Connexion SSH via clef RSA & Puttygen

>>> Client Windows

Description :

Dans ce cours nous allons apprendre à installer SSH et à le configurer pour qu'il utilise des clefs RSA à la place des mots de passe.

L'utilisation de clef RSA vous permet d'augmenter la sécurité au niveau de l'administration à distance de vos serveurs.

Connexion SSH via clef RSA & Puttygen

>>> Client Windows

L'utilisation de clef RSA vous permet d'augmenter la sécurité au niveau de l'administration à distance de vos serveurs.

Sommaire :

I) Installation et configuration de SSH

- Commencez par installer "SSH" :

```
aptitude -y install ssh
```

- Une fois installé ouvrez votre éditeur préféré (pour moi VIM) et éditez le fichier "/etc/ssh/sshd_config" :

```
vim /etc/ssh/sshd_config
```

- Modifiez les lignes ci-dessous :

```
# Lifetime and size of ephemeral version 1 server key

KeyRegenerationInterval 3600

ServerKeyBits 1024
```

- Modifiez "768" par "1024" ou "2048".

```
RSAAuthentication yes

PubkeyAuthentication yes

AuthorizedKeysFile %h/.ssh/authorized_keys
```

- Décommettez la ligne "#AuthorizedKeysFile %h/.ssh/authorized_keys" en supprimant le dièse.

```
# Change to no to disable tunnelled clear text passwords
```

```
PasswordAuthentication no
```

- Décommettez la ligne "#PasswordAuthentication yes" et changez "yes" en "no".

Enregistrez et quittez mais ne redémarrez pas votre serveur, ni le service SSH.

II) Création de l’utilisateur

Nous allons créer un nouvel utilisateur, mais vous pouvez aussi le faire sur le compte root ou sur un compte utilisateur existant.

```
root@debian:~# adduser vthymme
Ajout de l'utilisateur Â«Â vthymmeÂ Â»...
Ajout du nouveau groupe Â«Â vthymmeÂ Â» (1001)...
Ajout du nouvel utilisateur Â«Â vthymmeÂ Â» (1001) avec le groupe Â«Â vthymmeÂ Â»...
CrÃ©ation du rÃ©pertoire personnel Â«Â /home/vthymmeÂ Â»...
Copie des fichiers depuis Â«Â /etc/skelÂ Â»...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwdÂ : le mot de passe a Ã©tÃ© mis Ã jour avec succÃ¨s
Modification des informations relatives Ã l'utilisateur vthymme
Entrez la nouvelle valeur ou Â«Â EntrÃ©eÂ Â» pour conserver la valeur proposÃ©e
Nom complet []: Vincent thymme
NÂ° de bureau []:
TÃ©lÃ©phone professionnel []:
TÃ©lÃ©phone personnel []:
Autre []:
Ces informations sont-elles correctesÂ ? [O/n]
```

Maintenant que l’utilisateur existe, nous allons créer un nouveau dossier dans son répertoire :

```
mkdir /home/vthymme/.ssh
```

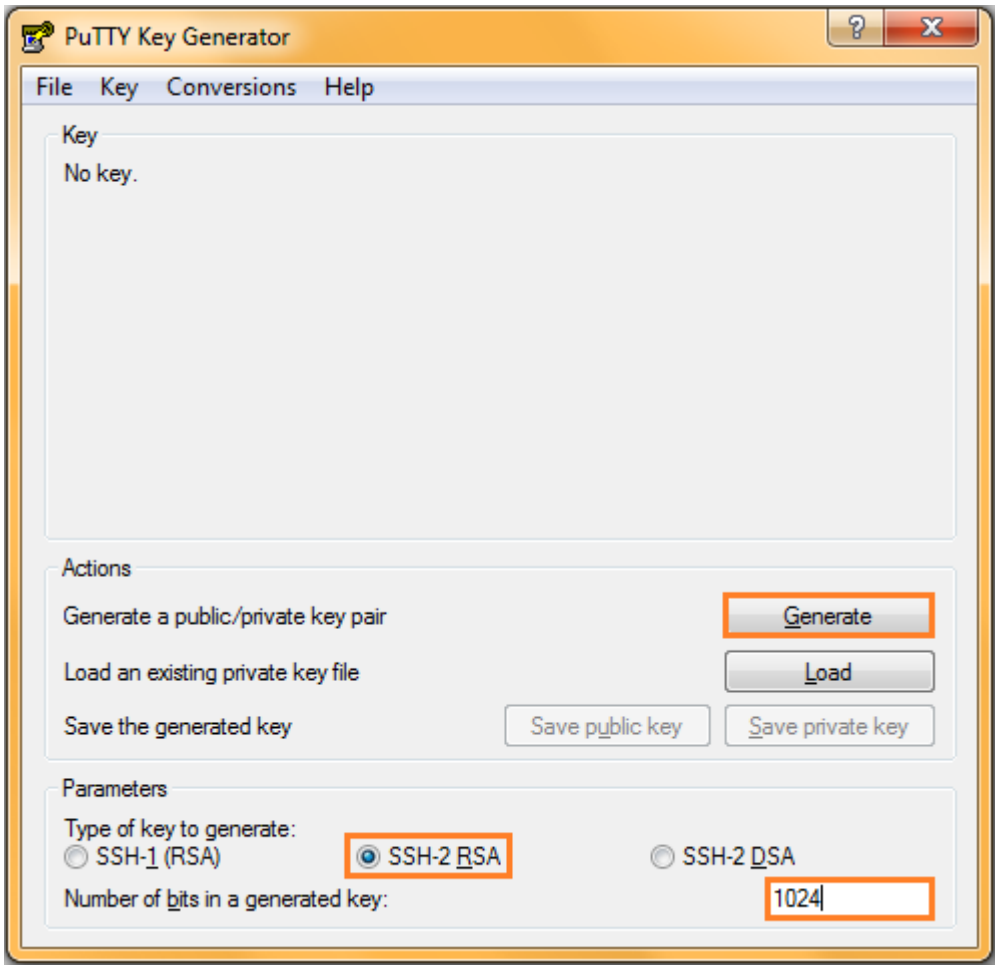
- Le "." avant SSH indique que c’est un dossier caché.

III) création des clefs RSA

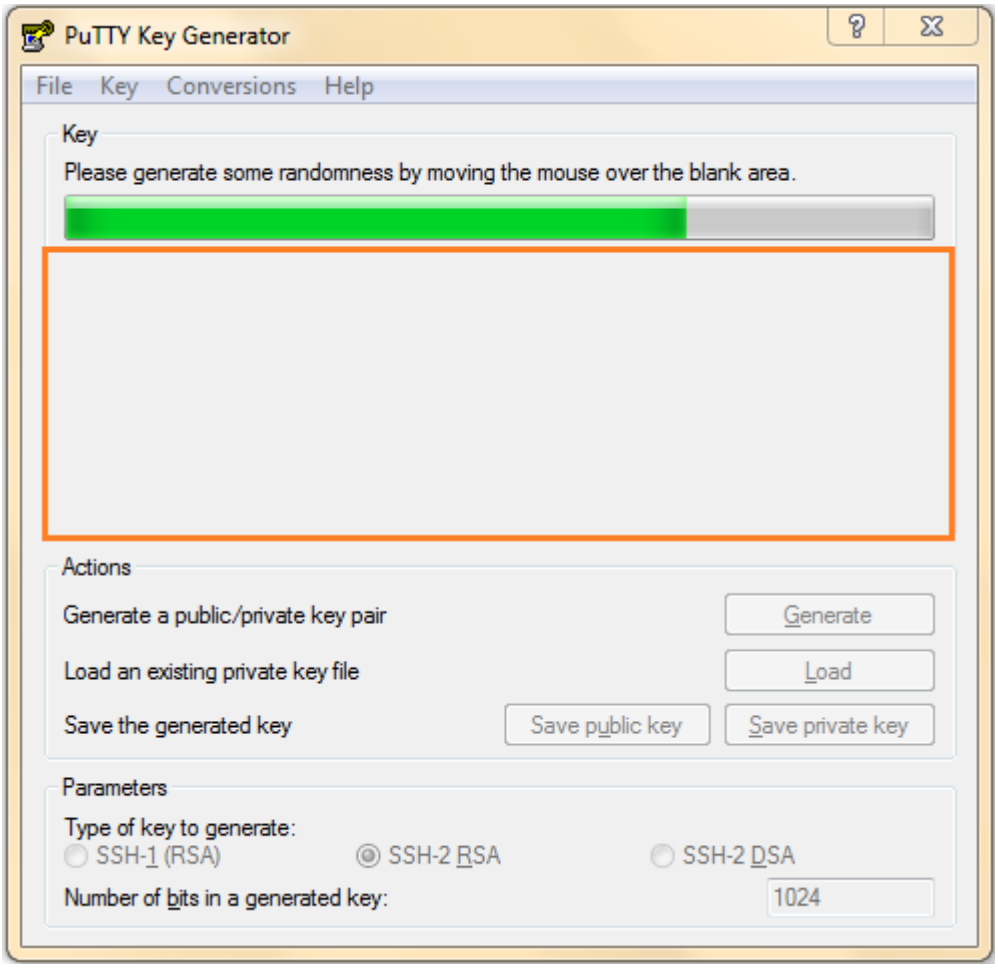
Installez "Putty" sur votre station de travail.

Cliquez ici pour télécharger

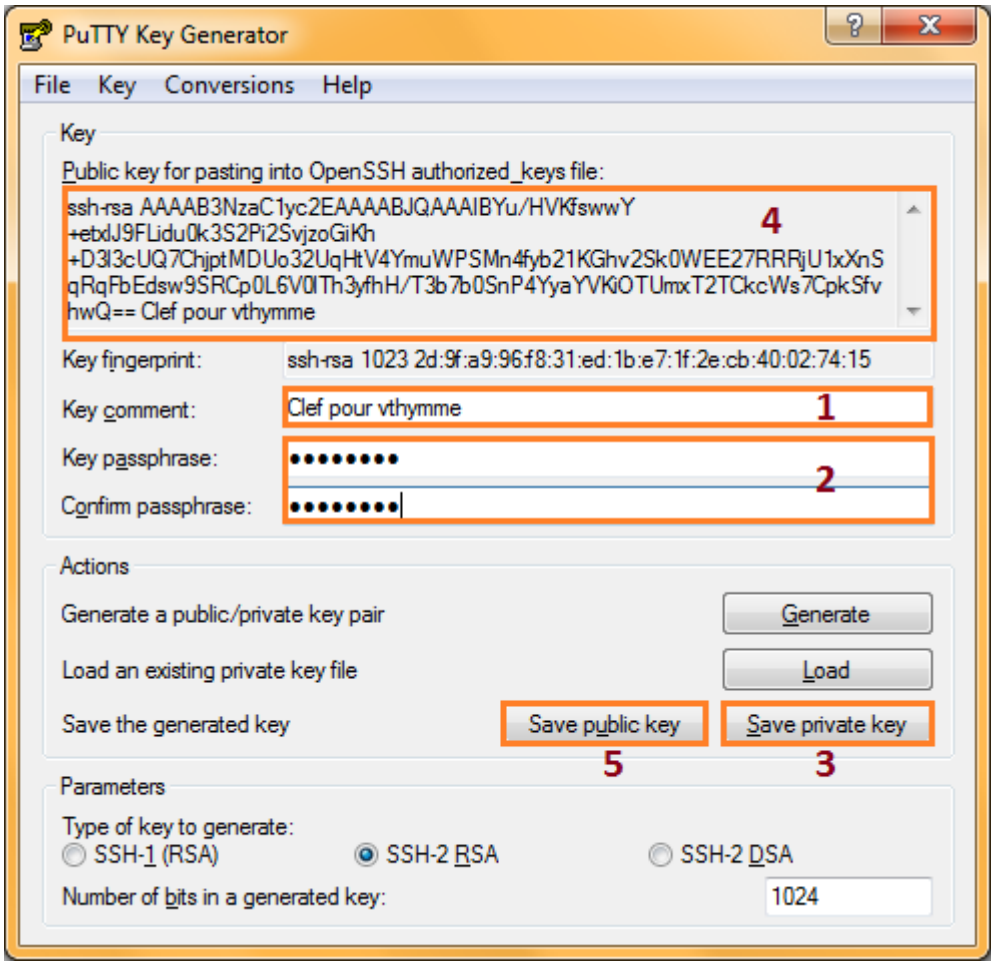
Ensuite ouvrez le logiciel "Puttygen" de la suite "Putty", il ressemble à ceci :



- Vérifiez que la case "**Number of bits in a generated key**" à la même valeur que celle dans la configuration SSH.
- Vérifiez que "**SSH-2 RSA**" soit sélectionné.
- Cliquez sur "**Generate**".



– Pour générer la clef RSA vous devez bouger le curseur de la souris dans la zone que j'ai entouré.



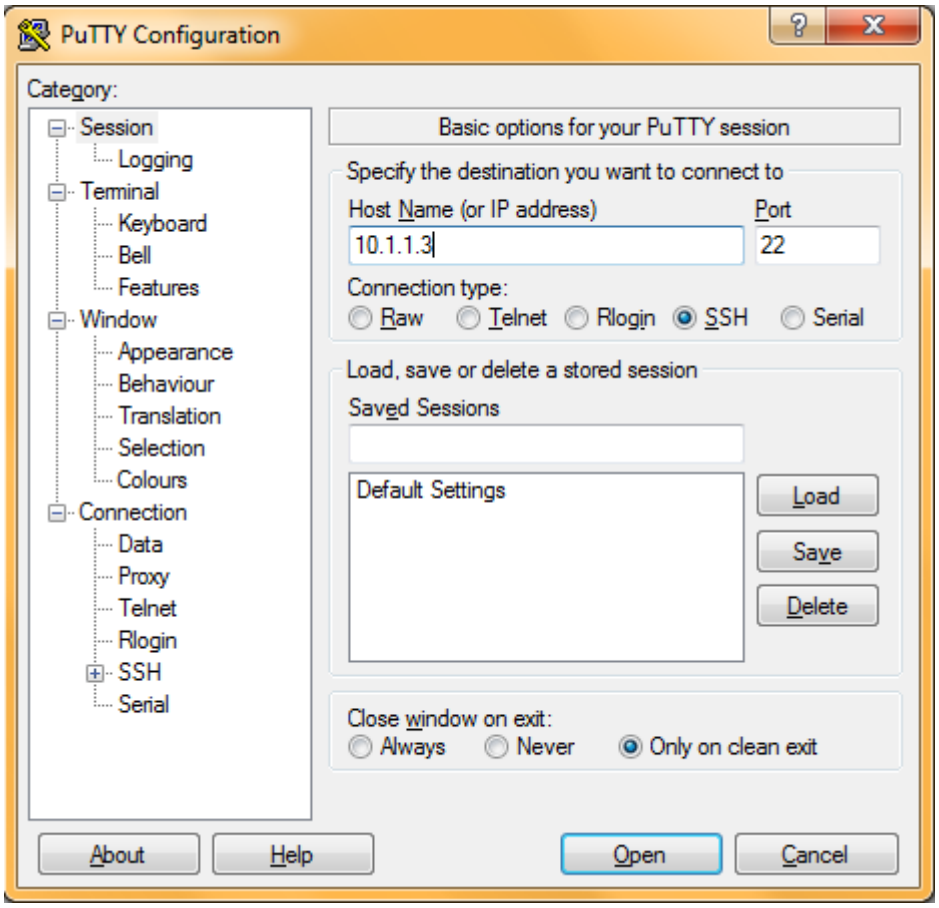
– 1. Renseignez le champ "**Key comment**".
– 2. Entrez un mot de passe pour que la clef RSA ne soit pas utilisée à votre insu (permet d'augmenter encore la sécurité).
– 3. Cliquez sur "Save private key", pour sauvegarder la clef Privée que vous devrez utiliser à partir de votre station pour vous connecter.

Deux méthodes s'offrent à vous ensuite :

– 4. Copiez le texte qui se trouve dans l'encadré 4, puis suivez les instructions du chapitre suivant.
– 5. Cliquez sur "**Save public key**", enregistrez le sous le nom "**authorized_keys**" et transférez se fichier dans le dossier "**/home/user/.ssh**" à l'aide d'un logiciel comme **"Filezilla"**.

IV) Configuration de la clef public sur le serveur

Ouvrez une connexion SSH avec "Putty". Vous allez peut être vous dire que dans la configuration que nous avons fait dans le premier chapitre, nous avons désactivé les connexions avec les mots de passes !!!
Vous avez raison mais nous n'avons pas redémarré le service SSH, donc les nouveaux paramètres ne sont pas pris en compte.



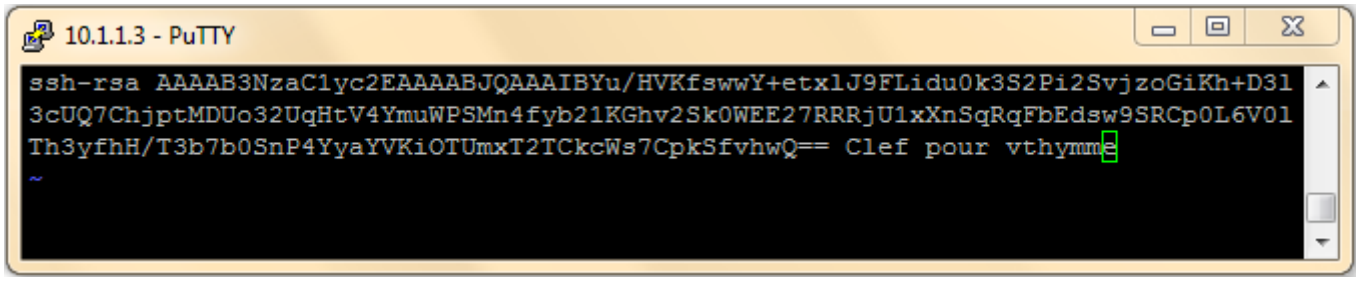
- Tapez l'adresse IP du serveur et cliquez sur "**open**"
- Authentifiez vous
- Ouvrez avec votre éditeur préféré, le fichier "**/home/user/.ssh/authorized_keys**"

Attention à l'écriture du nom de fichier.

```
vim /home/vthymme/.ssh/authorized_keys
```

Collez la clef publique dans le fichier. **(RAPPEL : pour coller avec "Putty" faite clique droit).**

Vous devriez obtenir quelque chose comme ceci :



Enregistrez et quittez.

V) Redémarrage du service SSH

On redémarre le service "SSH" :

```
/etc/init.d/ssh restart
```

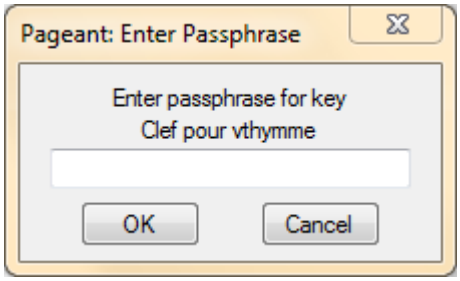
VI) Test de connexion

Nous allons maintenant essayer de nous connecter.

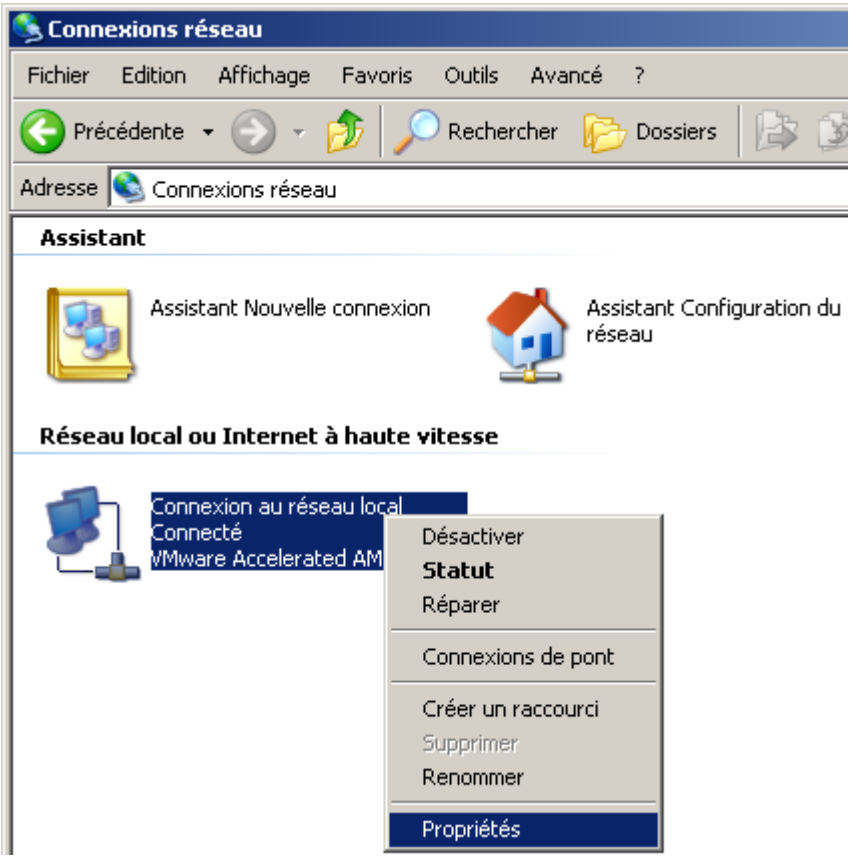
- Commencez par faire un double clic sur votre clef privée

L'icône ressemble à ceci :

Entrez la passphrase que vous lui avez mis :



Ensuite ouvrez "**Putty**" et entrez l'adresse IP du serveur :



Cliquez sur "**open**" et vous obtenez ceci :

```
login as: vthymme
Authenticating with public key "Clef pour vthymme" from agent
Linux debian 2.6.26-2-686 #1 SMP Thu Nov 25 01:53:57 UTC 2010 i686
```

```
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.
vthymme@debian:~$
```

Voilà vous n’avez plus qu’à recommencer l’opération pour les autres utilisateurs.