

# Installation apache2 sur debian et ssl

---

Debian est installé et démarré.

## apache2

En mode root, procéder aux installations et configurations.

Mettre le système à jour.

```
apt update && apt upgrade
```

Puis installation d'apache2

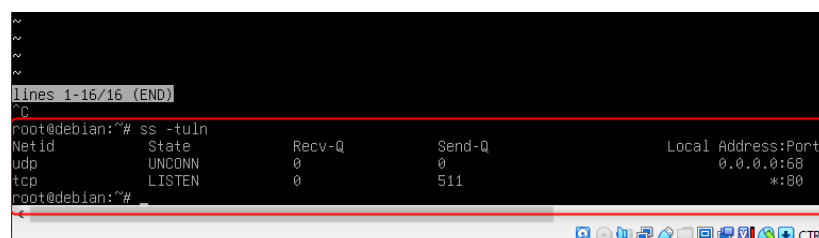
```
apt install apache2
```

Démarrer le service et demander son démarrage automatique avec l'OS.

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

Commande de vérification des ports ouverts.

```
ss -tuln
```



```
~  
~  
~  
~  
lines 1-16/16 (END)  
~C  
root@debian:~# ss -tuln  
Netid      State      Recv-Q     Send-Q     Local Address:Port  
udp        UNCONN     0           0           0.0.0.0:68  
tcp        LISTEN     0           511        *:80  
root@debian:~#
```

## Openssl

```
apt install openssl
```

Le certificat fonctionne avec un système de clé publique et privée. Il est nécessaire de les créer pour l'exemple elles seront **auto-signé**.

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

[illegible]

Des questions sont posées, il est possible de laisser sans réponse.

Pour éviter la lecture des clés par une personne extérieure, la permission de lecture est modifiée.  
Plus restrictif pour la clé privée.

```
chmod 440 /etc/apache2/server.crt
chmod 400 /etc/apache2/server.key
```

## Modifications des fichiers de configuration.

Modification des chemins dans default-ssl.conf

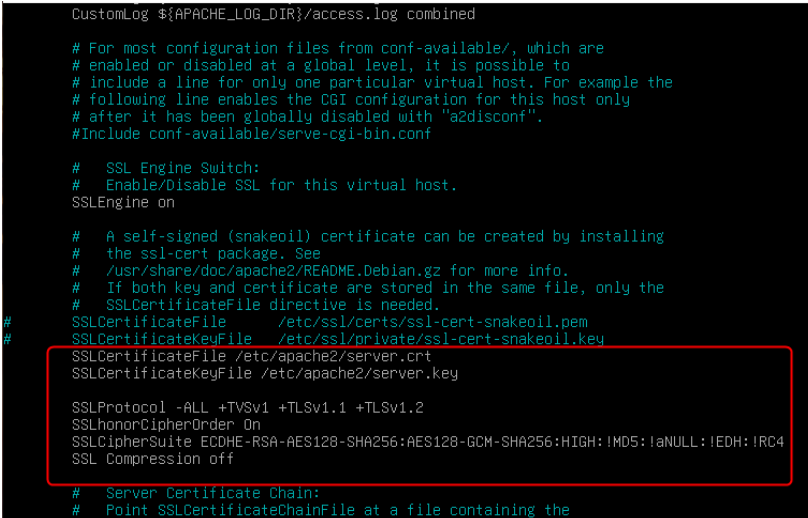
```
nano /etc/apache2/sites-available/default-ssl.conf
```

Effacer les lignes identiques et remplacer par :

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

et ajouter :

```
SSLProtocol -ALL +TLSv1.1 +TLSv1.2 +TLSv1.3
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off
```



```
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/ssl/certs/ssl-cert-snakeoil.pem
# SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
#
# SSLCertificateFile /etc/apache2/server.crt
# SSLCertificateKeyFile /etc/apache2/server.key

SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
```

Il faut maintenant activer le ssl et recharger apache.

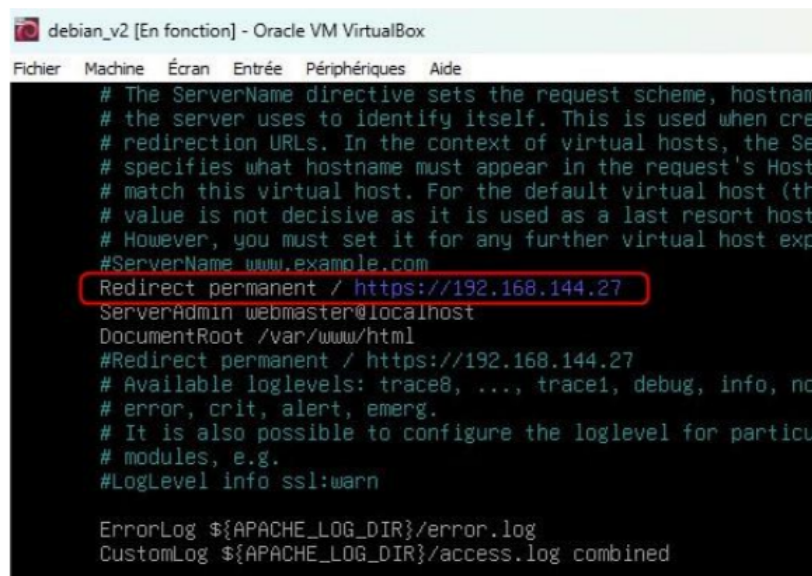
```
a2enmod ssl
a2ensite default-ssl.conf
service apache2 reload
```

Nous pouvons faire une redirection permanente pour aller sur le port 443.

```
nano /etc/apache2/sites-available/000-default.conf
```

Ecrire :

```
Redirect permanent / https://son_adresse_ip
```



```
debian_v2 [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating URLs. In the
# context of virtual hosts, the ServerName specifies what hostname must appear
# in the request's Host header to match this virtual host. For the default
# virtual host, the ServerName value is not decisive as it is used as a last
# resort host name. However, you must set it for any further virtual host
# expansion.
#ServerName www.example.com
Redirect permanent / https://192.168.144.27
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
#Redirect permanent / https://192.168.144.27
# Available loglevels: trace8, ..., trace1, debug, info, notice, error,
# 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
```

## Pare-feu

Pour gérer les ports, installation de ufw.

```
apt install ufw
```

Activer le pare-feu pour qu'il démarre avec l'OS.

```
ufw enable
```

Activation du port https 443.

```
ufw allow 443
```

Au besoin pour fermer un port :

```
ufw deny n°_du_port
```