# <u> JOB 1:</u>







- Pour commencer à configurer SSH, on va vérifier si le serveur SSH est déjà installé. La commande "dpkg -l" liste les paquets installés sur Debian. En utilisant "grep openssh-server", on recherche spécifiquement le paquet "openssh-server" parmi la liste. Si le paquet est installé, il s'affiche dans les résultats, vérifiant ainsi la présence du service SSH sur le système.
- puis vu que le serveur SSH ne sera pas installé, on va l'installer en faisant comme commande : "sudo apt update" et "sudo apt install openssh-server", sudo apt update" met à jour la liste des paquets disponibles, s'assurant qu'il est à jour. "sudo apt install openssh-server" installe le serveur SSH (openssh-server) sur le système Debian, permettant ainsi la configuration du service SSH pour les connexions distantes sécurisées.
- En dernier lieu, nous allons utiliser la commande "ssh azerty@10.0.2.15-p 22", cette commande "ssh azerty@10.0.2.15 -p 22" est utilisée pour se connecter à un serveur distant via SSH. On spécifie l'utilisateur, l'adresse IP du serveur, et éventuellement le port ("22" dans ce cas-là). Cette commande permet d'établir une connexion sécurisée et nécessite une authentification avant d'accéder au serveur distant.

# <u> JOB 2:</u>

- Pour commencer nous allons installer Apache grâce à la commande suivante : "**sudo apt install apache2**", la commande "sudo apt install apache2" installe le serveur web Apache2 sur le système Linux basé sur Debian, tel qu'ubuntu. Apache2 permet d'héberger des sites web et de fournir des services web. Le préfixe "sudo" est utilisé pour exécuter la commande en tant qu'administrateur, car l'installation de logiciels nécessite des privilèges élevés.
- Ensuite nous allons utiliser la commande : "sudo systemctl status apache2" pour vérifier l'état du service Apache. La commande "sudo systemctl status apache2" est utilisée pour vérifier l'état du service Apache2 sur un système Linux. Il affiche des informations sur l'exécution, les erreurs éventuelles et l'état du service. Cette commande est utile pour le dépannage et la surveillance du serveur web Apache2.
- Nous allons taper "firefox 127.0.0.1/index.html" qui nous ouvrira la page de lancement d'Apache sur firefox.



at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Debian's Apache2 default configuration is different from the upstream default configuration, and split

installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed

### Configuration Overview

into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

/etc/apache2/

### **JOB 3:**

Il existe plusieurs types de serveurs Web. Le terme "serveur Web" peut être utilisé pour se référer à un programme informatique qui utilise le protocole de transfert hypertexte (HTTP) pour fournir du contenu Web sur le World Wide Web de l'Internet ou d'un ordinateur qui sert à cette fin en exécutant un tel logiciel . Les serveurs Web les plus populaires sont Apache, Nginx et Microsoft IIS .

Apache est le serveur Web le plus couramment utilisé dans le monde. C'est un logiciel open-source et offre des possibilités de modification pratiquement illimitées. Il prend en charge une vaste gamme de technologies web gratuits, y compris PHP, Perl, Python, Ruby et de nombreuses technologies propriétaires. Il est disponible pour presque tous les principaux systèmes d'exploitation et plates-formes matérielles, y compris Microsoft Windows, Linux, BSD et autres systèmes UNIX et OS / X 1.

- Microsoft IIS est le deuxième serveur le plus utilisé sur l'Internet. Il s'agit du serveur primaire utilisé dans le déploiement des technologies Microsoft telles que "asp.net" tout en soutenant diverses autres technologies Web offertes par des tiers. Il ne fonctionne que sur les systèmes d'exploitation serveur de Microsoft cependant, et est un logiciel propriétaire nécessitant une licence 2.
- Nginx est un serveur Web open-source qui peut également être utilisé comme proxy inverse, équilibreur de charge HTTP et proxy de messagerie électronique pour les protocoles SMTP, POP et IMAP . Il est connu pour sa capacité à gérer simultanément un grand nombre de connexions .
- Il existe également d'autres types de serveurs tels que les serveurs FTP (File Transfer Protocol), les serveurs DNS (Domain Name System), les serveurs de messagerie électronique.









- En premier temps, nous allons faire un "sudo apt update" pour mettre à jour la liste des paquets disponibles dans les dépôts de logiciels du système Linux.
- Ensuite, nous allons installer Bind9, pour ce faire exécutons la commande : "sudo apt install bind9", qui sert à installer Bind9 sur Linux.
- Ensuite, on va taper dans le terminal: "sudo nano /etc/bind/named.conf.options", cette commande permet de configurer un forwarder, elle permet donc d'ouvrir le fichier de configuration des options du serveur DNS BIND pour des modifications en tant qu'administrateur.
- Après, nous allons rentrer dans cette commande ce script :
- "forwarders {

10.0.2.15;

8.8.8.8:

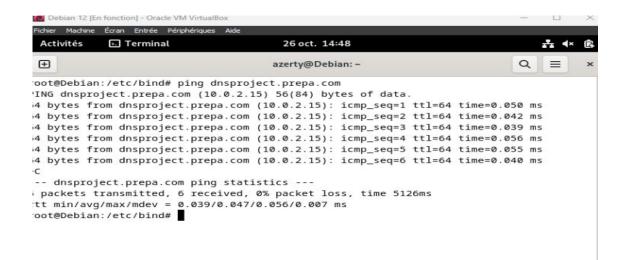
- Le bloc "forwarders" dans la configuration DNS BIND spécifie les serveurs DNS à consulter en cas d'incapacité à résoudre localement une requête DNS. Dans notre exemple, on utilise d'abord 10.0.2.15, un serveur local, puis 8.8.8.8, le serveur DNS public de Google, pour obtenir la réponse. Cela améliore la résolution DNS en utilisant ces serveurs comme relais.
- Ensuite, nous allons utiliser dans le terminal: "nano /etc/bind/named.conf.local", cette commande est utilisée pour éditer le fichier de configuration local de bind, un serveur DNS. Ce fichier contient des directives pour configurer les zones de domaines locaux et les serveurs DNS autoritaires. En l'éditant, on peut définir des paramètres spécifiques à notre domaine, tels que les enregistrements de zone et les autorisations de transfert de zone.
- Une fois rentrés dans le fichier nano, nous allons inscrire :
- "zone "local.lan" IN {

type master;

file "/etc/bind/dnsproject.prepa.com";

Le bloc de configuration "zone" indique au serveur DNS BIND de gérer la zone "local.lan" en tant que zone maître. Les informations de cette zone, telles que les enregistrements DNS, sont stockées dans le fichier "/etc/bind/dnsproject.prepa.com". Le serveur BIND est responsable de résoudre les noms de domaines de cette zone à l'aide de ce fichier.

- Donc nous allons taper dans le terminal: "s", cette commande copie un modèle de configuration de zone DNS ("db.local") vers un fichier ("dnsproject.prepa.com") que l'on peut personnaliser pour configurer la zone DNS du domaine "dnsproject.prepa.com".
- Ensuite, on va également taper dans le terminal : "nano /etc/bind/dnsproject.prepa.com", cette commande sert à éditer le fichier de configuration de zone pour le domaine "dnsproject.prepa.com" et à personnaliser la résolution des noms de domaine pour le domaine inscrit précédemment (dnsproject.prepa.com) ainsi que les enregistrements DNS de ce domaine.
- Avant d'appliquer les modifications, il nous reste à utiliser cette commande sur le terminal : "nano /etc/bind/named.conf.options" cette commande permet de changer à l'intérieur "any;" en "::1;".
- Il nous manque donc à redémarrer Bind en tapant : "sudo service bind9 restart" dans le terminal.
- Pour tester et voir si ça marche, il nous reste plus qu'à taper "ping dnsproject.prepa.com" sur le terminal.



# **JOB 5:**

### - Faites des recherches sur comment obtient-on un nom de domaine public ?

Pour obtenir un nom de domaine public, vous devez suivre les étapes suivantes :

- 1. Vérifiez la disponibilité du nom de domaine que vous souhaitez réserver.
- 2. Réservez le nom de domaine auprès d'un bureau d'enregistrement de nom de domaine, également appelé "registrar".
- 3. Protégez votre nom de domaine.

Le nom de domaine est un élément clé pour identifier votre site Web et permettre aux internautes d'y accéder facilement. Vous pouvez réserver un nom de domaine pour communiquer sur votre activité, rallier une clientèle et élargir votre réputation commerciale.

Il existe plusieurs sites Web qui offrent des services d'enregistrement de noms de domaine, tels que GoDaddy, Namecheap, Bluehost, etc. Vous pouvez également consulter la liste des extensions et des registres sur le site de l'IANA. Quelles sont les spécificités que l'on peut avoir sur certaines extensions de nom de domaine?

Les extensions de nom de domaine sont des suffixes qui sont ajoutés à la fin d'un nom de domaine pour identifier le type de site Web, l'emplacement géographique, l'organisation ou le but du site Web. Il existe plusieurs types d'extensions de nom de domaine, chacun ayant ses propres spécificités.

Les extensions de domaine génériques (gTLD) sont les plus courantes et comprennent des extensions telles que .com, .org, .net, .info, etc. Les extensions de domaine géographiques (ccTLD) sont spécifiques à un pays ou à une région et comprennent des extensions telles que .fr pour la France, .de pour l'Allemagne, etc. Les extensions de domaine de premier niveau (TLD) sont les plus courantes et comprennent des extensions telles que .edu pour les établissements d'enseignement, .gov pour les sites gouvernementaux.

Les spécificités des extensions de nom de domaine peuvent varier en fonction du type d'extension. Par exemple, les extensions de domaine géographiques peuvent être utilisées pour cibler un public local ou pour renforcer la crédibilité d'un site Web dans une région donnée. Les extensions de domaine génériques peuvent être utilisées pour identifier le type de site Web ou pour renforcer la crédibilité d'un site Web dans un secteur donné. Les extensions de domaine de premier niveau peuvent être utilisées pour identifier le but ou la nature d'un site Web.



### **JOB 6:**

- Pour commencer nous allons taper dans le terminal : "sudo nano /etc/apache2/sites-available/dnsproject.conf"
- Ensuite à l'intérieur de nano on tape : "<VirtualHost \*:80>

ServerName dnsproject.prepa.com DocumentRoot /var/www/html </VirtualHost>"

### Puis on ferme nano en enregistrant.

- On active notre Apache, pour ce faire on tape dans le terminal : "sudo a2ensite dnsproject.conf", cela permet d'activer Apache.
- On continue en redémarrant Apache en utilisant la commande : "sudo systemctl restart apache2".
- Puis pour finir on ajoute une entrée DNS locale en faisant comme commande dans le terminal : "sudo nano /etc/hosts".
- Et on ajoute dans le nano : "10.0.2.15 dnsproject.prepa.com", on quitte ensuite en enregistrant.
- Et pour le tester on tape dans la barre de recherche internet : "http://dnsproject.prepa.com" et on devrait avoir la page Apache qui s'ouvre.



This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### **Configuration Overview**

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

/etc/apache2/



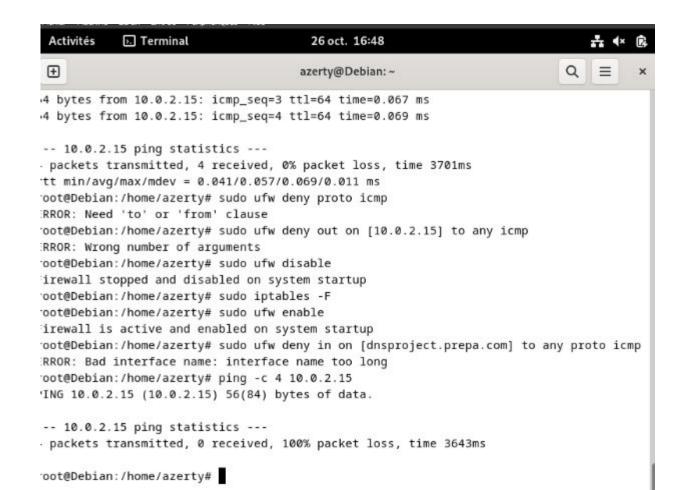
# **JOB 7:**





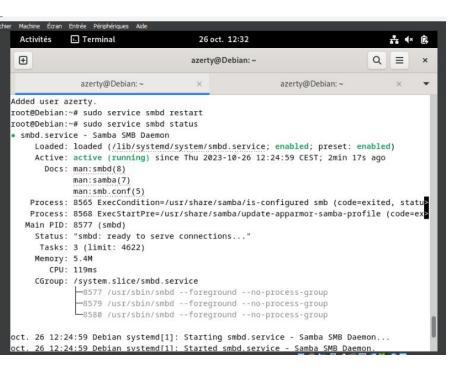


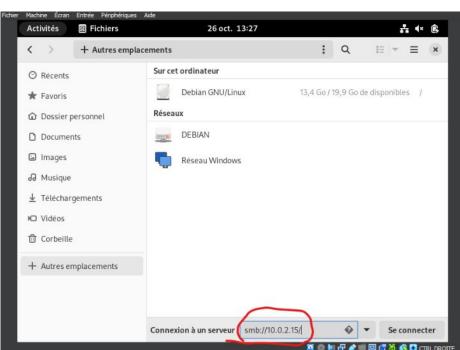
- En premier , on utilise "sudo apt-get update" pour mettre à jour la liste des paquets disponibles.
- Ensuite on utilise "sudo apt-get install ufw" pour installer UFW.
- Après on commence à configurer ufw, pour ce faire on tape "sudo ufw allow 80/tcp" qui permet d'autoriser le trafic HTTP (port 80).
- Ensuite on bloque le trafic LCMP (ping) en entrant dans le terminal : "sudo ufw deny proto icmp", sauf qui se peut que cette commande ne marche pas, il faudra alors taper dans le terminal : "sudo ufw deny 5353/udp".
- Il nous manque plus qu'à taper : "sudo ufw enable" dans le terminal pour activer UFW.
- En dernier on va tester la configuration UFW pour s'assurer que les règles ont été appliquées en tapant dans le terminal : "sudo ufw status".
- Pour voir si tout ce qu'on a fait marche, on va taper dans le terminal : "ping 10.0.2.15" si le ping ne marche pas c'est que c'est bon, on va également voir si la page Apache s'affiche sur internet en rentrant sur internet : "http://10.0.2.15" ou (et) encore "http://dnsproject.prepa.com".
- Il se peut que le ping marche toujours, pour régler ce problème-là, il suffit de taper la commande suivante : "sudo iptables -A INPUT -p icmp-icmp-type echo-resquest -j DROP" la commande consiste à bloquer les requêtes de ping entrantes (ICMP Echo Requests) vers un serveur en utilisant IPTables, renforçant ainsi la sécurité, mais peut perturber les outils de diagnostic réseau.



### **JOB 8:**







samba" cela permettra à Samba de s'installer. Ensuite on crée un dossier dans notre répertoire personnel, que l'on nommera "Partage", on lui attribuera les permissions de lecture/écriture à tous les utilisateurs en faisant la commande suivante dans le terminal : "chmod -R 777 ~/Partage".

En premier, on doit installer Samba, en premier on fait: "sudo apt-get update", ensuite on inscrit dans le terminal: "sudo apt-get install

- Puis on va commencer à configurer Samba en faisant la commande suivante dans le terminal : "sudo nano /etc/samba/smb.conf".
- Ensuite dans la commande nano, on ajoute tout à la fin cette commande : "[Partage]
  - browseable = yes read only = no
  - create mask = 0777 **directory mask = 0777", e**nsuite on oublie pas d'enregistrer avant de quitter.

comment = Dossier partagé path = /home/azerty/Partage

que tout marche normalement.

- Ensuite on doit créer un utilisateur Samba qui aura accès au dossier partagé, pour ce faire nous allons taper dans le terminal : "sudo
- smbpasswd -a azerty", ils vont juste après nous demander de créer un mot de passe et de le confirmer.
- Ensuite on redémarre Samba pour appliquer les modifications apportées en tapant dans le terminal : "sudo service smbd restart".
- On peut maintenant essayer de voir si ce qu'on a fait marche, en tapant en premier dans le terminal : "sudo service smbd status", si un message indiquant que Samba est actif (running) apparaît, c'est que ce qu'on a fait marche, ensuite on va dans nos fichiers sur Linux >

Autres emplacements > saisir l'adresse du serveur, à ce moment-la, on rentrera : "smb://10.0.2.15/", si le dossier "Partage" s'affiche c'est