Documentation Installation PKI

1. Configuration de la machine

1.1 Configuration Adresse IP / DNS

1. Nous allons commencer par attribuer une adresse IP à notre machine en créant le fichier de conf dans l’interfaces à l’aide de cette commande :

```
nano /etc/network/interfaces.d/<Nom de l'interface>.cfg
```

2. Mettre dans ce fichier ceci :

```
auto <Nom de l'interface>
iface <Nom de l'interface> inet static
    address <Adresse IP>
    gateway <passerelle par défaut>
    dns-nameservers <Adresse IP DNS 1>
    dns-nameservers <Adresse IP DNS 2>
```

3. Aller modifier le “resolv.conf” ce qui permet de configurer les DNS voici la commande :

```
nano /etc/resolv.conf
```

4. Supprimer tout le contenu de ce fichier et mettre ceci à la place

```
domain <Domaine>
search <Domaine>
nameserver <Adresse IP DNS 1>
nameserver <Adresse IP DNS 2>
```

5. Pour mettre à jour ces paramètres vous pouvez redémarrer le service réseau, voici la commande :

```
systemctl restart networking
```

1.2 Modification du nom de la machine

1. Le fichier à aller modifier pour modifier le nom de la machine est “hostname” voici la commande pour le modifier

```
nano /etc/hostname
```

2. Supprimer le contenu de ce fichier et y mettre le nom que vous voulez lui attribuer de cette façon :

```
<Nom de la machine>
```

3. Pour mettre à jour ces paramètres vous pouvez redémarrer votre machine avec la commande :

```
reboot
```

1.3 SSH

1.3.1 Création d’un utilisateur

1. La commande pour créer l’utilisateur “admin” est celle si :

```
adduser admin
```

2. Suite à cette commande vous devriez rentrer certaine information que vous pouvez laisser vide de cette façon juste lors du mot du passe vous vous devez d’en renseigner 1 :

```
root@nextcloud:~# adduser admin
Ajout de l'utilisateur « admin » ...
Ajout du nouveau groupe « admin » (1001) ...
Ajout du nouvel utilisateur « admin » (1001) avec le groupe
« admin » (1001) ...
Création du répertoire personnel « /home/admin » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour a
dmin
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la val
eur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]o
Ajout du nouvel utilisateur « admin » aux groupes supplémen
taires « users » ...
Ajout de l'utilisateur « admin » au groupe « users » ...
```

1.3.2 Installation / Configuration SSH

1. Nous allons commencer par installer le module SSH sur notre machine Linux à l'aide de cette commande :

```
apt update && apt upgrade && apt install ssh
```

2. Maintenant nous pouvons configurer le port par défaut du SSH pour cela nous pouvons aller modifier le fichier :

```
nano /etc/ssh/sshd_config
```

3. Vous pouvez modifier cette dans le fichier de cette façon :

```
#Port 22 -> Port <Port SSH>
```

4. Pour mettre à jour ces paramètres vous pouvez redémarrer le service SSH, voici la commande :

```
systemctl restart ssh
```

2. Configuration de la PKI

2.1 Installation / Configuration Initial PKI

1. Dans un premier nous allons installer le service de PKI nommer "easy-rsa" à l'aide de cette commande :

```
apt update && apt upgrade && apt install easy-rsa
```

2. Suite à l'installation nous allons créer le dossier qui nous permettra de configurer notre PKI de notre infrastructure à l'aide de cette commande

```
mkdir ~/easy-rsa
```

3. Suite à ça nous allons un line symbolique entre le dossier de Package Easy-RSA et notre dossier que nous venons de créer cela permettra qu'à chaque

mise à jour on est pas de fichier à modifié car ils seront directement modifier grâce au lien symbolique. Voici la commande pour cela :

```
ln -s /usr/share/easy-rsa/* ~/easy-rsa/
```

5. Ensuite nous pouvons nous déplacer dans noter dossier de config Easy-RSA pour commencer la configuration à l'aide de cette commande :

```
cd ~/easy-rsa
```

6. Cela nous permet d'initialiser ce dossier avec le système de Easy-RSA, voici la commande permettant ceci :

```
./easyrsa init-pki
```

7. Dans un premier temps nous allons supprimer qui peut créer des conflits, voici la commande qui permet de le supprimer :

```
rm pki/vars
```

8. Suite à ça nous allons modifier le fichier qui nous permettra d'avoir des paramètres par défaut pour nos futurs certificats, voici la commande :

```
nano vars
```

9. Dans ce fichier vous pouvez modifier ces lignes avec vos valeurs de cette façon

```
set_var EASYRSA_REQ_COUNTRY     "FR"
set_var EASYRSA_REQ_PROVINCE    "Mayenne"
set_var EASYRSA_REQ_CITY        "Laval"
set_var EASYRSA_REQ_ORG         "TYLO"
set_var EASYRSA_REQ_EMAIL       "yvosges@tylo.com"
set_var EASYRSA_REQ_OU          "IT"
```

10. Ensuite nous allons exécuter le script build-ca qui permet la création d'une autorité de certification et ensuite une paire de clé privée et clé public, voici la commande pour cela :

```
./easyrsa build-ca
```

11. Suite à la création du certificat sur la machine nous allons le copier dans le dossier certificats du système à l'aide de cette commande :

```
cp pki/ca.crt /usr/local/share/ca-certificates
```

12. Suite à la copie du fichier de certificat nous allons mettre à jour les certificats de la machine Linux, à l'aide de cette commande :

```
update-ca-certificates
```

2.2 Administration coté serveur WEB

Dans mon cas je suis sur un serveur Proxy qui centralise donc mes certificats HTTPS avec les autres serveur WEB étant en HTTP simple.

Donc dans mon cas je me rend sur mon serveur Proxy en tant que "root" pour effectuer toutes les modifications.

1. Dans un premier nous allons créer un dossier nommé "csr" qui nous permettra de stocker tout nos fichiers .csr ceci permet de ne pas mélanger les fichiers .csr avec les autres. Voici la commande pour ceci

```
mkdir /etc/ssl/csr
```

2. Ensuite nous allons créer nos clés privé (.key) et clé public (.csr) dans nos dossiers présent pour cela, voici les commandes pour cela :

```
openssl genrsa -out /etc/ssl/private/prv-site.key 2048

openssl req -new -key /etc/ssl/private/prv-site.key -out /e
tc/ssl/csr/csr-site.csr
```

3. Suite à la création de nos certificats nous pouvons copier notre clé public (.csr) sur notre serveur PKI, pour cela nous utilisons un système de SSH

donc vous vous devez de le configurer, voici la commande pour cela :

```
scp -P <Port SSH du serveur PKI> /etc/ssl/csr/csr-site.csr
<user>@<adresse IP>:/tmp/
```

2.3 Signature du Certificat

1. Suite à la copie de la clé privée sur le serveur PKI nous pouvons aller sur celui si et commencer la signature du certificat. Dans un premier nous allons nous redéplacer dans notre dossier “easy-rsa” à l’aide de cette commande :

```
cd ~/easy-rsa
```

2. Suite à ça nous allons importer dans notre dossier de configuration easy-rsa notre clé public .csr à l’aide de cette commande :

```
./easyrsa import-req /tmp/csr-site.csr crt-site
```

3. Ensuite nous pouvons vérifier dans le dossier reqs si cela à créer un fichier .reqs, suite à la commande vous pouvez voir un fichier au nom de “crt-site.reqs” cela est bon, voici la commande pour cela :

```
ls pki/reqs
```

4. Avant la création du fichier .crt nous allons ajouter une nouvelle variable d’environnement pour le paramètre Subject Alternative Name (SAN), voici la commande permettant cela :

```
export EASYRSA_EXTRA_EXTS="subjectAltName=DNS:<adresse DNS
de votre site WEB>"
```

5. Suite à l’ajout de la variable d’environnement nous pouvons ensuite signer le certificat à l’aide de cette commande :

```
./easyrsa sign-req server crt-site
```

6. Ensuite nous pouvons vérifier dans le dossier issued si cela à créer un fichier .crt, suite à la commande vous pouvez voir un fichier au nom de “crt-site.crt” cela est bon, voici la commande pour cela :

```
ls pki/issued
```

7. Suite à la signature du certificat par notre PKI nous pouvons ensuite le copier dans noter serveur WEB, pour moi mon serveur Proxy à l’aide de cette commande :

```
scp -P <Port SSH Serveur WEB ou Proxy> pki/issued/crt-site.
crt <user>@<addresse IP>:/tmp/
```

2.4 Configuration Certificat Coté Serveur WEB

1. Suite à la copie du fichier .crt sur le serveur Proxy nous pouvons retourner sur celui si pour terminer la configuration de se coter, dans un premier nous pouvons copier le fichier dans notre dossier “certs”, voici la commande pour cela :

```
cp /tmp/crt-site.crt /etc/ssl/certs/
```

2.4.1 Serveur Proxy / WEB Nginx

Si votre serveur Proxy ou votre serveur WEB est basée sur Nginx ceci vous concerne

1. Dans un premier temps vous pouvez aller modifier votre fichier “site.conf” à l’aide de cette commande :

```
nano /etc/nginx/sites-available/site.conf
```

2. Vous pouvez ajouter dans celui ces lignes qui permettront de relier votre fichier de configuration de votre page WEB à votre certificat signée :

```
ssl_certificate /etc/ssl/certs/crt-site.crt;
ssl_certificate_key /etc/ssl/private/prv-site.key;
```

3. Pour mettre à jour les changements dans voter fichier de configuration vous pouvez redémarrer votre service Nginx, voici la commande pour cela :

```
systemctl restart nginx
```

2.4.2 Serveur Proxy / WEB Apache2

Si votre serveur Proxy ou votre serveur WEB est basée sur Apache2 ceci vous concerne

1. Dans un premier temps vous pouvez aller modifier votre fichier “site.conf” à l’aide de cette commande :

```
nano /etc/apache2/sites-available/site.conf
```

2. Vous pouvez ajouter dans celui si ces lignes dans votre VirtualHost ce qui permettra à votre fichier de configuration d’identifier votre certificat signer

```
SSLCertificateFile /etc/ssl/certs/crt-site.crt
SSLCertificateKeyFile /etc/ssl/private/prv-site.key
```

3. Pour mettre à jour les changements dans voter fichier de configuration vous pouvez redémarrer votre service Apache2, voici la commande pour cela :

```
systemctl restart apache2
```

3. Configuration GPO Certificat

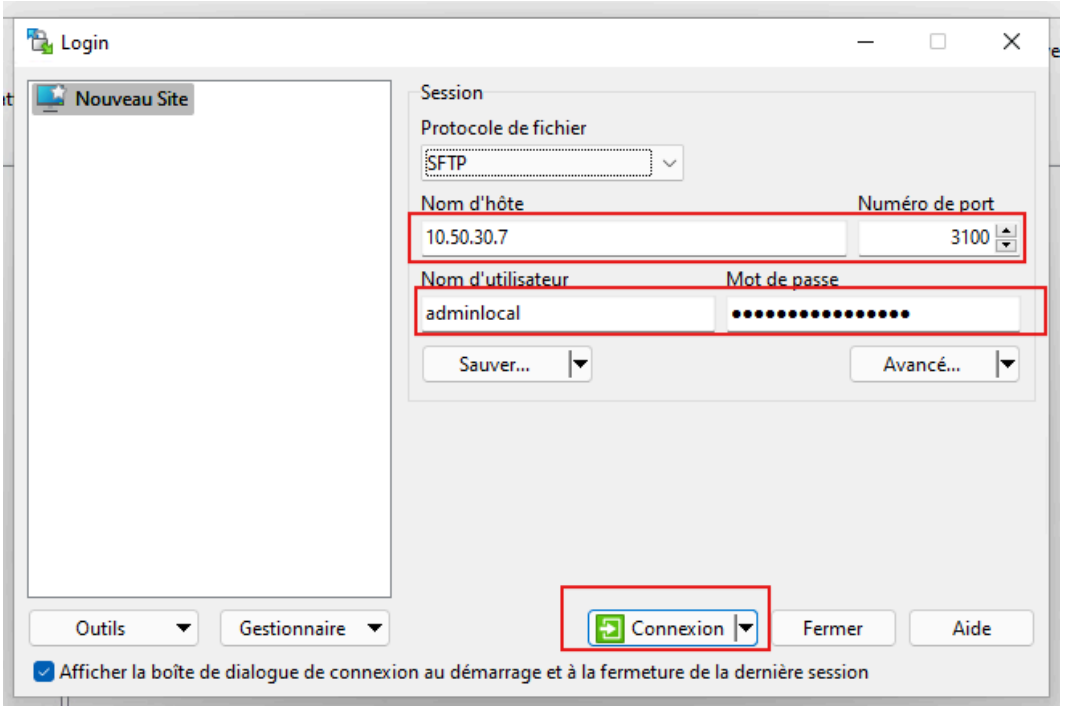
3.1 Récupération du ca.crt

Pour cette partie vous aurez besoin d'installer sur un poste Windows l'application WinSCP voici le lien vers celui si :

> WinSCP :: Official Site :: Download
> WinSCP is a free file manager for Windows supporting FTP, SFTP, S3 and WebDAV.
> https://winscp.net/eng/download.php

1. Donc suite à l'installation de ce logiciel sur votre poste vous pouvez vous connecter à votre machine Linux à distance de cette façon
   - Nom d'hôte : Adresse IP de votre serveur PKI
   - Numéro de port : Votre port SSH
   - Nom d'utilisateur : Votre utilisateur pour le SSH
   - Mot de passe : Mot de passe de l'utilisateur

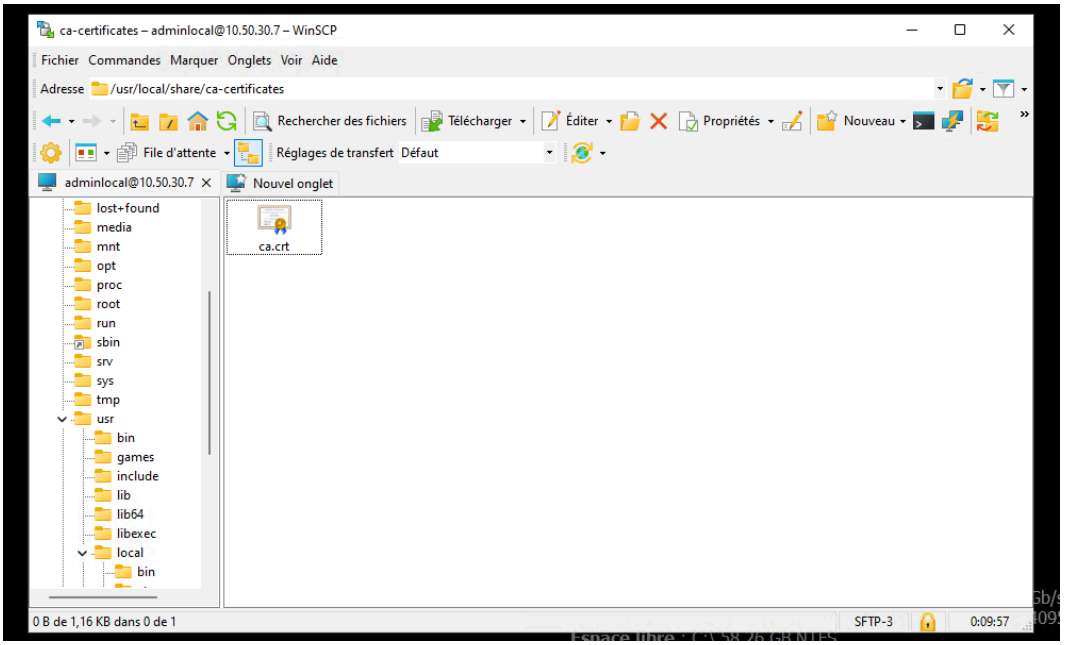
   Suite au renseignement vous pouvez cliquer sur "Connexion" de cette façon :



2. Suite à la connexion vous pouvez aller dans cette ordre dans les dossiers présent sur votre machine Linux :

   / <racine> → usr → local → share → ca-certificates

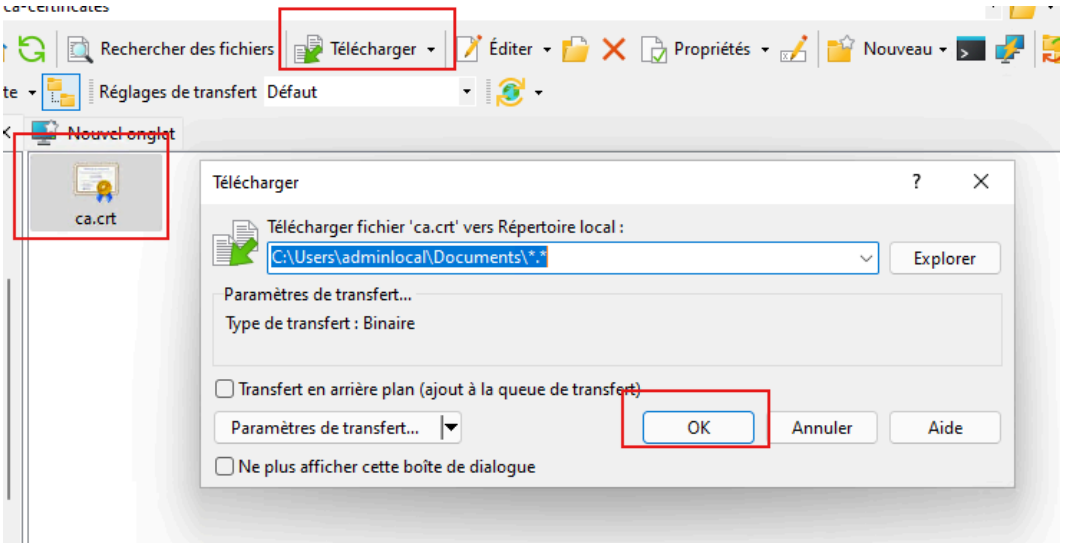
   Voici ce que vous devriez voir ensuite dans voter dossier “ca-certificates” :



3. Avant de télécharger le fichier vous pouvez aller sur votre serveur et modifier les droits du fichier “ca.crt” à l’aide de cette commande :

```
chmod 004 /usr/local/share/ca-certificates/ca.crt
```

4. Suite à ça vous pouvez retourner sur votre machine Windows et cliquer sur le fichier “ca.crt”, ensuite cliquer sur “Télécharger” et pour finir cliquer sur “OK” de cette façon :



5. Suite au téléchargement vous pouvez remettre les droits de base sur le fichier ca.crt sur la machine Linux, voici la commande permettant cela :

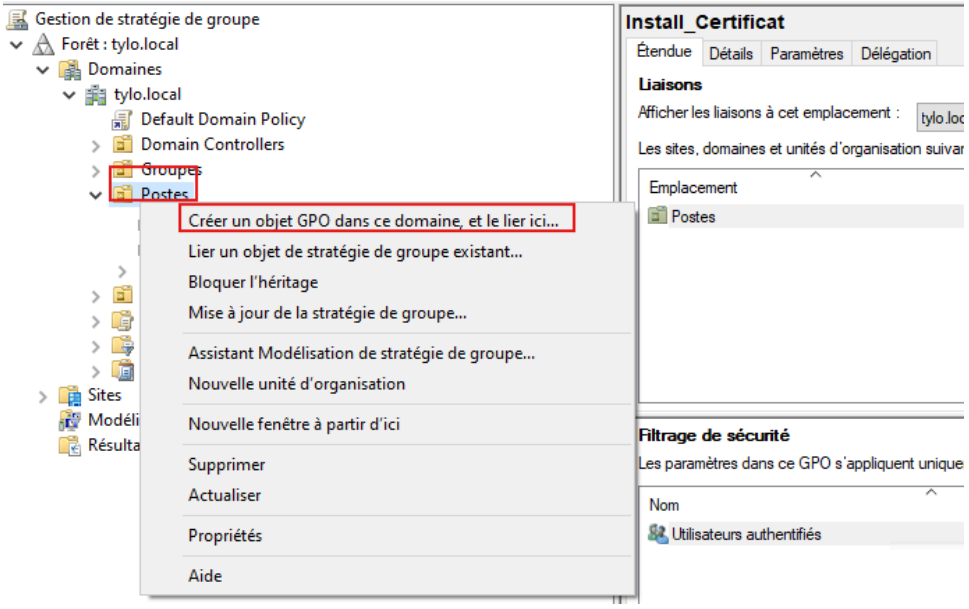
```
chmod 400 /usr/local/share/ca-certificates/ca.crt
```

3.2 Création de la GPO

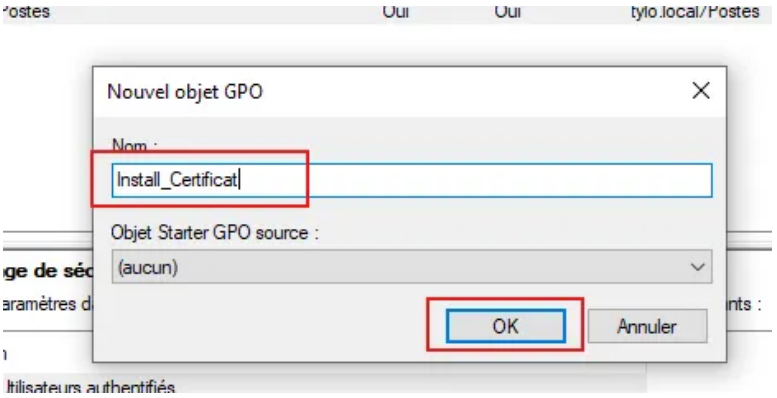
Suite à la récupération du fichier vous devez le positionner dans un dossier partagée accessible par le groupe “Ordinateurs du domaine” si cela n’est pas bon l’installation ne pourra pas s’effectuer car l’ordinateurs ne pourra pas accéder au dossier stockant le certificat.

Dans mon cas le fichier est stocké dans le dossier \\SRVFIL01\auto$\Certificat

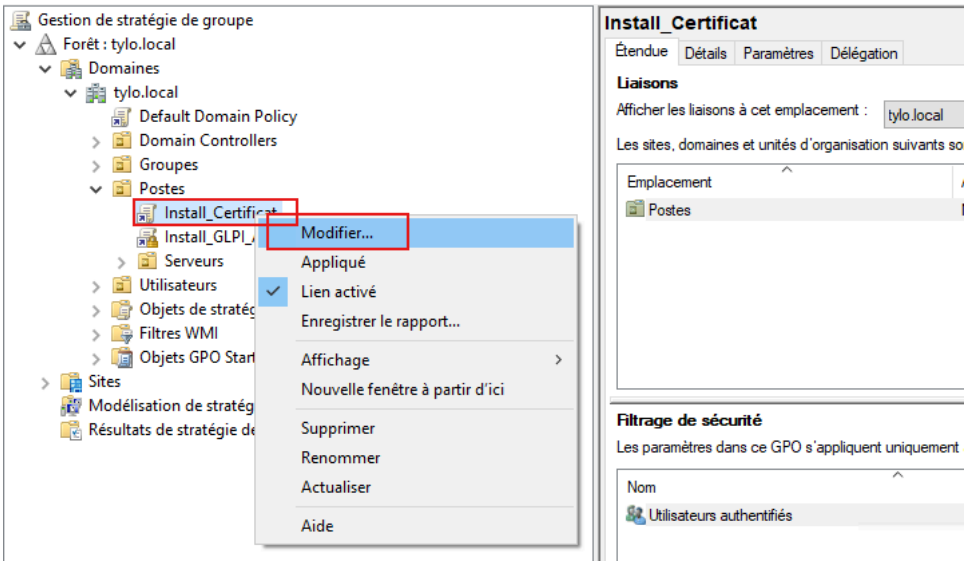
1. Vous pouvez vous rendre dans l’application nommé “Gestion des stratégies de groupe”, ensuite clique droit sur l’unité d’organisation qui contient vos postes du domaine, puis cliquer sur “Créer un objet GPO dans ce domaine, et lier ici...” de cette façon :



2. Donné un nom à la stratégie de groupe (essayé de donner un nom compréhensible et parlant) puis cliquer sur “OK” de cette façon :



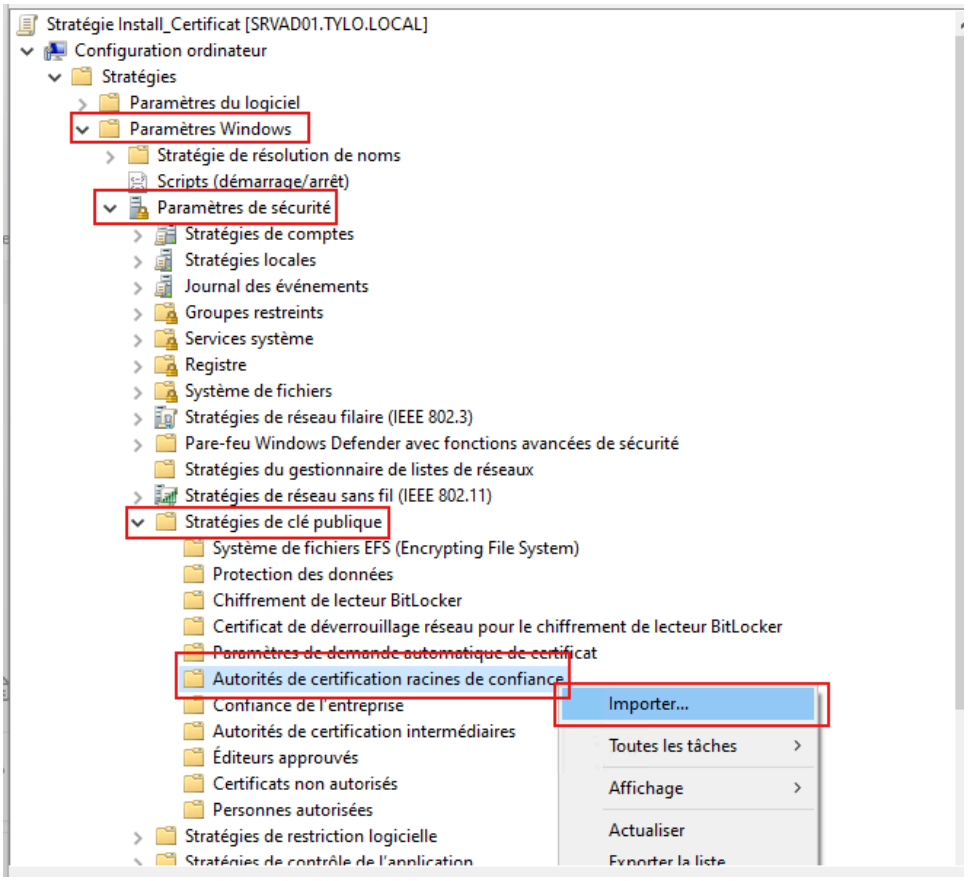
3. Suite à la création de notre règle nous allons commencer à l’administrer pour cela vous pouvez effectuer un clic droit sur votre règle puis cliquer sur “Modifier...” de cette façon :



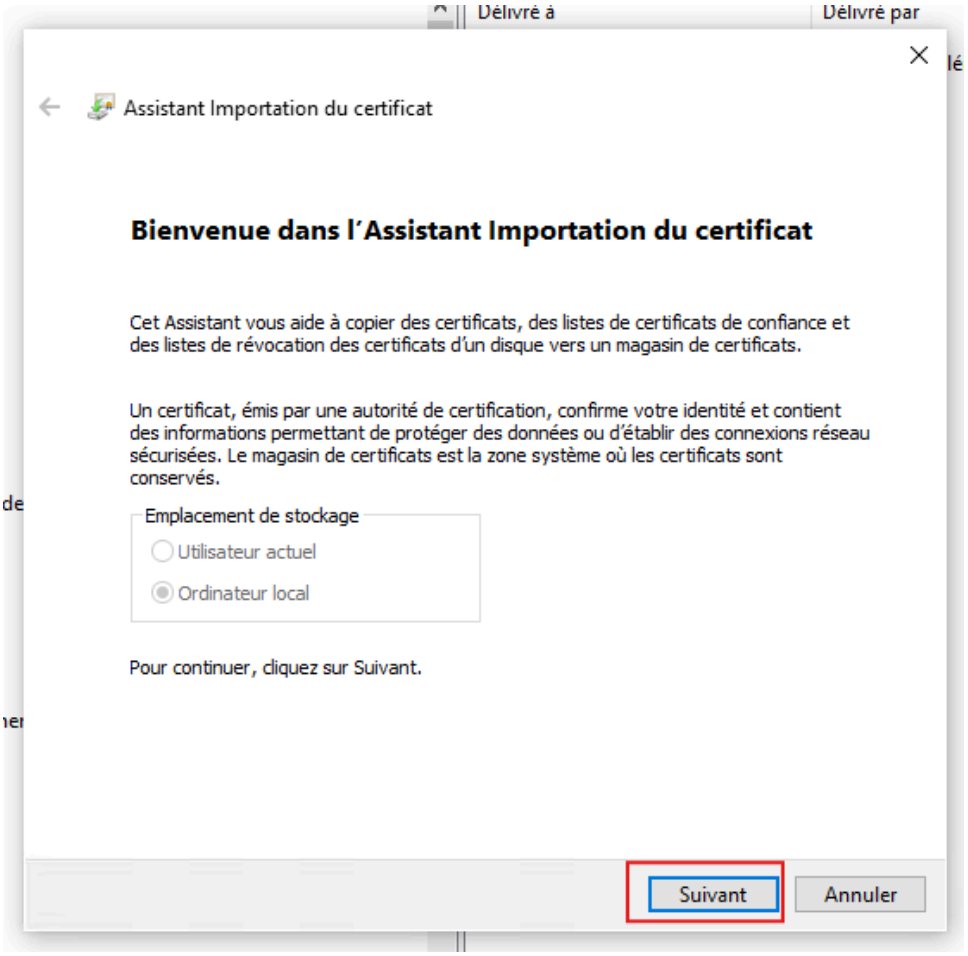
4. Suite à l'ouverture de la règle vous pouvez aller dans les dossiers :

   Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique

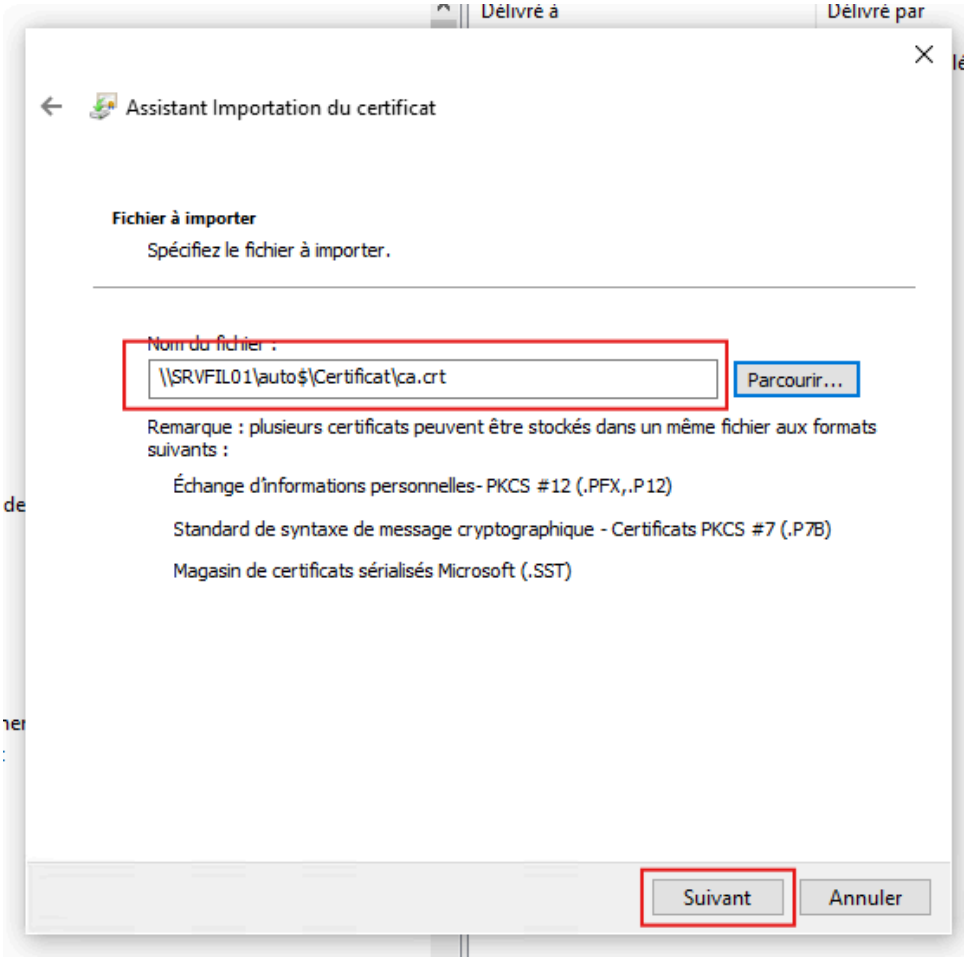
   Puis vous pouvez effectuer un clic droit sur le dossier "Autorités de certification racines de confiance" ensuite cliquer sur "Importer" de cette façon :



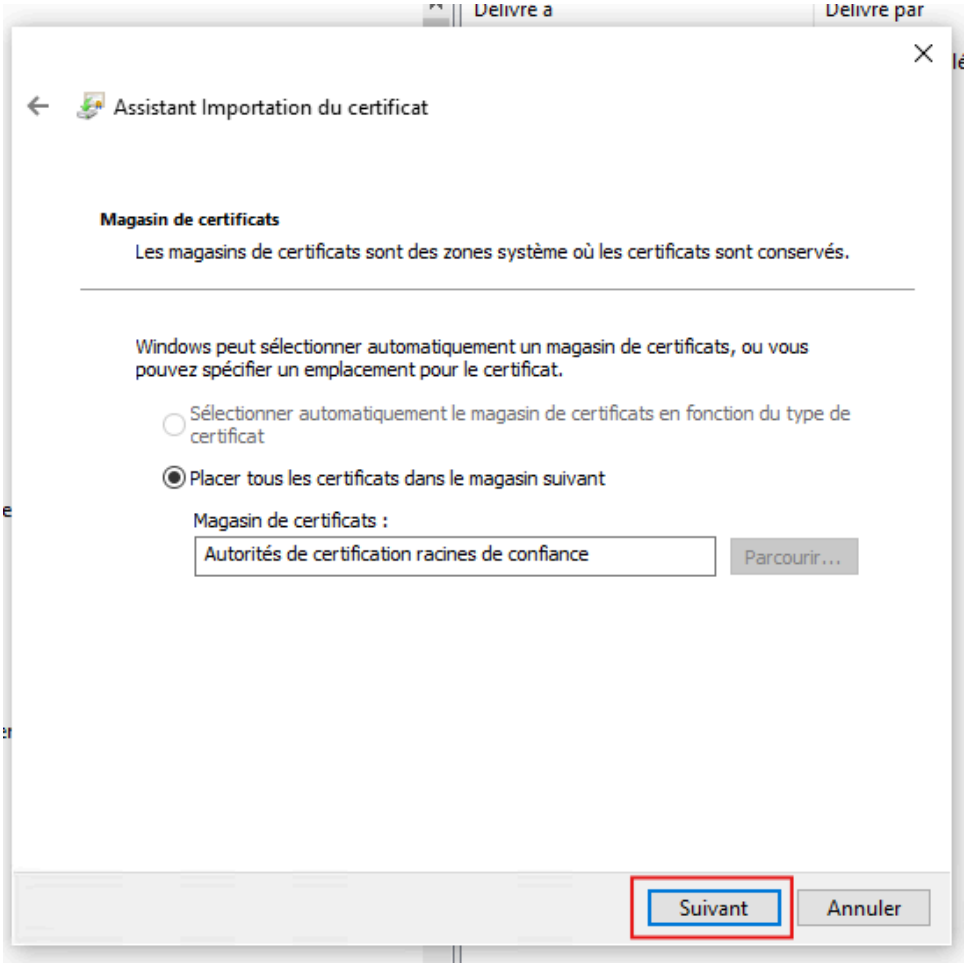
5. Dans un premier temps vous cliquer sur “Suivant” car dans ce cas de figure le certificat doit être installer sur l’ordinateur en local et non juste pour un utilisateur de cette façon :



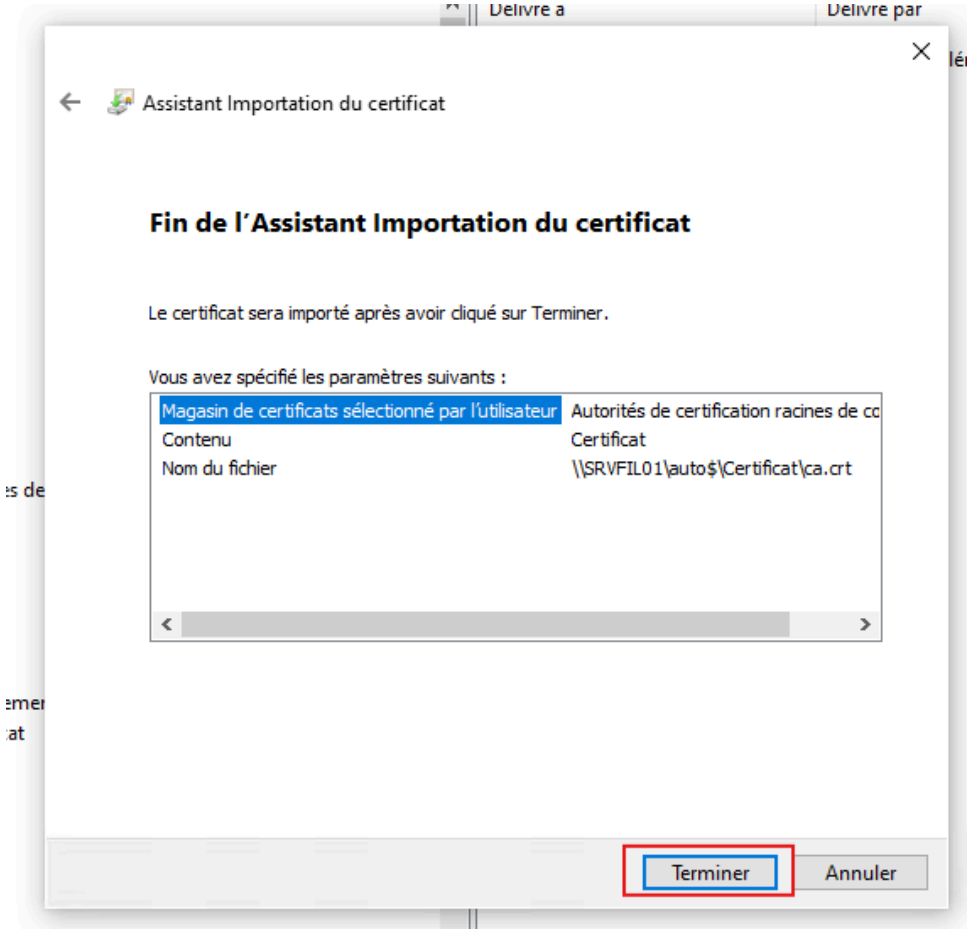
6. Ensuite vous pouvez rentrer le chemin réseau vers voter fichier “ca.crt” puis vous pouvez cliquer sur “Suivant” de cette façon :



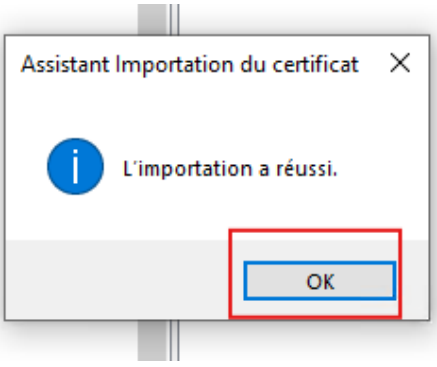
7. Dans notre cas de figure vous pouvez laisser par défaut ceci pour la prise en service du certificat que nous installons, donc vous pouvez directement cliquer sur “Suivant” de cette façon :



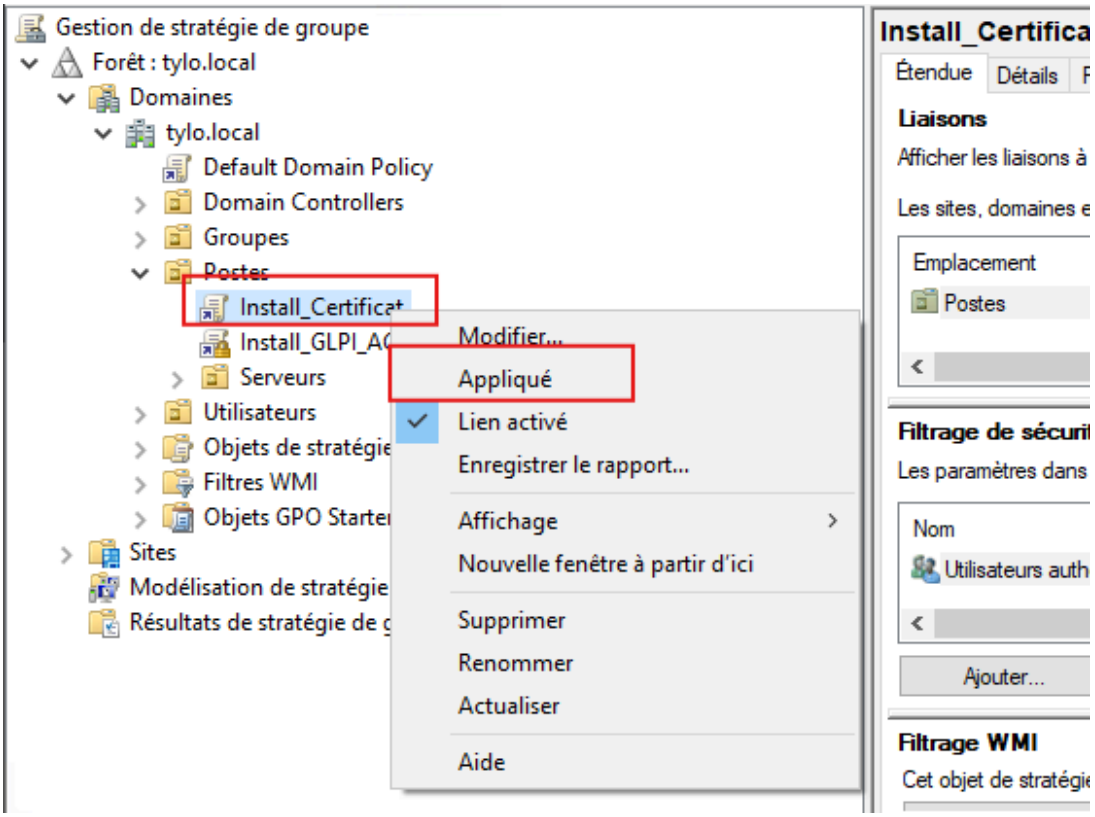
8. Suite à la configuration de l'importation du certificat nous pouvons la finaliser en cliquant sur "Terminer" sur cette page de cette façon :



9. Suite à finalisation de l'importation du certificat nous avons un petit temps de chargement puis nous pouvons voir le message d'importation réussi du certificat, vous pouvez cliquer sur "OK" sur cette pop-up puis vous pouvez fermer la page de modification de la règle ensuite.



10. Suite à la fermeture de la page de modification de la règle vous pouvez effectuer un clic doit sur votre règle, ensuite cliquer sur "Appliqué" pour permettre l'activation de votre règle de cette façon :


Gestion de stratégie de groupe
Forêt : tylo.local
Domaines
tylo.local
Default Domain Policy
Domain Controllers
Groupes
Postes
Install_Certificat
Install_GLPI_AG
Serveurs
Utilisateurs
Objets de stratégie
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie
Résultats de stratégie de g
Modifier...
Appliqué
Lien activé
Enregistrer le rapport...
Affichage
Nouvelle fenêtre à partir d'ici
Supprimer
Renommer
Actualiser
Aide
Install_Certifica
Étendue
Détails
Liaisons
Afficher les liaisons à
Les sites, domaines e
Emplacement
Postes
Filtrage de sécuri
Les paramètres dans
Nom
Utilisateurs auth
Ajouter...
Filtrage WMI
Cet objet de stratégie