

Nginx proxy manager

“ Faire du reverse proxy efficace avec Docker

Prérequis

Dans le cadre de cette explication, nous utiliserons l'interface web Portainer afin de faire nos manipulations sur Docker.

VPS / Serveur autohébergé

Nous aurons également besoin d'un VPS. Je vous en recommande un personnellement qui est très peu chère grâce à une offre étudiante et fera très bien le taf :

[PulseHeberg](#)

La première offre est à 15 €/an, ce n'est rien du tout !

Vous pouvez aussi utiliser un serveur autohébergé, à condition d'avoir la redirection de port active vers ce dernier sur votre box.

“ Vous devez avoir les ports **80**, **81** et **443** de disponible sur votre serveur, désactiver donc toute application les utilisant tel que apache, nginx, caddy, ...

Domaine

Puisque nous allons faire du reverse proxy, il est également nécessaire d'avoir un domaine (même gratuit) pour faire nos manipulations

Explication

Les différents types de réseau Docker

Le réseau Bridge (équivalant overlay de swarm)

Un réseau Bridgé est le type de réseau le plus utilisé dans Docker. Les réseaux Bridges créés par les utilisateurs sont semblables au réseau bridge par défaut créé à l'installation de Docker. Cependant, de nouvelles fonctionnalités sont ajoutées, la gestion du DNS par exemple. Lors de la création de nouveau réseau, une nouvelle interface est créée...

Docker daemon exécute un serveur DNS intégré qui fournit une résolution de noms aux conteneurs connectés au réseau créé par les utilisateurs, de sorte que ces conteneurs peuvent résoudre les noms de d'hôtes en adresses IP.

Si le serveur DNS intégré est incapable de résoudre la demande, il sera transmis à tous les serveurs DNS externes configurés pour le conteneur. Pour faciliter cela, lorsque le conteneur est créé, seul le serveur DNS intégré 127.0.0.11 est renseigné dans le fichier **resolv.conf** du conteneur.

Untitled.png

Le driver overlay

Si vous souhaitez une mise en réseau multihôte native, vous devez utiliser un driver overlay. Il crée un réseau distribué entre plusieurs hôtes possédant le moteur Docker. Docker gère de manière transparente le routage de chaque paquet vers et depuis le bon hôte et le bon conteneur.

Untitled 1.png

Le driver host

Ce type de réseau permet aux conteneurs d'utiliser la même interface que l'hôte. Il supprime donc l'isolation réseau entre les conteneurs et seront par défaut accessible de l'extérieur. De ce fait, il prendra la même IP que votre machine hôte.

Untitled 2.png

Ajout du réseau

Dans le cadre de notre manipulation, nous allons utiliser le réseau Bridge.

Pour cela, rendez-vous sur Portainer dans la section **Network**

Untitled 3.png

Cliquez sur **Add a network**

Untitled 4.png

Nommez votre réseau (dans mon cas **proxy_network**), sélectionnez le type de réseau **Bridge** et cochez **Enable manual container attachment**.

Créez le réseau.

[Untitled 5.png](#)

Le réseau apparaît alors dans la liste des réseaux.

[Untitled 6.png](#)

Installation Nginx Proxy Manager

Rendez-vous dans la section **Containers** et cliquez sur **Add container**

[Untitled 7.png](#)

Nommez votre instance, donc mon cas, **nginx_proxy_manager**, renseignez l'image docker `jc21/nginx-proxy-manager:latest` et ouvrez les ports :

- 443 ⇒ Port d'accès HTTPS
- 80 ⇒ Port d'accès HTTP
- 81 ⇒ Port du dashboard HTTP

[Untitled 8.png](#)

Au niveau des **Volumes**, il faudra connecter :

- /data ⇒ configuration de nginx proxy manager
- /etc/letsencrypt ⇒ stockage des certificats

[Untitled 9.png](#)

Dans la section **Network**, sélectionnez le réseau **Bridge** créé précédemment, dans mon cas **proxy_network**.

Pensez également à renseigner un **Hostname**.

[Untitled 10.png](#)

Mettez la **Restart policy** à **Always**

[Untitled 11.png](#)

Cliquez ensuite sur **Deploy the container**

[Untitled 12.png](#)

Notre container est correctement lancé avec les ports configurés ouverts

Connexion au dashboard

Pour accéder au dashboard, il faut se rendre en HTTP sur le port 81 de notre server : `http://ip-du-serveur:81/`

Les identifiants par défaut sont :

- Email : **admin@example.com**
- Password: **changeme**

À la première connexion, il vous sera demandé de changer vos identifiants, faites le ! Et surtout, renseignez une adresse email **valide**, c'est important pour la suite.

Une fois connecté, nous pouvons voir les différentes configurations mises en place ou non. Par défaut il n'y a rien de présent (Dans la capture, j'avais déjà setup 2-3 trucs).

Configuration du reverse proxy sur le dashboard

Actuellement, nous accédons au dashboard sur le port 81 avec une connexion HTTP. Ça n'est pas **ACCEPTABLE**. Le premier reverse proxy que nous allons créer sera destiné à accéder au dashboard lui-même via un domaine et une connexion HTTPS sécurisé.

Rendez-vous sur **Hosts** → **Proxy Hosts**, puis cliquez sur **Add Proxy Host**

Renseignez les différents champs du premier onglet **Details** :

- **Domain Names** : Le nom du domain par lequel nous souhaiterons accéder à notre reverse proxy, dans le cas du dashboard je l'appellerais `proxy.nospy.fr`
- **Scheme** : Le protocole d'accès à notre service interne. En l'occurrence, ça sera du HTTP.
- **Forward Hostname / IP** : Il s'agit du nom d'hôte / adresse ip de ce que nous souhaitons atteindre **au sein du réseau docker proxy_network**.
Puisque nous cherchons à atteindre le dashboard se trouvant sur le même container, nous renseignerons l'ip local 127.0.0.1 (mais si vous avez bien suivi, on aurait également pu

mettre le nom d'hôte que nous avons renseigné, à savoir **nginx_proxy**).

- **Forward Port** : Le port de destination. Le dashboard est accessible sur le port 81.
- Le reste des options parlent pour elles-mêmes, mais sont facultatives dans le cas du dashboard.

Untitled 17.png

Rendez-vous ensuite sur l'onglet **SSL**, où nous allons configurer le certificat SSL de notre site ainsi que la redirection HTTP → HTTPS.

- Sur le champ **SSL Certificate**, sélectionnez **Request a new SSL Certificate** pour générer un certificat Let's Encrypt et ainsi sécuriser notre page.
- Penser à cocher l'option **Force SSL**, c'est cette dernière qui forcera la redirection HTTP → HTTPS.
- **HTTP/2 Support** permet d'utiliser la version 2 de HTTP
<https://www.hosteur.com/ressources/articles/adopter-http-2>
- **HSTS Enabled** améliore la sécurité de notre flux <https://www.globalsign.com/fr/blog/qu-est-ce-que-le-hsts-comment-le-mettre-en-uvre>
- Veillez à ce que l'adresse email renseigné pour **Let's Encrypt** soit correct ! Sinon ça peut ne pas fonctionner...

Untitled 18.png

Untitled 19.png

Cliquez sur **Save** et patientez le temps que Nginx Proxy Manager mette en place le reverse proxy et configure le certificat SSL (cette étape peut prendre un peu plus d'une minute la première fois et nécessite que vous ayez correctement configuré votre nom de domaine pour qu'il pointe sur votre serveur).

Si tout s'est bien passé, nous devrions apercevoir dans la section **Hosts → Proxy Hosts** une ligne concernant notre reverse proxy mis en place.

La section **SSL certificates** devrait également contenir le certificat SSL Let's Encrypt généré pour notre nom de domaine. Le renouvellement de ce dernier est automatique, mais peut être déclenché manuellement.

Untitled 20.png

Untitled 21.png

Désormais, si nous essayons de nous connecter à notre domaine et qu'il est bien configuré (dans mon cas, proxy.nospay.fr) , nous devrions accéder à notre dashboard de manière sécurisée.

Untitled 22.png

Et voilà !

Une fois que vous avez bien accès à votre dashboard, de façon sécurisée cette fois-ci, nous allons modifier notre container pour fermer le port 81 au niveau du binding, car nous n'avons plus besoin qu'il soit accessible de l'extérieur grâce au reverse proxy interne.

Untitled 23.png

Untitled 24.png

Untitled 25.png

Reverse proxy sur un autre container

Ayez au préalable configuré vos noms de domaines et sous-domaines que vous comptez utiliser pour qu'ils pointent correctement sur vos serveurs

Maintenant que nous avons un dashboard sécurisé, nous allons configurer un reverse proxy sur un autre container. Dans mon cas, j'utiliserais une image **nginx** toute simple.

N'importe qu'elle image ayant un service web dessus fonctionnerait, vous devez juste avoir la connaissance de cette image, notamment le port utilisé, s'il nécessite l'activation de web sockets...

Je vais donc ajouter un container, et le mettre sur mon réseau créé précédemment (**proxy_network**) tout en spécifiant un nom d'hôte spécifique (dans mon cas **nginx_container**).

Untitled 26.png

Je ne ferai pas de redirection de port vers ma machine hôte, car tout sera géré en interne via notre reverse proxy.

Untitled 27.png

Retournons désormais sur **Nginx Proxy Manager** dans la section **Hosts → Proxy Hosts** et ajoutez un nouveau proxy.

- Au niveau du domaine, renseignez celui que vous souhaitez utiliser.
- Pour le **Scheme**, renseignez vous sur ce que votre image utilise en interne (dans le cas de mon image nginx ça sera du http).
- **Hostname** : le nom d'hôte du container cible (ici, je l'avais nommé **nginx_container**).
- **Forward Port** : même chose que le scheme (ici, 80).

Untitled 28.png

Dans l'onglet **SSL**, il faut aussi configurer correctement notre accès sécurisé, comme pour le dashboard.

Untitled 29.png

On sauvegarde et on va vérifier que tout s'est bien passé au niveau des **Proxy Hosts, SSL Certificates**.

Enfin, on va sur le domaine en question pour s'assurer que notre site est bien en ligne.

Untitled 30.png

Untitled 31.png

Untitled 32.png

Redirection `www.domain ? domain`

Dans certaines situations, on souhaiterait faire en sorte que notre site soit disponible sous le domaine www.domaine.com et également `domaine.com`. Dans cette situation, on aimerait bien que le domaine en `www.` redirige vers celui sans.

Pour cet exemple, je vais reprendre le site nginx que j'ai exposé dans l'exemple précédent.

Pour ce faire, nous allons nous rendre dans la section **Hosts → Redirection Hosts**

Cliquez sur **Add Redirection Host** et remplissez les champs comme il se doit.

- **Domain names** : Les différents domaines que l'on souhaite rediriger
- **Scheme** : le protocole HTTP sur lequel rediriger (on préférera HTTPS tout de même)
- **Forward domain** : le domain de destination sur lequel rediriger
- **HTTP Code** : le code HTTP de redirection que l'on souhaite transmettre
- **Preserve Path** : On garde le suffixe de notre requête et ne changeons que le domaine.

Untitled 33.png

Désormais, si je me rends sur le site www.nginx.nospy.fr, je serais automatiquement redirigé vers nginx.nospy.fr

Untitled 34.png

Wildcard DNS record

Celle-là, c'est cadeau !

Si vous avez un serveur sur lequel vous souhaitez rediriger plein de sous domain sans vous embêter à devoir les déclarer en permanence sur votre hébergeur DNS, vous pouvez déclarer un

Wildcard DNS record.

Cela fonctionne un peu comme un sorte de **Regex** où tout les sous domaines concernés par le filtre irons automatiquement vers une adresse IP, sans avoir à les configurer à chaque fois.

Dans mon exemple, je possède un domaine chez **OVH**, mais l'opération est faisable chez d'autre.

Admettons que je veuille que tout les domaine finissant par **.app.nospy.fr** redirige vers le même serveur (proxy.app.nospy.fr, vecolo.app.nospy.fr, plex.app.nospy.fr, ...).

Il faut se rendre sur votre zone DNS et déclarer deux entrées.

- La première sera une entrée de type **A**, concernera le sous domaine **app.nospy.fr**, elle pointerà vers l'ip de votre serveur.

[Untitled 35.png](#)

- La deuxième concernera tout les sous domaines qui découlerons de ce suffixe. Pour faire ça, on ajoute une nouvelle entrée de type **A**, mais qui concernera cette fois le sous domaine ***.app.nospy.fr**, et pointerà également vers l'ip de votre serveur.

[Untitled 36.png](#)

Vous vous retrouverez alors ave ces deux entrées, et désormais tout vos sous domaine irons automatiquement dessus, sauf pour les exceptions que vous aurez ajoutées vous-même ☐

[Untitled 37.png](#)

Ressources

[Fonctionnement et manipulation du réseau dans Docker](#)

[Nginx Proxy Manager](#)

[Qu'est-ce que le HTTP/2 et pourquoi l'adopter ?](#)

[Qu'est-ce que le HSTS et comment le met-on en œuvre ? - Blog - GlobalSign](#)

[Wildcard DNS record - Wikipedia](#)

[OVH Autorise enfin les wildcards pour les DNS des noms de domaines!](#)

Revision #3

Created 9 May 2022 19:45:31 by Noé Larrieu-Lacoste

Updated 24 October 2022 09:01:41 by Noé Larrieu-Lacoste