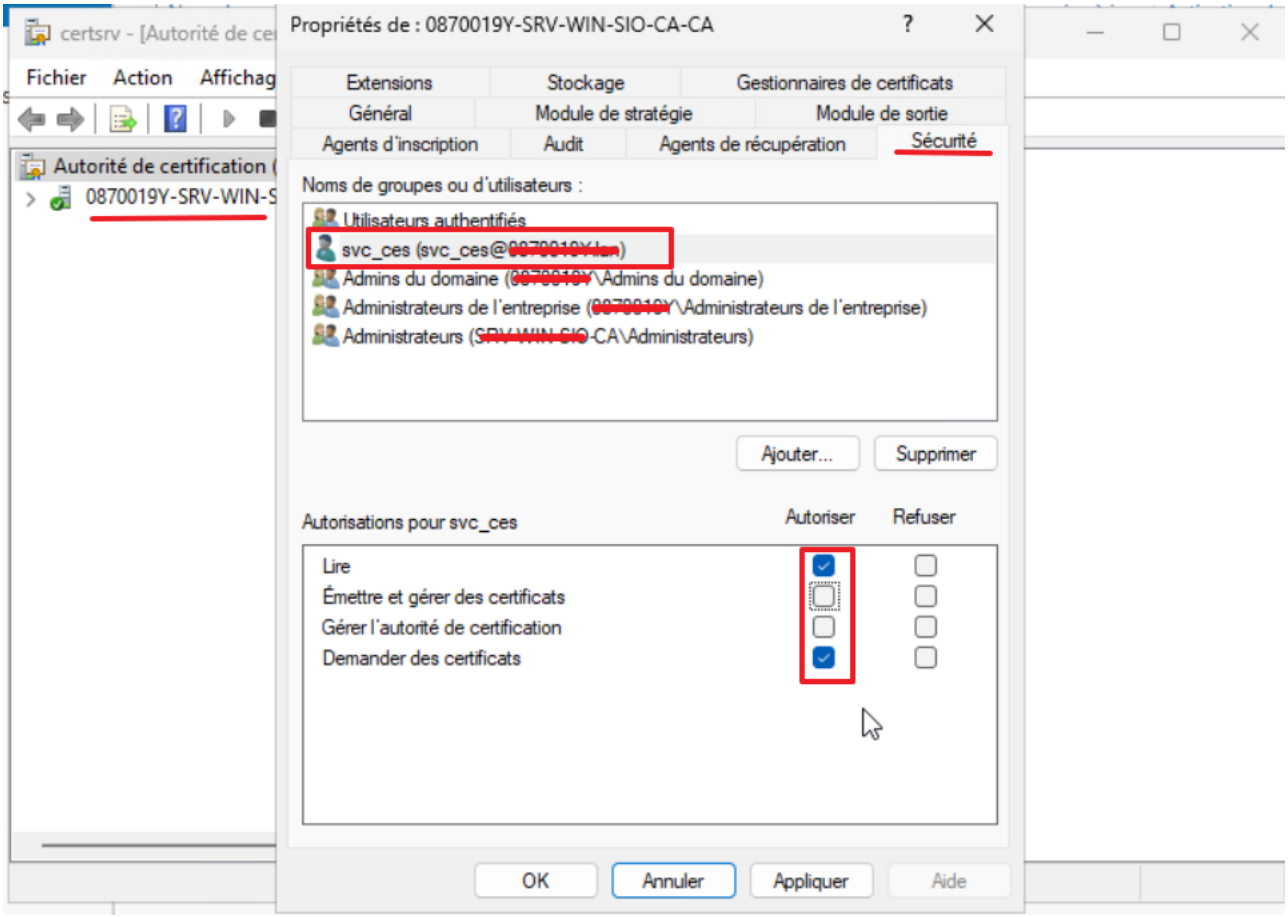
Gérer des certificats pour serveurs Debian avec la CA de Microsoft

- Le sous-composant **Service Web Inscription de certificats** du rôle **Service de certificats Active Directory** doit avoir été installé.

> Le **Service Web Inscription de certificats (CES)** permet à des machines et utilisateurs d'obtenir ou renouveler des certificats via HTTPS, même s'ils ne sont pas connectés au domaine (ex : ordinateurs en DMZ, machines distantes, BYOD...).

Création d'un compte dédié appelé svc_ces dans le domaine

- créer le compte **svc_ces**
- le mettre membre du groupe local **IIS_IUSRS** du serveur CES
    - Lui donner les droits sur la CA dans certsrv.msc → Propriétés → Sécurité :
        - ajouter le compte **svc_ces**
        - lui donner les droits :
            - Lire
            - Demander des certificats



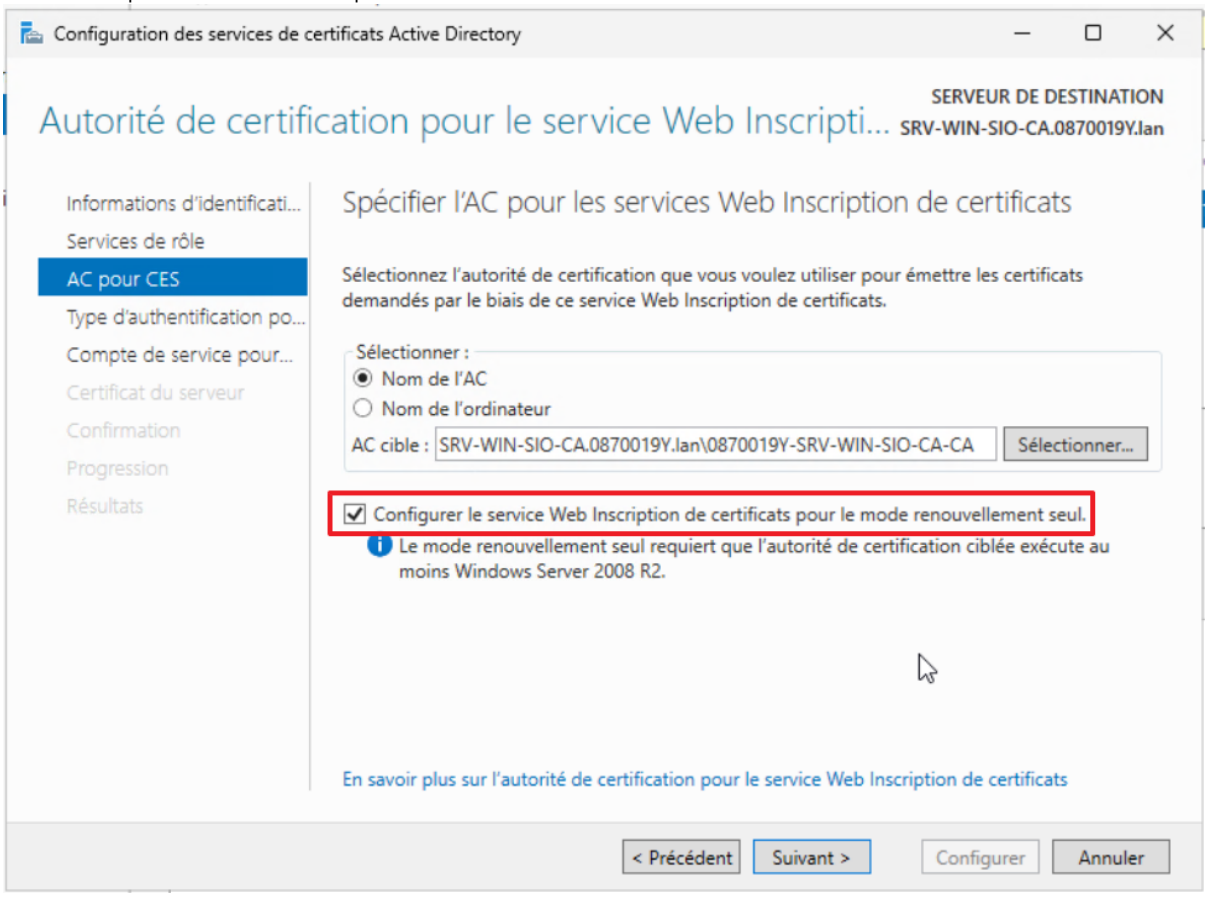
Le configurer comme Identité du pool d'applications CES dans IIS.

- Redémarrer IIS en ligne de commande en tant qu'administrateur

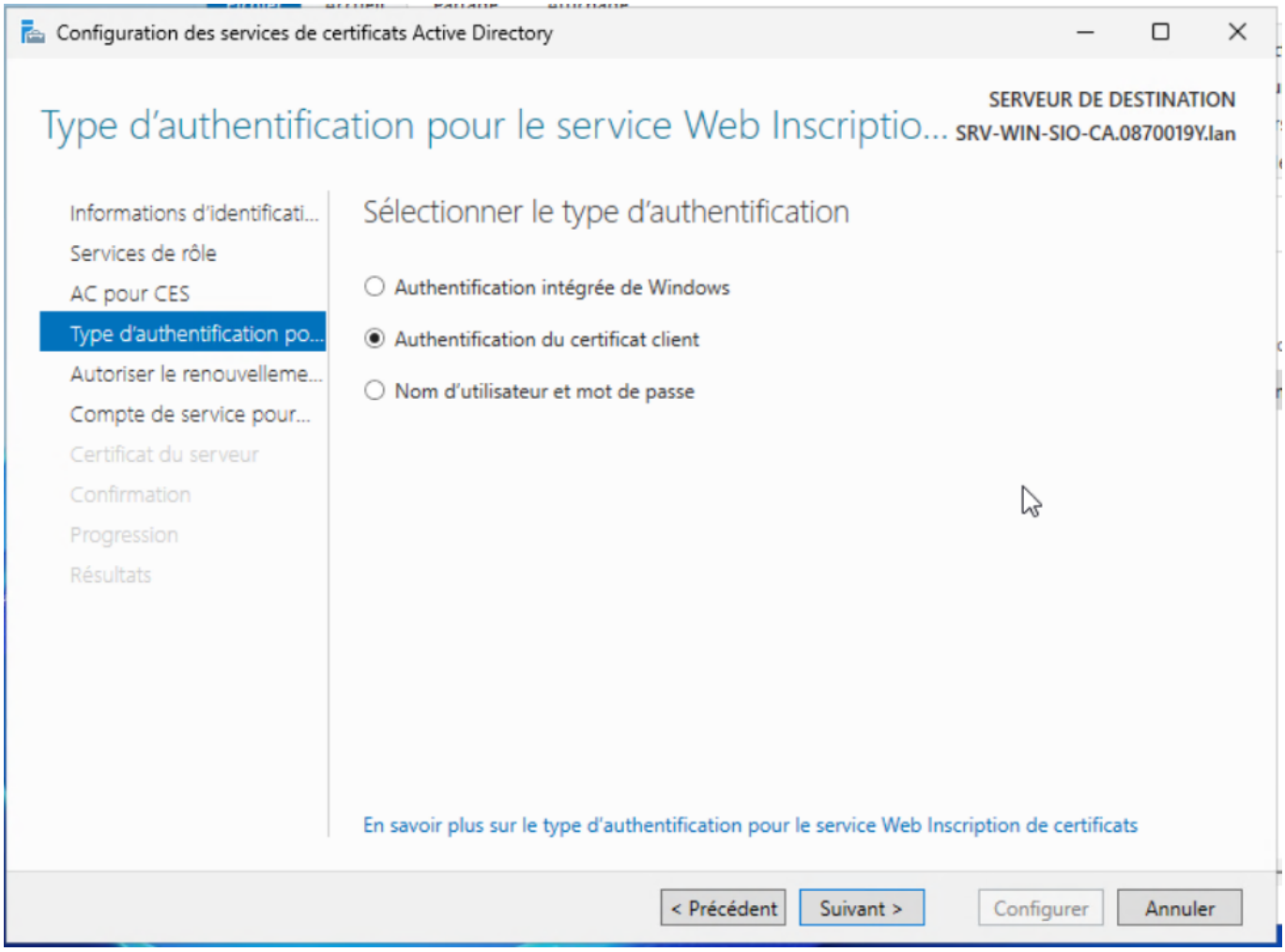
```
iisreset
```

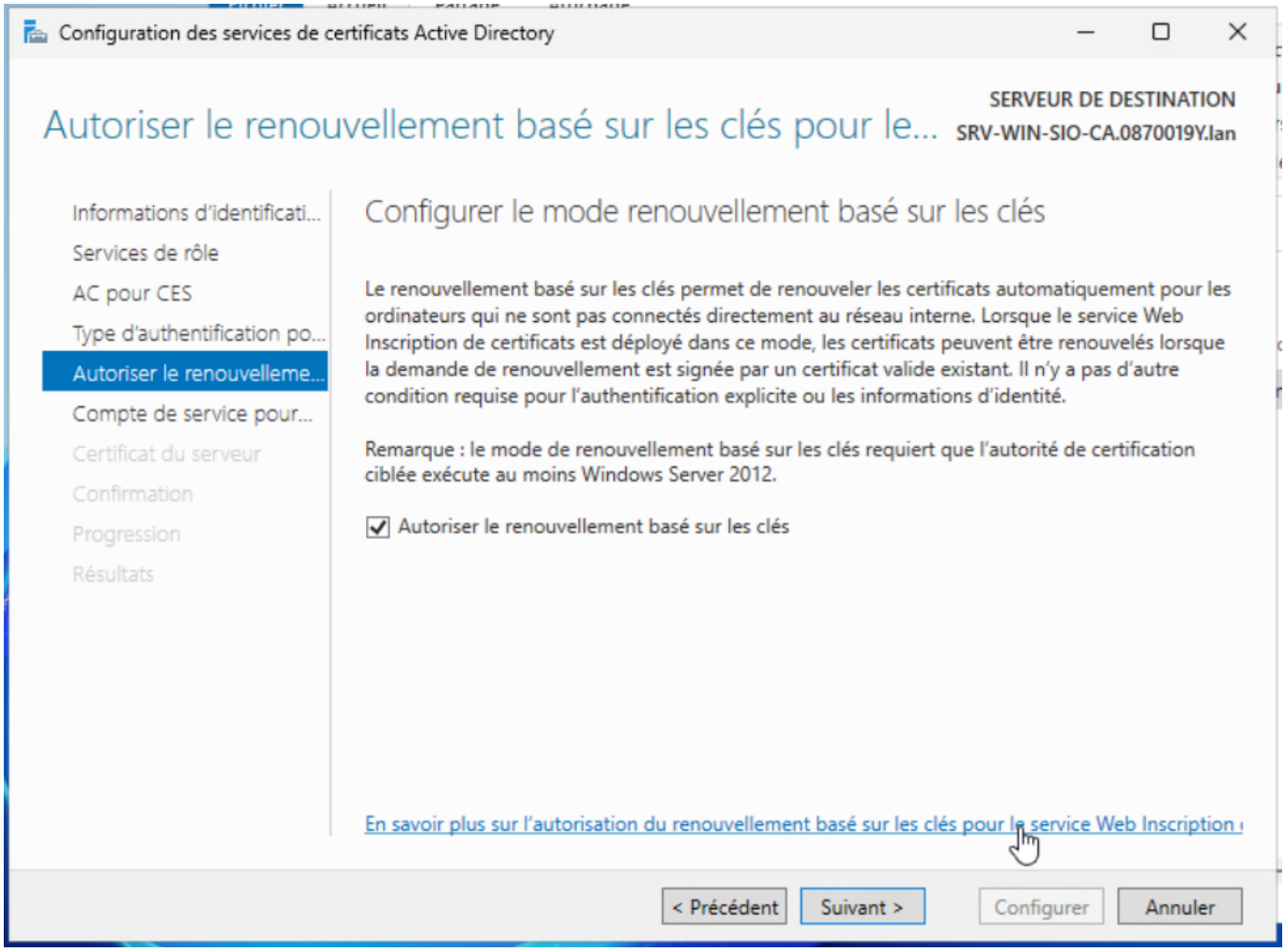
Configuration du service Web d'inscription des certificats

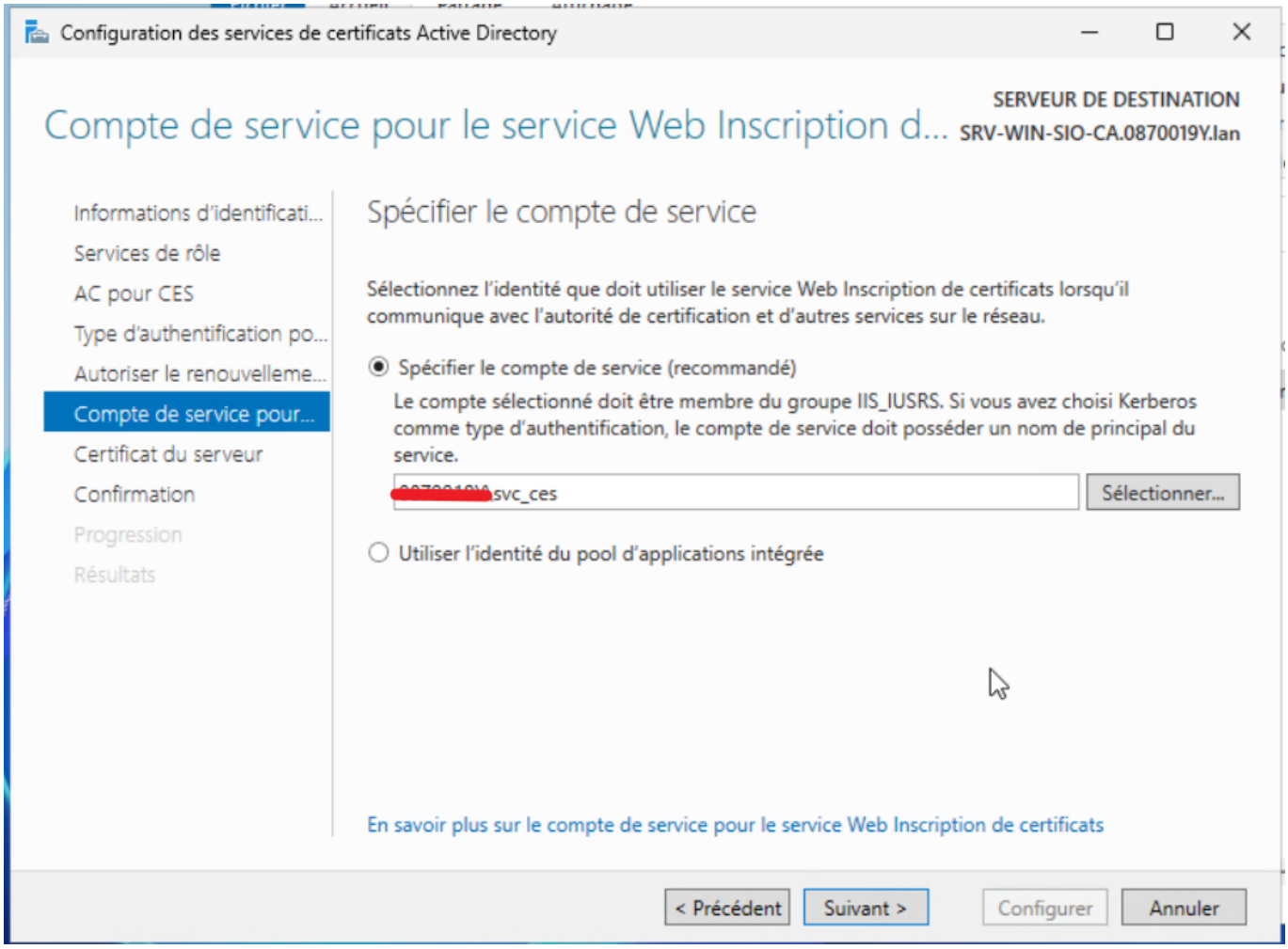
- Installation en **Renouvellement seul** :
  - ⇒ les clients peuvent demander uniquement de renouveler des certificats existants.

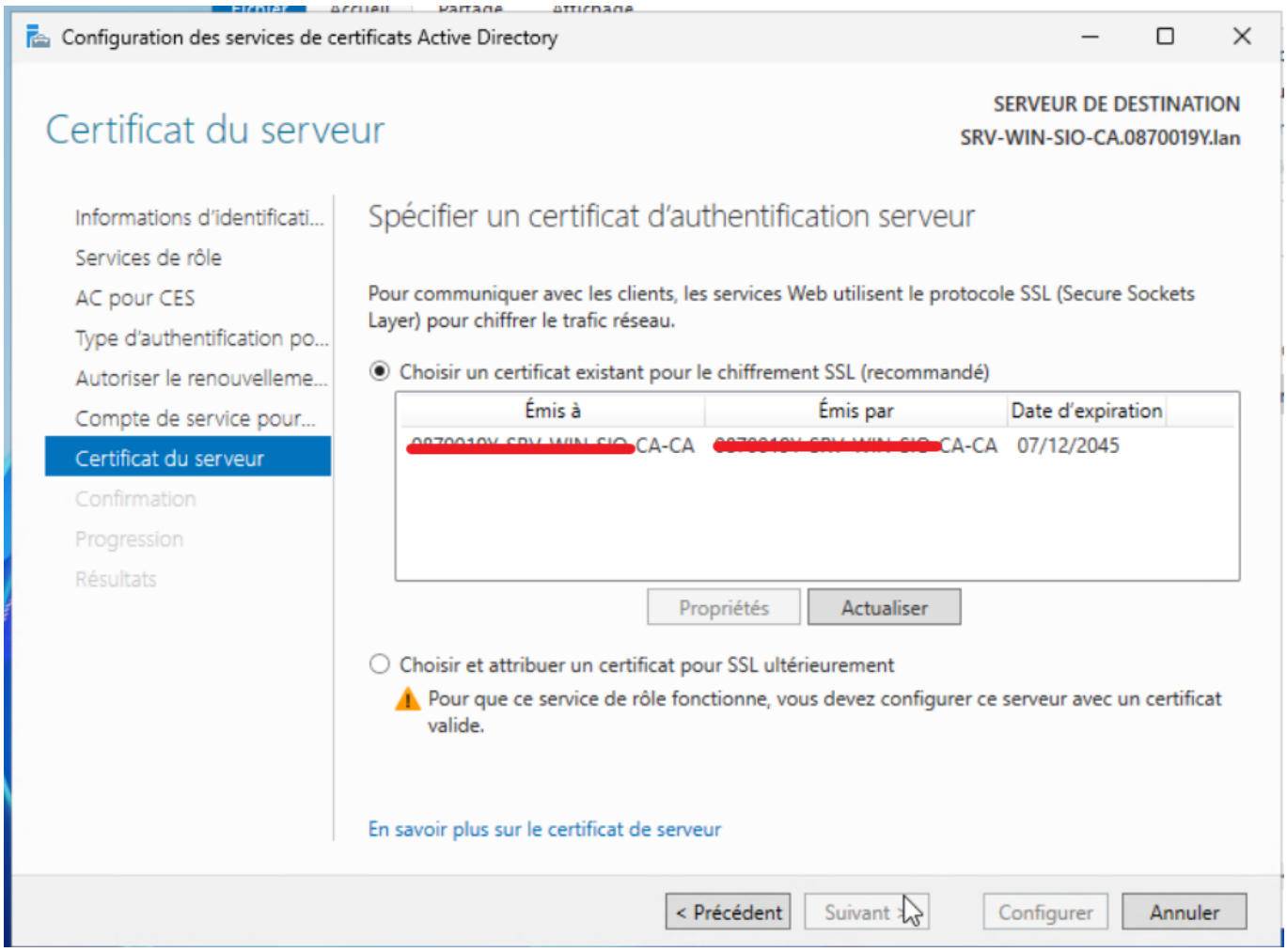


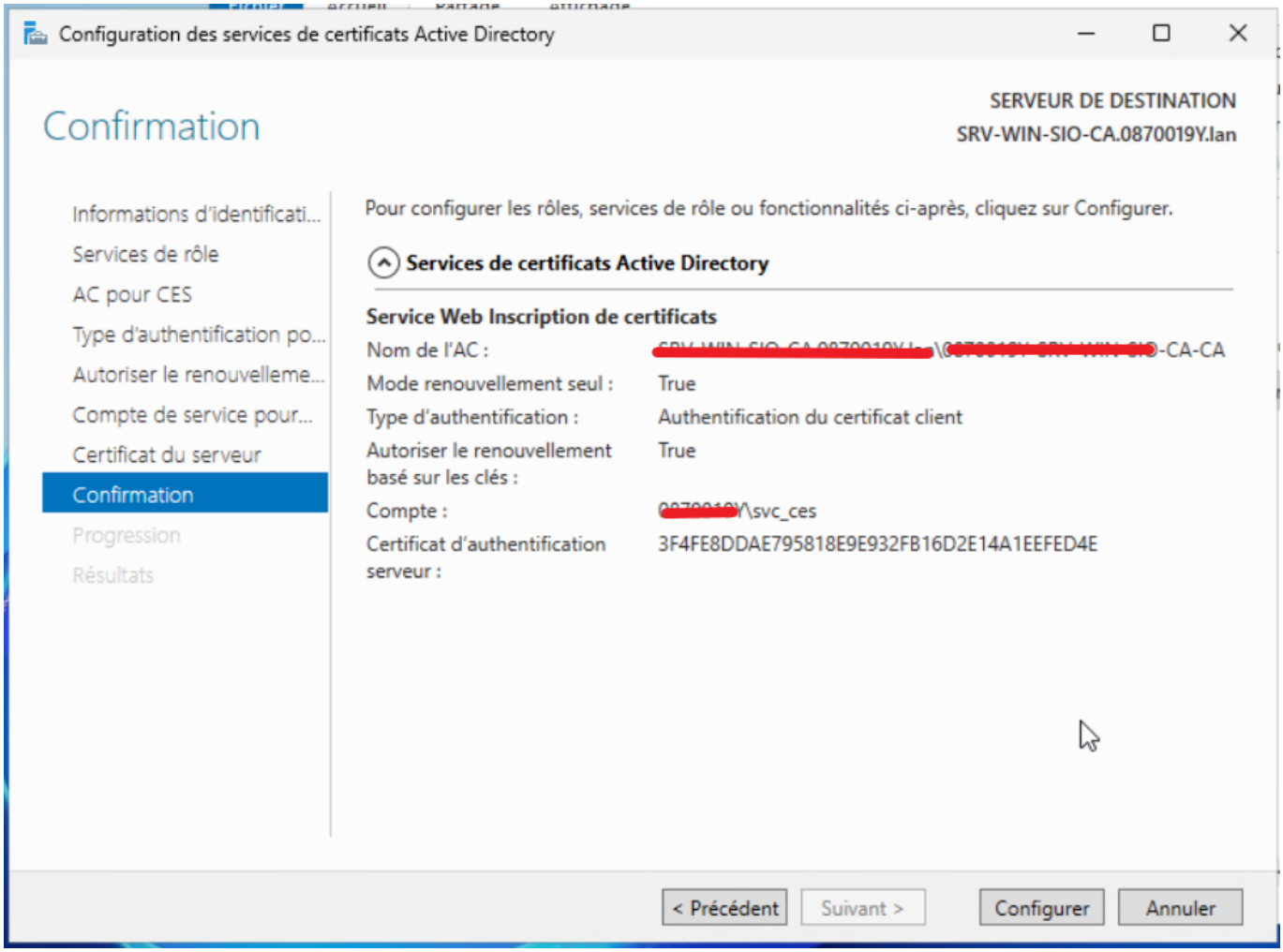
- Authentification est **Authentification du certificat client** :

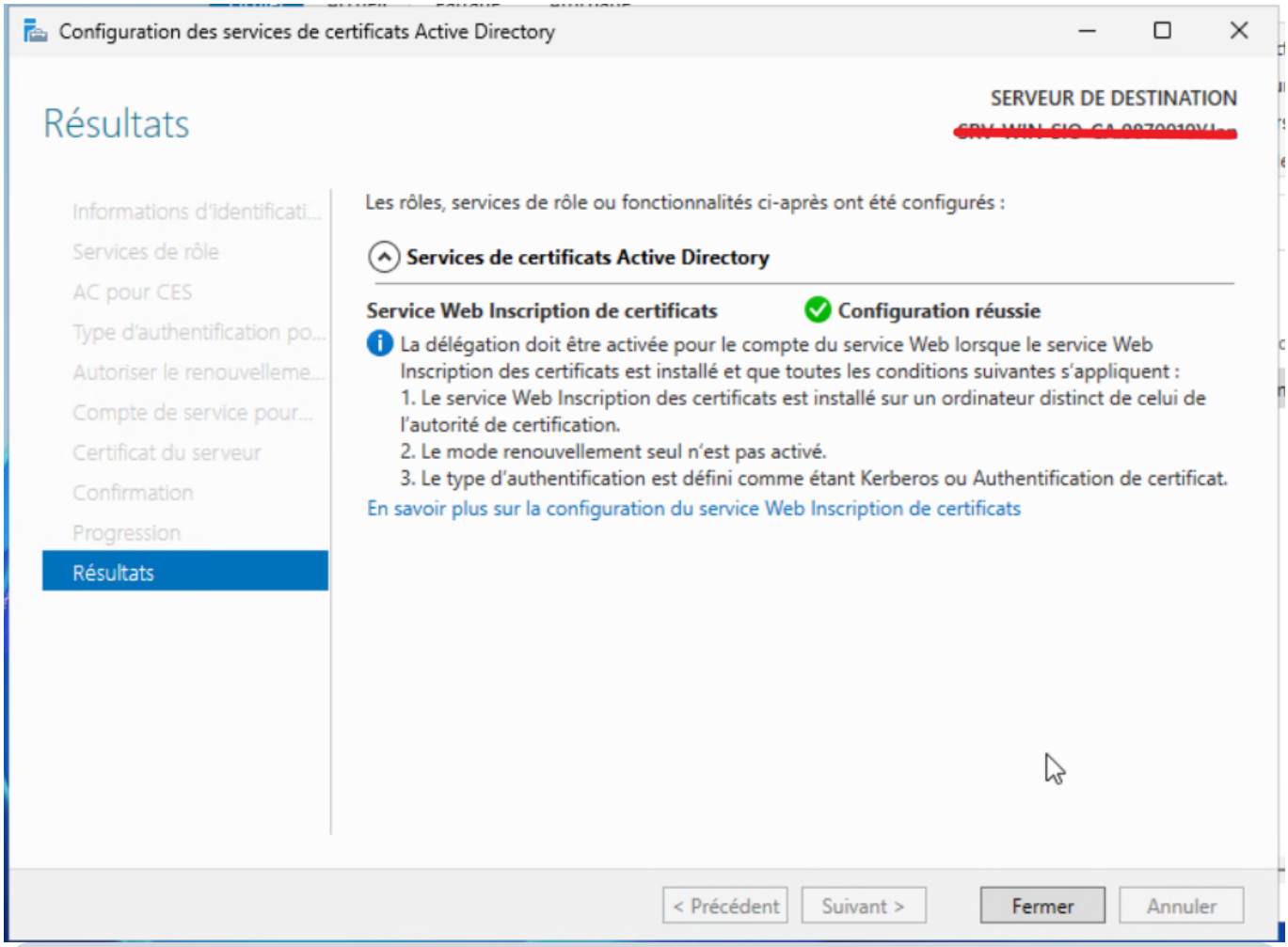

Configuration des services de certificats Active Directory
Type d'authentification pour le service Web Inscriptio...
SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan
Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvelleme...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats
Sélectionner le type d'authentification
Authentification intégrée de Windows
Authentification du certificat client
Nom d'utilisateur et mot de passe
En savoir plus sur le type d'authentification pour le service Web Inscription de certificats
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Autoriser le renouvellement basé sur les clés pour le...
SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan
Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvelleme...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats
Configurer le mode renouvellement basé sur les clés
Le renouvellement basé sur les clés permet de renouveler les certificats automatiquement pour les ordinateurs qui ne sont pas connectés directement au réseau interne. Lorsque le service Web Inscription de certificats est déployé dans ce mode, les certificats peuvent être renouvelés lorsque la demande de renouvellement est signée par un certificat valide existant. Il n'y a pas d'autre condition requise pour l'authentification explicite ou les informations d'identité.
Remarque : le mode de renouvellement basé sur les clés requiert que l'autorité de certification ciblée exécute au moins Windows Server 2012.
Autoriser le renouvellement basé sur les clés
En savoir plus sur l'autorisation du renouvellement basé sur les clés pour le service Web Inscription
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Compte de service pour le service Web Inscription d...
SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan
Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvelleme...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats
Spécifier le compte de service
Sélectionnez l'identité que doit utiliser le service Web Inscription de certificats lorsqu'il communique avec l'autorité de certification et d'autres services sur le réseau.
Spécifier le compte de service (recommandé)
Le compte sélectionné doit être membre du groupe IIS_IUSRS. Si vous avez choisi Kerberos comme type d'authentification, le compte de service doit posséder un nom de principal du service.
[redacted]svc_ces
Sélectionner...
Utiliser l'identité du pool d'applications intégrée
En savoir plus sur le compte de service pour le service Web Inscription de certificats
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Certificat du serveur
SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan
Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvelleme...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats
Spécifier un certificat d'authentification serveur
Pour communiquer avec les clients, les services Web utilisent le protocole SSL (Secure Sockets Layer) pour chiffrer le trafic réseau.
Choisir un certificat existant pour le chiffrement SSL (recommandé)
Émis à
Émis par
Date d'expiration
[redacted]CA-CA
[redacted]CA-CA
07/12/2045
Propriétés
Actualiser
Choisir et attribuer un certificat pour SSL ultérieurement
Pour que ce service de rôle fonctionne, vous devez configurer ce serveur avec un certificat valide.
En savoir plus sur le certificat de serveur
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Confirmation
SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan
Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvelleme...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats
Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.
Services de certificats Active Directory
Service Web Inscription de certificats
Nom de l'AC :
-CA-CA
Mode renouvellement seul : True
Type d'authentification : Authentification du certificat client
Autoriser le renouvellement basé sur les clés : True
Compte : Y\svc_ces
Certificat d'authentification serveur : 3F4FE8DDAE795818E9E932FB16D2E14A1EEFED4E
< Précédent
Suivant >
Configurer
Annuler



Principes de fonctionnement quand CES est configuré en renouvellement seulement :

- Le client envoie une requête de renouvellement (CSR)
- Il signe la requête avec la clé privée de son ancien certificat
- Le serveur CES valide que :
  - le certificat à renouveler est légitime
  - la signature correspond à la clé privée
  - la CA accepte les renouvellements

La CA délivre un nouveau certificat basé sur l'ancien.

Aucune demande de **nouveau certificat** n'est acceptée.

Cela permet :

- d'**exposer** CES via Internet,
- de permettre uniquement la **continuité**, pas de nouvelles inscriptions
- pour des appareils **non joints au domaine** mais **déjà équipés d'un certificat initial**
- en réduisant l'exposition du service d'inscription

Disposer des autorisation d'enrollement sur les modèles de certificat

- lancer la console des modèles de certificats certtmpl.msc,
- cliquez-droit sur le modèle voulu et accédez à ses propriétés puis l'onglet Sécurité :
- donner l'autorisation **Inscrire**

Configurer un serveur Debian

Obtenir un certificat initial (bootstrap)

- Lien https://www.it-connect.fr/ad-cs-comment-delivrer-un-certificat-tls-pour-un-serveur-web-linux/

Générer une clé privée et un CSR

Pour les services comme Apache, Nginx, HAProxy ou Postfix, les clé privées sont enregistrées dasn le dossier **/etc/ssl/private/** :

- répertoire défini pour contenir les clés privées sensibles
- avec les permissions suivantes : drwx–x–x root:root /etc/ssl/private

- En CLI

```
openssl genrsa -out /etc/ssl/private/server.key 2048
chmod 600 /etc/ssl/private/server.key
chown root:root /etc/ssl/private/server.key
```

Gestion de la clé pour HAProxy

HAProxy préfère un fichier unique PEM contenant (dans l'ordre) :

- la clé privée,
- le certificat du serveur,
- la chaîne intermédiaire

Ce fichier PEM unique est placé dasn le dossier **/etc/haproxy/certs/**

Contenu du fichier PEM :

```
-----BEGIN PRIVATE KEY-----
(key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(cert)
-----END CERTIFICATE-----
(intermediate chain)
```

- Droits :

```
chmod 600 /etc/haproxy/certs/nomsite.pem
chown root:root /etc/haproxy/certs/nomsite.pem
```

Gestion de la clé pour Apache2

Dossiers de la clé et du certificat

- clé privée : /etc/ssl/private/nomsite.key
- certificat : /etc/ssl/certs/nomsite.crt

Configuration du fichier pioru le site Web **/etc/apache2/sites-enabled/site.conf** :

```
SSLCertificateFile /etc/ssl/certs/nomsite.crt
SSLCertificateKeyFile /etc/ssl/private/nomsite.key
```

Gestion du certificat pour Tomcat9

- créer le dossier **/etc/tomcat9/ssl**
- créer le fichier keystore unique contenant :
    - la clé privée,
    - le certificat signé,
    - la chaîne intermédiaire ADCS

- Création du keystore PKCS12 depuis les fichiers PEM :

```
openssl pkcs12 -export \
   -inkey server.key \
   -   -in cert.pem \
```

```
   -    -certfile chain.pem \
   -    -out /etc/tomcat9/ssl/tomcat.p12
```

- Protection du certificat:

```
chmod 600 /etc/tomcat9/ssl/tomcat.p12
chown tomcat:tomcat /etc/tomcat9/ssl/tomcat.p12
```

Génération du fichier de demande de signature pour le certificat

Crée un fichier san.cnf pour ajouter un SAN (recommandé) pur un serveur exemple appelé guac.lab.local avec ce contenu :

```
[ req ]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[ dn ]
CN = guac.lab.local

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = guac.lab.local
DNS.2 = guac
```

- générer le CSR

```
openssl req -new -key guac.lab.local.key \
  -out guac.lab.local.csr \
  -config san.cnf
```

```
* vérifiez le csr
```

```
openssl req -text -noout -verify -in guac.lab.local.csr
Certificate request self-signature verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN=guac.lab.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:7f:55:b1:ca:09:23:12:fc:1b:d4:97:7a:76:
                    8e:50:37:24:ce:4a:e7:c8:3e:75:82:7b:78:9b:8b:
                    94:bb:6d:7e:31:6f:9c:25:77:4d:ab:55:c7:06:31:
                    09:dc:43:80:32:7f:5d:89:22:15:4c:ea:ea:ba:81:
                    79:6b:f0:16:53:3c:b1:38:db:04:33:bb:d2:04:24:
                    db:8f:d9:a6:a7:45:04:ea:ac:3d:eb:19:91:bb:ed:
                    d0:7b:8c:ba:6b:9b:a1:17:a2:cc:15:1b:c4:dc:fd:
                    b9:e7:dd:5c:47:d0:d9:53:93:70:4c:c8:1a:41:32:
                    84:e2:c5:63:3d:d2:93:96:81:0c:bf:d9:25:59:bd:
                    de:eb:99:56:e4:2d:06:ce:cb:33:92:98:a4:41:18:
                    5a:de:5d:8d:2a:b4:5b:c7:d2:d3:f1:e9:30:4c:ba:
                    93:fc:44:d5:f6:cf:7d:49:69:b7:b5:66:7d:99:4f:
                    1c:0a:cb:43:30:71:70:96:53:75:bc:18:43:ff:c8:
                    e6:94:00:2b:ad:d9:e5:a6:5b:cc:5a:c6:6b:1e:15:
                    69:35:a4:3c:30:80:e8:a7:c0:de:23:79:96:d5:ab:
                    0c:2d:48:ad:28:63:66:6c:dc:79:5f:e8:3d:b4:4e:
                    ab:6d:58:04:66:44:11:36:77:73:0a:50:7b:ed:59:
                    ad:01
                Exponent: 65537 (0x10001)
        Attributes:
            Requested Extensions:
```

```
            X509v3 Subject Alternative Name:
                DNS:guac.lab.local, DNS:guac
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        58:57:5e:29:66:bf:38:7d:b0:0f:c2:d5:cd:37:b9:51:ab:10:
        7f:4c:ac:f1:15:1f:82:8b:d1:ca:e3:8f:da:03:a2:24:1c:ac:
        78:f6:81:4c:8c:ac:0c:37:02:fe:ec:1f:f2:d0:51:d6:a3:f5:
        da:01:d4:aa:c3:27:d9:d3:f1:5b:99:00:14:b3:e0:32:a4:a1:
        2f:4c:2d:52:84:bc:da:fc:fd:c7:7c:ae:da:9c:b2:e3:78:24:
        74:62:3d:50:af:7a:de:b5:92:91:c9:fe:f1:90:5c:8c:11:a1:
        a7:ba:5b:ed:4f:59:05:7a:06:11:69:ca:d8:e4:1f:4e:ee:4b:
        63:81:47:58:10:e1:0a:cf:cb:b9:0c:76:f5:2c:d1:05:a0:b2:
        be:a5:da:dc:bc:9c:5e:9a:06:5b:0c:d8:13:a9:4a:fd:c3:c1:
        c0:ff:8b:0e:33:2b:b8:0d:c8:73:f4:d3:3b:22:e6:4e:80:e3:
        c5:f3:76:5b:a4:89:1c:f1:9b:6f:a9:88:ec:f7:f6:4e:58:2d:
        42:6d:c6:06:b9:58:fa:98:db:17:9a:5c:ce:64:3a:fc:e5:be:
        4f:08:58:ac:fe:3a:26:f1:ef:1d:09:9a:46:8c:2f:31:1b:68:
        e5:96:08:ea:63:35:63:8c:6f:fb:4a:5d:28:2a:00:a5:c6:b8:
        f8:b5:c4:ec
```

- ⇒ obtenir un fichier .cer.
- récupérer le certificat de l'autorité racine (Root CA), depuis Windows.

```
certutil -ca.cert rootCA.cer
```

- Copier le certificat .cer du serveur + celui de la CA dans le dossier conteneur LXC

Dans le conteneur LXC Convertir le certificat Microsoft en PEM

- convertir les fichiers .cer en .crt

```
openssl x509 -in guac.lab.local.cer -out guac.lab.local.crt
openssl x509 -in rootCA.cer -out rootCA.crt
```

Construire le fichier .pem pour HAProxy

HAProxy doit avoir un seul fichier .pem contenant :

- la clé privée du serveur
- le certificat serveur
- la chaîne CA (intermédiaires + racine)

```
cat guac.lab.local.key guac.lab.local.crt rootCA.crt > /etc/haproxy/certs/guac.lab.local.pem
```

- Donner des permissions sécurisées :

```
chmod 600 /etc/haproxy/certs/guac.lab.local.pem
```

Recharger HAProxy

```
haproxy -c -f /etc/haproxy/haproxy.cfg
systemctl reload haproxy
```

- Naviguer ensuite vers le site https://guac.lab.local