

## JOB 1-3

### Les différents serveurs web:

Apache HTTP Server

NGINX

Apache Tomcat

BusyBox httpd

Google Web Server

Internet Information Services (IIS)

lighttpd

Monkey web server

Hiawatha

NodeJS

Sun Java System Web Server

Tengine

Zeus Web Server

Gunicorn

Zazouminiwebserver

Abyss Web Server

Nous allons comparer Apache2 et NGINX qui sont les plus utilisés dans le monde.

### Les architectures

L'architecture **APACHE** est axée sur les processus ce qui consiste à créer un nouveau fil ou *thread* pour chaque requête.

Ce processus permet d'accomplir de nombreuses tâches en simultanée néanmoins son point faible est que cela consomme beaucoup de ressources.

L'architecture **NGINX** axée sur les événements ce qui consiste à traiter plusieurs requêtes dans un seul thread. Il peut exécuter des milliers de requêtes en un seul thread ce qui permet d'économiser des ressources.

## Les performances

Pour le contenu statique (PHP,CSS) **NGINX** est beaucoup plus rapide que **Apache** et consomme beaucoup moins de ressources (ram , cpu).

APACHE  
**10770 req/s**  
@ 512 PARALLEL REQUESTS

NGINX  
**20232 req/s**  
@ 512 PARALLEL REQUESTS

Pour le contenu dynamique (page animé) les 2 sont équivalents néanmoins **NGINX** nécessite d'utiliser un processus externe tandis que apache peut le faire lui même.

APACHE  
**108 req/s**  
@ 16 PARALLEL REQUESTS

NGINX  
**108 req/s**  
@ 16 PARALLEL REQUESTS

## Support de l'OS

**Apache** supporte les systèmes Unix tels LINUX et BSD et également MS Windows.

Tandis que **NGINX** supporte tous les systèmes UNIX et partiellement Windows.

## Configuration et distribution centralisée

**Apache** permet d'avoir des configurations additionnelles sur la base de répertoire via .htaccess mais cela le rendra un peu moins rapide pour interpréter les requêtes utilisateur.

Tandis que **NGINX** ne permet aucune configuration additionnelle du coup il interprète les requêtes utilisateur plus rapidement.

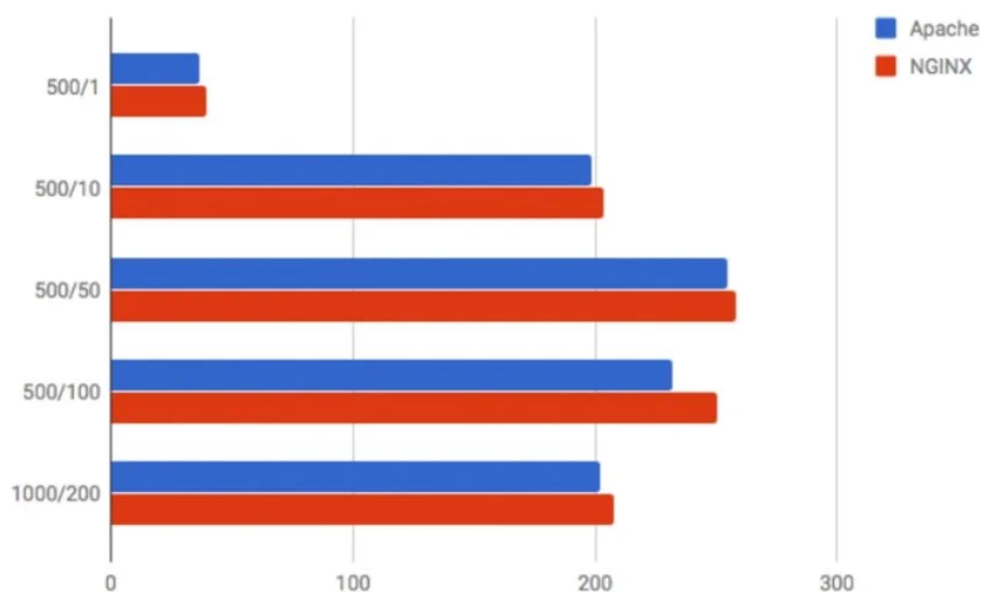
## Interprétation des requêtes

**Apache**, offre la possibilité d'interpréter la requête. Comme il est considéré comme une ressource physique sur l'emplacement du système de fichiers et qui peut nécessiter plus d'évaluation abstraite, il traite les requêtes comme des FSL(Fichier Système locale)

**NGINX** a été conçu pour être un serveur web et un serveur proxy inversé.

Il ne présente pas de mécanisme pour la spécification de la configuration pour le système de gestion des fichiers, mais privilégie plutôt l'URI pour cette tâche. Cela permet à **NGINX** de fonctionner facilement et cette configuration permet de faciliter les réponses à différents types de requêtes. Il ne vérifie pas le système de fichiers jusqu'à ce qu'il soit prêt à servir la requête.

C'est ce qui permet à **NGINX** d'être plus rapide en taux de transfert de données



**URI**: Similaire à l'**URL**, l'**URI** est également une chaîne de caractères qui identifie une ressource sur Internet en utilisant l'emplacement, le nom ou les deux. Il permet une identification uniforme des ressources. Un **URI** est en outre regroupé comme un localisateur, un nom ou les deux, ce qui signifie qu'il peut décrire une **URL**, un **URN** ou les deux

## **Les modules complémentaires**

**Apache** possède 60 modules complémentaires officiels téléchargeables et peuvent être activés ou désactivés et aussi d'autres modules non officiels.

**NGINX** compte à lui possède très peu de modules qui sont seulement disponible par des tiers ce qui fait de **NGINX** un serveur web qui ne nécessite que du minimum pour fonctionner et être ainsi léger et performant.

## **Flexibilité**

Comme on a pu le voir juste avant avec les modules **Apache** est plus flexible grâce à l'installation de plusieurs modules officiels qui permettent de personnaliser le serveur par le biais de modules dynamique. Tandis que **NGINX** ne peut pas supporter de modules dynamique il n'est donc pas très flexible.

## **Sécurité**

Nos 2 serveurs web sont très bien sécurisés, **Apache** avec ces modules qui permet de rajouter des sécurités telle qu'un anti DDOS et **NGINX** grâce à son petit code et ses balises sécurisées.

## Pour résumer

Apache	Nginx
Construit pour devenir un serveur Web	Il joue le rôle de serveur Web ainsi qu'un Reverse-Proxy
Ne peut pas traiter d'importantes requêtes simultanées avec haut trafic	Peut traiter de multiples requêtes clients simultanés en utilisant qu'un fragment des ressources disponibles
Utilise une approche multi-thread pour traiter les requêtes	Utilise une approche événementielle pour servir les requêtes des clients
Les modules sont chargés dynamiquement le rendant plus flexible	Les modules ne peuvent être chargés de manière dynamique. Ils doivent être compilés dans le Core du logiciel
Gère le contenu dynamique au sein du serveur lui même	Ne peut pas traiter le contenu dynamique

Apache2 Ubuntu Default Page

localhost



# Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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

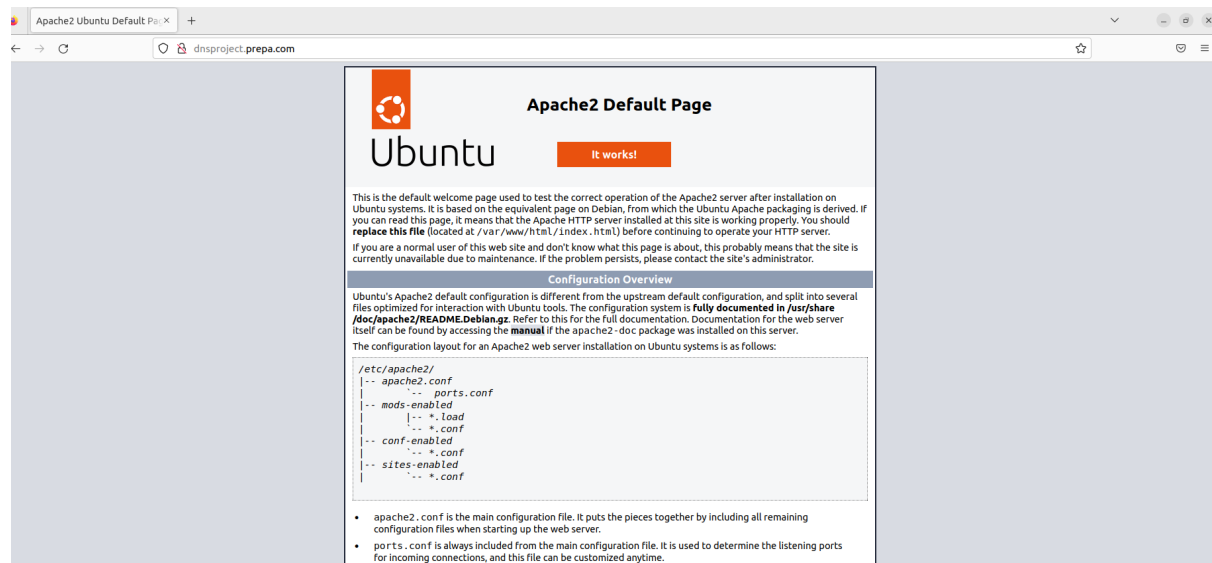
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. 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 Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

## JOB 4

```
clem@clem-virtual-machine ~$ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.126.130) 56(84) bytes of data:
64 bytes from dnsproject.prepa.com (192.168.126.130): icmp_seq=1 ttl=64 time=0.367 ms
64 bytes from dnsproject.prepa.com (192.168.126.130): icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from dnsproject.prepa.com (192.168.126.130): icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from dnsproject.prepa.com (192.168.126.130): icmp_seq=4 ttl=64 time=0.048 ms
64 bytes from dnsproject.prepa.com (192.168.126.130): icmp_seq=5 ttl=64 time=0.038 ms
^C
--- dnsproject.prepa.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4076ms
rtt min/avg/max/mdev = 0.036/0.107/0.367/0.130 ms
clem@clem-virtual-machine ~$
```



```
clem@clem-virtual-machine ~$ ping dnsproject.prepa.com
PING dnsproject.prepa.com (127.0.0.1) 56(84) bytes of data:
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=2 ttl=64 time=0.366 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=3 ttl=64 time=0.072 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=4 ttl=64 time=0.071 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=5 ttl=64 time=0.075 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=6 ttl=64 time=0.070 ms
64 bytes from dnsproject.prepa.com (127.0.0.1): icmp_seq=7 ttl=64 time=0.056 ms
```

## **JOB 5-Comment obtient-on un nom de domaine public ?**

### **Qu'est-ce qu'un "nom de domaine" ?**

Le nom de domaine est l'identifiant d'un site internet. Il constitue la partie la plus importante de l'adresse de ce site. Si l'on prend l'exemple suivant

**www.pommepoireolive.fr :**

**pommepoireolive** identifie le site

**.fr (ou .com etc...)** correspond à ce que l'on appelle "l'extension".

### **Il existe différent type d'extension**

**.fr** peut être attribué à toute entité ou personne ayant une existence légale en France, sans autre condition. (.be pour la Belgique. .it pour l'Italie etc...)

**.com** plus "global" que le .fr (à l'origine il était destiné aux entreprises commerciales), mais aussi moins "fiable" car aucune condition particulière n'est exigée pour son dépôt.

**.net** à l'origine destiné aux structures liées à Internet. Fonctionnant comme le .com, il peut aujourd'hui être déposé par toute personne.

**.org** à l'origine destiné aux structures à but non commercial. Il est aujourd'hui aussi "ouvert" que le .com.

Et il en existe encore davantage, le choix de l'extension dépend de nos besoins. Il est possible de déposer le même nom de domaine sous différente extension.


### **Comment déposer un nom de domaine ?**

Pour déposer un nom de domaine, il faut s'adresser à l'un des nombreux prestataires agréés. Il est fréquent qu'ils proposent en complément des services comme de l'hébergement, des solutions de création de site, un service de messagerie.

Exemples : Amen, Gandi, Mail Club, Ovh, Ikoula, Ionos, etc..





Ou bien par exemple pour un .fr, le site de l'Association française pour le nommage internet en coopération - Afnic - l'organisme qui gère uniquement les noms de domaine en suffixe .fr .

## Rechercher un nom de domaine



Rechercher

### Résultats de la recherche

	Prix HT /1re année
 <b>pommepoireolive.com</b> • Disponible	<b>8,99 €</b> puis 11,79 €/an 
<h3>Autres extensions</h3>	
<b>pommepoireolive.store</b> • Disponible	<del>46,99 €</del> <b>0,99 €</b> puis 50,99 €/an 
<b>pommepoireolive.pro</b> • Disponible	<b>3,49 €</b> puis 16,99 €/an 

Votre nom de domaine

FR ▼

VALIDER

« **pommepoireolive.fr** » est encore disponible. Nous vous conseillons de le réserver auprès d'un bureau d'enregistrement avant que quelqu'un d'autre ne le fasse car c'est la règle du « premier arrivé, premier servi » qui s'applique pour les noms de domaine.

[ACCÉDER À L'ANNUAIRE DES BUREAUX D'ENREGISTREMENT](#) ➔

[MENTIONS SPÉCIALES WHOIS](#) ▼

## Enregistrement automatique du nom de domaine dans le répertoire WHOIS

Une fois enregistré, le nom de domaine est directement repris dans la base de données WHOIS. Le WHOIS est un moteur de recherches permettant de voir la disponibilité des noms de domaine et de fournir des informations techniques et administratives sur le titulaire d'un nom de domaine.



## Quelles sont les spécificités que l'on peut avoir sur certaines extensions de nom de domaine ?

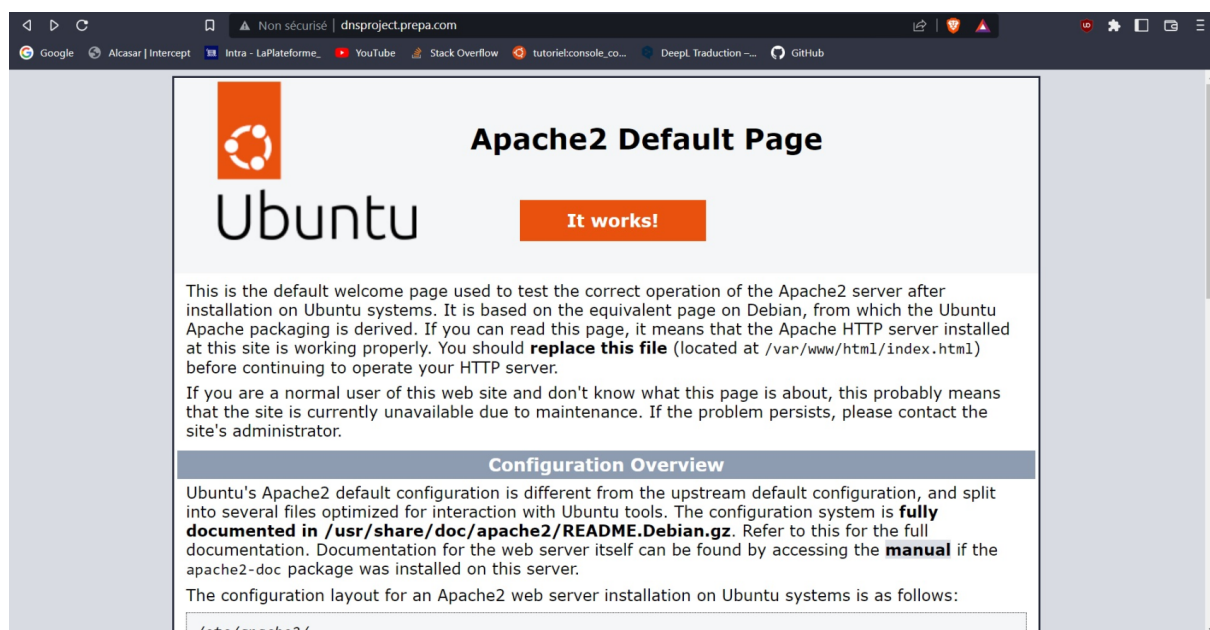
Pour les domaines de pays .fr .ca .it il permet de spécifier que le site est détenu par exemple par un français .fr un canadien .ca un italien .it .

Les **.gov** spécifient que ce site est détenu par le gouvernement .

De plus, l'ICANN (Internet Corporation for Assigned Names and Numbers), une organisation dont le but est de rendre internet stable et sécurisé, a autorisé les organismes à créer leurs propres extensions de domaine individuelles, tels que .toyota.

Chaque extension a sa spécificités qui permet aux utilisateurs de connaître sur quel type de sites il se dirige : site français, anglais ,gouvernemental , entreprise , éducation , recherche d'emploi , shopping etc... .

## JOB 6



## JOB 9

On configure le firewall pour que l'on puisse passer par le port 80 pour accéder a notre serveur apache2

To	Action	From
--	-----	----
80/tcp	ALLOW IN	Anywhere
80/udp	ALLOW IN	Anywhere
80/tcp (v6)	ALLOW IN	Anywhere (v6)
80/udp (v6)	ALLOW IN	Anywhere (v6)

On commente ses 8 lignes pour bloquer tous les ping possible à notre serveur.

```
GNU nano 6.2                                sudo nano before.rules
before.rules
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#
# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines

# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-output -m conntrack --ctstate INVALID -j DROP

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

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT
```

Et on recharge ufw

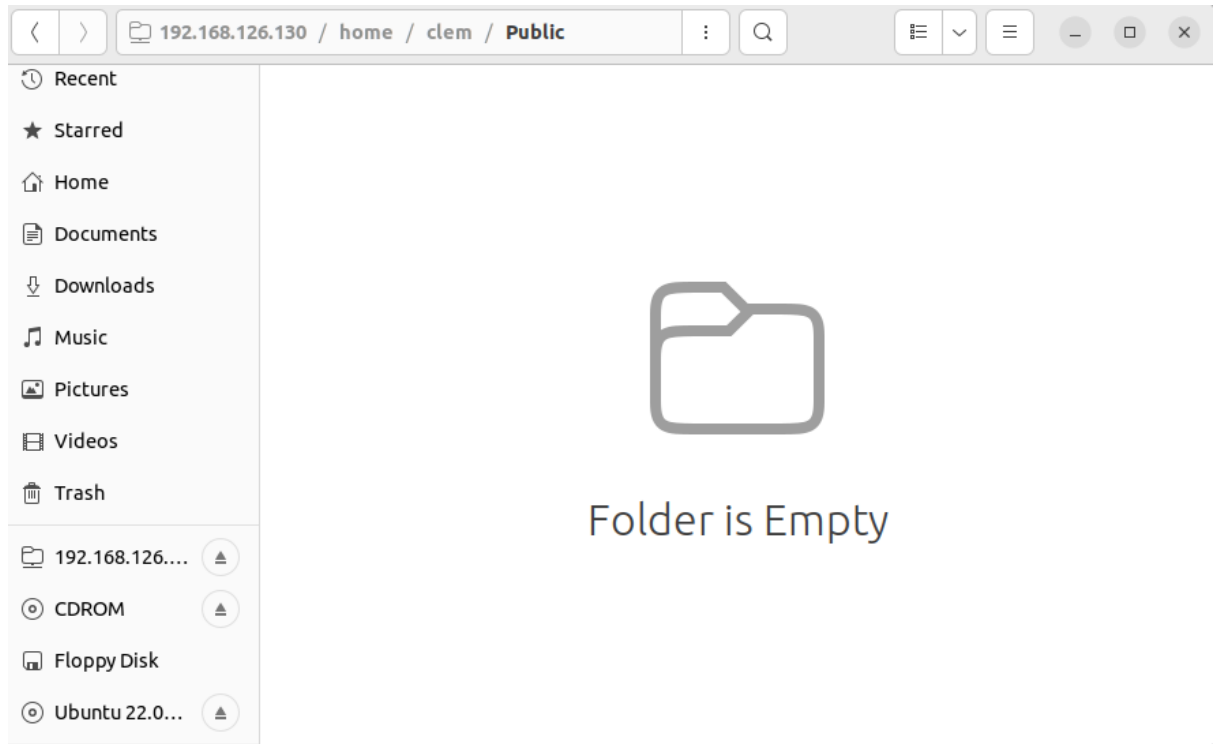
: sudo ufw reload

```
C:\Users\drago>ping 192.168.126.130

Envoi d'une requête 'Ping' 192.168.126.130 avec 32 octets de données :
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 192.168.126.130:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

## JOB 10

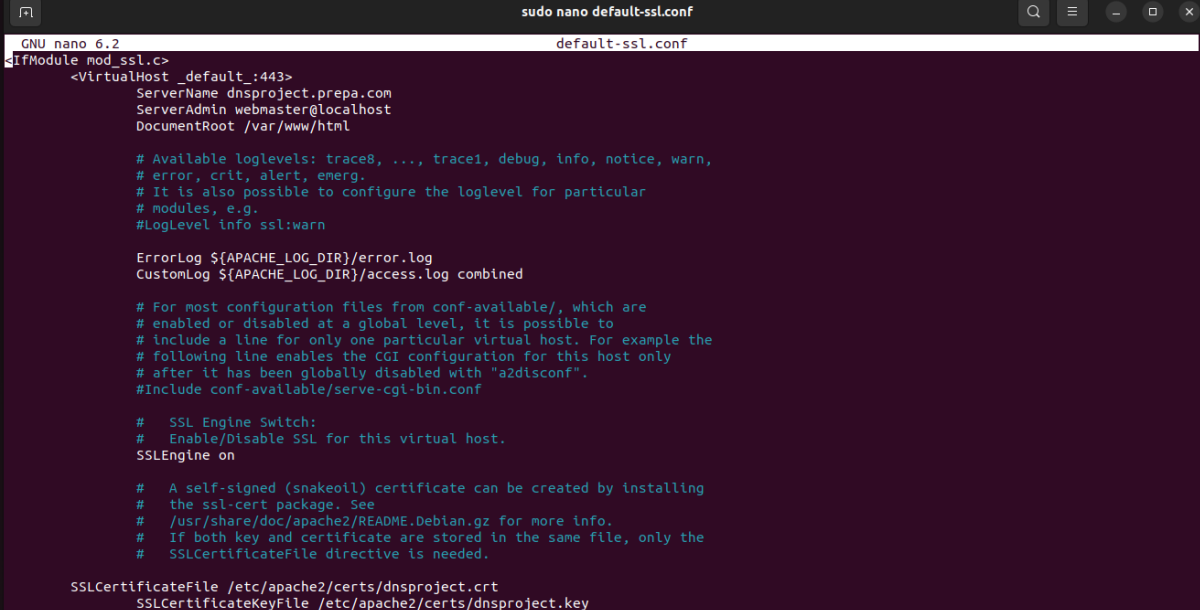


## JOB BONUS

### Création du certificat et des clé

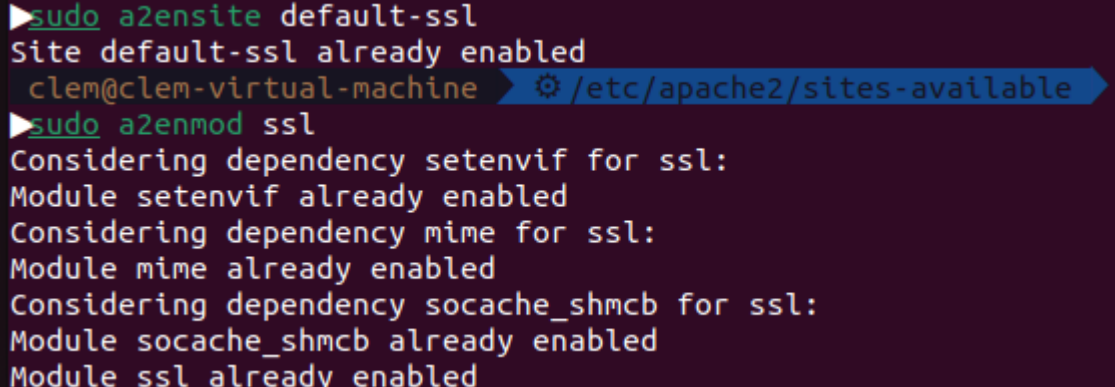
```
openssl req -new -x509 -nodes -sha1 -days 365 -key  
/etc/apache2/certs/dnsproject.key -out /etc/apache2/certs/dnsproject.crt  
-extensions usr_cert
```

### On configure le SSL du serveur apache



```
GNU nano 6.2 default-ssl.conf  
#IfModule mod_ssl.c>  
<VirtualHost _default_:443>  
    ServerName dnsproject.prepa.com  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
  
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
    # error, crit, alert, emerg.  
    # It is also possible to configure the loglevel for particular  
    # modules, e.g.  
    #LogLevel info ssl:warn  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    # For most configuration files from conf-available/, which are  
    # enabled or disabled at a global level, it is possible to  
    # include a line for only one particular virtual host. For example the  
    # following line enables the CGI configuration for this host only  
    # after it has been globally disabled with "a2disconf".  
    #Include conf-available/serve-cgi-bin.conf  
  
    # SSL Engine Switch:  
    # Enable/Disable SSL for this virtual host.  
    SSLEngine on  
  
    # A self-signed (snakeoil) certificate can be created by installing  
    # the ssl-cert package. See  
    # /usr/share/doc/apache2/README.Debian.gz for more info.  
    # If both key and certificate are stored in the same file, only the  
    # SSLCertificateFile directive is needed.  
  
    SSLCertificateFile /etc/apache2/certs/dnsproject.crt  
    SSLCertificateKeyFile /etc/apache2/certs/dnsproject.key
```

### On active le SSL



```
► sudo a2ensite default-ssl  
Site default-ssl already enabled  
clem@clem-virtual-machine ➤ /etc/apache2/sites-available  
► sudo a2enmod ssl  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Module socache_shmcb already enabled  
Module ssl already enabled
```

### Et on redémarre le serveur apache

```
sudo systemctl restart apache2
```



### Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to dnsproject.prepa.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

## Certificate

Internet Widgits Pty Ltd

#### Subject Name

Country	FR
State/Province	PACA
Locality	Marseille
Organization	Internet Widgits Pty Ltd

#### Issuer Name

Country	FR
State/Province	PACA
Locality	Marseille
Organization	Internet Widgits Pty Ltd

#### Validity

Not Before	Tue, 08 Nov 2022 13:33:07 GMT
Not After	Wed, 08 Nov 2023 13:33:07 GMT

#### Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	D0:D0:99:19:37:34:F5:60:4B:7C:D1:CC:64:DF:93:E3:B7:C0:7D:09:BA:8A:73:B...

## Lecteur du certificat : ClemLAPLATEFORME

### Général

### Détails

#### Émis pour

Nom commun (CN)	ClemLAPLATEFORME
Organisation (O)	ClemLAPLATEFORME
Unité d'organisation (OU)	ClemLAPLATEFORME

#### Émis par

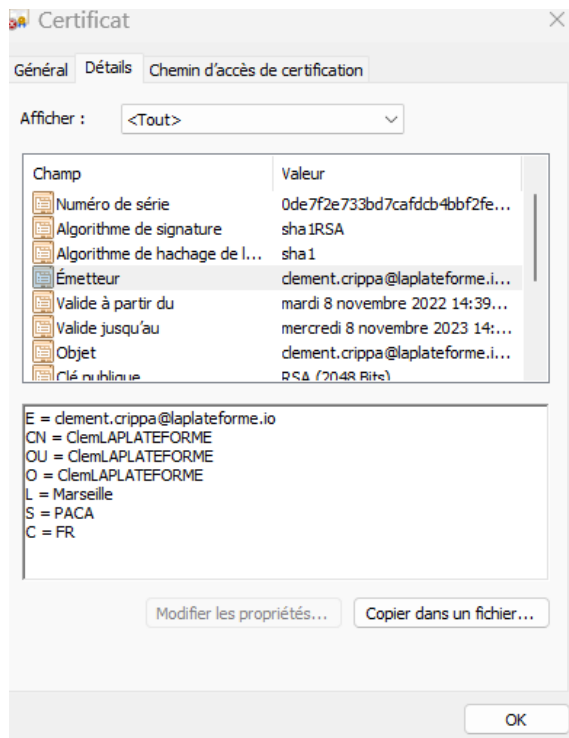
Nom commun (CN)	ClemLAPLATEFORME
Organisation (O)	ClemLAPLATEFORME
Unité d'organisation (OU)	ClemLAPLATEFORME

#### Durée de validité

Émis le	mardi 8 novembre 2022 à 14:39:00
Expire le	mercredi 8 novembre 2023 à 14:39:00

#### Empreintes

Empreinte SHA-256	7A E4 35 6E 26 5B DA F9 0E 9C 2D 4F AF BE 96 D3 BF 5C 77 C3 87 12 CB F8 12 7D 4D <del>83 9A</del>
Empreinte SHA-1	76 AF 9E 7D D2 07 03 54 4D 6B D6 1E <del>4D</del> 65 3C C7 58



## **Qu'est-ce qu'un certificat SSL ?**

Un certificat SSL affiche des informations importantes pour la vérification du propriétaire d'un site web et le cryptage du trafic web avec SSL/TLS, notamment la clé publique, l'émetteur du certificat et les sous-domaines associés.

Les certificats SSL permettent aux sites web de passer du HTTP au HTTPS, qui est plus sûr. Un certificat SSL est un fichier de données hébergé à l'origine d'un site web. Les certificats SSL rendent possible le cryptage SSL/TLS et contiennent la clé publique du site web et l'identité du site

### **Ils contiennent :**

- le nom de domaine pour lequel le certificat a été délivré
- la personne, l'organisation ou le dispositif à qui il a été délivré
- Quelle autorité de certification l'a délivré
- La signature numérique de l'autorité de certification
- Sous-domaines associés
- Date de délivrance du certificat
- Date d'expiration du certificat
- La clé publique

## **Qu'est-ce qu'un certificat SSL auto-signé ?**

C'est un certificat qui peut être créé par n'importe qui en générant un couplage de clés publiques-privées et en incluant toutes les informations mentionnées ci-dessus. Ces certificats sont appelés certificats auto-signés parce que la signature est numérique, au lieu d'être celle d'une autorité de certification.

Ce qui signifie que les certificats auto-signés peuvent être remplis de fausse information sur le serveur sur lequel on se rend.

C'est pour cela que notre certificat pour ce job est décrit comme étant non sécurisé car il est auto signé et n'a pas été vérifié par une autorité de certification.

Pour éviter les arnaque ou autre fraude les gros site internet utilise des certificats signée par une autorité de certification comme:

- Comodo
- Digicert
- GoDaddy
- GlobalSign
- Digicert
- StartCom
- Entrust
- Certum

Les autorités de certification permettent d'avoir une véritable certification que les informations écrites sur le certificat sont vraies ce qui permet de rassurer les utilisateurs sur la sécurité du serveur sur laquelle il se connecte.