HTTPS using Nginx and Let's encrypt in Docker

6 oct. 2021 • 5 min read

*This post is free for all to read thanks to the investment **Mindsers Courses** members have made in our independent publication. If this work is meaningful to you, I invite you to join our courses today.*

As it is a really common task, this post will guide you through with a step-by-step process to protect your website (and your users) using HTTPS. The specific part here is that we will do this in a docker environment.

In this post, I will use Docker Compose to make the tutorial simpler and because I like the infrastructure as code movement.

Nginx as a server

To be able to use nginx as a server for any of our projects, we have to create a Docker Compose service for it. Docker will handle the download of the corresponding image and all the other tasks we used to do manually without Docker.

```
version: '3'

services:
  webserver:
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
```

At anytime during the tutorial, you can run `docker compose up` to start the environment and see if everything goes well.

We have now a working raw installation of nginx that listens to ports `80` for HTTP and `443` for HTTPS.

```
version: '3'

services:
  webserver:
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
    restart: always
```

As I want the server to be always up and running, I tell Docker that it should take care of restarting the "webserver" service when it unexpectedly shuts down.

```
version: '3'

services:
  webserver:
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
    restart: always
    volumes:
      - ./nginx/conf/:/etc/nginx/conf.d/:ro
```

The ultimate goal of our installation isn't to serve the default welcome page of nginx. So, we need a way to update the nginx configuration and declare our website.

To accomplish that, we use the "volumes" feature of Docker. This means we map the folder located at `/etc/nginx/conf.d/` from the docker container to a folder located at `./nginx/conf/` on our local machine. Every file we add, remove or update into this folder locally will be updated into the container.

Note that I add a `:ro` at the end of the volume declaration. `ro` means "read-only". The container will never have the right to update a file into this folder. It is not a big deal, but consider it as a best practice. It can avoid wasting a few precious hours of debugging.

Now update the Docker Compose file as below:

```
version: '3'

services:
  webserver:
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
    restart: always
    volumes:
      - ./nginx/conf/:/etc/nginx/conf.d/:ro
      - ./certbot/www:/var/www/certbot/:ro
```

And add the following configuration file into your `./nginx/conf/` local folder. Do not forget to update using your own data.

```
server {
    listen 80;
    listen [::]:80;

    server_name example.org www.example.org;
    server_tokens off;

    location /.well-known/acme-challenge/ {
        root /var/www/certbot;
    }

    location / {
        return 301 https://example.org$request_uri;
    }
}
```

The configuration is simple. We explain to nginx that it has to listen to port `80` (either on IPv4 or IPv6) for the specific domain name `example.org`.

By default, we want to redirect someone coming on port `80` to the same route but on port `443`. That's what we do with the `location /` block.

But the specificity here is the other `location` block. It serves the files Certbot need to authenticate our server and to create the HTTPS certificate for it.

Basically, we say "always redirect to HTTPS except for the `/.well-know/acme-challenge/` route".

We can now reload nginx by doing a rough `docker compose restart` or if you want to avoid service interruptions (even for a couple of seconds) reload it inside the container using `docker compose exec webserver nginx -s reload`.

Create the certificate using Certbot

For now, nothing will be shown because nginx keeps redirecting you to a `443` port that's not handled by nginx yet. But everything is fine. We only want Certbot to be able to authenticate our server.

To do so, we need to use the docker image for certbot and add it as a service to our Docker Compose project.

```
version: '3'

services:
  webserver:
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
    restart: always
    volumes:
      - ./nginx/conf/:/etc/nginx/conf.d/:ro
      - ./certbot/www:/var/www/certbot/:ro
  certbot:
    image: certbot/certbot:latest
    volumes:
      - ./certbot/www/:/var/www/certbot/:rw
```

We now have two services, one for nginx and one for Certbot. You might have noticed they have declared the same volume. It is meant to make them communicate together.

Certbot will write its files into `./certbot/www/` and nginx will serve them on port `80` to every user asking for `/.well-know/acme-challenge/`. That's how Certbot can authenticate our server.

Note that for Certbot we used `:rw` which stands for "read and write" at the end of the volume declaration. If you don't, it won't be able to write into the folder and authentication will fail.

You can now test that everything is working by running `docker compose run --rm  certbot certonly --webroot --webroot-path /var/www/certbot/ --dry-run -d example.org`. You should get a success message like "The dry run was successful".

Now that we can create certificates for the server, we want to use them in nginx to handle secure connections with end users' browsers.

Certbot create the certificates in the `/etc/letsencrypt/` folder. Same principle as for the webroot, we'll use volumes to share the files between containers.

```
version: '3'

services:
  webserver:
```

```
    image: nginx:latest
    ports:
      - 80:80
      - 443:443
    restart: always
    volumes:
      - ./nginx/conf/:/etc/nginx/conf.d/:ro
      - ./certbot/www:/var/www/certbot/:ro
      - ./certbot/conf/:/etc/nginx/ssl/:ro
  certbot:
    image: certbot/certbot:latest
    volumes:
      - ./certbot/www/:/var/www/certbot/:rw
      - ./certbot/conf/:/etc/letsencrypt/:rw
```

Restart your container using `docker compose restart`. Nginx should now have access to the folder where Certbot creates certificates.

However, this folder is empty right now. Re-run Certbot without the `--dry-run` flag to fill the folder with certificates:

```
$ docker compose run --rm  certbot certonly --webroot --webroot-path
```

Since we have those certificates, the piece left is the `443` configuration on nginx.

```
server {
    listen 80;
    listen [::]:80;

    server_name example.org www.example.org;
    server_tokens off;

    location /.well-known/acme-challenge/ {
        root /var/www/certbot;
    }

    location / {
        return 301 https://example.org$request_uri;
    }
}

server {
    listen 443 default_server ssl http2;
    listen [::]:443 ssl http2;

    server_name example.org;
```

```
        ssl_certificate /etc/nginx/ssl/live/example.org/fullchain.pem;
        ssl_certificate_key /etc/nginx/ssl/live/example.org/privkey.pem;

        location / {
            # ...
        }
    }
```

Reloading the nginx server now will make it able to handle secure connection using HTTPS. Nginx is using the certificates and private keys from the Certbot volumes.

Renewing the certificates

One small issue you can have with Certbot and Let's Encrypt is that the certificates last only 3 months. You will regularly need to renew the certificates you use if you don't want people to get blocked by an ugly and scary message on their browser.

But since we have this Docker environment in place, it is easier than ever to renew the Let's Encrypt certificates!

```
$ docker compose run --rm certbot renew
```

This small "renew" command is enough to let your system work as expected. You just have to run it once every three months. You could even automate this process…

If you have any questions or advices, please create a comment below! I'll be really glad to read you. Also if you like this post, don't forget to share it with your friends. It helps a lot!

Written by Nathanaël Cherrier
Published in docker, coding-tech, ssl, nginx

Discussions

N'oublie pas de lire les Community Guidelines avant de commenter. 10 comments

P

P3dr0

Il y a un an

Hi, Thanks for sharing this tips ! was very useful . I'm actually usernamespace and when i try to start my webserver it dosen't due to permission error when loading certifcate. Got the following error: cannot load certificate "/etc/nginx/ssl/live/bucketlist-test.mylabs.ovh/fullchain.pem": BIO_new_file() failed (SSL: error:0200100D:system library:fopen:Permission denied:fopen('/etc/nginx/ssl/live/{domain}/fullchain.pem','r') error:2006D002:BIO routines:BIO_new_file:system lib). How can i fix this ? Thank you

0

Nathanaël Cherrier

Founder of Mindsers Blog · Il y a un an

Hi P3dr0 !

It seems that SE Linux context isn't right for your files. You can try to restore the context using :

$ restorecon /etc/nginx/ssl/*

0

R

Robin

Il y a un an

Hi, thanks for this great tutorial, it works very well for me. I just have a problem/question when I renew my certificate. After running "docker compose run --rm certbot renew" I got this error: Certificate not yet due for renewal / No renewals were attempted" I already restarted my docker and also the nginx service but still without success. Do you have a solution?

0

Arthur Madec-Prévost

Il y a un an

Hello !

If your certificate is working, it seems to be more a problem of due date, so no worry needed. Your certificate has an expiration date and until a few days before this date, you won't be able to renew the certificate.

It throws an error and says that certbot won't try to renew as there is no need to, but this is more of a warning than an error.

Arthur

1

RN **Roman N**

Il y a un an

I also have this problem, that when I try to renew, I receive message "No renewals were attempted", BUT my certificate is outdated and it expired "Tuesday, June 13, 2023 at 5:06:34 PM".

Can someone help with it and explain, why cerfs cannot be renewed?

0

Nathanaël Cherrier

Founder of Mindsers Blog · Il y a un an

Maybe it is because some files are missing in your /live/ folder. You can try to run the "certonly" command as if it was the first time, it will then create a new one without issue. If it eventually find the old certificate it will ask if you want to renew or expand it.

0

Tom

Il y a un an · Modifié

Even after successful run of
docker compose run --rm certbot certonly --webroot --webroot-path /var/www/certbot/ -d example.org
My certbot container keeps stopping and only I see when running dockers logs certbot is this:
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Certbot doesn't know how to automatically configure the web server on this system. However, it can still get a certificate for you. Please run "certbot certonly" to do so. You'll need to manually configure your web server to use the resulting certificate.

Which doesn't make much sense, as I just ran certbot certonly successfuly. Any ideas what might be causing it?

edit: It was due to permissions (user starting container didn't have permission to create files outside container).

1

J **Jamie Charles**
Il y a un an

I have the exact same issues, can you describe what you changed to fix this?

0

Ce commentaire a été supprimé.

Max
il y a 9 mois

Greetings. Congratulations on the post. I followed it step by step and I'm not sure why it's not generating the certificate. What I need is the following: I have an app that goes up in the container on port 8080 and I would like to make this app publicly available on port 80. Therefore, I need all public requests on port 80 to be directed to port 8080 within the container and for the domain certificate on port 80 to be able to renew itself automatically. If you can help, I would greatly appreciate it.

0

J **janlishak**
il y a 2 mois

To automate the renew process I use crontab and a bash script. For anyone interested here's my script. Don't forget to replace all three "/path/to".

renew.sh

```
#!/bin/bash
logfile="/path/to/log.txt"
current_date=$(date '+%Y-%m-%d %H:%M:%S')
docker_command_output=$(docker compose -f /path/to/docker-compose.yaml run --rm certbot renew 2>&1)
echo "$current_date" >> "$logfile"
echo "$docker_command_output" >> "$logfile"
```

‹ Configurer HTTPS avec Nginx, Let's Encrypt et Docker

PHP8's Named arguments ›

À propos

Pourquoi le Mindsers Blog
Accèder à l'espace de formation
S'inscrire pour soutenir le blog
Nos efforts pour la planète

Partenaires

Promouvoir sur nos media
Recruter dans notre communauté (bientôt disponible)
Embaucher notre développeur

Informations légale

Charte de la communauté
Mentions légales