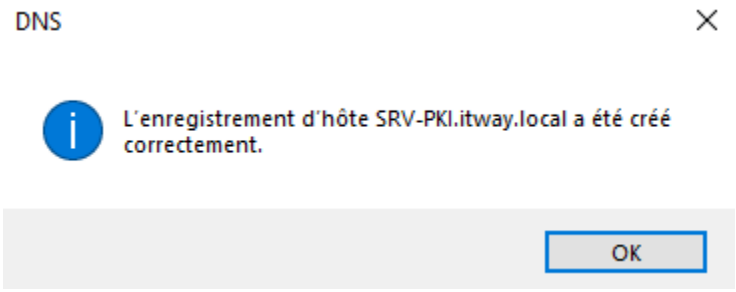
Configuration du serveur PKI (SRV-PKI.itway.local) dans l'AD

1. Création de l'enregistrement DNS pour SRV-PKI

Dans le serveur DNS de l'AD (172.16.50.2) :

1. Ouvrir **Gestionnaire DNS** (dnsmgmt.msc)
2. Développer **Zones de recherche directes** > **itway.local**
3. Clique droit > **Nouvel hôte (A ou AAAA)...**
4. Remplir :
    - Nom : srv-pki
    - Adresse IP : 172.16.50.3
5. Cocher "Créer un enregistrement de pointeur associé"
6. Cliquer sur **Ajouter un hôte**



✅ **Vérification** :

```
nslookup srv-pki.itway.local
```

→ Doit retourner `172.16.50.3`

3. Configuration de la confiance PKI dans l'AD

3.1. Exporter le certificat racine du serveur PKI

Depuis le serveur PKI (Debian) :

```
openssl x509 -in /chemin/vers/ca.crt -out /chemin/vers/ca.cer -outform DER
```

Cette commande convertit un certificat depuis un format `.crt` en PEM vers un `.cer` en **DER** compatible avec Windows.

Pour trouver le chemin du CA, regarder dans le fichier de config des chemins :

```
# Configuration des chemins
pki_ca_dir: "/etc/pki"
pki_ca_key_name: "ca.key"
pki_ca_cert_name: "ca.crt"
pki_openssl_conf: "/etc/ssl/openssl.cnf"
```

Donc le chemin de notre ca.crt est /etc/pki/certs/ca.crt

Il faut d'abord créer le répertoire Certs dans lequel nous allons stocker notre ca.cer.
mkdir C:\Certs

Ensuite il faut installer le service ssh sur windows s'il n'est pas installé. Ouvrir PowerShell en administrateur sur le serveur Windows et vérifier s'il est en cours d'exécution :
Get-Service sshd

Si le statut est "Running", alors tout est ok. Sinon, il faut le démarrer :
Start-Service sshd

Et s'il apparaît impossible de trouver un service assorti du nom "sshd", il faut l'installer.
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'

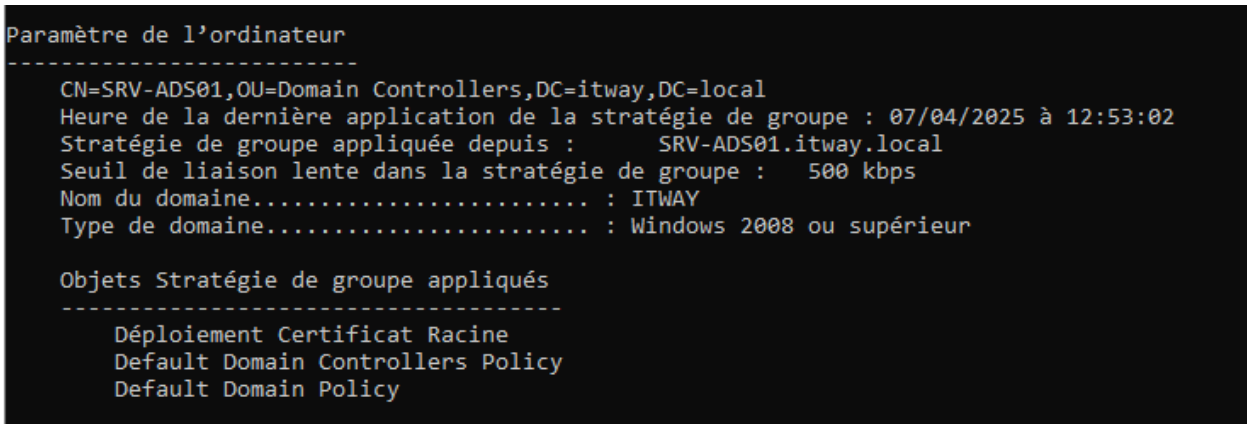
Vérifier s'il le service est installés côté client et serveur, sinon installer celui qui est manquant, dans notre cas il nous manquait le serveur que nous avons téléchargé et installé :
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

Puis vérifier l'installation :
Get-Service sshd

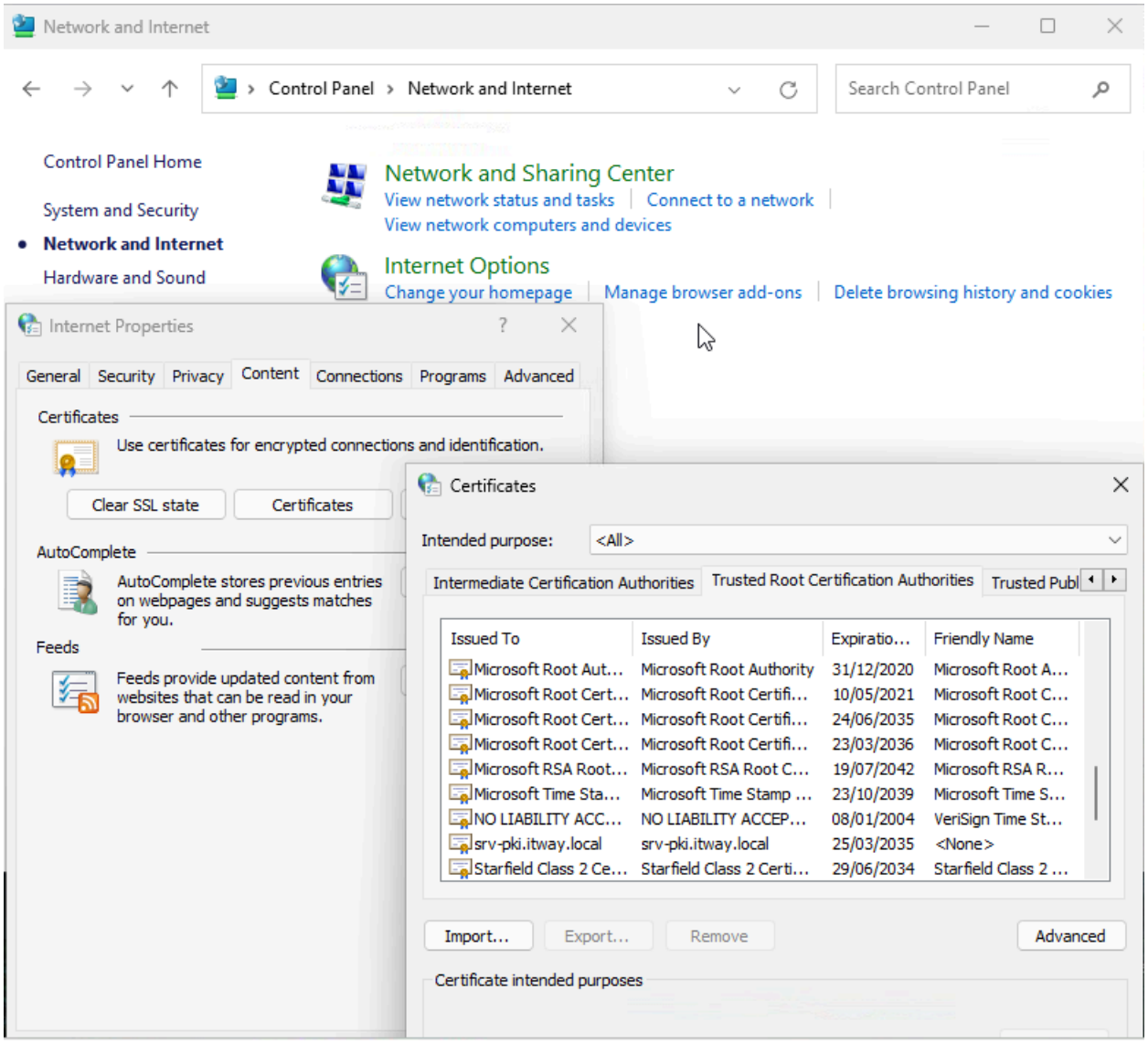
Si tout s'est bien passé, le service sera listé, probablement avec le statut "Stopped", alors il faudra le démarrer :
Start-Service sshd

Maintenant que tout est prêt, il faut copier ca.cer sur le contrôleur de domaine après avoir
Scp etc/pki/certs/ca.cer Administrator@172.16.50.2:C:\Certs

Faire gpo pour mettre ca dans magasin de certificats racine de confiance.
Gpupdate /force
Faire un gpresult /r dans l'AD pour voir si la gpo est mise en oeuvre



Pour tester, sur l'ordinateur user je vais dans le panneau de configuration > Réseau et internet > Options internet > onglet Contenu > Certificats > défiler jusqu'à l'onglet Autorités de certification racines de confiance et vérifier que l'autorité de certification que l'on vient de déployer est bien dans la liste.



On peut constater que le certificat de srv-pki-itway.local apparaît parmi les autorités de certification racine de confiance.