Tp-SSH

Valentin Drieux

- Installation de ssh
- Connection au ssh depuis une machine client
- Modification du port22 en port 2022.
- Créer un group ssh et etudiant puis 3 user.
- Key ssh

Installation de ssh:

Ecrire la commande #apt install openssh-server. Une fois fait il installe les services SSH.

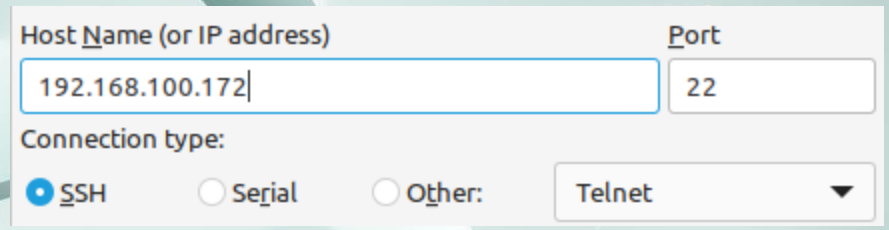
Que vous donne la commande which ssh ?

Cette commande permet de voir l'emplacement de l'exécutable ssh

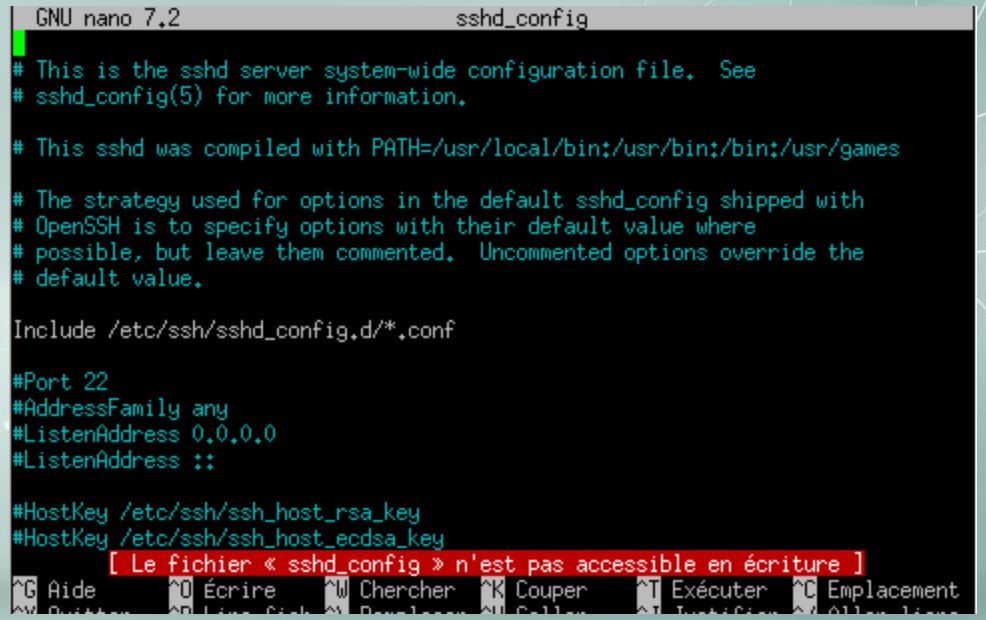
Connection depuis une machine client:

Pour cela il faut créer un user avec la commande #adduser drieux puis mettre un mdp "sio2020".

Ouvrir putty



Une fois connecter en mode client j'accède à l'exécutable sshd_config.



Je ne peux pas le modifier avec le user drieux car il n'a pas le droit

Modification du port22 en port 2022.

```
#Port 22
port 2022
```

Je modifie port 22 en port 2022 puis je restart sshd

La connexion c'effectue avec succè

Pour le voir il suffit de faire la commande #nmap 192.168.100.172

```
Not shown: 999 closed tc
PORT     STATE SERVICE
2022/tcp open  down
```

on remarque que le port 22 et bien remplacer par le port 2022.

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

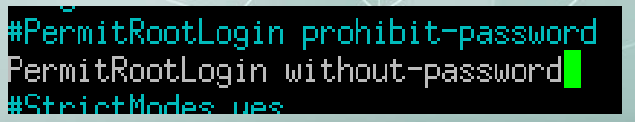
Pour établir une connexion au serveur SSH, il faut que le service SSH est en marche sur le serveur. Générez une paire de clés SSH sur le client, copiez la clé publique sur le serveur.

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

Changer le port SSH réduit les risques d'attaques automatiques en rendant le serveur moins visible pour les scanners de port. Cela augmente la sécurité en évitant le port par défaut (22).

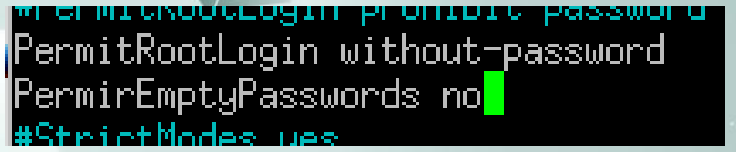
Pourquoi est-ce que la permission donnée (ou pas) à root est-elle importante à maitriser ?

Limiter l'accès à `root` via SSH est importante pour éviter qu'un attaquant n'obtienne un contrôle total du serveur.



Quelle est la différence entre PermitEmptyPasswords no et PermitRootLogin without-password ?

`#PermitEmptyPasswords no` empêche l'accès SSH avec un mot de passe vide, tandis que `#PermitRootLogin without-password` permet à l'utilisateur `root` de se connecter uniquement avec une clé SSH et non un mot de passe.



Créer un group ssh et etudiant puis 3 user.

Les commandes sont :

#addgroup ssh (cette commande permet de créer un group)

#adduser user1 (cette commande permet de créer un user)

#usermode –aG ssh user1 (cette commande permet de mettre user1 dans le groupe ssh

```
root@debiansio:~# chpasswd
user1:sio2025
user2:sio2025
user3:sio2025
```

```
root@debiansio:/home# mkdir .ssh
root@debiansio:/home# chmod 0770 ~/.ssh
```

Généré le fichier .ssh pour pouvoir généré la clé

```
root@debiansio:/home# ssh-keygen -t dsa -f ~/.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 /root/.ssh/id_dsa
Your public key has been saved in /root/.ssh/id_dsa.pub
The key fingerprint is:
SHA256:PN3u/SR2JTfz2EXpsk5ihTlQEeYeePBFzeZRvo+Jp98 root@client
The key's randomart image is:
+---[DSA 1024]----+
|          . =+oo o|
|           B .  *.|
|          o =  o.+|
|         . .+.+ .o.|
|        S .=.o.=+|
|          . .o.oBB|
|            oooB *|
|           ..+= = |
|             ooo.E|
+----[SHA256]-----+
```

Je génère le clé ssh dsa depuis le client

```
root@debiansio:/home/user1# ssh-copy-id -i ~/.ssh/id_dsa.pub root@192.168.100.172
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_dsa.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: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.100.172's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.100.172'"
and check to make sure that only the key(s) you wanted were added.
```

Ensuite, il faut envoyer une clé publique au serveur pour qu'il puisse nous identifier

```
user1@client:~$ ssh root@192.168.100.172
The authenticity of host '192.168.100.172 (192.168.100.172)' can't be established.
ED25519 key fingerprint is SHA256:yKYearKkT1e8uSJuTp2ZwPCSExmnAJB2tXPDSo85f9g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/user1/.ssh/known_hosts).
root@192.168.100.172's password:
Linux debiansio 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) 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 15:10:52 2025 from 192.168.100.61
root@debiansio:~#
```

Grace a cette commande je remarque que je peux me connecter en ssh depuis ma machine client avec une key

Question pour 1 seul utilisateur, user1 par exemple :

Deux fichiers sont générés. Affichez les deux. Y-a-t-il une différence? Est-ce normal et pourquoi ?

La clé Id_dsa est la clé privée, La clé Id_dsa.pub est la clé publique,

```
root@debiansio:~/.ssh# ls
authorized_keys  id_dsa  id_dsa.pub  known_hosts  known_hosts.old
```

Comparez les clés entre elles. Lesquelles se retrouvent dans le fichier (~/.ssh/authorized_keys), et pourquoi ?

```
ssh-dss AAAAB3NzaC1kc3MAAACBAP2KXIJb24O5vlgQ7oUM+i4LgIoBxX0cQBzNiXJEAYe0Kow9so0fbjT2FdmjJ0By1jFHV0D1iax1xVL5VYEWOVSfe6Xr
ssh-dss AAAAB3NzaC1kc3MAAACBAP2KXIJb24O5vlgQ7oUM+i4LgIoBxX0cQBzNiXJEAYe0Kow9so0fbjT2FdmjJ0By1jFHV0D1iax1xVL5VYEWOVSfe6Xr
ssh-dss AAAAB3NzaC1kc3MAAACBANuZHDkaRNS8ogxCtaqWECqodzxBWowWQE/MjKbS343QBJVmKr1SpaOEvPOX087N5QzM2ZWaAi95UHfPd0dR5cVe7RSy
ssh-dss AAAAB3NzaC1kc3MAAACBALUaZ4evu0D+IyMA+QPTrv8wAwNEFAUkZcjyA+hSS+/vKpIm2zphRQkLEqDGBaI2H3JZyLaLLtDh1w1LTi5NwQTqiUlZ
```

La clé Id_dsa est la clé privée, utilisée pour signer les requêtes d'authentification SSH et doit rester protégée sur votre machine. Si quelqu'un y accède, il pourrait se faire passer pour vous. La clé Id_dsa.pub, la clé publique, sert à authentifier l'utilisateur auprès du serveur. Elle peut être librement partagée et est ajoutée dans le fichier `~/.ssh/authorized_keys` sur le serveur, permettant ainsi une connexion sans mot de passe.

Cette image montre que la key fonctionne, pour cela il faut mettre la commande suivante #ssh user1@192.168.100.61

En vous aidant de l’aide ci-dessous, autorisez uniquement les utilisateurs des groupes root et ssh à se connecter. Indiquez ici votre configuration à cet effet:

Pour cela il faut aller dans l'excutable #nano /etc/ssh/sshd_config. Mettre la commande #AllowGroups root ssh et systemctl restart sshd.

Indiquez ici quels tests vous avez pratiqué pour valider votre configuration :

Il faut esseyer de ce connecter avec un user #ssh user1@192.168.100.61

```
#       ForceCommand cvs server
AllowGroups root ssh
PasswordAuthentication yes
```

Passwordauthentication yes permet de faire une authentification juste avec key sans le moindre mdp.