

TP connexion SSH

Date : 17/11/2025

Auteur : Valencelle Luka

Table des matières

1. Préparation du serveur et du client	3
2. Connexion par mot de passe	4
3. Connexion par clé SSH.....	5
4. Transfert de fichiers SCP	6
5. Redirection X11	7

1. Préparation du serveur et du client

J'ai préparé un serveur ubuntu 24.02 sans interface graphique ou j'ai installé openssh-server.

```
ubuntu tp SSH sur DESKTOP-JE7FC55 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:15:5d:01:22:0a brd ff:ff:ff:ff:ff:ff
inet 192.168.1.75/24 metric 100 brd 192.168.1.255 scope global dynamic eth0
valid_lft 86384sec preferred_lft 86384sec
inet6 fe80::215:5dff:fe01:220a/64 scope link
valid_lft forever preferred_lft forever
luka@ubuntu-tpssh:~$ systemctl status openssh-server
Unit openssh-server.service could not be found.
luka@ubuntu-tpssh:~$ sudo systemctl st
start status stop
luka@ubuntu-tpssh:~$ sudo systemctl st
start status stop
luka@ubuntu-tpssh:~$ sudo systemctl status open-
open-iscsi.service open-vm-tools.service
luka@ubuntu-tpssh:~$ sudo systemctl status ssh
[sudo] password for luka:
Sorry, try again.
[sudo] password for luka:
Sorry, try again.
[sudo] password for luka:
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Active: active (running) since Mon 2025-11-17 14:22:13 UTC; 2h 10min ago
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
      man:sshd_config(5)
Process: 1363 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 1365 (sshd)
Tasks: 1 (limit: 2187)
Memory: 6.4M (peak: 7.7M)
CPU: 85ms
CGroup: /system.slice/ssh.service
        └─1365 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

nov. 17 14:22:13 ubuntu-tpssh sshd[1365]: Server listening on :: port 22.
nov. 17 14:22:13 ubuntu-tpssh systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
nov. 17 14:22:17 ubuntu-tpssh sshd[1366]: Accepted password for luka from 192.168.1.34 port 64266 ssh2
nov. 17 14:22:17 ubuntu-tpssh sshd[1366]: pam_unix(sshd:session): session opened for user luka(uid=1000) by luka(uid=0)
nov. 17 14:22:18 ubuntu-tpssh sshd[1368]: Accepted password for luka from 192.168.1.34 port 64268 ssh2
nov. 17 14:22:18 ubuntu-tpssh sshd[1368]: pam_unix(sshd:session): session opened for user luka(uid=1000) by luka(uid=0)
nov. 17 16:21:19 ubuntu-tpssh sshd[1680]: Accepted password for luka from 192.168.1.34 port 60855 ssh2
nov. 17 16:21:19 ubuntu-tpssh sshd[1680]: pam_unix(sshd:session): session opened for user luka(uid=1000) by luka(uid=0)
nov. 17 16:21:19 ubuntu-tpssh sshd[1682]: Accepted password for luka from 192.168.1.34 port 60856 ssh2
nov. 17 16:21:19 ubuntu-tpssh sshd[1682]: pam_unix(sshd:session): session opened for user luka(uid=1000) by luka(uid=0)
luka@ubuntu-tpssh:~$ ****
```

J'ai également testé la connexion entre les mon serveur et mon client :

```
C:\Users\Luka>ping 192.168.1.75

Envoi d'une requête 'Ping' 192.168.1.75 avec 32 octets de données :
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.75 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.1.75:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Luka>
```

2. Connexion par mot de passe

Je me suis par la suite connecté à mon serveur en SSH avec l'utilisation d'un mot de passe :

```
C:\Users\Luka>ssh 192.168.1.75
The authenticity of host '192.168.1.75 (192.168.1.75)' can't be established.
ED25519 key fingerprint is SHA256:yS1kBXaE+QDaxcjhvUW3nFd6UTx4h6r+jIQ/97FkG4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.75' (ED25519) to the list of known hosts.
luka@192.168.1.75's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of lun. 17 nov. 2025 16:39:08 UTC

System load:  0.0               Processes:            166
Usage of /:   32.9% of 13.67GB   Users logged in:     1
Memory usage: 14%              IPv4 address for eth0: 192.168.1.75
Swap usage:   0%

La maintenance de sécurité étendue pour Applications n'est pas activée.

25 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou exécutez : sudo pro status

Last login: Mon Nov 17 16:21:19 2025 from 192.168.1.34
luka@ubuntu-tpssh:~$ |
```

Puis j'ai générer une paire de clé sur mon client windows :

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations.

PS C:\Users\Luka> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\Luka/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Luka/.ssh/id_ed25519
Your public key has been saved in C:\Users\Luka/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:0J7sKJCbPSD/Sd6+sognghe0e4ElzGIrZdu4UaQYuBo luka@DESKTOP-JE7FC5S
The key's randomart image is:
+--[ED25519 256]--+
|
|o . .
|o+ o . .
|E+=o. + .
|B+0= S
|*=+B. o
|oo+o* . .
|oo+*. =
|o=o =++.
+----[SHA256]-----+
PS C:\Users\Luka>
```

3. Connexion par clé SSH

Et j'ai par la suite transmis la clé publique de mon client vers mon serveur :

```
PS C:\Users\Luka> scp C:\Users\Luka\.ssh/id_rsa.pub luka@192.168.1.77:/home/Luka/.ssh  
luka@192.168.1.77's password:  
id_rsa.pub 100% 747 729.5KB/s 00:00
```

Et nous pouvons voir qu'il arrive bien sur le serveur SSH

```
luka@debian:~/.ssh$ ls  
id_rsa.pub  
luka@debian:~/.ssh$ |
```

Puis par la suite je me suis connecté via le certificat (Je n'ai pas trouvé de moyen de me connecté via la clé publique sans cette commande depuis windows ?)

```
PS C:\Users\Luka> ssh -i C:\Users\Luka\.ssh/id_rsa luka@192.168.1.77  
Linux debian 6.12.57+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.57-1 (2025-11-05) 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 Nov 17 18:30:30 2025 from 192.168.1.34  
luka@debian:~$ |
```

Afin d'être sûr que l'authentification par clé publique fonctionne, j'ai désactivé la connexion ssh via mot de passe :

```

# 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
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to "no" here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to "yes" to enable keyboard-interactive authentication. Depending on
# the system's configuration, this may involve passwords, challenge-response,
# one-time passwords or some combination of these and other methods.
# Beware issues with some PAM modules and threads.
KbdInteractiveAuthentication no

# Kerberos options

```

4. Transfert de fichiers SCP

J'ai créé sur mon client le dossier "Dataset" positionné dans :
C:\Users\Luka\Desktop\TP_Licence\TP_linux\SSH; puis j'ai fait le transfert SCP :

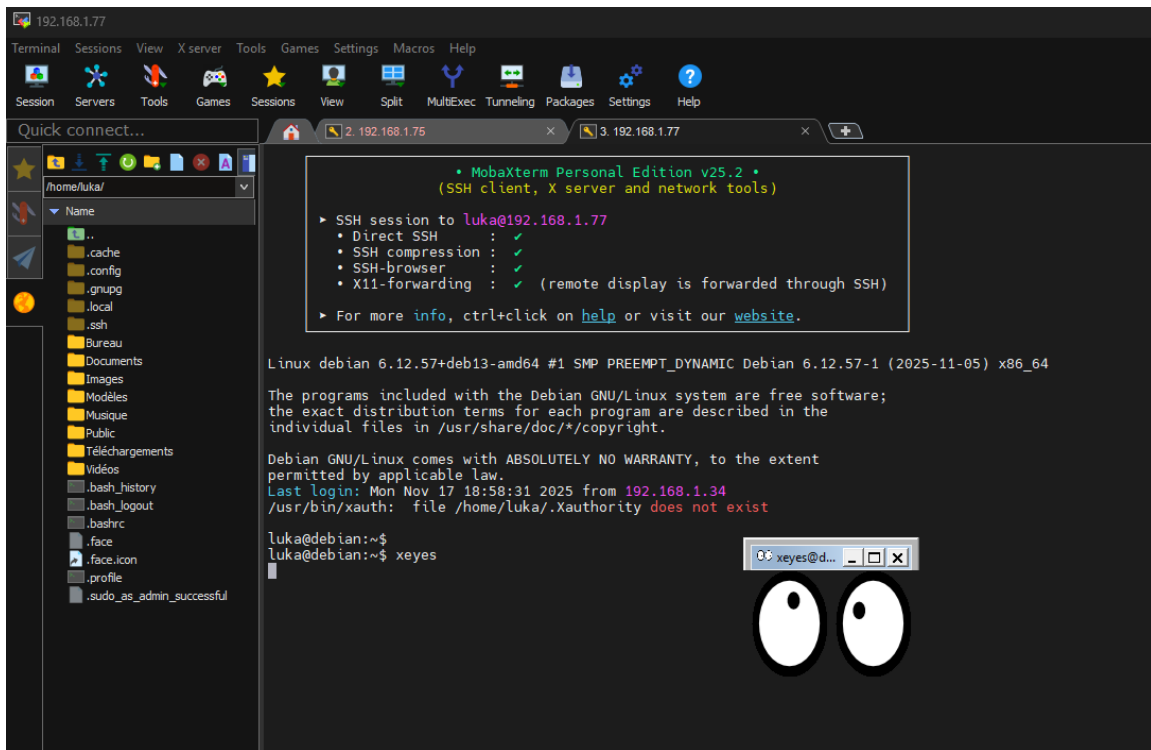
```
PS C:\Users\Luka> scp -r "C:\Users\Luka\Desktop\TP_Licence\TP_linux\SSH\dataset" luka@192.168.0.177:/home/Luka/  
PS C:\Users\Luka> scp -r "C:\Users\Luka\Desktop\TP_Licence\TP_linux\SSH\dataset" luka@192.168.1.77:/home/Luka/  
plop.txt 100% 0 0.0KB/s 00:00  
plap.txt 100% 0 0.0KB/s 00:00  
plip.txt 100% 0 0.0KB/s 00:00  
PS C:\Users\Luka> |
```

J'ai ensuite vérifié sur mon serveur avec tree afin que d'afficher l'arborescence :

```
luka@debian:~$ cd /home/luka/dataset  
luka@debian:~/dataset$ ls  
part1 part2 part3  
luka@debian:~/dataset$ sudo apt install tree  
Installation de :  
tree  
  
Sommaire :  
Mise à niveau de : 0. Installation de : 1Supprimé : 0. Non mis à jour : 0  
Taille du téléchargement : 59,4 kB  
Espace nécessaire : 132 kB / 23,0 GB disponible  
  
Réception de : 1 http://deb.debian.org/debian trixie/main amd64 tree amd64 2.2.1-1 [59,4 kB]  
59,4 ko réceptionnés en 0s (1 447 ko/s)  
Sélection du paquet tree précédemment désélectionné.  
(Lecture de la base de données... 139318 fichiers et répertoires déjà installés.)  
Préparation du dépaquetage de .../tree_2.2.1-1_amd64.deb ...  
Dépaquetage de tree (2.2.1-1) ...  
Paramétrage de tree (2.2.1-1) ...  
Traitement des actions différées (« triggers ») pour man-db (2.13.1-1) ...  
luka@debian:~/dataset$ tree  
.  
├── part1  
│   └── plop.txt  
├── part2  
│   └── plap.txt  
└── part3  
    └── plip.txt  
  
4 directories, 3 files  
luka@debian:~/dataset$
```

5. Redirection X11

Avec l'utilisation de MobaXterm j'ai pu lancer xeyes :



Avant ça j'ai configuré le fichier sshd_config tel que :

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost yes
#PermitTTY yes
```