Mise en place de SSL

Ressources

- Discussion sur Kimsufi et SSL
- Utilisation de Letsencryp
  - Certbot
- Mise en place d'un certificat avec Startssl

Principes avec Letsencrypt

- Letsencrypt est une autorité de certification qui permet d'obtenir des certificats gratuitement et de manière automatisée.
- Pour faciliter l'installation d'un certificat pour un domaine donné, Letsencrypt conseille d'utiliser Certbot :
  - Pour Debian 8 (Jessie) :
    - Ajouter cette ligne dans */etc/apt/sources.list* : `deb http://debian.mirrors.ovh.net/debian/ jessie-backports main`
    - Installer Certbot pour Ngninx : `sudo apt-get install certbot -t jessie-backports`
  - Lancer Certbot en mode “interactif” et suivre les indications : `certbot certonly`
  - Sinon, il est possible de passer directement les instructions. Ex. : `certbot certonly –webroot -w /home/git/gitlab/public -d git.clapas.org`
- Renouveler automatiquement les certificats Letsencryp (car ils ont une durée de validité de 90 jours) :
  - Faire un test de renouvellement : `certbot renew –dry-run`
    - Tester en s’arrêtant pour vérifier le fichier créé pour le “challenge” : `certbot certonly –webroot -w /home/admin/.letsencrypt/ -d sql.clapas.ovh –dry-run –debug-challenges`
    - Si le navigateur à mémoriser la redirection 301 de HTTP vers HTTPS, utiliser wget pour vérifier qu'il est possible de récupérer le fichier : `wget http://sql.clapas.ovh/.well-known/acme-challenge/<fichier-du-challenge>`
  - Commande effectuant le renouvellement si nécessaire (à mettre dans un cron) : `certbot renew –quiet –standalone –pre-hook “service nginx stop” –post-hook “service nginx start”`
  - Sous Debian Jessie, un cron a été installé automatiquement dans */etc/cron.d/certbot* :
    - modifier le fichier pour ajouter les hooks permettant à Nginx de redémarrer et l'utilisation du mécanisme “standalone” pour gérer le cas de Gogs (si les certificats sont renouvelés uniquement) :

```
 0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system && perl -e 'sleep int(rand(3600))' && certbot -q renew  --standalone --pre-hook "service nginx stop" --post-hook "service nginx start"
```

Erreur sec_error_expired_certificate

Si l'erreur **sec_error_expired_certificate**, apparait dans Firefox, essayer de redémarrer Nginx, surtout si vous êtes sûr que le certificat est valide.

HSTS, Header HTTP et Firefox

Dans Firefox, la suppression de l'envoie de l'entête HTTP sur le serveur puis du cache du navigateur ne suffit pas à supprimer la redirection vers HTTPS induite par le header HSTS. Pour supprimer un tel comportement, il faut éteindre son navigateur. Puis, ouvrir le dossier de son profil Firefox à la recherche du fichier **SiteSecurityServiceState.txt**. Une fois trouvé, supprimer la ligne correspondant au nom du domaine du site ayant le problème et enregistrer la modification. Au prochain redémarrage de Firefox le problème sera réglé.

Principes avec Startssl

A des fins de test, le certificat gratuit fournit par https://www.startssl.com fera l'affaire. Suivre les indications fournis pour créer le certificat et le Certificate Signing Request (CSR).

Utilisationde S/MIME avec Gmail

Avec Firefox, installer le module Gmail S/MIME sous Chrome c'est le module Mymail-Crypt for Gmail™.

Notes

- **CSR :** message envoyé par le client à l'autorité de certification pour demander un certificat électronique.
- **S/MIME :** (Secure / Multipurpose Internet Mail Extensions) norme de cryptographie et de signature numérique de courriel encapsulés en format MIME. Elle assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des données. (Source : Wikipedia)