Pasos para obtener el certificado y/o la renovación

1. Tener acceso por SSH al NAS.

2. Tener acceso al usuario root. En el anclado tienes el proceso para hacerlo.

3. Tener Docker instalado en DSM

4. Abrir los puertos 20000 redirigido al 443 y el 20001 al 80 en el router. El 20000 y el 20001 se pueden cambiar por los que sean más adecuados para cada caso.

5. Una vez accedes por SSH al NAS (recomiendo Mobaxterm porque permite ver el árbol de carpetas del NAS) con tu usuario y contraseña, ejecutar id para obtener el puid y el pgid. Si alguno tiene menos de 4 cifras, rellena con 0 al principio.

6.Ejecuta *sudo-i* para tener acceso root

```
sudo-i
```

7. Ejecutar lo siguiente para crear el contenedor

```
docker create \ --name=letsencrypt \ --cap-add=NET_ADMIN \ -e
PUID=TUPUID \ -e PGID=TUPGID \ -e TZ=Europe/Berlin \ -e
URL=TUNOMBRE.duckdns.org \ -e SUBDOMAINS= \ -e VALIDATION=duckdns
\ -e DUCKDNSTOKEN=SUSTITUIRPORTUTOKEN \ -e EMAIL=TUEMAIL(opcional)
\ -p 20000:443 \ -p 20001:80 \ -v
/volumePONTUVOLUMEN/docker/letsencrypt/config:/config \ --restart
unless-stopped \ linuxserver/letsencrypt
```

8. Entramos a /volumePONTUVOLUMEN/docker/ y creamos la carpeta letsencrypt y dentro de ella la carpeta config

9. Ejecutamos el contendor y comprobamos en el registro que el certificado se ha creado correctamente y las rutas donde se han creado.

10. Ahora depende de si tenemos el certificado ya instalado (paso 10) o lo vamos a renovar (paso 11).

11. En el caso de que no tengamos el certificado instalado:

-Lo primero es tener la clave privada y el certificado localizados.
-La clave privada esta en */volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/privkey.pem*
-El certificado en */volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/cert.pem*
-Se copian a una carpeta accesible desde DSM en el volumen que estemos usando
-En certificados vamos a Agregar, Añadir nuevo certificado, Importar certificado.
-En clave privada elegimos el archivo *privkey.pem*
-En certificado elegimos el archivo *cert.pem*
-Certificado intermedio lo dejamos en blanco.

LISTO, con eso tenemos el certificado instalado en DSM. El paso 11 y siguientes es obligatorio en este método.

12.Para renovaciones (CONFIRMADO QUE LA RENOVACIÓN FUNCIONA A 24/04/2020).- Hay que localizar la ruta donde ya tenemos instalado el certificado. Para eso necesitamos acceder por usuario root (ver paso 2) ya que si no el acceso a la carpeta no nos lo permite.

– La ruta donde se almacena el certificado es usr/syno/etc/certificate/_archive/NOMBREDECARPETACONNUMEROSYLETRAS. Fijaos en la fecha si tenéis varias, la que acabáis de crear tiene fecha mas reciente
– Crear la siguiente tarea programada en Panel de control-Programador de Tareas-Crear-Tareas Programadas-Scrip definido por el usuario

```
cd
/volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/ cp
/volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/cert.pem
usr/syno/etc/certificate/_archive/NOMBREDECARPETACONNUMEROSYLETRAS
cp
/volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/fullchain.pem
usr/syno/etc/certificate/_archive/NOMBREDECARPETACONNUMEROSYLETRAS
cp
/volumePONTUVOLUMEN/docker/letsencrypt/config/etc/letsencrypt/archive/MIDOMINIO.duckdns.org/privkey.pem
```

```
usr/syno/etc/certificate/_archive/NOMBREDECARPETACONNUMEROSYLETRAS
```

13. En el caso de que, aunque la renovación del certificado se haya realizado correctamente y en DSM diga que esta renovado, al entrar por web el certificado este caducado hay que realizar la renovación manualmente en el apartado de certificados de DSM.

-Entramos a Panel de control/Seguridad/Certificado
-Agregar
-Sustituir un certificado existente. En el desplegable con el dominio elegir *MIDOMINIO.duckdns.org.* Siguiente
-Importar certificado. Siguiente
-En clave privada buscamos privkeyX.pem (La X es el numero mas alto de archivo que tengamos, ya que no se borran los anteriores y se van sumando. Si tenemos privkey1.pem y privkey2.pem elegiremos el 2)
-En certificado buscamos certX.pem (La X es el numero mas alto de archivo que tengamos, ya que no se borran los anteriores y se van sumando. Si tenemos cert1.pem y cert2.pem elegiremos el 2)
-En certificado intermedio buscamos chainX.pem (La X es el numero mas alto de archivo que tengamos, ya que no se borran los anteriores y se van sumando. Si tenemos chain1.pem y chain2.pem elegiremos el 2) y pulsamos OK
-En el ultimo paso se reinicia el servidor web y queda el certificado renovado.