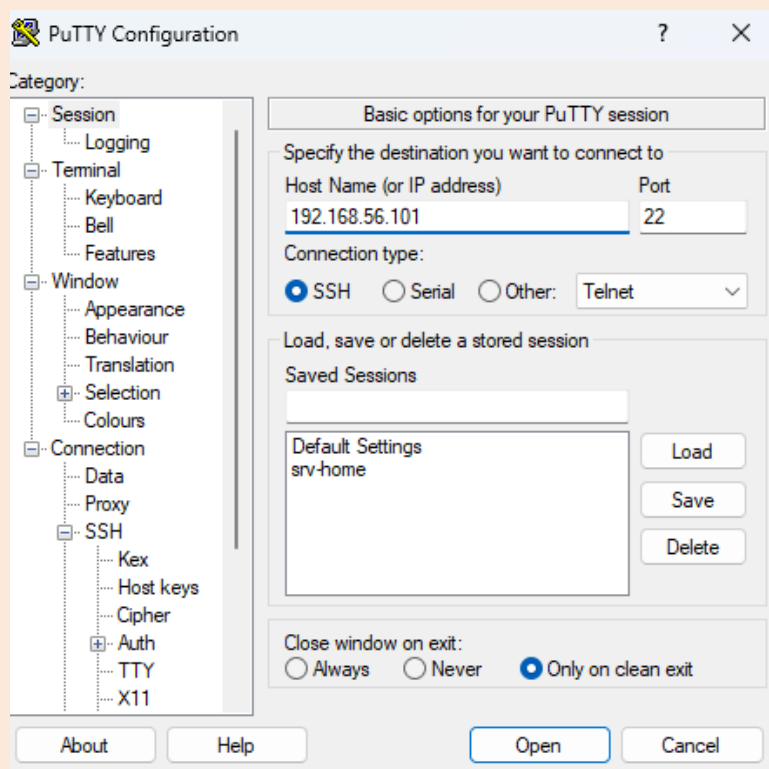
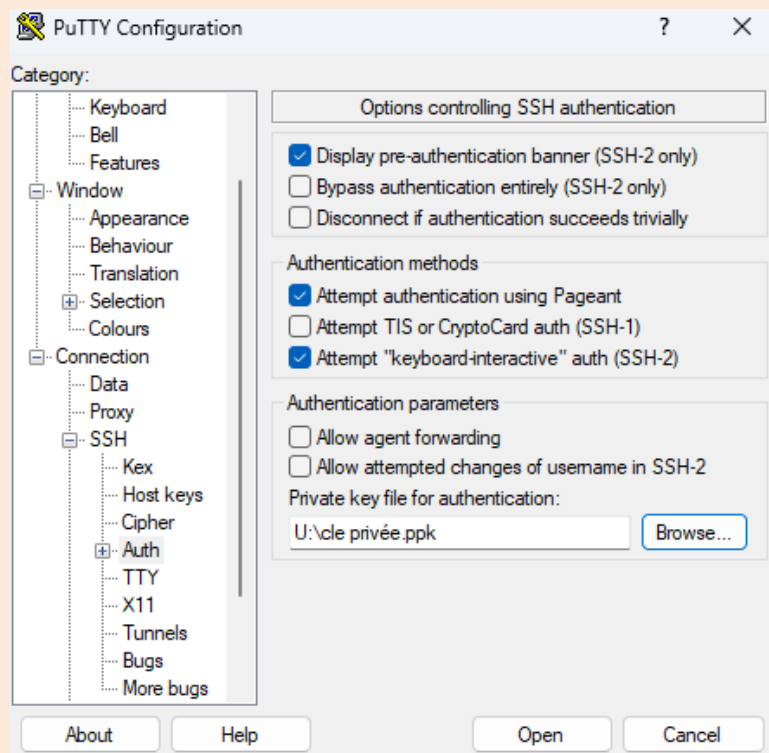
DONMEZ

Documentation Samba, NFS, CloneZilla et SSH avec échange de clés

Okan

SIO2

On va se connecter avec PuTTY en y mettant la clé privée enregistrée tout à l'heure.

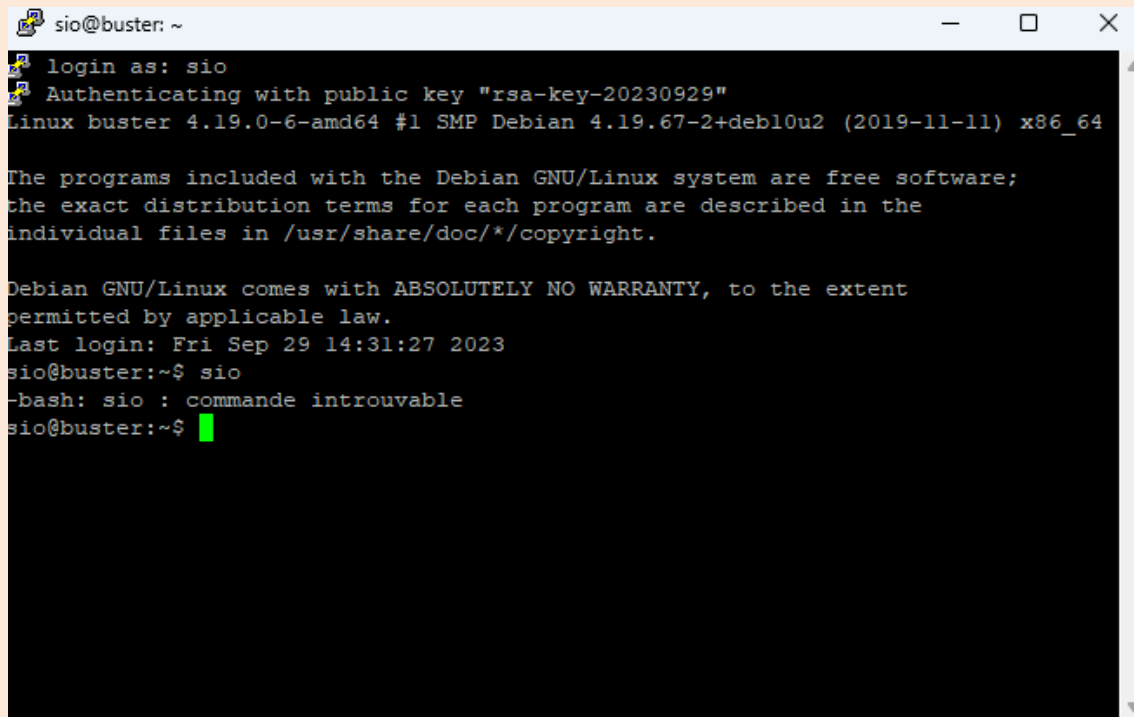


DONMEZ [Documentation Samba, NFS, CloneZilla et SSH avec échange de clés](#)

Okan

SIO2

Et on peut se connecter sans mot de passe !



```
sio@buster: ~  
login as: sio  
Authenticating with public key "rsa-key-20230929"  
Linux buster 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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 Sep 29 14:31:27 2023  
sio@buster:~$ sio  
-bash: sio : commande introuvable  
sio@buster:~$
```