Objectifs :

Apprendre à configurer le ssh sur une machine Debian.

Comprendre le fonctionnement du ssh et ses méthodes de sécurisation.

Apprendre à utiliser le ssh sur l’invite de commande, et les logiciels putty et MobaXterm.

Consignes :

Suivez chaque étape de façon à installer votre serveur SSH, le configurer et le tester.

# Installation du serveur SSH

Se connecter en SSH sur une machine est une utilisation très courante.

### Sur votre machine Debian :

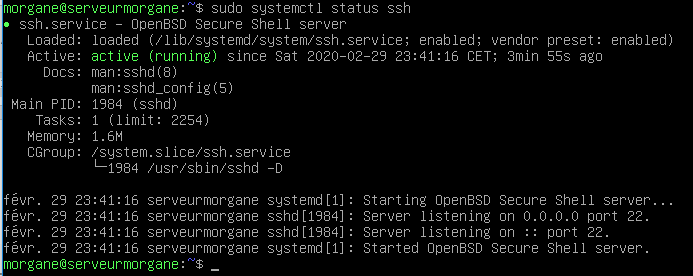
Installez le service ssh sur votre machine :

sudo apt install openssh-server

Une fois le service installé, vérifiez bien son fonctionnement en consultant son status :

sudo systemctl status ssh

Vous devez obtenir cela :



Vous constatez que le service est actif, et sur le serveur est en écoute sur toutes les adresses IP sur le port 22.

# Connexion avec un client SSH sur Windows

Un client SSH est souvent bien plus pratique à utiliser que l’invite de commande.

Au cours de la formation, vous allez découvrir deux clients ssh : putty et Mobaxterm.

Nous allons commencer par apprendre à utiliser Putty.

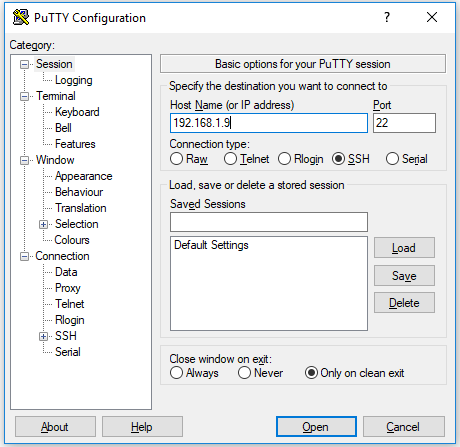
## Putty

Téléchargez le logiciel sur le site : <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Choisissez la version 64 bits.

Une fois installé, lancez le logiciel.

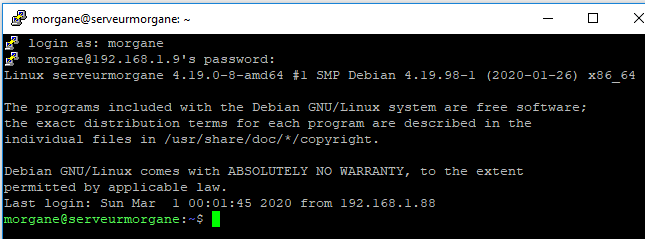
Sur la ligne « Hostname or IP address » saisissez l’adresse IP de votre machine Debian et le port du service SSH, par défaut celui-ci est 22.



Lancez la connexion en appuyant sur Open.

Vous allez avoir un message d’alerte. Répondez oui, le logiciel vous demande alors votre login (nom d’utilisateur Debian).

Saisissez-le. Puis saisissez votre mot de passe. Et vous voilà connecté avec Putty !



## MobaXterm

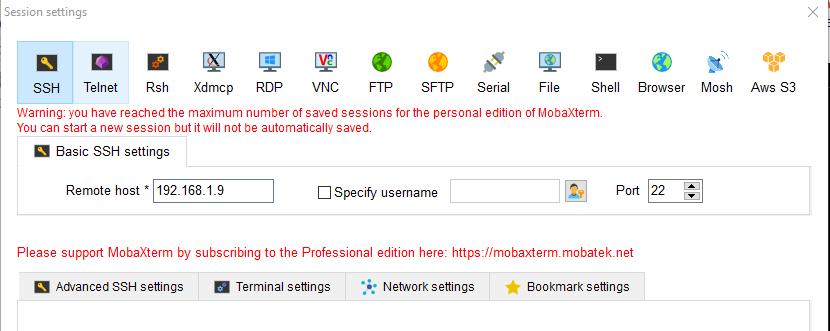
Télécharger le logiciel sur le site : <https://mobaxterm.mobatek.net/download-home-edition.html>

Choisissez la version « Installer Edition ».

Une fois installé, lancez le logiciel.

Cliquez sur « Session » en haut à gauche, puis sur « SSH » en haut à gauche.

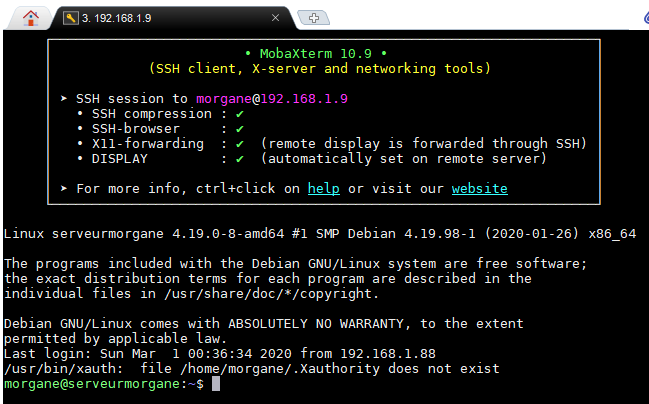
Dans la case « Remote host » saisissez l’adresse IP de votre machine Debian, et mettez le port SSH, par défaut, 22.

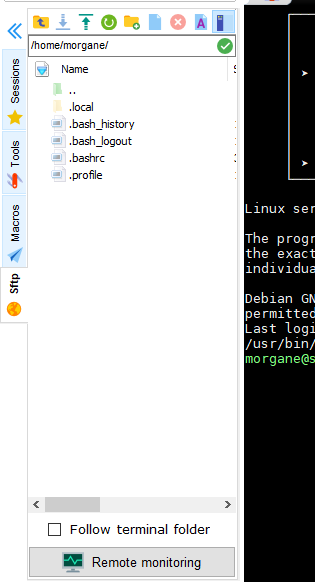


Cliquez sur OK en bas de la fenêtre.

Saisissez votre login utilisateur, puis votre mot de passe. Ensuite, vous avez un message qui vous demande si vous voulez sauvegarder votre mot de passe.

Vous voilà connecté avec MobaXterm !





L’un des avantages de MobaXterm par rapport à Putty est l’onglet présent à gauche, qui vous positionne automatiquement sur « sftp », qui est le service FTP qui passe par la connexion SSH.

À la connexion, il vous positionne dans votre dossier personnel. Dans la barre d’adresse, vous pouvez écrire directement le chemin où vous voulez vous rendre.

Pour remonter automatiquement d’un dossier enfant vers le dossier parent, vous pouvez cliquer sur le dossier avec une flèche, à gauche.

Vous pouvez donc vous balader dans l’arborescence. Mais il est grandement déconseillé d’utiliser ce service pour modifier, créer ou supprimer directement des documents ou des dossiers. Pour tout cela, passez directement par les lignes de commande.

## Sécurisez votre SSH

Partie uniquement pour la culture et comprendre le ssh, car c’est primordial pour vos connexions à distance sur des serveurs. Si vous êtes en retard, ou avez du mal, passez directement au TP suivant.

Pour info, la connexion SSH est déjà une connexion à distance sécurisée, mais on peut aller encore plus loin. Rien qu’en utilisant des paramétrages prés-conçu dans le fichier de configuration du ssh ( /etc/ssh/sshd\_config) il y a plein de méthode pour le sécuriser, comme faire une liste blanche des utilisateurs qui ont le droit de se connecter, changer le port d’écoute et de connexion, limiter le nombre de tentative de connexion, éteindre une session ssh après des minutes d’inactivité …..

Regardez ce fichier, et essayez de trouver certaines de ces options et même pleins d’autre.

Enfin, si vous êtes curieux et que ça vous intéresse, il y a aussi la possibilité de sécuriser votre connexion ssh en utilisant le système des clés de chiffrement asymétriques.