Apache

Configurer le SSL avec Apache 2

18/06/2013 Florian B. 14 Commentaires Apache, Configuration, HTTPS, Sécurité, SSL

Sommaire [-]

I. Présentation

Lorsqu'on met en place un serveur web Apache ou un serveur web complet LAMP utilisant Apache, le site par défaut qui est actif utilise le protocole non-sécurisé HTTP et écoute sur le port 80. Pour des soucis de sécurité et de confidentialité de l'information, il peut être intéressant de passer ce site en HTTPS qui écoute quant à lui sur le port 443.

Il y a plusieurs méthodes pour mettre en place un site HTTPS sous Apache 2 :

- Méthode rapide : Consiste à utiliser les certificats SSL par défaut d'Apache 2 (étape n°2 du tutoriel).
- Méthode manuelle : Consiste à générer des certificats SSL et de les indiquer dans la configuration d'Apache 2 (à partir de l'étape n°3 jusqu'à la fin).

Par défaut Apache 2 contient deux sites préconfigurés : « default » et « default-ssl » qui pointent tous les deux vers le répertoire « /var/www » mais le premier écoute sur le port 80 (HTTP) et le second sur le port 443 (HTTPS). Dans la configuration d'origine, seul le site « default » est actif ce qui permet d'accéder à la page « It Works ! » d'Apache tout de suite après avoir effectué l'installation. Vu que le site par défaut SSL, il est pré-configuré pour fonctionner. De ce fait, il suffit d'effectuer deux choses pour le rendre actif et opérationnel :

- Activer le module SSL d'Apache
- Activer le site « default-ssl » d'Apache

Une fois que ces deux activations sont effectuées, il suffit de recharger Apache et le site sera accessible en HTTPS. Voici les commandes à saisir :

```
a2enmod ssl
a2ensite default-ssl
service apache2 reload
```

Vous remarquerez qu'il n'y a pas eu besoin de générer de certificat SSL. En effet, il y en a déjà un par défaut (valable 10 ans) comme je vous le disais et on peut voir où il se trouve en regardant de plus près le fichier « default-ssl » situé dans « /etc/apache2/sites-available » :

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

III. Génération des certificats

La sécurisation des échanges entre le client et le serveur grâce au protocole HTTPS implique l'utilisation d'un certificat SSL. Pour cela, nous allons générer un certificat pour notre serveur web grâce à l'outil OpenSSL. On aurait pu également utiliser « ssl-cert » à la place de l'application OpenSSL.

Cette procédure requiert OpenSSL 1.0.1j au minimum.

Installez le paquet OpenSSL si vous ne l'avez pas :

```
apt-get update
apt-get install openssl
```

Remarque : Un réel certificat doit être signé par une autorité de certification (CA)

penser à déclarer dans vos navigateurs pour ne pas avoir de messages d'avertissement. En ce qui nous concerne, nous allons générer un certificat auto-signé (donc non certifié) qui est gratuit et très bien pour une utilisation personnelle puisqu'il n'offre pas les mêmes garanties en terme de sécurité. Notamment parce que n'importe qui peut auto-signer un certificat donc ça ne vérifie pas l'identité de l'émetteur.

Afin de générer le certificat et sa clé, saisissez la commande suivante :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256
-out /etc/apache2/server.crt -keyout /etc/apache2/server.key
```

Elle vous permettra d'obtenir un certificat « server.crt » valable pour 1 an (*365 days*) en s'appuyant sur la norme de cryptographie X.509 et, sa clé privée « server.key ». Pour plus de sécurité, la clé sera en RSA 2048 bits et le hashage SHA-256 plutôt que MD5.

> Note : Pour préciser la durée de validité du certificat indiquez l'option « -days » suivit du nombre de jours.

Pendant la génération, on vous demandera des informations concernant votre identité comme le code pays, la localité, une adresse mail, le nom de l'entreprise, etc...

```
root@lamp:~# cd /home/flo/
root@lamp:/home/flo# openssl req -new -x509 -nodes -out server.crt -keyout server.key
Generating a 1024 bit RSA private key
.................++++++
.............................++++++
writing new private key to 'server.key'
-----
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]:
Locality Name (eg, city) []:Coutances
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Neoflow.fr
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:Flo
Email Address []:contact@neoflow.fr
root@lamp:/home/flo#
```

Pour finir on modifie les permissions sur la clé afin de ne pas autoriser la lecture par les « autres » mais uniquement par le propriétaire et le groupe propriétaire.

```
chmod 440 /chemin/server.crt
```

IV. Configuration d'Apache

l'indiquer à Apache. Pour cela, éditez le fichier « default-ssl » contenant la configuration du site SSL. Il se trouve ici :

```
/etc/apache2/sites-available/default-ssl
```

Modifiez ces deux options si nécessaire afin d'indiquer le chemin vers vos fichiers :

```
SSLCertificateFile /chemin/server.crt
SSLCertificateKeyFile /chemin/server.key
```

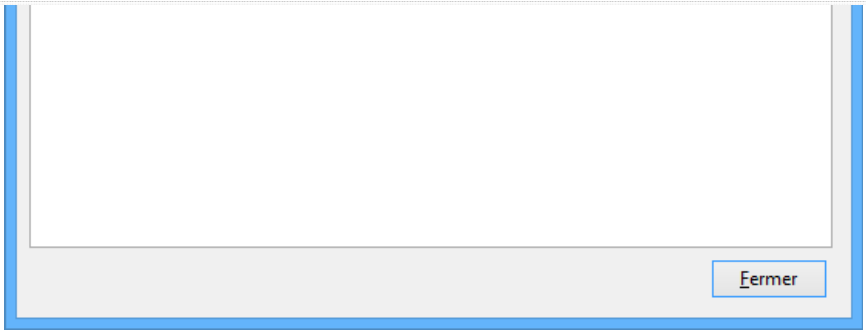
Suite aux dernières vulnérabilités découvertes au sein du protocole SSL en 2014, il est recommandé également d'effectuer la configuration suivante dans Apache pour plus de sécurité :

```
SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-
SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off
```

Enregistrez puis quittez le fichier de configuration du site SSL. Ensuite, activez le module SSL et le site SSL :

```
a2enmod ssl
a2ensite default-ssl
service apache2 reload
```

Accédez à votre site en utilisant le préfixe HTTPS dans l'URL, cela devrait fonctionner. D'ailleurs, si vous visualisez les informations du certificat obtenu vous verrez ce que vous avez saisit lors de la génération :



V. Désactiver le site HTTP

Si vous souhaitez qu'on accède à votre site web uniquement via le protocole HTTPS, il est intéressant de désactiver le site accessible sur le port 80 c'est-à-dire le site « default ». Pour cela on utilise la commande « a2dissite » qui permet de désactiver des sites dans Apache 2.

```
a2dissite default
```

Vous pouvez ensuite essayer d'accéder à votre site en HTTP et vous verrez qu'il n'est plus accessible.

VI. Rediriger le HTTP vers HTTPS automatiquement

Plutôt que de désactiver le site HTTP, on peut le laisser activer sauf qu'on va le configurer de façon à rediriger de manière permanente les requêtes HTTP vers HTTPS autrement dit les requêtes sur le port 80 vers le port 443.

Pour cela, modifiez le fichier suivant :

```
/etc/apache2/sites-available/default
```

Dans le virtualhost, ajoutez la ligne suivante :

```
Redirect permanent / https://server.domain.fr?
```

Adaptez la ligne ci-dessus avec votre nom de domaine. Ensuite, il ne vous reste plus qu'à recharger la configuration d'Apache puis de tester la redirection :

```
service apache2 reload
```

VII. Vérifiez votre configuration

SSL Labs

Partagez cet article

GÉRER LES POINTS DE RESTAURATION AVEC POWERSHELL

OFFICE TIMELINE, UN PLUG-IN INTÉRESSANT POUR POWERPOINT

Florian B.

Co-Fondateur d'IT-Connect, je souhaite partager mes connaissances et expériences avec vous, et comme la veille techno' est importante je partage aussi des actus.

florian has 1948 posts and counting.

See all posts by florian

Vous pourrez aussi aimer

Stagefright : Une faille Android inquiétante
29/07/2015 0

Calculer une empreinte md5 sous Linux
01/04/2013 0

Qu'est ce que le Directory Browsing/Listing ?
24/01/2014 1

14 pensées sur "Configurer le SSL avec Apache 2"

Permalink

Merci pour ces précieuses infos utiles aux néophytes tels que moi . Le tutoriel est d'autant plus clair qu'il est efficace .

Bonne continuation et merci .

Répondre

Florian Auteur de l'article
16/10/2013 à 13:01
Permalink

Merci de nous avoir donné votre avis ! N'hésitez pas à utiliser notre forum si besoin.

Bonne journée

Répondre

hammouch
10/03/2014 à 10:09
Permalink

D'abord merci pour tes clarifications..

Sauf que pour moi j'ai une plate-forme (intranet) sous windows2003 server + apache 2.2 dont j'accède via un certificat p12 installer dans le navigateur internet explorer 6 (j'ai 2 pages:page exploitant et page administrateur dont j'accède chacun par un certificat p12)

Mes certificats tiens leur fin et je vais perdre l'accès !!

Merci de m'aider à généré mes certificats auto-signés pour que je puisse avoir l'accès à ma plate-forme ?

Dans mon fichier de configuration httpd.conf j'ai cela :

SSLEngine On

SSLCertificateFile « C:/Program Files/Apache Software Foundation/Apache2.2 /conf/ssl/pmf.cer »

SSLCertificateKeyFile « C:/Program Files/Apache Software Foundation/Apache2.2 /conf/ssl/pmf.key »

SSLCACertificateFile « C:/Program Files/Apache Software Foundation/Apache2.2 /conf/ssl/ca_trusted/root.pem »

SSLCACertificatePath « C:/Program Files/Apache Software Foundation/Apache2.2

Dans ca_trusted j'ai :

root.pem

ejbca.pem

Vraiment je ne sais pas comment généré tous ces fichiers ?

Aider moi je vous serais très reconnaissant car je suis bloquer

Répondre

Ping :Activation https pour apache2 | DeusPullum

Ping :Configurer le SSL avec Apache 2 | WordPress

D@v
16/12/2014 à 17:00
Permalink

Bonjour

bon article, simple , clair et concis.
Par contre, il faudrait lui faire une mise à jour importante concernant la sécurité !
L'actualité SSL est très riche ces derniers temps avec notamment la faille SSL V3 (poodle)
De plus la commande openssl indiqué génère une signature en SHA1, c'est trop faible maintenant. Tout comme MD5.
Préciser aussi de désactiver le RC4.

Par exemple:

Generation certificat avec cle RSA 2048 bits et sha256
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key

Et dans la conf apache:
SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off

Un site intéressant pour auditer son site HTTPS:
https://www.ssllabs.com/ssltest/index.html

Répondre

Florent_ATo
08/01/2015 à 11:43
Permalink

Je rejoins le commentaire de D@v ci-dessus. Il me semble impératif de le mettre à jour en accord avec les dernières recommandations sur le plan de la sécurité.

Pour compléter ce dernier, il serait opportun de préciser la version minimale de OpenSSL: 1.0.1j (version « J »).

Répondre

Zala
30/01/2015 à 16:40
Permalink

Très bon tuto, merci bien ! Le même bientôt pour NGinX ? 🙂

Répondre

Maurice
08/04/2015 à 18:20
Permalink

Je trouve vos explications simples mais j'ai suivi le tutoriel et ca n'a pas marché. Je sais que le problème est à mon niveau car je n'ai jamais fais un truc pareil et que les installations pour le site ont été faites auparavant sans moi.
Est-ce parce que je me connecte en ssh pour faire les manipulations?

Répondre

Mickael Dorigny
08/04/2015 à 18:24
Permalink

Bonjour Maurice,

Non pas de lien avec le SSH. Je te propose de poster ton problème en détail sur notre forum, plus de gens pourront t'aider ainsi :). Et soit bavard en détail, n'oublie de vérifier tes logs, plus on a d'info, mieux c'est 🙂

http://www.it-connect.fr/forum/apache-f19.html
A bientôt

Répondre

pringles
01/05/2015 à 00:05
Permalink

Aider moi je ne peut plus enlever la redirection http ver https comment faire vite

Répondre

Mickael Dorigny
01/05/2015 à 00:47
Permalink

Bonjour,

Il me semble que la redirection présentée ici est un type de redirection enregistrée par les navigateurs web. Autrement dit quand le serveur répond par une redirection, le navigateur va savoir, la prochaine fois qu'il ira sur telle page, qu'il sera redirigé, il met donc l'information en cache et le fait tout seul les fois d'après.

Si tu as bien enlevé la configuration de ton vhost et redémarré le service Apache, je te conseil de bien vider ton cache navigateur, et d'essayer avec un autre navigateur, voir un autre PC pour valider que cela ne vient plus du serveur.

Répondre

Esteban
26/07/2015 à 23:16
Permalink

Salut, merci pour les tutos !

J'aimerais faire la démarche inverse: déactiver le ssl de mon serveur apache2. (Temporairement). Auriez-vous une solution? En fait le contraire de « a2ensite default-ssl »

Répondre

Serge Clercin
31/07/2016 à 17:32
Permalink

Merci pour cet article parfaitement clair.
Je suis retraité depuis quelques années et l'informatique fait partie de mes passe-temps.

J'ai visité pas mal de site avant de trouver celui-ci pour passer en https.

Bonne continuation.

Répondre

Laisser un commentaire

Commentaire

Nom *

Adresse de messagerie *

Site web

Enregistrer mon nom, mon e-mail et mon site web dans le navigateur pour mon prochain commentaire.

Je ne suis pas un robot
reCAPTCHA
Confidentialité - Conditions

Laisser un commentaire

Ce site utilise Akismet pour réduire les indésirables. En savoir plus sur comment les données de vos commentaires sont utilisées.

Espace annonceurs
Offres d'emploi
Politique de confidentialité
Rejoignez-nous !
Soutenir IT-Connect
Flux RSS des articles
RSS des commentaires
Site de WordPress-FR