

Installation et configuration de certificats SSL avec OpenSSL

Etape 1 : Créer un dossier qui va contenir le fichier de config de OpenSSL et les clés pour le certificat

```
root@debian:~# mkdir openssl.cnf/
```

Etape 2 : Créer le fichier de config OpenSSL qui contiendra les paramètres du certificat

```
root@debian:~# nano openssl.cnf
```

Etape 3 : Mettre ces paramètres dans le fichier openssl.cnf

```
[req]
default_bits      = 2048
distinguished_name = req_distinguished_name
x509_extensions   = v3_req
prompt            = no

[req_distinguished_name]
CN = ssl.test

[v3_req]
subjectAltName = @alt_names
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[alt_names]
IP.1 = 
DNS.1 = ssl.test
```

Etape 4 : Générer une clé server.key RSA2048 pour le serveur et une clé de demande de signature de certificat (CSR)

```
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr -config openssl.cnf
```

Le -config openssl.cnf dans la commande c'est pour préciser d'utiliser le fichier openssl.cnf pour la configuration de la clé lors de sa création.

Etape 5 : Générer le nouveau certificat auto-signé

```
openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt -extfile openssl.cnf -extensions v3_req
```

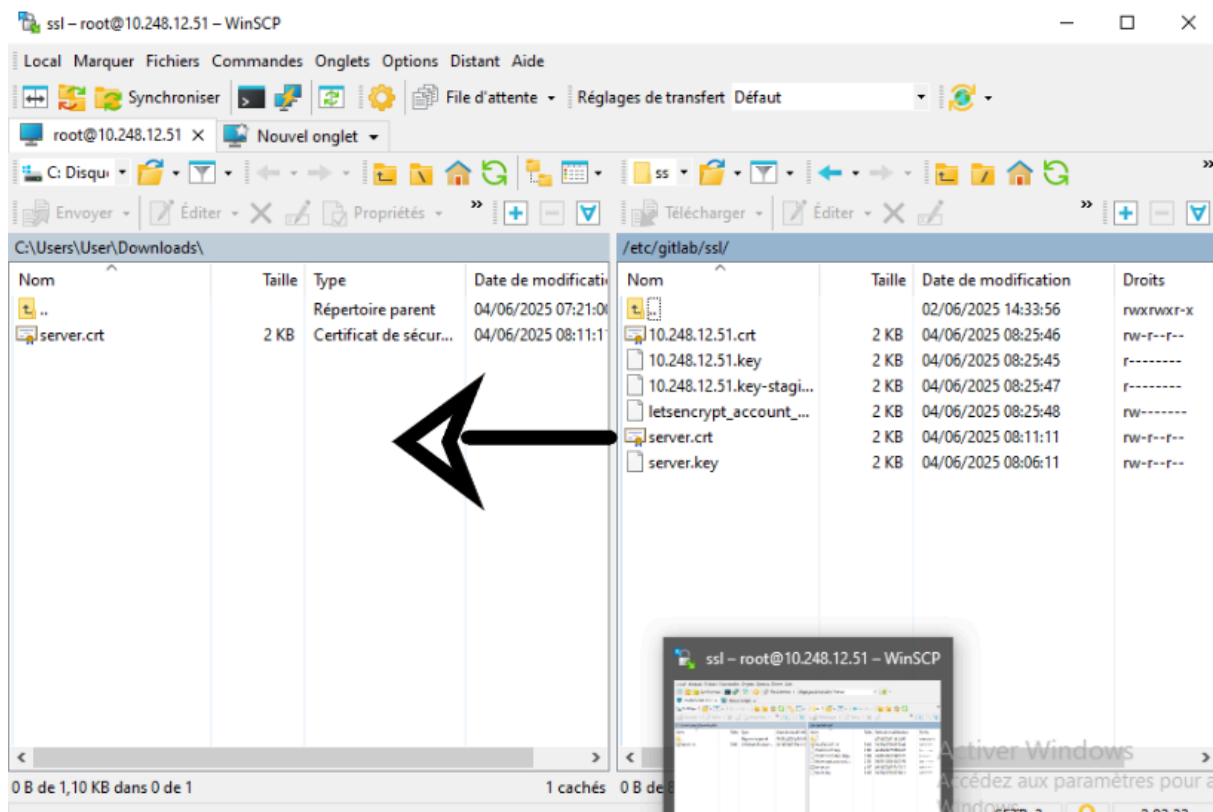
Etape 6 : Configurer le serveur avec notre certificat en mettant le fichier [server.key](#) et [server.crt](#) dans le dossier `/etc/gitlab/ssl/`

```
mv server.key /etc/gitlab/ssl/ mv server.crt /etc/gitlab/ssl/
```

Etape 7 : Redémarrer le serveur GitLab

```
gitlab-ctl reconfigure
```

Etape 8 : Importer le certificat `server.crt` sur le client W10



Etape 9 : Mettre le certificat dans autorité de certifications racines de confiances

Installer le certificat

Cocher Ordinateur Local

Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Emplacement de stockage

- ☐ Utilisateur actuel
☒ Ordinateur local

Cliquez sur Suivant pour continuer.

 Suivant

Annuler

Cocher "Placer tous les certificats dans le magasin suivant :" et sélectionner Autorité de certification racine de confiance

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 :

Autorités de certification racines de confiance

Parcourir...

Suivant

Annuler

Appuyer 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 co
Contenu	Certificat
< >	

Terminer

Annuler

On retrouve le certificat dans la liste

Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...
SRCI SA Certification Authority 2...	SRCI SA Root Certification Authority
SRCI SA Root Certification Autho...	SRCI SA Root Certification Authority
ssl.test	ssl.test
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...
Starfield Services Root Certificat...	Starfield Services Root Certificate A...