Si estás pensando en aplicar un certificado LetsEncrypt a un servicio HTTP/HTTPS alojado en un puerto diferente al 80 o al 443, la forma aconsejada para hacerlo es teniendo control sobre los registros DNS de ese nombre de dominio.

Esto es porque LetEncrypt, además de validar desafíos HTTP con el desafío HTTP-01, ofrece la posibilidad de comprobar la propiedad de un dominio mediante el desafío DNS-01. Para ello tendrás que ejecutar en el servidor web este comando como root:

```
certbot certonly --manual -preferred-challenge dns --test-cert
```

Si quieres indicar el nombre de dominio en la orden, ejecuta:

```
certbot certonly --manual -preferred-challenge dns -d tudominio.com
```

En esas órdenes, el argumento «manual» indica que no utilizaremos ningún plugin. Si las órdenes están bien escritas, LetsEncrypt te indicará, mediante un mensaje en la terminal, el nombre que debes darle al registro y el token que tendrás que meter dentro. Por ejemplo:

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.tudominio.com with the following value:

XPJa37BhKtSeYAHK3bu4BsNTk1r3QZ8W-vxqXH43Fro

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Entonces, antes de darle a Enter, tendrás que ir al panel de control del dominio, luego a la configuración de su DNS, finalmente, agregar un registro TXT con los datos que te proporciona LE. Luego de agregar el registro TXT deberás esperar unos minutos a que se propaguen todos los cambios. Si eres impaciente, desde otra CLI puedes comprobar si el registro ya se ha propagado. Esto lo haces ejecutando:

```
dig -t txt +short _acme-challenge.tudominio.com
```

-t txt significa que sólo pediremos el registro txt del DNS.

+short significa que sólo imprimiremos su valor.

Si la salida de ese comando es exactamente el token que LE nos ha dicho que pongamos en el registro, el registro ya se habrá propagado.

Una vez que todo es correcto, ya puedes darle al Enter y esperar a la notificación de LE sobre que el desafío ha sido superado.

Una vez que el certificado se haya creado, puedes decodificarlo ejecutando:

```
openssl x509 -in /etc/letsencrypt/live/tudominio.com/fullchain.pem
```

Lo normal es tener que renovar manualmente el certificado antes de que expire. Sin embargo, existe una forma de automatizar su renovación creando un servidor acme-dns.

NOTA: Si tampoco tienes control sobre el **DNS** del dominio para el cual quieres obtener el certificado, como último recurso puedes utilizar este hack.

Más info en este video: