Apache - Certbot SSL Certificate

Introduction

The Certbot Package is not included in Rocky Linux’s base repository by default. In order to obtain it, we must install the EPEL (Extra Packages for Enterprise Linux) repository. This repository provides additional software packages through open-source efforts. In addition to certbot, we must also install “mod_ssl,” which is a security module for Apache to support SSL/TLS protocols.

Prerequisites

You can now install the **Certbot package** and its **dependencies** for Rocky Linux with the following commands

```
sudo dnf install epel-release -y
sudo dnf install mod_ssl -y
sudo dnf install certbot python3-certbot-apache -y
```

Install SSL Certificate for Apache httpd

Upon completion of the installation, you will be able to get a Let’s Encrypt SSL certificate. Certbot offers various methods for obtaining an SSL Certificate, you may use one of the following commands.

Simple method to complete all sites that are configured

```
sudo certbot --apache
```

Alternately, you can use the “-d” flag with this command directly to specify multiple domains

```
certbot --apache -d http://website.com
```

When you run the above command, you will be prompted for a series of questions which you must answer in order to deploy the certificate successfully. In order to make things easier for beginners, I have separated each prompt into different boxes.

In order to verify the certificate, Let's Encrypt it will ask you to enter your email address

Also you will need to accept the following terms and conditions

After your first certificate is issued, you will be asked to share your email address to receive updates on new/campaigns with the Electronic Frontier Foundation. The decision is yours to make "Y or N"

Depending on your web server configuration, it will list your domains and ask which one you want to activate HTTPS for. You can select '1' or '2'. However, if you want all domains to begin using HTTPS, press ENTER

Certificate Automatic Renewal

Let's Encrypt certificates are generally valid for 90 days, so you need to renew them manually after that time. The following command needs to be run to renew the certificate.

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

However, we can automate the renewal process using cron jobs. In your crontab file, add the following entry:

```
0 0 1 * * /usr/bin/certbot renew >/dev/null 2>&1
```

Delete Certificate

If you wish to delete the certificate, use the following command

```
sudo certbot delete
```

Conclusion

We hope this article has helped you understand how to Secure Apache with SSL in Rocky Linux 9.1 step by step. You can also get help from Let's Encrypt's community site if you encounter any issues. Drop me your feedback/comments. Feel free to share this article with others if you like it.

Revision #2
Created 2 September 2024 20:54:36 by Steve Ling
Updated 2 September 2024 20:56:38 by Steve Ling