Installer un serveur web sur Debian 11 et y déployer WordPress.

Apache, **MariaDB**, et **PHP**.

2. Mise à jour du système

```
sudo apt update
sudo apt upgrade -y
```

3. Installer Apache

Apache est un serveur web populaire et simple à configurer.

```
sudo apt install apache2 -y
```

Vérifier qu'Apache est actif :

```
sudo systemctl status apache2
```

Accédez à votre serveur en ouvrant un navigateur à l'adresse : http://<IP_SERVEUR_debian>. Vous devriez voir la page "Apache2 Debian Default Page".

4. Installer MariaDB (Serveur de base de données)

```
sudo apt install mariadb-server -y
```

Sécuriser MariaDB :

```
sudo mysql_secure_installation
```

- Configurer un mot de passe root.
- Supprimer les utilisateurs anonymes.
- Désactiver l'accès root à distance.
- Supprimer la base de test.

Créer une base de données pour WordPress :

1. Connectez-vous à MariaDB :

   ```
   sudo mysql
   ```

2. Créez une base de données et un utilisateur :

   ```
   CREATE DATABASE wordpress;
   ```

```
CREATE USER 'wp_user'@'localhost' IDENTIFIED BY
'mot_de_passe_securise';
GRANT ALL PRIVILEGES ON wordpress.* TO 'wp_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

5. Installer PHP

WordPress nécessite PHP pour fonctionner.

```
sudo apt install php php-mysql libapache2-mod-php -y
```

Vérifier l'installation de PHP :

```
php -v
```

6. Télécharger, installer et configurer WordPress

Télécharger WordPress :

1. Allez dans le répertoire web :

   ```
   cd /var/www/html
   ```

2. Téléchargez WordPress :

   ```
   sudo wget https://wordpress.org/latest.tar.gz
   ```

3. Extrayez l'archive :

   ```
   sudo tar -xzf latest.tar.gz sudo rm latest.tar.gz
   ```

4. Renommez le fichier de configuration :

   ```
   sudo chown -R www-data:www-data /var/www/html
   sudo chmod -R 755 /var/www/html/ wordpress
   ```

5. Renommez le fichier de configuration :

   ```
   sudo cp wp-config-sample.php wp-config.php
   ```

6. Modifiez-le :

   ```
   sudo nano wp-config.php
   define('DB_NAME', 'wordpress');
   define('DB_USER', 'wp_user');
   ```

```
define('DB_PASSWORD', 'mot_de_passe_securise');
define('DB_HOST', 'localhost');
```

7. Activer le module de réécriture Apache

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

8. Accéder à WordPress

- Ouvrez un navigateur et accédez à : http://192.168.2.10/wordpress
- Suivez l'assistant d'installation de WordPress (choix de la langue, création d'un compte administrateur, etc.).

Installation et configuration d'IPFire (Routeur/PareFeu/DHCP)

2.1 Installer IPFire

Étape 1 : Télécharger l'ISO d'IPFire

1. Rendez-vous sur le site officiel d'IPFire.
2. Téléchargez l'ISO adapté à votre architecture (x86_64 pour la plupart des cas).

   https://www.ipfire.org/downloads/ipfire-2.29-core189
3. Conservez l'ISO dans un dossier accessible pour l'utilisation dans VirtualBox.

Étape 2 : Créer une VM pour IPFire

1. **Dans VirtualBox**, créez une nouvelle machine virtuelle :
   - **Nom** : IPFire.
   - **Type** : Linux.
   - **Version** : Other Linux (64-bit).
2. **Configurer les ressources** :
   - **RAM** : 1 Go.
   - **CPU** : 1 vCPU.
   - **Disque dur** : 5 Go en VDI.
3. **Configurer les adaptateurs réseau** :
   - **Adaptateur 1** : NAT (pour l'accès Internet, interface RED).
   - **Adaptateur 2** : Réseau interne (pour le réseau interne GREEN).

Étape 3 : Installer IPFire

1. Lancez la VM et montez l'ISO d'IPFire.
2. Suivez les étapes d'installation :
   - Acceptez la licence.
   - Sélectionnez le disque dur à utiliser et formatez-le.
   - Configurez un mot de passe pour admin (interface web) et root (console SSH).
   - Une fois l'installation terminée, redémarrez la VM et retirez l'ISO.

Étape 4 : Configuration initiale d'IPFire

1. À la fin du démarrage, suivez les étapes de configuration réseau :

- **Type de réseau** : Sélectionnez GREEN + RED.
- **Configuration des interfaces** :
  - **RED (NAT)** : Configuré pour obtenir une adresse IP via DHCP.
  - **GREEN (interne)** : Configurez une IP fixe, par exemple :
    - Adresse IP : 192.168.2.1.
    - Masque de sous-réseau : 255.255.255.0.
    - Rappel : toutes les machine du même réseau doivent avoir la même adresse réseau. 192.168.2.X

2. Sauvegardez les paramètres et redémarrez.

Étape 5 : Accéder à l'interface web d'IPFire

1. Depuis une autre machine connectée au réseau interne (GREEN), ouvrez un navigateur.
2. Accédez à l'adresse IP d'IPFire (exemple : https://192.168.2.1:444).
3. Connectez-vous avec les identifiants admin et le mot de passe défini.

2.2 Configurer les règles de pare-feu

Étape 1 : Accéder à la configuration du pare-feu

1. Depuis l'interface web d'IPFire, cliquez sur **Firewall** dans le menu principal.
2. Accédez à l'onglet **Firewall Rules**.

Étape 2 : Ajouter une règle pour l'accès SSH à Debian

1. Cliquez sur **Add a new rule**.
2. Configurez les paramètres suivants :
   - **Source** :
     - Type : GREEN (réseau interne).
     - Adresse IP : Any (ou une IP spécifique si vous voulez restreindre).
   - **Destination** :
     - Adresse IP : L'adresse IP fixe de votre machine Debian (par exemple, 192.168.2.10).
     - Protocole : TCP.

        - Port : 22 (port SSH).
3. Ajoutez un commentaire (ex. "Accès SSH à Debian") et cliquez sur **Add**.
4. Appliquez la règle en cliquant sur **Apply changes**.

Étape 3 : Ajouter une règle pour l'accès au serveur Apache

1. Cliquez sur **Add a new rule**.
2. Configurez les paramètres suivants :
    - **Source** :
        - Type : GREEN.
        - Adresse IP : Any (ou restreindre selon vos besoins).
    - **Destination** :
        - Adresse IP : L'adresse IP du serveur Apache (ex. 192.168.2.10).
        - Protocole : TCP.
        - Ports :
            - **80** (HTTP).
            - **443** (HTTPS).
3. Ajoutez un commentaire (ex. "Accès HTTP/HTTPS au serveur Apache") et cliquez sur **Add**.
4. Appliquez la règle.

Étape 4 : Ajouter une règle pour le Serveur DHCP/Ubuntu (Optionnel)

Le service DHCP peut être gérer par IPFire :

- **Range (192.168.2.100/24-192.168.2.200/24)**
    - **Client Windows 10 ou 11.**
- **IPs Fixe :**
    - **192.168.2.1 = IPFire**
    - **192.168.2.10 = Debian**
    - **192.168.2.11 = Ubuntu**
    - **192.168.2.12 = Serveur 2022**

1. Le protocole DHCP utilise les ports suivants :

   UDP 67 : pour les requêtes du client vers le serveur DHCP.

   UDP 68 : pour les réponses du serveur vers le client.

2. Cliquez sur **Add a new rule**.

3. Configurez les paramètres suivants :
    - **Source** :
        - Type : GREEN.
        - Adresse IP : Any (ou restreindre selon vos besoins).
    - **Destination** :
        - Adresse IP : L’adresse IP du serveur DHCP (ex. 192.168.2.11).
        - Protocole : UDP.
        - Ports :
            - **Source port 67**
            - **Destination port 68**
    - **Action :**
        - **Allow this traffic**
4. Ajoutez un commentaire (ex. "Accès aux service DHCP/Ubuntu") et cliquez sur **Add**.
5. Appliquez la règle.

Étape 5 : Tester les règles

1. Depuis une machine connectée au réseau GREEN, tentez d'accéder :
    - À Debian via SSH (ssh root@192.168.2.10).
    - Au serveur Apache Debian via un navigateur (http://192.168.2.10).
2. Vérifiez que les connexions fonctionnent correctement.

TP 4.2 : Gestion des utilisateurs avec un poste Linux joint à Active Directory

Contexte : Dans ce TP, nous allons ajouter une machine Ubuntu à un domaine Active Directory existant, géré par un serveur Windows Server. Le domaine Active Directory est utilisé pour centraliser la gestion des utilisateurs et des groupes.

L'objectif de ce TP est de comprendre comment intégrer une machine Linux dans une infrastructure Active Directory tout en permettant aux utilisateurs de se connecter avec leur compte AD sur la machine Linux.

Infrastructure :

- **Serveur AD** : Windows Server (2019 ou 2022)
    - Domaine : sisr.local
    - Adresse IP : .....
    - Masque de sous-réseau : .....
    - Passerelle : .....
    - Serveur DNS : 8.8.8.8
- **Client Ubuntu** : Ubuntu 20.04 ou supp
    - Adresse IP : .....
    - Masque de sous-réseau : .....
    - Passerelle : .....
    - DNS : .....

Objectifs :

1. Joindre un poste client Ubuntu au domaine Active Directory.
2. Permettre la connexion d'utilisateurs AD sur le poste Ubuntu.
3. Gérer les utilisateurs AD directement depuis le serveur.
4. Vérifier l'accès aux partages réseau et à l'infrastructure AD.

Étapes à suivre :

1. Installation d'une machine virtuelle Ubuntu :

Indiquez les étapes essentielles. Pensez à mettre à jour votre machine.

1. Configuration réseau sur la machine Ubuntu :

Modifiez l'adresse IP de la machine Ubuntu, pour qu'elle soit dans le même réseau que le serveur AD.

Indiquez les étapes essentielles.

2. Renommer la machine :

Donnez un nom significatif à la machine Ubuntu. Pensez à redémarrer votre machine.

Indiquez les étapes essentielles.

3. Installation des paquets pour joindre Ubuntu au AD :

Installez les paquets nécessaires pour joindre la machine Ubuntu au domaine Active Directory. (Pensez à mettre à jour votre machine avant chaque nouvelle installation de vos paquets)

sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin oddjob oddjob-mkhomedir packagekit

Pensez à commenter les captures d'écran.

4. Test de connexion au domaine :

Utilisez realm pour tester si le domaine est joignable.

realm discover SISR.LOCAL.

Pensez à commenter les captures d'écran.

4. Joindre le domaine :

Utilisez realm pour joindre la machine Ubuntu au domaine sisr.local.

Quelle commande permet de joindre la machine Ubuntu au domaine ?

Pensez à commenter les captures d'écran.

5. Vérification de la connexion des utilisateurs :

Testez la connexion d'un utilisateur du domaine (par exemple joyeux.nouveau @sisr.local) pour vous assurer qu'il peut se connecter à la machine Ubuntu.

Quelle commande permet de connecter joyeux.nouveau @sisr.local au domaine ?

Pensez à commenter les captures d'écran.

Vérifier que la machine Ubuntu se trouve bien dans la liste des computers sur l'AD.

Pensez à commenter les captures d'écran.

Testez la commande suivante sur Ubuntu : ***id joyeux.nouveau @sisr.local***

Commentez le résultat.

6. Création automatique des répertoires "home" :

Configurez la machine pour créer automatiquement le répertoire personnel des utilisateurs AD lors de leur première connexion. Pour cela vous devez :

Ouvrir le fichier common-session

sudo nano /etc/pam.d/common-session

Ensuite à fin de fichier, ajoutez la ligne.

session optional pam_mkhomedir.so skel=/etc/skel umask=077

Connectez-vous avec un autre compte utilisateur en ligne de commande

su – claire.lumiere@sisr.local

Commentez le résultat.

On redémarre la machine et on se connecte avec un autre utilisateur en mode graphique cette fois ci.

7. Accès aux répertoires partagés :

Accédez à un dossier partagé sur le serveur AD avec les identifiants d'un utilisateur du domaine, en utilisant le protocole SMB.

Assurez vous que l'utilisateur à bien les autorisations sur le dossier partagé.

Indique l'emplacement suivant dans un explorateur de fichier

smb://nomserveurAD/partage

Indiquer l'importance de smb

Pensez à commenter les captures d'écran.

Conclusion : Les utilisateurs du domaine AD pourront se connecter et accéder aux ressources depuis la machine Ubuntu. Cela permet de centraliser la gestion des

utilisateurs, facilitant leur administration et leur intégration dans l'environnement réseau global.