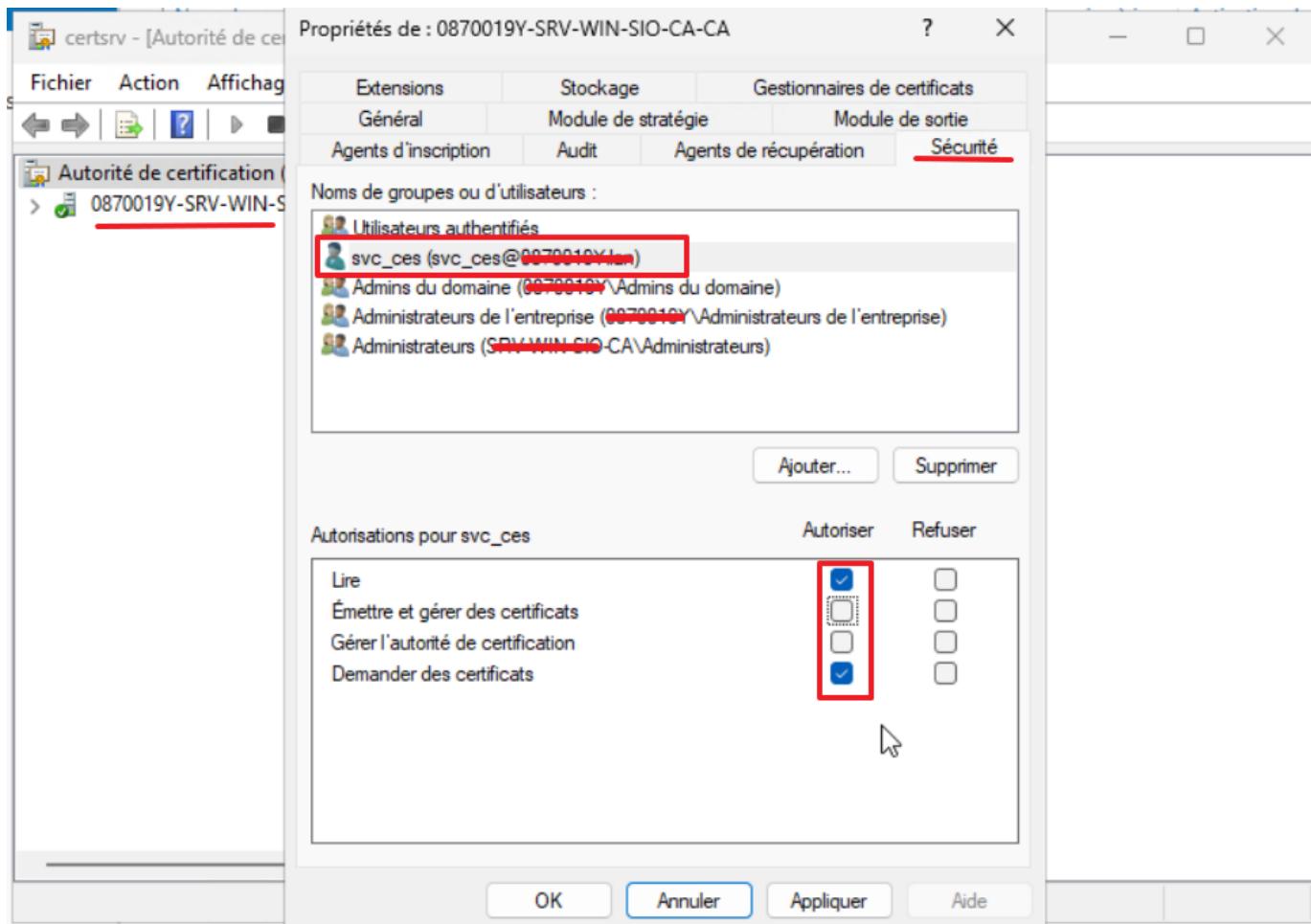


Gérer des certificats pour serveurs Debian avec la CA de Microsoft

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

Création d'un compte dédié appelé svc_ces dans le domaine

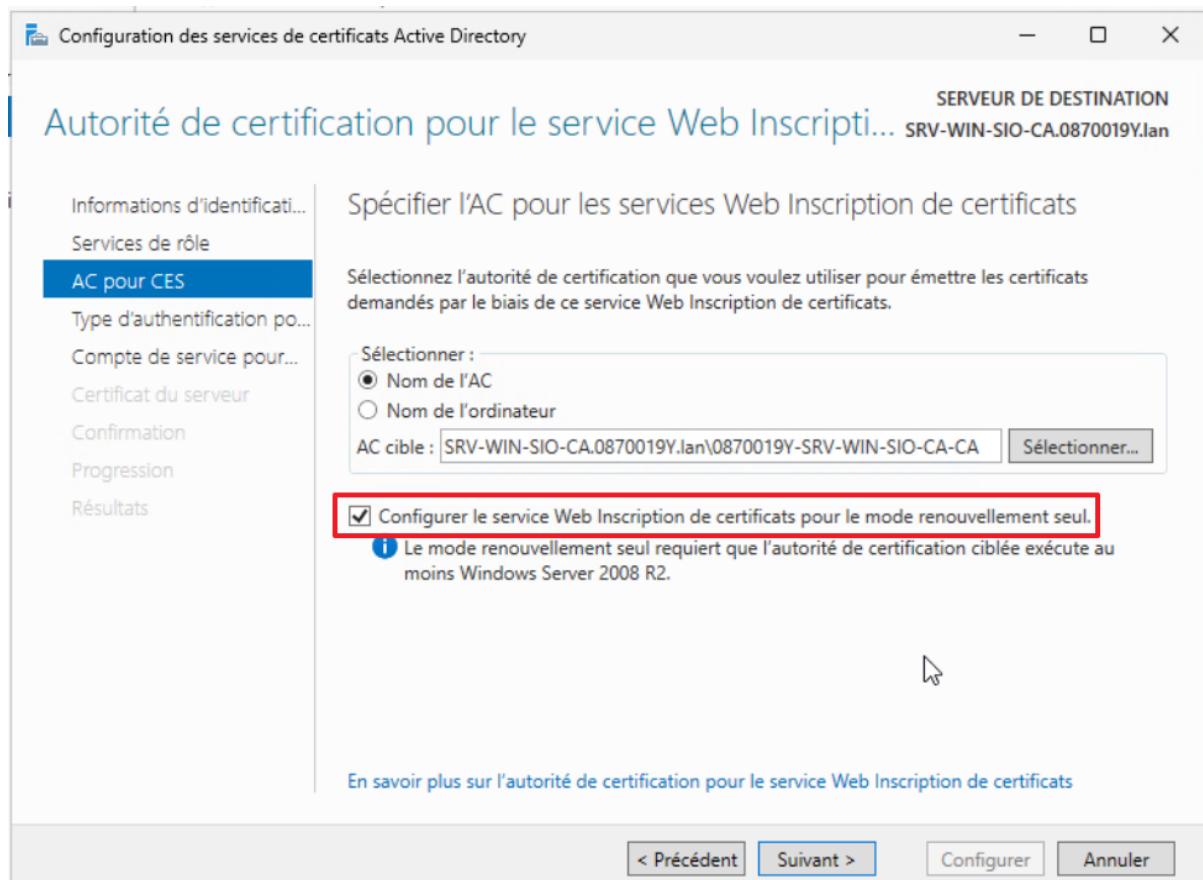
```
* créer le compte **svc_ces**
* le mettre membre du groupe local **IIS_IUSRS** du serveur CES
* Lui donner les droits sur la CA dans certsrv.msc → Propriétés → Sécurité :
  * Lire
  * Demander des certificats
  * Emettre et gérer des certificats
```



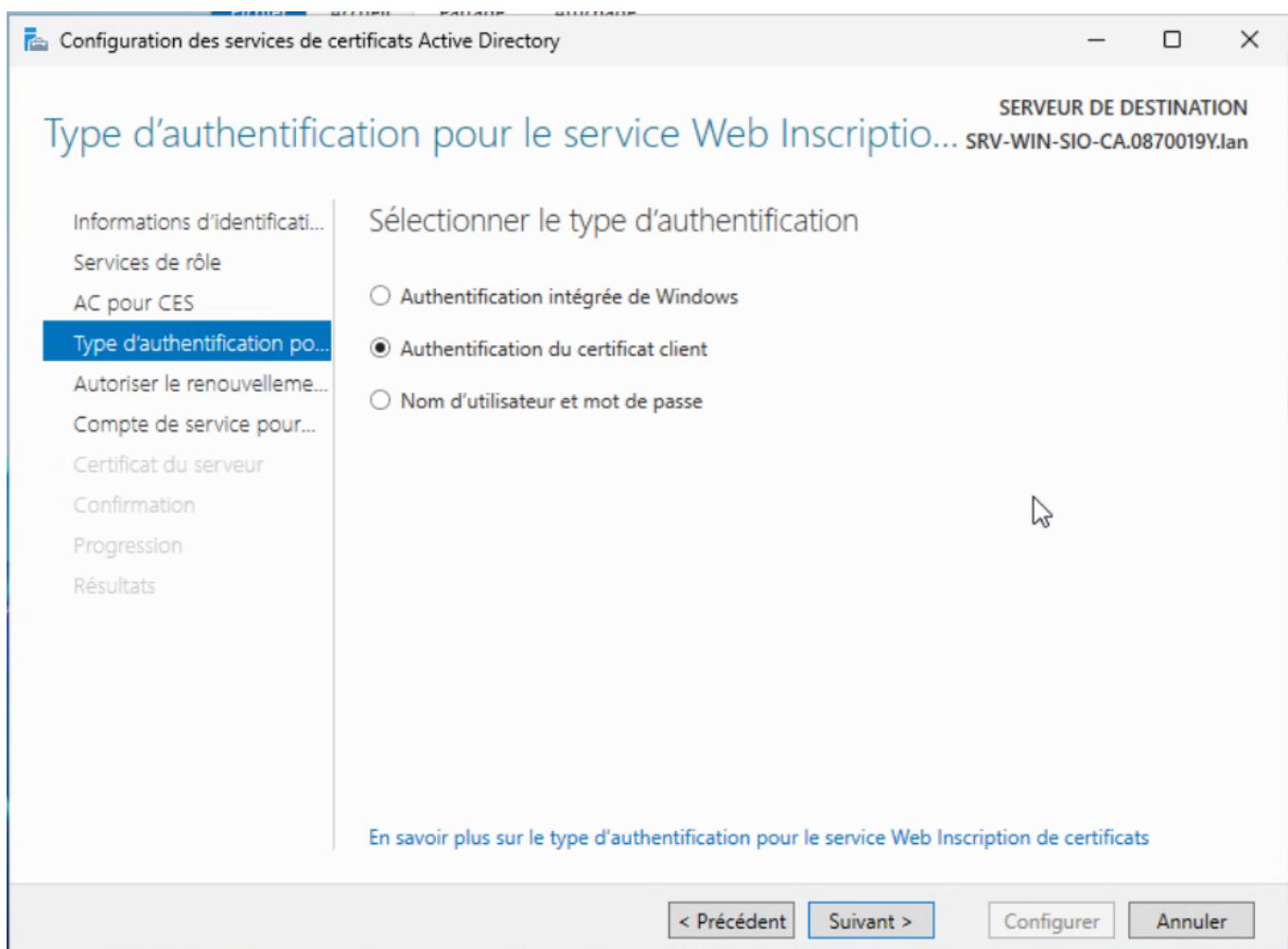
Le configurer comme Identité du pool d'applications CES dans IIS.

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

SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan

Autoriser le renouvellement basé sur les clés pour le...

Informations d'identificati... Services de rôle AC pour CES Type d'authentification po... **Autoriser le renouvellemen...** 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

SERVEUR DE DESTINATION
SRV-WIN-SIO-CA.0870019Y.lan

Compte de service pour le service Web Incription d...

Informations d'identificati...
Services de rôle
AC pour CES
Type d'authentification po...
Autoriser le renouvellemen...
Compte de service pour...
Certificat du serveur
Confirmation
Progression
Résultats

Spécifier le compte de service

Sélectionnez l'identité que doit utiliser le service Web Incription 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.
 Utiliser l'identité du pool d'applications intégrée

0870019Y.svc_ces

En savoir plus sur le compte de service pour le service Web Incription de certificats

< Précédent Configurer Annuler

Configurer un serveur Debian

Générer une clé privée et un CSR

- Obtenir un certificat initial (bootstrap) → L'utiliser pour s'authentifier auprès du CES → Automatiser le renouvellement du certificat via CES
- Installer automatiquement le nouveau certificat dans le système

From:
/- Les cours du BTS SIO

Permanent link:
</doku.php/reseau/certificat/camicicrosoft/accueil?rev=1768738573>

Last update: **2026/01/18 13:16**

