Configurer un site en https

Votre certificat a été généré grâce à **Certbot**. Il faut désormais configurer **Apache** pour utiliser de manière systématique ce certificat.

Voici mes prises de notes pour passer un site Internet **http** en **https**. Le configuration est destinée pour un site Internet dont le sous-domaine est **www**. Il est très facilement adaptable pour un site avec un sous-domaine différent.

```
  Configurer Apache 2
    http://www.perdu.com ==> https://www.perdu.com
```

Je viens de demander un certificat SSL pour le site Internet `perdu.com`. Il faut configurer Apache 2 pour que :

- les demandes en https utilisent le certificat SSL
- toutes les visites en http soit redirigées en https

Configurer

Je complète le fichier de configuration `/etc/apache2/sites-available/100-com.perdu.conf`. J'ajoute un bloc de redirection vers `https` :

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteCond %{REQUEST_URI} !\.well-known/acme-challenge/.*
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

Puis, j'ajoute un bloc pour la configuration SSL / https. Il s'agit d'un copier/coller de la configuration http. J'effectue quelques modifications :

- ErrorLog et CustomLog pour l’écriture des fichiers logs
- RewriteRule pour la redirection des URL sans www
- Ajout des options SSL
- Ajout de la gestion des certificats

```
<IfModule mod_ssl.c>
<VirtualHost *:443>

    ServerName perdu.com
    ServerAlias www.perdu.com
    Protocols h2 http/1.1

    DocumentRoot /var/www/perdu.com/www
```

```
    <Directory /var/www/perdu.com/www>
        Options -Indexes +MultiViews
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>


    <Location />
        Require all granted
    </Location>

    LogLevel warn
    ErrorLog ${APACHE_LOG_DIR}/www.perdu.com-https-error.log
    CustomLog ${APACHE_LOG_DIR}/www.perdu.com-https-access.log combined

    SSLCertificateFile /etc/letsencrypt/live/www.perdu.com/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/www.perdu.com/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/www.perdu.com/chain.pem
</VirtualHost>
</IfModule>
```

Les options SSL sont à créer une seule fois sur le serveur. Ces options sont communes à tous les sites Internet que je configure. Les options dans `/etc/apache2/mods-enabled/ssl.conf` sont les suivantes :

```
# Intermediate configuration
SSLProtocol -ALL +TLSv1.2
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-
RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-
SHA:!RC4:HIGH:!MD5:!aNULL:!EDH
SSLHonorCipherOrder     on
#SSLSessionTickets       off

SSLOptions +StrictRequire
SSLCompression          off

# HSTS (mod_headers is required) (15768000 seconds = 6 months)
Header always set Strict-Transport-Security "max-age=15768000"

# Always ensure Cookies have "Secure" set (JAH 2012/1)
Header edit Set-Cookie (?i)^(.*)(;\s*secure)??((\s*;)?(.*)) "$1; Secure$3$4"
```

Il convient de désactiver ces options dans le fichier `/etc/letsencrypt/options-ssl-apache.conf`

Ce qui donne une configuration globale suivante :

```
<VirtualHost *:80>

    ServerName perdu.com
    ServerAlias www.perdu.com
    Protocols h2 http/1.1

    DocumentRoot /var/www/perdu.com/www

    <Directory /var/www/perdu.com/www>
        Options -Indexes +MultiViews
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>


    <Location />
        Require all granted
    </Location>

    LogLevel warn
    ErrorLog ${APACHE_LOG_DIR}/www.perdu.com-http-error.log
    CustomLog ${APACHE_LOG_DIR}/www.perdu.com-http-access.log combined

    # Redirection des URL vers https
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteCond %{REQUEST_URI} !\.well-known/acme-challenge/.*
    RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]

</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost *:443>

    ServerName perdu.com
    ServerAlias www.perdu.com
    Protocols h2 http/1.1

    DocumentRoot /var/www/perdu.com/www

    <Directory /var/www/perdu.com/www>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>
```

```
    <Location />
        Require all granted
    </Location>

    LogLevel warn
    ErrorLog ${APACHE_LOG_DIR}/www.perdu.com-https-error.log
    CustomLog ${APACHE_LOG_DIR}/www.perdu.com-https-access.log combined
    SSLCertificateFile /etc/letsencrypt/live/www.perdu.com/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/www.perdu.com/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/www.perdu.com/chain.pem

</VirtualHost>
</IfModule>
```

Recharger

Après ces modifications, je recharge la configuration de Apache 2 :

```
sudo service apache2 reload
```

Zone DNS

Il est possible d'ajouter une option dans la zone DNS pour sécuriser l'authenticité de l'organisme de certification. Il s'agit du *DNS Certification Authority Authorization (CAA)* à activer grâce à un enregistrement **CAA** de la zone DNS :

```
www                IN CAA    128 issue "letsencrypt.org"
perdu.com.         IN CAA    128 issue "letsencrypt.org"
```

Tester

Vous pouvez tester votre site grâce à l'outil https://www.ssllabs.com/ssltest/analyze.html