Titre

Pré-requis

Installation de apache2 et openssl :

On utilise aperture (apt) pour mettre a jour la machine :

sudo apt update && sudo apt upgrade -y

Ensuite on installe openssl et apache2 :

sudo apt install apache2 openssl

Mise en place des services :

On lance les services d'apache2 avec systemctl :

```
sudo systemctl start apache2
sudo systemctl enable apache2
```

Ensuite on vérifie les services grâce à l'option status :

sudo systemctl status apache2

Résultat :

user@vbox:~\$	sudo sý	stemctl statu	s_apache2		ŝ.			
apache2.ser	rvice -	Ine Apache HI	IP Server					
Loaded:	Loaded	(/llb/systemd	/system/a	pacnez.se	rvice; er	abled; prese	t: enabled)	
Active:	active	(<mark>running</mark>) sin	ce Mon 20	25-02-10	10:06:44	CEI; 2 days	ago	
Docs:	https:/	/httpd.apache	.org/docs	/2.4/				
Main PID:	640 (ap	ache2)						
Tasks:	11 (lim	it: 2284)						
Memory:	93.7M							
CPU:	4.140s							
CGroup:	/system	.slice/apache	<pre>2.service</pre>					
	640	/usr/sbin/ap	ache2 -k	start				
	- 698	/usr/sbin/ap	ache2 -k	start				
	- 699	/usr/sbin/ap	ache2 -k	start				
	- 700	/usr/sbin/ap	ache2 -k	start				
	- 713	/usr/sbin/an	ache2 -k	start				
	- 715	/usr/sbin/an	ache2 -k	start				
	-10621	/usr/shin/an	ache2 -k	start				
	-10679	/usr/sbin/ap	ache2 -k	start				
	-10680	/usr/shin/ap	ache2 -k	start				
	10681	/usr/sbin/ap	ache2 k	start				
	10601	/usi/sbin/ap	ache2 -k	start				
	-10082	/usi/such/ap	achez -K	Start				
Eab 10 10.06	11 yhay	cyctomd[1].	Starting	anacha2 c	onvice	The Anache U	TTD Convor	
Feb 10 10:063	44 VDOX	systemd[1]:	Starting	apache2.s	ervice -	The Apache H	TIP Server	
reb 10 10:06:	:44 Vbox	systemd[1]:	Started a	pacne2.se	rvice – I	ne Apache HI	TP Server.	

On vérifie aussi sur notre navigateur :



Les services d'apache2 sont fonctionnels

Génération du certificat

Génération certificat SSL et d'une clé privé avec OpenSSL :

On utilise openssi pour générer le certificat :

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out
/etc/apache2/server.crt -keyout /etc/apache2/server.key
```

openssl req : C'est la commande OpenSSL pour créer une demande de certificat ou un certificat auto-signé.

-x509 : Indique à OpenSSL de générer un certificat auto-signé.

-nodes : Signifie "no DES", ce qui signifie que la clé privée ne sera pas chiffrée avec un mot de passe.

-days 365 : Spécifie que le certificat sera valide pendant 365 jours.

-newkey rsa:2048 : Crée une nouvelle clé privée RSA de 2048 bits.

-sha256 : Utilise l'algorithme de hachage SHA-256 pour signer le certificat.

- -out /etc/apache2/server.crt : Spécifie le fichier de sortie pour le certificat auto-signé.
- -keyout /etc/apache2/server.key : Spécifie le fichier de sortie pour la clé privée.

Résultat :



On nous demande plusieurs choses :

Champ	Exemple (dans mon cas)	Obligatoire
Country Name	FR	Oui
State or Province Name	IDF	Non
Locality Name	Paris	Non
Organization Name	IPSSI	Non
Organizational Unit Name	PRS	Non
Common Name	name	Oui
Email Address	no@mail.com	Non

Changement des droits sur le certificat :

On utilise **chmod** pour changer les droit sur le certificat :

```
sudo chmod 440 /etc/apache2/server.crt
```

chmod 440 : donne uniquement le droit de lecture au group de l'utilisateur et au propriétaire avec 4. Et donne aucun droit au autres avec 0.

Ensuite on vérifie que les droit soit bien modifié avec ls :

```
ls -l /etc/apache2/server.crt
```

Résultat :

user@vbox:~\$ ls -l /etc/apache2/server.crt
-r--r---_1 root root 1375 Feb 12 11:43 /etc/apache2/server.crt

On a bien r pour le propriétaire et le groupe de l'utilisateur.

Configuration d'apache

Configuration de l'emplacement des certifications :

On modifie l'emplacement des certifications dans le fichier de configuration de apache :

sudo nano etc/apache2/sites-available/default-ssl.conf

On modifie les deux lignes comme ceci :

SSLCertificateFile /etc/apache2/server.crt SSLCertificateKeyFile /etc/apache2/server.key

Activation du module SSL et du site SSL:

On active le module SSL avec a2enmod :

sudo a2enmod ssl

a2enmod : active un module apache.

On active le site en SSL avec a2ensite:

sudo a2ensite default-ssl

a2ensite : active un site apache.

On recharge le service avec service pour appliquer les modifications :

sudo service apache2 reload

On vérifie sur navigateur :

O 🗛 https://localhost



le site fonctionne bien en https.

Désactivation de du site en http

On utilise a2dissite pour désactiver le site par default (en http):

sudo a2dissite "000-default"

a2dissite : désactive un site apache.

Ensuite on recharge à nouveau le service apache2 :

sudo service apache2 reload

Redirection http -> https

On rajoute la redirection dans le document de configuration de notre site :

sudo nano /etc/apache2/sites-available/default-ssl.conf

80% 🟠

On rajoute ces lignes au debut du fichier :

```
<VirtualHost *:80>
Redirect permanent / https://localhost
</VirtualHost>
```

Le site nous renvoie directement sur la version https de celui-ci :

