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:

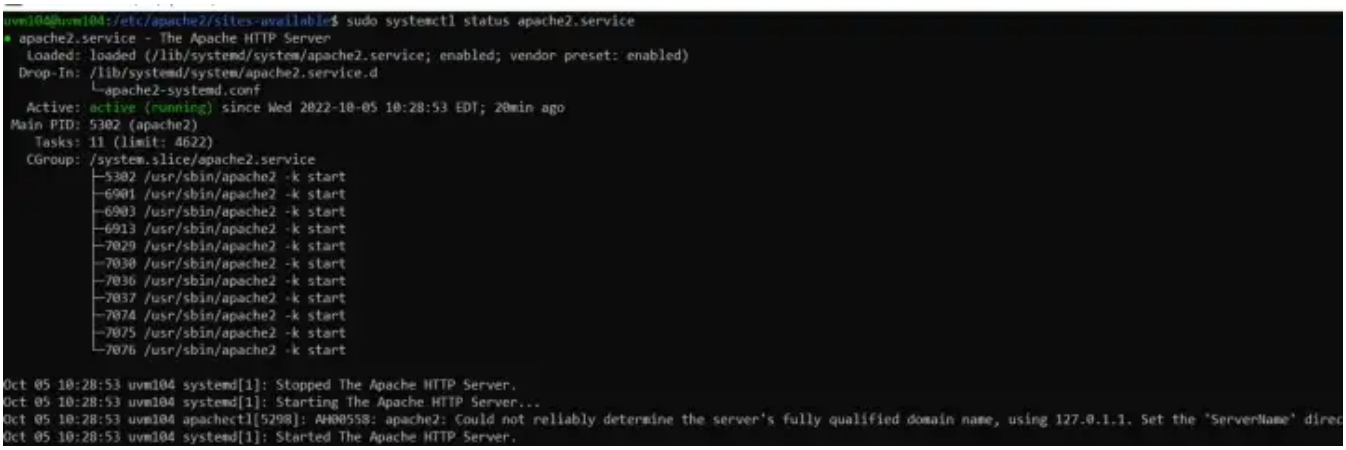
```
sudo apt install apache2
```

- Start and stop server

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

- Check the status

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

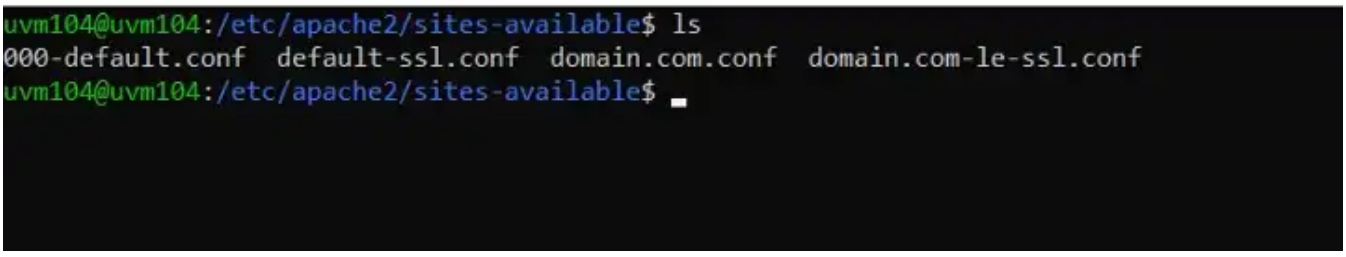


- Go to **/etc/apache2/sites-available/** and create **domain.com.conf**.

```
<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>
```



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>
```


```
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 to redirect 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$
```

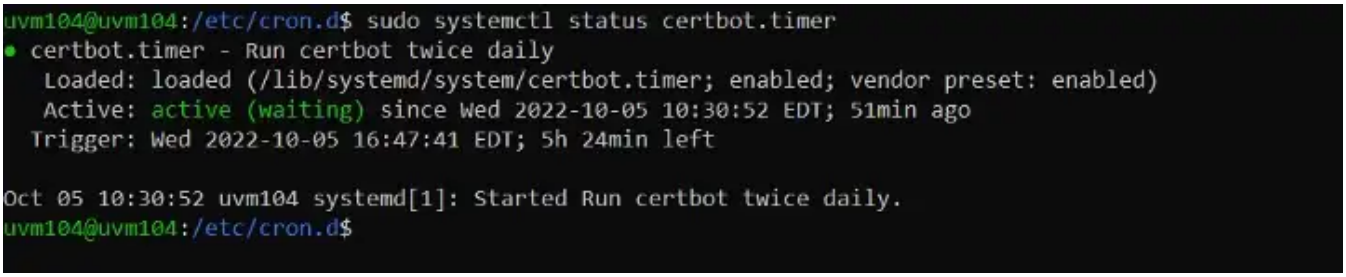
- This is the cronjob for certificate renewal.

```
# /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)
```

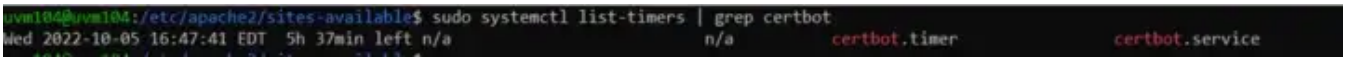
- To check the status of this service and make sure it's active and running, you can use below command.

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



- we can view all the systemctl timers like this.

```
sudo systemctl list-timers
```



- 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-let-s-encrypt-on-ubuntu-20-04

Ssl Certificate Apache Certbot Lets Encrypt