Práctica: HTTPS con Let’s Encrypt y Certbot

Implantación de Aplicaciones Web

José Juan Sánchez Hernández

Curso 2023/2024

Índice

Índice de figuras

Índice de cuadros

1 Práctica: HTTPS con Let's Encrypt y Certbot

En esta práctica tendremos que realizar la instalación de la pila LAMP y la **configuración de un certificado SSL/TLS con Let's Encrypt y Certbot** en el servidor web Apache, en una instancia EC2 de Amazon Web Services (AWS) con la última versión de Ubuntu Server.

1.1 Conceptos básicos

1.1.1 ¿Qué es HTTPS?

HTTPS (*Hyptertext Transfer Protocol Secure*) o protocolo seguro de transferencia de hipertexto, es un protocolo de la capa de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. (Fuente: Wikipedia)

Para poder habilitar el protocolo HTTPS en un sitio web es necesario obtener un **certificado de seguridad**. Este certificado tiene que ser emitido por una **autoridad de certificación** (AC). En esta práctica vamos a obtener un certificado para un dominio de la Autoridad de Certificación Let's Encrypt.

1.1.2 ¿Qué es Let's Encrypt?

Let's Encrypt es una autoridad de certificación que se puso en marcha el 12 de abril de 2016 y que proporciona certificados X.509 **gratuitos** para el cifrado de seguridad de nivel de transporte (TLS) a través de un proceso automatizado diseñado para eliminar el complejo proceso actual de creación manual, la validación, firma, instalación y renovación de los certificados de sitios web seguros. (Fuente: Wikipedia)

1.1.3 Cómo funciona Let's Encrypt

Se recomienda la lectura de la sección **Cómo Funciona Let's Encrypt** de la documentación oficial.

1.1.4 ¿Qué es Certbot?

Para poder obtener un certificado de Let's Encrypt para un dominio de un sitio web es necesario demostrar que se tiene control sobre ese dominio. Para realizar esta tarea es necesario utilizar un cliente del protocolo ACME (Automated Certificate Management Environment). El cliente ACME recomendado para esta tarea es Certbot porque es fácil de usar, tiene soporte para muchos sistemas operativos y dispone de una excelente documentación.

1.2 Tareas a realizar

A continuación se describen **muy brevemente** algunas de las tareas que tendrá que realizar.

1.2.1 Paso 1

Crear una instancia EC2 en Amazon Web Services (AWS).

Cuando esté creando la instancia deberá **configurar los puertos** que estarán abiertos para poder conectarnos por SSH y para poder acceder por HTTP/HTTPS.

- SSH (22/TCP)
- HTTP (80/TCP)
- HTTPS (443/TCP)

1.2.2 Paso 2

Obtener la dirección IP pública de su instancia EC2 en AWS.

1.2.3 Paso 3

Realizar la instalación y configuración de un sitio web. Para esta tarea puede hacer uso de los scripts que ha realizado en las prácticas anteriores.

1.2.4 Paso 4

Registrar un nombre de dominio en algún proveedor de nombres de dominio gratuito. Por ejemplo, puede hacer uso de Freenom o No-IP.

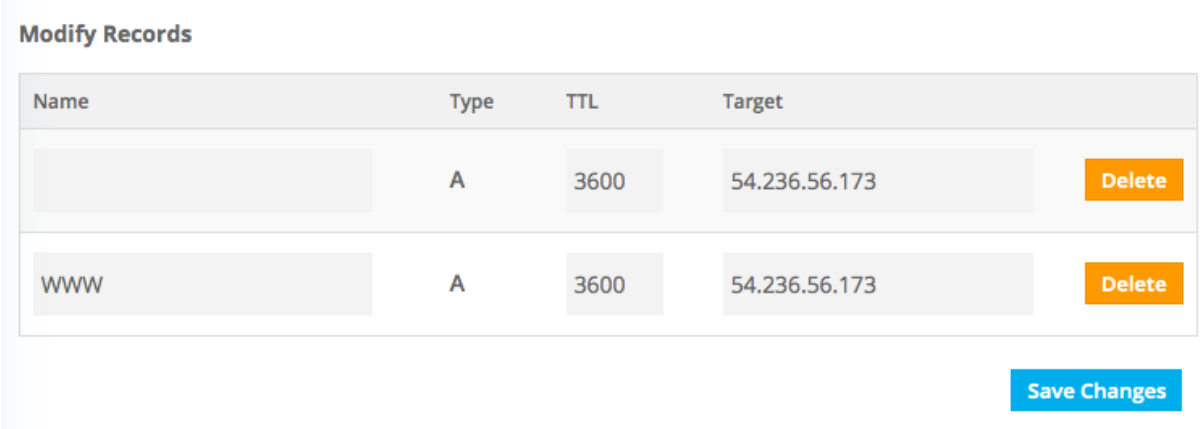
1.2.5 Paso 5

Configurar los registros DNS del proveedor de nombres de dominio para que el nombre de dominio de ha registrado pueda resolver hacia la dirección IP pública de su instancia EC2 de AWS.

Si utiliza el proveedor de nombres de dominio Freenom tendrá que acceder desde el panel de control, a la sección de sus dominios contratados y una vez allí seleccionar **Manage Freenom DNS**.

Tendrá que añadir dos registros DNS de tipo A con la dirección IP pública de su instancia EC2 de AWS. Un registro estará en blanco para que pueda resolver el nombre de dominio sin las www y el otro registro estará con las www .

Ejemplo: En la siguiente imagen se muestra cómo sería la configuración de los registros DNS para resolver hacia la dirección IP 54.236.57.173.



Nota: Tenga en cuenta que una vez que ha realizado los cambios en el DNS habrá que esperar hasta que los cambios se propaguen. Puede hacer uso de la utilidad dnschecker.org para comprobar el estado de propagación de las DNS.

1.2.6 Paso 6

Instalar y configurar el cliente ACME Certbot en su instancia EC2 de AWS, siguiendo los pasos de la documentación oficial.

Se recomienda visitar la página web oficial de Certbot y utilizar el formulario para indicar el software que vamos a utilizar (Apache, Ngingx, HAProxy, etc.) y el sistema operativo. Una vez que hemos realizado la selección nos aparecerán las instrucciones que tenemos que tenemos que seguir.

Ejemplo: A continuación se muestran los pasos que se han llevado a cabo para realizar la instalación y configuración de Certbot en una máquina con el **servidor web Apache** y el **sistema operativo Ubuntu 20.04.**

1. Realizamos la instalación y actualización de `snapd`.

```
sudo snap install core; sudo snap refresh core
```

2. Eliminamos si existiese alguna instalación previa de `certbot` con `apt`.

```
sudo apt remove certbot -y
```

3. Instalamos el cliente de Certbot con `snapd`.

```
sudo snap install --classic certbot
```

4. Creamos una alias para el comando `certbot`.

```
sudo ln -fs /snap/bin/certbot /usr/bin/certbot
```

5. Obtenemos el certificado y configuramos el servidor web Apache.

```
sudo certbot --apache
```

Durante la ejecución del comando anterior tendremos que contestar algunas preguntas:

- Habrá que introducir una dirección de correo electrónico. (Ejemplo: `demo@demo.es`)
- Aceptar los términos de uso. (Ejemplo: `y`)
- Nos preguntará si queremos compartir nuestra dirección de correo electrónico con la *Electronic Frontier Foundation*. (Ejemplo: `n`)
- Y finalmente nos preguntará el nombre del dominio, si no lo encuentra en los archivos de configuración del servidor web. (Ejemplo: `practicahttps.ml`)

A continuación se muestra un ejemplo de cómo es la interacción durante la ejecución del comando `sudo certbot --apache`.

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): demo@demo.es

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
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. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, 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
Account registered.
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated)  (Enter 'c' to cancel): practicahttps.ml
Requesting a certificate for practicahttps.ml
Performing the following challenges:
http-01 challenge for practicahttps.ml
Enabled Apache rewrite module
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-available/000-default-le-ssl.conf
Enabled Apache socache_shmcb module
Enabled Apache ssl module
Deploying Certificate to VirtualHost /etc/apache2/sites-available/000-default-
    le-ssl.conf
Enabling available site: /etc/apache2/sites-available/000-default-le-ssl.conf
Enabled Apache rewrite module
Redirecting vhost in /etc/apache2/sites-enabled/000-default.conf to ssl vhost
    in /etc/apache2/sites-available/000-default-le-ssl.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://practicahttps.ml
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
Subscribe to the EFF mailing list (email: demo@demo.es).

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/practicahttps.ml/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/practicahttps.ml/privkey.pem
   Your certificate will expire on 2021-05-01. 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"
 - 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
```

Una vez llegado hasta este punto tendríamos nuestro sitio web con **HTTPS habilitado y todo configurado para que el certificado se vaya renovando automáticamente**.

Nota:

También es posible especificar como argumentos las respuestas que nos hará `certbot` durante el proceso de instalación. Por ejemplo, las mismas respuestas que hemos dado durante la instalación manual se podrían haber indicado con los siguientes parámetros.

- Dirección de correo: `-m demo@demo.es`
- Aceptamos los términos de uso: `--agree-tos`
- No queremos compartir nuestro email con la *Electronic Frontier Foundation*: `--no-eff-email`
- Dominio: `-d practicahttps.ml`

Además, vamos a añadir el parámetro `--non-interactive` para que al ejecutar el comando no solicite al usuario ningún dato por teclado. Esta opción es útil cuando queremos automatizar la instalación de Certbot mediante un script.

```
sudo certbot --apache -m demo@demo.es --agree-tos --no-eff-email -d
    practicahttps.ml --non-interactive
```

Con el siguiente comando podemos comprobar que hay un temporizador en el sistema encargado de realizar la renovación de los certificados de manera automática.

```
systemctl list-timers
```

Se recomienda revisar los archivos de configuración del servidor web para ver cuáles han sido las cambios que ha realizado el cliente Certbot.

1.3 Entregables

Deberá crear un repositorio en GitHub con el nombre de la práctica y añadir al profesor como colaborador.

El repositorio debe tener el siguiente contenido:

- Un **documento técnico** con la descripción de todos los pasos que se han llevado a cabo.
- Los **scripts de Bash** que se han utilizado para automatizar la creación y configuración de un certificado SSL/TLS con Let's Encrypt y Certbot, en el servidor web Apache.

Además del contenido anterior puede ser necesario crear otros archivos de configuración. A continuación se muestra un ejemplo de cómo puede ser la estructura del repositorio:

```
.├──
 README.md├──
 conf│├──
    000-default.conf│
    └── default-ssl.conf└──
 scripts├──
     .env├──
     install_lamp.sh└──
     setup_letsencrypt_certificate.sh
```

1.3.1 Documento técnico

El documento técnico `README.md` tiene que estar escrito en Markdown y debe incluir **como mínimo** los siguientes contenidos:

- Descripción del proceso de creación y configuración del certificado SSL/TLS autofirmado en el servidor web Apache.

1.3.2 Scripts de Bash

El directorio `scripts` debe incluir los siguientes archivos:

- `.env`: Este archivo contiene todas las variables de configuración que se utilizarán en los scripts de Bash.
- `install_lamp.sh`: Script de Bash con la automatización del proceso de instalación de la pila LAMP.
- `setup_letsencrypt_certificate.sh`: Script de Bash con la automatización del proceso de creación y configuración de un certificado SSL/TLS con Let's Encrypt y Certbot.

2 Referencias

- HTTPS en Wikipedia.
- WordPress.
- Amazon Web Services (AWS).
- Let's Encrypt.
- TLS (Transport Layer Security).
- ACME (Automated Certificate Management Environment).
- Certbot.
- Ecosistema PKI y Certificados digitales. Conceptos básicos. Charla de Tomás de Hidalgo.

3 Licencia