Tuto : Configurer un serveur Apache

1) Installer le serveur Apache : *« yum install httpd »*

```
[root@15 ~]# yum install httpd_
```

2) Créer ou ajouter le ou les fichiers HTML dans **/var/www/html/**

```
Last login: Wed May  1 22:26:03 on tty1
[root@localhost ~]# vi /var/www/html/index.html
```

3) En cas de création d'un fichier html, ajouter ce code a l'intérieur de ce fichier.

```
<html>
        <head>
                <title>Mon site web</title>
        </head>
        <body>


        </body>
</html>
```

4) Lancer le serveur Apache (Il peut déjà être lancé grâce à la configuration de base)

```
[root@localhost ~]# systemctl enable httpd
[root@localhost ~]# systemctl start httpd
```

- la première ligne sert à lancer le service Apache automatiquement au démarrage du serveur.
- l'autre sert à démarrer le serveur immédiatement.

5) Ouvrir le fichier httpd.conf

```
[root@localhost ~]# vi /etc/httpd/conf/
httpd.conf  magic
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

6) Puis modifier les lignes suivantes

```
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.  e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName monreseau.fr
```

```
#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset off
```

- Sur la ligne **ServerAdmin**, mettre l'adresse e-mail de l'administrateur. (Pour ma part j'ai laissé celle par défaut.)
- Sur la ligne **ServerName**, entrer le nom du serveur choisie
- Sur la ligne **AddDefaultCharset**, ajoutez « off » afin que chaque page html déclarer ces propres Charset

Puis quitter le fichier en appuyant sur *« echap »* puis en tapant *« :wq! »*

7) Afin de vérifier si le fichier contient des erreurs, taper la commande *« apachectl configtest »*

```
[root@localhost ~]# apachectl configtest
Syntax OK
[root@localhost ~]#
```

8) Modifier les droits d'accès du fichier afin de mieux les protéger

```
[root@localhost ~]# cd /var/www/html
[root@localhost html]# find . -type d -exec chmod 0755 {} \;
[root@localhost html]# find . -type f -exec chmod 0644 {} \;
[root@localhost html]#
```

9) Recharger les nouvelles informations enregistrées précédemment

```
[root@localhost html]# systemctl reload httpd
[root@localhost html]#
```

Pour aller plus loin.. (HTTPS)

1) Installer le module **SSL**

```
[root@localhost ~]# yum install mod_ssl
```

2) Créer les dossier « ssl » sous **httpd/** puis « monreseau.fr » sous **ssl**. Puis rendez-vous à l'intérieur du dossier. (Pour le dossier **monreseau.fr**, mettez votre nom de domaine)

```
[root@localhost ~]# mkdir /etc/httpd/ssl
[root@localhost ~]# mkdir /etc/httpd/ssl/monreseau.fr
[root@localhost ~]# cd /etc/httpd/ssl/monreseau.fr
[root@localhost monreseau.fr]# openssl req -x509 -nodes -days -365 -newkey rsa:1024 -out monreseau.l
ocal.crt -keyout monreseau.local.key
Generating a 1024 bit RSA private key
....++++++
.....++++++
writing new private key to 'monreseau.local.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:Occitanie
Locality Name (eg, city) [Default City]:Montpellier
Organization Name (eg, company) [Default Company Ltd]:monreseau
Organizational Unit Name (eg, section) []:big data
Common Name (eg, your name or your server's hostname) []:www.monreseau.fr
Email Address []:contact@localhost
```

- Une fois dans le dossier entrer la commande *« openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out monreseau.local.crt -keyout monreseau.local.key ». Cette Commande permet de créer le certificat et la clé de chiffrement RSA. (Les noms des fichier doivent porter le même nom que le nom donnée au serveur dans les fichier de configuration)*
- Puis répondre au questionnaire.

3) Aller dans le fichier de configuration SSL

```
[root@localhost ~]# vi /etc/httpd/conf.d/ssl.conf
```

4) Modifier les informations suivantes :

```
<VirtualHost _default_:443>

#STS (Strict-transport-securitu) Permet d'obliger les navigateur a utiliser une connexion sécurisé.
Header always set Strict-Transport-Security \
        "max-age=63072000; includeSubDomains"
```

```
# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html"
ServerName monreseau.fr:443
```

```
SSLHonorCipherOrder on

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/httpd/ssl/monreseau.fr/monreseau.local.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/httpd/ssl/monreseau.fr/monreseau.local.key
```

- Ajouter la partie #STS
- SSLHonorCipherOrder on (Cette directive permet d'indiquer à Apache que l'ordre des procédés de chiffrements dans SSLCipherSuite doit être respecté. Autrement dit, la première correspondance trouvée doit être utilisée.)
- Indiquer les chemins du certificat et du chiffrement

Puis quittez le fichier en tapant *« echap »* puis *« :wq! »*

5) Créer le fichier *« monreseau.fr.conf »* dans **/etc/httpd/conf.d/**

```
[root@localhost ~]# vi /etc/httpd/conf.d/monreseau.fr.conf
```

6) Ajouter tout le texte ci-dessous dans le fichier nouvellement crée. Puis enregistrer et quitter.

```
<VirtualHost *:80>
        ServerName monreseau.fr
        ServerAlias www.monreseau.fr
        Redirect permanent / https://www.monreseau.fr/
</VirtualHost>

<VirtualHost *:443>
        ServerName monreseau.fr
        ServerAlias www.monreseau.fr
        DocumentRoot /var/www/html

        SSLEngine On
        SSLCertificateFile "/etc/httpd/ssl/monreseau.fr/monreseau.local.crt"
        SSLCertificateKeyFile "/etc/httpd/ssl/monreseau.fr/monreseau.local.key"
</VirtualHost>
```

7) Recharger les nouvelles informations enregistrées précédemment et voilà.

```
[root@localhost html]# systemctl reload httpd
[root@localhost html]#
```

Source :

- https://www.microlinux.fr/apache-ssl-centos-7/
- https://www.microlinux.fr/apache-centos-7/?_sm_nck=1#lancement
- http://guillaume-cortes.fr/serveur-web-apache-centos-7/
- https://www.josselinlie.be/comment-installer-apache-sur-centos-7/