

# Nginx avec TLSv1.3 sous Debian

Pour cela, il va vous falloir Nginx 1.13 ou plus, et OpenSSL 1.1.1 ou plus.

## Installation de Nginx depuis les backports Debian

Il va vous falloir ajouter les dépôts APT avec la commande :

```
# echo "deb http://ftp.fr.debian.org/debian/ stretch/backports main" > /etc/apt/backports.conf
```

Puis on met a jour les dépôts

```
# apt update
```

puis on installe Nginx

```
# apt install -y -t stretch-backports nginx
```

## Installation de OpenSSL depuis le dépôt de Sury

OpenSSL 1.1.1 n'est pas dans les dépôts officiel de Debian, mais dans le dépôt d'un certain [Sury](#) (Maintener de Debian depuis l'année 2000), au coté notamment de PHP 7.3 par exemple.

Pour configurer son dépôt il faut commencer par installer apt-transport-https :

```
# apt -y install apt-transport-https
```

puis récupérer la clé publique du dépôt :

```
# wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
```

ajouter le dépôt :

```
# echo "deb https://packages.sury.org/php/ stretch main" > /etc/apt/sources.list.d/php.list
```

Mettre a jour les dépôts et mettre a jour le système :

```
# apt update && apt dist-upgrade -y
```

## Configuration de Nginx

Il vous faudra configurer Nginx comme ceci afin d'activer le TLSv1.3 ainsi que les bonnes pratiques :

[nginx.conf](https://nginx.conf)

```
30.      ##
31.      # SSL Settings
32.      ##
33.
34.      ssl_protocols TLSv1.2 TLSv1.3;
35.      ssl_prefer_server_ciphers on;
36.      ssl_ecdh_curve secp384r1:prime256v1;
37.      ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA512:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-ECDSA-
CHACHA20-POLY1305-D:ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-
GCM-SHA512:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384;
38.      ssl_session_timeout 10m;
39.      ssl_session_cache shared:SSL:9m;
40.      ssl_session_tickets off;
41.      ssl_stapling on;
42.      ssl_stapling_verify on;
```

et pour finir redémarrer nginx

```
# systemctl restart nginx
```

From:  
<https://wiki.virtit.fr/> - VirtIT

Permanent link:  
[https://wiki.virtit.fr/doku.php/kb:linux:nginx:nginx\\_avec\\_tlsv1.3\\_sous\\_debian\\_stretch?rev=1552321354](https://wiki.virtit.fr/doku.php/kb:linux:nginx:nginx_avec_tlsv1.3_sous_debian_stretch?rev=1552321354)

Last update: **2019/03/11 16:22**

