liste des commades :

- Afficher le répertoire en cours = pwd
- Changer de répertoire = cd/”emplacement”
- Revenir au répertoire précédent = cd ..
- Lister les fichiers présents dans un répertoire = ls - Lister les fichiers présents dans un répertoire avec leurs droits associés, sous forme de liste et en incluant les fichiers cachés = ls -al
- Créer un fichier = touch
- Insérer du texte dans un fichier = sed
- Supprimer un fichier = rm
- Afficher le contenu d’un fichier =
- Créer un répertoire = mkdir
- Créer un lien symbolique = ln
- Supprimer un répertoire = rmdir
- Copier un répertoire = cp -r
- Renommer un répertoire = mv
- Déplacer un répertoire = mv
- Chercher un fichier sur votre disque en se basant sur son nom = find -name
- Rechercher du texte dans un fichier = grep [“text”] [nom du fichier]
- Afficher le texte “Bonjour tout le monde” =
- Afficher l’historique des commandes qui ont été tapées = history - Afficher la version du système d’exploitation installée = lsb_release -a
- Afficher la date et l’heure = date
- Afficher la durée depuis laquelle le système d’exploitation est allumé = uptime
- Rechercher les mises à jour disponibles pour le système = apt-get update
- Installer les nouvelles mises à jour disponibles depuis la dernière recherche = apt-get dist-upgrade
- Se connecter en tant que superutilisateur = sudo - root
- Installer l’éditeur de texte “emacs” = apt-get install emacs
- Connaître son/ses adresses ip = sudo ifconfig

how to install a server in local :

Première étape installer une virtual machine pour cela téléchargez oracle VM virtual box sur leur site

installer oracle vm en suivant les instruction

ensuite aller sur la page de debian et téléchargez l'image de ce dernier

ouvrez Oracle VM et puis Cliquez sur l'icône Nouveau dans la barre de menus de VirtualBox.

Cela lancera l'Assistant Nouvelle machine virtuelle. Le premier écran n'est qu'un écran de bienvenue, alors cliquez sur Continuer pour continuer.

suivez toutes les instructions afficher a l’ecran

une fois que votre debian est installer ouvrez votre console debian

Étape 1: Connectez-vous via SSH
Lorsque votre serveur est créé, Snel vous envoie un e-mail avec le nom d'utilisateur, le mot de passe et l'adresse IP du serveur par défaut. Pour la première connexion, vous devez utiliser ces informations d'identification pour vous connecter à votre serveur.

Si vous ne savez pas comment vous connecter, veuillez consulter notre article "Comment se connecter à votre serveur avec SSH".

Étape 2: Modifier le mot de passe de l'utilisateur connecté
Lors de la première connexion, il est très important de changer le mot de passe de l'utilisateur actuel. Utilisez la commande suivante pour la même chose.

passwd
Il vous demandera de fournir votre mot de passe existant à moins que vous ne soyez connecté en tant qu'utilisateur root.

Étape 3: créer un nouvel utilisateur Sudo
Si vous êtes connecté en tant qu'utilisateur root, il est recommandé de créer un utilisateur sudo. Si vous êtes connecté en tant qu'utilisateur sudo avec un nom d'utilisateur au format client_xxxxxx_x, que Snel a déjà créé pour vous, il est toujours recommandé de créer un nouvel utilisateur sudo.

Un utilisateur Sudo est un utilisateur disposant de privilèges de superutilisateur. En termes simples, cet utilisateur peut exécuter des commandes et des tâches d'administration en tant qu'utilisateur root.

Pour créer un nouvel utilisateur, exécutez la commande suivante. Vous pouvez remplacer l'exemple de nom d'utilisateur happysnel par tout ce que vous voulez.

sudo adduser happysnel
Remarque: vous pouvez omettre d'utiliser la commande sudo si vous êtes connecté en tant qu'utilisateur root. Fournissez les informations requises telles que votre nom et votre mot de passe et un utilisateur sera créé pour vous.

client_xxxxx_x@vps:~$ sudo adduser happysnel
Adding user `happysnel' ...
Adding new group `happysnel' (1001) ...

Adding new user `happysnel' (1001) with group `happysnel' ...
Creating home directory `/home/happysnel' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for happysnel
Enter the new value, or press ENTER for the default
	Full Name []: Happy Snel
	Room Number []:
	Work Phone []:
	Home Phone []:
	Other []:
Is the information correct? [Y/n] y
Ajoutez votre utilisateur nouvellement créé au groupe sudo. Les utilisateurs du groupe sudo sont des utilisateurs sudo dans Debian 10.

sudo usermod -aG sudo happysnel
Étape 4: connexion en tant qu'utilisateur nouvellement créé
Quittez la session de terminal en cours en exécutant la commande de déconnexion et connectez-vous à nouveau en utilisant ssh comme nouvel utilisateur.

ssh happysnel@192.168.0.1
192.168.0.1 est un exemple d'adresse IP.

Étape 5: Désactivez la connexion racine via SSH
Recherchez le paramètre actuel pour la connexion root via SSH en exécutant la commande suivante.

sudo cat / etc / ssh / sshd_config | grep PermitRootLogin
Vous pouvez voir la sortie suivante.

[happysnel @ vps ~] $ sudo cat / etc / ssh / sshd_config | grep PermitRootLogin
PermitRootLogin sans mot de passe
le paramétrage de "PermitRootLogin sans mot de passe".
Comme dans la sortie ci-dessus, il est défini sur sans mot de passe. Cela signifie que l'authentification par mot de passe est désactivée, cependant, l'authentification par clé publique est activée. Ce qui est bien dans la plupart des cas. Assurez-vous qu'il ne doit pas être commenté ou ne doit pas être défini sur yes.

Pour désactiver complètement la connexion root, modifiez le fichier en exécutant la commande suivante.

sudo nano / etc / ssh / sshd_config
Et changez la ligne comme suit.

PermitRootLogin non
Enregistrez le fichier et redémarrez le serveur SSH en exécutant la commande suivante.

sudo systemctl redémarrer sshd
Maintenant, si vous essayez de vous connecter en tant qu'utilisateur root, cela ne vous laissera pas entrer.

Étape 6: Mettez à jour votre serveur
Il est important d'installer les derniers correctifs de sécurité et mises à jour sur votre serveur. Exécutez la commande suivante pour mettre à jour les listes de packages locaux.

sudo apt-get mise à jour
Maintenant, mettez à jour les packages.

mise à jour sudo apt-get -y
Remarque: si vous recevez des invites indiquant qu'un package ou un fichier mis à jour est disponible, mais que la version installée est modifiée. Choisissez conserver la version locale actuellement installée.

Étape 7: Définition du fuseau horaire
Vous voudrez peut-être que votre serveur soit dans le même fuseau horaire que vous. Exécutez la commande suivante pour obtenir une liste des fuseaux horaires disponibles.

timedatectl liste-fuseaux horaires
La liste des fuseaux horaires disponibles est également disponible ici.

Une fois que vous avez identifié votre fuseau horaire, définissez-le à l'aide de la commande suivante.

sudo timedatectl set-timezone Europe / Amsterdam
Vous pouvez confirmer le fuseau horaire en exécutant la commande suivante.

hostnamectl
Étape 8: définir le nom d'hôte
Vérifiez votre nom d'hôte existant en exécutant la commande suivante.

```
happysnel@vps:~$ hostnamectl
   Static hostname: vps.snelexample.site
         Icon name: computer-vm
           Chassis: vm
        Machine ID: cfc70e29ed8440108dfa33dd59160dc9
           Boot ID: 3ccca50362244cf7a001d1c45d41223f
    Virtualization: kvm
  Operating System: Debian GNU/Linux 10 (buster)
            Kernel: Linux 4.19.0-5-amd64
      Architecture: x86-64
```

To set a hostname, run the following command.

sudo hostnamectl set-hostname host.snelexample.site

Remplacez host.snelexample.site par votre nom d'hôte réel. De préférence, il doit s'agir d'un nom de domaine complet (FQDN). Mais, si vous n'êtes pas sûr de vouloir ajouter un nom de domaine complet, une étiquette pour identifier le serveur fonctionne également.

Pour résoudre le nom d'hôte sur votre serveur local, vous devrez l'ajouter au fichier / etc / hosts. Modifier le fichier d'hôtes par exécution

Ajoutez votre nom d'hôte à la fin de la ligne commençant par 127.0.0.1. Par example.

127.0.0.1 localhost host.snelexample.site
Étape 9: Configurer un pare-feu
Debian 10 n'est pas fourni avec un pare-feu par défaut installé. Vous pouvez installer UFW (Uncomplicated Firewall) en exécutant la commande suivante.

sudo apt-get -y installer ufw
Tout d'abord, refusez l'accès à tout le trafic entrant en exécutant la commande.

sudo ufw par défaut refuser l'entrée
Autorisez également l'accès à tout le trafic sortant en exécutant la commande.

sudo ufw par défaut autoriser les sorties
Maintenant que notre stratégie par défaut est créée, autorisons le port SSH par défaut 22 à travers le pare-feu. Exécutez la commande.

sudo ufw autoriser 22
Vous pouvez également exécuter:

sudo ufw autorise ssh
Comme UFW sait que le port par défaut pour SSH est 22.

Maintenant que toutes nos règles sont en place, démarrez le pare-feu UFW en exécutant.

sudo ufw activer
Il vous demandera la confirmation, car l'activation d'UFW peut perturber la connexion SSH existante. Vous pouvez continuer et appuyer sur y car nous avons déjà ouvert le port 22 à travers le pare-feu. Vous obtiendrez une sortie similaire.

happysnel @ host: ~ $ sudo ufw enable
La commande peut interrompre les connexions ssh existantes. Poursuivre l'opération (y | n)?
y
Le pare-feu est actif et activé au démarrage du système
Vous pouvez afficher l'état du pare-feu en exécutant la commande.

état sudo ufw
Vous devriez voir une sortie similaire.

happysnel @ host: ~ $ sudo ufw status

Statut: actif

To	Action	From
22	ALLOW	Anywhere
22/tcp	ALLOW	Anywhere
22 (v6)	ALLOW	Anywhere (v6)
22/tcp (v6)	ALLOW	Anywhere (v6)

Step 10: SSH Port Change (Optional)
Malicious bots on the internet continuously target the default SSH port 22. You can change it to any other port so that your server is not a victim of continues attacks of bots on port 22. To change the SSH port, open the SSH configuration file again by running the following command.

#Port 22
Décommentez-le et remplacez-le par le port de votre choix entre 1024 et 65535.

Par exemple.

Port 2200
Enregistrez le fichier et quittez l'éditeur.

Ouvrez le port 2200 depuis le pare-feu en exécutant la commande.

sudo ufw autoriser 2200
Depuis, nous n'avons plus besoin d'ouvrir le port 22, bloquez-le à l'aide de la commande.

sudo ufw supprimer autoriser 22
sudo ufw supprimer autoriser ssh

Maintenant, redémarrez le serveur SSH en exécutant la commande suivante.

sudo systemctl redémarrer sshd
Rechargez également les règles de pare-feu UFW en exécutant la commande.

rechargement sudo ufw
Maintenant, si vous essayez de vous connecter depuis un autre terminal sans spécifier de port, il ne vous laissera pas entrer. Modifiez la commande SSH pour vous connecter afin d'inclure le numéro de port.

ssh -p 2200 happysnel@192.168.0.1
192.168.0.1 est un exemple d'adresse IP.

Étape 11: Redémarrez
Maintenant que nous avons mis à jour les packages et configuré le serveur. Redémarrez le serveur afin que, s'il y a des modifications en attente, elles soient appliquées.

une fois que tout ça est fait vous n’aurais plus qu’as installer vos langages tel que php grace aux lignes de commandes tel que

sudo apt-get install php -->pour installer php
sudo apt-get install mysql-server → pour installer mysql
sudo apt-get install mariadb-server → pour installer maria db
sudo apt-get-install apache → pour installer apache

pour tout ses installations suivez simplement les instruction qui sont afficher a l’ecran qui vous guideront dans votre installation.

Pour ce qui est de la securisation il faut utiliser un certificat TLS SSL