

Amine ATMANI BTS SIO

RAPPORT AP4

Si votre serveur a internet, deux méthodes pour installer OpenSSH, soit via la commande powershell suivante :

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

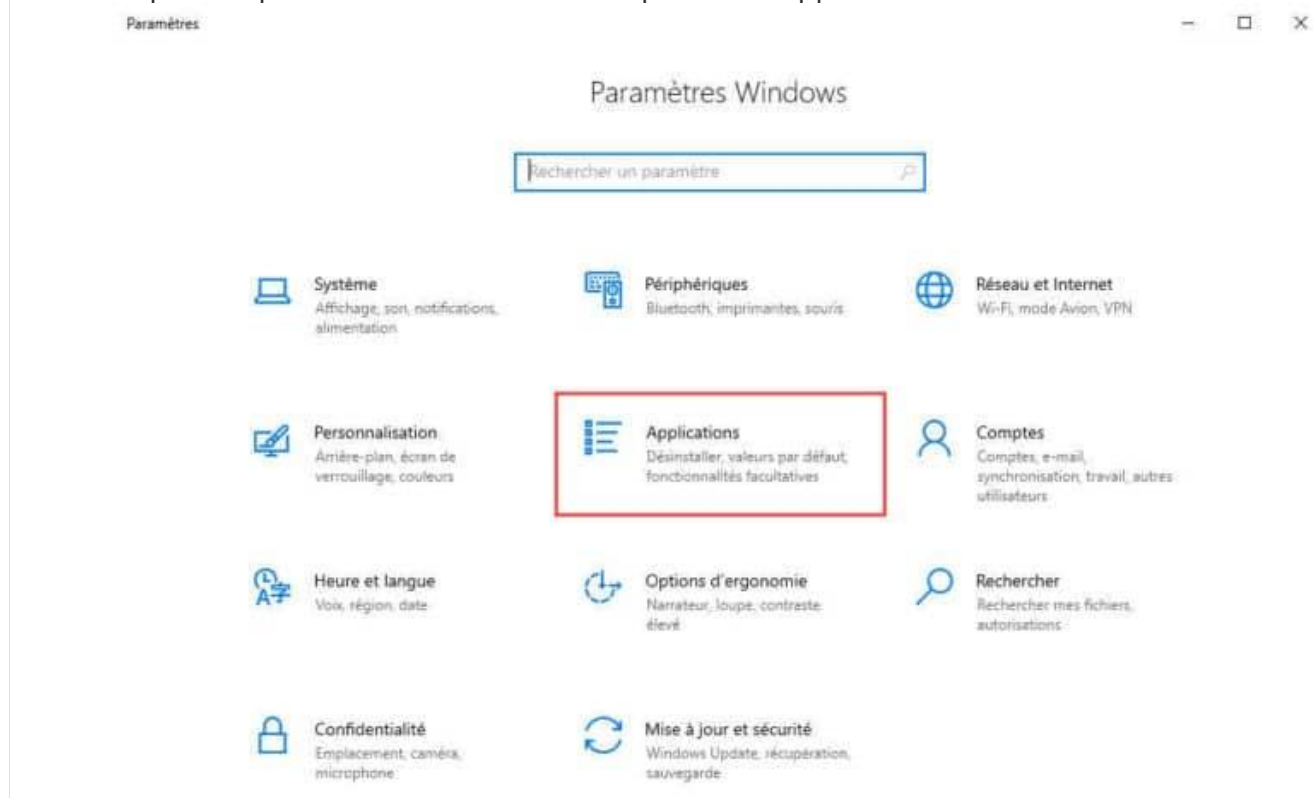
```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows
PS C:\Users\Administrateur> Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

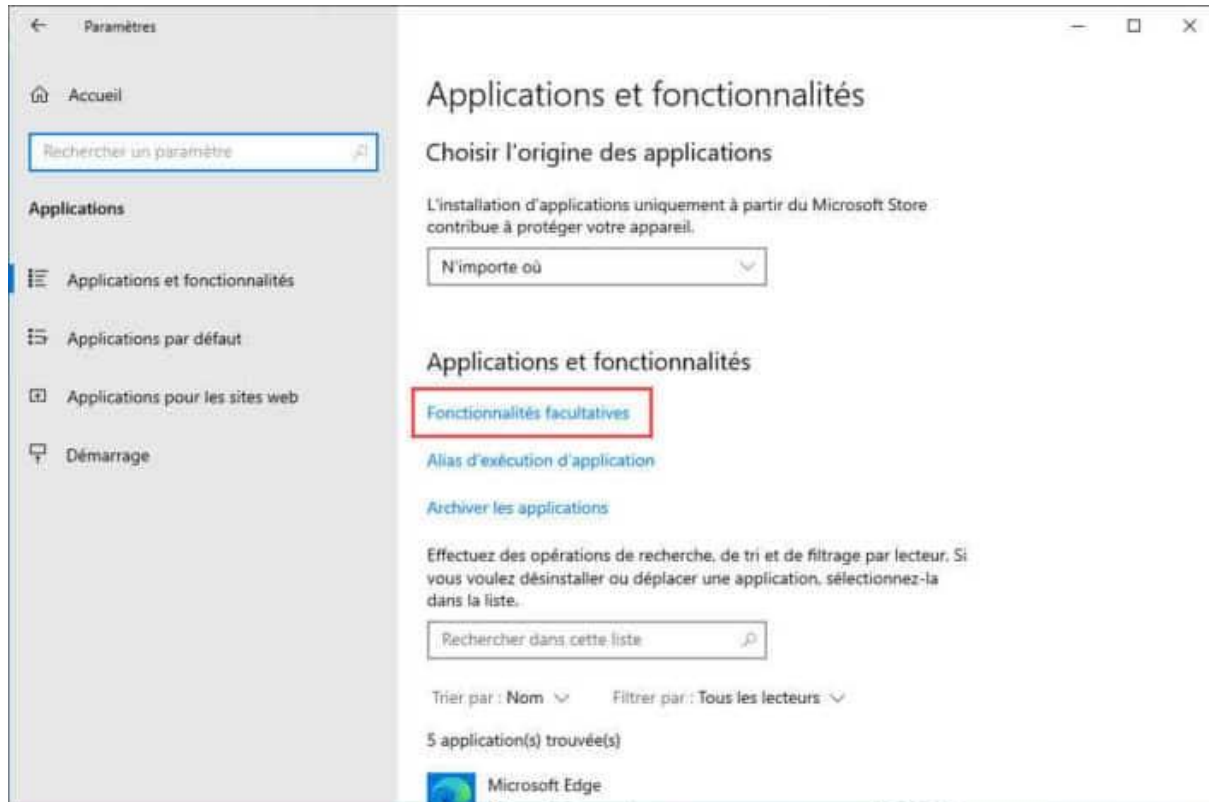
Path      :
Online    : True
RestartNeeded : False
```

Soit directement depuis les paramètres de Windows :

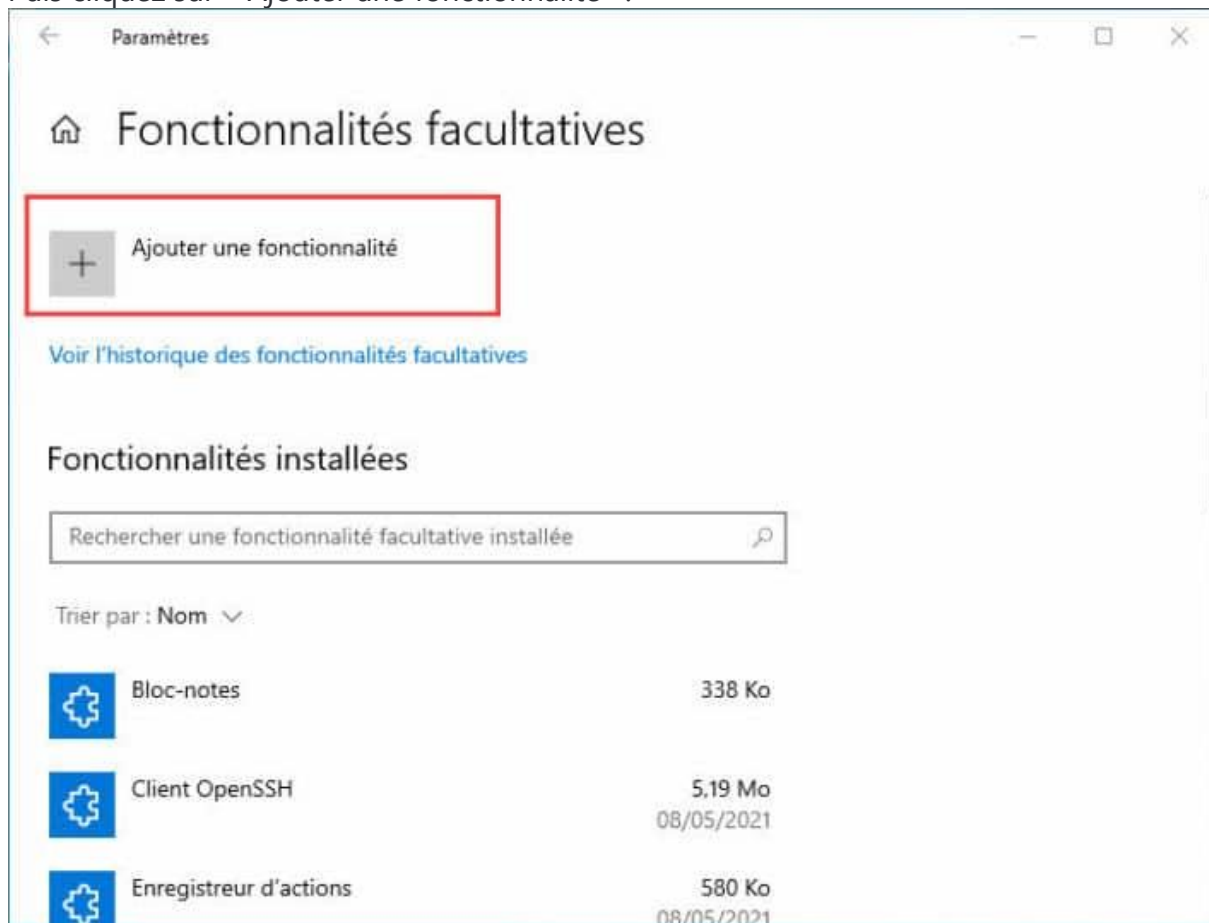
1. Depuis les paramètres de Windows, cliquez sur « Applications ».



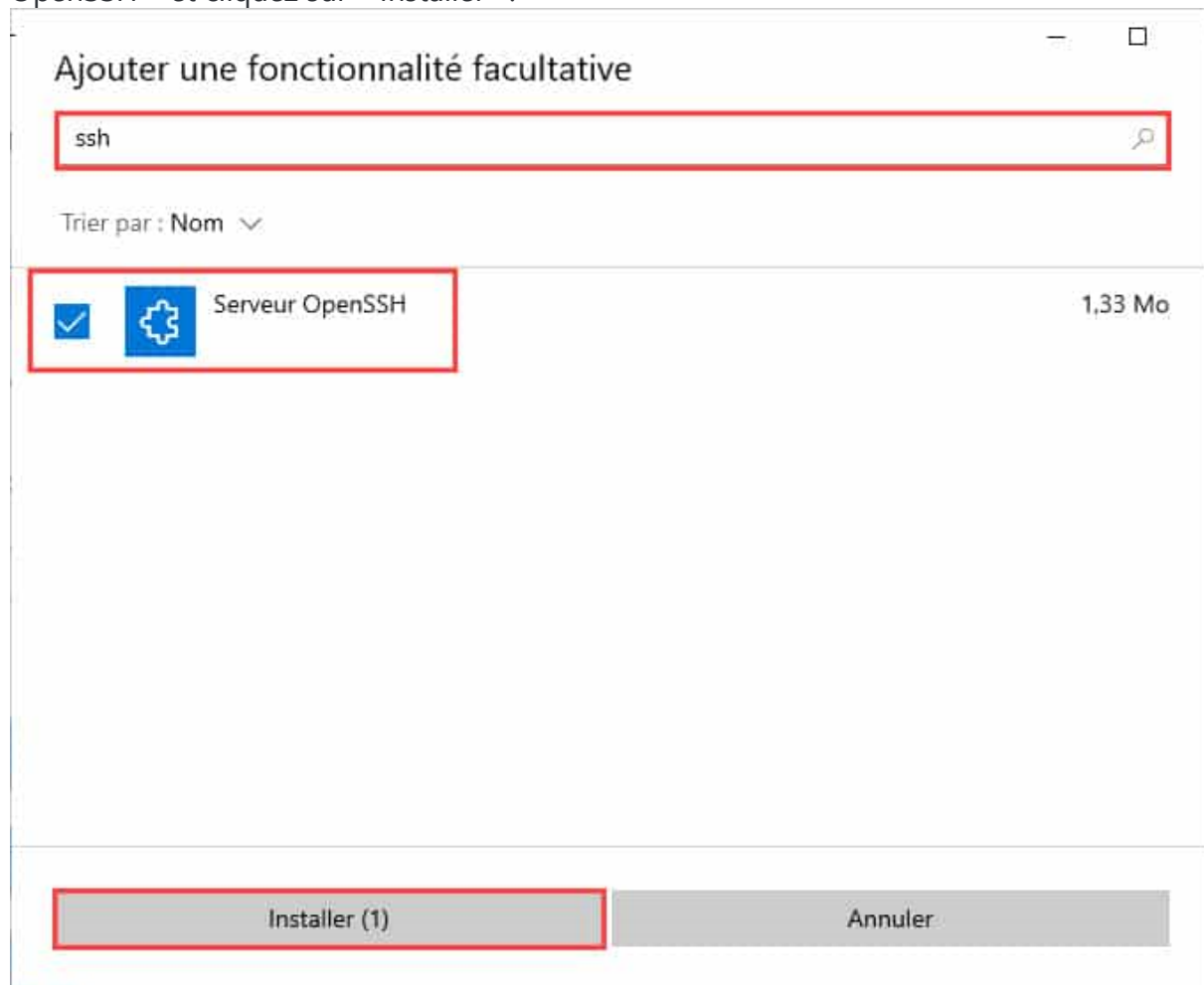
2. Sélectionnez « Fonctionnalités facultatives ».



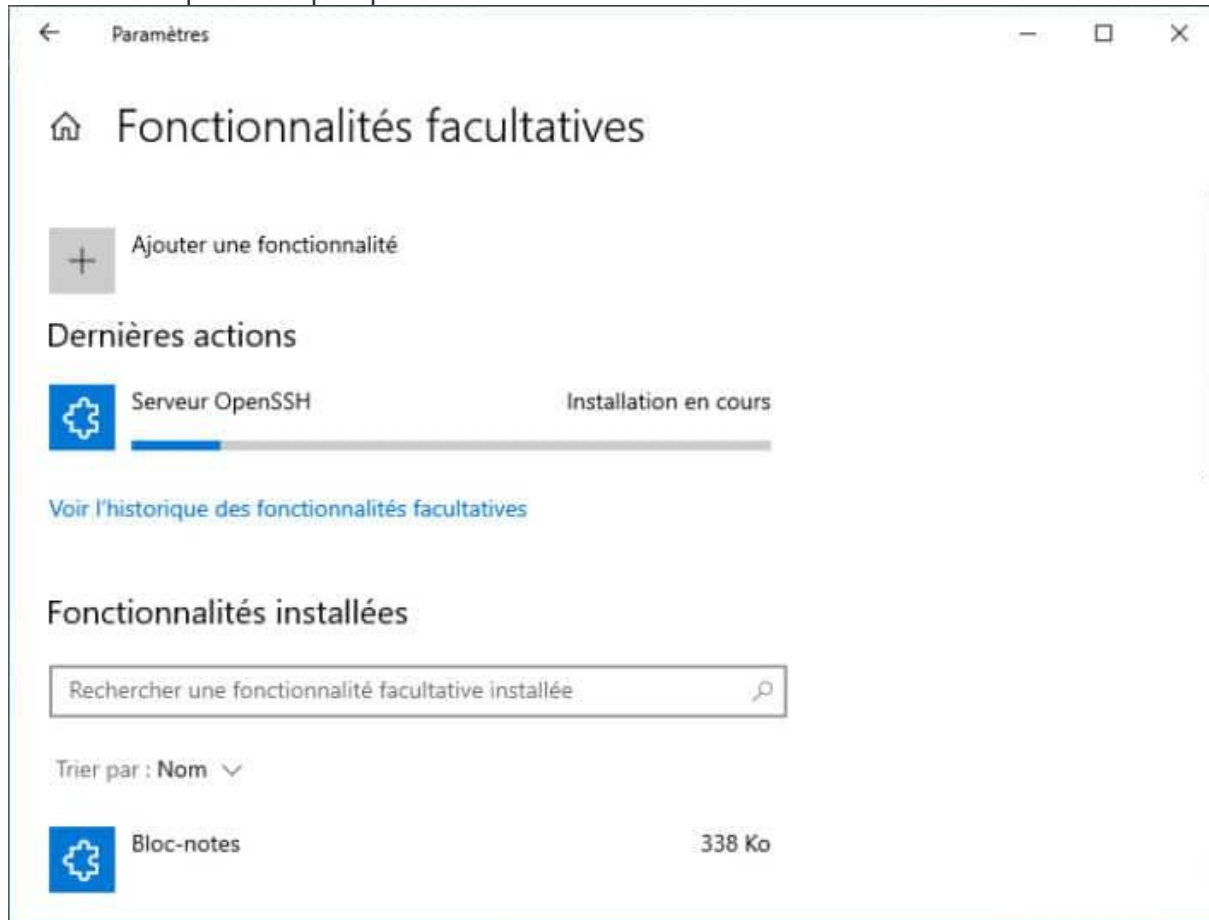
3. Puis cliquez sur « Ajouter une fonctionnalité ».



4. Dans la zone de recherche, tapez « SSH », puis sélectionnez « Serveur OpenSSH » et cliquez sur « Installer ».



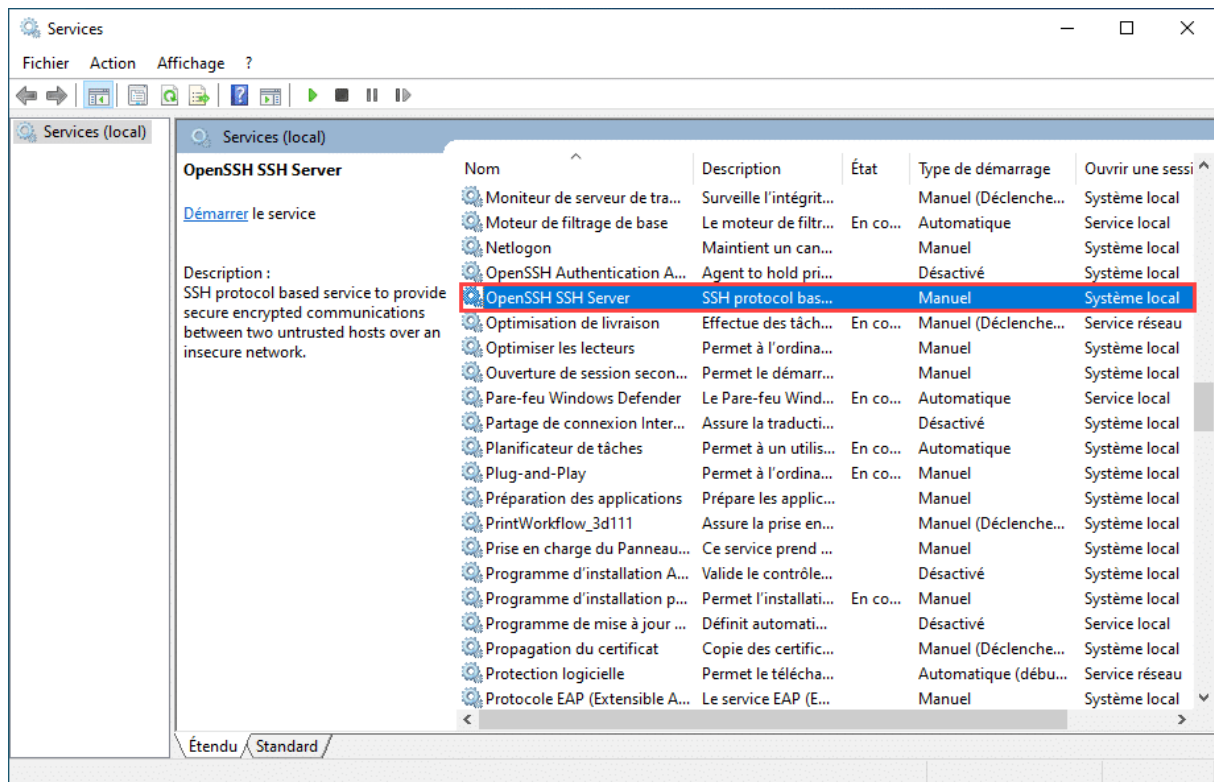
5. L'installation prendra quelques secondes.



Maintenant que le serveur OpenSSH est installé. Nous allons pouvoir parler de la configuration.

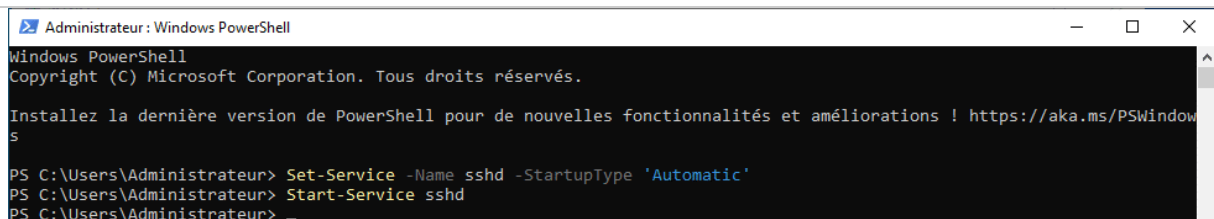
Configuration SFTP avec OpenSSH Serveur.

Maintenant que OpenSSH Server est installé, un nouveau service est disponible. Cependant, par défaut, il n'est pas démarré et pas en automatique non plus.



Cela signifie qu'il ne sera pas démarré automatiquement avec Windows. Dans mon cas, je souhaite démarrer le service et de faire en sorte qu'il démarre automatiquement avec Windows. Nous pouvons le faire directement depuis le service lui-même ou encore via powershell via les commandes suivantes :

```
Set-Service -Name sshd -StartupType 'Automatic'
Start-Service sshd
```



Puisque nous sommes sous Powershell, profitons-en pour ouvrir également le port 22, port par défaut du SSH et donc de notre SFTP. Attention, si vous souhaitez faire tourner votre serveur SFTP sur un autre port, alors adapter la commande. Ici on ouvre le port 22 sur le pare-feu de Windows :

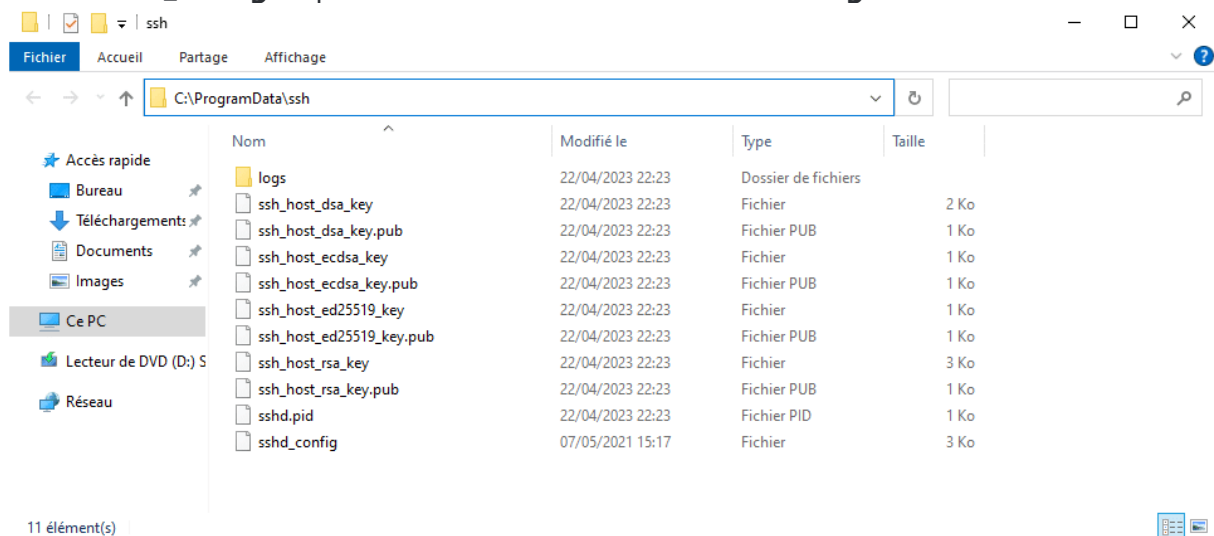
```
New-NetFirewallRule -Protocol TCP -LocalPort 22 -Direction Inbound -Action Allow -DisplayName SSH
```

```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\Administrateur> Start-Service sshd
PS C:\Users\Administrateur> New-NetFirewallRule -Protocol TCP -LocalPort 22 -Direction Inbound -Action Allow -DisplayName SSH

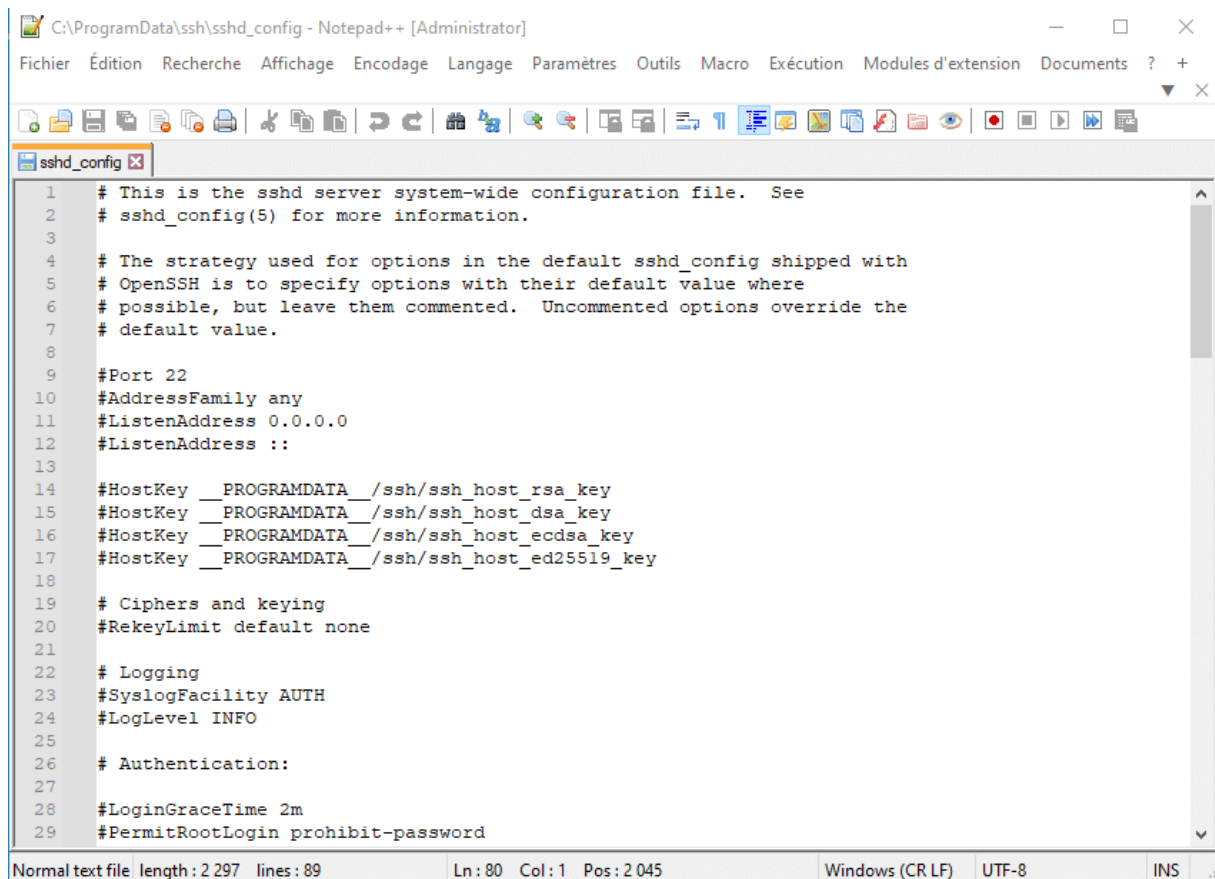
Name                               : {07c7197c-0d0a-4caa-ad31-f5e4d9461fcb}
DisplayName                        : SSH
Description                       :
DisplayGroup                      :
Group                             :
Enabled                           : True
Profile                           : Any
Platform                         : {}
Direction                        : Inbound
Action                            : Allow
EdgeTraversalPolicy               : Block
LooseSourceMapping               : False
LocalOnlyMapping                 : False
Owner                             :
PrimaryStatus                    : OK
Status                           : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus                : NotApplicable
PolicyStoreSource                : PersistentStore
PolicyStoreSourceType            : Local
RemoteDynamicKeywordAddresses    : {}

PS C:\Users\Administrateur>
```

Maintenant que notre serveur OpenSSH est démarré et autorisé sur le parefeu, nous allons le configurer en fonction de nos besoins. Pour cela, tout se passe sur le fichier **sshd_config** disponible dans le dossier suivant : **C:\ProgramData\ssh**



Éditer le fichier **sshd_config** avec votre éditeur préféré. Dans mon cas, notepad++.



```
1 # This is the sshd server system-wide configuration file. See
2 # sshd_config(5) for more information.
3
4 # The strategy used for options in the default sshd_config shipped with
5 # OpenSSH is to specify options with their default value where
6 # possible, but leave them commented. Uncommented options override the
7 # default value.
8
9 #Port 22
10 #AddressFamily any
11 #ListenAddress 0.0.0.0
12 #ListenAddress ::
13
14 #HostKey _PROGRAMDATA_/ssh/ssh_host_rsa_key
15 #HostKey _PROGRAMDATA_/ssh/ssh_host_dsa_key
16 #HostKey _PROGRAMDATA_/ssh/ssh_host_ecdsa_key
17 #HostKey _PROGRAMDATA_/ssh/ssh_host_ed25519_key
18
19 # Ciphers and keying
20 #RekeyLimit default none
21
22 # Logging
23 #SyslogFacility AUTH
24 #LogLevel INFO
25
26 # Authentication:
27
28 #LoginGraceTime 2m
29 #PermitRootLogin prohibit-password
```

Ici nous verrons ensemble les principaux paramètres que vous pourriez être en mesure de modifier.

Changement de port

#Port 22 : Ici, vous pouvez décommenter cette ligne pour changer le port par défaut pas celui que vous voulez (adapter alors la configuration de votre pare-feu en conséquence)

Autorisation de connexion

Il y a plusieurs méthodes pour autoriser une connexion sur votre serveur. Dans mon cas, j'utilise un group dédié aux SFTP, ainsi, tous les utilisateurs de ce groupe peuvent s'y connecter. J'ajoute donc la ligne suivante au fichier de configuration :

```
AllowGroups domain\sftp_users
```

Changer le dossier par défaut

Le dossier par défaut est le dossier racine du profil utilisateur, si ce n'est pas votre souhait, alors vous pouvez tout à fait changer ce dossier via la commande suivante :


```
ChrootDirectory C:\SFTP
```

Si vous préférez faire un dossier spécifique par utilisateur, c'est également possible en ajouter les lignes suivantes :

```
Match User utilisateur1
ChrootDirectory c:\SFTP\utilisateur1
ForceCommand internal-sftp
X11Forwarding no
AllowTcpForwarding no
```

```
Match User utilisateur2
ChrootDirectory c:\SFTP\utilisateur2
ForceCommand internal-sftp
X11Forwarding no
AllowTcpForwarding no
```

Supprimer l'accès root / administrateur

Si vous souhaitez supprimer l'accès au groupe administrateur local par mesure de sécurité, il faudra commenter les lignes suivantes (à la fin du fichier de configuration) :

```
#Match Group administrators
#   AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

puis ajouter la ligne suivante :

```
DenyGroups administrateurs
```

Une fois votre configuration terminée, enregistrer le fichier puis redémarrer le service openSSH server pour que le fichier de configuration soit lu à nouveau et appliqué. Vous pouvez le faire depuis le gestionnaire de services ou via powershell en utilisant la commande suivante :

```
Restart-Service "sshd"
```

Et voilà ! Vous savez maintenant comment configurer un serveur SFTP sous Windows. Vous pouvez tester ça avec n'importe quel client SFTP.

