La Plateforme
La grande école du numérique pour tous

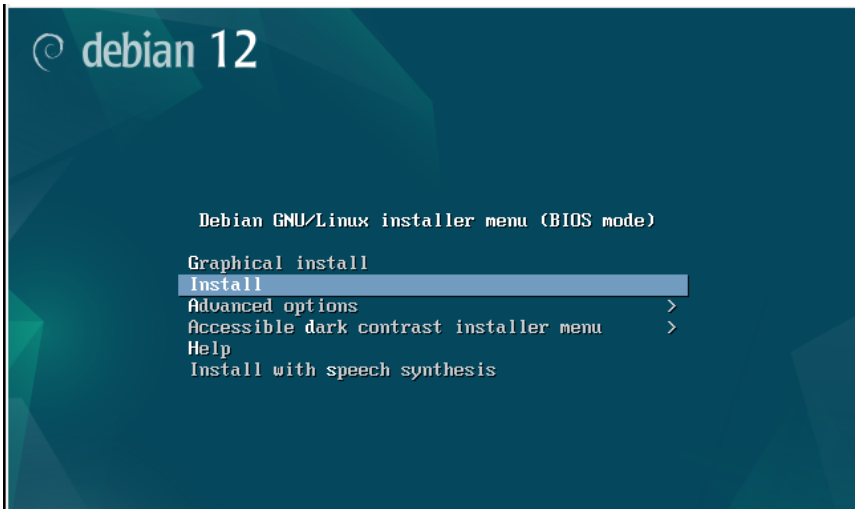
DHCP, DNS, FTP et SSH

ABEDELMOUAMINE BEN AHMED
RYMA ABDERRAHIM
AHMED AOUAD

Installation de Debian sans interface graphique :

Pour installer Debian sans interface graphique, on peut suivre les étapes suivantes :

1. Tout d'abord, on télécharge l'image d'installation de Debian sur le site officiel (https://www.debian.org/distrib/).
2. On crée deux machines virtuelles dans le logiciel de virtualisation (dans notre cas VMware) avec les paramètres suivants :
   - Mémoire RAM : 1 Go minimum
   - Disque dur : au moins 20 Go
   - Carte réseau : configurée en mode bridge pour qu'elles puissent se communiquer dans un même réseau virtuel
   - ISO d'installation : l'image d'installation de Debian téléchargée précédemment
3. Démarrer les machines virtuelles et lancer l'installation de Debian en suivant les étapes du processus d'installation. Voici quelques points importants à prendre en compte pendant l'installation :
   - Sélectionner l'option d'installation sans interface graphique lorsque on est invité à choisir l'environnement de bureau.
   - Configurer l'adresse IP, le nom d'hôte et les paramètres réseau de chaque machine virtuelle de manière à ce qu'elles puissent communiquer entre elles dans le même réseau virtuel.
4. Configuration réseau :
   - Une fois que les deux machines virtuelles ont été installées et démarrées, configurer les adresses IP statiques pour chaque machine.



Mise à jour des systèmes:

Vérifier et appliquer les mises à jour nécessaires sur les deux machines.

1. Connexion aux machines virtuelles :
   - Utiliser le logiciel de virtualisation pour ouvrir des consoles pour les deux machines virtuelles.
2. Se connecter en tant qu'utilisateur root :
   - Se connecter en tant qu'utilisateur root ou utiliser la commande **sudo** pour exécuter les commandes avec des privilèges administratifs.
3. Mise à jour de la liste des paquets :
   - Avant de procéder à la mise à jour, faut mettre à jour la liste des paquets disponibles en exécutant la commande suivante : **apt update**
4. Mise à jour des paquets :
   - Une fois que la liste des paquets est mise à jour, on peut appliquer les mises à jour disponibles en exécutant la commande : **apt upgrade**
   - On peut également inclure l'option **-y** pour confirmer automatiquement toutes les demandes de confirmation : **apt upgrade -y**
5. Mise à jour du système :
   - Pour effectuer des mises à jour système, y compris les mises à jour de sécurité, on peut exécuter la commande suivante : **apt dist-upgrade**

Encore une fois, on peut utiliser l'option -y pour confirmer automatiquement toutes les demandes de confirmation :

apt dist-upgrade -y

En suivant ces étapes, vous pouvez vérifier et appliquer les mises à jour nécessaires sur les deux machines virtuelles Debian.

(On répète ces étapes sur les deux machines virtuelles).

```
root@debian:/home/debian2# apt update
Ign :1 cdrom://[Debian GNU/Linux 12.4.0 _Bookworm_ - Official amd64 DVD Binary-1 with firmware 2023
210-17:57] bookworm InRelease
Err :2 cdrom://[Debian GNU/Linux 12.4.0 _Bookworm_ - Official amd64 DVD Binary-1 with firmware 2023
210-17:57] bookworm Release
  Veuillez utiliser apt-cdrom afin de faire reconnaître ce cédérom par votre APT. apt-get update ne
peut être employé pour ajouter de nouveaux cédéroms
Lecture des listes de paquets... Fait
E: Le dépôt cdrom://[Debian GNU/Linux 12.4.0 _Bookworm_ - Official amd64 DVD Binary-1 with firmware
20231210-17:57] bookworm Release n'a pas de fichier Release.
N: Les mises à jour depuis un tel dépôt ne peuvent s'effectuer de manière sécurisée, et sont donc dé
sactivées par défaut.
N: Voir les pages de manuel d'apt-secure(8) pour la création des dépôts et les détails de configura
ion d'un utilisateur.
root@debian:/home/debian2# apt upgrade -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:/home/debian2# apt dist-upgrade -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:/home/debian2#
```

Configuration du Serveur DHCP :

Un serveur DHCP (Dynamic Host Configuration Protocol) : est un serveur réseau qui distribue automatiquement des adresses IP et d'autres informations de configuration réseau à tous les appareils qui se connectent à un réseau informatique. Plutôt que de configurer manuellement chaque appareil avec une adresse IP statique, un serveur DHCP attribue dynamiquement une adresse IP disponible à chaque appareil au moment de sa connexion au réseau. Cela simplifie

grandement la gestion des adresses IP sur un réseau, en particulier sur les réseaux de grande taille.

1. Installez un serveur DHCP sur la première machine :
   - Se connecter à la première machine virtuelle Debian.
   - S'assurer que le système est à jour en exécutant :
     sudo apt update
     sudo apt upgrade
   - Installez le serveur DHCP en exécutant la commande :
     sudo apt install isc-dhcp-server
2. Configurez le serveur DHCP pour attribuer des adresses de classe B aux machines connectées au réseau :
   - Ouvrez le fichier de configuration du serveur DHCP avec un éditeur de texte :
     sudo nano /etc/dhcp/dhcpd.conf
   - Dans le fichier on ajoute les ligne suivante pour spécifier la plage d'adressage de classe B à attribuer à la machine:

```
subnet 172.16.0.0 netmask 255.255.0.0 {
  range 172.16.0.10 172.16.255.254;
  option subnet-mask 255.255.0.0;
  option routers 172.16.0.1;
  option domain-name-servers 8.8.8.8;
}
```

   - Redémarrer le service DHCP pour appliquer les modifications en utilisant la commande suivante : **sudo systemctl restart isc-dhcp-server**

3.S'Assurer que la machine hébergeant le serveur DHCP possède une adresse IP fixe:

- Éditer le fichier de configuration du réseau en utilisant un éditeur de texte tel que nano . Le fichier de configuration réseau se trouve généralement dans le répertoire **/etc/network/interfaces**.
- Trouver la ligne correspondant à l'interface réseau que on souhaite configurer avec une adresse IP fixe. I
- Ajouter les lignes suivantes pour configurer l'adresse IP fixe :

  address <adresse IP>

  netmask <masque de sous-réseau>

  gateway <passerelle par défaut>

- Redémarrer le service réseau en tapant la commande suivante dans le terminal :
  sudo systemctl restart networking

- Vérifier que l'adresse IP a bien été configurée en tapant la commande suivante dans le

terminal : **ip a**

On doit voir l'adresse IP configurée pour l'interface réseau que on a modifiée. On doit s’assurer également que le serveur DHCP est en cours d'exécution et attribue les adresses IP aux clients correctement.

Installation du Serveur FTP et SSH :

Un serveur FTP (File Transfer Protocol) est un type de serveur qui permet le transfert de fichiers entre un client et un serveur via le protocole FTP. Le FTP est un protocole standard utilisé pour transférer des fichiers sur un réseau, notamment sur Internet.

Un serveur SSH (Secure Shell) est un type de serveur qui permet aux utilisateurs de se connecter à distance à un système informatique de manière sécurisée et d'exécuter des commandes sur ce système. SSH utilise un protocole de communication crypté pour sécuriser la connexion entre le client et le serveur, offrant ainsi un moyen sécurisé de contrôler des systèmes à distance.

- **Installer et configurer proFTPd** :

Exécuter la commande suivante pour installer **proFTPd** :

```
sudo apt update
sudo apt install proftpd
```

Une fois **proFTPd** installé, on peut éditer son fichier de configuration pour limiter le nombre de sessions de connexion et définir les identifiants.

sudo nano /etc/proftpd/proftpd.conf

Dans ce fichier, on peut ajouter les lignes suivantes pour limiter à une seule session de connexion :

MaxClients 1

Ensuite, pour définir les identifiants, ajoute ou modifie la section **DefaultRoot** pour inclure les

informations suivantes :

```
DefaultRoot ~
User laplateforme
Password Marseille13!
```

Après avoir effectué les modifications, on redémarre le service proFTPd pour appliquer les changements :

sudo systemctl restart proftpd

- **Installer et configurer SSH** :

On peut l'installer en utilisant la commande suivante :

sudo apt install openssh-server

Il est recommandé d'utiliser les paramètres par défaut pour SSH, mais doit s’assurer que le service est bien actif.

- **Utiliser le serveur SSH pour les connexions au FTP en SFTP, renforçant ainsi la sécurité** :

Avec SSH installé, le serveur FTP sera accessible via SFTP en utilisant le même nom d'utilisateur (laplateforme) et mot de passe (Marseille13!) que ceux définis pour proFTPd.

(On doit s’assurer simplement que le port 22 (par défaut pour SSH) est accessible depuis votre réseau)

Installation du Serveur DNS :

Un serveur DNS (Domain Name System) est un composant essentiel d'Internet. Son rôle principal est de traduire les noms de domaine faciles à retenir, tels que "example.com", en adresses IP numériques utilisées par les ordinateurs pour identifier et communiquer entre eux sur le réseau.

Installation et configuration du Serveur DNS :

- Sur la première machine virtuelle Debian (debian1):Installer un serveur DNS en utilisant la commande **sudo apt install bind9**
- Éditer le fichier de zone principale du serveur DNS en utilisant un éditeur de texte **nano** . Le fichier de zone principale se trouve généralement dans /**etc/bind/named.conf.local**.
- Ajouter une zone pour le domaine **ftp.com** avec le lien DNS souhaité "dns.ftp.com" pointant vers l'adresse IP de la deuxième machine (debian2) où le serveur FTP est installé :

```
zone "ftp.com" {
    type master;
    file "/etc/bind/db.ftp.com";
};
```

- Créer le fichier de zone pour le domaine **ftp.com** en utilisant le nom **dns.ftp.com** et définir les enregistrements DNS appropriés à l'intérieur.

```
$TTL    604800
@       IN      SOA     ns1.ftp.com. admin.ftp.com. (
                        2022091901 ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@       IN      NS      ns1.ftp.com.
dns     IN      A       192.168.1.2
```

- Redémarrez le service BIND pour appliquer les modifications :

  sudo service bind9 restart

Maintenant, le lien "dns.ftp.com" pointe vers l'adresse IP de la deuxième machine où le serveur FTP est installé.

Test de Connexion au Serveur SFTP

- **Lancement du Client SFTP :**

Ouvrez un client SFTP sur votre système local. Vous pouvez utiliser des clients SFTP tels que **FileZilla, WinSCP,** ou utiliser la commande **sftp** dans un terminal.

```
sftp laplateforme@dns.ftp.com
```

- **Connexion au Serveur SFTP :**

Dans le client SFTP, on spécifie l'adresse du serveur en utilisant le nom de domaine configuré : "**dns.ftp.com**".

On entre les identifiants fournis pour l'accès au serveur :

Identifiant : **laplateforme** Mot de passe : **Marseille13!**

Puis on lance la connexion pour établir la connexion au serveur SFTP.

- **Vérification de la Connexion :**

Une fois la connexion établie, on vérifie que on peut naviguer dans les répertoires de fichiers du serveur SFTP.

On peut essayer de transférer un fichier de notre système local vers le serveur SFTP et vice versa pour confirmer que les opérations de transfert fonctionnent correctement.

Paramètres de Sécurité Additionnels

Afin de renforcer la sécurité du serveur SFTP, plusieurs mesures supplémentaires peuvent être prises pour limiter l'accès non autorisé et garantir la confidentialité des données. Voici les paramètres de sécurité à mettre en place :

Restreindre l'Accès aux Identifiants Fournis :

- Configurer le serveur SFTP pour autoriser l'accès uniquement avec les identifiants fournis, c'est-à-dire l'identifiant "**laplateforme**" et le mot de passe "**Marseille13!**". Cela garantira que seuls les utilisateurs autorisés peuvent se connecter au serveur.

Changement du Port de Service :

- Configurer le serveur SFTP pour fonctionner sur un port non standard, tel que le port **6500**, au lieu du port par défaut (généralement le port 22). Cela rendra plus difficile pour les attaquants de scanner et d'accéder au service SFTP, car le port utilisé est différent de celui attendu.

Éviter les Connexions Anonymes ou Invitées :

- Désactiver toute possibilité de connexion anonyme ou invité sur le serveur SFTP. Cela garantira que seuls les utilisateurs authentifiés avec des identifiants valides peuvent accéder au serveur, renforçant ainsi la sécurité et la confidentialité des données stockées.

En combinant ces mesures de sécurité supplémentaires, on crée un environnement plus sécurisé pour le serveur SFTP, réduisant ainsi les risques potentiels d'accès non autorisé, de compromission des données et d'exploitation par des attaquants. Ces pratiques exemplaires en matière de sécurité renforcent la protection des données sensibles et contribuent à assurer l'intégrité et la confidentialité des informations stockées sur le serveur.