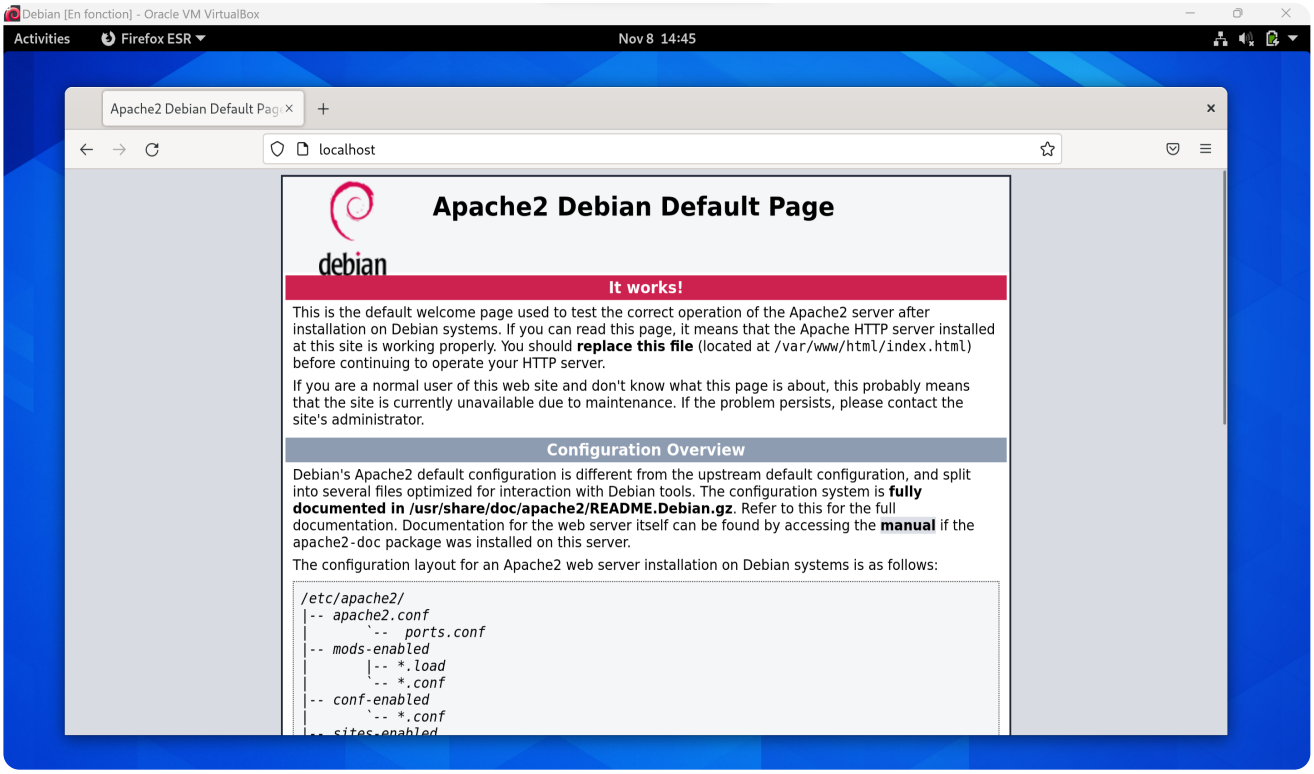
DDWS-DOC

JOB 01

Pour cet exercice j'utilise une machine virtuelle Debian avec interface graphique.
Je choisis VirtualBox comme hyperviseur.
Je switch mon utilisateur en root.

JOB 02

```
apt update upgrade
apt install apache2
```



JOB 03

il existe des dizaines de serveurs web différents.

Apache HTTP server est le plus utilisé, il est open source, stable, polyvalent et mis a jour régulièrement.

Nginx est beaucoup plus performant qu'Apache dans le traitement de nombreuses demandes simultanées, et utilise moins de stockage par connexion client.

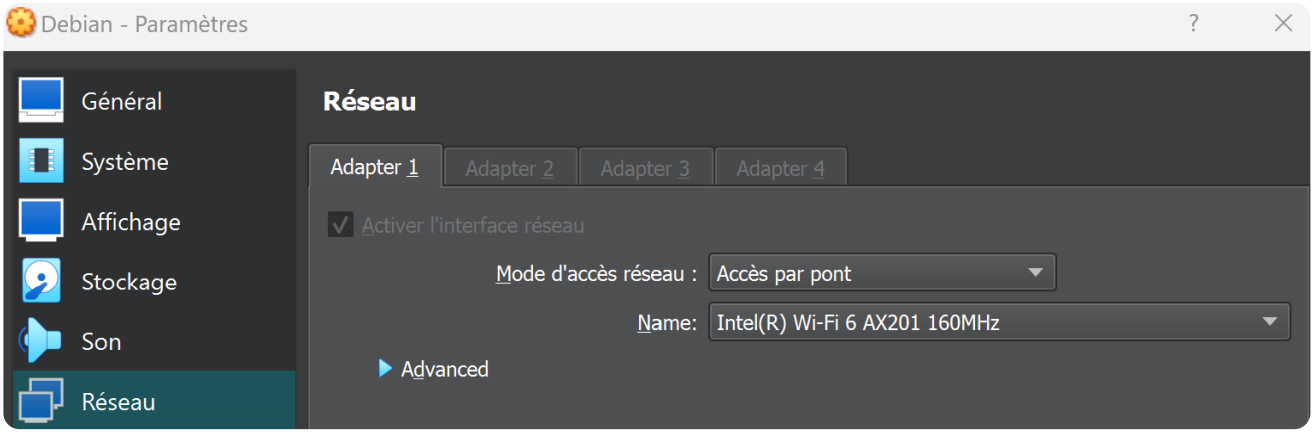
IIS quant à lui propose une prise en charge avancée des langages de programmation. Il s'installe et s'administre via le gestionnaire de serveur comme tous les rôles windows server.

JOB 04

J'installe bind9 et les utilitaires nécessaires à la configuration d'un serveur DNS.

```
apt -y install bind9 bind9utils dnsutils
```

Je change ensuite le mode d'accès réseau de ma machine virtuelle (bridge).



J'utilise la commande hostname -I pour connaître mon IP.

```
hostname -I
10.10.29.213
```

Je me déplace ensuite dans le dossier où sont situées les config de bind.

```
cd /etc/bind
```

Je modifie donc les fichiers de configuration pour associer l'addresse IP au nom de serveur dnsproject ainsi qu'au nom de domaine prepa.com.

```
cp dblocal direct
nano direct
```

```
$TTL    604800
@       IN      SOA     prepa.com. dnsproject.prepa.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dnsproject.prepa.com.
```

```
dnsproject      IN      A       10.10.29.213
www     IN      CNAME   dnsproject.prepa.com.
```

```
cp direct inverse
nano inverse
```

```
$TTL    604800
@       IN      SOA     prepa.com. dnsproject.prepa.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dnsproject.prepa.com.
dnsproject      IN      A       10.10.29.213
213     IN      PTR     dnsproject.prepa.com.
```

```
nano named.conf.local
```

```
zone "prepa.com" IN {
        type master;
        file"/etc/bind/direct";
};
zone "29.10.10.in-addr-arpa" IN {
        type master;
        file"/etc/bind/inverse";
};
```

```
nano /etc/resolv.conf
```

```
search prepa.com
nameserver 10.10.29.213
```

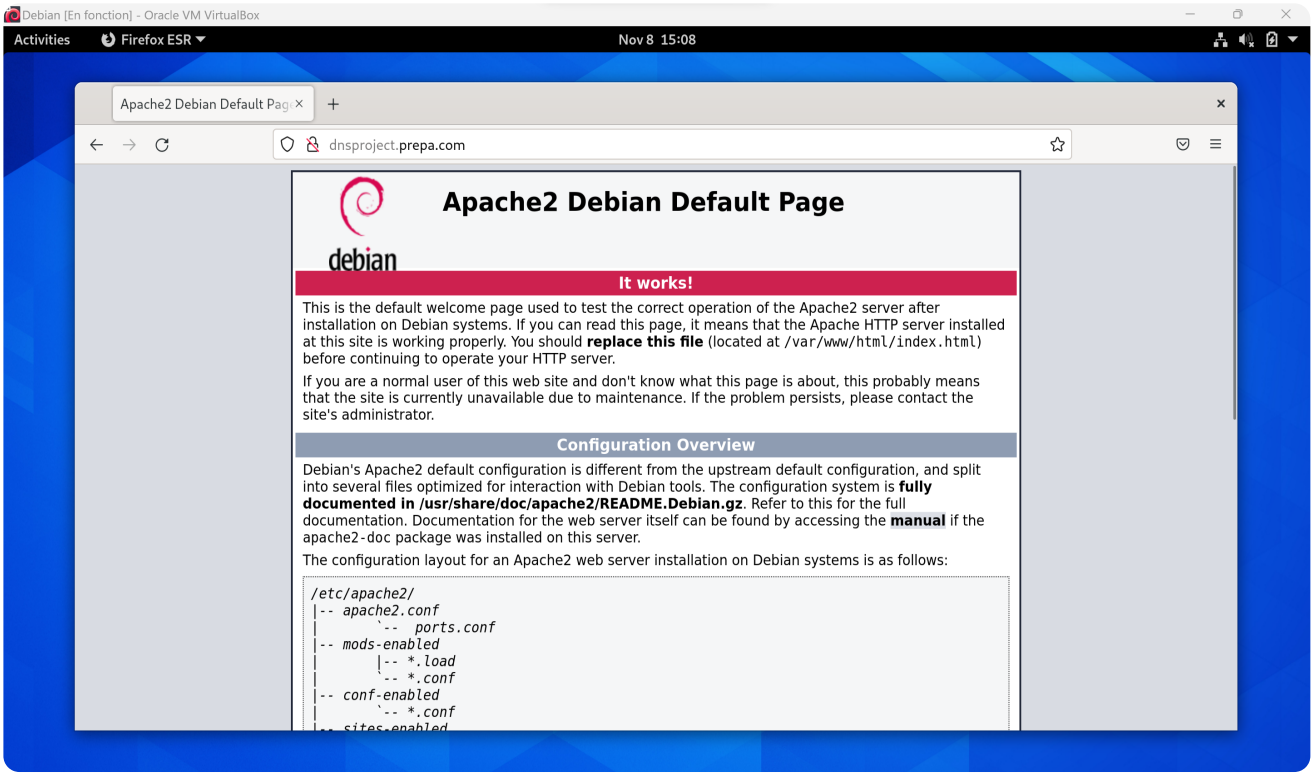
Je redémarre alors le service bind9 pour appliquer les changements.

```
systemctl restart bind9
```

Je peux maintenant ping le nom de domaine.

```
ping dnsproject.prepa.com
```

Apache est dorénavant accessible via le nom de domaine sur la machine virtuelle.



JOB 05

Pour acquérir le nom de domaine désiré, il faut s'adresser aux nombreux prestataires agréés. Il existe deux types de nom de domaine dits de "premier niveau" :

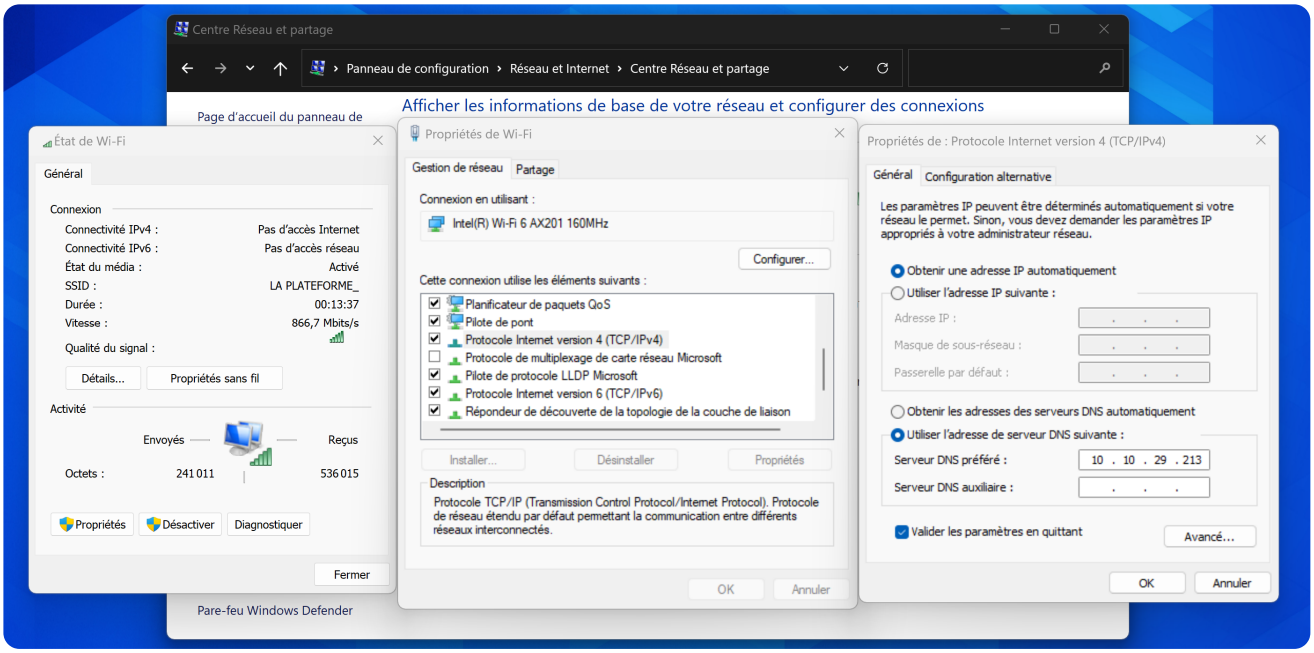
- Les domaines génériques (gTLD), certains peuvent être libres (.com, .net, .info, .org...) et d'autres réservées à certains organismes (.int, .edu, .gov...).
- Les codes pays (ccTLD) qui sont composés de 2 lettres conformément à la norme ISO 3166 (.fr, .es, .it, .uk, .de...). On compte actuellement 244 ccTLD.

Le choix de l'extension du nom de domaine dépend de la stratégie commerciale et du public-cible : Pour un positionnement à l'echelle mondiale, l'extension de domaine .com sera la plus adaptée. Bien que conçue initialement pour les organisations commerciales elle est aujourd'hui l'extension la plus utilisée. Elle est conventionnelle quand on echange une adresse internet.

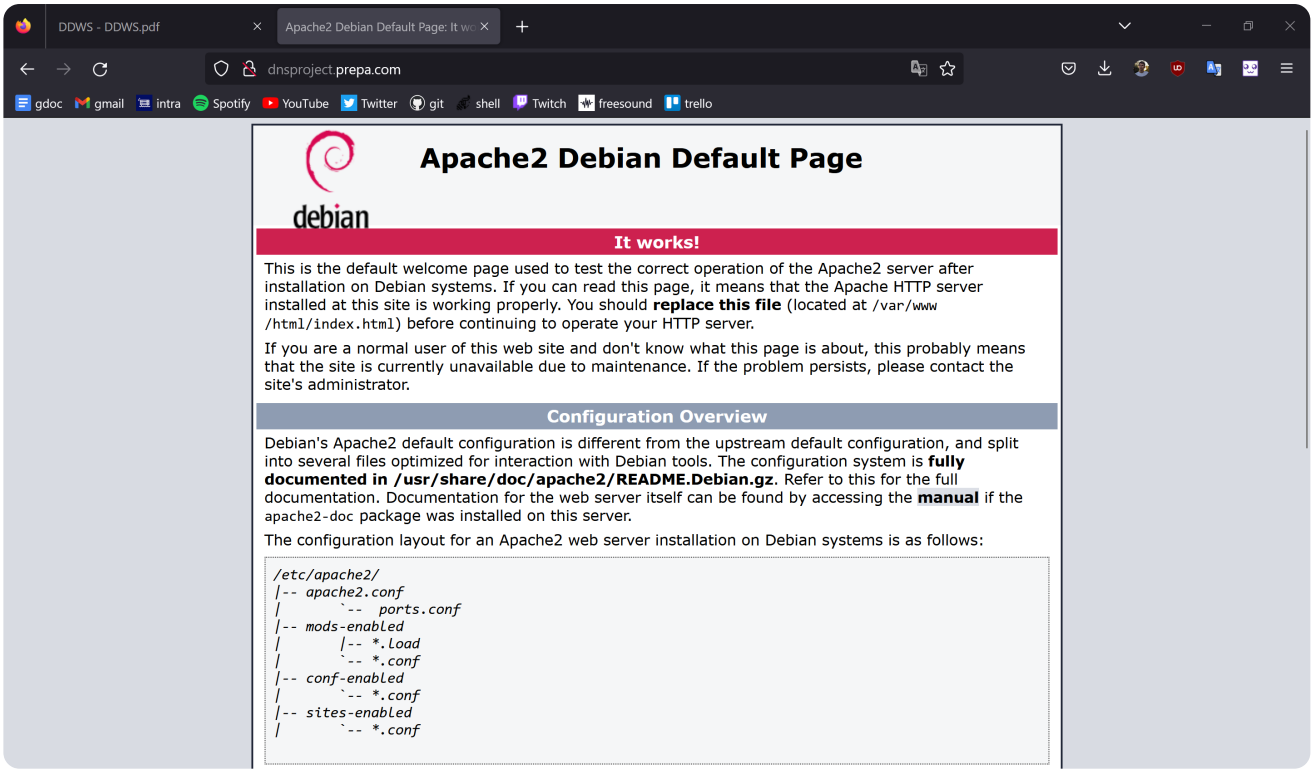
Le choix d'une ccTLD réduira nécessairement la portée du site mais aura l'avantage d'illustrer l'ancrage des activités présentées dans l'aire géographique choisie et de rassurer les visiteurs du pays en question.

JOB 06

Il suffit maintenant d'ajouter l'IP de la machine virtuelle en tant qu'adresse de serveur DNS préférée sur son host.



Apache peut maintenant être accédé depuis le nom de domaine.



JOB 07

J'installe les paquets nécessaires à la mise en place du DHCP.

```
apt -y install isc-dhcp-server
dpkg -l | grep dhcp-server
```

Ainsi que les paquets nécessaires au test du service.

```
apt -y nmap install
```

Puis je configure le serveur.

```
nano /etc/default/isc-dhcp-server
```

```
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
INTERFACESv4="enp0s3"
```

```
nano /etc/dhcp/dhcpd.conf
```

```
authoritative;
subnet 10.10.29.0 netmask 255.255.255.0 {
  range 10.10.29.100 10.10.29.200;
  option domain-name-servers 10.10.29.213;
  option domain-name "prepa.com";
  option routers 10.10.29.213;
  option broadcast-address 10.10.29.255;
  default-lease-time 6000;
  max-lease-time 7200;
}
```

Je restart le service pour appliquer la config.

```
systemctl restart isc-dhcp-server
```

Je teste alors si le DHCP offre une IP avec la commande suivante :

```
nmap --script broadcast-dhcp-discover
```

```
root in ~
➜ nmap --script broadcast-dhcp-discover
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 14:27 CET
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 10.10.29.144
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 10.10.29.213
|     IP Address Lease Time: 5m00s
|     Subnet Mask: 255.255.255.0
|     Router: 10.10.29.213
|     Domain Name Server: 10.10.29.213
|     Domain Name: prepa.com
|_    Broadcast Address: 10.10.29.255
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.27 seconds
```

JOB 09

J'installe le paquet ufw pour le firewall.

```
apt -y install ufw
```

Puis je le configure.

```
cd /etc/ufw
nano before.rules
```

```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type source-quench -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

Je démarre et relance le service pour appliquer la config.

```
ufw enable
ufw reload
```

Je teste de ping depuis mon hôte.

```
C:\Windows\System32>ping dnsproject.prepa.com

Envoi d'une requête 'ping' sur dnsproject.prepa.com [10.10.29.213] avec 32 octets
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 10.10.29.213:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Je peux maintenant désactiver le pare-feu.

```
ufw disable
```

Et tester de ping à nouveau depuis mon hôte.

```
C:\Windows\System32>ping dnsproject.prepa.com

Envoi d'une requête 'ping' sur dnsproject.prepa.com [10.10.29.213] avec 32 octets
```

```
Réponse de 10.10.29.213 : octets=32 temps<1ms TTL=64
Réponse de 10.10.29.213 : octets=32 temps<1ms TTL=64
Réponse de 10.10.29.213 : octets=32 temps<1ms TTL=64
Réponse de 10.10.29.213 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.10.29.213:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Pour aller plus loin...

Je démarre le module SSL d'Apache.

```
a2enmod ssl
```

Je redémarre le service Apache.

```
systemctl restart apache2
```

Je génère une clé et un certificat SSL.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/dnsp
```

Après avoir backup le fichier config par défaut, je remplace le port 80 avec le port 443 pour activer la connexion https.

```
cd /etc/apache2/sites-available/
cp default-ssl.conf dnsproject.prepa.com-ssl.conf
nano dnsproject.prepa.com-ssl.conf
```

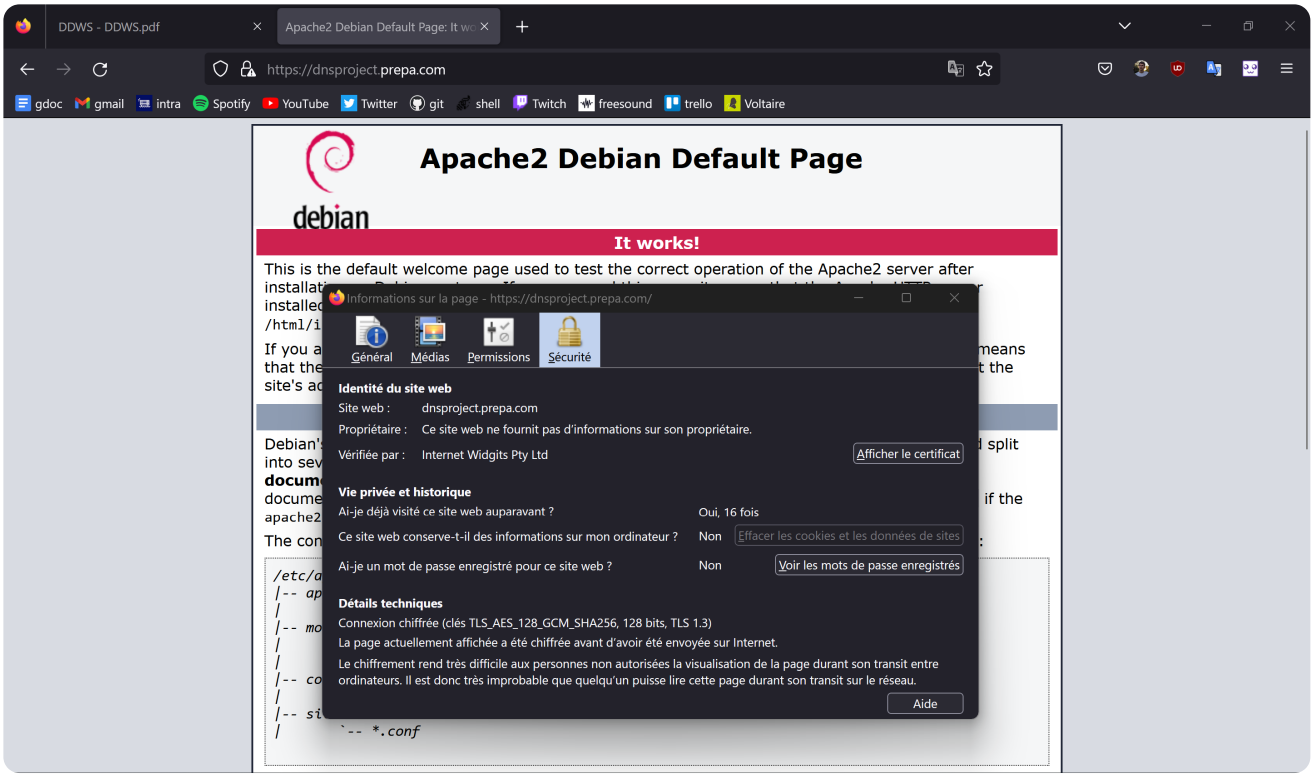
```
<VirtualHost *:443>

SSLEngine on
SSLCertificateKeyFile /etc/ssl/private/dnsproject.prepa.com.key
SSLCertificateFile /etc/ssl/certs/dnsproject.prepa.com.crt
```

J'active la version SSL du nom de domaine et je redémarre le service.

```
a2ensite dnsproject.prepa.com-ssl.conf
systemctl restart apache2
```

Mon navigateur m'avertit qu'il n'a pas confiance en ce certificat car il est auto-signé, je peux malgré tout accéder au site.



- Un certificat auto-signé est un certificat SSL gratuit qui est généré par le serveur qui l'a édité. Il n'est donc pas émis par une Autorité de Certification. Le SSL permet de garantir une navigation sécurisée entre l'utilisateur et le site web, il certifie l'identité du webmaster.
- Les certificats auto-signés n'étant pas émis par une Autorité de Certification, ils affichent une erreur de sécurité sur tous les navigateurs web, ce qui incite les visiteurs à quitter la page.