Бесплатный SSL-сертификат от Letsencrypt для Apache

При попытке установить сертификат, выяснилось, что клиент py27-letsencypt заменён на py27-certbot и теперь обновление сертификатов *letsencrypt* делаем так.

Проект *letsencrypt*, даёт возможность свободно получить SSL/TLS сертификаты. Цель сделать шифрованное соединение максимально доступным. Проект развивается. На FreeBSD ставится клиент letsencrypt, ему нужны 80 и 443 порты. Через него запрашиваются и скачиваются сертификаты для указанных доменов. Пока сертификаты ставим в ручную, но в будущем letsencrypt обещает процесс полностью автоматизировать.

Устанавливаем *certbot*:

```
root@tst: cd /usr/ports/security/py-certbot
root@tst: make install clean
```

Запускаем:

```
root@tst: certbot certonly --agree-tos --email postmaster@tst-amo.pp.ua -d tst-amo.pp.ua
```

Увидим процесс, если выбираем пункт (1), то – предварительно останавливаем вебсервер :

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log

How would you like to authenticate with the ACME CA?
-------------------------------------------------------------------------------
1: Spin up a temporary webserver (standalone)
2: Place files in webroot directory (webroot)
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
Starting new HTTPS connection (1): acme-
```

```
v01.api.letsencrypt.org
Obtaining a new certificate
Performing the following challenges:
tls-sni-01 challenge for tst-amo.pp.ua
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved
at
  /usr/local/etc/letsencrypt/live/tst-amo.pp.ua/fullchain.pem.
Your
 cert will expire on 2017-10-08. To obtain a new or tweaked
version
 of this certificate in the future, simply run certbot again.
To
 non-interactively renew *all* of your certificates, run
"certbot
 renew"
 - If you like Certbot, please consider supporting our work
by:

Donating to ISRG / Let's Encrypt:
https://letsencrypt.org/donate
 Donating to EFF: https://eff.org/donate-le
```

Когда установка SSL сертификата Apache будет завершена, вы найдете созданные файлы сертификатов в папке /usr/local/etc/letsencrypt/live. В этой папке будут четыре файла (точнее ссылки на них):

cert.pem - ваш сертификат домена;
chain.pem - сертификат цепочки Let's Encrypt;
fullchain.pem - cert.pem и chain.pem вместе;
privkey.pem - секретный ключ вашего сертификата.

Вставляем сертификаты в Апач.

Теперь вы можете зайти на сайт по https. Чтобы проверить как работает SSL и правильно ли выполнена установка ssl сертификата на сайт, вы можете открыть в браузере такую ссылку:

https://www.ssllabs.com/ssltest/analyze.html?d=example.com&latest

Установка SSL/TLS сертификата на сервер для каждого из доменов

Пробрасываем, и/или открываем 80 443 порты в httpd-vhosts.conf, для нужных доменов прописываем:

```
#site.ru
<VirtualHost *:80>
    ServerName site.ru
    DocumentRoot «/site.ru/site.ru»
    Redirect permanent «/» «https://site.ru/»
</VirtualHost>
<VirtualHost *:80>
    ServerName www.site.ru
    DocumentRoot «/site.ru/site.ru»
    Redirect permanent «/» «https://site.ru/»
</VirtualHost>
<VirtualHost *:443>
    ServerName www.site.ru
    DocumentRoot «/site.ru/site.ru»
    Redirect permanent «/» «https://site.ru/»
                                        SSLCertificateFile
/usr/local/etc/letsencrypt/live/site.ru/fullchain.pem
                                    SSLCertificateKeyFile
/usr/local/etc/letsencrypt/live/site.ru/privkey.pem
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3
</VirtualHost>
<VirtualHost *:443>
    SecRuleEngine On
    ServerName site.ru
    ServerAlias www.site.ru
    ServerAdmin admin@site.ru
    DocumentRoot «/site.ru/site.ru»
    ErrorLog «/var/log/site.ru-error_log»
    CustomLog «/var/log/site.ru-customlog» combined
                                        SSLCertificateFile
/usr/local/etc/letsencrypt/live/site.ru/fullchain.pem
                                    SSLCertificateKeyFile
/usr/local/etc/letsencrypt/live/site.ru/privkey.pem
    SSLEngine on
```

```
    SSLProtocol all -SSLv2 -SSLv3
…
</VirtualHost>
```

Производится редирект с 80 на 443 для всех запросов, также реализованна склейка www и не www как для http так идля https. Модуль mod_rewrite не используем, не рекомендуется, всегда есть альтернативы.

Сертификат выдаётся на 3 месяца, далее делаем обновление, или заранее настраиваем автообновление через *скрипт + crontab*. Обновление действует следующие 3 месяца.

Для проверки можно запустить скрипт

```
/usr/local/bin/certbot renew --dry-run
```

Если отработает нормально – ставим и задачу в cron, и перезагрузку Apache

```
crontab -e

31 1 8 * * /usr/home/svm/bin/certbot.sh
32 1 8 * * /usr/local/sbin/apachectl reload
```

Сам скрипт:

```
#!/bin/sh
/usr/local/bin/certbot renew
```

```
root@tst: certbot renew
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-------------------------------------------------------------------------------
Processing     /usr/local/etc/letsencrypt/renewal/tst-amo.pp.ua.conf
-------------------------------------------------------------------------------
Cert not yet due for renewal

The following certs are not due for renewal yet:
  /usr/local/etc/letsencrypt/live/tst-amo.pp.ua/fullchain.pem
```

(skipped)
No renewals were attempted.

Проверяем, например, на сайтах

https://www.sslshopper.com/
https://rus.gogetssl.com/check-ssl-installation/