Получение сертификата Let's Encrypt для HTTPS при помощи Certbot в FreeBSD 14.1

Сайт по незащищенному протоколу HTTP ? Любой сайт должен работать через HTTPS, а для этого нужен сертификат которому доверяют веб-браузеры. Существует сервис Let's Encrypt который выдает бесплатно сертификаты для сайта сроком на 3 месяца, а после можно бесплатно их перевыпустить. Для управления и автоматического обновления сертификатов существует утилита Certbot. В статье будет рассмотрена работа Certbot в FreeBSD и настройка nginx для работы с HTTPS протоколом.

Оглавление статьи:

1. Установка Certbot

Устанавливаем через пакеты

```
pkg install py311-certbot
```

Или устанавливаем из портов

```
cd /usr/ports/security/py-certbot/ && make install clean
```

После установки было выведено сообщение: что можно установить плагины для автоматической настройки Apache или Nginx, как включить автоматическое обновление сертификатов.

FreeBSD certbot успешно установлен, выедено сообщение как включить автоматическое

В статье будет показан процесс ручной настройки и добавление сертификатов в веб-сервер nginx и включение автоматического обновления сертификатов Let's Encrypt.

2. Создание аккаунта Let's Encrypt

Создаем аккаунт командой:

```
certbot register
```

Указываем свой email адрес

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): tommywirser@notby.net
```

Соглашаемся с договором по использованию Let's Encrypt

```
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

Отказываемся от передачи своего email адреса и получения новостей и рекламы

```
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
```

```
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
```

Аккаунт успешно создан.

3. Получение сертификата для сайта

Для получения сертификата используем команду:

```
certbot certonly -d notby.net
```

где **notby.net** — доменное имя сайта для которого необходимо выпустить сертификат Let's Encrypt.

Будет преложено два варианта как проверить собственность доменного имени сайта:

1. запустить встроенный веб-сервер certbot (не походит, так как уже есть рабочий веб-сервер);
2. использовать рабочий веб-сервер, например nginx.

Выбираем 2 вариант

Далее необходимо указать путь до каталога сайта. В каталоге сайте будет создан каталог .well-known/acme-challenge/ с файлами для проверки домена.

Указываем каталог сайта

Image not found or type unknown

Получение сертификата Let's Encrypt для домена notby.net командой “certbot certonly -d

Нажимаем `Enter` и дожидаемся завершение процесса получения сертификата.

Image not found or type unknown

Консоль FreeBSD, сертификат Let's Encrypt успешно получен для домена notby.net, путь

Сертификат Let's Encrypt успешно выдан сроком на 3 месяца.

Аналогично происходит получение сертификатов для других сайтов, если это необходимо. Можно получить сертификаты для неограненного количества сайтов.

Если во время получения сертификата произошла ошибка, возможны следующие причины:

- Для утилиты certbot недостаточно прав на создание каталога проверки домена внутри каталога сайта;
- Невозможно получить доступ по URL адресу http://<домен>/.well-known/acme-challenge/.

Проверяем что каталог сайта имеет права как минимум 5 (r-x) для пользователя веб-сервера или любых пользователей.

```
ls -lh /usr/local/www/
```

```
drwxr-x---  2 www www  1.0K Feb 21 12:33 notby.net
```

Добавляем в конфигурацию nginx в раздел настроек сайта следующие строки:

```
location /.well-known {
root /usr/local/www/notby.net/; # Каталог сайта.
}
```

4. Настройка nginx для работы с HTTPS

Настраиваем nginx на обслуживания сайта через HTTPS по 443 порту с указанием путей сертификатов Let's Encrypt и перенаправление всего трафика с HTTP на HTTPS.

Открываем **конфигурационный файл настроек для сайта** или **nginx.conf**, вносим измерения в раздел настроек сайта

```
# Вместо домена notby.net указывай свой домен сайта.
# Блок server для домена notby.net по 80 порту (HTTP).
server {
listen 80; # Порт сервера.
server_name notby.net; # Домен сайта.

# Настройка location для получения Let's Encrypt сертификата через HTTP, можно перенести в раздел HTTPS.
# Каталог .well-known будет создан certbot'ом на время получения сертификата Let's Encrypt.
location /.well-known {
```

```
    root /usr/local/www/notby.net/;
  }

  #Перенаправление всего трафика с http на https.
  location / {
    return 301 https://$host$request_uri;
  }
}

# Блок server для домена notby.net по 443 порту (HTTPS).
server {
  listen 443 ssl; # 443 порт, поддержка SSL.
  http2 on; # Использовать HTTP/2.
  server_name notby.net; # Домен сайта.

  # Пути к списку сертификатов, на моменте выдачи сертификата они были указаны.
  ssl_certificate /usr/local/etc/letsencrypt/live/notby.net/fullchain.pem;
  ssl_certificate_key  /usr/local/etc/letsencrypt/live/notby.net/privkey.pem;
  # Сертификат для параметра ssl_stapling
  ssl_trusted_certificate /usr/local/etc/letsencrypt/live/notby.net/chain.pem;

  ssl_protocols TLSv1.3; # Разрешенные протоколы (только TLS 1.3).
  ssl_prefer_server_ciphers off; # Использовать клиентские шифры.

  # OCSP stapling, для ssl_stapling обязательный ssl_trusted_certificate параметр.
  ssl_stapling on;
  ssl_stapling_verify on;

  # Настройки location оставляем как было раньше или меняем если что-то нужно поменять. -:)

  location / {
    root  /usr/local/www/notby.net/; # Каталог сайта.
    index  index.html index.php; # Файлы в качестве индекса.
  }

  location ~ \.php$ {
    fastcgi_pass  unix:/var/run/php-fpm.sock;
    fastcgi_param  SCRIPT_FILENAME /usr/local/www/notby.net/$fastcgi_script_name;
    include    fastcgi_params;
  }
```

```
}
```

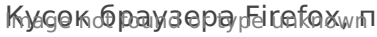
Сохраняем файл и перезапускаем веб-сервер nginx

```
service nginx restart
```

5. Проверка HTTPS и перенаправление с HTTP

Открываем в веб-браузере свой сайт по протоколу **http**://<адрес сайта>/, должно произойти автоматическое перенаправление на **https**://<адрес сайта>/

Нажимаем значок рядом с адресом сайта и видим что сайт работает по защищенному соединению с сертификатом Let's Encrypt.



Кусок браузера Firefox, проверка наличия сертификата сайта notby.net, соединение защ

Теперь все пользователя будет автоматически перенаправлятся на HTTPS протокол, даже не заметив каких-то измерений.

Поисковые системы также со временем изменят протокол сайта или можно зайти в панель управления сайтами в поисковой системе и указать что сайт переехал на HTTPS.

6. Проверка обновлений сертификатов

После настройки веб-сервера запускаем проверку получения нового сертификата

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

Параметр **--dry-run** указывает что будет происходить симуляция получения нового сертификата.

Симуляция получения нового сертификата командой “certbot renew --dry-run”, тестовое

Тестовое получение сертификата успешно пройдено.

7. Автоматическое обновление сертификатов

Утилиту Certbot необходимо добавить в файл **/etc/periodic.conf** (периодическое выполнение заданий), чтобы она автоматически перевыпустила сертификаты сайтов, срок действия которых заканчивается.

Открываем в текстовом редакторе файл **/etc/periodic.conf** или создаем его

```
nano /etc/periodic.conf
```

Добавляем строку

```
weekly_certbot_enable="YES"
```

Открыт файл /etc/periodic.conf в текстовом редакторе nano, добавлена строка weekly_cer

Сохраняем файл. Теперь раз в неделю будет происходить проверка сертификатов сайтов и если сертификату остается меньше двух недель, он будет обновлен автоматически.

8. Изменение email адреса аккаунта

Если в дальнейшим потребуется изменить email адрес аккаунта Let's Encrypt, используем команду:

```
certbot update_account --email new@email.com
```

где **new@email.com** — новый email адрес.

Будет предложено подписатся на новости и немного рекламы, отвечаем **N** если неинтересно.

Обновление email адреса аккаунта Let's Encrypt командой “certbot update_account --emai

Email адрес успешно обновлен.

Revision #1
Created 29 September 2025 09:26:17 by buzz

Updated 29 September 2025 09:27:54 by buzz