APACHE configuration et sécurisation

Cette fiche de procédure contient les étapes importantes pour la configuration du service apache et de la sécurisation sous Debian 11

Explication d'Apache

Apache est un serveur web open-source, un logiciel qui permet de diffuser des pages web sur internet. Il est utilisé pour héberger des sites web et des applications web, ainsi que pour servir des fichiers et des données sur le réseau. Apache est l'un des serveurs web les plus populaires et les plus utilisés dans le monde, offrant une grande flexibilité et une grande fiabilité pour les développeurs et les administrateurs de serveurs.

Installation d'Apache

Vérifier les dépôts Debian avant l'installation en mode root :

```
apt update
apt upgrade -y
apt install apache2
systemctl status apache2 (vérifie si le service est en cour d'execution)
```

Configuration d'Apache

Pour vérifier que le service est bien activé saisir sur un navigateur : Affichant une page lie à apache

```
http://localhost
```

Le répertoire courant ou se trouve « index.html » se trouve dans :

```
cd /var/www/html
```

Le fichier de configuration principale d'apache contenant les directives pour le fonctionnement se trouve dans :

```
cd /etc/apache2/apache2.conf
```

Apache utilise des hôtes virtuels pour héberger plusieurs sites web sur le même serveur qui sont situé dans :

```
cd /etc/apache2/site-available/000-defaut.conf
```

Ainsi Apache dispose de modules et les fichiers de configuration sont situés dans :

```
cd /etc/apache2/mods-available
```

Et pour activer un module :

```
a2enmod « le nom du module »
```

Sécurisation d'Apache

Pour supprimer la visibilité de la version d'apache faut ajouter dans le fichier :

```
cd /etc/apache2/conf-available/security.conf
```

Et mettre :

```
ServerTokens Prod

ServerSignature Off
```

Autoriser que le trafic nécessaire pour communiquer avec le serveur web « Apache » avec iptables :

```
apt install iptables
```

Règles de filtrage :

```
iptables -P INPUT DROP «politique par défaut »

iptables -P OUTPUT ACCEPT «politique par défaut »

iptables -A INPUT -p tcp --dport http -j ACCEPT « Cette règle autorise le trafic HTTP entrant. »

iptables -A INPUT -p tcp --dport https -j ACCEPT « Cette règle autorise le trafic HTTPS entrant. »

iptables -A OUTPUT -p udp --dport 53 -j ACCEPT « Cette règle autorise le trafic DNS sortant UDP »

iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT  « Cette règle autorise le trafic DNS sortant TCP »

iptables -A INPUT -j DROP

« Cette règle bloque tous les autres paquets entrants qui n'ont pas été autorisés par les règles précédentes. »
```