

SSL sur votre serveur dédié

Activation

L'option **SSL** est compilée directement dans votre serveur web (Apache). Il faut juste l'activer. En suite il faut acheter les certificats SSL officiels.

Le serveur web (HTTP) fonctionne sur le port 80. Le serveur SSL (HTTPS) fonctionne sur le port 443

Vérifiez d'abord que votre serveur apache n'écoute déjà pas sur le port 443:

```
# netstat -tanpu | grep ":443"
#
```

Non, pas de serveur qui écoute le port 443.

```
# cat /etc/sysconfig/apache
# Uncomment the following line and restart Apache to activate SSL
# OPTIONS="-DSSL"
```

Il suffit de commenter l'option et redémarrer le serveur web:

```
# pico /etc/sysconfig/apache
# cat /etc/sysconfig/apache
# Uncomment the following line and restart Apache to activate SSL
OPTIONS="-DSSL"
# /etc/rc.d/init.d/httpd restart
Arrêt de httpd : [ OK ]
Démarrage de httpd : [ OK ]
# netstat -tanpu | grep ":443"
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 25030/httpd
```

Et voilà le travail.

Sécurité

Très important. Il existe une faille de sécurité très simple à exploiter dans toutes les versions d'openssl inférieures à 0.9.6k. Il faut obligatoirement appliquer les patches de sécurité d'ovh avant réouverture de la machine. Sinon votre machine sera hackée en quelques jours (il existe énormément de scans des réseaux faits par les hackers pour découvrir les machines victimes).

Pour voir quelle version vous avez:

```
rpm -qa | grep ssl
```

Vous devez obtenir quelque chose du genre :

OVH

openssl-devel-0.9.6k-1
openssl-0.9.6k-1
openssl-perl-0.9.6k-1

Si vous avez une version antérieure à celle ci-dessus, par exemple si vous avez openssl-0.9.6i ce n'est pas bon. Refermez le port 443. Et appliquez les patchs. Vous avez des explications sur [ReleasePatchSecurite](#)