SSL

SSL, à ne pas confondre avec Super Soupe au Lait, un personnage interprété par Gustave de Kervern (Groland).

Bon c'est pas tout ça, SSL c'est en fait très sérieux et pas du tout rigolo.

Transport Layer Security (TLS), et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le protocole SSL a été développé à l'origine par Netscape. L'IETF, en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

source: https://fr.wikipedia.org/wiki/Transport_Layer_Security

Note Fred: dans ce triste monde de surveillance policière et de pirates malintentionnés, SSL (utilisé par https) est devenu incontournable, dès qu'il s'agit de passer des infos un peu sensibles (mots de passes, infos personnelles etc) et de garantir que le site qui vous parle est bien celui qu'il prétend être.

installer SSL sur un localhost

on peut avoir besoin d'un “pseudo” certificat sur une machine locale (localhost)

```
a2enmod default-ssl
systemctl restart apache2
```

installer un certificat auto-signé

Note Fred: je vous déconseille cette option, maintenant que Let's Encrypt est disponible, c'est nettement plus simple et surtout pérenne. Voir *infra* pour des explications et un tuto.

- http://wiki.gandi.net/fr/ssl/multiplecertononehostipport
- http://www.demenageur-site.com/blog/2012/06/plusieurs-certificats-ssl-pour-differents-virtualhosts-sur-une-seule-ip/
- http://jeyg.info/des-certificats-signes-par-votre-autorite-de-certification-avec-openssl/

Tutoriel Vidéo Divers

- Comprends le SSL: https://www.grafikart.fr/tutoriels/divers/comprends-ssl-tls-745
- Openssl, Création de certificats et CA autosignés: https://www.linuxtricks.fr/wiki/openssl-creation-de-certificats-et-ca-autosignes

Let’s Encrypt



Fix Me!: désormais le site de let's encrypt recommande d'utiliser ce client pour obtenir un certificat: https://certbot.eff.org/

- https://yourserverpb.com/lets-encrypt-apache/
- https://lemag.sfeir.com/https-everywhere-avec-lets-encrypt/

https://letsencrypt.org/

Let’s Encrypt is a new Certificate Authority: It’s free, automated, and open. In Public Beta

Suivre cet excellent tuto pour installer ça simplement sur votre serveur:
https://www.grafikart.fr/formations/serveur-linux/apache-ssl-letsencrypt

J'ai pris la liberté de recopier de ce tuto les commandes de base - modifier bien sûr mondomaine.red par votre/vos domaine/s.

```
sudo git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt -
-depth=1
#later
#cd /opt/letsencrypt
#sudo git pull
/opt/letsencrypt/letsencrypt-auto
/opt/letsencrypt/letsencrypt-auto --apache -d monmondomaine.red -d
www.monmondomaine.red
```

il faut bien sûr modifier vos config apache si ce n'est pas déjà fait et ajouter les certificats créés par letsencrypt et recharger les fichiers de config apache

```
<IfModule mod_ssl.c>
  <VirtualHost *:443>
    ...
    SSLCertificateFile /etc/letsencrypt/live/mondomaine.red/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/mondomaine.red/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf
    ...
```

```
  </VirtualHost>
</IfModule>

/etc/init.d/apache2 reload
```

Tester

- https://www.ssllabs.com/ssltest/analyze.html?d=radeff.red&latest
- https://www.ssllabs.com/ssltest/analyze.html?d=www.radeff.red&latest

Renouvellement

```
 /opt/letsencrypt/letsencrypt-auto --apache --renew-by-default  -d
monmondomaine.red -d www.monmondomaine.red
```

Script auto à mettre dans un cron hebdo:

```
sudo curl -L -o /usr/local/sbin/le-renew http://do.co/le-renew
sudo chmod +x /usr/local/sbin/le-renew

sudo le-renew mondomaine.red
```

et le cron

```
sudo crontab -e
0 3 * * 1 /usr/local/sbin/le-renew domaine.fr >> /var/log/le-renew.log
```

Merci encore à https://www.grafikart.fr/formations/serveur-linux/apache-ssl-letsencrypt pour son excellent tuto, sans lequel je ne m'en serai jamais sorti!

Problèmes divers

Mixed content

https://www.whynopadlock.com/

On est pas tous pour https

Un article assez provo, mais plutôt intelligent et pas dénué d'humour contre l'abus d'https : http://michael.orlitzky.com/articles/lets_not_encrypt.xhtml

Vaut mieux payer ?

Certain·e·s croient qu'en payant leur certificat SSL cela le rend plus crédible.

Que nenni, billevesée et coquecigrue ! Un certificat Let's Encrypt gratuit est tout aussi fiable.

Argumentaire d'un spécialiste : *Scott Helme, Debunking the fallacy that paid certificates are better than free certificates, and other related nonsense*

From:
https://radeff.red/dokuwiki/ - **Radeff's Wiki**

Permanent link:
https://radeff.red/dokuwiki/info:ssl

Last update: **2024/03/14 10:23**