How to get a Let's Encrypt certificate while using CloudFlare

Issuance Tech

jgrahamc 2015-12-08 16:28:54 UTC #1

This seems to have come up a couple of times so here's how to do it.

It's not necessary to disable CloudFlare to use Let's Encrypt.

If you're configuring Let's Encrypt for the first time for a site already active on CloudFlare, all that is needed to successfully verify and obtain your certificate and private key pair is to use the webroot method for verification.

Download `certbot`, the recommended Let's Encrypt client and change to the download directory:

```
wget https://dl.eff.org/certbot-auto
chmod a+x certbot-auto
```

(OS-specific instructions can be found on the **`certbot` homepage**.)

Run the script for automatic installation:

```
./certbot-auto
```

Using the `certbot` client with the `certonly` command and the `--webroot` flag, we're able to verify and obtain the cert/key pair using HTTP verification. An example command might look like:

```
./certbot-auto certonly --webroot --webroot-path /usr/share/nginx/html/ --renew-by-de
```

where

`--webroot-path` is the directory on your server where your site is located (nginx used in the example)
`--renew-by-default selects` renewal by default when domains are a superset of a previously attained cert
`--email` is the email used for registration and recovery contact.
`--text` displays text output
`--agree-tos` agrees to Let's Encrypt's Subscriber Agreement
`-d` specifies hostnames to add to the SAN.

Successful completion of this verification method will show text similar to the following:

```
IMPORTANT NOTES
- Congratulations! Your certificate and chain have been saved at
/etc/letsencrypt/live/example.tld/fullchain.pem. Your cert will expire on
2016-03-03. To obtain a new version of the certificate in the future, simply
run Let's Encrypt again.
```

As a note, both the cert and key will be saved to /etc/letsencrypt/live/example.tld/ . After both have been obtained, you'll need to manually update your virtual host to use this key/cert pair.

I have installed Let's Encrypt SSL. Can I use cloudflare with it?

Letsencrypt with cloudfare

The server could not connect to the client to verify the domain

Installing LE SSL Cert in a VPS while using ClouFlare

I have installed Let's Encrypt SSL. Can I use cloudflare with it?

What's an automated renewal?

Cerbot renewal dry run error

Dry-run cert renewal shows incorrect challenge

Need to generate cert for Windows Xampp install

How can I update my certbot in fedora 25

jsha 2015-12-09 23:33:01 UTC #2

NextStarTechnologies 2016-01-01 23:25:45 UTC #3

For what it's worth I chased my tail with this for a bit… I kept getting an error:
Error: The server could not connect to the client to verify the domain
Turning off CloudFlare SSL support did the trick

baldengineer 2016-01-17 20:02:40 UTC #4

I'm running discourse with cloudflare as my cdn. I generated my cert before enabling cloudflare, which was relatively simple. However, now I can't renew.

Any ideas what to use for the --webroot_path when running discourse? I can't seem to find a directory or path that discourse is using for nginx.

Koyaanis 2016-02-07 00:01:36 UTC #5

Hello I followed all steps and made it to the congratulations part. I now have 4 files saved at /etc/letsencrypt/live/DOMAIN/ called: cert.pem, chain.pem, fullchain.pem and privkey.pem.

When looking at my config file at /etc/nginx/sites-available/default I have these 2 lines:
```
ssl_certificate cert.pem;
ssl_certificate_key cert.key;
```
I do have the cert.pem file but what about the cert.key? I can't seem to find it.

Help much appreciated.

sahsanu 2016-02-07 00:56:55 UTC #6

Hello **@Koyaanis** ,

As you are using nginx, in `ssl_certfile` directive you should specify the **fullchain.pem** file (it includes your domain cert and the intermediate cert). And for `ssl_certificate_key` directive you should specify the **privkey.pem** file:

```
ssl_certificate /etc/letsencrypt/live/HEREYOURDOMAIN/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/HEREYOURDOMAIN/privkey.pem;
```

Note: Use always the full path to the cert files.

Cheers,
sahsanu

Koyaanis 2016-02-07 03:57:35 UTC #7

Thanks a lot that worked!

---

rugk 2016-02-07 22:18:47 UTC #8

You should also suggest to set Cloudflares SSL mode at least to “Full SSL (Strict)” or (better) use keyless SSL. Because all other SSL options of Cloudflare are very flawed and always keep in mind that Cloudflare man-in-the-middles your “secure” connection.

More at **@scotthelme** ’s blog:

> **CloudFlare's great new features and why I won't use them**
>
> CloudFlare recently announced two great new features, Keyless SSL and Universal SSL. Here's why I won't use them.

---

andrewjs18 2016-03-20 22:53:53 UTC #9

Hi,

If we have sites loading from more than 1 web root, how do we specify this in the command? do I have to generate a new cert for every site that loads from a different web root?

---

sahsanu 2016-03-20 23:48:37 UTC #10

Hello **@andrewjs18** ,

> andrewjs18:
>
> If we have sites loading from more than 1 web root, how do we specify this in the command? do I have to generate a new cert for every site that loads from a different web root?

Take a look to `./letsencrypt-auto --help webroot` and you will see two options to specify a webroot per domain/domains.

Example using **-w** (**–webroot-path**):

```
./letsencrypt-auto here_your_options -w /var/www/domain.tld -d domain.tld -d
www.domain.tld -w /var/www/otherdomain.tld -d otherdomain.tld -d www.otherdomain.tld
```

Example using **–webroot-map**:

```
./letsencrypt-auto here_your_options --webroot-map
'{"domain.tld,www.domain.tld":"/var/www/domain.tld",
```

```
"otherdomain.tld,www.otherdomain.tld":"/var/www/otherdomain.tld"}'
```

Cheers,
sahsanu

---

andrewjs18 2016-03-21 03:08:53 UTC #11

Thank you. I'll give it a try tonight.

---

andrewjs18 2016-03-21 07:50:15 UTC #12

@sahsanu , not quite sure what I'm doing wrong here. when I run ./letsencrypt-auto, it asks me which sites I'd like to activate HTTPS for, I choose them, then it errors out with a similar error as I'll post below.

I then moved on to the instructions provided here: **How to get a Let's Encrypt certificate while using CloudFlare**

after doing so, it errored out, with the following: **http://pastebin.com/ARyRQTNe**

any help is greatly appreciated!

thanks!!!

---

gothic.ie 2016-03-21 08:55:20 UTC #13

again you (according to the error) tried tls authenticatinng (which only works if their is an existing cert)

instead of the previously advised webroot auth method

---

sahsanu 2016-03-21 08:59:08 UTC #14

Hello **@andrewjs18** ,

I recommend to put the options you will use in the command line and use the webroot method.

For example;

```
./letsencrypt-auto certonly --email youruser@yourdomain.tld --text --renew-by-default
--agree-tos --webroot -w /home/site/public_html/ -d mysite.com -d www.mysite.com -w
/home/site2/public_html/ -d sub1.mysite.com -w /home/site3/public_html/ -d
sub2.site.com -w /home/site4/public_html/ -d sub3.mysite.com --dry-run
```

Replace your email, your domain names and webroot path with the real ones and execute again the command. If you get no error you could remove the last parameter `--dry-run` and launch again the command (`--dry-run` option simulates all the process but doesn't issue the certificate so you can check that all will work fine once you are ready).

Cheers,
sahsanu

---

andrewjs18 2016-03-21 19:53:13 UTC #15

@sahsanu , thanks.

just tried rerunning the command…this time it returned a different error:

Failed authorization procedure. **sub.mysite.com** (http-01): urn:acme:error:unauthorized :: The client lacks sufficient authorization :: Invalid response from **http://sub.mysite.com/.well-known/acme-**

challenge/ZVeBvGjXcf_uoKZyrGcANNKrBt04l_2--OW8ccT_0yo [104.18.52.40]: 404

IMPORTANT NOTES:

- If you lose your account credentials, you can recover through e-mails sent to **email@me.com**.
- The following errors were reported by the server:

  Domain: **sub.mysite.com**
  Type: unauthorized
  Detail: Invalid response from **http://sub.mysite.com/.well-known/acme-challenge/ZVeBvGjXcf_uoKZyrGcANNKrBt04l_2–OW8ccT_0yo** [104.18.52.40]: 404

  To fix these errors, please make sure that your domain name was entered correctly and the DNS A record(s) for that domain contain(s) the right IP address.
- Your account credentials have been saved in your Let's Encrypt configuration directory at /etc/letsencrypt. You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Let's Encrypt so making regular backups of this folder is ideal.

---

sahsanu 2016-03-21 20:06:16 UTC #16

@andrewjs18 , the error is clear, the challenge can't be accessed to verify your domain.

Put a simple test file in `/path/to/document/root/for/sub.mysite.com/.well–known/acme–challenge/testfile` and try to access it using your web browser `http://sub.mysite.com/.well–known/acme–challenge/testfile`. If you get the content of testfile all is ok, if you receive a 404 Not found something is wrong in your conf.

Also, re-check that you wrote the correct webroot-path for your **sub.mysite.com** domain when you executed the letsencrypt-auto command.

Cheers,
sahsanu

---

andrewjs18 2016-03-21 20:16:57 UTC #17

@sahsanu ah…that's what it was, a slight directory issue in my command. thanks for all of your help!

I liked seeing this:

IMPORTANT NOTES:

- The dry run was successful.

---

sahsanu 2016-03-21 20:18:48 UTC #18

@andrewjs18 , you are welcome. I'm glad you get it working, now, remove `––dry–run` and get your certs 😉

---

andrewjs18 2016-03-21 20:24:29 UTC #19

@sahsanu , just finished that up.

when I go to automate the renewal of the certs, can I just stuff the same command I ran to get the certs into a file that's then set up in crontab?

---

pfg 2016-03-21 20:29:09 UTC #20

That would work, but `letsencrypt renew` is a better option since it's smarter about which options it uses, when it actually renews the certificates, etc.

Just put it in a daily cronjob, test it once, and you should be good to go. 😄

---

andrewjs18 2016-03-24 06:33:44 UTC #21

@pfg , do I need to include my other commands when running letsencrypt renew, like so:

./letsencrypt-renew certonly --email youruser@yourdomain.tld --text
–renew-by-default --agree-tos --webroot -w /home/site/public_html/ -d
mysite.com -d **www.mysite.com** -w /home/site2/public_html/ -d
sub1.mysite.com -w /home/site3/public_html/ -d **sub2.site.com** -w
/home/site4/public_html/ -d **sub3.mysite.com** --dry-run

---

pfg 2016-03-24 11:25:58 UTC #22

No, Let's Encrypt will try to renew using the settings you last used for your certificates. This should do:

```
./letsencrypt-auto renew
```

Take a look at the **documentation** for more details.

---

andrewjs18 2016-03-24 19:54:22 UTC #23

@pfg , perfect…thanks!

Bill_Hendricks 2016-08-11 14:23:07 UTC #24

How do you do it with certbot-auto?

If I've already installed it with certbot-auto by simply dissabling cloudflare to install it and then re-enable it…

Thanks.

Bill_Hendricks 2016-09-21 06:26:49 UTC #25

Has letsencrypt-auto been renamed certbot-auto? If not where are the installation instructions for letsencrypt-auto?

---

pfg 2016-09-21 06:59:58 UTC #26

Yes, the client was renamed a while back. Both commands are essentially compatible.

@jgrahamc I hope you don't mind - I've updated the instructions to account for the client rename and the new install instructions in order to avoid confusion.

---

jgrahamc 2016-09-21 08:05:27 UTC #27

Thank you for doing that. That's great.

TELunus 2017-03-02 09:04:35 UTC #28

Hmm, something's odd here. I seem to have a problem only when I do a dry-run?

- without --dry-run I get:
- but when I try with --dry-run I get:

This worries me somewhat, because of course it means I haven't been able to test `certbot renew` with `certbot renew --dry-run` as the latter gives me the same error as shown above.

---

tpilant 2017-03-02 22:40:29 UTC #29

I found that if you just disable the domain name to run thru cloudflare the certs will install without a problem. After finished installing then re-enable cloudflare pass thru

---

mnordhoff 2017-03-03 10:13:46 UTC #30

> TELunus:
>
> without --dry-run I get:

Since you've issued certificate(s) for those names recently, Let's Encrypt probably remembers that it's valid, and doesn't *actually* try to validate it again. (It currently remembers authorizations for 60 days, a number which will probably change in the future.)

> TELunus:
>
> but when I try with --dry-run I get:

… but when you use `--dry-run`, if you haven't recently issued any other staging certificates for those names, it *won't* remember and *will* validate them. (The staging server has a totally separate database of authorizations.)

And, obviously, validation fails.

http://minecraft.klippenstein.org/.well-known/acme-challenge/ and **http://philip.klippenstein.org/.well-known/acme-challenge/** both redirect to **https://minecraft.klippenstein.org.well-known/acme-challenge/**, an URL with an obviously invalid domain name. You can see for yourself with a web browser or something like `curl`.

it sounds like there's a missing "/" in your web server configuration. For example, maybe it has "`Redirect / https://minecraft.klippenstein.org`" where it should be "`Redirect / https://minecraft.klippenstein.org/`".

(You could also exclude `/.well-known/acme-challenge/` from the redirect, if you want. But i don't know how to do that in Apache off hand.)

Speaking of `--dry-run`, you've issued 3 identical certificates in the last couple days. If you keep doing that you'll start running into the **rate limits**. If you're testing things, you should make more use of `--dry-run` in the future.

---

ingber 2017-03-21 11:24:26 UTC #31

> sahsanu:
>
> ./letsencrypt-auto certonly --email youruser@yourdomain.tld --text --renew-by-default --agree-tos --webroot -w /home/site/public_html/ -d **mysite.com** -d **www.mysite.com** -w /home/site2/public_html/ -d **sub1.mysite.com** -w /home/site3/public_html/ -d **sub2.site.com** -w /home/site4/public_html/ -d **sub3.mysite.com** --dry-run

Thanks for this detail. I was having failures with sub-domains in subdirectories. However, I had to correct one glitch:

./letsencrypt-auto certonly --email youruser@yourdomain.tld --text --renew-by-default --agree-tos --webroot -w /home/site/public_html/ -d **mysite.com** -d **www.mysite.com** -w /home/site2/public_html/ -d **sub1.mysite.com** -w /home/site3/public_html/ -d **sub2.site.com** -w /home/site4/public_html/ -d **sub3.mysite.com** --dry-run\

This did not work unless I put in the explicit -w for **www.mysite.com**:

./letsencrypt-auto certonly --email youruser@yourdomain.tld --text --renew-by-default --agree-tos --webroot -w /home/site/public_html/ -d **mysite.com** -w /home/site/public_html/ -d **www.mysite.com** -w /home/site2/public_html/ -d **sub1.mysite.com** -w /home/site3/public_html/ -d **sub2.site.com** -w /home/site4/public_html/ -d **sub3.mysite.com** --dry-run

---

minamoto 2017-12-08 03:33:02 UTC #32

Hi

I'm running the following command:

```
certbot ––nginx certonly ––webroot ––webroot–path /home/domainname/public/public_htr
```

but I get the following error:

> Could not choose appropriate plugin: Too many flags setting configurators/installers/authenticators 'nginx' -> 'webroot'

I'm running nginx server under Ubuntu 16.10 with Cloudflare Pro Cache everything rule.

Any help?

---

jared.m 2017-12-08 05:49:21 UTC #33

This really should be a new topic, as it's almost entirely unrelated to the (very old) one you commented on.

However, the issue is you're sending both the --nginx and --webroot flags. These are two different plugins. I'm also confused why you're issuing --nginx at all, when you're also sending certonly. Certonly tells Certbot to explicitly not do anything that nginx would do, except for use nginx as an authenticator. However, you're using Cloudflare so you're (correctly) attempting to use the webroot authenticator.

Unless you have a compelling reason to need certonly, try this:

```
certbot –i nginx –a webroot ––webroot–path /home/domainname/public/public_html/ ––email my@email.com ––text ––agree–tos –d ...
```

Note that I left renew-by-default out. There are rather few reasons you actually want to use that flag, and it can lead to rate limit issues in many cases.

---

schoen 2017-12-08 19:24:02 UTC #34

> jared.m:
>
> Note that I left renew-by-default out. There are rather few reasons you actually want to use that flag, and it can lead to rate limit issues in many cases.

@minamoto , can you tell us where you found a suggestion to use `--renew-by-default`? Maybe we can write to whoever is mentioning it in documentation and get it changed. (`--renew-by-default` was confusingly named, I think originally by me, and has since been renamed to `--force-renewal`. It doesn't mean "enable autorenewal in the future", it means "force renewal of this certificate right now". The "by default" here means "without asking, even if it appears to be unnecessary".)

Sam9999 2018-02-21 21:49:45 UTC #35

I have read all this discussion and I have all time the some error. Domains are accessible and working but still have the error:

Failed authorization procedure. www.digestum.eu (http-01): urn:acme:error:connection :: The server could not connect to the client to verify the domain :: Fetching **http://www.digestum.eu/.well-known/acme-challenge/iUnQo6Fg8Mw3dktyNYKr_9N_nKeXt9FcdNpjo4AmEFo:** Timeout

Domains was under cludfare I have paused and after deleted under cloudfare, flushed the DNS on google, installed all certbot and cerbot-auto and try the --standalone with apache2 stopped, but all time the some error, maybe I have to put down the firewall, even is oper for the port 80 and 443 that works under apache2.
If don't work I have to delete/purge it ?

---

schoen 2018-02-22 00:35:30 UTC #36

> Sam9999:
>
> Failed authorization procedure. www.digestum.eu (http-01): urn:acme:error:connection :: The server could not connect to the client to verify the domain :: Fetching **http://www.digestum.eu/.well-known/acme-challenge/iUnQo6Fg8Mw3dktyNYKr_9N_nKeXt9FcdNpjo4AmEFo:** Timeout

You are advertising the IPv6 address 2001:b07:2ea:23a5:222:68ff:fe65:fab5 via an AAAA record in DNS, but your server is currently only reachable over IPv4, not IPv6. The certificate authority is trying to reach your server on IPv6 because of the AAAA record, and isn't able to.

Sam9999 2018-02-22 07:55:40 UTC #37

Hi,
I have put the file on
http://digestum.eu/.well-known/acme-challenge/ddYg5HJOsoLetr5EuxQOLpwwoLHIV-uTH0WC66_FOjQ
And is readable … I have to understand what you means, the domain is set on IP4 and IP6 in DNS but the IP is shared then the certificate authority can read the file only over domain… as all others.
Do you means that is better to delete the IP6 AAAA record from DNS?

ha ok… now work:
IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/digestum.eu/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/digestum.eu/privkey.pem

Your cert will expire on 2018-05-23. To obtain a new or tweaked version of this certificate in the future, simply run certbot-auto again. To non-interactively renew *all* of your certificates, run "certbot-auto 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**

---

schoen 2018-02-22 08:24:48 UTC #38

> Sam9999:
>
> Do you means that is better to delete the IP6 AAAA record from DNS?

The *very* best thing would be to make your site reachable over IPv6. 🙂

Sam9999 2018-02-22 08:52:54 UTC #39

I think that for that is not in me, because it's the provider, fastweb, that can allow that, mi web server I think work with IP6 too.
I have try and over IP6 is not redirect to me and mi webserver even I have a IP6 connected to me, I can see that in some web sites that show your ip6.
But I'll ask about that… tank you.
For now work and configured… **https://digestum.eu/**
After a problem now all is very simple…

---

cyl19910101 2018-02-27 02:30:45 UTC #40

I have a question related to this one that is: is it possible to verify a new sub-domain under CloudFlare with 1. "Always use HTTPS" is on. 2. SSL full(strict) mode?

I tried to get an SSL by choosing "Place files in webroot directory", under the two options configured I mentioned above, Lets Encrypt's verification request will be redirect to something like **https://example.domain/.well-known/something**, and CloudFare will try to connect my server using https but the SSL isn't issued yet…

I've tried a page rule: "http://*example.domain/.well-known/*" – diable security, but it doesn't work…

I can temporarily disable "Always use HTTPS" while tring to get a certificate, that would work, just curious that if it's possible to do that with "Always use HTTPS" is on.

Patches 2018-02-27 04:10:57 UTC #41

Setting SSL mode to *flexible* temporarily should be a little less disruptive and continue to encrypt most of your origin connections, especially if you have to change the settings for a whole zone that is mostly working fine.

With a page rule you could set the SSL mode or Always HTTPS setting in a page rule for the entire subdomain temporarily while you're setting it up. I don't think the SSL settings are effective at the path level.

---

cyl19910101 2018-02-27 04:52:56 UTC #42

Thanks a lot for replying! Looks like change to flexible is a reasonable way to go.

For other readers information, please aware that if you redirect all http requests to https in your server and with flexible mode on you will get into infinite redirect loop, disable YOUR REDIRECT(not the CloudFlare redirect) before you switch to flexible mode.

---

minamoto 2018-03-01 03:13:39 UTC #43

> schoen:
>
> > jared.m:
> >
> > Note that I left renew-by-default out. There are rather few reasons you actually want to use that flag, and it can lead to rate limit issues in many cases.
>
> **@minamoto** , can you tell us where you found a suggestion to use `--renew-by-default`? Maybe we can write to whoever is mentioning it in documentation and get it changed. (`--renew-by-default` was confusingly named, I think originally by me, and has since been renamed to `--force-renewal`. It doesn't mean "enable autorenewal in the future", it means "force renewal of this certificate right now". The "by default" here means "without asking, even if it appears to be unnecessary".)

Hi.
No one mentioned that command.

I mixed some commands from the manual up and thought it would be working.
You are right BTW
