

Pré-requis

I) Créer votre site web

Avant de vouloir mettre en ligne votre site, je vous conseille de le préparer avec un éditeur de texte adapté comme **Visual Studio** (<https://code.visualstudio.com/Download>), **PhpStorm** (<https://www.jetbrains.com/phpstorm/>) , etc

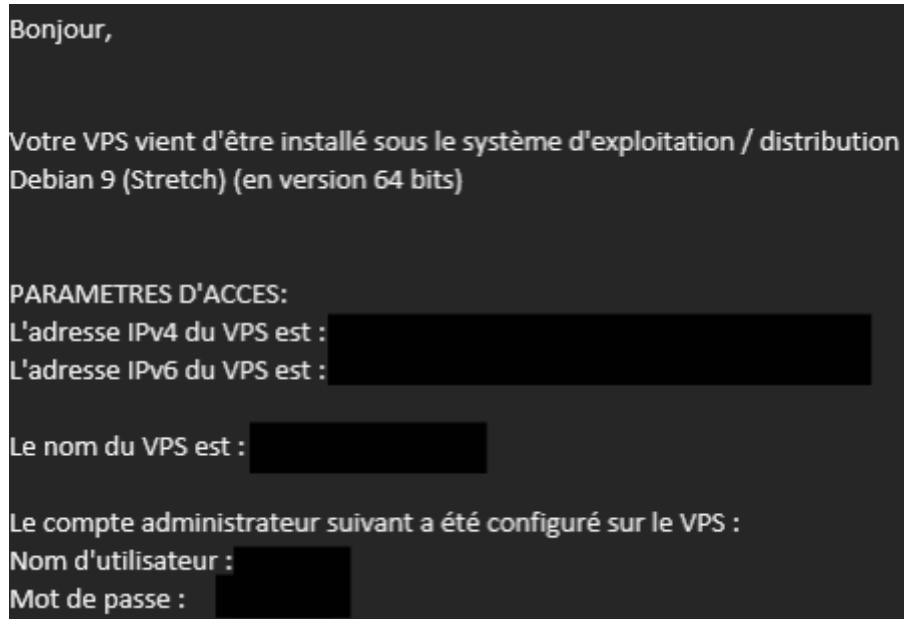
Afin de faire des tests en local, installez vous une base de donnée **Wamp** (<http://www.wampserver.com/en/download-wampserver-64bits/>)

Cela vous permettra de savoir a quoi ressemblera votre site une fois en ligne, donc amusez-vous a tester le plus de chose possible!

II) Acheter un serveur VPS

Pour avoir un serveur **VPS**, rendez-vous ici et choisissez l'offre qui correspond à vos besoins sur le site d'OVH.

Une fois le mail avec vos informations réceptionné, vous pourrez commencer.



Bonjour,

Votre VPS vient d'être installé sous le système d'exploitation / distribution Debian 9 (Stretch) (en version 64 bits)

PARAMETRES D'ACCES:

L'adresse IPv4 du VPS est : [REDACTED]

L'adresse IPv6 du VPS est : [REDACTED]

Le nom du VPS est : [REDACTED]

Le compte administrateur suivant a été configuré sur le VPS :

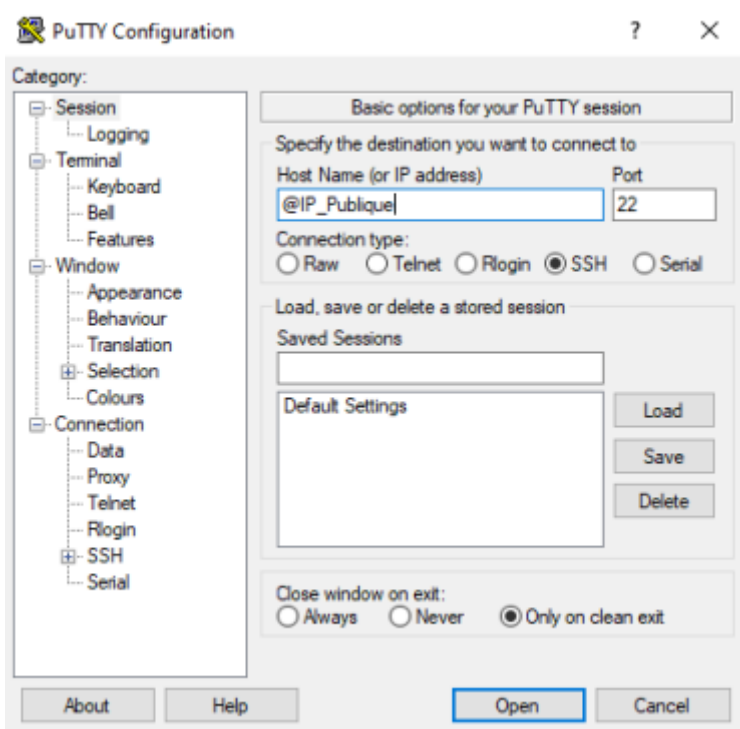
Nom d'utilisateur : [REDACTED]

Mot de passe : [REDACTED]

III) Débuter avec le VPS

a) Se connecter au VPS

Pour vous connecter a votre VPS fraîchement créé, lancer **PuTTY** ou n'importe quel autre logiciel de ce genre. La connexion se fait à l'aide de l'@IP publique et du port de base du SSH (port 22) de votre serveur renseignée dans le mail :



Pour vous y connecter avec un linux utilisez la commande :

```
ssh root@IPV4_VPS
```

Une fois que vous serez connecté, entrez les informations d'identifications fournies dans le mail reçu précédemment :

Le compte administrateur suivant a été configuré sur le VPS :

Nom d'utilisateur : [REDACTED]

Mot de passe : [REDACTED]

b) Changer le port de connexion au VPS

Lorsque vous serez connecté au VPS, mettez a jour les paquets du système :

```
apt update  
apt upgrade
```

Puis changez le mot de passe du VPS :

```
passwd
```

Nous allons maintenant changer le port d'écoute du service SSH afin d'éviter des tentatives d'intrusions sur le serveur, rendez-vous dans le fichier de configuration de SSH avec l'éditeur de texte de votre choix (ici **nano**) :

```
nano /etc/ssh/sshd_config
```

Au début du fichier, retirez le `#` sur la ligne en surbrillance ci-dessous et mettez le port que vous souhaitez :

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

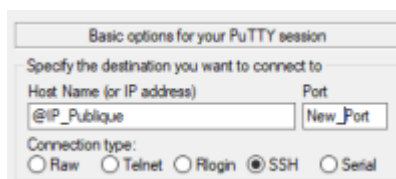
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

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

Redémarrez ensuite le service SSH :

```
systemctl restart ssh.service
```

Pour vos futures connections au VPS, pensez à changer le port sur PuTTY :



Pareil si vous utilisez un linux :

```
ssh root@IP_VPS -p VotrePort
```

c) Création d'un utilisateur avec les droits Admin

Nous allons a présent créer un utilisateur avec des droits restreints qui pourra se connecter au serveur et aura les droits **SUDO** :

```
adduser NomUser
```

Suite a la commande entrez les informations d'identification de ce nouvel utilisateur.

Testez si SUDO est bien installé :

```
sudo ls -la /root
```

Si ce n'est pas le cas alors faite la commande :

```
apt install sudo
```

Attribuez ensuite les droits :

```
usermod -aG sudo Nom_User
```

Vous pouvez désormais effectuer des actions Root avec votre utilisateur!

Si vous souhaitez repasser avec l'utilisateur Root, utilisez la commande suivante :

```
su
```

d) Désactivation de l'accès SSH Root

Nous allons maintenant désactiver l'accès SSH a l'utilisateur Root, ouvrez de nouveau avec votre éditeur de texte le fichier :

```
nano /etc/ssh/sshd_config
```

Et commentez `#` la ligne `PermitRootLogin yes` :

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Sauvegardez le fichier et redémarrez une nouvelle fois le service SSH :

```
systemctl restart ssh.service
```

Dans un futur chapitre nous sécuriseront l'accès encore + à l'aide d'un Firewall.

Revision #9

Created 19 January 2023 13:09:46 by Admin

Updated 19 January 2023 14:03:39 by Admin