??

????????????? Main Web ?? Nginx ??????????????

1. ?????????? Reverse Proxy ????????????????????????
   ????????????? Reverse Proxy ?????????????? IP ???
2. ?????? Let's Encrypt ??? SSL ????????
   Main Web -----[HTTP]----- Reverse Proxy -----[HTTPS]----- Client
3. ???????
   - ? Main Web ????????????? Reverse Proxy ? HTTP ??
   - ? Reverse Proxy ??????????? HTTPS
4. ?? docker ???? Reverse Proxy ????? Lets Encrypt ??????

Reverse Proxy with Nginx

?? docker-compose.yml

```
version: "2"

services:
  nginx-proxy:
    restart: always
    image: nginx
    container_name: nginx-proxy
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - "/docker_vol/nginx-proxy/etc-nginx/conf.d:/etc/nginx/conf.d"
      - "/docker_vol/cert-letsencrypt:/etc/letsencrypt"
      - "/docker_vol/data-letsencrypt:/data/letsencrypt"
```

???????

```
mkdir -p /docker_vol/nginx-proxy/etc-nginx/conf.d
mkdir -p /docker_vol/cert-letsencrypt
mkdir -p /docker_vol/data-letsencrypt
```

?? Nginx ???
/docker_vol/nginx-proxy/etc-nginx/conf.d/proxy.conf

```
server {
    listen 80;
    server_name www.your.domain;

    location / {
        proxy_pass http://your-main-web-ip;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
```

```
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
  }
}
```

TIP:

- http://your-main-web-ip ???????? IP ??

- ??????????????????? 80 port ??

??nginx-proxy ?? (?? docker-compose)

????????????????????? containers

#> docker-compose up -d

?????????

#> docker-compose ps

```
  Name          Command         State                Ports
-------------------------------------------------------------------------------------
nginx-proxy   nginx -g daemon off;   Up      0.0.0.0:443->443/tcp, 0.0.0.0:80->80/tcp
```

TIPs?

???????????????????? proxy.conf ????????????????????? proxy.conf ????????

Reverse Proxy ????

?? nginx-proxy ?????????????????? http://reverse-proxy-ip ??????????????????????

Lets Encrypt

?? Reverse Proxy ??????? docker ???? Let's Encrypt ????? Reverse Proxy ????

?????

1. ????????????? www.your.domain
2. ??????? DNS ????? A/AAAAA ????? Reverse Proxy ?? IP

????????

1. ??????????
2. ?3???????????

???????

?? /docker_vol/nginx-proxy/etc-nginx/conf.d/proxy.conf
???????

```
server {
   listen 80;
   server_name www.your.domain;

   # Statically serve all files in .well-known, which is the location where letsencrypt stores the proof file
   location /.well-known/ {
      alias /data/letsencrypt/.well-known/;
   }
}
```

TIP:

/.well-known ???????????????? HTTP ???

?? nginx-proxy ??

```
docker-compose stop
docker-compose start
```

??????

```
docker run -it --rm \
 -v "/docker_vol/cert-letsencrypt:/etc/letsencrypt" \
 -v "/docker_vol/data-letsencrypt:/data/letsencrypt" \
 -v "/docker_vol/log-letsencrypt:/var/log/letsencrypt" \
 deliverous/certbot \
 certonly \
 --webroot --webroot-path=/data/letsencrypt \
 -d www.your.domain
```

TIPs?

- www.your.domain ????????????????????????????????? -d first.my.web -d second.my.web -d third.my.web

- ??????????? email??????? email?

- ???????????? HTTP ??????? /.well-known/????????????????????????????? /data/letsencrypt?

??????

???????????

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/www.your.domain/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/www.your.domain/privkey.pem
  Your cert will expire on 2018-05-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. 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

???????
container ??

- /etc/letsencrypt/live/www.your.domain/fullchain.pem
- /etc/letsencrypt/live/www.your.domain/privkey.pem

Host ??

- /docker_vol/cert-letsencrypt/live/www.your.domain/fullchain.pem
- /docker_vol/cert-letsencrypt/live/www.your.domain/privkey.pem

TIP?

????????????????????????????????? docker ???? -d <new-host-name> ???????????????? email?????
?? email ???? /docker_vol/cert-letsencrypt/??

??????
Lets Encrypt ??????????????????????????

```
#> docker run -it --rm \
 -v "/docker_vol/cert-letsencrypt:/etc/letsencrypt" \
 -v "/docker_vol/data-letsencrypt:/data/letsencrypt" \
 -v "/docker_vol/log-letsencrypt:/var/log/letsencrypt" \
 deliverous/certbot \
 renew \
 --webroot --webroot-path=/data/letsencrypt

 #> docker-compose kill -s HUP nginx-proxy
```

NOTE: ????? -d your.domain.com????????????

Cronjob:

0 0 */15 * * docker run -it --rm -v "/docker_vol/cert-letsencrypt:/etc/letsencrypt" -v "/docker_vol/data-letsencrypt:/data/letsencrypt" deliverous/certbot renew --webroot --webroot-path=/data/letsencrypt && docker-compose kill -s HUP nginx-proxy

TIP:

- ?????? 60 ???????????????? 90 ??

- ?????????? domain?????????????

- ????????? log ? /docker_vol/log-letsencrypt/letsencrypt.log

?????????

```
------------------------------------------------------------------------------
Processing /etc/letsencrypt/renewal/r13.osslab.tw.conf
------------------------------------------------------------------------------
Cert is due for renewal, auto-renewing...
Plugins selected: Authenticator webroot, Installer None
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for r13.osslab.tw
Using the webroot path /data/letsencrypt for all unmatched domains.
Waiting for verification...
Cleaning up challenges

------------------------------------------------------------------------------
new certificate deployed without reload, fullchain is
/etc/letsencrypt/live/r13.osslab.tw/fullchain.pem
------------------------------------------------------------------------------

The following certs were successfully renewed:
  /etc/letsencrypt/live/r13.osslab.tw/fullchain.pem (success)
```

?? Reverse Proxy ?? SSL with Letsencrypt

???????????????? Reverse Proxy ??? SSL ?????

?? /docker_vol/nginx-proxy/etc-nginx/conf.d/proxy.conf
???????

```
   listen 443;    #????? 80 ?? 443
...
   # SSL Settings
   ssl on;
   ssl_certificate     /etc/letsencrypt/live/www.your.domain/fullchain.pem;
```

```
  ssl_certificate_key /etc/letsencrypt/live/www.your.domain/privkey.pem;

  ssl_session_timeout 5m;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # omit SSLv3 because of POODLE (CVE-2014-3566)
  ssl_ciphers
'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDH
  ssl_prefer_server_ciphers on;
```

?? nginx-proxy ??

```
docker-compose stop
docker-compose start
```

FAQ

Q: ?????????

> Currently, the renew verb is capable of either renewing all installed certificates that are due to be renewed or renewing a single certificate specified by its name. If you would like to renew specific certificates by their domains, use the certonly command instead. The renew verb may provide other options for selecting certificates to renew in the future.

A: ??????????????????????

```
#> docker run -it --rm \
 -v "/docker_vol/cert-letsencrypt:/etc/letsencrypt" \
 -v "/docker_vol/data-letsencrypt:/data/letsencrypt" \
 -v "/docker_vol/log-letsencrypt:/var/log/letsencrypt" \
 deliverous/certbot \
 renew \
 --webroot --webroot-path=/data/letsencrypt
```

> NOTE?????? -d your.domain.com