2. Configurer une clé SSH

Il est très important de comprendre le fonctionnement des clés SSH.
Un administrateur serveur doit toujours utiliser des clés SSH pour accéder a son serveur.

- La clé SSH
- Génération d'une clé SSH
- Déployer la clé publique
    - Le déploiement d'une clé publique
- Utiliser une clé SSH
    - Se connecter avec une clé SSH

La clé SSH

Lorsqu'on parle d'une clé SSH c'est en réalité des clés asymétriques, par principe, vous avez deux clés (on parle de paire de clés) :

une clé publique, que vous pouvez diffuser librement, voire mettre à disposition sur un serveur de clés ;

et une clé privée, qui constitue véritablement votre « identité », et ne doit jamais être diffusée : elle reste simplement présente dans votre dépôt de clés personnel.

Génération d'une clé SSH

En ligne de commande

Sur le client avec le terminal `PowerShell`.

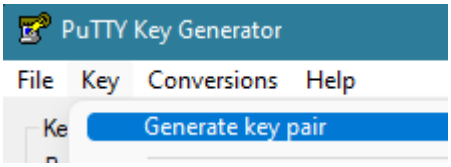
> Par défaut, ssh-keygen créera une paire de clés RSA de 2048 bits, ce qui est suffisamment sûr pour la plupart des cas d'utilisation (vous pouvez éventuellement passer l'indicateur `-b 4096` pour créer une clé plus grande de 4096 bits).

```
> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/chemin/vers/id_rsa): $SSH_KEY_NAME
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
> cat /chemin/vers/$SSH_KEY_NAME.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDcDQOcpmaXyM9EVrJ8pw82BP77/LQ5SMUkhO8IZHhdjmTqInIQ44ROggcnOcdb9k
MaiPfFS86zvDYSc52JKbCbff0tL29G5UT9TfHHZDBzNthE5mURfsNg4CeoS5Xeu8pap3ZYi+74r3Cwv/bJxXnwnfciR1Wo
Rqdg+46KzmHf9Rk/ittXMRMcl+XY2CfvlKKze293H4mffDefU4bEc9vtEkwvQuB8kxLjXv29dJ1UUAoKRnEmFpHWjqSes3
xmnE2W9cz6WMWXcJRDooCx8e6GST6dtap3nzgxX6jQoORy4TauSoim7YL0fld6OxlGTUg/DBikOY0H4RBBXMI5KxUbdpyN
RYefDBm1BVlE4TM/7z6p3H2qyJu0jqSoe+gXF1fYfcCXD4+WPqL+uFCeFXBvOu7HzgFlK5OHOMA1zxLZdUgWuTg5HFoUju
oRsWpqhcCvl/ah4LuJlihM6eMiN6RCc0VU/jhN7EW3UGPTE6Ue/Bing/NWe6QaeCyY9vmU+Y0= username@DESKTOP-
A651448
```

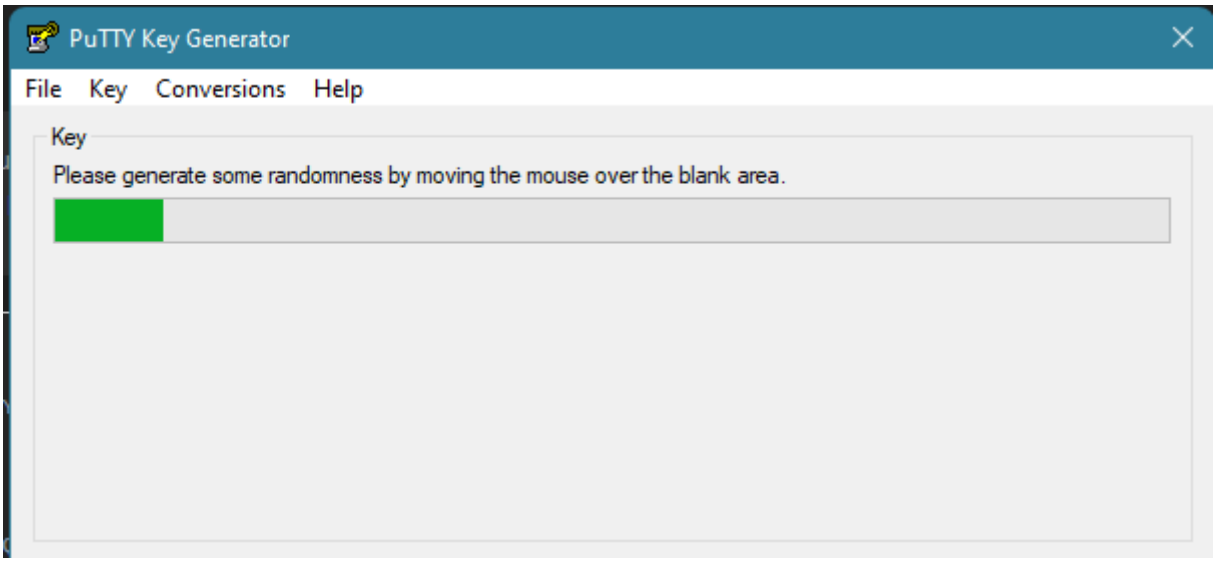
Copier le contenu de la clé publique `$SSH_KEY_NAME.pub` pour l'envoyer sur le serveur.

Via PUTTYgen

Ouvrez PUTTYgen et dans la barre des outils appuyez sur **Key** puis **Generate Key pair**.



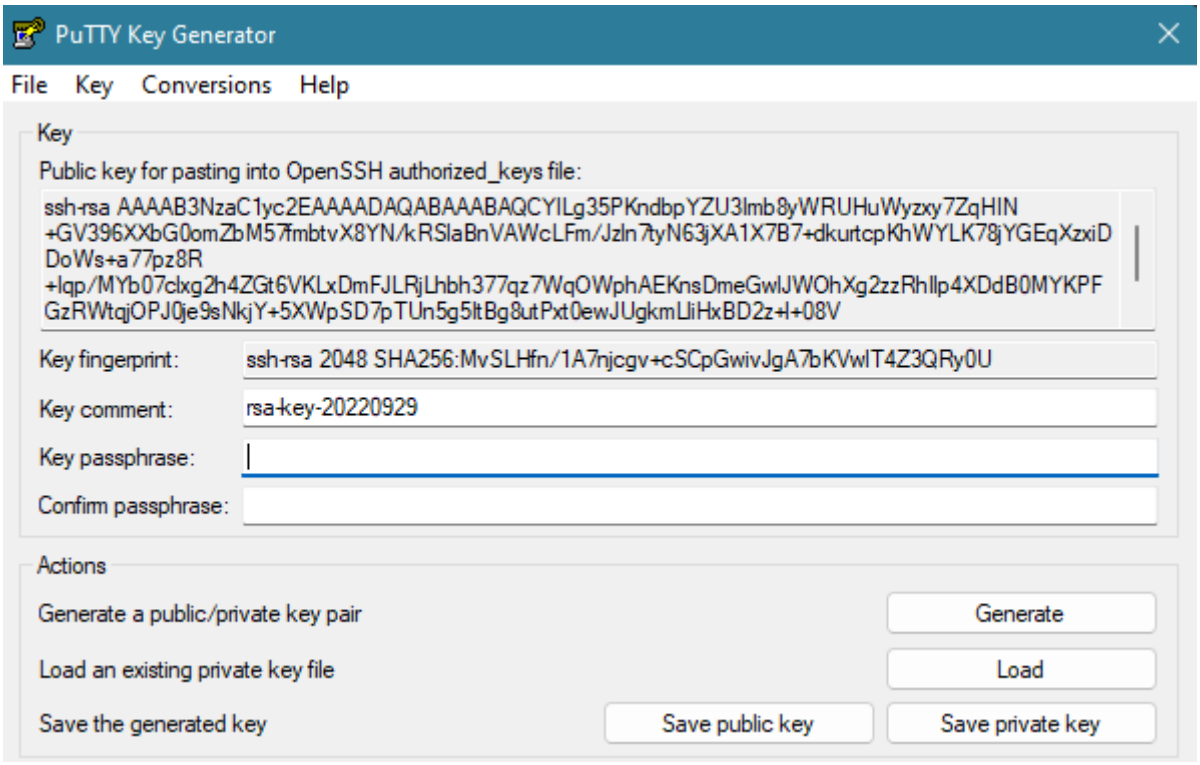
Bouger la souris jusqu'à que la barre de progressions soit arrivé a 100%.



Bravo vous avez créé une clé privé et publique.

> Avant de les enregistrer il est fortement conseillé de mettre une passphrase.

PuTTY Key Generator affiche directement la clé publique a copier et coller sur le serveur de destination.



Pour enregistrer la clé publique Appuyer sur le bouton `Save public key` et donner lui **un nom en .pub** comme l'exemple ci dessous.

Pour enregistrer la clé privé appuyer sur le bouton `Save private key` et donner **un nom en .ppk** a votre clé privé, comme l'exemple ci dessous.

Déployer la clé publique

Le déploiement d'une clé publique

Copier la clé publique sur le serveur

Pour ce faire il existe 2 méthodes différentes.

1) Avec la commande ssh-copy-id

```
ssh-copy-id <username>@<ip.addresse>
```

La sortie :

```
Output
The authenticity of host '203.0.113.1 (203.0.113.1)' can't be established.
ECDSA key fingerprint is fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)?
```

Cela signifie que votre ordinateur local ne reconnaît pas l'hôte distant. Cela se produira la première fois que vous vous connecterez à un nouvel hôte. Tapez "yes" et appuyez sur ENTER pour continuer.

2) Sans la commande

Si vous ne disposez pas de `ssh-copy-id`, mais que vous avez un accès SSH par mot de passe à un compte sur votre serveur, vous pouvez télécharger vos clés à l'aide d'une méthode SSH classique.

Copier le contenu de la clé publique `$SSH_KEY_NAME.pub` qui est sur votre poste pour l’envoyer sur le serveur.

```
# Afficher le contenu de la clé publique
> cat public_key.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCV3UI3s8JmhDR2t1o08bMSp5QarR4pKVxfuqtga73BhwTlF5jgcksjJ5v745HDXD
4zQQcFRbXip1uhLoO3oI98Ak4
/tPp0jJW6jN8s4xZbM89V+AAeoo92na3OwqzJfVsgQEwfbT73IgeUkJNPmDSu7dOCrIsNA7f5RdoYmbsOsWUxS9U8Z/UwZ
trqwqqNm/xOLOLIXh8ZL8hYYvQ0zOvRmt
```

```
kSNlgv4mqbBrpefUCvpZIM+UmvLa2EkxpL23z5NMFBFxPLd9jYEYmC3sPC9fSxsZuQ/Y5R0ElG+JyVn20GqzBeyt/1h332
tyclg5r7aGubVZqlxx3pS1QBvUJN1dnVS
LVl91spHnXmengGZAqVxkHQoPVhTcxsU7sAQrmawdpQNnld906h5LRXACh+bwgsc18Wevtno0rkddCdfgNyZuqBKtzZicA
GIFASZ77i5b83i5frWXpVMnbyFYIKkg6f
WX8YXJVLEE0K9YYf+l6qyh57tzwE586j52rlu465wL0= user@userdemo
```

Une fois le contenu copié :

```
# Se connecter sur le serveur en question
> ssh username@ip.address
# Création du répertoire SEULEMENT Si c'est la première fois
> mkdir .ssh
# Création/Modification du fichier avec les clés publiques
> nano .ssh/authorized_keys
# Coller le contenu de la clé publique $SSH_KEY_NAME.pub dans le fichier "authorized_keys"
```

> Dans le cas ou vous créez le dossier et le fichier avec le super utilisateur vous allez devoir donner les droits à l'utilisateur concerné par ces modifications.

Pour donner les droits au dossier et au fichier il suffit d'exécuter les 2 commandes suivantes :

```
chmod -R go= ~/.ssh
```

et

```
chown -R username:username ~/.ssh
```

Utiliser une clé SSH

Se connecter avec une clé SSH

Pour se connecter avec une clé SSH il suffit de rajouter le paramètre `-i` dans la commande SSH.

```
> ssh -i /chemin/vers/$SSH_KEY_NAME username@ip.address
# Entrer la passphrase
```