TP– Admin à distance: SSH

Ladriere Valentine

Installation du serveur SSH Debian

Vérifier que SSH n'est pas déjà installé avec which ssh

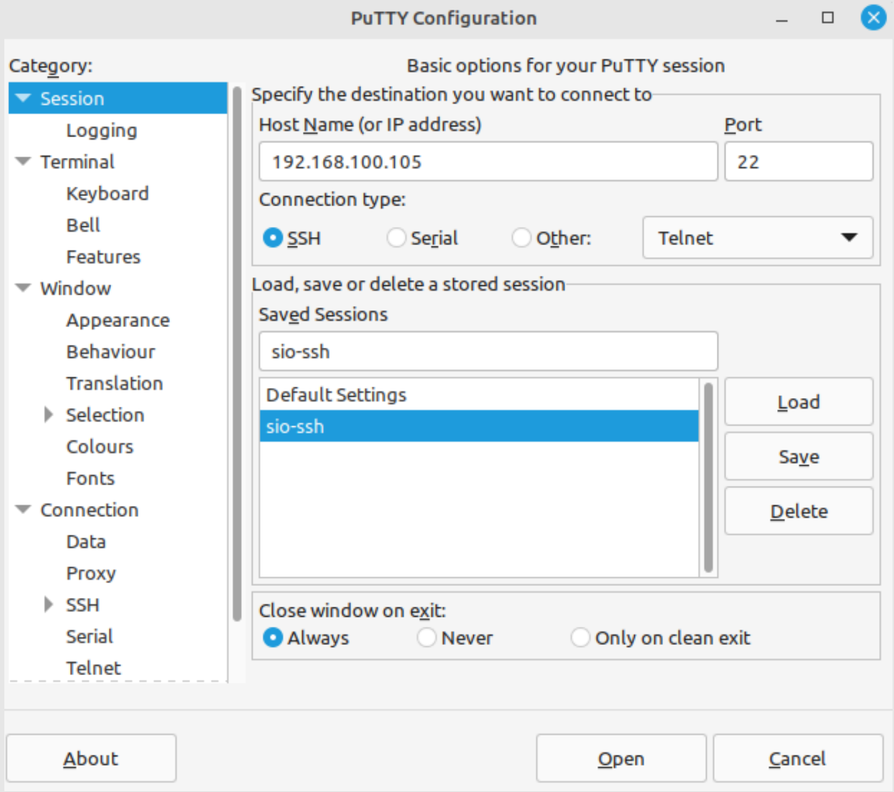
```
root@LADRIERESSH:~# which ssh
/usr/bin/ssh
```

Installer le paquet ssh

```
root@LADRIERESSH:~# apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
openssh-server is already the newest version (1:9.2p1-2+deb12u3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Configuration d'une connexion SSH sous Windows10

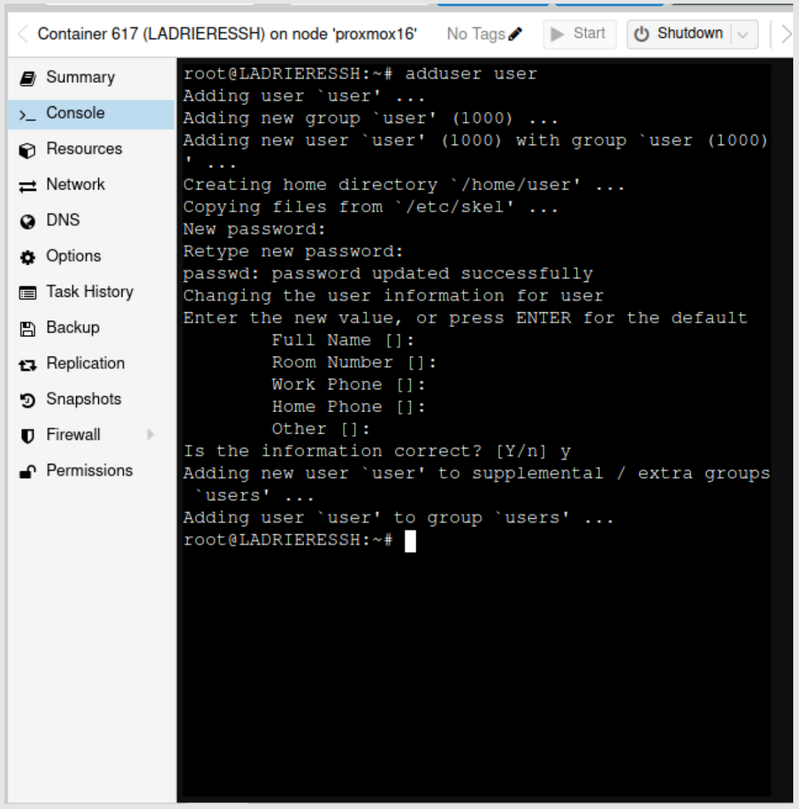
Je lance putty sur ma machine

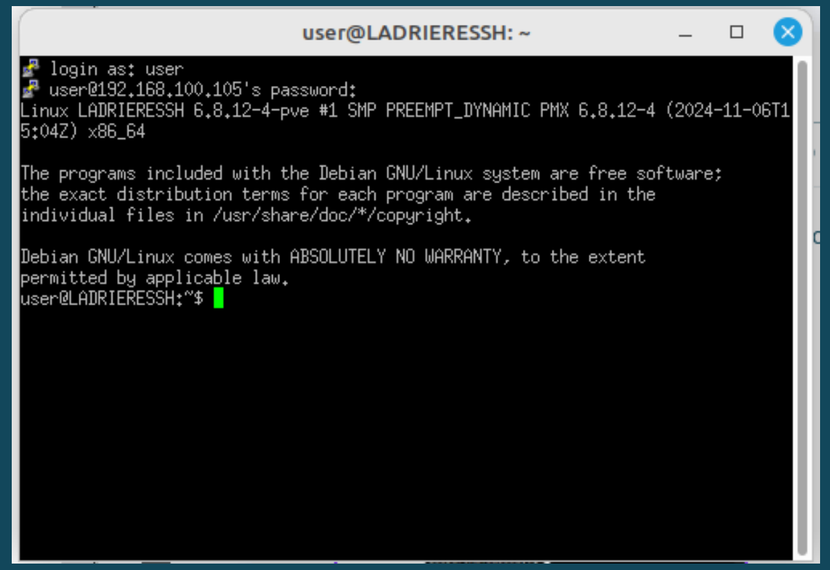


Je crée un "preset" en rentrant d'abord l'adresse ip de mon serveur ssh, j'indique ensuite un nom dans "Saved Sessions" puis je clique sur "Save" pour sauvegarder le preset. Quand je voudrais accéder à mon serveur via putty j'aurai juste à cliquer sur le preset en dessous de "Default Settings"

Configuration d'une connexion SSH sous Windows10

Je crée un user pour pouvoir me connecter sous le login user dans la console sur proxmox





J'ouvre ma session putty et saisis les login que j'ai saisi dans la configuration de l'utilisateur sur proxmox

Configuration d’une connexion SSH sous Windows10

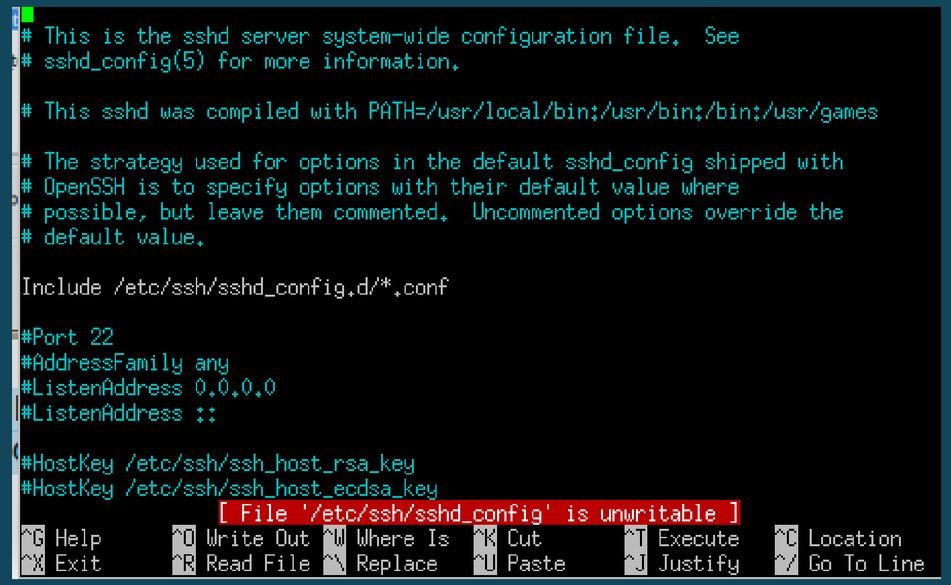
Pouvez-vous afficher le fichier etc/ssh/sshd_config ? Le modifier ?

J’execute cat etc/ssh/sshd_config, cela m’affiche des lignes:

```
user@LADRIERESSH:~$ cat /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
```

Pour le modifier il faudra l’éxecuter avec un éditeur de fichier, faites:

“nano /etc/ssh/sshd_config”



Vous ne pourrez pas écrire dans le fichier car vous n’avez pas les droits. Le fichier /etc/ssh/sshd_config est un fichier de configuration système qui contrôle le comportement du serveur SSH. Seuls les utilisateurs privilégiés (comme root) peuvent le

Configuration et sécurisation d'un serveur SSH et d'un client Debian

```
root@LADRIERESSH:~# nano /etc/ssh/sshd_config
```

```
  GNU nano 7.2                        /etc/ssh/sshd_config *

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::


^G Help          ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit          ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

Redémarrer ensuite le service SSH : service ssh restart

```
root@LADRIERESSH:~# service ssh restart
```

Je me connecte maintenant à mon serveur:

Je peux me connecter sans problème

Configuration et sécurisation d'un serveur SSH et d'un client Debian

Que faut-il faire pour établir une connexion au serveur?

Si l'on se reconnecte immédiatement, les modifications ne seront pas encore prises en compte. Cependant, après un redémarrage de la machine, le port aura officiellement changé.

Quel est l'intérêt d'un changement de port ?

Changer de port permet de savoir qu'il ne s'agit pas d'un SSH car le port 22 est souvent associé au SSH

Configuration et sécurisation d'un serveur SSH et d'un client Debian

PermitRootLogin no|yes|without-password:
PermitRootLogin: Définit si oui ou non le super-utilisateur Root a l'autorisation de se connecter par ssh.

PermitEmptyPasswords Définit si le serveur accepte la connexion à un compte
utilisateur ne possédant pas de mot de passe

Gérer l'accès root :

- Modifier PermitRootLogin no pour interdire la connexion root.

Interdire les mots de passe vides :

- PermitEmptyPasswords no

Pourquoi est-ce que la permission donnée (ou pas) à root est-elle importante à maitriser ?

Réduction des risques d'attaques
Meilleure traçabilité des actions

Gérer les clés d'authentification sur le serveur et le client

Après avoir remis la configuration du port 22:

```
root@LADRIERESSH:~# groupadd etudiant
root@LADRIERESSH:~# groupadd ssh
```

Créer les utilisateurs:

adduser user1

adduser user2

adduser user3

Les mettre dans les groupes:

```
root@LADRIERESSH:~# usermod -aG etudiant user1
root@LADRIERESSH:~# usermod -aG ssh user1
root@LADRIERESSH:~# usermod -aG ssh user2
root@LADRIERESSH:~# usermod -aG etudiant user3
```

Mettre un utilisateur existant dans un groupe existant:

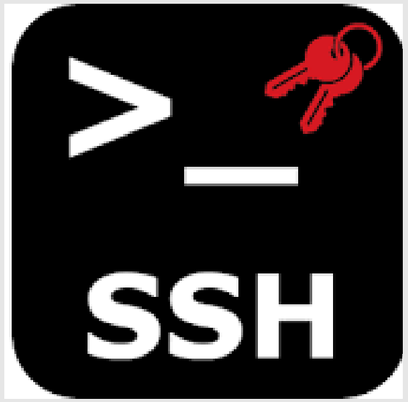
- usermod → Modifie un utilisateur.
- -aG → Ajoute (-a) l'utilisateur à un groupe secondaire (-G).
- etudiant/ssh → Nom du groupe existant.
- user1 → Nom de l'utilisateur existant.

Changer les mots de passe des users:

```
root@LADRIERESSH:~# chpasswd
user1:Password1
user2:Password1
user3:Password1
root@LADRIERESSH:~#
```

Faites CTRL + D à la fin du processus

Gérer l’échange des clés publiques



Clé SSH: une clé SSH est un identifiant d’accès pour le protocole réseau SSH (Secure Shell). Ce protocole réseau sécurisé authentifié et chiffré est utilisé pour la communication à distance entre des machines sur un réseau ouvert non sécurisé

Gérer l’échange des clés publiques

Créer des clés d’authentification:
créer un répertoire .ssh pour chaque utilisateur pour pouvoir générer nos clés dans ce dossier.

Pour créer ces dossiers: connectez vous a chaque utilisateur et dirigez vous dans le répertoire avec la commande cd /home/nomuser

Une fois dans ce dossier créer un dossier .ssh avec la commande mkdir .ssh

Pour l’utilisateur root il faut d’abord créer un dossier home puis ensuite un dossier .ssh

```
login as: user1
user1@192.168.100.105's password:
Linux LADRIERESSH 6.8.12-4-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-4 (2024-11-06T1
5:04Z) 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.
user1@LADRIERESSH:~$ mkdir .ssh
user1@LADRIERESSH:~$ cd /home/user1/.ssh
user1@LADRIERESSH:~/.ssh$
```

Répétez ceci pour tous les users

```
root@LADRIERESSH:~# mkdir home
root@LADRIERESSH:~# cd /home
root@LADRIERESSH:/home# mkdir .ssh
root@LADRIERESSH:/home# cd /home/.ssh
root@LADRIERESSH:/home/.ssh#
```

Gérer l’échange des clés publiques

Donner des droits d’accées au fichier avec la commande chmod 0770 /home/nomuser/.ssh pour chaque utilisateur:

```
root@LADRIERESSH:~# chmod 0770 /home/user1/.ssh
root@LADRIERESSH:~# chmod 0770 /home/user2/.ssh
root@LADRIERESSH:~# chmod 0770 /home/user3/.ssh
root@LADRIERESSH:~# chmod 0770 /home/.ssh
```

Maintenant il faut que vous générer vos clés pour chaque utilisateur à l’aide de la commande “ssh-keygen -t dsa -f /home/nomuser/.ssh/id_dsa”
Entrez une passphrase en respectant les normes de complexité d’un mot de passe (12 caractères minium, caractères spéciaux, lettres , chiffres)

```
root@LADRIERESSH:~# ssh-keygen -t dsa -f /home/user1/.ssh/id_dsa
Generating public/private dsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user1/.ssh/id_dsa
Your public key has been saved in /home/user1/.ssh/id_dsa.pub
The key fingerprint is:
SHA256:fuiGA+mm6UHVjwwvAHuKckIg61LBaGqIqSJwtwRjfAI root@LADRIERESSH
The key's randomart image is:
+---[DSA 1024]----+
|E=.              |
|+=B...           |
|B++=o .          |
|X=.oo+ o         |
|Xooo.o+ S        |
|*+  +. . .       |
|o .. . .o .      |
|   oo o...       |
| .+o   o.        |
+----[SHA256]-----+
```

Répétez ce processus pour chaque utilisateur

Les deux clés sont bien là:
Il y en a deux car il y en a une publique et une privée
La clé publique sert à s’identifier sur le serveur.

```
user1@LADRIERESSH:~$ ls -l ~/ .ssh/
.ssh/:
total 8
-rw------- 1 root root 1438 Mar  3 14:02 id_dsa
-rw-r--r-- 1 root root  606 Mar  3 14:02 id_dsa.pub

/home/user1/:
total 0
```

Gérer l’échange des clés publiques

Envoyez une clé publique au serveur pour qu’il puisse nous identifier à l’aide la commande “ssh-copy-id -i ~/.ssh/id_dsa.pub root@adresseIPserveurSSH”.

Si cela ne fonctionne pas, suivez ces étapes:
vérifiez les droits sur .ssh : ls -ld ~/.ssh

Si vous voyez quelque chose comme :
drwx------ 2 root root 4096 Mar 3 10:00 /home/user1/.ssh
Cela signifie que .ssh appartient à root, ce qui empêche user1 d'accéder à ses propres clés.
Corrigez cela :
chown user1:user1 /home/user1/.ssh chmod 700 /home/user1/.ssh

Sur le client

```
user1@LADRIERESSH:~$ ls -l ~/ .ssh/id_dsa
-rw------- 1 root  root  1438 Mar  3 14:02 .ssh/id_dsa

/home/user1/:
total 0
```

Sur le serveur

```
root@LADRIERESSH:~# chown user1:user1 /home/user1/.ssh/id_dsa
root@LADRIERESSH:~# chmod 600 /home/user1/.ssh/id_dsa
```

Sur le client

```
user1@LADRIERESSH:~$ ls -l ~/ .ssh/id_dsa
-rw------- 1 user1 user1 1438 Mar  3 14:02 .ssh/id_dsa
```

Sur le client on peut enfin envoyer la clé

```
user1@LADRIERESSH:~$ ssh-copy-id -i ~/.ssh/id_dsa.pub user1@192.168.100.105
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user1/.ssh/id_dsa.pub"
The authenticity of host '192.168.100.105 (192.168.100.105)' can't be established.
ED25519 key fingerprint is SHA256:yUL0qYv5FFYn5z4UMISjinHURSAbfX1JS7Kf5ll6Ftc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are al
ready installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to ins
tall the new keys
user1@192.168.100.105's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'user1@192.168.100.105'"
and check to make sure that only the key(s) you wanted were added.
```

Répétez le processus pour chaque user

Gérer l’échange des clés publiques

Quelles clés se trouvent dans le dossier authorized_keys?
Ouvrez ses fichiers:
Déplacez vous dans le fichier .ssh
“ cd /home/nomutilisateur/.ssh”
En faisant un ls, nous pouvons voir qu’il y a plusieurs fichiers

```
root@LADRIERESSH:/home/user1/.ssh# ls
authorized_keys  id_dsa  id_dsa.pub  known_hosts  known_hosts.old
```

Ouvrez le fichier known_hosts : “cat known_hosts”
Dans ce fichier on peut retrouver la clé publique de tous les serveurs SSH sur lesquels ce compte s’est connecté.

```
root@LADRIERESSH:~# cd /home/user1/.ssh
root@LADRIERESSH:/home/user1/.ssh# cat known_hosts
|1|xtXvT6+1uFmYZQftwqJE4mGaNLs=|VyIyu57N6g8XUBC0C73qEbKA9/0= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIzU7
UoQ1r0wv8f5lh3IfusKAKLL201Q5waOvtaxz
|1|EwfNvtKLHqnup+YaD7tK2VKfWZk=|Pb7iOWt6ybSk6VaIkI3j90RyQc4= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDAY
Ox/PqBRQPGUAfA0I6SXnfoZlg8HbdtjYcBk3tMkgTOVxIYwO4k1VN/4wwQXL6Ud0cA61G4T/SZy/nzXJfZnvXGXkuf/d0tTFy9B/Bt
myZDUeo8BmDUqtSM9D7k1kIQw291/mTzeVLOQQk5Z6kz+hDWGCaFUJ14Y9ayW4qpgmo51Mo0MrTrGDDjaEEOdkXoJGOuyXkC6DAit1
sqNoZbj90q8XY5UrG5ybMRRToC6xDe0VS0EaEDrbbHsKPPSatr3oau2MhEvh1fL+udVqBBchwr81tDKWdxdaJnIzrAZV89nNEXYXS6
EfzmhlDfbxK791hXmaioMhIDbNJXLzvh3+EV2gNdNShbE3jowZXNYLu36frE1VXrJEdOEPf1jKL9nCY0aP7nguNac05rh6D7TmEcoW
HAJrd6C2kP6LsC5tCJo/CcmKNP+sCImuHCcw53JaA9Ey25PwfT8y5cAOj5G/2Je+za8TbpKjU6VibIZLYVMau6E=
|1|hvqEHAZqNGSqoBMISaOM1Be63v0=|Q+hcS+Q2LqBqeFsljsA5/Rxrvp4= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItb
dHAyNTYAAAAIbmlzdHAyNTYAAABBBG1XD0hQL6wAIIDg0EKn+5grDAALrOUVg/OciK8rCJp5p5hDsDX+RrgOBa740Ekh27IVUQRgly
EJknH63DoE=
```

Dans le fichier id_dsa on peut y retrouver la clé privée

```
root@LADRIERESSH:/home/user1/.ssh# cat id_dsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAdJTIiVT
No17VKOE5c4kItAAAAEAAAAAEAAAGyAAAAB3NzaC1kc3MAAACBAPSfMjvmeLPwpsFD6NpS
bgM8nqvfSXA1+1hya1yCg9O2SaUJt1CjOAxCJ4iMWWyyatHi0M0GMnygwoU2aAtRjTnpyh
cxse6uQois+rLhXQb0Nc9OejsdspqG6bRgQiZa0L9StOV301mR9YyRYT/iTse4q8C/KO8P
jvOkwUyGqcpRAAAAFQDgj027f8zW1CGbjjXdONZ1qDMDLQAAAIEAvxgKtM1oNQyH5vix5Y
dCBWpAOFQxd25XqYciZee7HkHx0E7FInYJSC4b2M0HLB00byYrQpOfg3bfypomcp1wxbKg
5J196p7gGcERG1gKf3xbeqKOv8WPT4E0hBicadxzpFPq/tmUWidpEBKOvRbHCviGWwY7MX
ec1iODrPxYLjEAAACAdQM66OegurZINrYs4YMjIO/cdYo+pOAVI8CPxSGIOzLr//HVgpT+
OUSuzmqgIF2SLQawwej8HNdJkLTa5D0ezGTEFcWgk1siYGo1NsVbNriJW+zx5D+eX1LXx5
IkkLKbpOpU45C58Yag7DCftd76+rHIKFAur8oDw7QJEivzOgYAAAHw81IMRYHZ/qZQrZ4U
JqG75QNS1qXxcIgDqHoHl9dvz5WMbeg1EA1/dcmYPWyK7iE7Jgxzxv02ucd2PxPHozYSw0
bfxLlid7jna8QKxY1aUu8rRl47Hrc5As3gSqulsAecvbs1B1yBRePPP3W7olaWiwcUpDEp
yLVfA8y9ccDvFubKe6UOoIobZ21/CuzEPsUGb5sD9e2L99bLMQ6K824wR8t5yggplF8U8P
Q2dRWw8afyk0R9wk00s5nuKOd5cZm4k2wpV3utaoefDJqgR3lpY74NbI45LyWJoTnfSzZV
mYLd1D1/PEbz45MuyENo3uGFJkH0gpb2djfR7FyAwdytxJxtGaCOJ3Iu/NgZ8je7s/9uvG
CXAsagg+M40sj1z3CJRiVRXAZPj5c8YPe2AK6lGz9pXtU4KxY6ls2vvHjgqxAHl9a4WK33
2xT4u9vDBuQaCfxttQwYbc65CnZ6SmiariCUyTK6nyGCnLDqH9bU9cdAPpmzsW+N8hHEdG
6nBm/4irvr68gDzgt4PjoyeVT0sOYGskAchetnYYv+FKemlmPLC/2kBVoiNWPg1HgAwW+L
5tIuRTTwbb3DnveGgL8/3DrIbuOIsUqK1Bqj+8mWX6juFqIo0XpMRbaYo7b8s74yp+F5Gv
mCK6Faq51xsYVuOg==
-----END OPENSSH PRIVATE KEY-----
```

Gérer l'échange des clés publiques

Dans le fichier id_dsa.pub on peut y retrouver la clé publique qui sera ajouté au fichier authorized_keys

```
root@LADRIERESSH:/home/user1/.ssh# cat id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBAPSfMjvmeLPwpsFD6NpSbgM8nqvfSXA1+1hya1yCg9O2SaUJt1CjOAxCJ4iMWWyyatHi0M0GMnygw
oU2aAtRjTnpyhcxse6uQois+rLhXQb0Nc9OejsdspqG6bRgQiZa0L9StOV30lmR9YyRYT/iTse4q8C/KO8PjvOkwUyGqcpRAAAAFQDgj0
27f8zWlCGbjjXdONZ1qDMDLQAAAIEAvxgKtMloNQyH5vix5YdCBWpAOFQxd25XqYciZee7HkHx0E7FInYJSC4b2M0HLB00byYrQpOfg3b
fypomcp1wxbKg5J196p7gGcERG1gKf3xbeqKOv8WPT4E0hBicadxzpFPq/tmUWidpEBKOvRbHCviGWwY7MXec1iODrPxYLjEAAACAdQM6
6OegurZINrYs4YMjIO/cdYo+pOAVI8CPxSGIOzLr//HVgpT+OUSuzmqgIF2SLQawwej8HNdJkLTa5D0ezGTEFcWgk1siYGo1NsVbNriJW
+zx5D+eX1LXx5IkkLKbpOpU45C58Yag7DCftd76+rHIKFAur8oDw7QJEivzOgY= root@LADRIERESSH
```

La clé publique se retrouve dans le fichier authorized_keys car lorsqu'un utilisateur souhaite se connecter au serveur SSH, le serveur vérifie la clé publique fournit par l'utilisateur avec celles présentes dans le fichier authorized_keys.
Si une correspondance est trouvée, l'utilisateur est autorisé à se connecter sans fournir de mot de passe

Tester la connexion au serveur SSH

Pour vous connecter au serveur SSH à distance il suffit d'entrer la commande ssh nomuser@adresseIP –p port

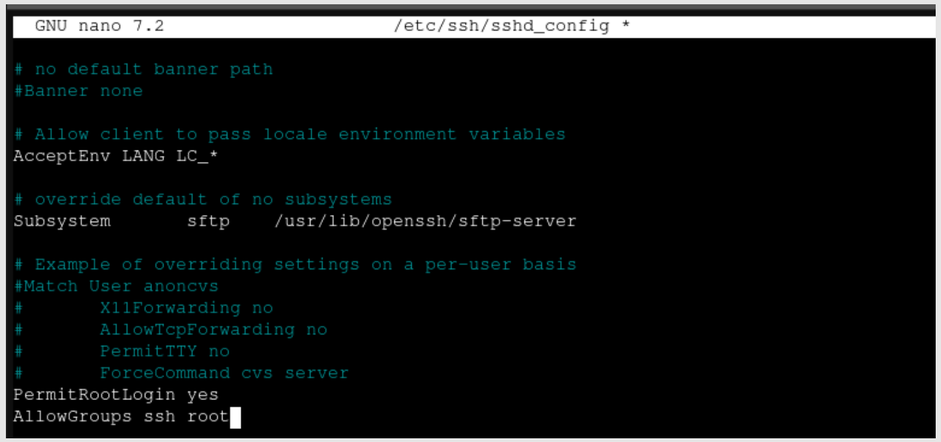
```
user1@LADRIERESSH:~$ ssh user3@192.168.100.105 -p 22
user3@192.168.100.105's password:
Linux LADRIERESSH 6.8.12-4-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-4 (2024-11-06T1
5:04Z) x86_64

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: Mon Mar  3 15:46:02 2025 from 192.168.20.89
```

Pour savoir qui s'est connecté à votre serveur SSH il vous suffit de rentrer la commande who sur votre
serveur et vous aurez l'heure et utilisateur connecter à votre serveur SSH

```
root@LADRIERESSH:~# who
root     tty1         Mar  3 12:42
user1    pts/3        Mar  3 14:49 (192.168.20.89)
user1    pts/4        Mar  3 16:05 (192.168.20.89)
user3    pts/5        Mar  3 16:12 (192.168.100.105)
```

Tester la connexion au serveur SSH

Si vous voulez limiter la connexion de certains utilisateurs sur le serveur SSH, vous devez modifier le fichier de configuration “sshd_config” et ajouter la ligne AllowGroups + nomgroupe ou alors Allowusers + nom users



Quand on essayera de se connecter avec le user3, on aura un accès refusé car il n’est pas autorisé de se connecter au serveur SSH alors que le userl et le user2 seront autorisés à se connecter

Pour savoir qui s’est connecté à votre serveur SSH il vous suffit de rentrer la commande who sur votre serveur et vous aurez l’heure et utilisateur connecter à votre serveur SSH

Connexion avec la clé d’authentification

Pour vous connecter avec la clé d’authentification, vous devez modifier le fichier sshd et basculer la ligne de commande “PasswordAuthentication yes” en “PasswordAuthentication no”.

Cette ligne permet de se connecter au serveur SSH avec un mot de passe ou alors avec la clé en no

Il se peut que cette ligne de commande « bug », si c’est le cas, cela est du à un bug provenant du serveur SSH directement