DDWS

Job 01

Pour ce sujet, il vous faudra installer une VM Debian, avec interface graphique.

Télecharger une image disque de Debian sur debian.org

Utiliser un hyperviseur type Oracle VM VirtualBox, créer une VM (machine/nouvelle machine →séléctionner l'image disque préalablement téléchargée.

Si vous souhaitez faciliter l'utilisation de votre serveur depuis votre hôte, vous pouvez très bien lui configurer SSH.

Dans Debian, ouvrir le terminal entrer les lignes de commande suivante :
apt-get update
apt-get install openssh-server

Job 02

Installer un serveur Apache2

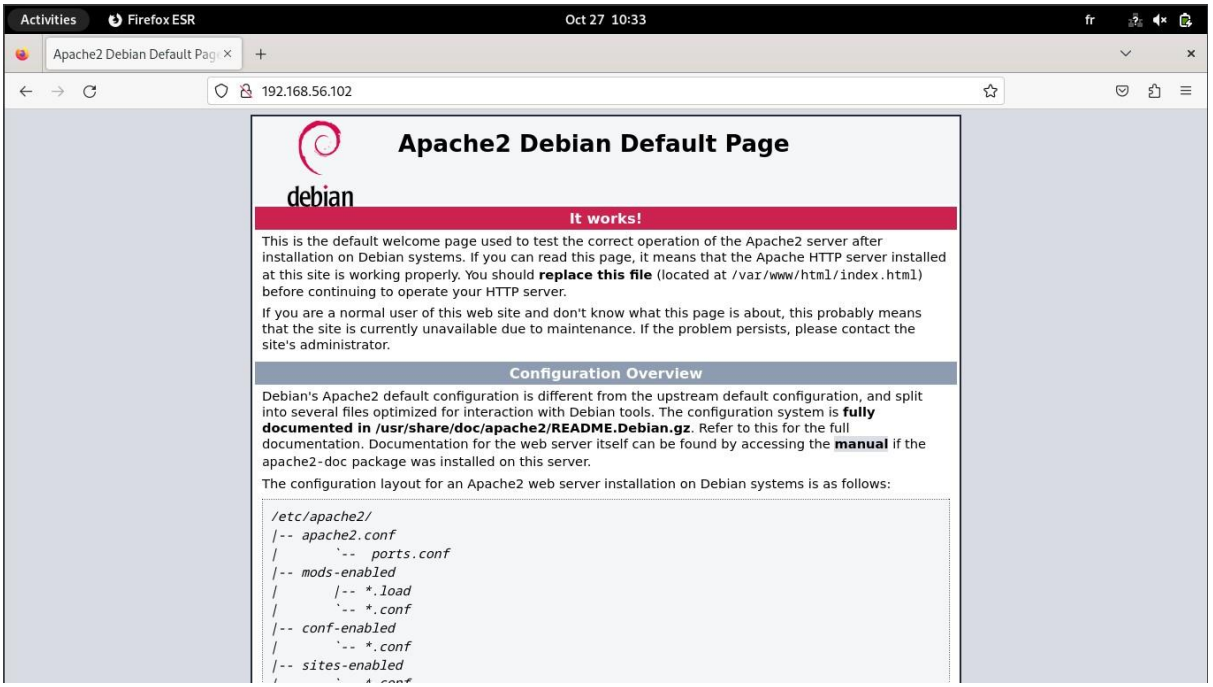
Dans le terminal, entrer les lignes de commande suivante :

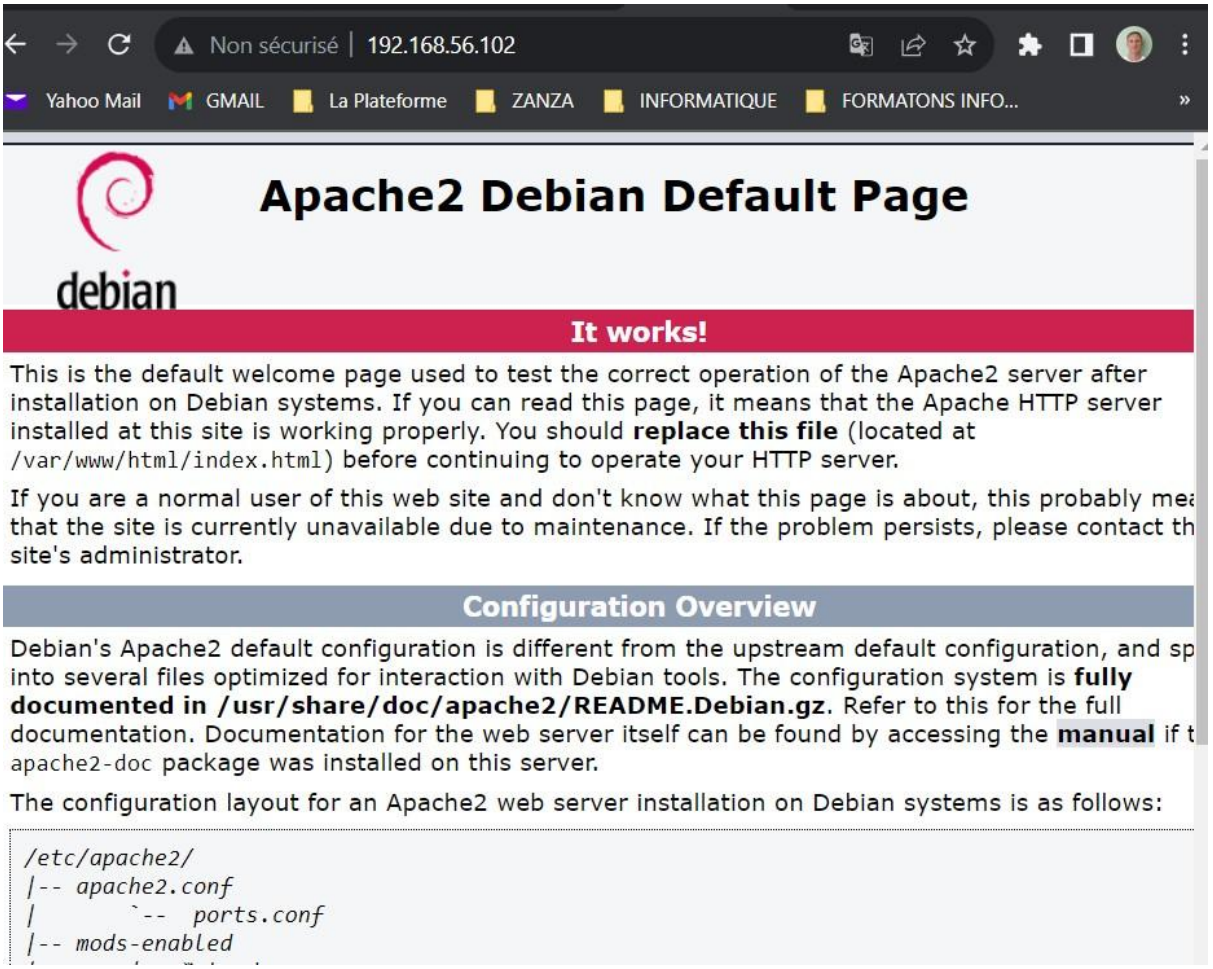
su
mot de passe
apt-get install apache2

systemctl status apache2
pour démvoir l'état d'apache2
systemctl start apache2
pour démarrer apache2
systemctl stop apache2
pour arrêter apache2

ip a
pour connaître l'adresse ip, en l'occurence, l'Ip est 192.168.56.102

Sur debian démarrer un navigateur et entrer l'IP qu'on vient de récupérer dans la barre de recherche, cela affiche :

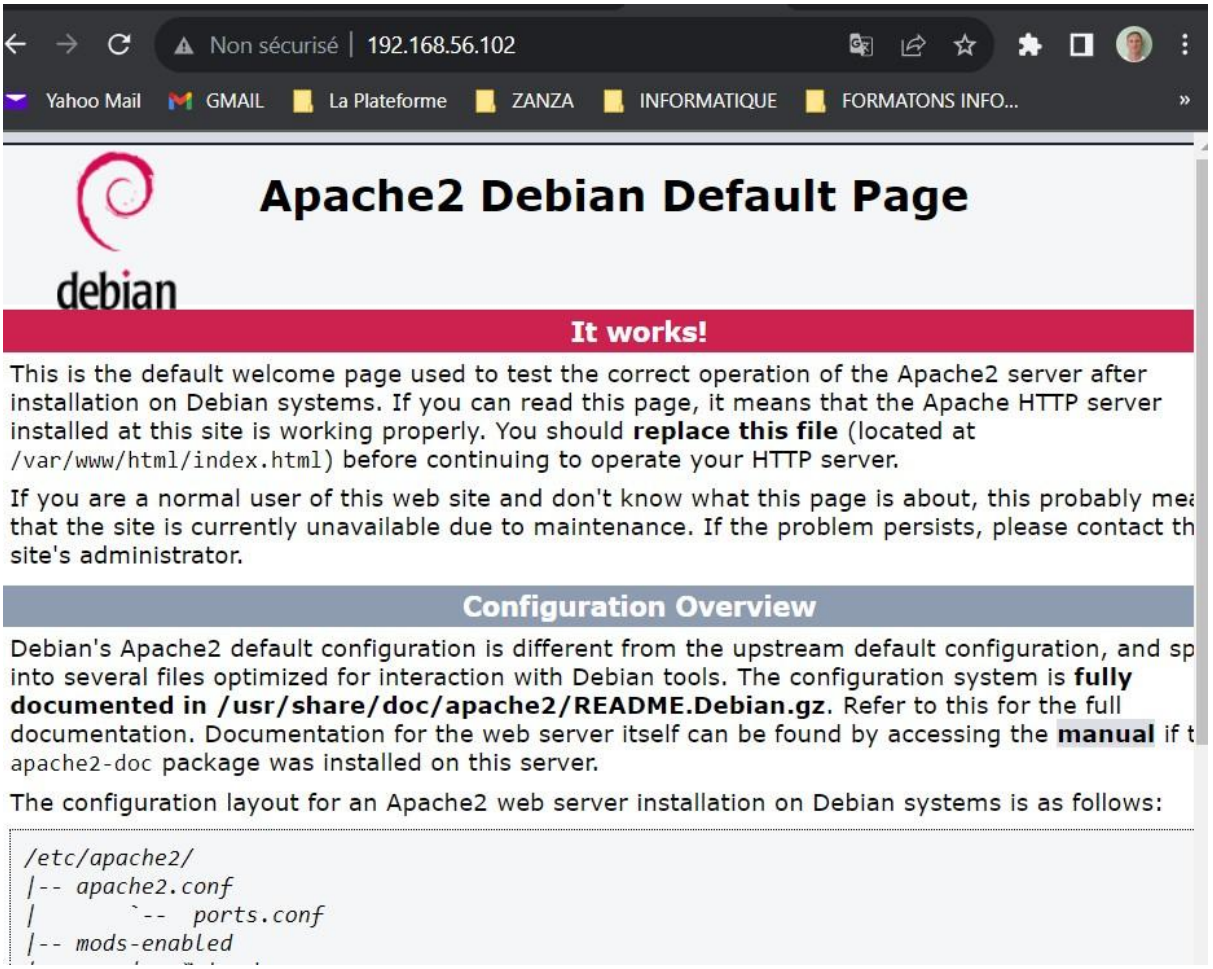

Activities
Firefox ESR
Oct 27 10:33
fr
Apache2 Debian Default Pag
192.168.56.102
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache 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/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled


Non sécurisé | 192.168.56.102
Yahoo Mail
GMAIL
La Plateforme
ZANZA
INFORMATIQUE
FORMATONS INFO...
Apache2 Debian Default Page
debian
It works!
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 mea
that the site is currently unavailable due to maintenance. If the problem persists, please contact th
site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and sp
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 t
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/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled

Le serveur web devra être atteignable depuis votre hôte.
Sur Debian, barre de menu du haut (ou symbole de clé plate) Périphériques / Réseau / Réglages réseaux / Mode d'accès réseau : Réseau privé hôte.

Cela ne semble pas fonctionner si ce paramètre est sur NAT.

Maintenant sur windows (hôte), le navigateur à bien accès au serveur apache (192.168.56.102 au dernier démarrage de debian).



Job 03

Produisez une documentation sur les différents serveurs Web existants ainsi que les avantages et inconvénients de chacun des serveurs.

Un serveur Web est généralement un ordinateur installé dans un data center
Il stocke les fichiers qui servent aux navigateurs pour afficher les sites web aux clients

C'est un élément de base du modèle client/serveur.

Le serveur utilise le protocole HTTP pour fournir les fichiers que les utilisateurs ont demandé via des requêtes transmises par les clients.

Tous les ordinateurs qui hébergent des sites Web doivent disposer de programmes serveurs Web. Les principaux serveurs Web sont :

- Apache (le plus répandu)
- IIS (Internet Information Server) de Microsoft
- Nginx (prononcé engine X) de NGINX.
- LiteSpeed
- NetWare de Novell
- Google Web Server (GWS)
- La gamme des serveurs Domino d'IBM.

2 OS sont utilisés par les serveurs :
Linux
Windows

Les serveurs utilisent aussi en background des programmes clés appelés Daemons (software servers) :

- HTTP server
- FTP server
- Email server
- DataBase server

Il y a aussi de nombreux programmes en background mais accessibles par les utilisateurs tels que WordPress, Dupral …

Les principaux enjeux pour la sélection du serveur :
Stabilité, performance, sécurité, facilité d'utilisation, compatibilité

Serveurs Web Apache

Le serveur web Apache est l'un des serveurs web les plus populaires sur le marché. Il est open source et peut être installé sur la plupart des systèmes d'exploitation tels que Windows, Linux, macOS, etc. Le serveur web Apache est conçu pour gérer des sites web statiques et dynamiques.

Avantages:
Peut être facilement personnalisé avec des modules tiers
Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, etc.
Disponible gratuitement et open source
Inconvénients:
Difficile à configurer pour les débutants
Peut nécessiter des ressources matérielles supplémentaires pour gérer des charges élevées de trafic web
Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source

Serveurs Web Nginx

Nginx est un serveur web open source conçu pour gérer les sites web à haute performance. Il est souvent utilisé pour les sites web à haute charge de trafic tels que les sites de médias sociaux, les sites de commerce électronique, les sites de streaming, etc.
Avantages:
Conçu pour gérer les sites web à haute performance avec une charge élevée de trafic
Peut être facilement personnalisé avec des modules tiers
Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, SMTP, POP3, etc.
Disponible gratuitement et open source
Inconvénients:
Peut être difficile à configurer pour les débutants
Peut nécessiter des ressources matérielles supplémentaires pour gérer des charges élevées de trafic web
Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source

Serveurs Web Microsoft IIS

Microsoft IIS est un serveur web développé par Microsoft pour les systèmes d'exploitation Windows. Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites d'entreprise, les sites d'informations, etc.
Avantages:
Intégré avec les systèmes d'exploitation Windows
Facile à configurer pour les utilisateurs de Windows
Prend en charge plusieurs protocoles de communication tels que HTTP, HTTPS, FTP, SMTP, etc.
Inconvénients:
Ne fonctionne que sur les systèmes d'exploitation Windows
Peut ne pas être adapté aux sites web à haute performance avec une charge élevée de trafic
Les mises à jour de sécurité peuvent être retardées en raison du processus de développement propriétaire de Microsoft

Serveurs Web Lighttpd

Lighttpd est un serveur web open source conçu pour être léger et rapide. Il est souvent utilisé pour les sites web à faible charge de trafic tels que les sites de développement, les blogs personnels, etc.
Avantages:

Conçu pour être léger et rapide
Peut gérer
des charges de trafic légères à moyennes
Peut être facilement personnalisé avec des modules tiers
Disponible gratuitement et open source
Inconvénients:
Peut ne pas être adapté aux sites web à haute performance avec une charge élevée de trafic
Peut être difficile à configurer pour les débutants
Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source

Serveurs Web Node.Js

Node.js est un environnement d'exécution JavaScript open source conçu pour exécuter des applications côté serveur. Il est souvent utilisé pour les applications web à haute performance telles que les applications de streaming en temps réel, les applications de chat, etc.
Avantages:
Conçu pour les applications web à haute performance
Peut être facilement personnalisé avec des modules tiers
Disponible gratuitement et open source
Peut être utilisé pour exécuter des applications de backend et de frontend
Inconvénients:
Peut nécessiter des compétences en développement JavaScript pour la configuration et la personnalisation
Peut ne pas être adapté aux sites web à faible charge de trafic
Les mises à jour de sécurité peuvent être retardées en raison du processus de développement open source

En conclusion, il existe plusieurs types de serveurs web qui conviennent à des tâches spécifiques en fonction des exigences de votre site web. Apache et Nginx sont les serveurs web les plus populaires pour gérer des charges élevées de trafic, tandis que Microsoft IIS et Lighttpd sont plus adaptés aux sites web à faible charge de trafic. Node.js est idéal pour les applications web à haute performance. Il est important de comprendre les avantages et les inconvénients de chaque serveur web avant de faire votre choix final.

Job 04

Mettez en place un DNS sur votre serveur Linux qui fera correspondre l'adresse IP de votre serveur au nom de domaine local suivant : "dnsproject.prepa.com"
Votre serveur devra donc pouvoir se ping via ce nom de domaine.

Bind
"Berkeley Internet Name Daemon"
c'est l'un des serveurs DNS (Domain Name System) les plus populaires, il est largement utilisés sur les systèmes Unix et Linux

Repasser en réseau NAT :
Sur Debian, barre de menu du haut (ou symbole de clé plate) Périphériques / Réseau / Réglages réseaux / Mode d'accès réseau : réseau NAT.

Les packages à installer sont :

bind9	serveur BIND
bind9-host	client BIND
bind9utils	outils DNS

Dans le terminal de debian, entrer la commande suivante :

apt install bind9

Installer les paquets

apt install -y bind9utils bind9-docs dnsutils

Il ne trouve pas bind9-docs

apt install –y bind*

permet d'installer directement tous les paquets de bind

Ensemble de fichiers de configuration que l'on va modifier au fur et à mesure :
/etc/bind/named.conf
/etc/bind/named.conf.options
/etc/bind/named.conf.local
/etc/bind/db.dnsproject.prepa.com

ip : 10.0.2.15
ip : 192.168.56.102

named.conf

Fichier de configuration de BIND.
Il permet de déclarer les fichiers de zones.
Généralement situé dans le répertoire **/etc/bind/named.conf**.
Y accéder en utilisant un éditeur de texte ou une commande comme nano
nano /etc/bind/named.conf :

```
include “/etc/bind/named.conf.options”;
include “/etc/bind/named.conf.local”;
include “/etc/bind/named.conf.default-zones”;
```

named.conf.options

Fichier de configuration qui définit le comportement global du serveur BIND.
Notamment la manière dont il gère les requêtes DNS et interagit avec d’autres serveurs DNS sur internet
nano /etc/bind/named.conf.options :

```
options {
    directory "/var/cache/bind";
    version "Bind Server";

    forward {
        8.8.8.8;
        1.1.1.1;
    };

    listen-on port 53 {localhost; 192.168.56.102;};
    dnssec-validation auto;
    allow-recursion { 127.0.0.1; };
    auth-nxdomain no;
    listen-on-v6 { any;};
};
```

forwarders *: Cette option permet de spécifier des serveurs DNS vers lesquels le serveur BIND doit envoyer des requêtes DNS pour la résolution des noms de domaine. Cela peut être utile pour configurer des serveurs DNS de relais ou pour utiliser des serveurs DNS spécifiques pour améliorer les performances ou la sécurité.*

listen-on *: Cette option définit les adresses IP et les ports sur lesquels le serveur BIND écoutera les requêtes DNS. Vous pouvez spécifier les adresses IP locales sur lesquelles le serveur BIND doit écouter.*

allow-query *: Cette option permet de définir quelles adresses IP sont autorisées à effectuer des requêtes DNS auprès du serveur BIND. Vous pouvez restreindre l'accès pour des raisons de sécurité.*

***recursion** : Cette option contrôle si le serveur BIND effectue des résolutions récursives pour les clients. Si activée, le serveur effectuera des requêtes DNS pour les clients qui ne sont pas capables de résoudre eux-mêmes les noms de domaine.*

***forward only** : Cette option indique au serveur BIND de ne faire que des résolutions de noms de domaine pour lesquels il agit en tant que serveur de relais. Il n'effectuera pas de résolutions récursives.*

***dnssec-enable** : Active ou désactive la prise en charge de DNSSEC (Domain Name System Security Extensions), un ensemble de mécanismes de sécurité pour garantir l'intégrité et l'authenticité des données DNS.*

named.conf.local

Edition du fichier de configuration principal BIND
nano /etc/bind/named.conf.local:

```
zone "dnsproject.prepa.com" {
    type master;
    file "/etc/bind/db.dnsproject.prepa.com";
    notify yes;
    allow-update { none; };
    allow-transfer { 192.168.56.102; };
    also-notify { 192.168.56.102; };
};
```

db.dnsproject.prepa.com

Création et édition du fichier de zone
afin de définir les enregistrements DNS appropriés pour votre domaine
(les ; sont des commentaires)

Ce fichier de zone déclare un enregistrement SOA (Start of Authority) pour le domaine, un enregistrement NS (Name Server), et un enregistrement A pour l'adresse IP du domaine

nano /etc/bind/db.dnsproject.prepa.com

```
; Fichier de zone pour dnsproject.prepa.com

$TTL 86400
        @   IN  SOA ns.dnsproject.prepa.com. admin.dnsproject.prepa.com. (
                    202310261   ;   serial
                    3600        ;   refresh
                    1800        ;   retry
                    604800      ;   expire
                    86400 )     ;   minimum

        ; Enregistrements pour le domaine
```

```
        IN  NS  ns.dnsproject.prepa.com.    ;

@       IN  A   10.0.2.4
ns      IN  A   10.0.2.4
www     IN  A   10.0.2.4
```

Vérification de la syntaxe du fichier de configuration BIND en exécutant la commande suivante :

```
sudo named-checkconf
```

On vérifie enfin que le service est bien configuré:

```
named-checkconf  /etc/bind/named.conf
named-checkzone  dnsproject.prepa.com /etc/bind/db.dnsproject.prepa.com
```

Redémarrez le service DNS :

```
sudo service bind9 restart
```

Vérifiez que le service a redémarré avec succès :

```
sudo systemctl status bind9
```

Job 05

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

Il faut vérifier la disponibilité du nom de domaine et le louer chez un bureau d'enregistrement (registrar)
https://www.nom-domaine.fr/ ou ionos , ovh, LWS, etc…
Ces registrars sont coordonnées au niveau national par l'AFNIC (association chargée de gérer le registre des noms de domaine en France) et au niveau international par l'ICANN

Quelles sont les spécificités que l'on peut avoir sur certaines extensions de nom de domaine ?
Extensions de noms de domaine ou domaines de premier niveau ou TLD Top-Level Domain

Géographiques (ccTLDs - Country Code Top-Level Domains) avoir une adresse légale dans le pays en question : .fr .it

Thématiques ou sectorielles : .gov pour les agence gouvernementale, .edu education

Restrictions professionnelles : . museum .aero

Restrictions basées sur la localisation : .asia

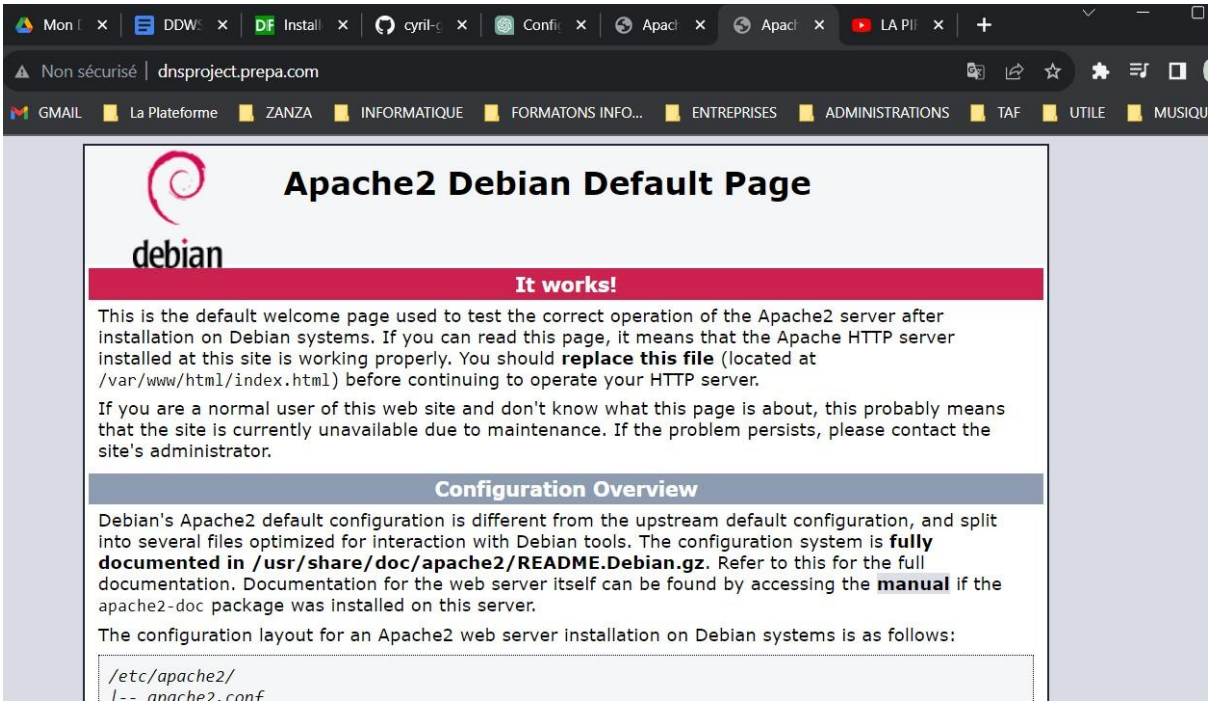
Restrictions basées sur la langue ou le script : .pyc pour le russe en cyrillique

Restrictions basées sur la langue ou le script

Extensions ouvertes (gTLDs - Generic Top-Level Domains) : Par exemple, certaines extensions peuvent être réservées pour des marques déposées (gTLDs personnalisés) ou être proposées à un coût plus élevé (premium domains).

Job 06

Connectez votre hôte au nom de domaine local de votre serveur, pour que votre page apache soit accessible via ce même nom de domaine.



Job 07

Mettez en place un pare-feu en utilisant ufw sur votre serveur principale de manière que votre hôte puisse accéder à la page apache par défaut, mais qu'il ne puisse plus ping votre serveur.

Installation de UFW (si ce n'est pas déjà fait) :

```
apt install ufw -y
```

contrôle d'ufw

```
systemctl status ufw
```

Cela nous apprend que le pare-feu n'est pas activé.

Il faut le paramétrer, l'activer et enfin vérifier son état :

```
ufw allow 22/tcp
ufw allow 80/tcp
ufw allow 443/tcp
ufw enable
ufw status
```

Job 08

Mettez en place sur votre serveur un dossier partagé avec les autres membres de votre réseau (soit la où les autres machines virtuelles). Ils pourront partager des fichiers dans ce dossier, ainsi que récupérer des fichiers depuis ce dossier.

Ce dossier doit être accessible dans votre gestionnaire de fichier en interface graphique.

Pour aller plus loin...

Faites l'installation d'un certificat pour votre serveur web, pour activer le HTTPS sur votre serveur web Apache.
Vous devrez donc pouvoir utiliser votre serveur web de manière sécurisée.
N'hésitez pas à utiliser openSSL pour générer votre certificat.
Renseignez-vous aussi sur la différence entre les certificats SSL donnés par des organismes extérieurs et le vôtre auto-signé ?

Pourquoi votre certificat apparaît-il comme non sécurisé dans votre navigateur ?
Répondez à ces questions dans votre documentation

Pour aller encore plus loin ...

Installer un DHCP en dehors de celui de VMWare.

Rendu
Le projet est à rendre sur https://github.com/prenom-nom/DDWS
Le rendu devra contenir votre documentation complète de votre installation et les Réponses aux questions posées.
Pensez à mettre votre repos en public.