

## Création d'une autorité de certification

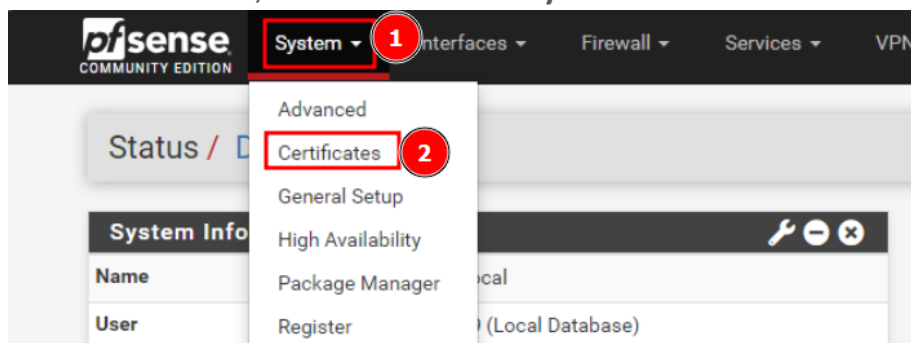
Version de PfSense : 2.7.0

1 – Création de l'autorité de certification.....	1
2 – Création du certificat pour les applications Web .....	3
3 – Déploiement du certificat sur un GLPI.....	5
4 – Déploiement de l'autorité de certification sur vos machines manuellement .....	6
5 – Déploiement de l'autorité de certification via GPO .....	8

Mon PfSense ainsi que ma machine GLPI ont été ajoutées dans le cache de mon serveur DNS comme sous-domaine. Cela est à prendre en compte pour le reste de la procédure.

### 1 – Création de l'autorité de certification

Sur votre PfSense, rendez-vous dans **System -> Certificate**



## Cliquez sur Add

Authorities Certificates Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Jumas Authority	✓	self-signed	1	CN=jumas.local Valid From: Tue, 30 Jan 2024 14:22:33 +0100 Valid Until: Fri, 27 Jan 2024 14:22:33 +0100		

## Donnez un nom à votre certificat

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

**Create / Edit CA**

**Descriptive name**

The name of this entry as displayed in the GUI for reference.  
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, " , ' .

**Method**

Dans le champ **Common Name**, rentrez votre nom de domaine par exemple, puis cliquez sur **Save**.

**Internal Certificate Authority**

**Key type**

The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm**

The digest method used when the CA is signed.  
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

**Lifetime (days)**

**Common Name**

Vous devriez vous retrouver avec votre autorité

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Jumas Authority	✓	self-signed	1	CN=jumas.local Valid From: Tue, 30 Jan 2024 14:22:33 +0100 Valid Until: Fri, 27 Jan 2024 14:22:33 +0100		



Modifiez ensuite le **Common Name** par \*.<nom\_de\_domaine> (dans mon cas ce sera \*.jumas.local)

En ajoutant une wildcard devant le nom, cela nous permet d'utiliser le même certificat pour chaque application Web.

Si vous préférez générer un certificat par application web, alors mettez le nom de votre application web.

**Digest Algorithm**    
The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

**Lifetime (days)**    
The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

**Common Name**

Dans la partie **Certificate Attributes** modifiez comme l'image ci-dessous

**Certificate Attributes**





**Attribute Notes** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.   
 For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type**    
 Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Alternative Names**     
 Type Value   
 Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

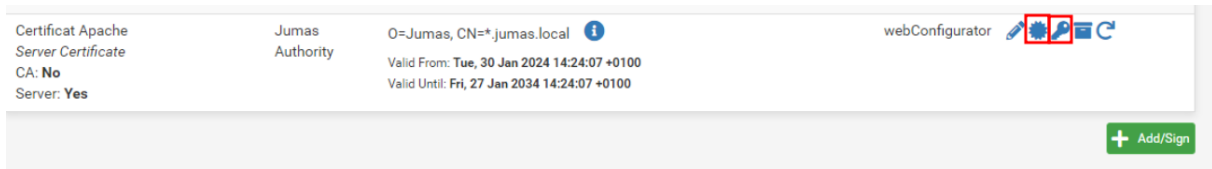
**Add SAN Row**

Vous devriez vous retrouver avec votre certificat

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (65a515b8b784a) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-65a515b8b784a ⓘ Valid From: Mon, 15 Jan 2024 12:23:36 +0100 Valid Until: Sun, 16 Feb 2025 12:23:36 +0100		  
Certificat Apache Server Certificate CA: No Server: Yes	Jumas Authority	O=Jumas, CN=*.jumas.local ⓘ Valid From: Tue, 30 Jan 2024 14:24:07 +0100 Valid Until: Fri, 27 Jan 2024 14:24:07 +0100	webConfigurator	  

### 3 – Déploiement du certificat sur un GLPI

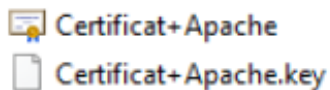
Il va falloir en premier lieu télécharger le certificat et la clé privé dans les options de votre certificat



Vous devriez vous retrouver avec deux fichiers.

Un fichier \*.crt

Un fichier \*.key



Il va maintenant falloir transférer ces deux certificats sur votre machine GLPI grâce à un serveur web python, ou l'outil scp inclut avec ssh.

Transférez ces deux fichiers dans l'emplacement **/etc/ssl/** sur votre GLPI

```
root@SRVA-GLPI:/etc/ssl# ls
Certificat+Apache.crt  Certificat+Apache.key  certs  openssl.cnf  private
root@SRVA-GLPI:/etc/ssl# _
```

Utilisez ensuite la commande suivante :

> **a2enmod ssl**

Il va falloir ensuite modifier le fichier Virtualhost de GLPI qui se trouve dans **/etc/apache2/sites-available/\*.conf**

```
root@SRVA-GLPI:/etc/ssl# nano /etc/apache2/sites-available/support.jumas.local.conf _
```

Il va maintenant falloir rediriger le trafic HTTP vers HTTPS, et ajouter les lignes SSL comme ci-dessous

```
<VirtualHost *:80>
  ServerName support.jumas.local
  Redirect permanent / https://support.jumas.local
</VirtualHost>

<VirtualHost *:443>
  ServerName support.jumas.local
  DocumentRoot /var/www/glpi/public
  ServerAlias www.jumas.local

  SSLEngine on
  SSLCertificateFile /etc/ssl/Certificat+Apache.crt
  SSLCertificateKeyFile /etc/ssl/Certificat+Apache.key

  <Directory /var/www/glpi/public>
    Require all granted
    RewriteEngine On
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php [QSA,L]
  </Directory>
</VirtualHost>
```

Redirection HTTP vers HTTPS

Ajout du SSL et des certificats

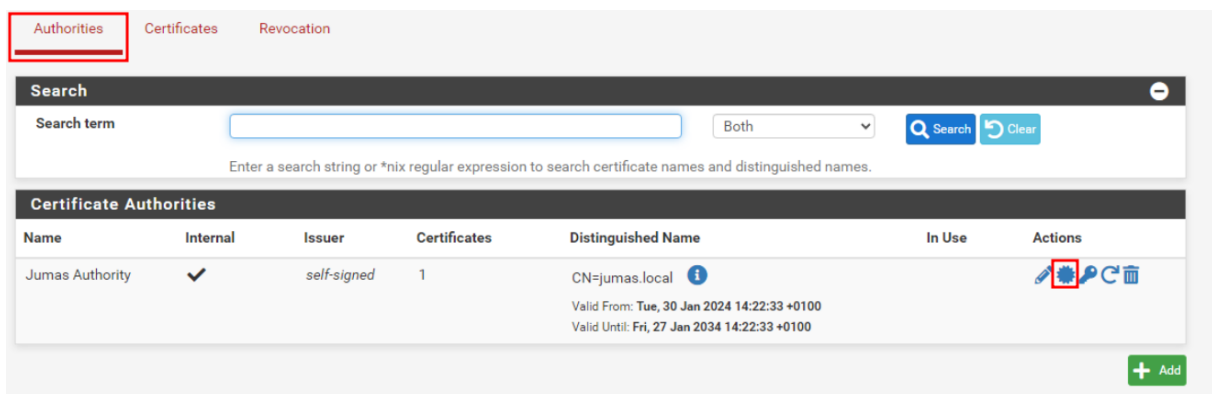
Il faut maintenant redémarrer votre service apache avec la commande suivante  
> `sudo systemctl restart apache2`

## 4 – Déploiement de l'autorité de certification sur vos machines manuellement

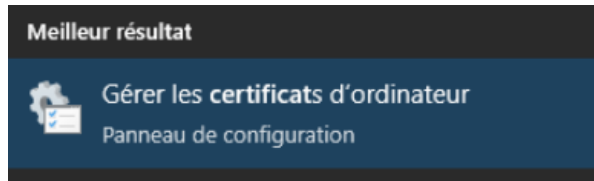
Afin que vos machines puissent reconnaître l'autorité de certification, il va falloir installer le certificat sur ces machines.

Nous verrons dans cette partie comment le faire pour des machines Windows.

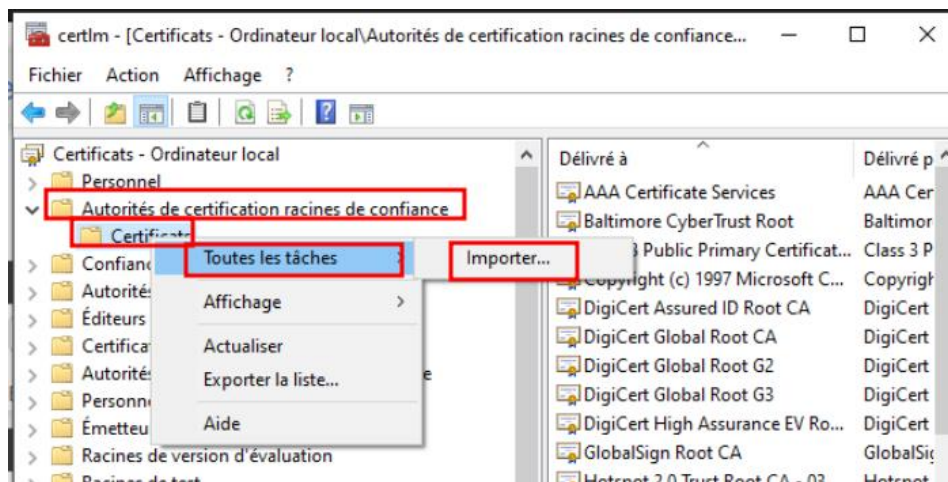
Il va donc falloir récupérer le certificat de votre autorité de certification sur votre PfSense



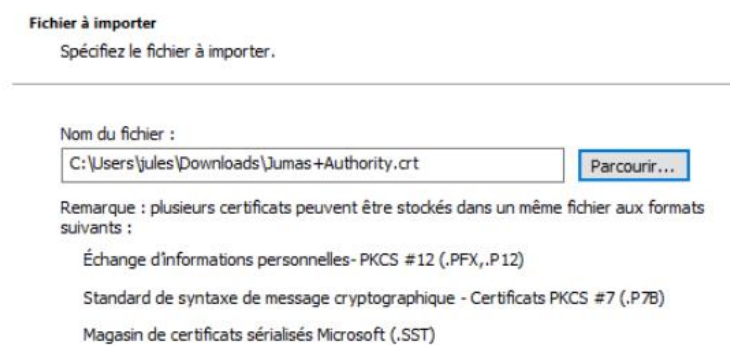
Il va maintenant falloir importer ce certificat sur votre machine Windows, pour ce faire rendez vous dans la console qui gère les certificats d'ordinateur



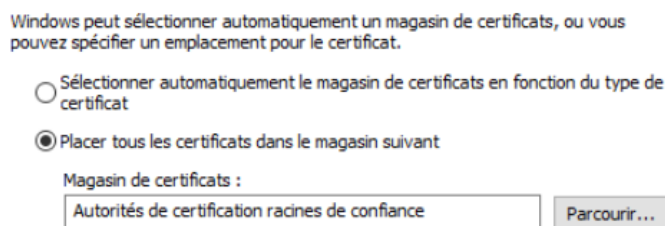
Allez ensuite **dans Autorité de certification racines de confiance** et importez votre certificat



Sélectionnez votre certificat dans la nouvelle fenêtre

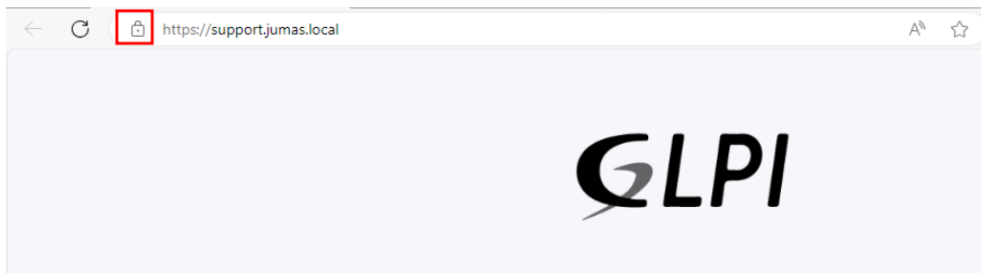


Laissez cette option par défaut



Une fois terminé, redémarrez votre machine.

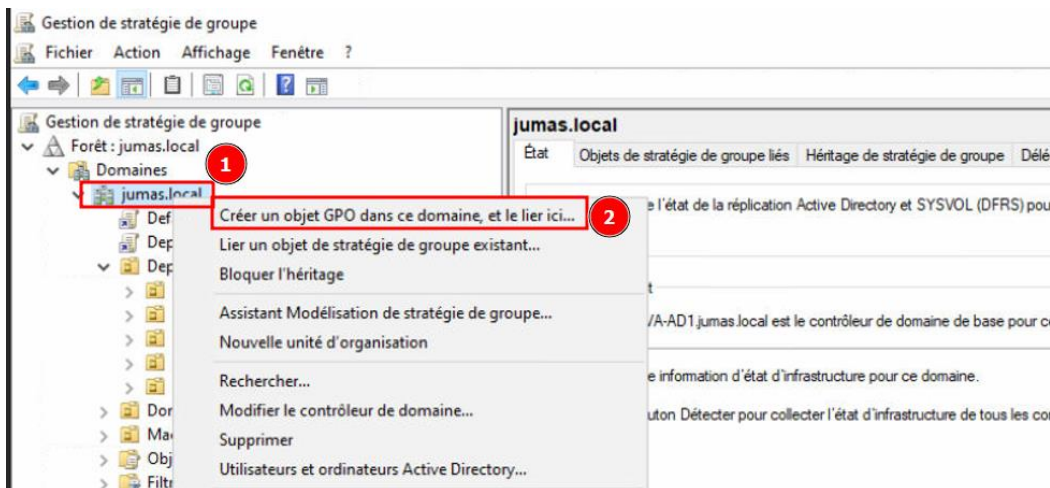
Vous devriez maintenant avoir accès à votre interface en HTTPS.



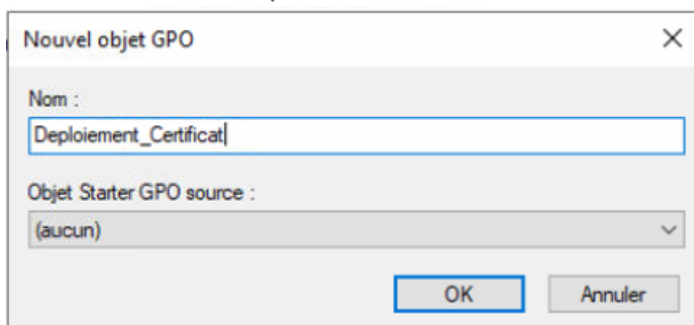
## 5 – Déploiement de l'autorité de certification via GPO

Rendez-vous dans votre serveur Active Directory et ouvrez la console de gestion de stratégie de groupe

Faites un clic droit au niveau de votre domaine afin de créer une nouvelle GPO et de la lier à la racine du domaine

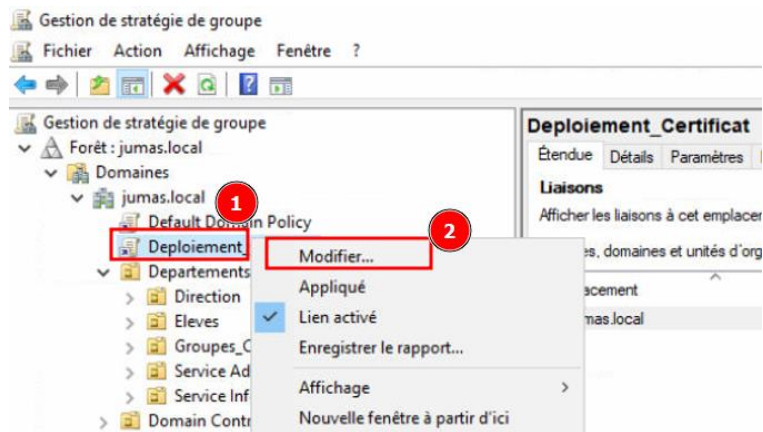


Donnez un nom explicite à votre GPO

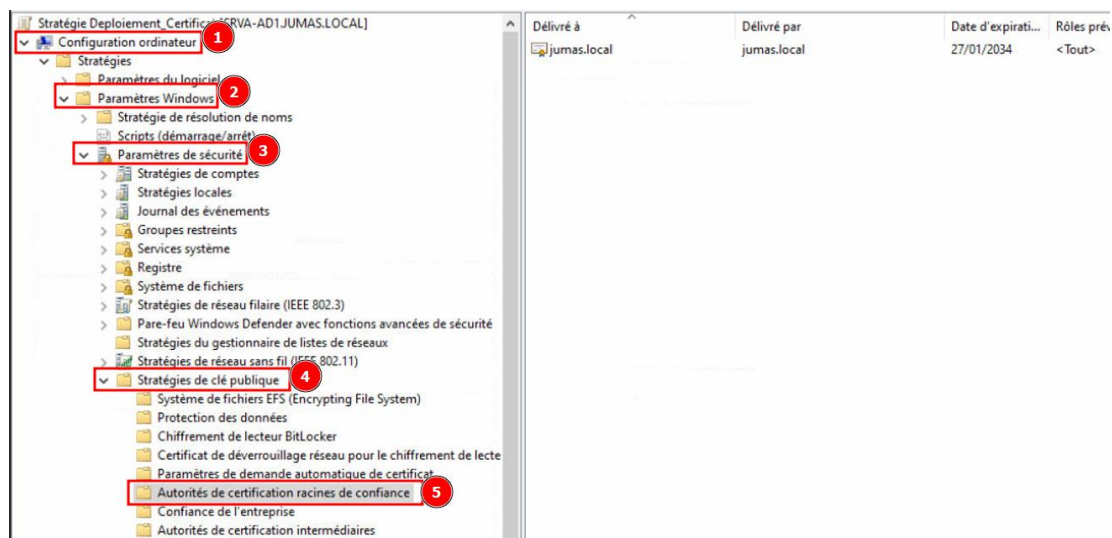




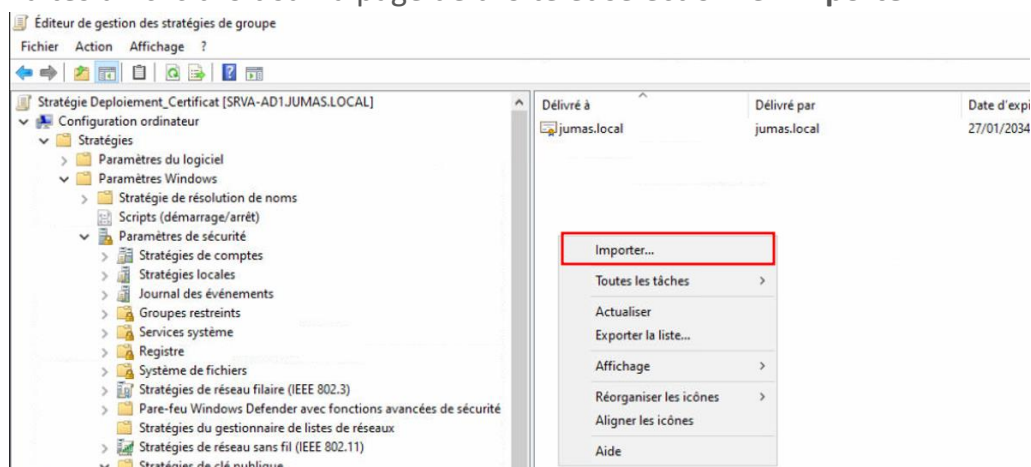
Faites un clic droit sur votre GPO et sélectionnez **Modifier**



Maintenant rendez-vous dans **Configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de clé publique -> Autorités de certification racine de confiance**



Faites un clic droit sur la page de droite et sélectionnez **Importer**



## Sélectionnez votre certificat

**Fichier à importer**  
Spécifiez le fichier à importer.

---

Nom du fichier :

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

- Échange d'informations personnelles- PKCS #12 (.PFX,.P12)
- Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
- Magasin de certificats sérialisés Microsoft (.SST)

## Laissez ce paramètre par défaut

**Magasin de certificats**  
Les magasins de certificats sont des zones système où les certificats sont conservés.

---

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

☐ Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
 ☒ Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Vous pouvez maintenant cliquer sur **Terminer**

**Fin de l'Assistant Importation du certificat**

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné par l'utilisateur	Autorités de certification racines de cc
Contenu	Certificat
Nom du fichier	C:\Users\Administrateur\Downloads\J

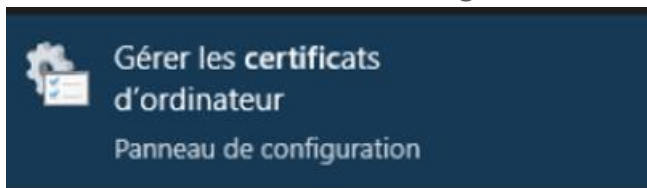
<

Vous devriez voir votre certificat affiché

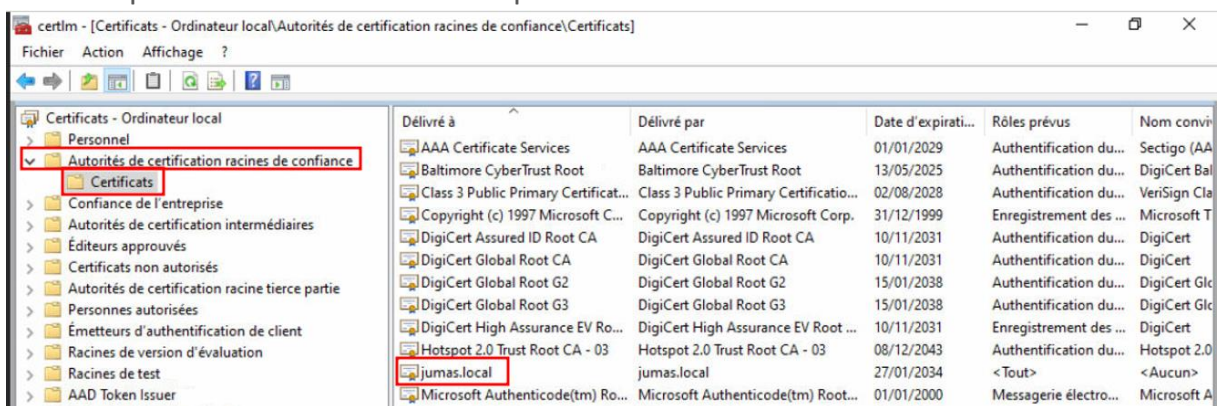
Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial	Statut
jumas.local	jumas.local	27/01/2034	<Tout>	<Aucun>	

Afin de s'assurer que la GPO est fonctionnelle, nous allons vérifier sur un ordinateur du domaine.

Rendez-vous dans la console de gestion des certificats



Vérifiez que votre certificat est bien présent



Si tel est le cas, alors la GPO est fonctionnelle.

**Fin de la procédure.**