

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 la 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>

Revision #1

Created 27 November 2023 15:54:45 by Lauris_Adm

Updated 27 November 2023 16:04:30 by Lauris_Adm