Table des matières :

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

User : arthur et root

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer un serveur équilibrage de charges au moyen du service Keepalived sous Debian.

OS	Distribution	Version
Debian	Linux	8.5

1. Le fichier openssl.cnf

On commence par crée l'arborescence :

```
arthur@debian8:~$ mkdir tpssl
arthur@debian8:~$ mkdir certs/
arthur@debian8:~$ mkdir private/
arthur@debian8:~$ mkdir crl/
arthur@debian8:~$ mkdir newcerts
```

On crée le fichier index vide

```
arthur@debian8:~$ touch index.txt
```

On crée le fichier serial avec la valeur 01

```
arthur@debian8:~$ echo '01'> serial
```

```
arthur@debian8:~$ tree
.
└── tpssl
    ├── certs
    ├── crl
    ├── index.txt
    ├── newcerts
    ├── private
    └── serial
```

On copie le fichier openssl.cnf dans le répertoire tpssl.

```
arthur@debian8:~$ cp /etc/ssl/openssl.cnf /home/arthur/tpssl/
```

On modifie ensuite le fichier copier pour modifie la valeur dir

```
arthur@debian8:~/tpssl$ nano openssl.cnf _
```

```
dir               = /home/arthur/tpssl_    # Where everything is kept
```

2. Création des certificats :

1. Création du certificat de l'autorité de certification

Cette étape consiste à crée la paire de clés privée/publique puis un certificat racine autosigné.

On aura donc une clé privée protégée par un mot de passe et une demande de certificat numérique valable 3650 jours.

```
arthur@debian8:~/tpssl$ openssl req -new -x509 -extensions v3_ca -keyout private
/cakey.pem -out cacert.pem -days 3650 -config ./openssl.cnf
Generating a 2048 bit RSA private key
...+++
..+++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:14
Locality Name (eg, city) []:caen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Les deux fichiers de certificats sont maintenant apparus :

```
arthur@debian8:~/tpssl$ ls
cacert.pem  certs  crl  index.txt  newcerts  openssl.cnf  private  serial
```

2. Extraction du certificat racine :

L'extraction consiste à afficher une sortie écran d'un certificat. On peut alors vérifier que le certificat est conforme aux attentes.

```
arthur@debian8:~/tpssl$ openssl x509 -text -in cacert.pem
```

Pour sauvegarder vos fichiers, procédez à leur archivage :

```
arthur@debian8:~/tpssl$ tar -czf rootca.tar.gz private/cakey.pem cacert.pem
arthur@debian8:~/tpssl$ ls
cacert.pem  crl         newcerts     private         serial
certs       index.txt   openssl.cnf  rootca.tar.gz
```

3. Création d'un certificat SSL pour un serveur web :

3. Création de la paire de clé et de la demande de certificat :

```
arthur@debian8:~/tpssl$ openssl req -config ./openssl.cnf -new -keyout private/w
ebkey.pem -out certs/newreq.pem
```

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:14
Locality Name (eg, city) []:caen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:techrom
Organizational Unit Name (eg, section) []:service reseau
Common Name (e.g. server FQDN or YOUR name) []:techrom.fr
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:root
An optional company name []:
```

On rajoute un mot de passe pour plus de sécurité

On vérifie la présence des 2 fichiers webkey.pem et newreq.pem

```
arthur@debian8:~/tpssl$ ls
cacert.pem  crl         newcerts     private         serial
certs       index.txt   openssl.cnf  rootca.tar.gz
arthur@debian8:~/tpssl$ cd private
arthur@debian8:~/tpssl/private$ ls
cakey.pem  webkey.pem
```

4. Signature de la demande de certificat par l'autorité :

```
arthur@debian8:~/tpssl$ openssl ca -config ./openssl.cnf -policy policy_anything
 -out certs/webcert.pem -infiles certs/newreq.pem
```

Il faudra répondre yes aux deux questions.

5. Vérification du chemin de certification

L'objectif est de vérifier que la signature du certificat a bien été effectuée par notre autorité de certification. Cela prouve que le chemin de certification est correct. Pour cela on utilise la commande verify d'openssl :

```
arthur@debian8:~/tpssl$ openssl verify -Cafile cacert.pem certs/webcert.pem
usage: verify [-verbose] [-CApath path] [-CAfile file] [-purpose purpose] [-crl_
check] [-no_alt_chains] [-attime timestamp] [-engine e] cert1 cert2 ...
recognized usages:
        sslclient       SSL client
        sslserver       SSL server
        nssslserver     Netscape SSL server
        smimesign       S/MIME signing
        smimeencrypt    S/MIME encryption
        crlsign         CRL signing
        any             Any Purpose
        ocsphelper      OCSP helper
        timestampsign   Time Stamp signing
```

4. Installation du certificat SSL

6. Export des certificats et de la clé privée

Décryptage de la clé privée du serveur web

La commande suivante permet de générer un nouveau fichier contenant la clé privée non cryptée (webkey-clair.pem)

```
arthur@debian8:~/tpssl$ openssl rsa -in private/webkey.pem -out private/webkey-c
lair.pem
Enter pass phrase for private/webkey.pem:
writing RSA key
```

Copier ensuite les fichiers webcert.pem, webkey-clair.pem dans le répertoire SSL d'Apache. (À faire en root)

```
root@debian8:~# cp /home/arthur/tpssl/private/webkey-clair.pem /etc/apache2/ssl/
```

```
root@debian8:~# cp /home/arthur/tpssl/certs/webcert.pem /etc/apache2/ssl/
```

7. Configuration d'Apache :

```
root@debian8:/etc/apache2/ssl# a2enmod ssl
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 s
elf-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian8:/etc/apache2/ssl# service apache2 restart
```

Nous devons crée un hôte virtuel (virtual host) pour qu'Apache soit capable de répondre aux requêtes SSL (https).

```
root@debian8:/etc/apache2/sites-available# nano default-ssl.conf
```

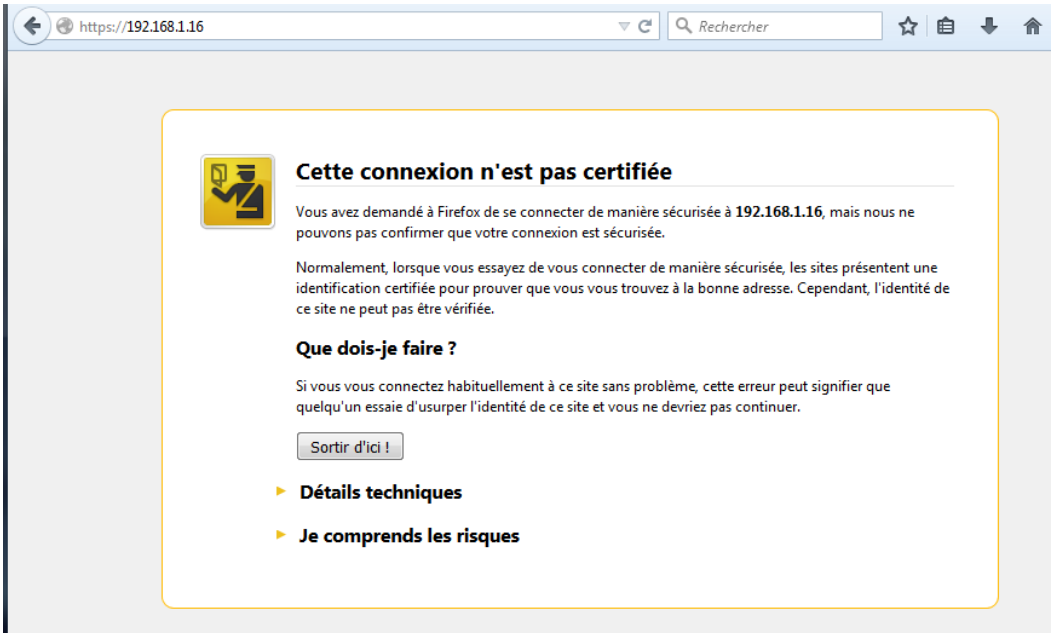
```
SSLCertificateFile      /etc/apache2/ssl/webcert.pem
SSLCertificateKeyFile /etc/apache2/ssl/webkey-clair.pem
```

```
root@debian8:/etc/apache2/sites-available# a2ensite default-ssl.conf
```

On lance le navigateur firefox avec l'url

```
root@debian8:/etc/apache2/sites-available# service apache2 reload
```

On test sur le navigateur firefox : en https



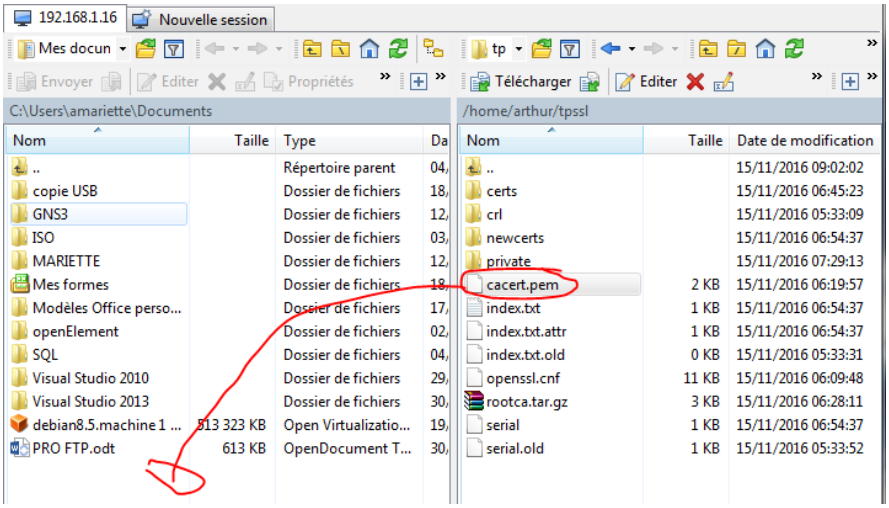
On doit choisir « sortir d'ici » car le certificat n'a pas été vérifié par une autorité de certification de confiance.

8. Ajout de notre autorité de certification dans le navigateur FIREFOX

Afin d'éviter le message d'acceptation du certificat, il est possible de configurer le navigateur pour qu'il accepte tous les certificats venant de notre autorité de certification. Pour cela, il faut absolument copier le certificat racine (cacert.pem) sur le poste du client et l'importer dans la configuration du navigateur.

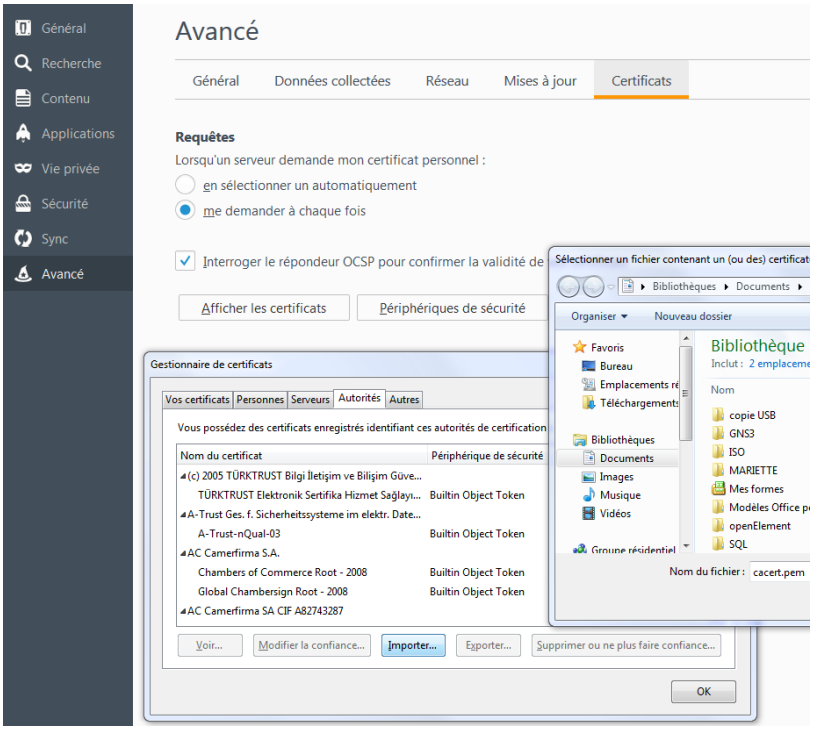
/options/avancé [chiffrement] – afficher les certificats -importer

On utilise FTP pour copier le fichier de la VM vers notre le pc client, on se connecte avec notre session de vm arthur.



On retourne sur firefox pour importer le certificat :

/options/avancé [chiffrement] – afficher les certificats -importer

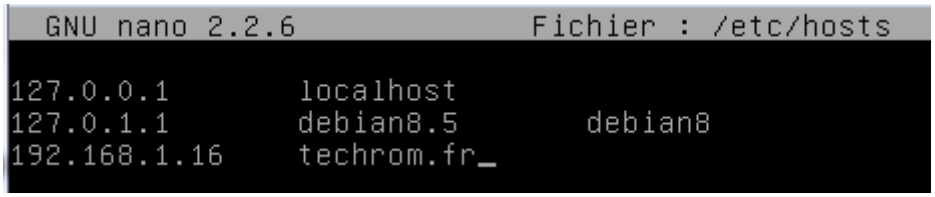


Une boite de dialogue apparait, on coche les 3 cases.

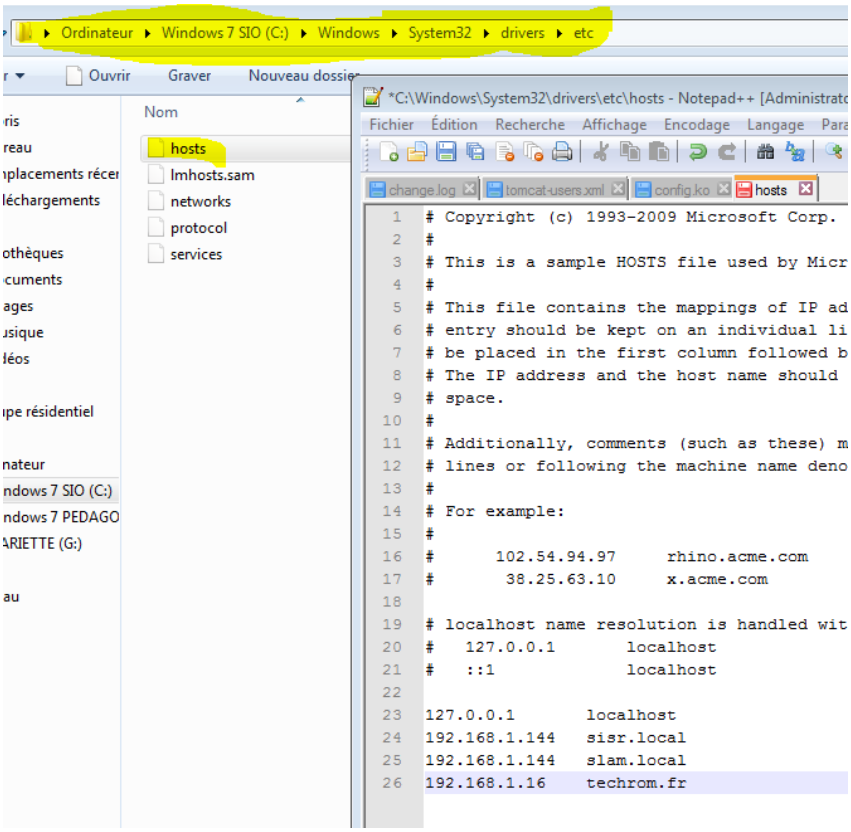
Il reste un problème de résolution de noms DNS. En effet, la valeur du champ « Common Name » du certificat crée précédemment est « techrom.fr ». Si vous n'accédez pas au serveur web avec URL basée sur le même nom, la plupart des navigateurs affichent un message d'avertissement. Ce problème pourra être résolu lorsque le nom de domaine du serveur

1. Résolution du problème DNS

Afin de résoudre ce problème dans pour autant modifier le système de résolution DNS, nous allons installer une résolution statique DNS par l'intermédiaire du fichier /etc/hosts. Ajouter la ligne suivante :



On va enregistrer aussi sur notre pc client ds une session avec les droits admin



On test dans notre navigateur avec https://techrom.fr