

Proxy d'application : générer et utiliser un certificat wildcard *.domaine.fr avec Let's Encrypt

Présentation

La publication d'une application locale utilise par défaut le nom de domaine **.msapproxy.net**.

L'utilisation d'un nom de domaine personnalisé à la place du nom de domaine **.msapproxy.net** nécessite les démarches suivantes :

- Activer un domaine personnalisé dans Azure
- Configurer un CNAME dans le DNS du domaine personnalisé vers l'URL d'Azure Application Proxy. Par exemple :
 - app.mondomaine.fr → app-mondomainefr.msapproxy.net
- Téléverser dans Azure un certificat SSL correspondant au domaine personnalisé avec les caractéristiques suivantes:
 - Être un PFX
 - Contenir la clé privée
 - Avoir pour CN et SAN *.mondomaine.fr (wildcard)

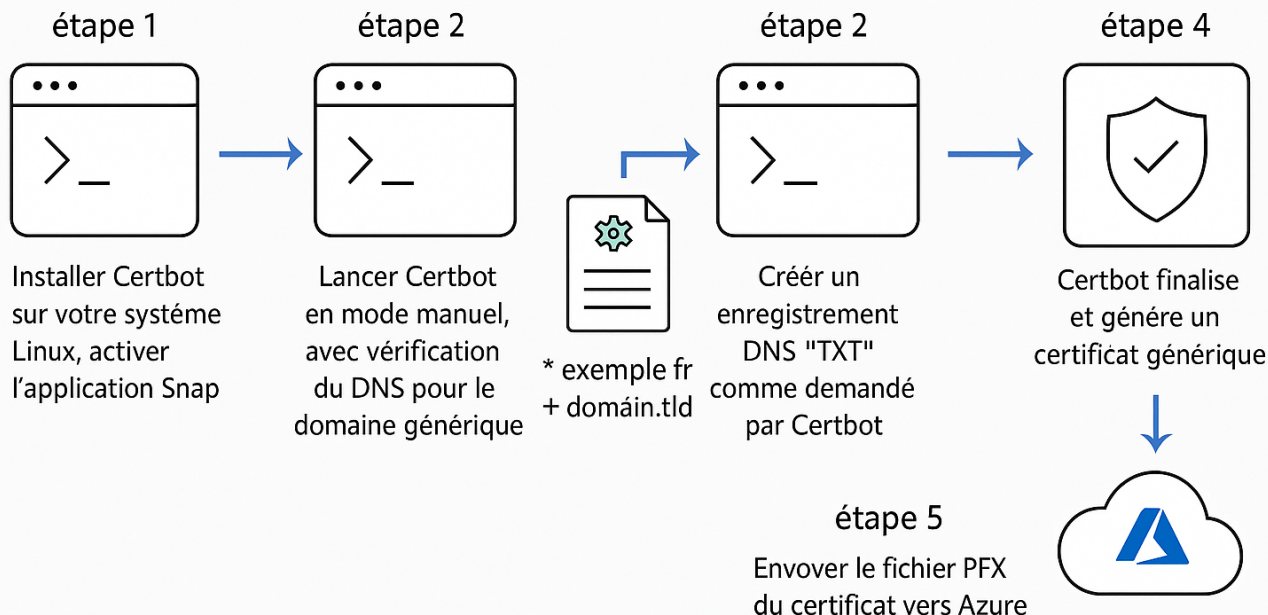
Les SAN sont obligatoires pour Chrome/Edge (sinon NET::ERRCERTCOMMONNAMEINVALID)

Si tout est bien configuré, Azure gère correctement HTTPS et le navigateur verra un certificat :

- CN = app.mondomaine.fr
- Délivré par l'Autorité de certification du domaine personnalisé

Obtenir un certificat générique avec Let's Encrypt

Pour le domaine et l'ensemble des sous-domaines (*.exemple.fr)



Attention Let's Encrypt ne permet les certificats wildcard que via validation DNS, jamais par validation HTTP.

Installer Certbot

- Installer Python3 + venv + pip

```
apt update && apt upgrade -y  
apt install python3 python3-pip python3-venv
```

- Créer un environnement Certbot

```
python3 -m venv /opt/certbot/
```

- activer l'env (optionnel)

```
# activation (optionnel)  
source /opt/certbot/bin/activate
```

- Installer Certbot dans l'env

```
/opt/certbot/bin/pip install --upgrade pip  
/opt/certbot/bin/pip install certbot certbot-dns-cloudflare
```

- Créer un lien pour l'utiliser directement :

```
ln -s /opt/certbot/bin/certbot /usr/bin/certbot
```

Lancer Certbot en mode DNS automatique (wildcard)

Fonctionnement :

Certbot communique directement avec Cloudflare

- crée le TXT automatiquement
- attend validation
- supprime le TXT

Utiliser Cloudflare

- Créer un token API Cloudflare
- Créer fichier credentials ./secrets/cloudflare.ini

```
dns_cloudflare_api_token = TOKEN
```

- sécuriser le fichier

```
chmod 600 ./secrets/cloudflare.ini
```

Lancer certbot

```
certbot certonly \  
--dns-cloudflare \  
--dns-cloudflare-credentials ~/.secrets/cloudflare.ini \  
-d "*.educ-valadon-limoges.fr" \  
-d educ-valadon-limoges.fr
```

```
certbot certonly --manual --preferred-challenges=dns -d *.educ-valadon-limoges.fr -d educ-valadon-limoges.fr
```

- Certbot affiche la chaîne TXT à placer dans votre DNS. Exemple :

```
Créer un enregistrement :  
Nom : _acme-challenge.domaine.fr  
Valeur : D7Jks829skd1lQWmy9fJsd9S3Xke
```

Ajouter l'enregistrement DNS TXT

- Dans votre gestionnaire DNS :

Type	Nom	Valeur
TXT	_acme-challenge.domaine.fr	clé fournie par Certbot

- Attendre 1 à 2 minutes (ou plus selon votre hébergeur DNS)

Ensuite, retournez dans le terminal et validez.

Récupérer les fichiers générés

- Certbot génère les certificats dans `/etc/letsencrypt/live/domaine.fr/` :

Fichier	Rôle
fullchain.pem	Certificat complet (inclut autorités intermédiaires)
privkey.pem	Clé privée
cert.pem	Certificat individuel

Convertir les fichiers en PFX pour Azure

Azure exige un fichier PFX avec certificat + clé privée.

```
openssl pkcs12 -export \  
-out wildcard-domaine-fr.pfx \  
-inkey /etc/letsencrypt/live/domaine.fr/privkey.pem \  
-in /etc/letsencrypt/live/domaine.fr/fullchain.pem \  
-password pass:VotreMotDePassePFX` `
```

- Gardez le mot de passe : Azure vous le demandera.

Importer le certificat dans Azure Application Proxy

- Se connecter au Azure Portal
- Allez dans Entra ID → Application d'entreprise
- Sélectionnez votre application publiée
- Accéder à la rubrique Proxy d'application
- Cliquer sur le lien de téléchargement du certificat
 - Téléversez wildcard-domaine-fr.pfx
 - Entrez le mot de passe PFX
- Enregistrez

Azure utilise maintenant votre wildcard pour ce domaine.

Vérifier

Dans le navigateur accédez à <https://app.domaine.fr>

Vous devez voir :

- Icône de connexion sécurisée
- Certificat émis pour : *.domaine.fr
- Aucune alerte "site non sécurisé"

Configurer le renouvellement automatique du certificat

Le certificat est valide 4 mois.

From:
/ - **Les cours du BTS SIO**

Permanent link:
</doku.php/reseau/cloud/azure/syncroazure/certificat?rev=1778406105>

Last update: **2026/05/10 11:41**

