Let's Encrypt wildcard

lets encrypt

info

- https://www.jesusamieiro.com/generar-un-certificado-ssl-wildcard-con-lets-encrypt/
    - https://www.whatsmydns.net/
    - https://dnschecker.org/#TXT/_acme-challenge.fidmag.org
    - https://mxtoolbox.com/SuperTool.aspx?action=txt%3a_acme-challenge.example.com&run=toolpage#
- https://redeslinux.net/guia-completa-pfsense-con-ddns-de-cloudflare-certificados-lets-encrypt-y-haproxy-para-proxy-inverso-y-balanceo-de-carga-de-servicios/
- https://discourse.haproxy.org/t/using-ssl-with-haproxy-for-docker-containers/307
- https://github.com/BradJonesLLC/docker-haproxy-letsencrypt/blob/master/certs.sh
- https://github.com/BradJonesLLC/docker-haproxy-letsencrypt

renovación autmatizada auth.acme-dns.io

- primera vegada:

```
sudo curl -o /etc/letsencrypt/acme-dns-auth.py
https://raw.githubusercontent.com/joohoi/acme-dns-certbot-joohoi/master/acme-dns-auth.py
sudo chmod +x /etc/letsencrypt/acme-dns-auth.py
sudo certbot certonly --manual --manual-auth-hook /etc/letsencrypt/acme-dns-auth.py --preferred-challenges dns --debug-challenges -d "*.fidmag.org" -d "fidmag.org"
```

- creat registre CNAME:

```
_acme-challenge.fidmag.org CNAME 1569f935-7bf3-4630-9c3d-5846ad7c956e.auth.acme-dns.io.
```

```
dig _acme-challenge.fidmag.org CNAME +short
```

- renovacions per cron

```
0 7,19 * * * certbot renew --quiet --deploy-hook "/home/fidmag/certbot/renew-dns.sh" > /home/fidmag/certbot/last_exec 2>&1
```

    - simulacro:

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

    - comprobar fichero configuración renovación:

      /etc/letsencrypt/renewal/fidmag.org.conf

      ```
      # Options used in the renewal process
      [renewalparams]
      account = ***
      pref_challs = dns-01,
      authenticator = manual
      ```

```
server = https://acme-v02.api.letsencrypt.org/directory
key_type = ecdsa
manual_auth_hook = /etc/letsencrypt/acme-dns-auth.py
```

- Let's encrypt recomienda comprobar 2 veces al día (Gemini dixit)
- `--deploy-hook`: script a ejecutar si la renovación es exitosa

- certificats.config

```
# configuració
#declare -a CERTIFICATS=("matebcn.eu" "fruitsmontmany.es"
"estellar.cat")
declare -a CERTIFICATS=($(basename -s .conf
/etc/letsencrypt/renewal/*.conf))
```

```
#!/usr/bin/env bash

SCRIPT_SOURCE=`dirname "$0"`
source ${SCRIPT_SOURCE}/certificats.config

for cert "${CERTIFICATS[@]}"; do
    if [[ -f /home/mate/webservices/certs/${cert}.pem ]]; then
        sudo cp -f /home/mate/webservices/certs/${cert}.pem
/home/mate/webservices/certs/old/${cert}.pem.old
    fi

    if [[ -f /home/mate/webservices/certs/${cert}.pem.key ]]; then
    sudo cp -f /home/mate/webservices/certs/${cert}.pem.key
/home/mate/webservices/certs/old/${cert}.pem.key.old
    fi

    sudo cp -f /etc/letsencrypt/live/${cert}/fullchain.pem
/home/mate/webservices/certs/${cert}.pem && \
    sudo cp -f /etc/letsencrypt/live/${cert}/privkey.pem
/home/mate/webservices/certs/${cert}.pem.key && \
    sudo chmod +r /home/mate/webservices/certs/* && \

    docker compose -f /home/mate/webservices/docker-compose.yml restart
haproxy-proxy

done
```