

Unifi

- [Installation Unifi sous debian 12](#)
- [Configuration Unifi avec certificat https let's encrypt](#)

Installation Unifi sous debian 12

Procédure pour installer un serveur Unifi sur debian 12. Elle fonctionne sur une machine vierge avec rien d'installé.

Installation Serveur MongoDB

Pour commencer, s'assurer que le système est bien à jour:

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

Installation MongoDB

Unifi utilise une base MongoDB pour le stockage de ces données. La version utilisée est assez ancienne (V4.4), il faut donc au préalable installer libSSL1.1, qui n'est pas disponible dans les dépôts de base de debian 12.

Téléchargement package de **libSSL**

```
wget https://ftp.debian.org/debian/pool/main/o/openssl/libssl1.1_1.1.1n-0+deb10u3_amd64.deb
```

Installation **libSSL**:

```
dpkg -i libssl1.1_1.1.1n-0+deb10u3_amd64.deb
```

Pour installer **MongoDB server v4.4**, on suit la [procédure officielle](#):

On s'assure que les prérequis sont bien installés:

```
sudo apt-get install gnupg curl
```

On va ajouter le repository officiel de MongoDB pour l'installation de ce dernier. Il faut ajouter la clé publique de ce dépôt:

```
curl -fsSL https://pgp.mongodb.com/server-4.4.asc | sudo gpg -o  
/usr/share/keyrings/mongodb-server-4.4.gpg --dearmor
```

Il reste à créer un nouveau fichier source, afin d'ajouter un nouveau dépôt dans la base du système:

```
echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-4.4.gpg ]  
http://repo.mongodb.org/apt/debian buster/mongodb-org/4.4 main" | sudo tee  
/etc/apt/sources.list.d/mongodb-org-4.4.list
```

Enfin, il reste à mettre à jour les caches d'Apt et à installer MongoDB:

```
sudo apt update  
sudo apt install mongodb-org
```

Installation Unifi

Pour terminer l'installation d'Unifi, il reste plus qu'à installer les packages:

```
sudo apt install unifi
```

Si tout s'est bien passé, le serveur unifi doit être accessible à partir de l'URL suivante:

<http://localhost:8080> ou http://ip_serveur:8080

Script d'installation

Si cette procédure ne fonctionne pas, ou si l'installation concerne un autre système, ou une autre version de debian, un script à été développé pour ça: [→ Script Glenn R](#)

Sources

[→ Article Unifi](#)

Configuration Unifi avec certificat https let's encrypt

Il est possible de configurer l'interface web d'unifi pour qu'elle utilise un certificat let's encrypt à la place d'un autosigné.

Pour cela on va utiliser certbot pour la génération du certificat et l'ajouter dans JAVA.

il faut bien évidemment que la machine soit accessible publiquement et qu'un nom de domaine pointant dessus soit existant, afin de pouvoir générer le certificat.

Installation de certbot:

```
apt install certbot
```

Génération du certificat let'sencrypt, il faut utiliser l'option 1, accepter les conditions et mettre l'URL de l'Unifi:

```
certbot certonly
```

Conversion en format PKCS 12 du certificat let'sencrypt.

Remplacer *nomDeDomaineUnifi.ltd* par le vrai nom de domaine, changer le mot de passe à la fin de la commande

```
openssl pkcs12 -export -inkey /etc/letsencrypt/live/nomDeDomaineUnifi.ltd/privkey.pem -in /etc/letsencrypt/live/nomDeDomaineUnifi.ltd/fullchain.pem -out /tmp/cert.p12 -name unifi -password pass:myPassword
```

Importation du certificat dans le base de certificat de JAVA (unifi tourne sur du JAVA), bien penser à renseigner le mot de passe, celui qu'on vient de définir:

```
keytool -importkeystore -deststorepass aircontrolentreprise -destkeypass aircontrolentreprise -destkeystore /var/lib/unifi/keystore -srckeystore /tmp/cert.p12 -srcstoretype PKCS12 -srcstorepass myPassword -alias unifi noprompt
```

On supprime le fichier certificat pkcs12

```
rm /tmp/cert.p12
```

Restart des service unifi pour prise en compte:

```
systemctl restart unifi.service
```

Ensuite on va créer un script pour le renouvellement automatique du certificat:

```
vi /emplacement/scripts/renew_unifi_certSSL.sh:
```

```
#!/bin/bash
# Demande de certificat auprès de let'sencrypt
certbot renew --quiet --no-self-upgrade
# Convertir certificat au format PKCS #12 format
openssl pkcs12 -export -inkey /etc/letsencrypt/live/nomDeDomaineUnifi.ltd/privkey.pem -in
/etc/letsencrypt/live/nomDeDomaineUnifi.ltd/fullchain.pem -out /tmp/cert.p12 -name unifi -
password pass:myPassword
# Chargez-le dans le keystore java
keytool -importkeystore -deststorepass aircontrolentreprise -destkeypass aircontrolentreprise
-destkeystore /var/lib/unifi/keystore -srckeystore /tmp/cert.p12 -srcstoretype PKCS12 -
srcstorepass myPassword -alias unifi -noprompt
# Suppression du fichier certificat
rm /tmp/cert.p12
/etc/init.d/unifi restart
```

On rend le script executable:

```
chmod +x /emplacement/scripts/renew_unifi_certSSL.sh
```

ajout tache panifié au crontab, dans /etc/crontab:

```
00 23 5 * * root /emplacement/scripts/renew_unifi_certSSL.sh
```

Doc utilisé:

<https://www.wifi-france.com/le-blog/entry/44>