

# PROCEDURE OPEN-SSH

Installation et Configuration d'un serveur SSH : serveur et client, d'une paire clé publique et privée.

Mise en place d'un serveur SSH sur Linux

# **BTS Services Informatiques aux Organisations Option Solutions d'Infrastructure, Systèmes et Réseaux**

**Epreuve E4 : Conception et Maintenance de solutions  
Informatiques.**

## **Documentation technique**

**Projet 2 : Mise en place d'un service SSH pour une connexion client.**



---

## *Sommaire*

---

- Mise en place de l'infrastructure réseaux.....p.4
- Création d'une identité numérique pour les connexions en ssh de comptes utilisateurs en créant une paires de clés (privé et publique) .....p.7
- Passphrase et agent ssh.....p.7
- Configuration du fichier sshd config.....p.8
- Création d'une bannière ssh.....p.9
- Test de la connexion ssh avec une solution mobile (smartphone).....p.10
- La double authentification google.....p.10
- Activer le client SSH intégré à Windows.....p.12

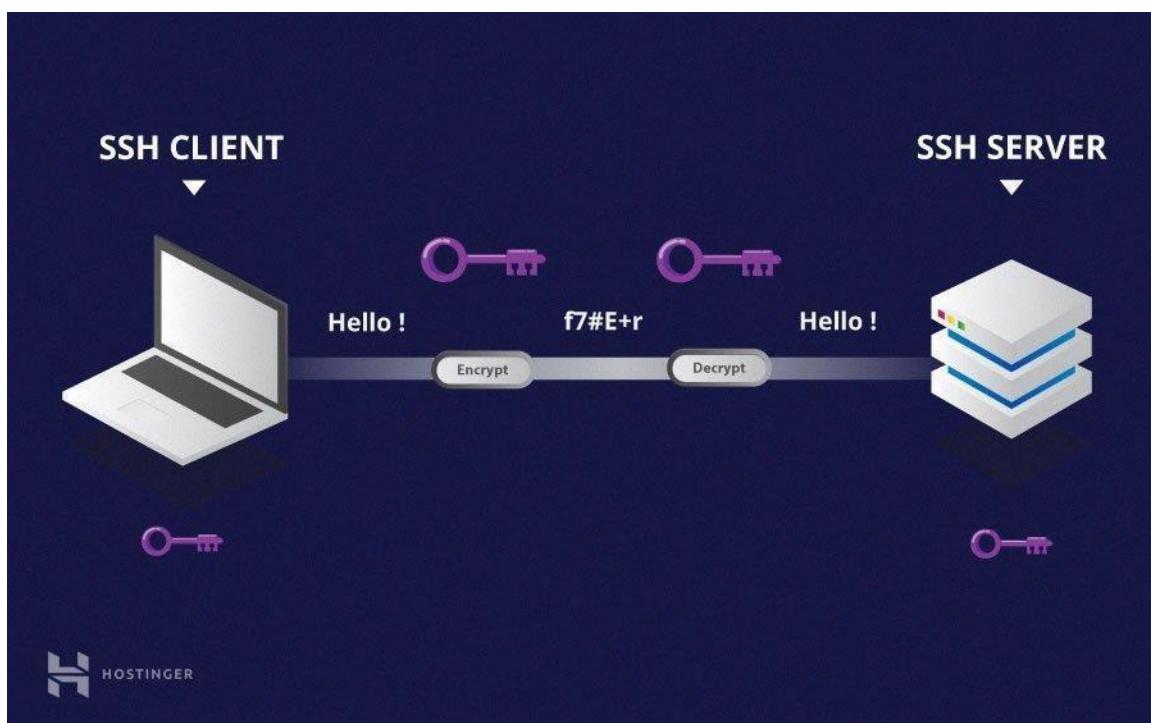
---

## *Introduction*

---

### OpenSSH

OpenSSH est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.



### LVM Crypté

Lorsqu'une partition LVM cryptée est utilisée, la clé de cryptage est stockée dans la mémoire (RAM). ... Si cette partition n'est pas cryptée, le voleur peut accéder à la clé et l'utiliser pour décrypter les données des partitions cryptées. C'est pourquoi, lorsque vous utilisez des partitions chiffrées LVM, il est recommandé de chiffrer également la partition d'échange.

Diminuer les surfaces d'attaques sur nos serveurs et clients SSH :

Nous allons sécuriser le disque dur et les menus de démarrage sur les machines virtuels : Mise en place de l'infrastructure

- Installer les machines virtuelles : 2 Serveurs sous Linux Debian 11, Windows 10, et Smartphone,
- Installation LVM chiffré (Disque dur).

## Installation du serveur Debian 11 sous Linux



Choisir le pays d'emplacement « France »



Choisir la langue du paquet installer en français



Configurer la langue du clavier en français



Les options sont en cours d'installation



## Définir le mot de passe administrateur (root)

Par sécurité, rien n'est affiché pendant la saisie.  
Mot de passe du superutilisateur (« root ») :

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

## Crée un utilisateur

Entrez le nom de l'utilisateur kaiser  
Définir puis confirmer le mot de passe

## Lancement du partitionnement de disque : utiliser le disque en LVM Chiffré

Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

**Assisté - utiliser un disque entier**

Assisté - utiliser tout un disque avec LVM

Assisté - utiliser tout un disque avec LVM chiffré

Manuel

## Appliquer les modifications au disque

 Partitionner les disques

Avant que le gestionnaire de volumes logiques (LVM : « Logical Volume Manager ») puisse être configuré, le schéma actuel de partitionnement doit être appliqué au disque. Ces changements seront irréversibles.

Une fois le gestionnaire de volumes logiques configuré, aucune modification ne peut être apportée, pendant l'installation, aux tables de partitions des disques qui contiennent des volumes physiques. Avant de continuer, veuillez vous assurer que le schéma de partitionnement actuel de ces disques vous convient.

Les tables de partitions des périphériques suivants seront modifiées :  
SCSI1 (0,0,0) (sda)

Écrire les modifications sur les disques et configurer LVM ?

Non

Oui

Les partitions primaires et logiques ont été créées sur le disque



## Configuration du serveur Debian 11 sous Linux

Configuration de la carte réseau du serveur ssh 1 de même pour Windows 10

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file C:\Users\Tooba\Doc...
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Définir le nom du serveur

```
root@debian:~# hostnamectl set-hostname sshserver1
```

Mise à jour du serveur

```
root@debian:~# apt update && apt upgrade
Ign :1 cdrom:///[Debian GNU/Linux 11.2.0 _Bullseye_ - Official
Err :2 cdrom:///[Debian GNU/Linux 11.2.0 _Bullseye_ - Official
      Veuillez utiliser apt-cdrom afin de faire reconnaître ce cédéroms
Réception de :3 http://deb.debian.org/debian bullseye InRelease
Réception de :4 http://security.debian.org/debian-security b...
Réception de :5 http://deb.debian.org/debian bullseye-updates
```

Installer le paquet openssh-server sur le serveur ssh 1

```
root@sshserver1:~# apt install openssh-server
```

Crée l'utilisateur kaiser puis définir son mot de passe

```
root@sshserver1:~# adduser kaiser
```

Création d'une identité numérique de l'utilisateur kaiser

Se rendre dans le dossier .ssh de l'utilisateur kaiser

```
root@sshserver1:~# cd /home/kaiser
root@sshserver1:/home/kaiser# mkdir .ssh
root@sshserver1:/home/kaiser# cd /home/kaiser/.ssh
```

---

### *Définir le nom et le mot de passe de la paire de clés privée et publique ainsi que le Passphrase*

---

```
root@sshserver1:/home/kaiser/.ssh# ssh-keygen -t rsa -b 1024
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): kaiser_rsa
Enter passphrase (empty for no passphrase): _____
Enter same passphrase again: _____
Your identification has been saved in kaiser_rsa
Your public key has been saved in kaiser_rsa.pub
The key fingerprint is:
SHA256:j8ZTh3nVXGeWqd84H4q7AugRGStmY2iZrUDMN2otFKI root@sshserver1
The key's randomart image is:
+---[RSA 1024]---+
|+..          B|
|o= o .      Bo|
|E O . +     o o|
|.O 0 +     o o|
|+ * o o S + o ...
|   o o + o  oo.|
|       * . . . o.|
|       . o . . .|
|           oo|
+---[SHA256]---+
```

---

## *Configuration du fichier SSHD\_CONFIG*

---

Afin d'éviter les attaques de force brute on change le port ssh par défaut

```
root@sshserver1:~# nano /etc/ssh/sshd_config
```

Sur sshserver 1 on change le port 22 en 33

```
Include /etc/ssh/sshd_config.d/*.conf

Port 33
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
allowusers kaiser
LoginGraceTime 1m
PermitRootLogin yes
#StrictModes yes
```

Ctrl + x : enregistrer le fichier sshd\_config > oui

Redémarrer le service sshd : service sshd restart

```
root@sshserver1:~# exit
deconnexion
Connection to 192.168.64.65 closed.
PS C:\Users\Tooba> ssh kaiser@192.168.64.65
ssh: connect to host 192.168.64.65 port 22: Connection refused
PS C:\Users\Tooba> ssh kaiser@192.168.64.65 -p 33
kaiser@192.168.64.65's password:
Linux sshserver1 5.10.0-13-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) 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.
Last login: Thu Apr 21 06:19:27 2022 from 192.168.64.108
kaiser@sshserver1:~$
```

Activation de la clé de l'agent ssh : Se connecter avec l'utilisateur root

```
root@sshserver1:/home/kaiser/.ssh# exec ssh-agent bash
root@sshserver1:/home/kaiser/.ssh# ls
kaiser_rsa  kaiser_rsa.pub
root@sshserver1:/home/kaiser/.ssh# ssh-add kaiser_rsa
Enter passphrase for kaiser_rsa:
Identity added: kaiser_rsa (root@sshserver1)
```

## *Création de la bannière*

Installer le programme figlet pour crée une bannière de connexion SSH

```
root@sshserver1:~# apt install figlet
```

Le fichier de la bannière à bien été crée dans le dossier .ssh de l'utilisateur kaiser

```
root@sshserver1:~# figlet Bienvenu. Connexion SSH Kaiser > /home/kaiser/.ssh/banner
```

`nano /etc/ssh/sshd_config` : Il faut aller chercher le fichier de configuration ssh déclarer le chemin de la bannière enregistrer les modifications (ctrl+x) > oui

```
# no default banner path  
Banner /home/kaiser/.ssh/banner
```

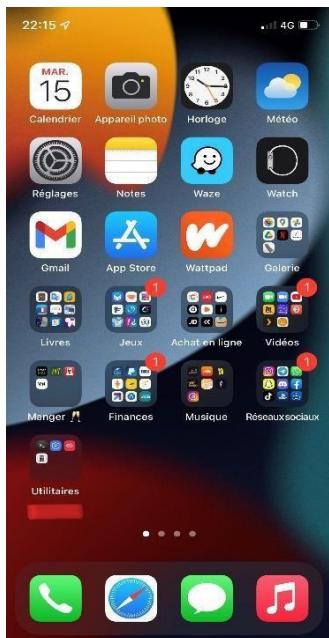
Après redémarrer le service ssh : **service ssh restart**

#### Vérification du contenu de la bannière

## Connexion avec une solution mobile

Sur le serveur ssh1 avec l'utilisateur kaiser

Vérification de l'emprunt numérique > enter le mot de passe > connexion réussie



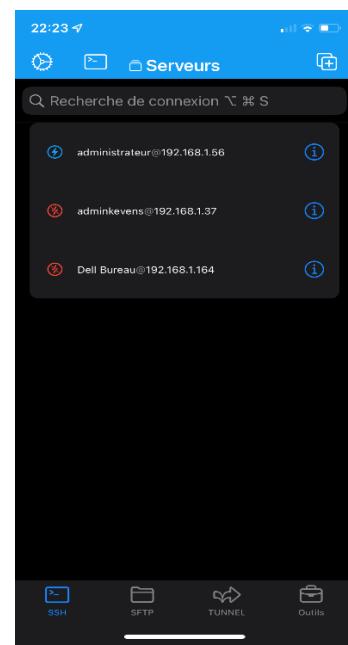
Sur mon téléphone



Télécharger apk WebSSH



Entrez l'adresse IP et le port du serveur  
Avec le nom et le mot utilisateur.



Le serveur SSH apparaitre.



Voilà ! vous êtes connectée sur votre serveur SSH.

---

## Double authentification google

---

Installation du google authentificateur :

```
apt install libpam-google-authenticator
```

Se rendre pour modifier le fichier sshd de la double authentification

```
nano /etc/pam.d/sshd
```

Ajouter 2 lignes à la fin du fichier

```
# authentification google  
auth required pam_google_authenticator.so|
```

Ctrl X + yes

Rédemarre le service : service sshd restart ou systemctl restart sshd

Généré le QRCode de la double authentification google

```
root@sshserver1:~# google-authenticator
```

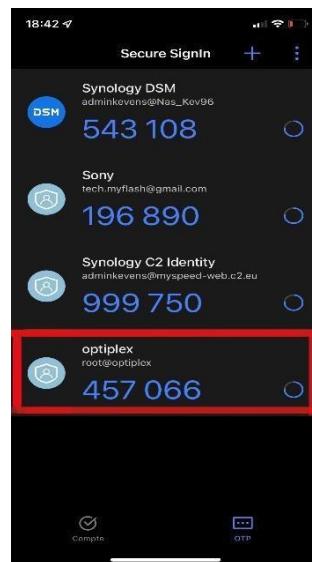


## Questions de renforcement de la sécurité authentifiée

```
Your new secret key is: 4RCOU5A2IB37J6BWCZRC5SEFA
Enter code from app (-1 to skip): 918038
Code confirmed
Your emergency scratch codes are:
43263684
38579593
98493906
92047573
28480205
Do you want me to update your "/root/.google_authenticator" file? (y/n) Y
Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) Y
By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) Y
If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) Y
```

## Test de la double authentification en root.

Dans un premier temps il faut installer Secure Signin sur votre téléphone.

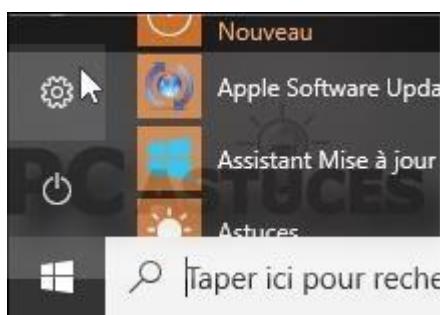


Et puis se connecter sur le serveur SSH en root, entrez le mot de passe root. Il va vous demander de vérification code de double authentification sur ton téléphone vous prenez le code à 6 chiffres.

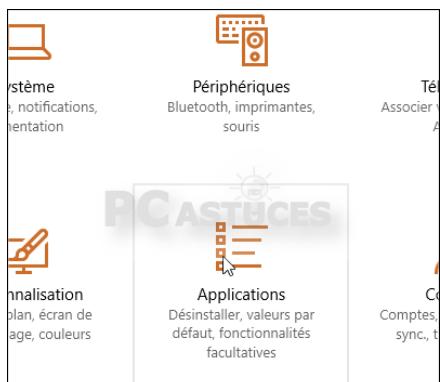
## Activer le client SSH intégré à Windows

Depuis la mise à jour Fall Creators Update, Windows intègre un client OpenSSH vous permettant de vous connecter à un serveur Secure Shell. Plus besoin donc de passer par un utilitaire tiers comme Putty.

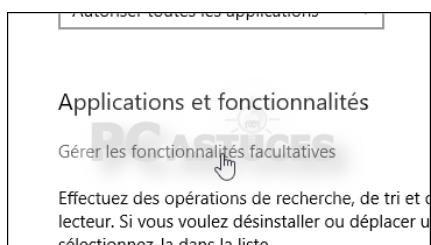
1. Le client SSH est disponible en tant qu'option et n'est pas installé par défaut. Pour l'installer, cliquez sur le bouton **Démarrer** puis sur **Paramètres**.



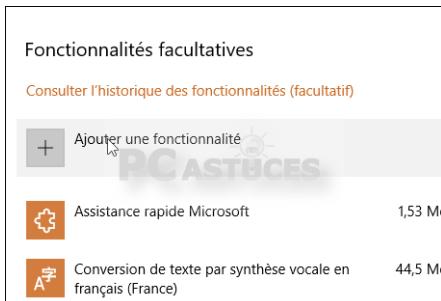
2. Cliquez sur **Applications**.



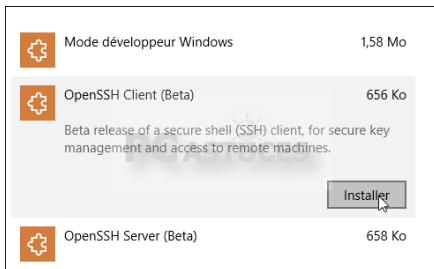
3. Cliquez sur **Gérer les fonctionnalités facultatives**.



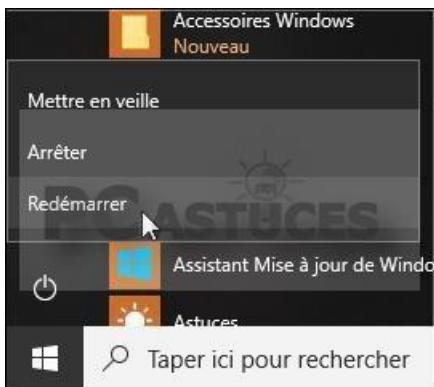
4. Cliquez sur **Ajouter une fonctionnalité**.



5. Cliquez sur **OpenSSH Client (Beta)** puis cliquez sur le bouton **Installer**.



6. Redémarrez votre ordinateur.



7. Vous pouvez désormais utiliser le client SSH en utilisant la commande **ssh** dans une fenêtre PowerShell ou d'Invite de commandes. Saisissez la commande et validez par **Entrée** pour connaître la syntaxe de la commande.

```
Sélection Invite de commandes
Microsoft Windows [version 10.0.16299.125]
c) 2017 Microsoft Corporation. Tous droits réservés.

:\Users\Clément>ssh
sage: ssh [-46Aacf8KKMNnqsTtvVxxYy] [-b bind_address] [-c cipher_spec]
      [-D [bind_address]:]port] [-E log_file] [-e escape_char]
      [-F configfile] [-i pkcs11] [-i identity_file]
      [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
      [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
      [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
      [user@]hostname [command]

:\Users\Clément>
```

8. Les options et la syntaxe sont les mêmes que la commande ssh sous Linux ou MacOS.

```
C:\Users\Clément>ssh 192.168.1.29
The authenticity of host '192.168.1.29 (192.168.1.29)' can't be established.
ED25519 key fingerprint is SHA256:a5Wjvh8MezGvgf3X6t6xdwBL2DnEfylRhnc2+OfcQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.29' (ED25519) to the list of known hosts.
Clément@DESKTOP-HF5QKQP:~192.168.1.29's password: -
```