

Obtenga un certificado SSL con Letsencrypt Certbot

Descripción general

Antes de que letsencrypt genere y entregue un certificado, debe comprobar si usted controla los registros DNS de ese dominio. Para eso, le pide que cree un registro TXT que pueda consultar a través del sistema de nombres de dominio.

Para eso, utiliza certbot para solicitar su certificado. Le proporciona lo que necesita en el registro TXT. Usted crea el registro TXT mediante la interfaz del servicio DNS que utiliza y, una vez propagado el nuevo registro, pulsa "Continuar", lo que permite a certbot completar la tarea y guardar su certificado.

Instalar Certbot

```
sudo apt update
sudo apt install certbot
```

Pide su certificado

```
sudo certbot certonly --manual --preferred-challenges dns -d tusitio.ejemplo.com

# En este punto, se le solicitará un registro TXT similar a este:
# nombre: _acme-challenge.tusitio.ejemplo.com
# valor: Tv1E2PLJyIU1ePiLfw-bv8SdAq4wa3QDud76zfB7asU
# Se le pedirá que presione "Enter" para continuar.
# Espere a que se completen los pasos a continuación antes de continuar.
```

Agregar el registro TXT

Usando su interfaz web a su servicio DNS, agregue un registro TXT similar a este.

`_acme-challenge.tusitio TXT Tv1E2PLJyIU1ePiLfw-bv8SdAq4wa3QDud76zfB7asU`

Los registros DNS tardan en propagarse, por lo que primero debe asegurarse de que el registro se haya propagado antes de presionar "Continue" en el mensaje de certbot.

Verificar que se haya propagado

En otra ventana de terminal, escriba el siguiente comando de vez en cuando hasta que su registro TXT aparezca en la sección de respuestas.

```
dig -t txt _acme-challenge.tusitio.ejemplo.com
```

Continuar certbot en la ventana de terminal original

Presione Enter. Sus archivos de certificado estarán aquí: `/etc/letsencrypt/live/tusitio.ejemplo.com`

`fullchain.pem`:

Contiene el certificado SSL de su dominio y los certificados intermedios necesarios para formar una cadena de confianza válida que remonte al certificado raíz de Let's Encrypt.

`privkey.pem`:

Su clave privada, que debe mantenerse en secreto para proteger su sitio web.

`cert.pem`:

Contiene el certificado SSL específico de su dominio.

`chain.pem`:

Contiene los certificados intermedios que vinculan el certificado de su dominio a la CA raíz.