Solicitar certificado Wildcart para un dominio

Para crear un dominio del tipo wildcard, es decir del tipo *.midominio.es, necesitamos tener acceso a la configuración DNS de nuestro dominio para poder crear un registro del tipo **txt** en el mismo.

Para solicitar un certificado en el entorno de pruebas de Let' s Encrypt ejecutamos:

```
certbot certonly --manual --preferred-challenges=dns --email
admin@midominio.es --server https://acme-v02.api.letsencrypt.org/directory -
-agree-tos -d *.midominio.es
```



Necesitas usar tu correo y tu dominio. En este caso además estoy usando el entorno de producción **acme-v02.api.letsencrypt.org** . Cambialo si vas a hacer pruebas

Para hacer pruebas cambia la URL del servidor por **acme-staging-v02.api.letsencrypt.org**



```
certbot certonly --manual --preferred-challenges=dns --email
admin@midominio.es                                  --server
https://acme-staging-v02.api.letsencrypt.org/directory --agree-
tos -d *.midominio.es
```

Al ejecturar el comando, en la consola te pedirá que crees un registro del tipo TXT en tu DNS con el valor que te muestra, en mi caso me indica que cree

```
_acme-challenge.midominio.es with the following
value:ukU9H9rPQVbC37nG0p35QzA7CQf7FmMD7QQnC3APm9w
```



En strato sólo poner como prefijo _acme-challenge, sin el nombre de dominio

Configurar el certificado en nginx

Ficheros

Fichero /etc/nginx/sites-available/midominio_es

```
server {
    listen 80;
    listen [::]:80;
    root /var/www/midominio_es;
```

```
    index index.php index.html index.htm;
    server_name midominio.es www.midominio.es;
    location ~ /\.well-known/acme-challenge/ {
        allow all;
    }
    location / {
        return 301 https://$host$request_uri;
    }
}
server {
    listen 443 ssl http2;
    root /var/www/midominio_es;
    index index.php index.html index.htm;
    server_name midominio.es www.midominio.es;
    location / {
        try_files $uri $uri/ /index.php?q=$uri&$args;
    }
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SH>
    ssl_prefer_server_ciphers On;

    ssl_certificate /etc/letsencrypt/live/midominio.es/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/midominio.es/privkey.pem;
    ssl_trusted_certificate /etc/letsencrypt/live/midominio.es/chain.pem;
    ssl_stapling on;
    ssl_stapling_verify on;
    add_header Strict-Transport-Security "max-age=31557600;
includeSubDomains";
}
```

Index.html

creamos el fichero /var/www/midominio_es/index.html con el siguiente contenido

```
<html>
<head></head>
<body>
         <h1>Esta es mi pagina index.html</h1>
         <p>Hola MUNDO</p>
</body>
</html>
```

Creamos en/etc/nginx/sites-enable un enlace al fichero que hemos creado en sites_available

```
ln -s /etc/nginx/sites-available/midominio_es /etc/nginx/sites-enabled/
```

Referencias

- https://www.jesusamieiro.com/generar-un-certificado-ssl-wildcard-con-lets-encrypt/

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=seguridad:letsencrypt:wildcards

Last update: **182023/01/ 13:37**