

Table des matières

- Manipuler les commandes SSH** 2
 - Générer une clé** 2
 - Ajouter une clé** 2
 - Exporter sa clé** 2
 - Connexion** 3
 - Local 3
 - Distante 3
 - Kill session Fantôme 3
 - PKCS & Yubikey** 3
 - Keys SSH** 4
 - Contrôle de l'agent** 4



Manipuler les commandes SSH

Générer une clé

Vous pouvez faire cela dans 2 formats différents en fonction de la version de ssh sur votre poste.
RSA ou **ed25519**

```
ssh-keygen -t rsa -b 4096 -C "Le_Nom_De_Ma_Clé"
```

Ici, on génère une clé de 4096 bits au format RSA.

```
ssh-keygen -t ed25519 -C "Le_Nom_De_Ma_Clé"
```

Ici, on génère une clé au format ed25519 plus sûres et plus performantes.

Ajouter une clé

Pour ajouter votre clé dans le magasin de votre agent, sur votre poste.

```
ssh-add Le_Nom_De_Ma_Clé
```

Le prompt vous notifiera de l'ajout avec un message success !

Exporter sa clé

Il peut être nécessaire d'enregistrer sa clé sur un serveur distant pour se connecter à celui-ci via sa clé ssh.

Ici aussi, 2 méthodes :

La simple copie de votre clé sur le serveur distant, dans le fichier `.ssh/authorized_keys` du profile avec lequel vous vous connecterez.

L'assistant `ssh-copy-id`:

Ex:

```
ssh-copy-id username@remote_host
```

```
The authenticity of host '111.111.11.111 (111.111.11.111)' 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)? yes
```

Ensuite, l'utilitaire recherchera sur votre compte local la clé `ma_clé.pub` que nous avons créée précédemment. Lorsqu'il trouvera la clé, il vous demandera le mot de passe du compte de l'utilisateur distant;

```
/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  
username@111.111.11.111's password:
```

```
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh 'username@111.111.11.111'"  
and check to make sure that only the key(s) you wanted were added.
```

Connexion

Local

```
ssh user@ip_machine
```

Distante

```
ssh -p 22852 user@mon.domaine.fr
```

Dans ce cas précis, le port est volontairement changé pour le NAT à destination du serveur distant.

Kill session Fantôme

```
who  
pi pts/0 2025-09-20 10:30 (10.60.60.60)  
pi pts/1 2025-09-20 10:29 (10.60.60.65)
```

```
pkill -9 -t pts/0
```

PKCS & Yubikey

Utiliser la Yubikey avec SSH:

Charger le module PAM pour l'utilisation de sa clé RSA avec l'agent SSH:

```
ssh-add -s /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

Décharger le module de l'agent:

```
ssh-add -e /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

Keys SSH

Visualiser sa Clé ssh-rsa:

```
ssh-add -L
```

Contrôle de l'agent

```
eval "$(ssh-agent -s)"
```

From:

<https://wiki.mazinger.fr/wiki/> - My Personal Wiki

Permanent link:

<https://wiki.mazinger.fr/wiki/doku.php?id=linux:commande:shell:ssh>

Last update: **2025/09/20 10:40**

