Nginx Proxy Manager

J'utilise l'image de JC21
Voici le compose :

```
services:
  app:
    image: 'jc21/nginx-proxy-manager:latest'
    restart: unless-stopped
    ports:
      - '80:80'
      - '81:81'
      - '443:443'
    volumes:
      - data:/data
      - letsencrypt:/etc/letsencrypt
volumes:
  data:
  letsencrypt:
```

Pour accéder à Nginx proxy manager, il suffit d'aller à l'adresse http du serveur sur le port 81 (qui peut être personnalisé).
Ne pas oublier d'ouvrir les ports 80 et 443 du routeur.

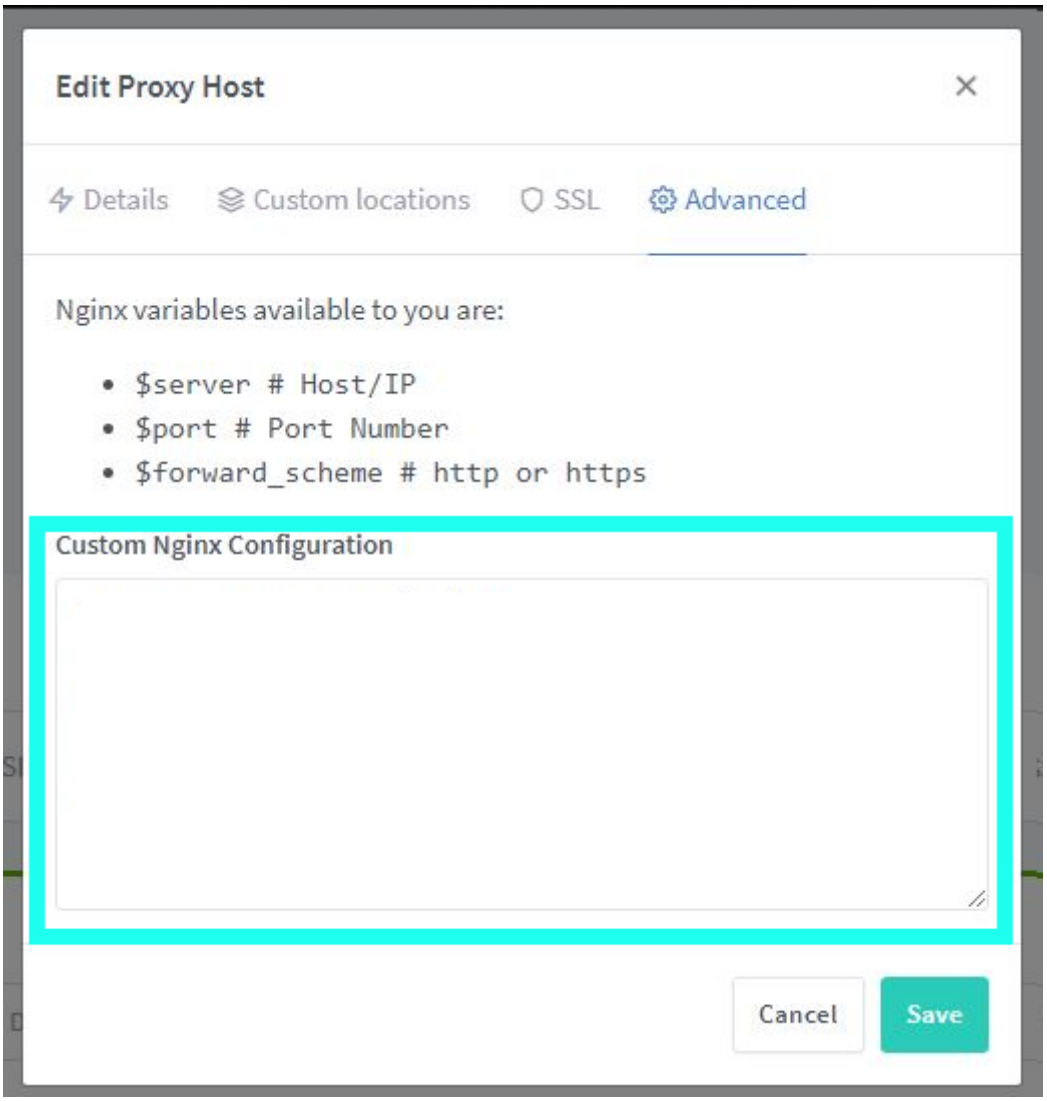
Login par défaut

```
admin@example.com
changeme
```

Source

Ajouter des protections

Ajout de configuration avancé Nginx




```
# Active la protection contre les attaques XSS (Cross-Site Scripting) dans le navigateur web, en bloquant les scripts potentiellement malveillants.
more_set_headers "X-XSS-Protection: 1; mode=block";
# Empêche le navigateur d'effectuer une détection automatique du type de contenu, ce qui empêche certaines attaques de type MIME Sniffing.
more_set_headers "X-Content-Type-Options: nosniff";
# Indique aux moteurs de recherche de ne pas indexer et suivre les liens de cette page.
# Mettre index et follow pour un site web devant être référencer.
more_set_headers "X-Robots-Tag: noindex, nofollow";
# Contrôle les informations de référent envoyées lors de la navigation entre sites web, évitant ainsi les fuites d'informations sensibles.
more_set_headers "Referrer-Policy: no-referrer-when-downgrade";
# Force le navigateur à utiliser HTTPS pour les ressources chargées, au lieu d'HTTP, améliorant ainsi la sécurité.
more_set_headers "Content-Security-Policy: upgrade-insecure-requests";
# Désactive la fonctionnalité d'intérêt des cohorts, qui peut avoir des implications sur la confidentialité des données.
more_set_headers "Permissions-Policy: interest-cohort=()";
```

```
# Empêche le chargement de cette page dans un iframe, sauf si le site est de la même origine, évitant ainsi les attaques de type Clickjacking.
more_set_headers "X-Frame-Options: SAMEORIGIN";
# Indique qu'aucune politique de domaine croisé n'est autorisée, ce qui empêche certaines attaques impliquant du contenu cross-domain.
more_set_headers "X-Permitted-Cross-Domain-Policies: none";
```

Le niveau de sécurité peut être vérifié sur ce site => https://securityheaders.com/

Revision #11
Created 8 January 2023 10:34:18 by Julien
Updated 4 March 2025 12:46:40 by Julien