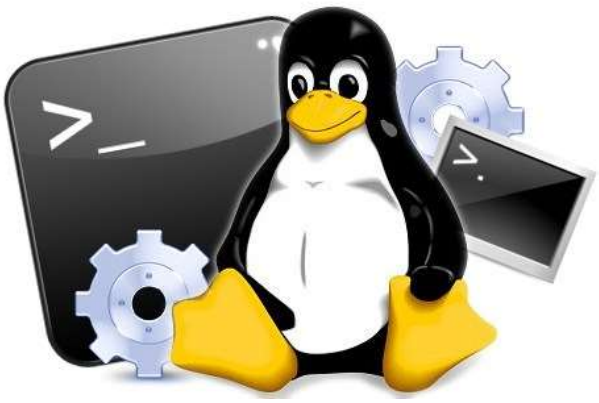
Documentation d'installation

Installation autorité de certification



18/03/2018

Yohan Fresneau

Sommaire

1. Prérequis 3
2. Qu'est-ce qu'un certificat 3
3. Installation autorité de certification 3
4. Configuration de apache2 4
5. Ajout du certificat sur le navigateur 5
6. Vérification du fonctionnement du certificat 6

1. Prérequis

Nous devons avoir une machine Linux, avec une IP fixe et un nom de machine qui permet de l'identifier facilement, ainsi que son réseau fonctionnel.

2. Qu'est-ce qu'un certificat

Une autorité de certification est une tierce de confiance, qui nous permet de certifier que c'est bien cette machine qui à créer le certificat, à quel serveur il est destiné et à quel site. Un certificat est un moyen d'identifier un serveur et permet de chiffrer les échanges. Cela est très utile, car cela permet de rajouter une sécurité, car le certificat nous permet de certifier que nous somme bien sur le bon site et non un site pirate.

3. Installation autorité de certification

Pour créer nos clés et notre certificat, nous devons effectuer ces commandes

```
cd /etc/ssl/
mkdir clés
cd clés
openssl genrsa -out clefreshome.key { taille clé défaut : 2048 }
openssl req -new -x509 -days 365 -key clefreshome.key -out freshomecertgen.crt
```

Country Name (2 letter code) [AU]: ***FR***

State or Province Name (full name) [Some-State]: ***Centre-val-de-loire***

Locality Name (eg, city) []: ***Tours***

Organization Name (eg, company) [Internet Widgits Pty Ltd]: ***Lycée Paul Louis Courier***

Organizational Unit Name (eg, section) []: ***BTS SIO***

Common Name (e.g. server FQDN or YOUR name) []: ***ca.freshome.lan***

Email Address []: ***yohan.fresneau@outlook.fr***

Informations à saisir lors de la commande

```
openssl genrsa -out cletestlogin.key { taille clé défaut : 2048 }
openssl req -new -key cletestlogin.key -out testlogin.csr
```

Country Name (2 letter code) [AU]: ***FR***

State or Province Name (full name) [Some-State]: ***Centre-val-de-loire***

Locality Name (eg, city) []: ***Tours***

Organization Name (eg, company) [Internet Widgits Pty Ltd]: ***Lycée Paul Louis Courier***

Organizational Unit Name (eg, section) []: ***BTS SIO***

Common Name (e.g. server FQDN or YOUR name) []: ***testlogin.freshome.lan***

Email Address []: ***yohan.fresneau@outlook.fr***

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: ***Toor01***

An optional company name []:

Informations à saisir lors de la commande

```
openssl x509 -req -in testlogin.csr -out testlogin.crt -CA freshomecertgen.crt -CAkey clefreshome.key -CAcreateserial -CAserial ca.srl
```

Une fois cette commande effectuée, un message nous informe que l'on est bien signé.

4. Configuration de apache2

Nous allons activer le module qui nous permet de passer notre site en mode SSL

```
a2enmod ssl
```

*Permet d'activer le module "**SSL**"*

Nous allons maintenant activer le site SSL

```
a2ensite default-ssl
```

*Permet d'activer notre site "**SSL**"*

Nous allons spécifier notre certificat et notre clé privé

```
nano /etc/apache2/sites-available/default-ssl.conf
```

ServerName testlogin.freshome.lan

SSLCertificateFile /certificats/testlogin.crt

SSLCertificateKeyFile /certificats/cletestlogin.key

*Fichier modifié "**/etc/apache2/sites-available/default-ssl.conf**"*

Nous allons rediriger le flux non sécurisé du port 80 vers 443

```
nano /etc/apache2/sites-available/000-default.conf
```

ServerName testlogin.freshome.lan

Redirect / https://testlogin.freshome.lan/

*Fichier modifié "**/etc/apache2/sites-available/000-default.conf**"*

Nous devons redémarrer le serveur afin d'appliquer les modifications

```
/etc/init.d/apache2 restart
```

Nous allons créer ces dossiers sur les deux serveurs web

```
mkdir /certificats/
chmod 777 /certificats/
```

Permet de créer le dossier et mettre les permissions de lecture et d'écriture à tout le monde

Nous allons maintenant mettre nos clés et certificats sur nos serveurs web. Nous allons les déplacer grâce au SSH.

```
scp testlogin.crt administrateur@testlogin1.freshome.lan:/certificats/
scp testlogin.crt administrateur@testlogin2.freshome.lan:/certificats/
scp cletestlogin.key administrateur@testlogin1.freshome.lan:/certificats/
scp cletestlogin.key administrateur@testlogin2.freshome.lan:/certificats/
```

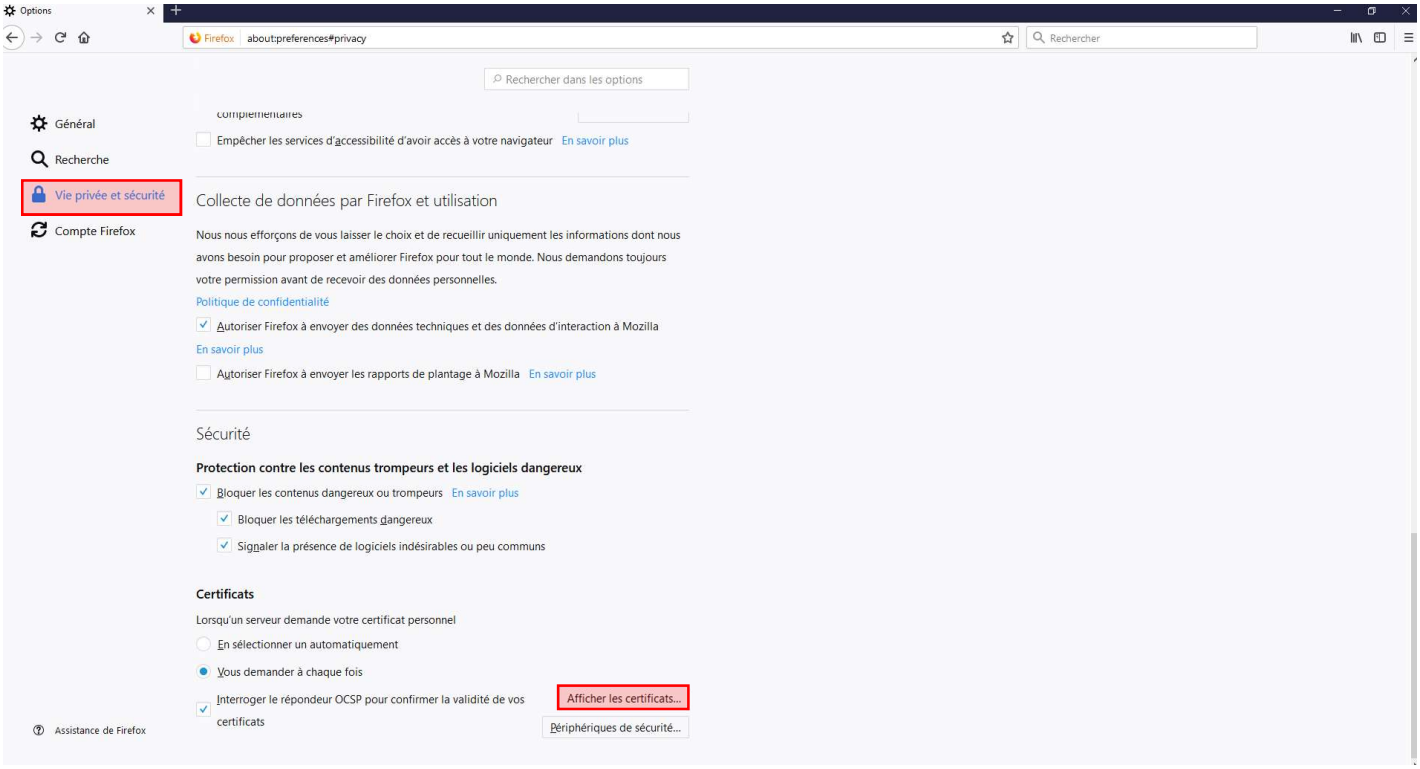
Permet d'envoyer depuis le serveur de certification les certificats vers notre serveur web

5. Ajout du certificat sur le navigateur

Pour récupérer le certificat, nous pouvons utiliser "**Filezilla**" client ou "**WinSCP**".

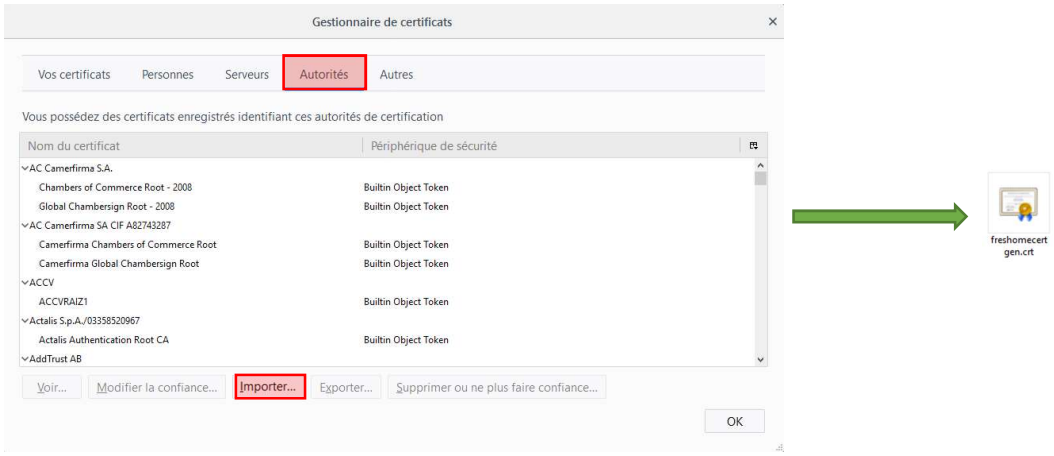
Nous devons prendre le fichier portant le nom : **freshomecertgen.crt**

Ce fichier se trouve dans : **/etc/ssl/clés/**



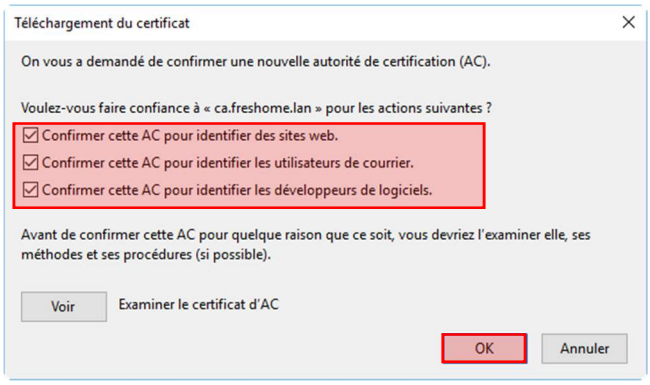
*Nous devons nous rendre dans les options de Firefox, puis "**Vie privée et sécurité**" et pour finir "**Afficher les certificats**"*

Nous allons importer notre certificat de confiance dans le navigateur



*Pour ajouter le certificat, on doit aller dans "**Autorités**", puis "**Importer**" et on choisit notre fichier "**freshomecrtgen.crt**"*

On confirme l'ajout du certificat



*On coche toutes les cases, puis on clique sur "**Ok**" afin d'ajouter le certificat*

6. Vérification du fonctionnement du certificat

Lorsque l'on se rend sur le site https://testlogin.freshome.lan/, nous avons une redirection transportant vers le port 443 et nous avons bien le SSL active indentifiable au cadenas vert.

Notre certificat n'est pas valide ou non ajouté, si nous avons ce message