DEVOPS / HOW TO'S

FOLLOW:

NEXT STORY
Bash Scripting: Learn to use REGEX (Part 2- Intermediate)

PREVIOUS STORY
Configuring redis MASTER SLAVE setup

SEARCH BAR

To search type and hit enter

FACEBOOK FAN PAGE

Linuxtechlab

Complete guide to configure SSL on Nginx with Let’s Encrypt

(Ubuntu/Centos/RHEL)

BY SHUSAIN · PUBLISHED DECEMBER 11, 2018 · UPDATED DECEMBER 13, 2018

Securing your websites with an SSL certificate is now a must for all website admins, else the web browsers will mark the website as unsafe to visit, causing the loss of website traffic. But SSL certificate is not cheap, but there is a way around to get an SSL certificate for free with only downside that we need to renew SSL cert every 90 days but that process can also be automated.

In this tutorial, we will discuss how we can configure a SSL certificate on Nginx with Let’s encrypt. We have already discussed in our previous tutorial about how we can configure **SSL cert with Let’s certificate on Apache Web Server,** so if you are using Apache you can check that tutorial. Now let’s start with the process to configure SSL on Nginx with Let’s Encrypt.

Recommended Read : Simple way to configure Nginx Reverse Proxy

Here we will discuss the method for Ubuntu & CentOS/RHEL using a let’s encrypt tool called certbot. So let’s start with Pre-requisites,

Also Read : Analyzing APACHE logs in CLI (& GUI) using GoAccess

Pre-Requisites

– We will need a registered Domain address,
– We will need a CentOS/RHEL or Ubuntu server with Ngnix installed. Installation steps are mentioned below,

Ubuntu

Nginx is available with default Ubuntu Repositories. So simple install it using the following command,

```
$ sudo apt-get update && sudo apt-get install nginx
```

CentOS/RHEL

We need to add some repos for installing nginx on CentOS & we have created a detailed **ARTICLE HERE for nginx installation** on CentOS/RHEL.

Now start the services & enable it for boot,

```
# systemctl start nginx
```

RECENT POSTS

- Bash Scripting: Learn to use REGEX (Part 2- Intermediate)
- Complete guide to configure SSL on Nginx with Let's Encrypt (Ubuntu/Centos/RHEL)
- Configuring redis MASTER SLAVE setup

```
# systemctl enable nginx
```

Once its installed, we can move to next part i.e. installing let’s encrypt & issuing of SSL certificate for website.

Let’s Encrypt on Ubuntu

Firstly we need to install Certbot on Ubuntu system, but its not available with default Ubuntu repositories. Install the Ubuntu repos with the following command,

```
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository universe
$ sudo add-apt-repository ppa:certbot/certbot
$ sudo apt-get update
```

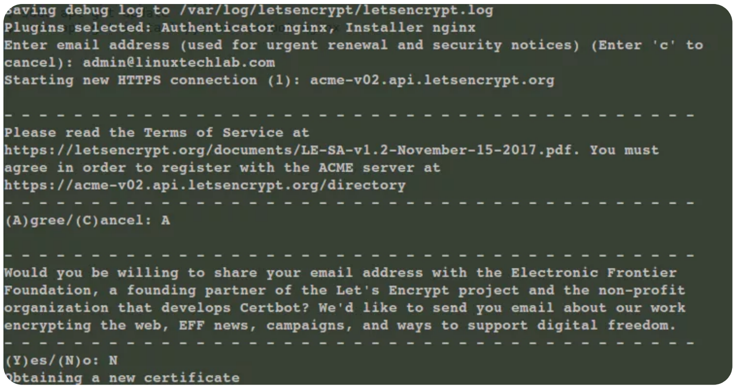
Now to install the Certbot , execute the following command from terminal,

```
$ sudo apt-get install python-certbot-nginx
```

Now, we will issue a new SSL certificate using certbot command. Use the following command as reference ,

```
$ sudo certbot –nginx -d linuxtechlab.com -d www.linuxtechlab.com
```

Here linuxtechlab.com is the name of the website for which the certificate will be issues, replace this with the name of your website. If this is the first time you are using Certbot, you will be asked to enter an Email address & also to agree to User Agreement,



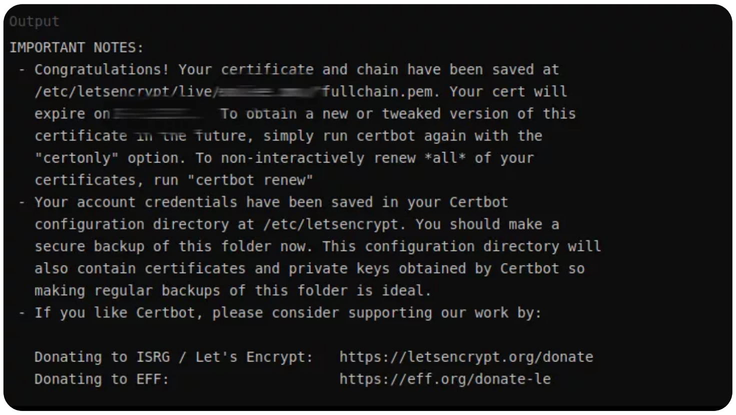
```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): admin@linuxtechlab.com
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing 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
Obtaining a new certificate
```

Now certbot will then check with let’s encrypt server to verify that you are the web admin of the domain that you are trying to get an SSL for (usually you need to place two files with random text provided by let’s encrypt at location http://domain-name/.well-known/acme-challenge. more details on that **HERE**).

Once site ownership has been confirmed, we will be asked to configure redirect settings for Nginx, you can choose 1 (No-Redirect) or 2 (Redirect). If you choose 1, than you will have to configure redirect yourselves in Nginx configuration afterwards, with option 2 , the configuration will be updated & Nginx will be reloaded to implement the new changes made.



```
Output
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/[redacted]fullchain.pem. Your cert will
   expire on [redacted]  To obtain a new or tweaked version of this
   certificate in the future, simply run certbot again with the
   "certonly" option. To non-interactively renew *all* of your
   certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   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 Certbot so
   making regular backups of this folder is ideal.
 - 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
```

Our cert is now installed & new configurations also have been loaded. As mentioned above, we need to renew the cert every 90 days, for that we can create a new cronjob, mentioned at the end of this tutorial.

Now let’s discuss the SSL issue procedure for CentOS & RHEL,

Let’s Encrypt on CentOS/RHEL

To install Certbot on CentOS, we will need to first install EPEL repositories first on our system. Install EPEL using following command on your system,

RHEL/CentOS 7

# rpm -Uvh https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-

```
release-7-11.noarch.rpm
```

RHEL/CentOS 6 (64 Bit)

```
# rpm -Uvh http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

RHEL/CentOS 6 (32 Bit)

```
# rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
```

Now we to install certbot use the following command,

```
# yum install certbot-nginx
```

Once the certbot has been installed, we can then issue the SSL certificate with the same command as mentioned above,

```
# certbot –nginx -d linuxtechlab.com -d www.linuxtechlab.com
```

Now the process will same as has been mentioned above for Ubuntu. Now after the cert has been installed, we need to make sure that the certificate is renewed before 90 days.

Automatic Certificate Renewal

Following cron job will take care of the automatic certificate renewal,

```
# crontab -e
```

```
05 01 30 * * /usr/bin/certbot renew –quiet
```

this job will renew certificate every 30 days at 1:05 AM. We can also run the following command to dry-run or test the renewal of certificate,

```
# certbot renew –dry-run
```

This completes our tutorial on how to configure SSL on Nginx with Let’s encrypt. Please feel free to send any questions or queries you have regarding this tutorial.

If you think we have helped you or just want to support us, please consider these :-

Connect to us: Facebook | Twitter | Google Plus

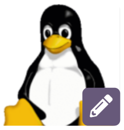
Donate us some of your hard earned money:

Donate

Linux TechLab is thankful for your continued support.

Share this post:

Tags: let's encrypt nginx ssl



Shusain

Passionate about Linux & open source. Loves to learn, read & write about Linux as well as new technologies.

YOU MAY ALSO LIKE...

WordPress installation on Centos/RHEL 7

MAY 30, 2017

Important PostgreSQL commands you should know

SEPTEMBER 27, 2018

Nagios Server : Adding Windows host to Nagios server for monitoring

FEBRUARY 13, 2017

2 RESPONSES

Comments 2 **Pingbacks** 0

Adrian December 12, 2018 at 4:52 pm

Are you sure that you want to try and renew the certificate every day!?

Surely once a month is more than enough

Reply

Shusain

December 13, 2018 at 3:23 pm

You are right but this also works, but surely 30 days will also work fine.

Reply

LEAVE A REPLY

Comment

Name * **Email** *

Website

□ **Notify me of follow-up comments by email.**

□ **Notify me of new posts by email.**

Post Comment

Privacy Policy

Free E-Books

Contact us/ Donate us