

# Sécuriser Apache2 sur un serveur

Dans cette procédure, je vais vous montrer quelques bases pour sécuriser vos serveurs Apache2. Je vous recommande de faire une sauvegarde de votre serveur avant toutes modifications, quelques opérations peuvent être sensibles pour serveur Apache2.



## Prérequis pour sécuriser Apache2 sur un serveur :

- Un serveur Apache2
- Avoir fait une sauvegarde de ce serveur

## Modifications sur la configuration Apache2 :

Pour sécuriser un serveur Apache2, la première étape à faire sur un serveur Apache2. C'est de cacher la version du service.

# Not Found

The requested URL /asdf was not found on this server.

---

Apache/2.4.7 (Ubuntu) Server at 127.0.0.1 Port 80

## Not Found

The requested URL was not found on this server.

Le but va être de passer de la première image à la deuxième. Pour cela il faut modifier la configuration de Apache2 :

```
vim /etc/apache2/conf-enabled/security.conf
```

Remplacer : ServerSignature On

Par : ServerSignature Off

Il est également possible de faire cette étape avec la commande suivante :

```
sed -i 's/ServerSignature On/ServerSignature Off/g' /etc/apache2/conf-enabled/security.conf
```

La seconde étape de sécurisation du serveur Apache2 sera de désactiver la lisibilité des fichiers présents dans les dossiers :

```
vim /etc/apache2/conf-enabled/security.conf
```

Ajouter ceci à la fin du fichier :

```
<Directory /var/www>
  Options -Indexes
</Directory>
```

## Index of /assets/css

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">bootstrap-grid.css</a>	2019-02-13 14:47	63K	
 <a href="#">bootstrap-grid.css.map</a>	2019-02-13 14:47	148K	
 <a href="#">bootstrap-grid.min.css</a>	2019-02-13 14:47	47K	

# Forbidden

You don't have permission to access this resource.

Maintenant, il faut redémarrer le service Apache2 pour que la configuration soit prise en compte :

```
sudo systemctl restart apache2
```

Ensuite avoir un système à jour permet de limiter les possibles intrusions.

```
sudo apt update && sudo apt full-upgrade -y
```

Il est aussi recommandé d'installer un certificat et de forcer la communication avec le protocole HTTPS afin de chiffrer chaque communication.

Je recommande l'utilisation de firewall comme Iptables ou UFW. Attention à ne pas bloquer les ports que vous utilisez. Comme le 80/443 pour l'utilisation web et le 22 pour l'utilisation du protocole SSH. Si vous n'avez pas changé les ports par défaut.

Je conseille aussi d'utiliser une machine en tant que reverse proxy dans le but de limiter les possibles accès à vos données qui sont accessibles depuis les serveurs web que vous possédez. De plus, en cas de Cyber attaque il s'agira du serveur qui contiendra ce reverse proxy qui sera le premier à subir l'attaque. Il vous offrira aussi un cache permettant d'obtenir de meilleur temps de réponses lors des chargements des pages de votre site Web. Attention, il ne faut pas abuser de ce cache et le nettoyer régulièrement sinon il pourrait être source d'intrusion.

Il est également recommandé d'utiliser un parseur de logs (comme CrowdSec) afin de détecter les comportements anormaux : **Installer CrowdSec pour Apache sur Debian 11**

---

Revision #1

Created 30 January 2025 17:08:38 by Nicolas

Updated 30 January 2025 17:09:19 by Nicolas