Documentation Technique **Configuration** SSH avec authentification forte vers une machine **Debian en console** depuis une machine Windows

Creer une machine **Debian** en **mode console**

Installer **Sudo** avec le compte root

```
root@debianssh:/home/cobra# apt install sudo
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
sudo est déjà la version la plus récente (1.9.13p3-1+deb12u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debianssh:/home/cobra#
```

Créer second compte **cobra** et lui donner la possibilité d'**executer** la commande **sudo**

```
root@debianssh:/home/cobra# adduser cobra
```

Tester que le compte **cobra** puisse utiliser **sudo**

```
root@debianssh:/home/cobra# su cobra
cobra@debianssh:~$ sudo apt install vim
[sudo] Mot de passe de cobra :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
vim est déjà la version la plus récente (2:9.0.1378-2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
cobra@debianssh:~$
```

Desactiver la connexion root distante

nano /etc/ssh/sshd_config

Changer de **prohibit-password** à **no**

```
PermitRootLogin no
```

Sur la machine Debian, utiliser la commande "**ssh-keygen -t rsa -b 4096**" pour générer une clé SSH de 4096 octets en utilisant l'algorithme RSA

Recuperer le fichier "**id_rsa**" depuis la machine Windows dans un terminal Powershell

Ex : **scp /home/cobra/.ssh/id_rsa cobra@10.74.3.180 C:\Users\arnau\Desktop\scp**

Sur la machine Debian

Modifier le fichier **sshd_config**

nano /etc/ssh/sshd_config

Ajouter « **.ssh/id_rsa.pub** » à la fin de la ligne **AuthorizedKeysFile**

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

Changer **PasswordAuthentication** « **yes** » à « **no** »

```
PasswordAuthentication no
```

Changer **KbdInteractiveAuthentication** « **no** » à « **yes** »

```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication yes
```

Ajout de la ligne : **ChallengeResponseAuthentication yes**

```
UsePAM yes
ChallengeResponseAuthentication yes
```

Indiquer l'ordre des étapes d'authentification à suivre au début du fichier

```
AuthenticationMethods publickey,password publickey,keyboard-interactive
```