SSL de LAN

Si vous voulez seulement mettre à jour les certificats car ils ont expirés, allez à la section UPDATE DES CERTIFS.

/!\ Des fois, le renew ne fonctionne pas, il suffit de le refaire /!

Les certifs sont générés sur ozone.

Pour générer les certificats pour un site dont les DNS sont sur le serveur et gérés avec bind9, et dont on veut avoir le SSL en LAN, il faut effectuer la commande suivante :

```
certbot certonly --manual --preferred-challenges=dns --manual-public-ip-logging-ok --manual-auth-hook /etc/letsencrypt/authenticator.sh --manual-cleanup-hook /etc/letsencrypt/cleanup.sh -d admin.lan.air-eisti.fr
```

- --manual : permet de génerer le certificat grâce à des hook (les scripts shells)
- --preferred-challenges=dns : demande de générer le certificat pour DNS-01 et permet de l'utiliser sur des DNS "locaux". Il faut déployer un record DNS TXT pour le temps de la validation
- --manual-public-ip-logging-ok : accepte automatiquement que l'IP soit loggé, sinon il faut le confirmer à la main
- --manual-auth-hook /etc/letsencrypt/authenticator.sh : execute authenticator.sh avant de générer les certificats, permet de déployer le record DNS TXT
- --manual-cleanup-hook /etc/letsencrypt/cleanup.sh : execute cleanup.sh après la génération des certificats, permet d'enlever le record DNS TXT
- -d admin.lan.air-eisti.fr spécifie le nom de domaine

avec authenticator.sh :

```
#!/bin/bash

DOMAIN=$CERTBOT_DOMAIN
VALIDATION=$CERTBOT_VALIDATION

DNS_PATH="/etc/bind/db.ext.air-eisti.fr"

# On cherche à modifier le sérial, qui est au format AAAAMMJJXX avec XX le numéro de version du jour, par défaut 00
# On incrémente de 1 à chaque modification effectuée le même jour que la précédente
```

```
DATE=$(date +%Y%m%d)
# Variable settant la recherche du commentaire présent sur la ligne du serial
NEEDLE="serial"
curr=$(/bin/grep -e "${NEEDLE}$" $DNS_PATH | /bin/sed -n "s/^\s*\([0-
9]*\)\s*;\s*${NEEDLE}\s*/\1/p")
if [ ${#curr} -lt ${#DATE} ]; then
   serial="${DATE}00"
else
   prefix=${curr::-2}
   if [ "$DATE" -eq "$prefix" ]; then # same day
     num=${curr: -2} # last two digits from serial number
     num=$((10#$num + 1)) # force decimal representation, increment
     serial="${DATE}$(printf '%02d' $num )" # format for 2 digits
   else
     serial="${DATE}00" # just update date
   fi
fi
/bin/sed -i -e "s/^\(\s*\)[0-9]\{0,\}\(\s*;\s*${NEEDLE}\)$/\1${serial}\2/" ${DNS_PATH}

# Déploie le DNS TXT record pour valider la demande de certificat
SOUSDOMAINE=${DOMAIN%*.*.*} # enleve .air-eisti.fr
echo "_acme-challenge.$SOUSDOMAINE IN TXT \"$VALIDATION\"" >> ${DNS_PATH}

# Application des changements
service bind9 restart
```

et cleanup.sh :

```
#!/bin/bash

DOMAIN=$CERTBOT_DOMAIN
VALIDATION=$CERTBOT_VALIDATION

DNS_PATH="/etc/bind/db.ext.air-eisti.fr"

# On cherche à modifier le sérial, qui est au format AAAAMMJJXX avec XX le numéro de version
du jour, par défaut 00
# On incrémente de 1 à chaque modification effectuée le même jour que la précédente
```

```
DATE=$(date +%Y%m%d)
# Variable settant la recherche du commentaire présent sur la ligne du serial
NEEDLE="serial"
curr=$(/bin/grep -e "${NEEDLE}$" $DNS_PATH | /bin/sed -n "s/^\s*\([0-
9]*\)\s*;\s*${NEEDLE}\s*/\1/p")
if [ ${#curr} -lt ${#DATE} ]; then
   serial="${DATE}00"
else
   prefix=${curr::-2}
   if [ "$DATE" -eq "$prefix" ]; then # same day
     num=${curr: -2} # last two digits from serial number
     num=$((10#$num + 1)) # force decimal representation, increment
     serial="${DATE}$(printf '%02d' $num )" # format for 2 digits
   else
     serial="${DATE}00" # just update date
   fi
fi
/bin/sed -i -e "s/^\(\s*\)[0-9]\{0,\}\(\s*;\s*${NEEDLE}\)$/\1${serial}\2/" ${DNS_PATH}

# Déploie le DNS TXT record pour valider la demande de certificat
SOUSDOMAINE=${DOMAIN%*.*.*} # enleve .air-eisti.fr
/bin/sed -i -e "/_acme-challenge.$SOUSDOMAINE IN TXT \"$VALIDATION\"/d" ${DNS_PATH}

# Application des changements
service bind9 restart
```

Quand on ne sera plus sous OPNSense, il faudra probablement ajouter la copie du cert.pem et du privkey.pem dans l'endroit où il faut à cleanup.sh, ils sont localisés dans /etc/letsencrypt/live/ Actuellement il faut copier coller dans le clicodrome d'OPNSense.

/!\ Apparemment, certbot 0.19 renew automatiquement, mais c'est pas sur, certbot renew --dry-run le fait en tout cas /!

De plus, on ne peux pas renew automatiquement les certificats (ils ont une durée de vie de 90 jours), donc il faut réeffectuer la commande pour recréer tous les certificats et re copier-coller dans OPNSense.

On peux faire une tache cron pour refaire la commande en y ajoutant --force-renewal (sinon certbot demande si on veut renew ou ne rien faire) à interval réguliers.

exemple pour un renew tout les mois

```
0 0 1 * * certbot certonly --manual --force-renewal --preferred-challenges=dns --manual-public-ip-logging-ok --manual-auth-hook /etc/letsencrypt/authenticator.sh --manual-cleanup-hook /etc/letsencrypt/cleanup.sh -d admin.lan.air-eisti.fr
```

Update des certifs

Si tout ce passe bien, le renew est automatique, du coup il suffit de faire les étapes suivantes.

Pour les VM du core et du portail captif :

depuis ozone, mettez les clefs dans votre home, accessible par votre user. Les clefs sont dans /etc/letsencrypt/archive/urlDuSite, n'oubliez pas d'enlever les anciennes et les garder celle avec le plus récent numéro, et enlever ce numéro (ex: privkey3.pem -> privkey.pem)

Il faudra le faire pour les 3 domaines suivants (avec ip de la VM pour se co en ssh):

```
portal.lan.air-eisti.fr (machine : portal.lan.air-eisti.fr / 10.82.0.66)
core.lan.air-eisti.fr (machine : main-web.net.air-eisti.fr / 10.82.0.65)
lpmng.lan.air-eisti.fr (machine : main-web.net.air-eisti.fr / 10.82.0.65)
```

en réseau de lan, il faut être dans le vlan admin puis :

```
ssh root@10.82.0.40
(demander mdp à admin)
ssh -i first_key_openstack centos@IPDeLaVM
(ça va calculer pendant un petit peu de temps, vous pouvez à la place récupérer la clef depuis barium puis
ssh -i first_key_openstack centos@portal.lan.air-eisti.fr depuis votre session (en fermant le ssh depuis barium))
```

Puis

```
scp -r votreUser@air-eisti.fr:~/urlDuSite ./urlDuSite
cp -R urlDuSite /etc/key/
```

pour tester si la maj a bien été faite :

```
curl urldusite
```

Révision #2
Créé 2020-12-29 17:00:49 UTC par blacksponge
Mis à jour 2020-12-29 17:11:18 UTC par blacksponge