Compte rendu d'Installation d'un « OpenSSL »

Table des matières

Objectif(s) :

L'objectif principal du TP est la création d'une autorité de certification et la création de certificat SSL. Le certificat SSL sera ensuite déployé sur le serveur Web Apache. Nous verrons comment :

- *Créer / Gérer des certificats / Tester / Vérifier des certificats*
- *Réaliser d'une chaîne de certification*
- *Initialiser d'une communication SSL entre client/serveur*

Légende :

- Les commandes ou les chemins (absolue/relatif) sont en gras, souligné et en italique ex :
  - ***Apt-get update***
- Des captures d'écrans ont été prises afin de faciliter la compréhension du lecteur.

Machine	Os	Distribution	Version	C/S	IP
POSTE21	Debian	Linux	8.5	S	192.168.1.141 Samba4

Sujet :

OpenSSL est un utilitaire cryptographique qui implémente les protocoles réseau Secure Sockets Layer (SSL v2/v3, couche de sockets sécurisé) et Transport Layer Security (TLS v1, sécurité pour la couche de transport) ainsi que les stadards cryptographiques liées dont ils ont besoin.

Le programme openssl est un outil de lgine de commande pour utiliser les différentes fonctions cryptographiques de la librairie crypto d'OpenSSL à partir du shell. Il peut être utilisé pour :

- Création de paramètres des clefs RSA (Rivest Shamir Adleman), DH (Diffie-Hellman) et DSA (Digital Signature Algorithm),
- Création de certificats X.509, CSRs (CertificateSigningRequest) et CRLs (CertificateRevocation List),
- Calcul de signature de messages,
- Chiffrement et Déchiffrement,
- Test SSL /TLS client et server,
- Gestion de mail S/MIME (Secure/Multipurpose Internet Mail Extensions) signé ou chiffrés.

Openssl commande [option_commande] [arguments_commande]

Openssl [commandes-standard-liste | commandes-signature-messages-liste | commande-chiffrement-liste]

Les commandes-pseudo commande-standard-liste, commandes-signature-message-liste, et commande-chiffrement-liste génèrent une liste (une entrée par ligne) des noms de toutes les commandes standards, commandes de signature de messages (exemple MD5) ou commandes de chiffrment, respectivement, qui sont disponible dans le présent utilitaire openssl.

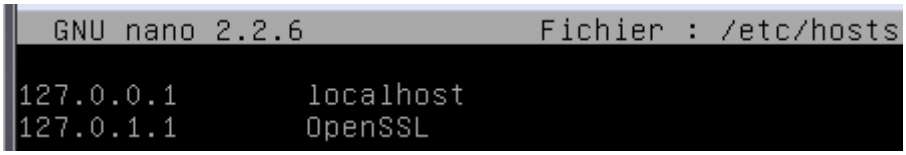
Les pages « man » vous permettent de connaître toutes les commandes dépendantes d'openssl. Une traduction en francais existe à l'adresse suivante :

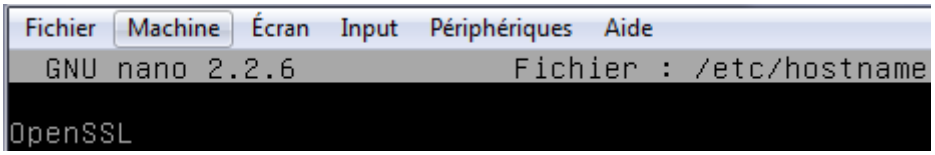
http://www.delafond.org/traducmanfr/man/man1/openssl.1.html

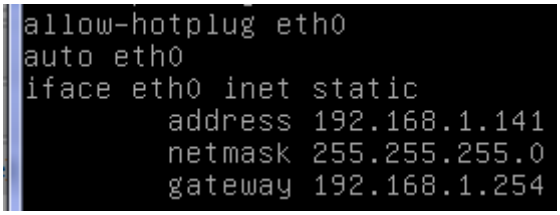
Configuration principale :

On va commencer par configurer la machine en mettant correctement le hostname et le host et l'adresse IP :

#/etc/hostname
#/etc/hosts
#/etc/network/interfaces







Une fois la configuration de la machine effectuée on va mettre à jour la machine :

#apt-get update
#apt-get upgrade
#apt-get dist-upgrade

Le fichier openssl.cnf :

Il faut organizer les différents certificats de façon à ce que les clients et serveurs puissant les trouver et les tester. Il est possible de profiter de l'organisation proposée dans le fichier de configuration d'openssl (fichier openssl.cnf).

Celui-ci utilise l'organisation suivante :

- $dir = le répertoire de base ou sont situées tous les différents certificats, clés privées, etc.
- $dir/certs = le répertoire ou sont conservés les certificats (plus exactement, des noms de la forme has.O)
- $dir/crl = le répertoire ou sont conservées les listes de révocation.
- $dir/newcerts = le répertoire ou sont stockés les certificats nouvellement créees.
- $dir/private = le répertoire ou sont stockées les clés privées
- $dir/serial = le fichier qui contient le procain numéro de série pour tout nouveau certificat qui sera crée. Il sert à initialiser le compteur de certificats (on peut le créer par la commande : « echo '01' > serial »)
- $dir/index.txt = le fichier d'index de la base de données des certificats (on peu le créer par al commande « touch index.txt).

Remarque :

- Le répertoire $dir devra vous appartenir
- Le certificat racine est placé directement dans $dir.
- La clé privée du certificat racine est dans $dir/private.
- Pour tester la validité d'un certificat, il faut tester la validité de la chaîne complète des certificats jusqu'au certificat racine. Ainsi, si par exemple un client souhaite valider le certificat du serveur, il devra avoir acces aux certificats apache.pem et ca.pem. Il faut donc posséder localement les certificats permettant de tester la chaîne de certificats.

Afin de stocker tous les fichiers contenant les certificats, les clés privées et publiques, il faut créer un répertoire dédié. Créer les répertoires suivant dans votre espace personnel.

~tpssl/private

~tpssl/certs

~tpssl/crl

~tpssl/newcerts

Copiez le fichier ***openssl.cnf*** (***/etc/ssl/openssl.cnf)*** dans le répertoire tpssl. Modifier la variable dir dans le fichier openssl.cnf (par exemple /home/lletort/tpssl). Créer également les fichiers ***index.txt et serial***

```
drwxr-xr-x 2 letort letort  4096 nov.  18 14:50 certs
drwxr-xr-x 2 letort letort  4096 nov.  18 14:51 crl
-rw-r--r-- 1 letort letort     0 nov.  18 14:51 index.txt
drwxr-xr-x 2 letort letort  4096 nov.  18 14:51 newcerts
-rw-r--r-- 1 letort letort 10845 nov.  18 15:05 openssl.cnf
drwxr-xr-x 2 letort letort  4096 nov.  18 14:51 private
-rw-r--r-- 1 letort letort     3 nov.  18 14:51 serial
```

2. Création des certificats

2.1. Création du certificats de l'autorité de certification :

Cette étape consiste à créer la paire de clés privée/publique puis un certificat racine autosigné (signifie qu'une signature numérique a été ajoutée. Cette signature a été créée à partir du certificat lui-même). A l'issue de cette étape, nous aurons :

- Une clé privée protégée par un mot de passe (cakey.pem)
- Une demande de certificat numérique valable 3650 jours (cacert.pem)

Les renseignements suivants devront être fournis impérativement :

Nom de champ	Descriptif	Exemple
PEM passphrase	Mot de passe permettant de crypter la clé privée	Password1234
Country Name	Les 2 lettres du pays ou à été créé le certificat	FR
State or Province Name	Région ou département	14
City Or Locality	Ville	Caen
Organization Name	Nom exact de l'entreprise	Techrom
Organizational Unit	Unité d'organisation	Service réseau
Common Name	Nom descriptif du certificat	CA techrom

Voici la commande :

openssl req –new –x509 –extensions v3_ca-keyout private/cakey.pem –out cacert.pem –days 3650 –config ./openssl.cnf

Vérifiez la présence des deux fichiers ***cakey.pem*** et ***cacert.pem*** .Observez l'en-tête du fichier ***cakey.pem***

La clé privée est protégée avec une variante de l'algorithme 3DES. Le mot de passe saisi sera indispensable pour lire la clé.

```
lletort@Lab:~/tpssf$ 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]:Techrom
Organizational Unit Name (eg, section) []:Service réseau
Common Name (e.g. server FQDN or YOUR name) []:CA techrom
Email Address []:
```

```
lletort@Lab:~/tpssf$ ls -la
total 44
drwxr-xr-x 6 lletort lletort  4096 nov.  15 09:33 .
drwxr-xr-x 3 lletort lletort  4096 nov.  15 09:32 ..
-rw-r--r-- 1 lletort lletort  1334 nov.  15 09:33 cacert.pem
drwxr-xr-x 2 lletort lletort  4096 nov.  15 08:33 certs
drwxr-xr-x 2 lletort lletort  4096 nov.  15 08:33 crl
-rw-r--r-- 1 lletort lletort     0 nov.  15 08:33 index.txt
drwxr-xr-x 2 lletort lletort  4096 nov.  15 08:33 newcerts
-rw-r--r-- 1 lletort lletort 10846 nov.  15 09:22 openssl.cnf
drwxr-xr-x 2 lletort lletort  4096 nov.  15 09:32 private
-rw-r--r-- 1 lletort lletort     3 nov.  15 08:33 serial
lletort@Lab:~/tpssf$ ls private
cakey.pem
```

2.2. 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.

#openssl x509 –text –in cacert.pem

Pour sauvegarde vos fichiers, procédez à leur archivage :

```
tar -czf rootca.tar.gz private/cakey.pem cacert.pem
```

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

Un certificat SSL peut être utilisé afin de sécuriser les échanges entre le serveur Web et des clients potentiels. Ce certificat, installé sur un serveur Web, est transmis au client lorsqu'un échnage sécurisé est demandé.

Le certificat SSL, associé à une paire de clés publique/privée, permet au serveur d'échanger des données cryptées avec le navigateur du client.

Il faut donc :

- Créer une nouvelle paire de clé publique/privée (webkey.pem)
- Créer une nouvelle demande de certificat pour le serveur qui contiendra la clé publique (newreq.pem)
- Signer cette demande de certificat avec le certificat de l'autorité (cacert.pem) et obtenir un nouveau certificat (webcert.pem)

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

Les renseignements suivants devront être fournis impérativement :

Nom de champ	Descriptif	Exemple
PEM passphrase	Mot de passe permettant de crypter la clé privée	Password1234
Country Name	Les 2 lettres du pays ou à été créé le certificat	FR
State or Province Name	Région ou département	14
City Or Locality	Ville	Caen
Organization Name	Nom exact de l'entreprise	Techrom
Organizational Unit	Unité d'organisation	Service réseau
Common Name	Nom descriptif du certificat	techrom.fr

```
lletort@Lab:~/tpssf$ openssl req -config ./openssl.cnf -new -keyout private/webkey.pem -out certs/newreq.pem
Generating a 2048 bit RSA private key
..............................+++
.................+++
writing new private key to 'private/webkey.pem'
```

```
lletort@Lab:~/tpssf$ openssl req -config ./openssl.cnf -new -keyout private/webkey.pem -out certs/newreq.pem
Generating a 2048 bit RSA private key
..............................+++
.................+++
writing new private key to 'private/webkey.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]:Techrom
Organizational Unit Name (eg, section) []:Service réseau
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 []:Root1
An optional company name []:
```

Vérifiez la présence des 2 fichiers ***webkey.pem*** et ***newreq.pem***

```
lletort@Lab:~/tpssf/private$ ls -l
total 8
-rw-r--r-- 1 lletort lletort 1834 nov.  15 09:33 cakey.pem
-rw-r--r-- 1 lletort lletort 1834 nov.  15 09:58 webkey.pem
lletort@Lab:~/tpssf/private$ cd ..
lletort@Lab:~/tpssf$ ls -l
total 40
-rw-r--r-- 1 lletort lletort  1334 nov.  15 09:33 cacert.pem
drwxr-xr-x 2 lletort lletort  4096 nov.  15 09:58 certs
drwxr-xr-x 2 lletort lletort  4096 nov.  15 08:33 crl
-rw-r--r-- 1 lletort lletort     0 nov.  15 08:33 index.txt
drwxr-xr-x 2 lletort lletort  4096 nov.  15 08:33 newcerts
-rw-r--r-- 1 lletort lletort 10846 nov.  15 09:22 openssl.cnf
drwxr-xr-x 2 lletort lletort  4096 nov.  15 09:56 private
-rw-r--r-- 1 lletort lletort  2496 nov.  15 09:46 rootca.tar.gz
-rw-r--r-- 1 lletort lletort     3 nov.  15 08:33 serial
lletort@Lab:~/tpssf$ cd certs/
lletort@Lab:~/tpssf/certs$ ls -l
total 4
-rw-r--r-- 1 lletort lletort 1041 nov.  15 09:58 newreq.pem
```

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

Il faut maintenant signer ce certificat afin qu'il puisse être déployé sur le serveur Web. Pour cela, la clé privée de l'autorité de certification sera nécessaire puisqu'elle est la seule à pouvoir créer la signature numérique.

```
anthony@Poste9:~/tpssl$ openssl ca -config ./openssl.cnf -policy policy_anything
 -out certs/webcerts.pem -infiles certs/newreq.pem
Using configuration from ./openssl.cnf
Enter pass phrase for /home/anthony/tpssl/private/cakey.pem:
```

Il faut bien entendu rentrer le mot de passe que l'on a rentré précédemment (dans notre cas root).

Ensuite les détails du certificat seront affichés, et on nous demandera de valider. Il faut répondre yes à toutes les questions :

```
Certificate is to be certified until Nov 15 07:19:52 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

3.3. 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 :

#openssl verify –Cafile cacert.pem certs/webcert.pem

Si l'on obtient OK, c'est que le certificat est validé.

4. Installation du certificat SSL

4.1. Export des certificats et de la clé privée

Les éléments nécessaires à Apache2 pour prendre en charge SSL sont les suivants :

- Le certificat du serveur (webcert.pem)
- La clé privée non cryptée du serveur

Remarque

Le fait d'accéder à la clé privée du serveur pose un sérieux problème de sécurité. En effet, si quelqu'un s'empare de cette clé, il pourra décrypter tous les échanges entre le serveur et ses clients. Il est possible de maintenir un cryptage de la clé privée grâce à un mot de passe. Dans ce cas, dès que le serveur Apache2 démarre, il demandera le mot de passe. Dans ce TP, nous allons laisser la clé privée non-cryptée.

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) :

#openssl rsa –in private/webkey.pem –out private/webkey-clair.pem

Copie des fichiers dans le répertoire d'Apache2

Copier les fichiers webcert.pem, webkey-clair.pem dans le répertoire SSL d'Apache (àcréer si nécessaire).

4.2. Configuration d'Apache

Il faut d'abord configurer le serveur Web pour qu'il utilise SSL. Le module doit donc être activé. Il s'agit de créer un lien symbolique entre les 2 répertoires suivants :

- /etc/apache2/mod-available/
- /etc/apache2/mod-enabled/

#a2enmod ssl

Maintenant on va configurer le serveur web pour qu'il utilise SSL. Le module doit donc être activé, on va donc utiliser la commande suivante :

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

- Editer le fichier /etc/apache2/sites-available/default-ssl et modifier le chemin des certificats.
- Activer cet hôte virtuel puis redémarrer Apache2.

#a2ensite default-ssl

Puis on redémarre apache2 :

#systemctl restart apache2

Lancer le navigateur Firefox avec l'url https://localhost ou https://@IP. Un message apparaît, n'acceptez pas ce certificat qui n'a pas été vérifié par une autorité de certification de confiance.

4.3. 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 client et l'importer dans la configuration du navigateur.

/options/options/avancé [chiffrement] – affiché les certificats – importé

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 une 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 sera configuré correctement.

4.4. Résolution d'un problème DNS :

Afin de résoudre ce problème sans 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 :

#192.168.1.142 techrom.fr

Lancer de nouveau votre navigateur favori FireFox et rendez-vous sur la page d'accueil du serveur Web en utilisant le protocole HTTPS.

- Réaliser une capture de trame à l'aide du sniffeur Wireshark

- Que constatez-vous ?

- Conclure.