

Installation du serveur SSH

Avant utilise cette cammande pour update : `apt-get update`

```
(root@kali)-[~]
# apt-get update
Réception de :1 http://kali.download/kali kali-rolling InRelease [41,5 kB]
Réception de :2 http://kali.download/kali kali-rolling/main amd64 Packages [1
9,1 MB]
Réception de :3 http://kali.download/kali kali-rolling/main amd64 Contents (d
eb) [44,4 MB]
Réception de :4 http://kali.download/kali kali-rolling/contrib amd64 Packages
[101 kB]
Réception de :5 http://kali.download/kali kali-rolling/contrib amd64 Contents
(deb) [219 kB]
Réception de :6 http://kali.download/kali kali-rolling/non-free amd64 Package
s [192 kB]
Réception de :7 http://kali.download/kali kali-rolling/non-free amd64 Content
s (deb) [863 kB]
Réception de :8 http://kali.download/kali kali-rolling/non-free-firmware amd6
4 Packages [33,0 kB]
Réception de :9 http://kali.download/kali kali-rolling/non-free-firmware amd6
4 Contents (deb) [16,9 kB]
54,9 Mo réceptionnés en 2min 15s (481 ko/s)
Lecture des listes de paquets... Fait
```

Pour installer le serveur SSH , on va installer la suite OpenSSH. Utiser la commande suivante : `sudo apt install openssh-server`

```
(root@kali)-[~]
# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  openssh-client openssh-sftp-server
Paquets suggérés :
  keychain libpam-ssh monkeysphere molly-guard ufw
Les paquets suivants seront mis à jour :
  openssh-client openssh-server openssh-sftp-server
3 mis à jour, 0 nouvellement installés, 0 à enlever et 2449 non mis à jour.
Il est nécessaire de prendre 1 496 ko dans les archives.
Après cette opération, 1 001 ko d'espace disque seront libérés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://kali.download/kali kali-rolling/main amd64 openssh-sft
p-server amd64 1:9.6p1-4 [65,4 kB]
Réception de :3 http://mirror.leitecastro.com/kali kali-rolling/main amd64 op
enssh-client amd64 1:9.6p1-4 [975 kB]
Réception de :2 http://kali.download/kali kali-rolling/main amd64 openssh-ser
ver amd64 1:9.6p1-4 [456 kB]
1 496 ko réceptionnés en 1min 12s (20,7 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 466363 fichiers et répertoires déjà install
és.)
Préparation du dépaquetage de .../openssh-sftp-server_1%3a9.6p1-4_amd64.deb .
..
```

Pour démarrer le service SSH avec SysVinit, utilisez la commande suivante : `/etc/init.d/ssh start`

```
(root@kali)-[~]
# /etc/init.d/ssh start
Starting ssh (via systemctl): ssh.service.
```

Sécurisation du serveur SSH :

- a) Modifier le port d'écoute : entre le fichier utilise la commande `/etc/ssh/sshd_config`

Remplacer la valeur du port 22 par 22 par exemple. Lesse lememe port

```
Include /etc/ssh/sshd_config.d/*.conf
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- b) Interdire les connexions à distance en root :

Configurez "PermitRootLogin" sur "prohibit-password" pour exiger une clé SSH pour se connecter en tant que root. Sinon, utilisez "no" pour interdire complètement la connexion en tant que root, renforçant ainsi la sécurité.

```
# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Enregistrez le fichier modifié et redémarrez le serveur ssh avec la commande : `/etc/init.d/ssh restart`

```
(root@kali)-[~]
# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
```

- c) Ajouter un compte utilisateur

La commande suivante permet d'ajouter un nouveau compte utilisateur sur un système

Linux : `adduser nom_utilisateur`

```
# adduser test
Ajout de l'utilisateur « test » ...
Ajout du nouveau groupe « test » (1001) ...
Ajout du nouvel utilisateur « test » (1001) avec le groupe « test » (1001) ..
.
Création du répertoire personnel « /home/test » ...
```

Assurer vous que le compte utilisateur existe déjà dans la machine cliente, sinon créer un nouveau compte d'utilisateur. `ssh test@10.0.0.100 -p 22`

```
(root@kali)-[~]
# ssh test@10.0.0.100 -p 22
```

```
The authenticity of host '[192.168.1.241:220 ([192.168.1.211:220)]' can't
be established. ECDSA key fingerprint is Shh256:0cpguBu?i•LM/DrutQDd1u/01WU7Wm2RcL6KCIv/.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
```

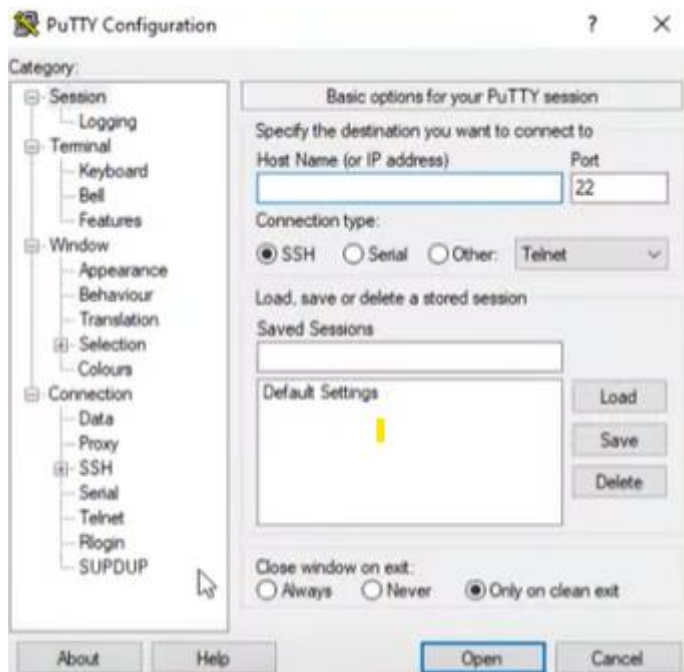
Pour vous déconnecter, tapez `logout` : La commande pour vous déconnecter de la session SSH est simplement :

```
(test@kali)-[~]
└─#logout
Connection to 10.0.0.100 closed
(test@kali)-[~]
```

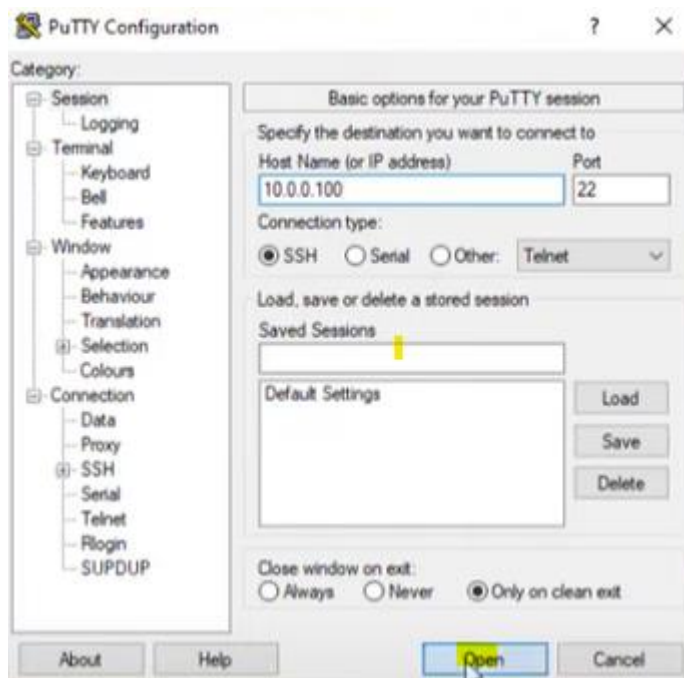
b) Se connecter à partir d'une machine cliente Windows :

J'utilise personnellement – s'appelle PuTTY. Vous pouvez télécharger PuTTY depuis son site officiel. <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Une fois que c'est fait et installé, lancez **PuTTY**. Une fenêtre comme celle de la figure suivante devrait s'afficher.



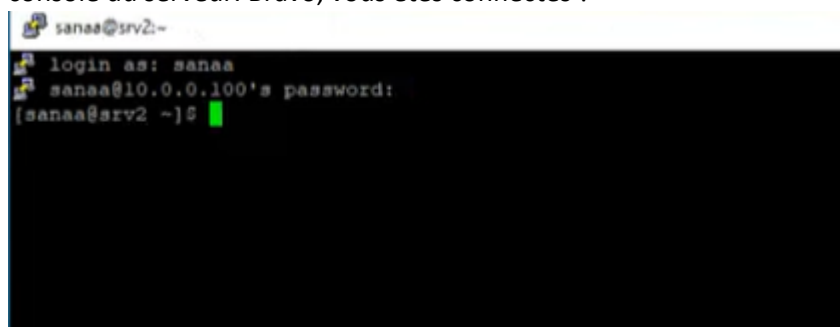
Dans ce cas, je vais entrer l'adresse IP de mon PC Linux (serveur ssh) situé sur le même VMnet que la machine Windows (10.0.0.100) et le port (22)



La première fois que vous vous connectez à votre serveur, PuTTY devrait vous demander une confirmation comme sur la figure suivante.



Dans ce cas j'ai choisi l'utilisateur **sanaa**. Entrez ensuite le mot de passe la console du serveur devrait vous afficher un message de bienvenue puis un prompt qui correspond à la console du serveur. Bravo, vous êtes connectés !



Pour vous déconnecter, tapez **logout** ou son équivalent :

6. L'identification automatique par clé :

a) Authentification par clé depuis Linux

Pour mettre en marche ce **mode d'authentification**, nous allons d'abord devoir effectuer des opérations sur la machine du client, puis nous enverrons le résultat au serveur.

```
ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

tapez Entrée directement sans rien écrire, et la clé ne sera pas chiffrée sur votre machine ;

```
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Maintenant écrire une phrase pour protéger la clé privée

```
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:CL4+WCLQT/mTSQEKjU38PDfHTmkoR5UeITVLUQvnq/k root@kali
The key's randomart image is:
+--[RSA 3072]--+
|. *. ... oO=o |
|..+. .ooo* . "the quieter you become, the more you are able
|..o.o =.oo |
|. ..B.*.B . |
|. .o.B.Os . |
|. . o.= .o |
|. .+. .o |
|... . |
|.. E |
+--[SHA256]--+
```

Votre clé publique devrait se trouver dans `~/.ssh/id_rsa.pub`. Votre clé privée, elle, se trouve dans `~/.ssh/id_rsa`.

```
(root@kali)-[~]
# ls ~/.ssh

id_rsa  id_rsa.pub
```

id_rsa : votre clé privée, qui doit rester secrète. Elle est chiffrée si vous avez rentré une passphrase ;


```

# cat ~/.ssh/id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAAABbhospTqq
fbB1+7pEWpUAKXAAAAGAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQDPURwkm50V
QDsuyXqKVgYODnhDFUm3PMEWPPVOp1YDxLVY0yUiKyXC57evJh4Y771H0f4fc6l278veZh
yNsIOB5c5P8sNUoqq+abIsAHvMEzpep0xj5xp8+9yQ00ZRM6bMFgUVks569K0DIg5ITJKz
sEV+wca2m8huDug+nD09MNBHouE2GGnBfdRlg7qlqzSukBUCq0jt03sBuU9jopRy1KsAEW
KXNJl1WN9gK+RJIGsX1VWmdKCRfVS9mQXiBK9N86hmIpB287s9pS7Cku5Ws/cAdSrmsx3j
HQzTU8Pj23kiJvMjwIbg0m3wIc6hnhMC2jiRgPs+vh+/pwS8FT48+ud0cPyLHFMxARTpV
A5c8AHueVWtfuyFX4luNYsZFLewGyh7kxPn2tUFxR5F/cfq2wa5rVyZjIqpWHHyAyURuM7
Vi1+9dLWXL/m820fxBscn/YVsiKSIOHBgklETZxfE9SNK3ZzEHqRKUfzL6x756PksTFw3M
jKoYvI8e1bCGMAAAWAKRCgcklmIFn2gRIVUEuR0jGLbg2tHdgcUptyiyiKBYvUzG0TArUT
VI6eJnmXzYTi4zz3U1bX13/WWZCbIipYc3zoTmsp/M3YpwdFu1x4fMjWDLdr8ksMzEsn1/
W/WVzpqS5H+ul+/rvNtD6MZVgjbMJIrSa5k1yLfcjVsAO2+LjGuqdMa+e+wrNfVU/Ngw+
71SqMIR5J921KERxXMqQL/M4zcolms01tC3FqkaMfypD3OWNpl1xsGpQQL1H8dXJhCJlkk
chtrQw9zCDlnpqVxgo7Jw0oYv9mnv4S9iIkFHX8wjYHQoIk/mVWgkOEIULBiyEGjrHe60q
3dGKOLK54Md0VhV7EBPs0NF1YQ9V4qKoooOgvbLeInOmBOBWYfZq8IWQJ5CfclSudM7LVP
hl1FkuK0fVYoDZDzRTchbSoMgp00ol2sjgJhsdE05NB/WDNP+3jWQmGrRfG0t40tpYfyHa
0x1gtU0qEbLZTfjE/an2bXxTur5EEP9V0ZPhsJvAO09XcuBZ/as2+irNnzfHZov02NeeXu
Z1+pQDN8EW5bucWpVeOKgLYWSWASo+gQX8YNbrIDXgJYbyHB2B2IHwYmkN0r3Rdh8UAST
keZ+CsjjLRXikBw9Z+viRAmASmwqvg79w7KeMbd5n7i7w0jUije95zbZQ9+RsCH/3RzU9B
0L3WBdmj9SvqZMQWQCcWPRB3slWoYHNZQwp4USYLaFbc/sQfcC2XuWtK3EvA6UQZLCFUR8
J1NH3YcnnfWw1wWboWhf1SfRnxd2t0PnZ0+8BZ6Tiii0dBvaFk1GDTDZxFe2/7RKhDGe1+

```

- **id_rsa.pub** : la clé publique que vous pouvez communiquer à qui vous voulez, et que vous devez envoyer au serveur ;

```

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDPURwkm50VQDsuyXqKVgYODnhDFUm3PMEWPPVOp
iYDxLVY0yUiKyXC57evJh4Y771H0f4fc6l278veZhYnsIOB5c5P8sNUoqq+abIsAHvMEzpep0xj5x
p8+9yQ00ZRM6bMFgUVks569K0DIg5ITJKzsEV+wca2m8huDug+nD09MNBHouE2GGnBfdRlg7qlqzS
ukBUCq0jt03sBuU9jopRy1KsAEWKXNJl1WN9gK+RJIGsX1VWmdKCRfVS9mQXiBK9N86hmIpB287s9
pS7Cku5Ws/cAdSrmsx3jHQzTU8Pj23kiJvMjwIbg0m3wIc6hnhMC2jiRgPs+vh+/pwS8FT48+ud0c
PyLHFMxARTpVVA5c8AHueVWtfuyFX4luNYsZFLewGyh7kxPn2tUFxR5F/cfq2wa5rVyZjIqpWHHyA
yURuM7Vi1+9dLWXL/m820fxBscn/YVsiKSIOHBgklETZxfE9SNK3ZzEHqRKUfzL6x756PksTFw3Mj
KoYvI8e1bCGM= root@kali

```

Le plus simple pour cela est d'utiliser la commande spéciale `ssh-copy-id`. Utilisez-la comme ceci :

Vous serez ensuite invité à entrer le mot de passe du compte auquel vous voulez vous connecter (dans cet exemple celui du compte `ali` sur la machine serveur `ssh`), si tout se passe bien, vous devez voir le message suivant indiquant l'ajout d'une clé :

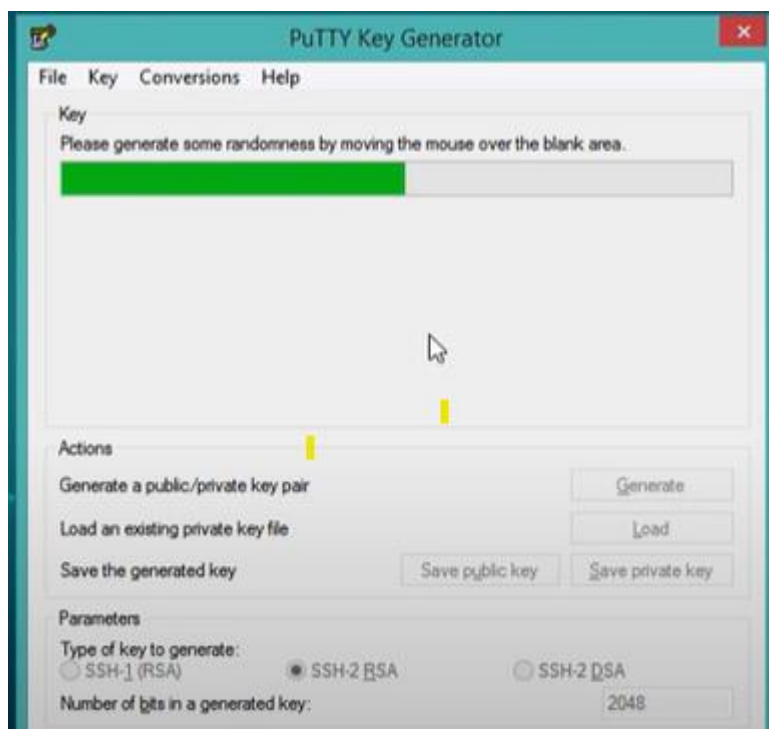
```

#ssh-copy-id ali@10.0.0.100 -p 22
/bin/ssh-copy-id: INFO: attempting to log in with the new keys), to filter
/bin/ssh-copy-id: INFO: 1 keys) remain to be installed - if you are promp
number of key(s) added: 1
Now try logging into the machine, with: "ssh 'ali@10.0.0.100'" and check to

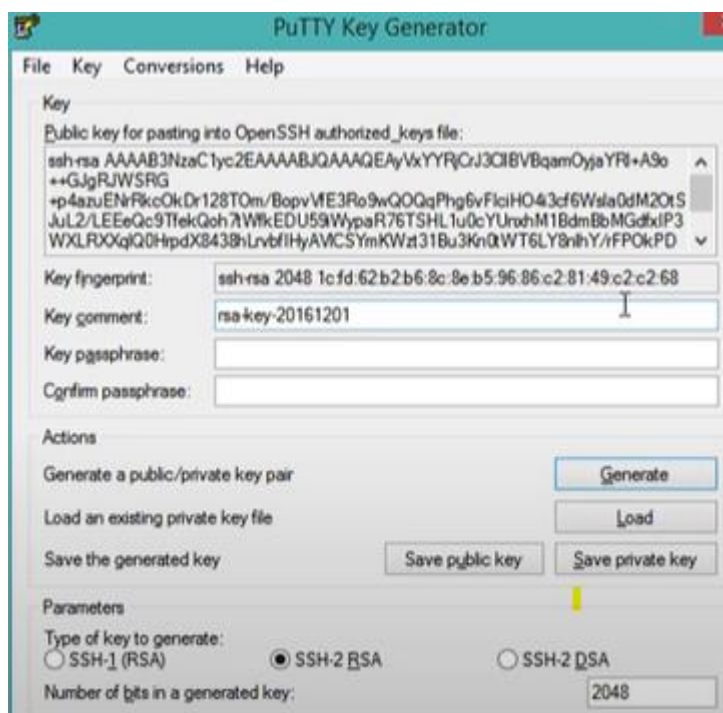
```

b) Authentification par clé depuis Windows (PuTTY)

Pour l'aider à générer cette paire, le programme vous propose quelque chose d'assez amusant : vous devez bouger la souris dans la fenêtre (figure suivante)



Une fois que c'est fait, on vous affiche la clé publique (figure suivante) :



- Envoyer la clé publique au serveur

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
2rQAcq1ZsyDMheFkkSS
+2cIO2fKWBSBqTsqiD9MdGkVKiiNTVbCB5gC0nvTXf/7uuTHtYvmWsJfRpz1nkaQq1SsrOkJDP9atHkUh5OL
+6cvLth1fhSa+llk8tVzNG5g77pnd94OJV6T6rYRe6vktIYmS3Mlc1dYXuLDnTDhDEnxYrDlx
+M4RTIjAgf178begZkPQH1D13I3ezqXamYbbrwm3U4wnzKhk7FU0rj7NaoNsgXSs3DocLVn7JGF7pqKTbU6Kg3
YsRreAYgU0JlcE6Ow8oaQaAhy+F3h root
```

Key fingerprint: ssh-rsa 2048 SHA256:RCRmn3C9FyAyDG2XDurJ51vufNscwkuFnB6HKylEFPQ

Key comment: root

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

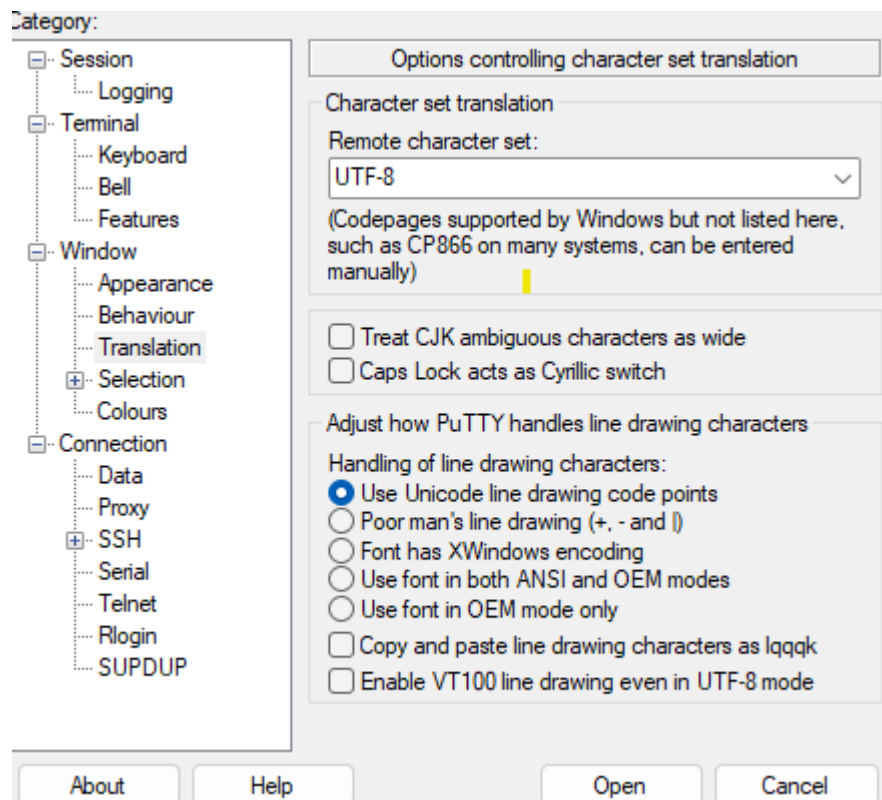
your public key is displayed in PuTTYgen, that you should not have closed. To paste the key into the console, use the Shift + Insert key combination instead of Ctrl + V.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDHtDofRkA3V5K15mDC8xwvthj2MtaK4REuqz1CqEE0M2mDtShtM2rQAcq1ZsyDMheFkkSS+
2cIO2fKWBSBqTsqiD9MdGkVKiiNTVbCB5gC0nvTXf/7uuTHtYvmWsJfRpz1nkaQq1SsrOkJDP9atHkUh5OL+
6cvLth1fhSa+llk8tVzNG5g77pnd94OJV6T6rYRe6vktIYmS3Mlc1dYXuLDnTDhDEnxYrDlx+M4RTIjAgf178begZkPQH1D13I3ezqXamYbbrwm3U4wnzKhk7FU0rj7NaoNsgXSs3DocL
n7JGF7pqKTbU6Kg3YsRreAYgU0JlcE6Ow8oaQaAhy+F3h root
```

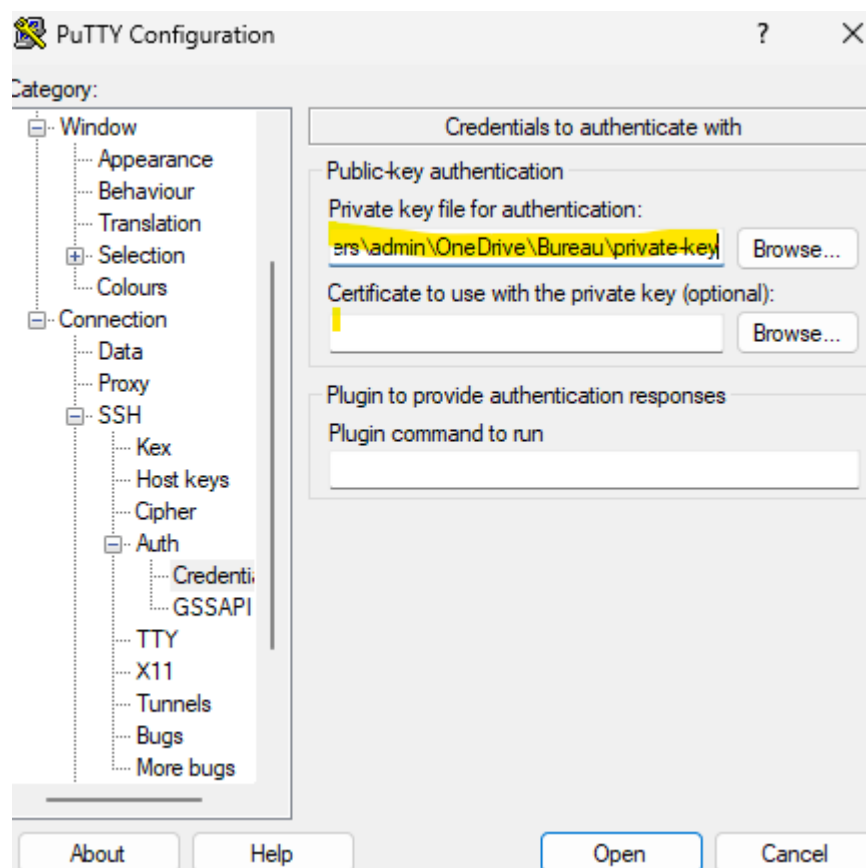
Disconnect and relaunch PuTTY. We will now configure it so that it connects with the key

- Configurer PuTTY pour qu'il se connecte avec la clé

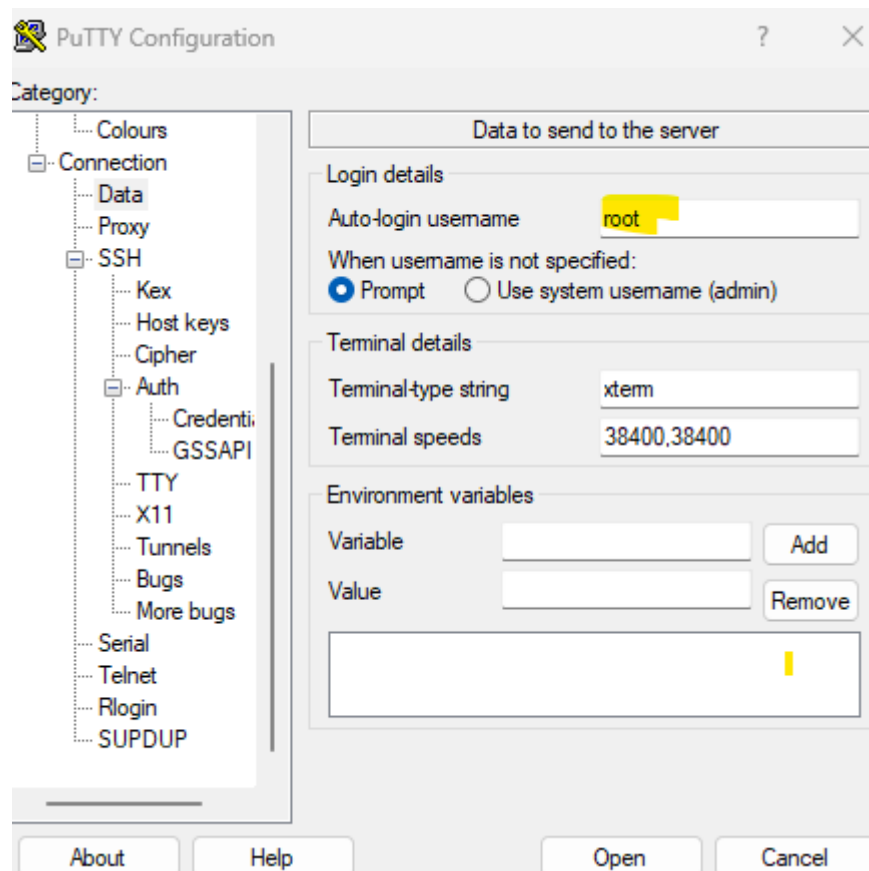
Set the value of the dropdown list to UTF-8, as in the following figure.



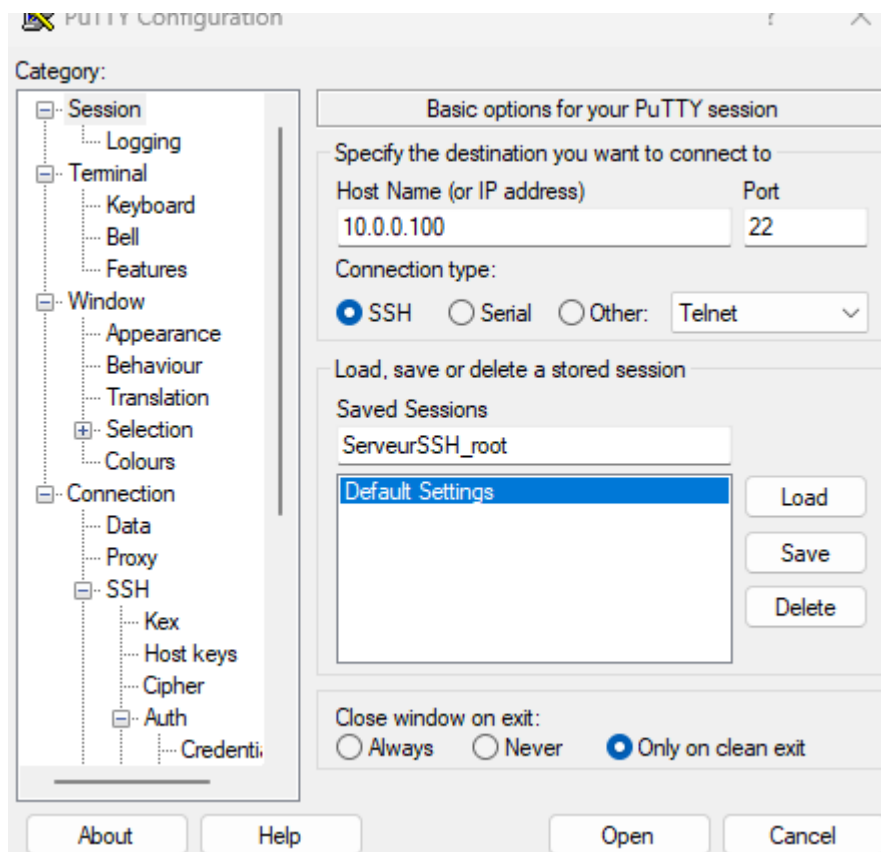
Maintenant, rendez-vous dans Connection → SSH → Auth->Credentials. Cliquez sur le petit bouton « Browse » pour sélectionner votre clé privée (figure suivante).



aussi d'aller dans Connection → Data et d'entrer votre login dans « Auto-login username », comme la figure suivante vous le montre.



Retournez à l'accueil en cliquant sur la section « Session » tout en haut (figure suivante). Entrez l'IP du serveur. Ensuite, je vous recommande fortement d'enregistrer ces paramètres.



- L'agent SSH Pageant

L'agent SSH installé avec PuTTY s'appelle « Pageant ». Je vous recommande de le lancer au démarrage de l'ordinateur automatiquement

« Pageant » est pratique, il vaut mieux

l'arrêter si vous devez vous absenter de votre ordinateur un long moment et que quelqu'un risque de l'utiliser. Sinon, n'importe qui peut se connecter à vos serveurs sans avoir à entrer de mot de passe.

