Procédure : HTTPS

Dans ce tutoriel, je vais vous expliquer comment créer et gérer plusieurs site web avec un serveur Apache.

Dans ce tuto je vais travailler avec une machine virtuelle (VM) Debian 8.

Pour installer une VM je vous invite à consulter la procédure correspondante à l'adresse suivante : http://jerome.rouget.org/documents/installation_vm.pdf

Bon maintenant que nos machines virtuelles sont installées, installons nos serveurs !

Table des matières

Avant de commencer il faut savoir quel est votre enregistrement DNS, pour cela il faut lire le fichier des enregistrements de votre zone, que j'ai appelé `db.robotech.local`
Celui qui m'intéresse est www.robotech.local.

```
root@procedure-dns:/# more /etc/bind/db.robotech.local
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                        2016041203      ; Serial
                         60             ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@                       IN      NS      localhost.
procedure-dns.          IN      NS      192.168.130.161
www.robotech.local.     IN      A       192.168.130.162
root@procedure-dns:/#
```

Ce qu'on veut c'est accéder à www.robotech.local en HTTPS sans protestation du navigateur.
Pour cela, nous allons créer un dossier nommé SSL à la racine et suivre les étapes :

```
root@procedure-web:/# mkdir ssl ; cd ssl
root@procedure-web:/ssl#
```

Etape 1 : Créer la clé privée de l'autorité de certification (cleprivee.key)

```
openssl genrsa -des3 -out cleprivee.key 2048
```

```
root@procedure-web:/ssl# openssl genrsa -des3 -out cleprivee.key 2048
Generating RSA private key, 2048 bit long modulus
.+++
.....................................................................
.................................+++
e is 65537 (0x10001)
Enter pass phrase for cleprivee.key:
Verifying - Enter pass phrase for cleprivee.key:
```

Entrer un mot de passe, puis vérifiez-le.

Etape 2 : Créer le certificat correspondant à cette autorité de certification (CA.crt)

```
openssl req -new -x509 -days 365 -key cleprivee.key -out CA.crt
```

```
root@procedure-web:/ssl# openssl req -new -x509 -days 365 -key cleprivee.key -out CA.crt
Enter pass phrase for cleprivee.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:SGBD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bureau des certificats
Organizational Unit Name (eg, section) []:internet
Common Name (e.g. server FQDN or YOUR name) []:www.robotech.local
Email Address []:root@localhost
root@procedure-web:/ssl#
```

Ici on vous demande plusieurs informations, vous pouvez mettre la même chose que moi, elles ne sont pas réellement importantes, **SAUF** une **TRES IMPORTANTE** : `Common Name (e.g. server FQDN or YOUR name) []` : ici vous devez mettre la ligne que nous avons vérifiée dans le fichier `db.robotech.local`.

Etape 3 : Créer une clé privée pour le site web (webkey.key)

```
openssl genrsa -des3 -out webkey.key 2048
```

```
root@procedure-web:/ssl# openssl genrsa -des3 -out webkey.key 2048
Generating RSA private key, 2048 bit long modulus
.....................+++
.....................................................+++
e is 65537 (0x10001)
Enter pass phrase for webkey.key:
Verifying - Enter pass phrase for webkey.key:
root@procedure-web:/ssl#
```

Entrer un mot de passe, puis vérifiez-le.

Etape 4 : Créer une demande de signature (Certificate Signed Request)

```
root@procedure-web:/ssl# openssl req -new -key webkey.key -out webcsr.csr
Enter pass phrase for webkey.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:Austria
Locality Name (eg, city) []:Zloveck
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Grand chef
Organizational Unit Name (eg, section) []:Verif
Common Name (e.g. server FQDN or YOUR name) []:www.robotech.local
Email Address []:webmaster@localhost

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@procedure-web:/ssl#
```

Entrez le mot de passe que vous avez entrez pour la clé web (webkey.key). Puis même chose qu'à l'étape 2 il faut absolument respecter la ligne « `Common Name (e.g. server FQDN or YOUR name) [] :` ».

Etape 5 : Faire signer la demande par l'autorité de certification (webcertif.crt)

`openssl x509 -req -in webcsr.csr -out webcertif.crt –sha256 -CA CA.crt -CAkey cleprivee.key -CAcreateserial -days 365`

***[EDIT** : j'ai remplacé le **sha1** par **sha256** pour augmenter la sécurité, cela permettra que dans l'url https:// apparaitra en vert, et non pas comme ceci : ~~https://~~]*

```
root@procedure-web:/ssl# openssl x509 -req -in webcsr.csr -out webcertif.crt -sha1 -CA CA.crt
-CAkey cleprivee.key -CAcreateserial -days 365
Signature ok
subject=/C=AU/ST=Austria/L=Zloveck/O=Grand chef/OU=Verif/CN=www.robotech.local/emailAddress=we
bmaster@localhost
Getting CA Private Key
Enter pass phrase for cleprivee.key:
root@procedure-web:/ssl#
```

Entrez juste une passphrase.

Etape 6 : Vérification des fichiers en notre possession.

```
root@procedure-web:/ssl# ls -la
total 32
drwxr-xr-x  2 root root 4096 avril 14 15:44 .
drwxr-xr-x 23 root root 4096 avril 14 15:35 ..
-rw-r--r--  1 root root 1468 avril 14 15:39 CA.crt
-rw-r--r--  1 root root   17 avril 14 15:44 CA.srl
-rw-r--r--  1 root root 1743 avril 14 15:37 cleprivee.key
-rw-r--r--  1 root root 1342 avril 14 15:44 webcertif.crt
-rw-r--r--  1 root root 1070 avril 14 15:42 webcsr.csr
-rw-r--r--  1 root root 1751 avril 14 15:40 webkey.key
root@procedure-web:/ssl#
```

Si vous avez bien respecté les étapes jusqu'ici, vous devriez avoir dans votre dossier ssl ces fichiers suivants.

Etape 7 : Copie des fichiers dans les bons répertoires et changement des droits.

Nous allons copié la clé web et le certificat web dans les répertoires qui nous servirons plus tard pour le fichier de configuration d'Apache.

```
cp webkey.key /etc/ssl/private/

cp webcertif.crt /etc/ssl/certs/
```

```
root@procedure-web:/ssl# cp webkey.key /etc/ssl/private/
root@procedure-web:/ssl# cp webcertif.crt /etc/ssl/certs/
```

Puis nous modifions les droits pour que ceux-ci soit lisibles.

```
chmod 640 /etc/ssl/private/webkey.key

chgrp ssl-cert /etc/ssl/private/webkey.key
```

```
root@procedure-web:/ssl# chmod 640 /etc/ssl/private/webkey.key
root@procedure-web:/ssl# chgrp ssl-cert /etc/ssl/private/webkey.key
```

Etape 8 : Le fichier CA.crt doit être importé dans le navigateur.

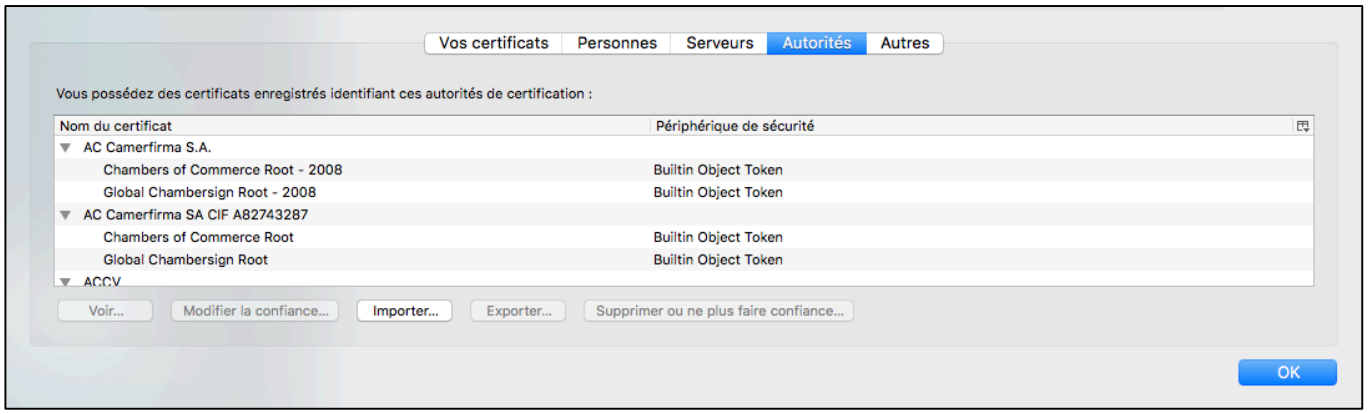
Comme je suis sur Mac, j'ai copié le fichier CA.crt avec la commande « scp », des logiciels sous Windows existent pour effectuer la même chose.

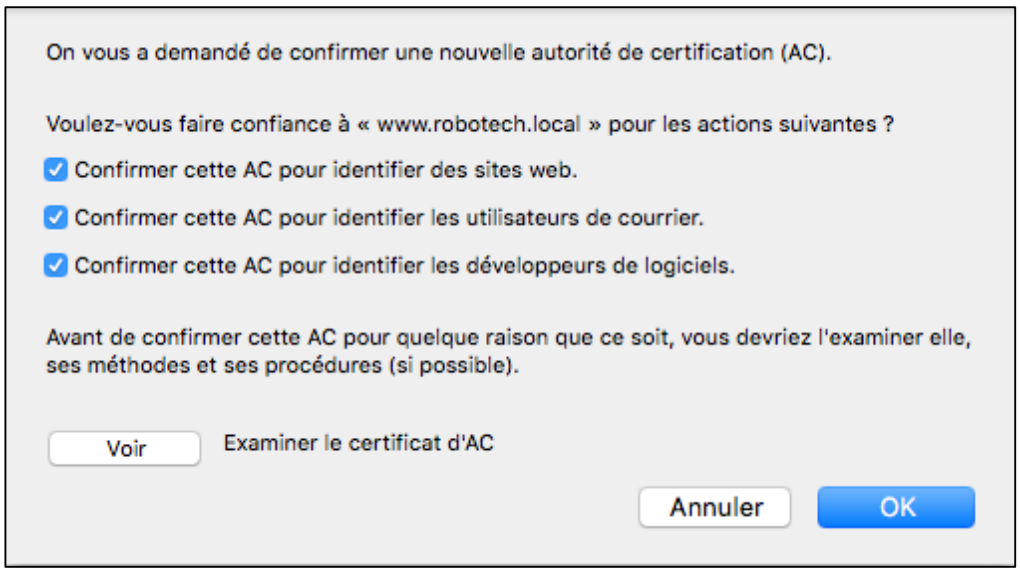
scp nom-d-utilisateur@addip:/chemin/vers/le/fichier /chemin/sur/votre/poste

```
scp jerome@192.168.130.162:/ssl/CA.crt /Users/jerome/Desktop
```

```
rouget:~ jerome$ scp jerome@192.168.130.162:/ssl/CA.crt /Users/jerome/Desktop/
jerome@192.168.130.162's password:
CA.crt                                        100% 1468     1.4KB/s   00:00
rouget:~ jerome$
```

Dans les préférences de votre navigateur (ici Firefox), importé votre certificat CA.crt comme suit :





Etape 9 : Paramétrer Apache pour le site virtuel www.robotech.local

Commençons par accéder au répertoire où sont stocké les fichiers de configuration des virtualhosts.

```
root@procedure-web:/# cd /etc/apache2/sites-available/
root@procedure-web:/etc/apache2/sites-available# ls -l
total 12
-rw-r--r-- 1 root root 1332 oct.  24 10:37 000-default.conf
-rw-r--r-- 1 root root 6437 oct.  24 10:37 default-ssl.conf
root@procedure-web:/etc/apache2/sites-available#
```

Puis nous allons copier le fichier de configuration par défaut pour les virtualhosts en HTTPS et l'appelé robotech-ssl.conf par exemple.

```
root@procedure-web:/etc/apache2/sites-available# cp default-ssl.conf robotech-ssl.conf
root@procedure-web:/etc/apache2/sites-available# vim robotech-ssl.conf
```

Ensuite nous allons le modifier… Dans la balise <VirtualHost> du haut nous allons mettre l'adresse IP de notre site web suivit du port 443, qui est le port web HTTPS.

```
<VirtualHost 192.168.130.162:443>
        ServerAdmin webmaster@localhost
        ServerName www.robotech.local
        DocumentRoot /var/www/robotech
```

Puis nous allons également modifier les deux lignes suivantes. Il suffit juste d'indiquer le bon chemin vers le répertoire qui contient le certificat web (webcertif.crt) pour la première ligne, et celui pour la clé web (webkey.key) dans la deuxième ligne. Enfin vous pouvez enregistrer et quitter le fichier.

```
SSLCertificateFile      /etc/ssl/certs/webcertif.crt
SSLCertificateKeyFile /etc/ssl/private/webkey.key
```

Pour activer le virtualhost, tapez la commande `a2ensite robotech-ssl.conf` et relancez apache avec la commande `service apache2 reload`

```
root@procedure-web:/etc/apache2/sites-available# a2ensite robotech-ssl.conf
Enabling site robotech-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
```

Vous devez aussi activer le « mod » ssl. Pour cela, accéder au répertoire mods-available avec la commande suivante : `cd /etc/apache2/mods-available`
Activer-le : `a2enmod ssl.load`
Et lorsqu'on vous le demande, tapez : `service apache2 restart`
Il est fort probable que pour redémarrer le service on vous demande d'indiquer la passphrase que vous avez entrez plus tôt.

```
root@procedure-web:/etc/apache2/mods-available# a2enmod ssl.load
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed
certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@procedure-web:/etc/apache2/mods-available# service apache2 restart
Enter passphrase for SSL/TLS keys for www.robotech.local:443 (RSA): ********
root@procedure-web:/etc/apache2/mods-available#
```

Etape 10 : Accéder au site

Ouvrez un navigateur tel que Firefox ici, puis tapez l'adresse de votre site sans oublié d'ajouter https devant.

Vous pouvez voir votre certificat en cliquant sur le petit cadenas vert

Bien joué ! Vous venez de créer un site web en HTTPS avec Apache.

Vous pouvez reprendre la procédure depuis le début si vous désirez faire d'autres site web en HTTPS.