



Pramod Shehan

[Follow](#)Oct 5, 2022 · 3 min read · [Listen](#)[Save](#)

SSL enabled with Apache and Certbot(Let's Encrypt)



What is Let's Encrypt?

Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group.

It provides X.509 certificates for Transport Layer Security encryption at **no charge**. The certificate is **valid for 90 days**.

Install Apache and server maintain

- Execute the following command to install Apache2:

```
sudo apt install apache2
```

- Start and stop server

```
sudo systemctl stop apache2.service
sudo systemctl start apache2.service
```

- Check the status

```
sudo systemctl enable apache2.service
```

```
uvm104@uvm104:/etc/apache2/sites-available$ sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2022-10-05 10:28:53 EDT; 20min ago
     Main PID: 5302 (apache2)
       Tasks: 11 (limit: 4622)
    CGroup: /system.slice/apache2.service
            └─5302 /usr/sbin/apache2 -k start
               6901 /usr/sbin/apache2 -k start
               6903 /usr/sbin/apache2 -k start
               6913 /usr/sbin/apache2 -k start
               7029 /usr/sbin/apache2 -k start
               7030 /usr/sbin/apache2 -k start
               7036 /usr/sbin/apache2 -k start
               7037 /usr/sbin/apache2 -k start
               7074 /usr/sbin/apache2 -k start
               7075 /usr/sbin/apache2 -k start
               7076 /usr/sbin/apache2 -k start

Oct 05 10:28:53 uvm104 systemd[1]: Stopped The Apache HTTP Server.
Oct 05 10:28:53 uvm104 systemd[1]: Starting The Apache HTTP Server...
Oct 05 10:28:53 uvm104 apache2[5298]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' direct
Oct 05 10:28:53 uvm104 systemd[1]: Started The Apache HTTP Server.
```

- Go to `/etc/apache2/sites-available/` and create `domain.com.conf`.

```
<VirtualHost *:80>
```

```
DocumentRoot /var/www/html
```

```
ServerName <DOMAIN_NAME>.com
```

```
ServerAlias www.<DOMAIN_NAME>.com
```

```
ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
</VirtualHost>
```

```
uvm104@uvm104:/etc/apache2/sites-available$ ls
000-default.conf default-ssl.conf domain.com.conf domain.com-le-ssl.conf
uvm104@uvm104:/etc/apache2/sites-available$
```

after installed ssl certificate using certbot, `domain.com-le-ssl.conf` is generated.

- This is `domain.com-le-ssl.conf` file.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>

DocumentRoot /var/www/html
ServerName <DOMAIN_NAME>.com
ServerAlias www.<DOMAIN_NAME>.com

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

Include /etc/letsencrypt/options-ssl-apache.conf
SSLCertificateFile
/etc/letsencrypt/live/<DOMAIN_NAME>.com/fullchain.pem
SSLCertificateKeyFile
/etc/letsencrypt/live/<DOMAIN_NAME>.com/privkey.pem
</VirtualHost>
</IfModule>
```

[Open in app](#) ↗[Get unlimited access](#)

```
sudo a2dissite 000-default
```

- Enable new **domain.com.conf**

```
sudo a2ensite domain.com.conf
```

- After that we should need to restart the apache server.

Certbot installation and renewal process

- Install certbot

```
sudo apt install certbot python3-certbot-apache
```

- Here we are using apache plugin to configure the ssl certificate using certbot.

```
sudo certbot --apache
```

There are several steps to configure ssl certificates using apache.

1. configure email -> **add your email address**
2. Please read the terms of service -> **Y**
3. We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom
-> **N**

after that there is an another option to select the domain which we need to enable ssl certificates. Those domain names are retrieving from the domain.com.conf file.

4. Which names would you like to activate HTTPS for?

5. Please choose whether or not you want to redirect all HTTP traffic to HTTPS, removing HTTP access -> **2**

SSL certificates provided by Let's Encrypt are valid only for 90 days. The Certbot has a cronjob that will take care of renewing any SSL certificate that is within thirty days of expiration.

```
uvm104@uvm104:/etc/cron.d$ ls | grep cert
certbot
uvm104@uvm104:/etc/cron.d$
```

- This is the cronjob for certificate renewal.

```
# /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(43200))' && certbot -q renew
certbot (END)
```

- To check the status of this service and make sure it's active and running, you can use below command.

```
sudo systemctl status certbot.timer
```

```
uvvm104@uvvm104:/etc/cron.d$ sudo systemctl status certbot.timer
● certbot.timer - Run certbot twice daily
   Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
   Active: active (waiting) since Wed 2022-10-05 10:30:52 EDT; 51min ago
   Trigger: Wed 2022-10-05 16:47:41 EDT; 5h 24min left

Oct 05 10:30:52 uvvm104 systemd[1]: Started Run certbot twice daily.
uvvm104@uvvm104:/etc/cron.d$
```

- we can view all the systemctl timers like this.

```
sudo systemctl list-timers
```

```
uvvm104@uvvm104:/etc/apache2/sites-available$ sudo systemctl list-timers | grep certbot
Wed 2022-10-05 16:47:41 EDT 5h 37min left n/a n/a certbot.timer certbot.service
```

- To test the renewal process, you can do a dry run with certbot like this.

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

References

<https://pramodshehan.medium.com/ssl-enabled-with-nginx-and-certbot-lets-encrypt-c01031075112>

<https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-lets-encrypt-on-ubuntu-20-04>

Ssl Certificate Apache Certbot Lets Encrypt