Let's Encrypt

Let’s Encrypt (в переводе с английского: Давайте шифровать) — центр сертификации, начавший работу в бета-режиме с 3 декабря 2015 года, предоставляющий бесплатные криптографические сертификаты X.509 для TLS шифрования (HTTPS). Процесс выдачи сертификатов полностью автоматизирован.

Проект Let’s Encrypt создан для того, чтобы большая часть интернет-сайтов смогла перейти к шифрованным подключениям (HTTPS). В отличие от коммерческих центров сертификации, в данном проекте не требуется оплата, переконфигурация веб-серверов, использование электронной почты, обработка просроченных сертификатов, что делает процесс установки и настройки TLS-шифрования значительно более простым. Например, на типичном веб-сервере на базе Linux, требуется исполнить две команды, которые настроят HTTPS шифрование, получат и установят сертификат примерно за 20-30 секунд.

Пакет с утилитами автонастройки и получения сертификата включён в официальные репозитории дистрибутива Debian. Разработчики популярных браузеров, Mozilla и Google намерены постепенно отказаться от поддержки незашифрованного протокола HTTP путём отказа от поддержки новых веб-стандартов для http-сайтов.

https://letsencrypt.org/

Let's Encrypt wildcard

Certbot

Certbot — набор скриптов для автоматизации процессов создания и обновления сертификатов Let's Encrypt.

https://certbot.eff.org

Certbot documentation

acme.sh

acme.sh альтернатива Certbot

https://github.com/Neilpang/acme.sh

Центр сертификации Let’s Encrypt [АйТи бубен]

Apache

Настройка Apache под Debian 8 (jessie).

Примеры файлов здесь.

Debian 9 (stretch)

1. Устанавливаем необходимые пакеты:

```
apt-get install certbot python-certbot-apache
```

2. Настраиваем Apache:

```
certbot --apache
```

Проверка:

- Список сертификатов и возможность их обновления (automatic renewal)

```
certbot renew --dry-run
```

- Данные о задании автообновления

```
systemctl list-timers grep certbot.timer
```

---

https://certbot.eff.org/lets-encrypt/debianstretch-apache

Debian 8 (jessie)

CertBot: Apache on Debian 8 (jessie)

1. Устанавливаем необходимые пакеты:

```
apt-get install python-certbot-apache -t jessie-backports
```

Если необходимо, то модно установить пакет с документацией:

```
apt-get install python-certbot-doc
```

2. Настраиваем Apache:

```
certbot --apache
```

В процессе настройки программа будет задавать ряд вопросов.

Если возникает ошибка:

```
Expected </VirtualHost> but saw </VirtualHost></IfModule>
```

Нужно выполнить:

```
for f in /etc/apache2/sites-available/*; do sed -i '$a\' "$f"; done
```

и повторить команду настройки.

В случае успешной установки вы увидите поздравление:

```
Congratulations! You have successfully enabled
https://wiki.yola.ru
```

А также предложение выполнить анализ вашего сайта:

```
You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=wiki.yola.ru
```

Debian 7 (wheezy)

Настройка Apache под Debian 7 (wheezy).

Apache on Debian 7 (wheezy)

Почтовые серверы

Использование сертификатов для почтовых серверов:

- Dovecot
- Postfix

Тестирование:

```
openssl s_client domain.ru:443
openssl s_client -starttls smtp -connect domain.ru:587
```

Сертификаты Let'sEncrypt и Postfix,Courier-pop/imap или Dovecot | Блокнот обычного админа =)

Добавление домена


```
certbot --apache -d example.com -d www.example.com
```

Обновление сертификата

Поскольку сертификат Let's Encrypt выдаётся на 90 дней, нужно настроить автоматическое обновление сертификата.

В пакете для Debian присутствует файл настройки для Cron который выполняет процедуру проверки срока действия сертификата и выполняет его обновление только в том случае, если до окончания действия сертификата остаётся 30 или менее дней. Протокол выполнения процедуры обновления записывается в файл `/var/log/letsencrypt/letsencrypt.log`. Вот это файл для Cron:

/etc/cron.d/certbot

```
# /etc/cron.d/certbot: crontab entries for the certbot package
#
# Upstream recommends attempting renewal twice a day
#
# Eventually, this will be an opportunity to validate certificates
# haven't been revoked, etc.  Renewal will only occur if expiration
# is within 30 days.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system && perl -e 'sleep
int(rand(3600))' && certbot -q renew
```

Ручное обновление

Также можно вручную настроить Cron, вот пример:

```
1 4 * * 1 /usr/bin/certbot renew >> /var/log/letsencrypt/certbot-renew.log
```

Замена файлов ключа после обновления

Замена файлов ключа в Apache:

apache-ssl_keys-change.sh

```
#!/bin/bash

prefix='domain.ru'                # префикс
file_private='privkey.pem'        # имя файла ключа
file_cert='cert.pem'              # имя сертификата

path1=/etc/letsencrypt/live/      # путь к исходным файлам
path2_private=/etc/ssl/private/   # путь конечным файлам  private
path2_cert=/etc/ssl/certs/        # путь конечным файлам  cert

file1_private=$path1$prefix/$file_private            # полный путь и имя исходного ключа
file1_cert=$path1$prefix/$file_cert                  # полный путь и имя исходного сертификата
file2_private=$path2_private$prefix"_"$file_private  # полный путь и имя конечного ключа
file2_cert=$path2_cert$prefix'_'$file_cert           # полный путь и имя конечного сертификата


cp -f $file1_cert $file2_cert
cp -f $file1_private $file2_private
chmod 0600 $file2_private

service apache2 reload
```

TLS-SNI-01 validation is reaching end-of-life

Нужен `certbot` версии старше 0.28

certbot-update.sh

```
#!/bin/bash

apt-get remove certbot
cd /usr/local/sbin
wget https://dl.eff.org/certbot-auto
chmod a+x certbot-auto
```

Выполняем для проверки:

```
/usr/local/sbin/certbot-auto renew
```

Пример задания для Cron

```
0 0,12 * * * /usr/bin/python -c 'import random; import time; time.sleep(random.random() * 3600)'
&& /usr/local/sbin/certbot-auto renew
```

How to stop using TLS-SNI-01 with Certbot - Client dev - Let's Encrypt Community Support

Install Certbot for Apache on Debian 8 (jessie)

IdenTrust DST Root CA X3 2021-09-30

30 сентября 2021 конец срока действия IdenTrust DST Root CA X3.

Тест:

```
faketime -f '@2021-10-01 00:00:00' curl https://letsencrypt.org/
```

Чтобы проверить наличие сертификата ISRG Root X1 в числе доверенных:

```
awk -v cmd='openssl x509 -noout -subject' ' /BEGIN/{close(cmd)};{print | cmd}' < /etc/ssl/certs/c
```

Решение

- Вариант 1:

  В файле `/etc/ca-certificates.conf` нужно найти строчку:

  ```
  mozilla/DST_Root_CA_X3.crt
  ```

  и поставить в начало сроки символ «!»:

  ```
  !mozilla/DST_Root_CA_X3.crt
  ```

  Далее, необходимо выполнить команду:

  ```
  sudo update-ca-certificates
  ```

- Вариант 2:

  Установить новый сертификат ISRG Root X1 (до 2035-06-04).
  источник, источник 2

Устаревание корневого сертификата IdenTrust приведёт к потере доверия к Let's Encrypt на старых устройствах

30 сентября: Let's Encrypt и конец срока действия IdenTrust DST Root CA X3 / Хабр

Ссылки

https://ru.wikipedia.org/wiki/Let's_Encrypt

Certbot: An automatic client for enabling HTTPS on your website.

https://wiki.debian.org/ru/LetsEncrypt

Установка ssl сертификата Apache от Lets Encrypt

Создание сертификата Let’s Encrypt для Apache в Debian 8

Letsencrypt: Expected </VirtualHost> but saw </VirtualHost></IfModule>

https://github.com/sprokhorov/zabbix_letsencrypt

How To Secure Nginx with Let's Encrypt on Debian 8

opennet.ru: Вступили в силу требования к удостоверяющим центрам по проверке CAA-записей в DNS

opennet.ru: Использование CAA записей в DNS для защиты от генерации фиктивных HTTPS-сертификатов

opennet.ru: Let's Encrypt занял 36% рынка удостоверяющих центров

opennet.ru: Проект Let's Encrypt ввёл в строй протокол ACMEv2 и поддержку масок

How to secure Postfix using Let's Encrypt - UpCloud

wiki.calculate-linux: Let's Encrypt - получение бесплатного сертификата

http://sysadminmosaic.ru/letsencrypt/letsencrypt

2021-10-04 16:37