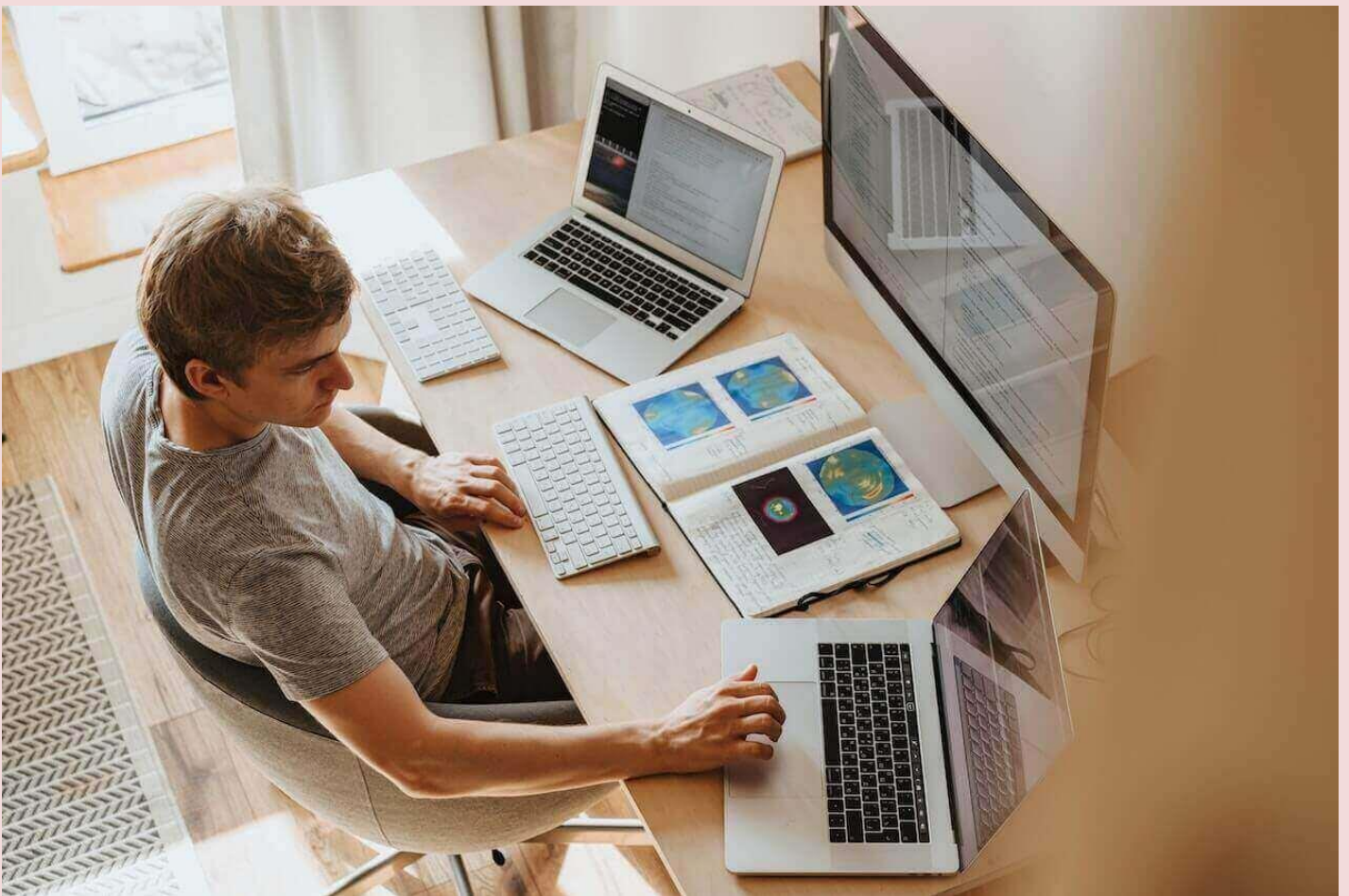
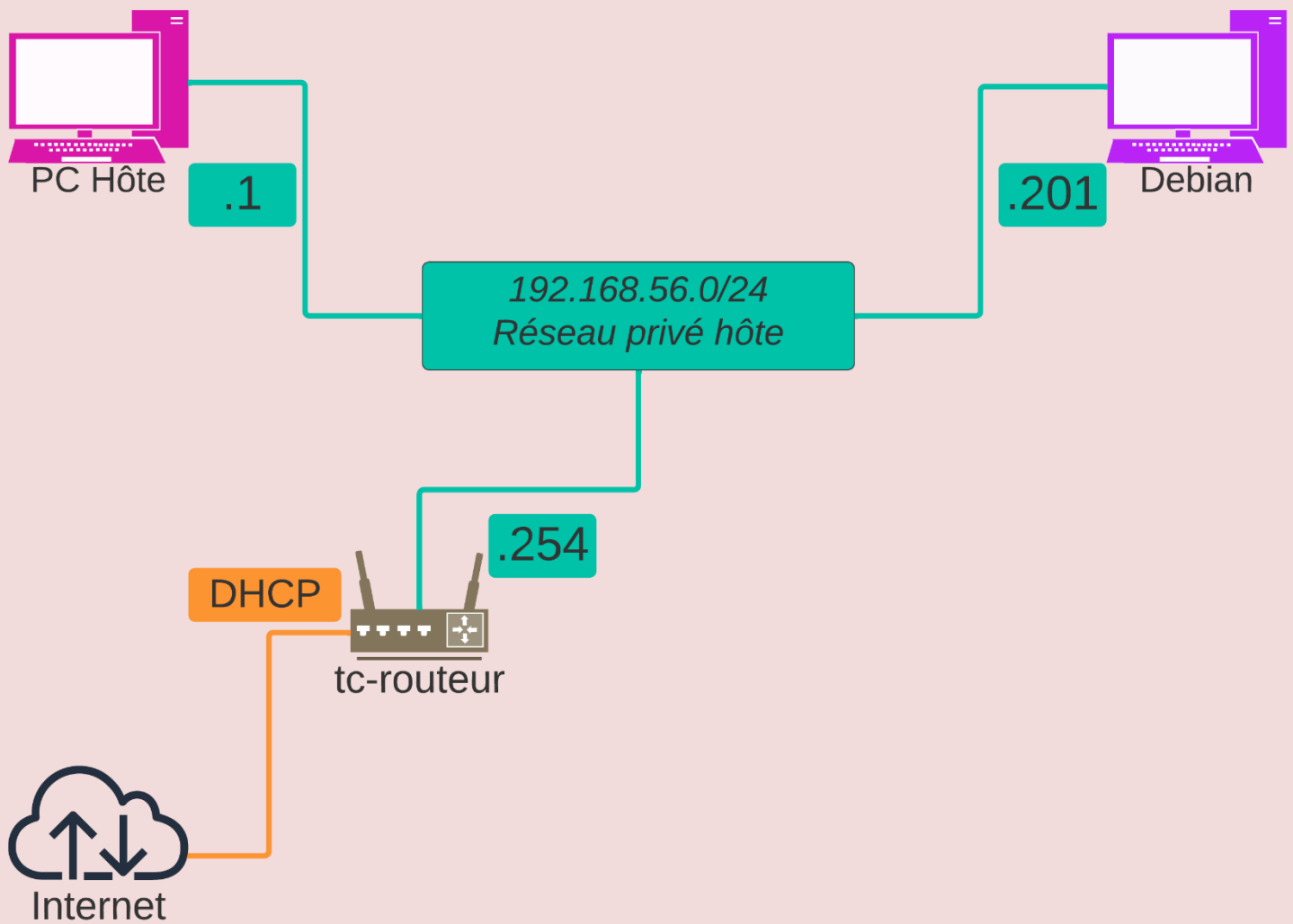


**Cette documentation vous présente les 5  
meilleurs logiciels d'accès à distance !**



Notre réseau :



## Table des matières

1) Telnet.....	4
1.1) Qu'est-ce que Telnet ? .....	4
1.2) Installation de Telnet .....	4
2) SSH .....	7
2.1) Qu'est-ce que SSH ? .....	7
2.2) Installation de SSH .....	7
3) RDP .....	9
3.1) Qu'est-ce que RDP ? .....	9
3.2) Installation de RDP .....	9
4) VNC .....	12
4.1) Qu'est-ce que VNC ? .....	12
4.2) Installation de VNC .....	12
5) Remmina .....	14
5.1) Qu'est-ce que Remmina ? .....	14
5.2) Installation de Remmina .....	14

## 1) Telnet

### 1.1) Qu'est-ce que Telnet ?

Telnet est un protocole de communication réseau utilisé pour établir des connexions textuelles bidirectionnelles à travers un réseau informatique, généralement via une connexion TCP/IP. Il permet à un utilisateur de se connecter à distance à un serveur ou à un autre dispositif réseau pour exécuter des commandes, envoyer des données et recevoir des informations texte.

Cependant, il est important de noter que Telnet présente des inconvénients importants en matière de sécurité. Les données transmises via Telnet, y compris les noms d'utilisateur et les mots de passe, sont généralement transmises en texte clair, ce qui les rend vulnérables aux interceptions malveillantes. Pour cette raison, Telnet a été largement remplacé par des protocoles plus sécurisés tels que SSH (On va y venir juste après !) pour les opérations sensibles nécessitant une sécurité accrue.

Telnet est un protocole de type client-serveur s'appuyant sur TCP. Les clients se connectent généralement sur le port 23 du serveur.

### 1.2) Installation de Telnet

Avant toute commande, nous allons d'abord mettre à jour les paquets avec la commande suivante : `apt update`

Puis, nous pouvons continuer avec la commande `apt install telnetd` qui va nous permettre de lancer l'installation de ce dernier :

```
root@buster:~# apt install telnetd_
```

Après installation, nous pouvons donc démarrer telnet en tapant la commande suivante :

```
root@buster:~# systemctl start inetd
```

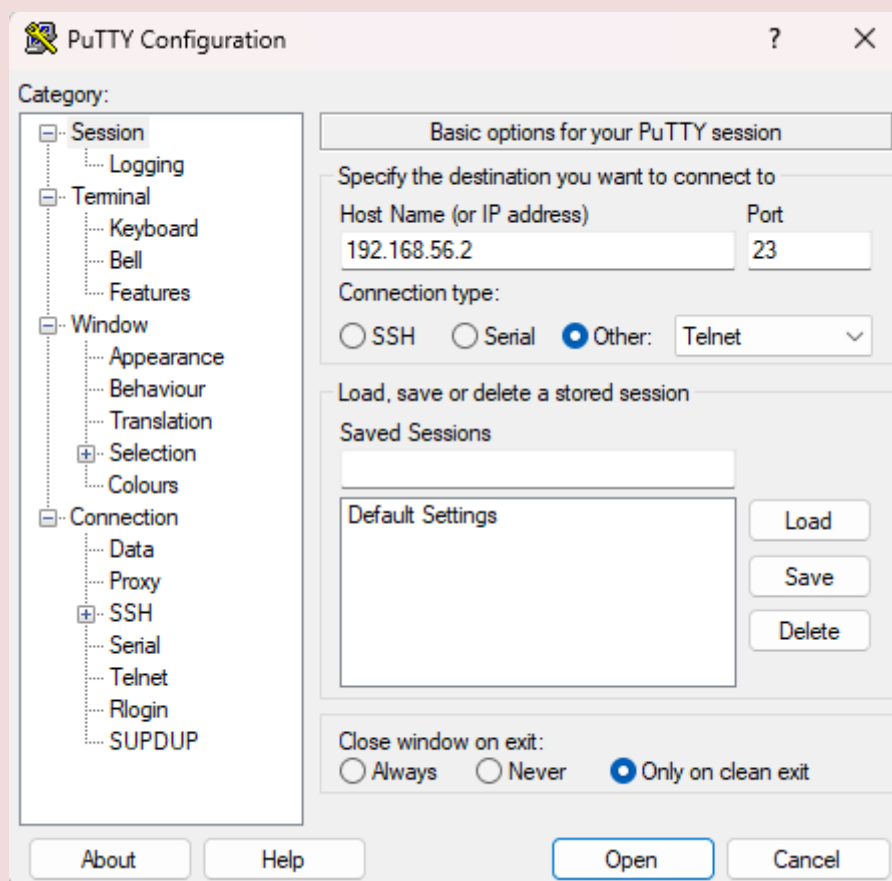
Nous allons maintenant vérifier que telnet est bien démarré avec la commande suivante :

```
root@buster:~# systemctl status inetd
• inetd.service - Internet superserver
   Loaded: loaded (/lib/systemd/system/inetd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-09-08 14:17:51 CEST; 1min 51s ago
     Docs: man:inetd(8)
   Main PID: 288 (inetd)
    Tasks: 1 (limit: 1149)
   Memory: 1.1M
   CGroup: /system.slice/inetd.service
           └─288 /usr/sbin/inetd

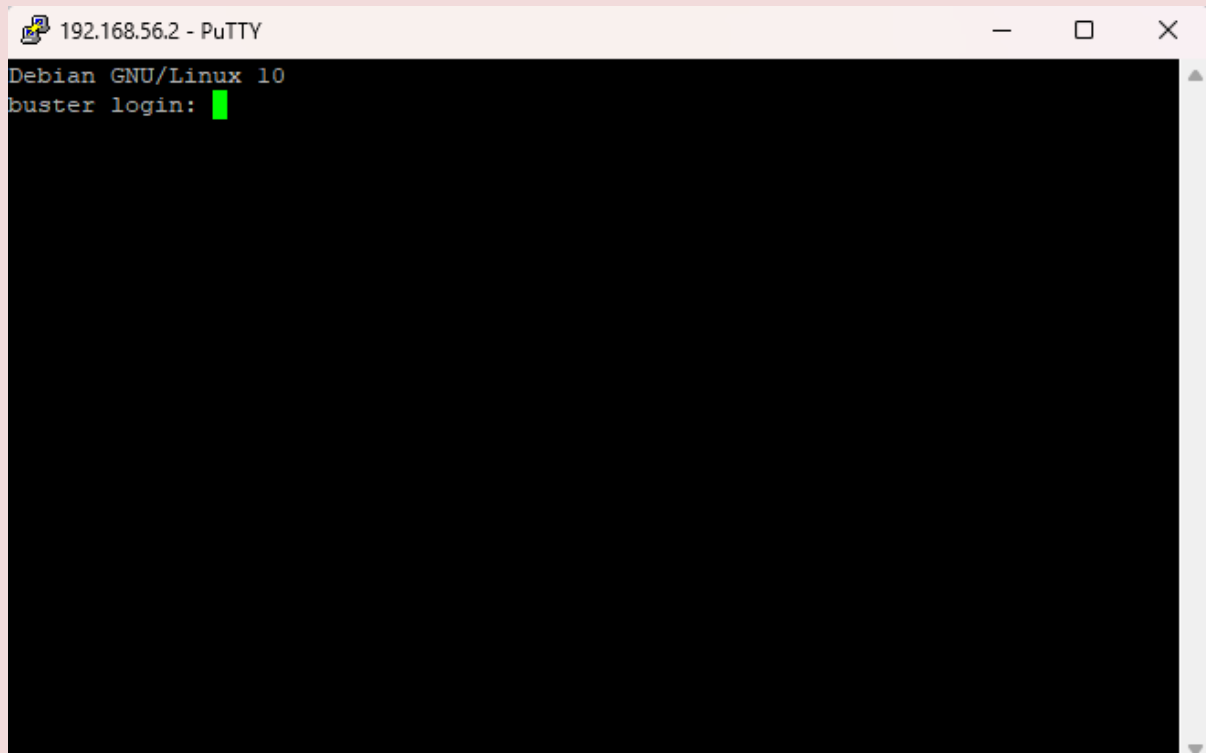
sept. 08 14:17:51 buster systemd[1]: Starting Internet superserver...
sept. 08 14:17:51 buster systemd[1]: Started Internet superserver.
root@buster:~#
```

Vu que le service est démarré, nous pouvons basculer sur PuTTY qui va nous permettre de nous connecter à la machine en accès à distance via telnet.

Nous renseignons l'IP de cette dernière puis choisissons « Other » et « Telnet ».

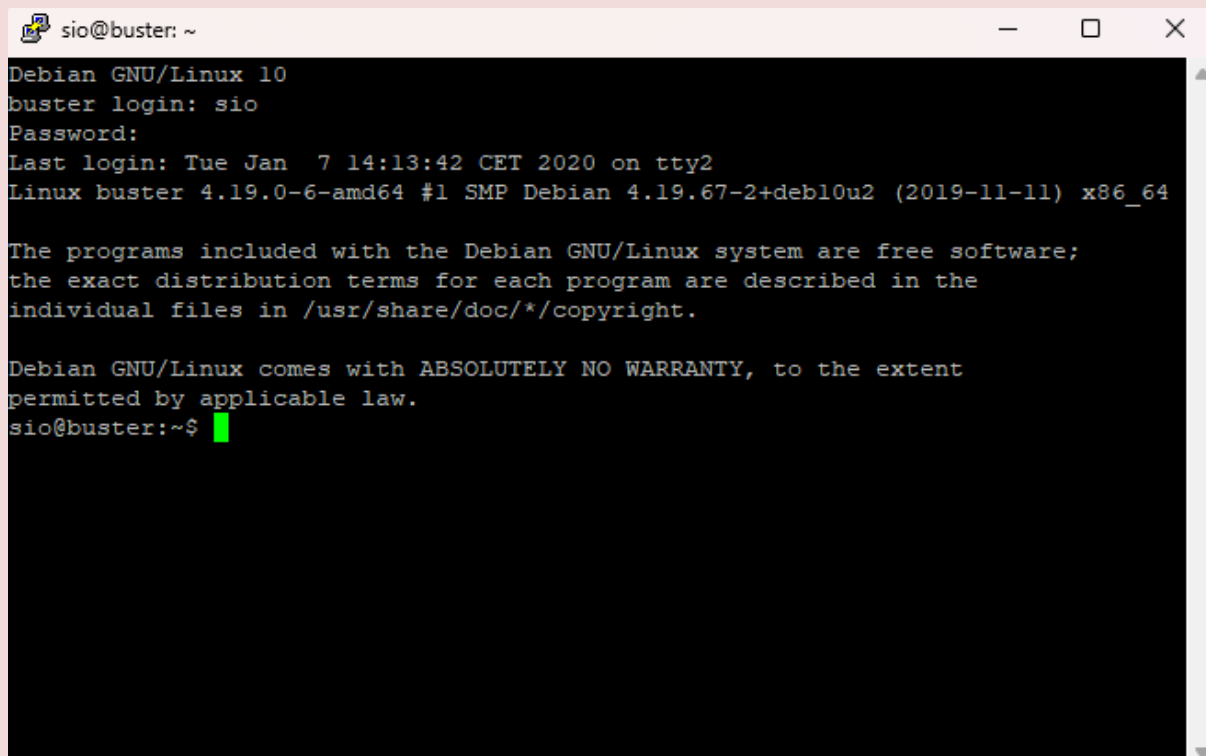


Une fois arrivé ici, nous allons nous connecter avec le login/mdp soit sio/sio.



```
192.168.56.2 - PuTTY
Debian GNU/Linux 10
buster login: █
```

Nous voici connecté à distance sur notre machine virtuelle Debian !



```
sio@buster: ~
Debian GNU/Linux 10
buster login: sio
Password:
Last login: Tue Jan  7 14:13:42 CET 2020 on tty2
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.
sio@buster:~$ █
```

## 2) SSH

### 2.1) Qu'est-ce que SSH ?

SSH, ou Secure Shell, est un protocole de communication sécurisé utilisé pour établir des connexions sécurisées et chiffrées entre deux dispositifs informatiques via un réseau. Il est largement utilisé pour l'administration à distance, l'accès sécurisé à des systèmes, le transfert de fichiers et d'autres opérations réseau nécessitant un haut niveau de sécurité. SSH a été développé pour résoudre les problèmes de sécurité associés au protocole Telnet, qui transmet les données en texte clair et est vulnérable aux interceptions malveillantes.

En raison de ses caractéristiques de sécurité avancées, SSH est devenu le choix préféré pour l'accès à distance et la gestion de serveurs et de dispositifs réseau dans les environnements informatiques professionnels et est fortement recommandé pour toute opération nécessitant une communication sécurisée sur un réseau.

### 2.2) Installation de SSH

Avant toute commande, nous allons d'abord mettre à jour les paquets avec la commande suivante : `apt update`

Puis, nous pouvons continuer avec la commande `apt install ssh` qui va nous permettre de lancer l'installation de ce dernier :

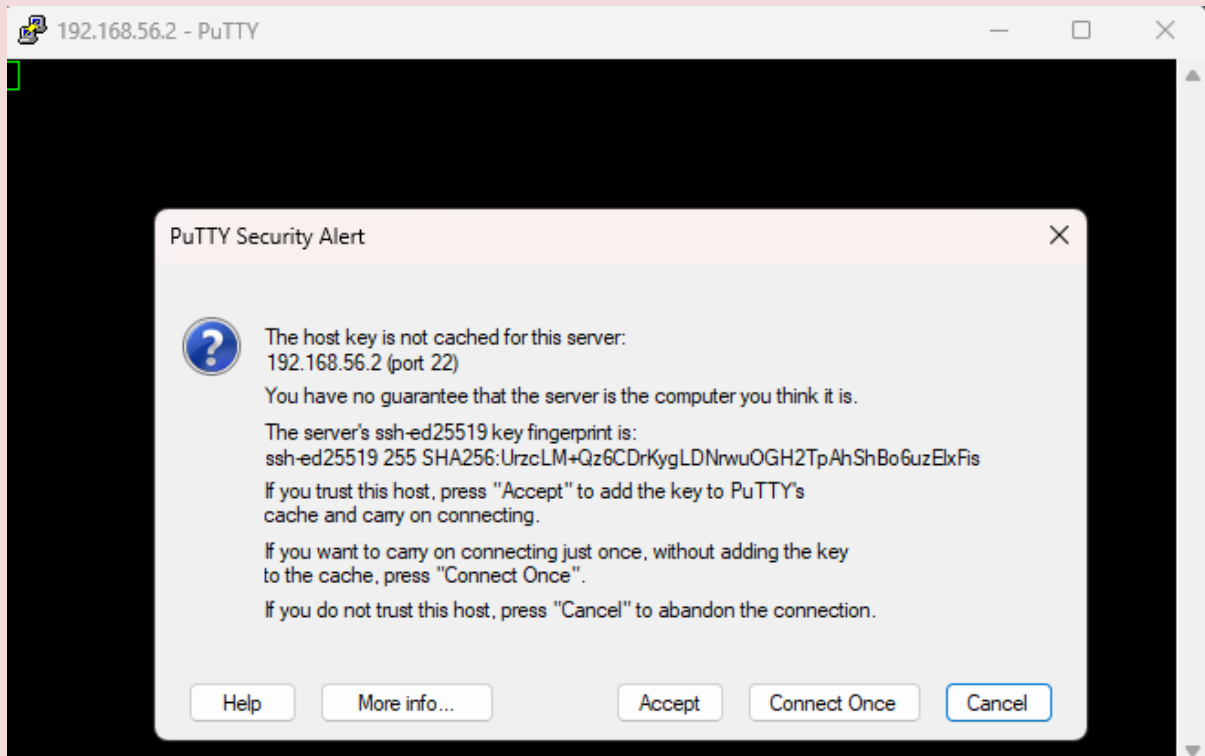
```
root@buster:~# apt install openssh-server
```

Puis, nous pouvons éventuellement vérifier que celui-ci est bien démarré en exécutant la commande : `systemctl status ssh`

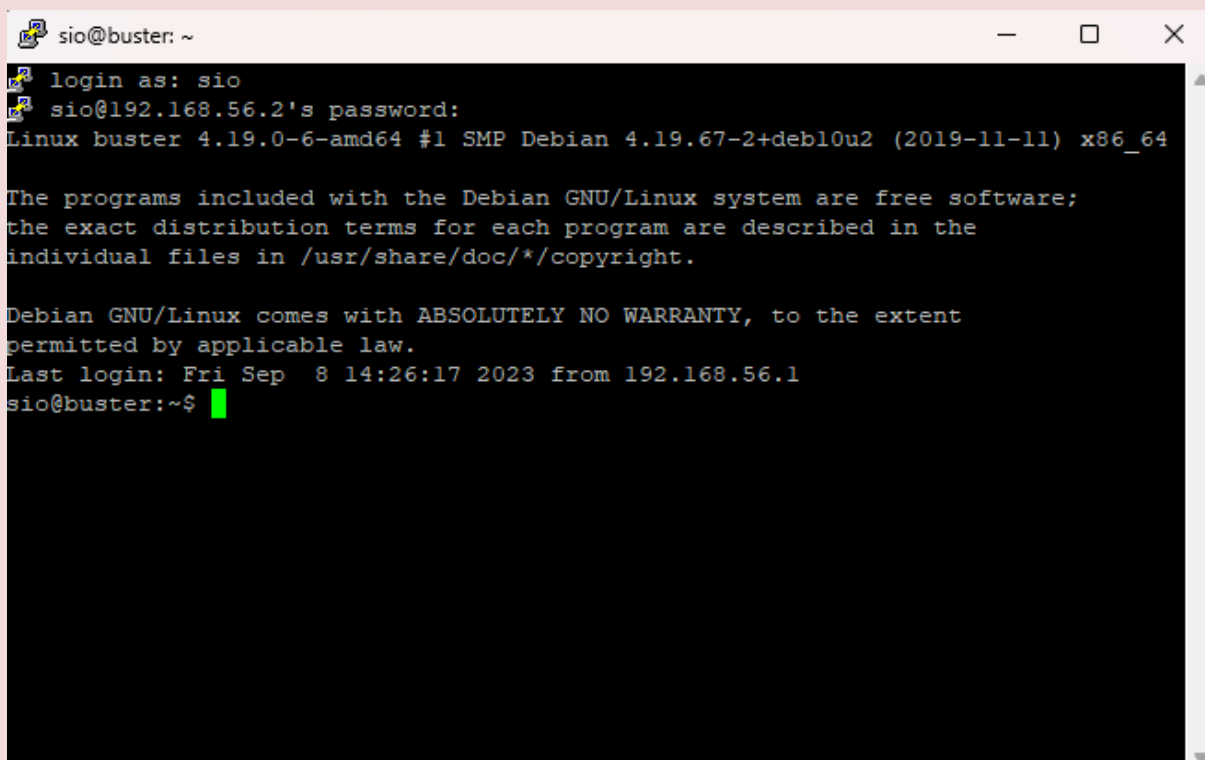
```
root@buster:~# systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-09-08 14:17:51 CEST; 2min 43s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 286 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 294 (sshd)
     Tasks: 1 (limit: 1149)
    Memory: 4.5M
   CGroup: /system.slice/ssh.service
           └─294 /usr/sbin/sshd -D

sept. 08 14:17:51 buster systemd[1]: Starting OpenBSD Secure Shell server...
sept. 08 14:17:51 buster sshd[294]: Server listening on 0.0.0.0 port 22.
sept. 08 14:17:51 buster sshd[294]: Server listening on :: port 22.
sept. 08 14:17:51 buster systemd[1]: Started OpenBSD Secure Shell server.
```

Maintenant nous allons nous connecter en renseignant correctement l'adresse IP puis en sélectionnant « SSH ».



Nous voilà connecter sur notre machine Debian à distance en SSH !





### 3) RDP

#### 3.1) Qu'est-ce que RDP ?

RDP signifie Remote Desktop Protocol, ce qui se traduit littéralement par "Protocole de Bureau à Distance" en français. Il s'agit d'un protocole de communication développé par Microsoft. RDP permet à un utilisateur de se connecter à un ordinateur distant sur un réseau ou via Internet et d'accéder à son bureau, ses fichiers et ses applications comme s'il était physiquement présent devant cet ordinateur distant.

Pour utiliser RDP, vous avez généralement besoin d'un logiciel client RDP (tel que le client Bureau à distance de Microsoft) sur l'ordinateur à partir duquel vous souhaitez vous connecter, ainsi que la possibilité d'accéder à l'ordinateur distant via une adresse IP ou un nom d'hôte, ainsi que des informations d'identification appropriées (nom d'utilisateur et mot de passe) pour vous authentifier sur l'ordinateur distant. Une fois la connexion établie, vous pouvez contrôler l'ordinateur distant comme si vous étiez devant lui.

#### 3.2) Installation de RDP

Avant toute installation de paquet, il faut bien évidemment faire un apt update.

Puis juste après nous pouvons exécuter la commande suivante :

```
root@cz-image:~# apt install xrdp
```

Nous pouvons maintenant vérifier que RDP est bien démarré.

```
root@cz-image:~# systemctl status xrdp
● xrdp.service - xrdp daemon
   Loaded: loaded (/lib/systemd/system/xrdp.service; enabled; vendor preset: ena
   Active: active (running) since Wed 2023-09-20 15:14:19 CEST; 6s ago
     Docs: man:xrdp(8)
           man:xrdp.ini(5)
   Main PID: 1253 (xrdp)
    Tasks: 1 (limit: 1137)
   Memory: 1.2M
    CGroup: /system.slice/xrdp.service
            └─1253 /usr/sbin/xrdp

sept. 20 15:14:18 cz-image xrdp[1252]: (1252)(140686928680768)[DEBUG] Testing if
sept. 20 15:14:18 cz-image xrdp[1252]: (1252)(140686928680768)[DEBUG] Closed soc
sept. 20 15:14:18 cz-image systemd[1]: xrdp.service: Can't open PID file /run/xr
sept. 20 15:14:19 cz-image systemd[1]: Started xrdp daemon.
sept. 20 15:14:19 cz-image systemd[1]: /lib/systemd/system/xrdp.service:8: PIDFi
sept. 20 15:14:19 cz-image systemd[1]: /lib/systemd/system/xrdp.service:8: PIDFi
sept. 20 15:14:19 cz-image systemd[1]: /lib/systemd/system/xrdp.service:8: PIDFi
sept. 20 15:14:19 cz-image systemd[1]: /lib/systemd/system/xrdp.service:8: PIDFi
sept. 20 15:14:20 cz-image xrdp[1253]: (1253)(140686928680768)[INFO ] starting x
sept. 20 15:14:20 cz-image xrdp[1253]: (1253)(140686928680768)[INFO ] listening
```

Nous allons ajouter un nouvel utilisateur qui va nous permettre juste après de nous connecter avec ce compte utilisateur à distance sur notre machine hôte.

```
root@cz-image:~# sudo adduser root ssl-cert
sudo: impossible de déterminer le nom de l'hôte cz-image: Nom ou service inconnu
Ajout de l'utilisateur « root » au groupe « ssl-cert »...
Adding user root to group ssl-cert
Fait.
```

Puis, nous mettons un mot de passe :

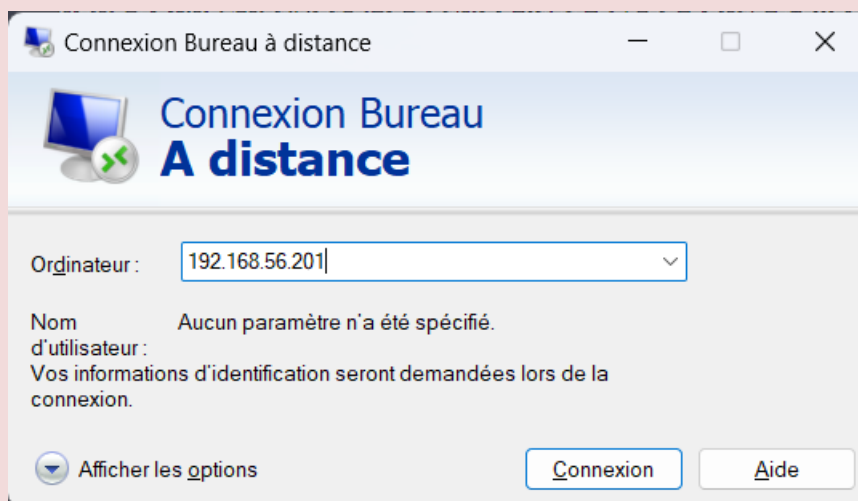
```
root@cz-image:~# sudo passwd root
sudo: impossible de déterminer le nom de l'hôte cz-image: Nom ou service inconnu
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
```

Enfin, nous redémarrons RDP avec la commande suivante :

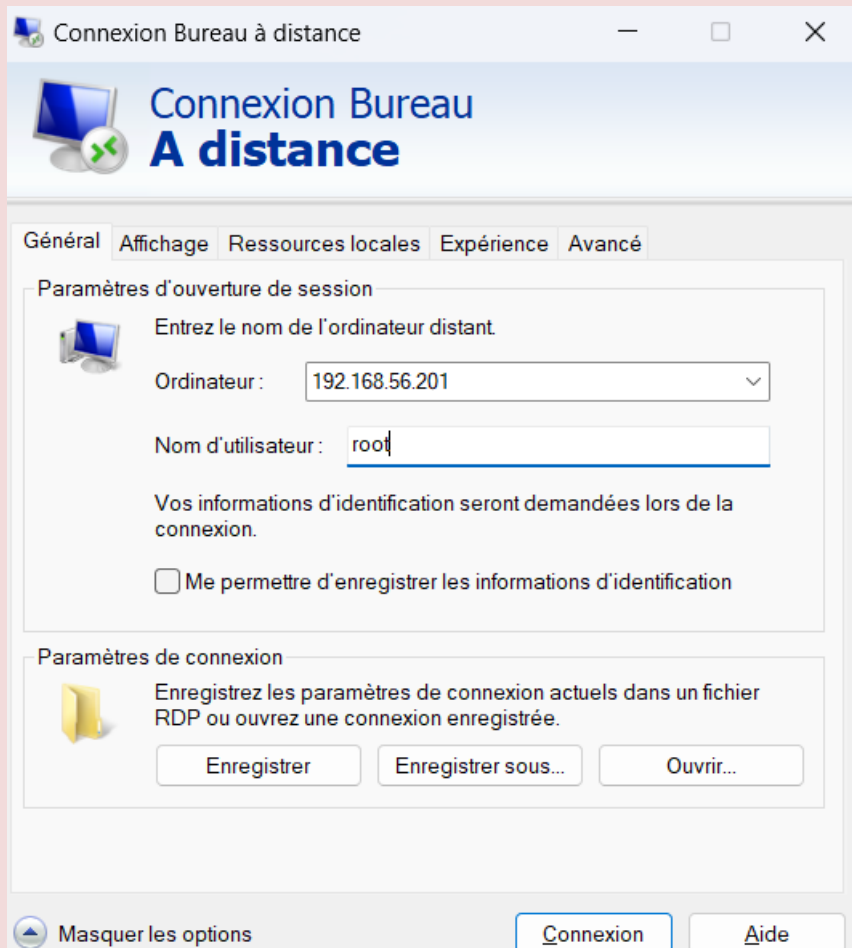
```
root@cz-image:~# systemctl restart xrdp
```

Nous basculons sur le logiciel connexion bureau à distance sur Windows.

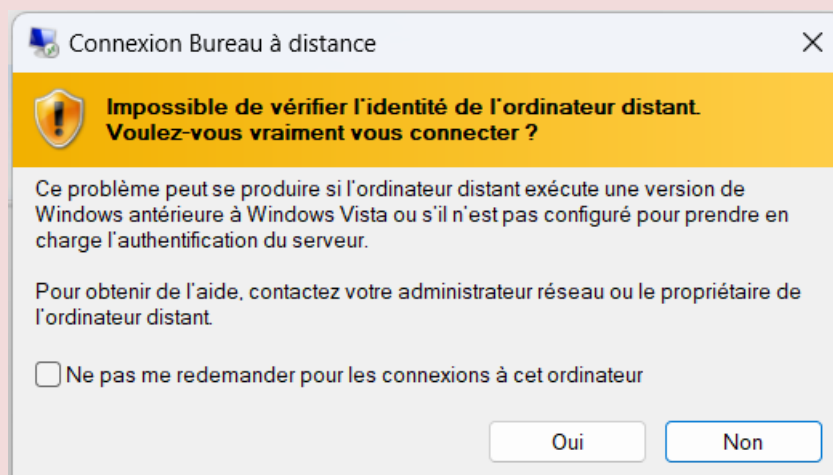
Nous renseignons l'IP puis déroulons les options juste en dessous.



Nous pouvons mettre le nom d'utilisateur saisi juste au-dessus lors de la création du nouvel utilisateur.



Nous pouvons sélectionner « oui ».



Et nous voici connecté à distance sur notre machine via RDP.

## 4) VNC

### 4.1) Qu'est-ce que VNC ?

VNC, ou Virtual Network Computing, est un système de partage d'écran et un protocole de communication qui permet à un utilisateur de visualiser et de contrôler à distance un ordinateur depuis un autre ordinateur ou un appareil compatible, généralement via Internet ou un réseau local. Contrairement à RDP (Remote Desktop Protocol) qui est spécifique à Microsoft, VNC est une technologie plus générique et multiplateforme, ce qui signifie qu'elle peut être utilisée pour interagir avec des ordinateurs exécutant différents systèmes d'exploitation, tels que Windows, MacOS, Linux, et d'autres.

VNC est utilisé dans de nombreuses situations, notamment pour l'assistance à distance, l'administration de serveurs, le dépannage informatique, l'accès à distance aux postes de travail, et bien d'autres applications. Il existe plusieurs implémentations de VNC disponibles, y compris des logiciels open source tels que TightVNC, RealVNC et UltraVNC, qui permettent aux utilisateurs de choisir la solution qui correspond le mieux à leurs besoins spécifiques.

### 4.2) Installation de VNC

Avant toute installation de paquet, il faut bien évidemment faire un apt update.

Puis juste après nous pouvons exécuter la commande suivante :

```
root@cz-image:~# apt install tightvncserver_
```

Nous allons directement exécuter « vncserver » pour configurer le mot de passe lors de notre connexion à distance plus tard.

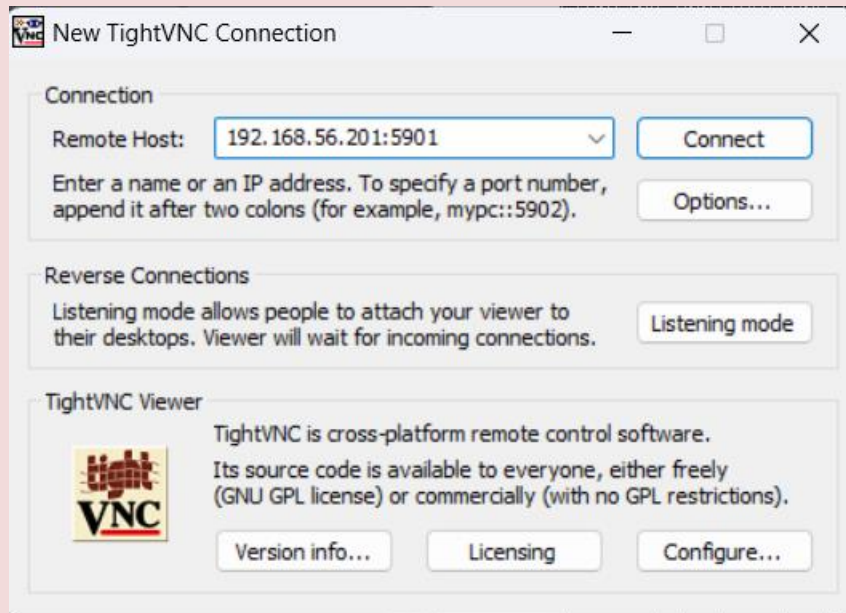
```
root@cz-image:~# vncserver
You will require a password to access your desktops.
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
xauth: file /root/.Xauthority does not exist
xauth: (argv):1: bad display name "cz-image:1" in "add" command
xauth: file /root/.Xauthority does not exist

New 'X' desktop is cz-image:1

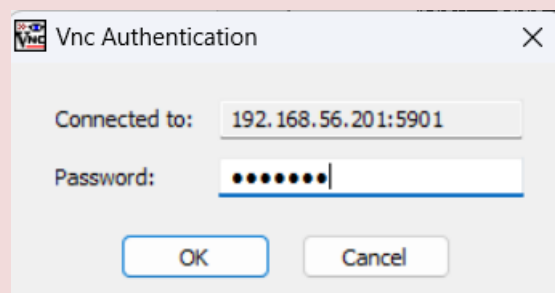
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/cz-image:1.log
```

Il faut en effet côté client, installer le logiciel TightVNC pour pouvoir nous connecter à distance sur notre machine.

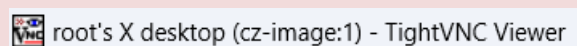
Après avoir installer le logiciel, nous le lançons puis nous pouvons renseigner l'IP de la machine Debian avec à la suite le port VNC qui est ici 5901 (« 01 ») car c'est notre première session.



Juste après, il nous demande le mot de passe ce qui est tout à fait normal, nous rentrons celui que l'on a rentré au-dessus lors de la configuration.



Nous voici connecté à distance sur notre machine Debian via TightVNC.



## 5) Remmina

### 5.1) Qu'est-ce que Remmina ?

Remmina est un logiciel open source de client de bureau à distance pour les systèmes d'exploitation Linux et Unix-like. Il offre aux utilisateurs la possibilité de se connecter à distance à d'autres ordinateurs, serveurs ou postes de travail, généralement via des protocoles de bureau à distance tels que RDP (Remote Desktop Protocol), VNC (Virtual Network Computing), SSH (Secure Shell), NX, XDMCP, SPICE, et d'autres. Remmina est conçu pour fournir une interface utilisateur conviviale et unifiée pour accéder à des ordinateurs distants exécutant divers systèmes d'exploitation et protocoles.

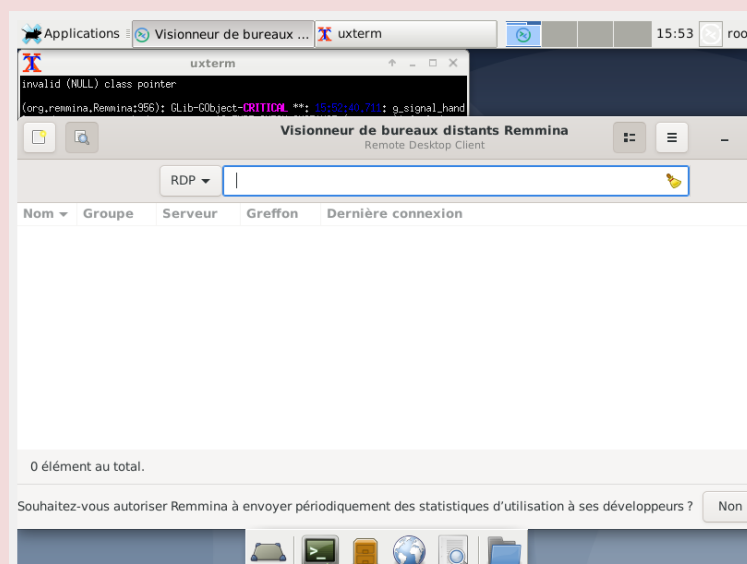
Remmina est un choix populaire parmi les utilisateurs de Linux et d'autres systèmes Unix-like qui ont besoin de se connecter à distance à d'autres ordinateurs, que ce soit pour l'administration de serveurs, le travail à distance ou d'autres besoins liés au bureau à distance. En raison de sa nature open source, il est généralement disponible gratuitement et peut être installé sur la plupart des distributions Linux.

### 5.2) Installation de Remmina

Nous sommes maintenant habitués à exécuter un apt update avant toute installation de paquet.

```
root@cz-image:~# apt install remmina
```

En exécutant juste « remmina », nous obtenons cela :



Nous allons créer un nouveau profil de connexion pour se connecter à distance plus tard via notre machine Windows.

**Préférences de bureau distant**

**Profil**

Nom: Connexion rapide

Groupe:

Protocole: RDP — Remote Desktop Protocol

Précommande: command %h %u %t %U %p %g --option

Post-commande: /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g

**Basique**    Avancé    Tunnel SSH

Serveur:

Nom d'utilisateur:

Mot de passe de l'utilisateur:

Domaine:

Définitions d'affichage: ☒ Utiliser la taille de fenêtre initiale    ☐ Utiliser la définition d'affichage du client

Nous renseignons les informations nécessaires ci-dessus.

Puis, sur la machine Windows (hôte), nous pouvons renseigner l'IP, le nom d'utilisateur et le mot de passe choisis.

Nous voilà connecté à distance sur notre machine Debian via Remmina !

**Vous êtes maintenant capable de vous connecter à une machine à distance avec ces 5 logiciels sans difficulté !**

