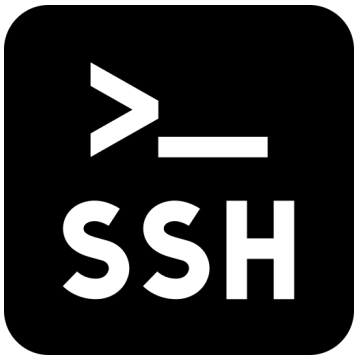
Gallimedia
agence digitale

Documentation interne : Mettre en place une connexion SSH sous Windows.



https://gallimedia.com/
Auteur : Mathieu Morgat

I - Sommaire

II - Présentation du protocole SSH

Description : Le protocole SSH désignant Secure Shell permet la connexion distante à une autre machine de façon sécurisée.

SSH met a disposition un terminal Shell sécurisé qui permet de lancer des commandes comme si l'on étais sur l'ordinateur distant, sans avoir à être sur place. Il possède aussi un protocole de transfert de fichiers sécurisé.

Ce protocole fut créé pour la communication entre machines Linux ou Unix, mais on peut l'utiliser sous Windows via le CMD ou Powershell avec OpenSSH, ainsi que différents logiciels/émulateurs de terminaux tel que PuTTY ou Cygwin. Par défaut, il utilise le port ordinateur 22.

Les liaisons SSH sont sécurisées et l'authentification à la machine distante requiert un login, ainsi qu'un mot de passe. De plus, l'utilisation de clés de chiffrement permet une meilleure authentification et ainsi de mieux restreindre les accès.

Ce protocole est très répandu, et est souvent mis en parallèle avec des protocoles tel que SCP ou SFTP pour interagir avec une machine distante.

III - Mettre en place une connexion SSH sous Windows avec CMD

Description: Le CMD ou Invite de commande est un terminal qui permet de lancer des commandes sous Windows, ou d'exécuter des scripts. Il est l'équivalent Windows du Shell Unix, il possède quelques commandes en commun, mais il est moins puissant et plus basique. Powershell quand à lui possède beaucoup de fonctionnalités en commun avec les terminaux Unix. OpenSSH est une fonctionnalité Windows qui permet d'utiliser le protocole SSH. Pour utiliser OpenSSH sous Windows, nous pouvons utiliser le CMD ou Windows Powershell.

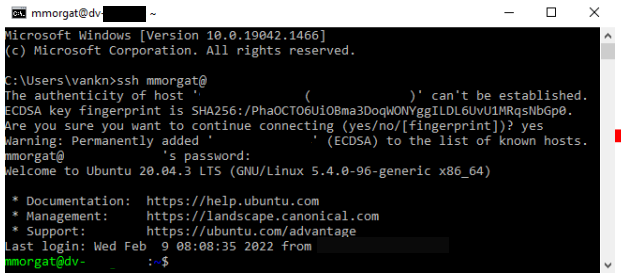
1. OpenSSH est une fonctionnalité Windows installée par défaut. Si elle ne fonctionne pas, allez voir l'étape annexe 5.

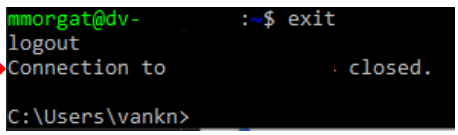
Pour lancer une simple connexion SSH, il faut lancer la commande ssh avec la syntaxe suivante dans le terminal :
ssh <identifiant>@<serveur>

A noter : Si vous êtes sûr d'avoir le bon mot de passe mais qu'il est refusé, passez à l'étape 2. pour ajouter une clé d'authentification.

Lors de la première connexion, un message vous demandera si vous souhaitez ajouter la machine distante dans la liste des hôtes connus, tapez « yes ». Ensuite vous devrez taper votre mot de passe Linux afin de vous connecter. (1)
Vous pouvez maintenant fermer la connexion en tapant « exit » (2).

(1)





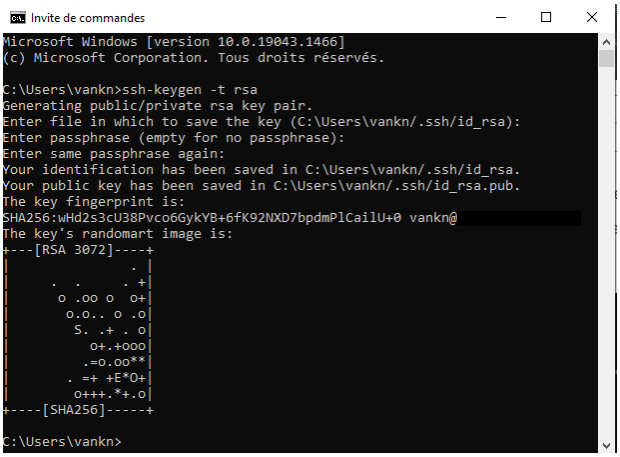
(2)

2. Pour mettre en place une clé RSA, il faut utiliser la commande :
ssh-keygen -t rsa

Si l'algorithme rsa n'est plus approprié pour le serveur voulu, votre administrateur réseau vous dira quel algorithme vous devrez utiliser. L'emplacement et le nom de la clé vous seront demandés, puis vous devrez créer un passphrase et le confirmer. **Il est obligatoire de créer un passphrase lors de la création d'une clé.** Il garanti que la connexion provient de vous. Vous ne serez donc pas responsable en cas d'utilisation non autorisée de votre compte.

Le « randomart » de la clé sera affiché, il ne s'agit que d'un outil pour visuellement faciliter la vérification de clé.

III - Mettre en place une connexion SSH sous Windows avec CMD



Résultat de la commande ssh key-gen

Il vous faudra maintenant envoyer le fichier id_rsa.pub présent dans le dossier C:/users/<votre nom>/.ssh/ à votre administrateur système, afin de l'ajouter dans les clés autorisées sur la machine distante.
Lors de votre prochaine connexion, votre passphrase sera demandé.

3. Pour écrire une seule fois votre passphrase, vous pouvez utiliser ssh-agent.
Il est nécessaire d'utiliser Powershell en tant que administrateur, pour utiliser les commandes suivantes :

Get-Service ssh-agent | Set-Service -StartupType Manual
(Permet de lancer ssh-agent)
Start-Service ssh-agent
ssh-add C:/users/<votre nom>/.ssh/id_rsa
(Ajoute la clé à ssh-agent)

```
C:\Users\vankn>ssh-add
Enter passphrase for C:\Users\vankn/.ssh/id_rsa:
Identity added: C:\Users\vankn/.ssh/id_rsa (vankn@                )
```

Après avoir entré votre passphrase, vous n'aurez plus à le taper lors de vos prochaines connexions aux machines distantes qui utilisent cette clé.

4. Pour spécifier un port de lecture lors de la connexion, il faut utiliser l'option -p suivit du numéro de port lors de la tentative de connexion avec la commande ssh.
Exemple avec une connection sur un mauvais port :

```
C:\Users\vankn>ssh -p 8080 mmorgat@
ssh: connect to host                port 8080: Connection timed out
```

III - Mettre en place une connexion SSH sous Windows avec CMD

5. Si la commande ssh ne fonctionne pas, il est possible de l'installer de deux manières :

-Sous Windows 10 en tant que compte administrateur, il faut aller dans :

Applications>Fonctionnalités facultatives.

Si OpenSSH n'est pas présent, appuyez sur « Ajouter une fonctionnalité».

Il faut ensuite entrer « openSSH » dans le champ de recherche et ajouter le Client OpenSSH.

-Pour toute les version Windows, il faut utiliser le logiciel Windows PowerShell. Tout d'abord, vérifiez si OpenSSH est installé grâce à la commande :

Get-WindowsCapability -Online | Where{ $_.Name -like 'OpenSSH.Client*' }

Si il n'est pas installé, faites la commande :

Add-WindowsCapability -Online -Name OpenSSH.Client

IV - Mettre en place une connexion SSH sous Windows avec PuTTY

Description: PuTTY est un logiciel open source gratuit de connexion SSH, qui permet beaucoup de flexibilité au niveau de ses paramètres et qui est facile à prendre en main. En plus de ses fonctionnalités SSH, il permet de faire des transferts SFTP ainsi que de créer des paires de clés privées/publiques.

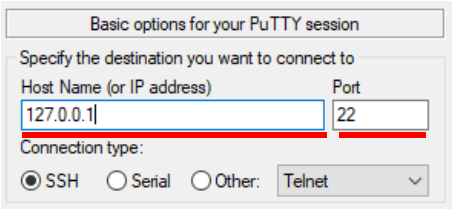
1. Pour télécharger le logiciel PuTTY, il faut se rendre sur la page officielle : https://www.putty.org/
Sur la page de téléchargement, il faut choisir : putty-64bit-0.76-installer.msi

2. Lors de l'installation de PuTTY, les seules options importantes sont le dossier d'installation par défaut que l'on peut changer et la création des raccourcis bureau désactivé par défaut.

Après avoir installé PuTTY, vous aurez quatre nouveaux exécutables :
-PuTTY client SSH.
-PuTTYgen générateur de paire de clés.
-PSFTP client SFTP.
-Pageant client d'authentification via clé privée.

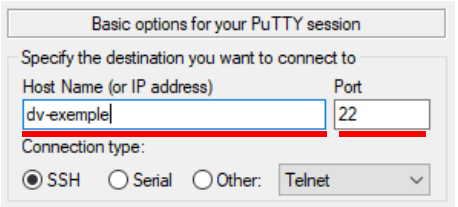
Nous allons nous concentrer sur PuTTY puis sur PuTTYgen.

3. Pour une simple connexion vers un appareil local ou distant, il faut changer le champ « Host Name ».
Il est possible de mettre l'adresse IP de la machine, ou bien le nom de la machine (Hostname).



Dans la première image, l'adresse IP correspond à la machine « dv-exemple » sous Ubuntu.

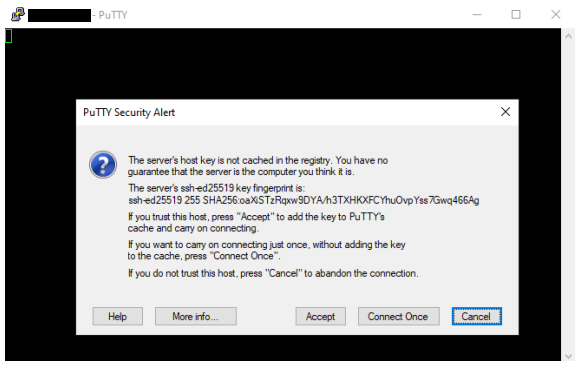
Dans la seconde image, « dv-exemple » est le hostname de la machine distante que nous souhaitons contrôler.



Il faut ensuite appuyer sur le bouton « Open » en bas de la fenêtre afin de lancer une connexion vers la machine voulue.

A noter : Le port d'écoute de base de SSH est le port 22, si vous devez utiliser un port spécifique, il vous faut le changer dans le champ « Port ».

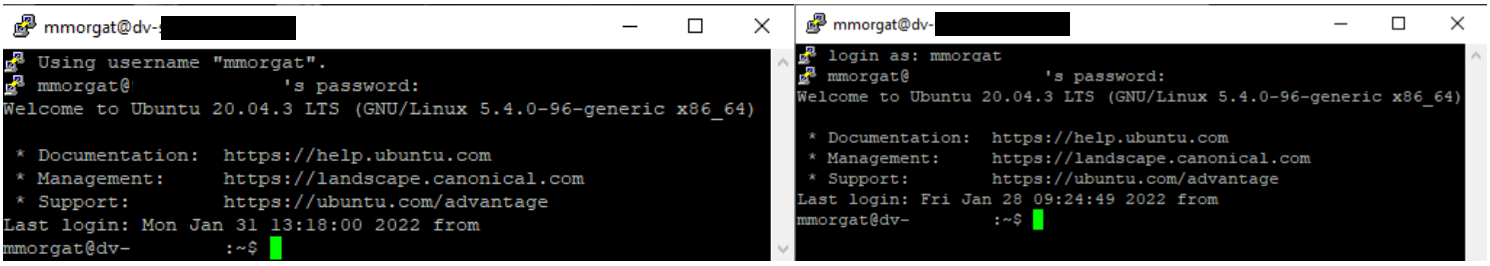
4. Après l'ouverture d'une connexion, un terminal SSH va s'ouvrir. Un message d'avertissement apparaîtra, il faudra appuyer sur « Accept », afin d'enregistrer la machine distante dans la Cache de PuTTY, si il s'agit bien de la machine que vous souhaitez accéder.



IV - Mettre en place une connexion SSH sous Windows avec PuTTY

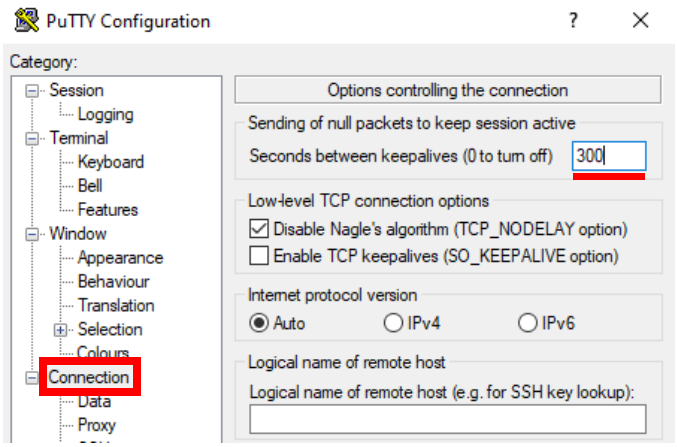
Après avoir accepté, la fenêtre SSH demandera un identifiant pour se connecter sur la machine, puis un mot de passe.

Exemples dans les deux cas de figure vus précédemment :



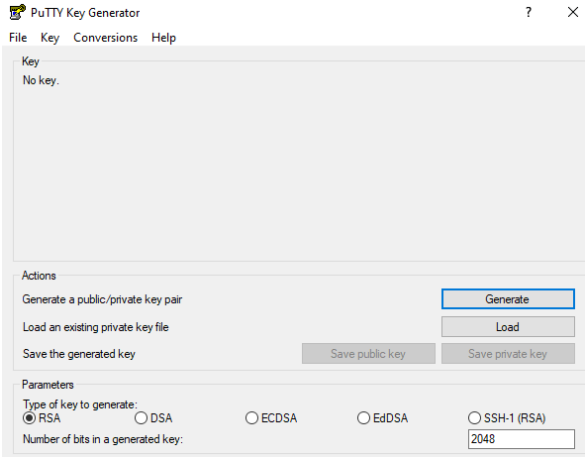
On peut maintenant fermer la connexion en tapant « exit » dans cette fenêtre.
Lorsque la machine n'est pas sur le réseau local, des déconnections intempestives peuvent avoir lieu et bloquent la fenêtre SSH ou ferment la connexion lors d'inactivité / instabilité de connexion.

Pour y remédier, il faut retourner dans le panneau de configuration et ouvrir la catégorie « Connection », je conseille de mettre 300 dans le premier champ « Keepalives » :

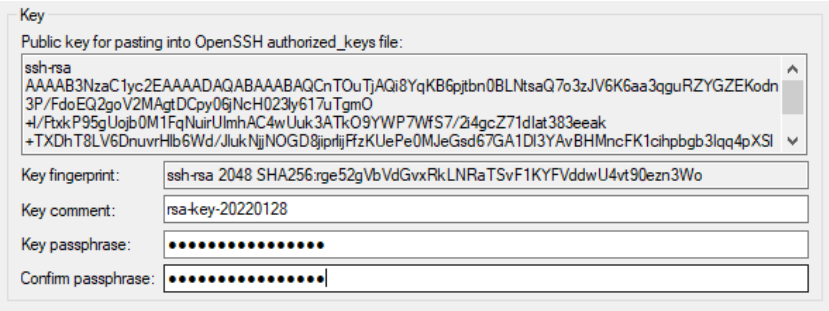


5. Maintenant qu'une connexion sommaire a été établie, nous allons voir comment créer une clé RSA avec une passphrase, utilisée lors de la connexion et l'authentification vers la machine.

Nous allons lancer le logiciel PuTTYgen afin de créer une clé Publique et une clé Privée.
Il faut appuyer sur le bouton « Generate » et bouger la souris, afin de générer la clé.



IV - Mettre en place une connexion SSH sous Windows avec PuTTY

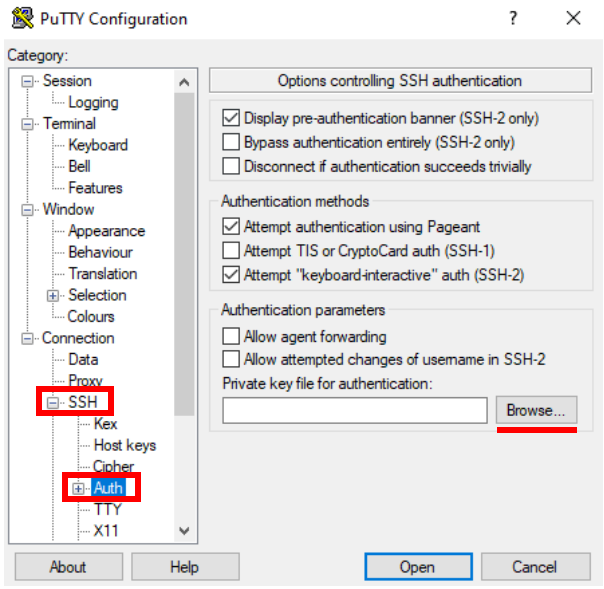


Maintenant que la paire de clés a été créée, vous pouvez lui assigner un passphrase qui vous sera demandé à la place de votre mot de passe Linux. Vous pouvez maintenant enregistrer les deux clés avec « Save public key » et « Save private key ».

-Pour la clé publique, un fichier texte sans extension sera créé. Vous pourrez l'envoyer à un administrateur système, afin de l'ajouter dans les clés autorisées sur la machine distante.

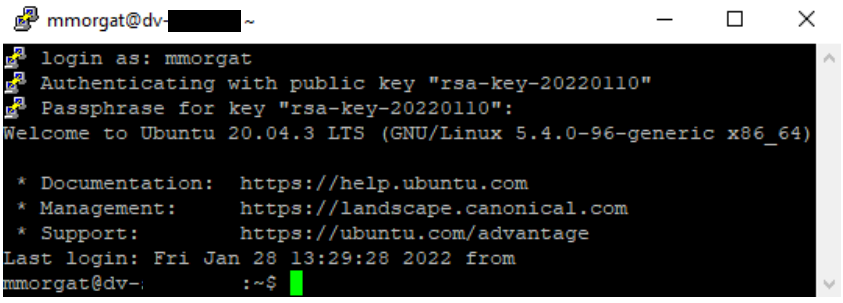
-Pour la clé privée, un fichier propre à PuTTY de type .ppk sera créé.
Pour que PuTTY prenne en compte cette clé lors d'une connexion, nous allons retourner sur PuTTY et ouvrir la sous-catégorie « Auth » dans « SSH » :

6. Dans cette sous-catégorie, nous allons appuyer sur le bouton « Browse » et nous allons sélectionner la clé privée .ppk que nous venons de générer.
De cette manière, elle sera prise en compte lors de la prochaine connexion SSH.



Si l'on relance la connexion vers le serveur, et que la clé a été ajoutée dans les clés autorisées, nous aurons « Passphrase for key [...] : » au lieu de « [user]@[IP/hostname]'s password : »

Exemple en image :

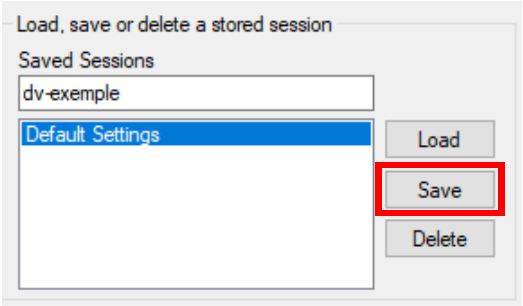


Nous pouvons maintenant fermer la connexion avec « exit ».

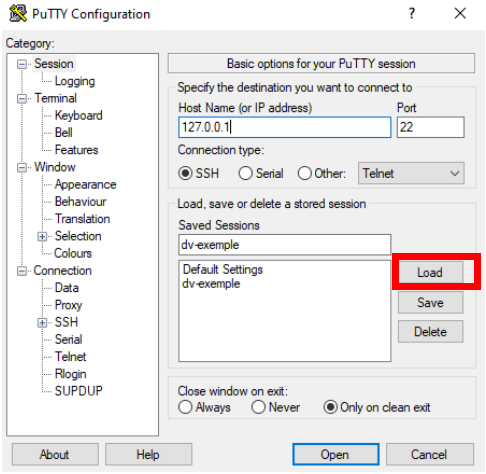
On peut remarquer qu'il faut faire les paramétrages à chaque lancement de PuTTY. C'est pour cela que nous allons créer et sauvegarder un profil de session.

IV - Mettre en place une connexion SSH sous Windows avec PuTTY

7. Si nous voulons créer un profil pour se connecter à la machine dv-stagiare, nous allons refaire les paramétrages précédents, hormis la création de clé. Après cela, nous allons taper le nom de profil voulu dans le champ suivant dans la catégorie principale « Sessions ».



Maintenant, dès que nous souhaitons nous connecter à une machine spécifique et ainsi charger l'IP ou hostname correspondant, ainsi que tout autre paramètre propre à cette connexion, il faut simplement choisir le profil voulu et faire « Load ».



Maintenant que PuTTY est opérationnel et paramétré, il y a certains aspects de son utilisation utiles à connaître.

8.1 Lors de l'utilisation de PuTTY, si vous souhaitez fermer la connexion de manière propre, il vous faut simplement taper "exit" dans le terminal plutôt que de fermer la fenêtre. Sinon il est possible que des connexions mal fermées restent actives jusqu'au redémarrage de la machine distante.

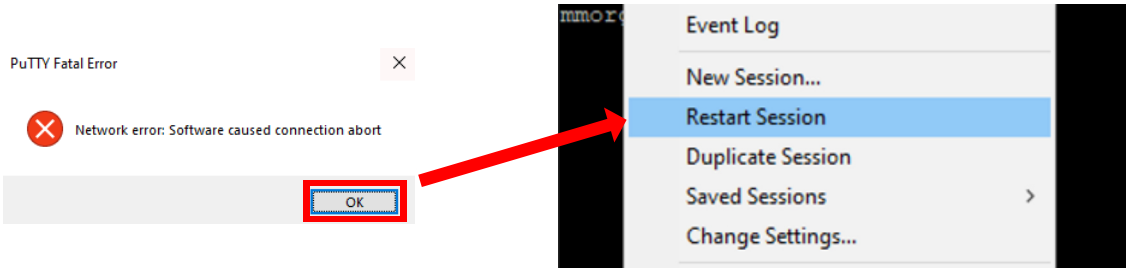
Dans ce cas-là, si un document était édité via « nano » ou « vim » sous Linux, le document sera inaccessible. Il faut donc faire un « pstree -p » et de chercher la connexion SSH qui utilise nano ou vim. Prenez en compte son ID et faites la commande :
sudo kill [ID processus SSH]

8.2 Copier coller du texte de la fenêtre SSH à Windows et vice-versa est particulier puisque Ctrl + C et Ctrl + V ne fonctionne pas dans la fenêtre :

-Pour copier depuis la machine, il faut sélectionner le texte qui sera automatiquement mis dans le presse papier Windows.

-Pour coller sur la machine le contenu du presse papier Windows il faut simplement faire un clic droit.

8.3 Si une déconnexion a lieu, il faut simplement faire un clic droit sur le nom de la fenêtre SSH et faire « Restart session » :



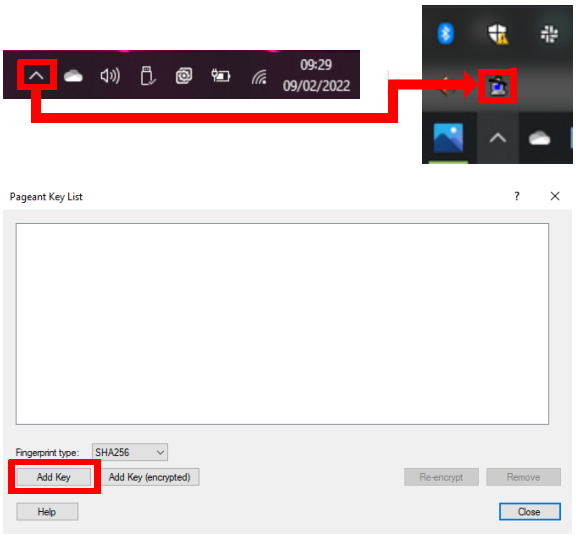
8.4 Vous pouvez aller dans la sous catégorie « Data » de « Connection » et ajouter votre identifiant dans le champ « Auto login » afin de ne plus avoir à entrer votre login lors de

IV - Mettre en place une connexion SSH sous Windows avec PuTTY

8.5 Attention, les clés PuTTY et les clés OpenSSH ne sont pas interchangeables.

9. Un autre outil installé avec PuTTY est Pageant, il vas nous servir à n'avoir qu'une seule demande de passphrase à effectuer.

Pour cela, nous allons lancer Pageant, le logiciel vas se lancer en arrière plan. Il vous faudra trouver son icône à droite de la barre des taches. Lorsque la fenêtre est ouverte, il faut ajouter la clé privée que nous utilisons pour nous connecter sur PuTTY en appuyant sur le bouton « Add key ».
Mettez la même clé ppk que vous utilisez dans « Auth ».



Pageant vous demandera le passphrase de la clé entrée.

Lorsque vous essayerez de vous connecter via PuTTY, vous serez automatiquement connecté sur la machine distante, sans avoir à entrer de mot de passe ou de passphrase.

A noter : Dès lors que la session Windows, ou que Pageant seras fermé, il faudra relancer Pageant et lui redonner la ou les clés voulues.

Exemple de connexion avec Pageant configuré