

# Projet Docker

Lp Devops 1

Amine ABOUSALHAM

## Description :

Mon projet consiste à installer Graylog, un outil de récupération de logs. Il s'agit d'un logiciel open-source qui utilise MongoDB pour stocker ses données de configuration et Elasticsearch pour stocker les logs des applications.

Ce projet consiste également à installer Redis sur un conteneur pour tester la récupération des logs.

## Identifiants Graylog par défaut :

**Login :** admin

**Mot de passe :** projetDevops

Pour changer le mot de passe, il faut générer un hash avec la commande suivante :

**echo -n "Enter Password: " && head -1 < /dev/stdin | tr -d '\n' | sha256sum | cut -d " " -f1**

Puis placer le hash sur le paramètre GRAYLOG\_ROOT\_PASSWORD\_SHA2 dans le fichier docker-compose.yml

```
graylog:
  image: graylog/graylog:4.2
  environment:
    - root_timezone=Europe/Paris
    # username: admin | Password: projetDevops
    - GRAYLOG_ROOT_PASSWORD_SHA2=bda1e3e2ccc60e986d713a14c82ae612a9d080a8810ab901d408b53b9f8ee8d
    GRAYLOG_HTTP_EXTERNAL_URI=http://127.0.0.1:9000/
```

## Déroulement :

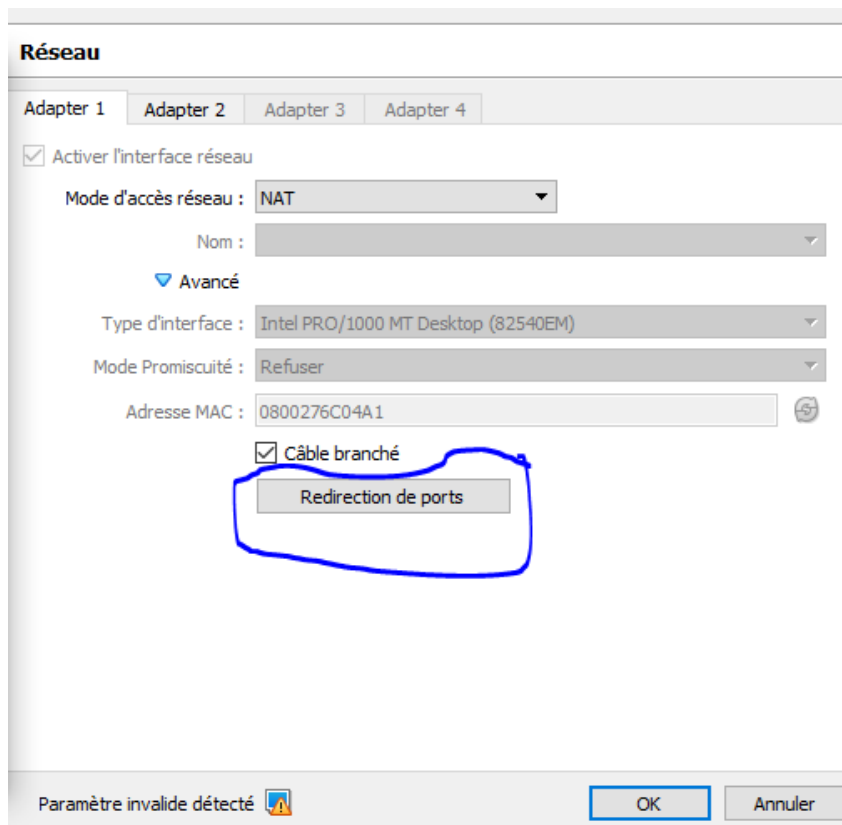
-Extraire le .zip fournie par mail

-Une fois à l'intérieur du dossier projet\_docker\_amine, tapez **docker-compose up**

-Une fois les images téléchargées et les conteneurs lancés, accéder à l'adresse de Graylog :

<http://127.0.0.1:9000/>

-Si vous êtes sur une machine virtuelle fonctionnant en NAT, il faut rediriger le port 9000 sur Virtual Box :



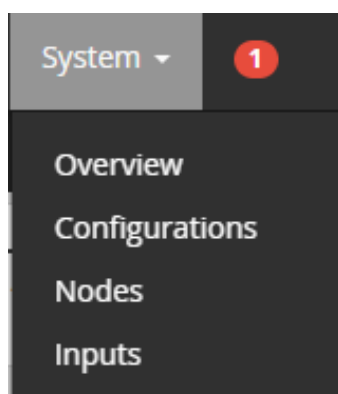
Règles de redirection de ports

Nom	Protocole	IP hôte	Port hôte	IP invité	Port invité
redis	TCP	127.0.0.1	9000		9000
ssh	TCP	127.0.0.1	2222		22

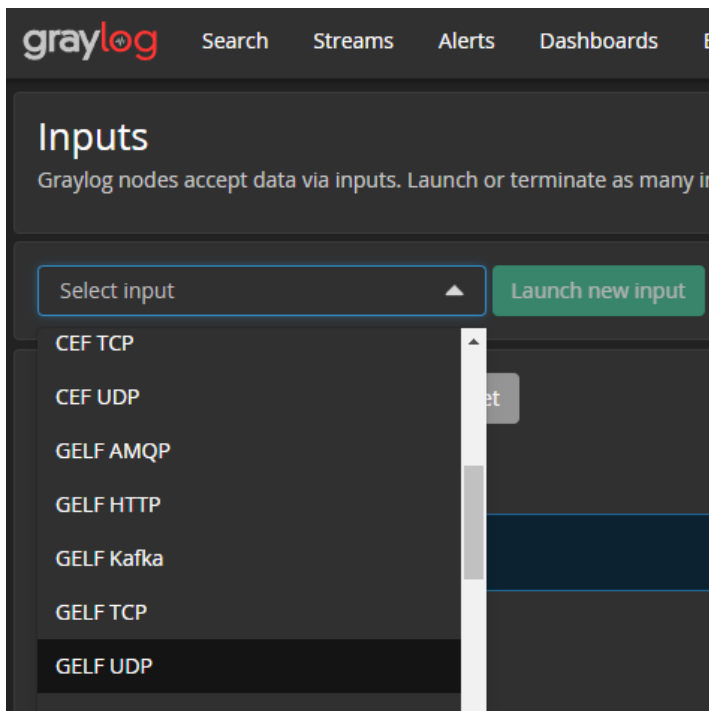
- Graylog peut parfois prendre du temps à se lancer, il faut attendre une bonne dizaine de minutes dans ces cas-là.

- Se connecter avec l'identifiant fourni ci-dessous.

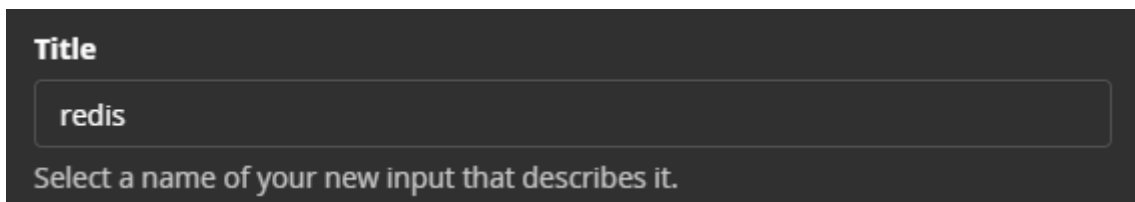
-Une fois sur l'interface graphique, dans la barre de navigation, allez sur System/Inputs.



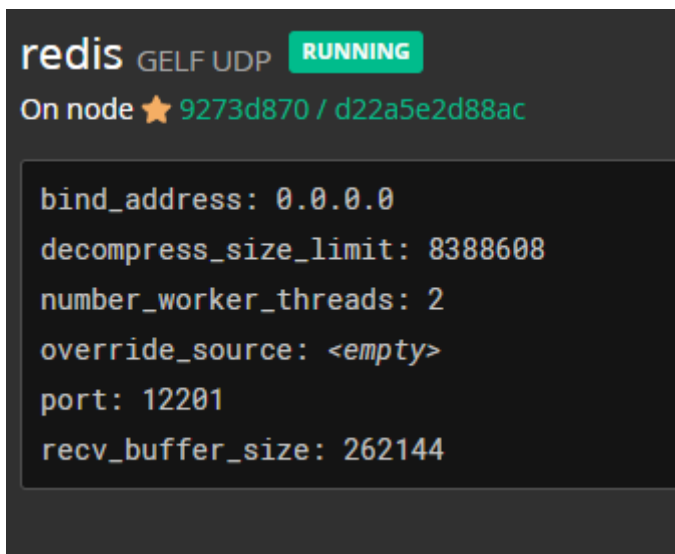
-Créer un Inputs Gelf UDP.



-Sélectionnez un titre et sauvegardez.



L'input doit être à présent lancé :



-Ensuite, on va tester l'envoi d'un log de Redis. Pour cela, on va stopper le conteneur Redis.

-Ouvrez un autre terminal et tapez :

## Docker stop redis

-Sur « show received messages », Vous devriez à présent observez les logs de Redis :

2022-02-15 13:15:26.211 +00:00	
1:M 15 Feb 2022 13:15:26.210 * DB saved on disk	
✉ 908f6aa0-8e62-11ec-9354-0242ac150004	
Timestamp	command
2022-02-15 13:15:26.211	docker-entrypoint.sh redis-server
Received by	container_id
redis on <a href="#">P 9273d870 / d22a5e2d88ac</a>	13c3864858e417995f7db7c936959d8c6ee263b66e1750227e6b0277f30ff86a
Stored in index	container_name
graylog_0	redis
Routed into streams	created
• <a href="#">All messages</a>	2022-02-15 12:47:15.348 +00:00
	image_id
	sha256:3900abf4155226f3f62401054b872ce0c85b5c3b47275cae3d16a39c8646e36b
	image_name
	redis:alpine
	level
	6
	message
	1:M 15 Feb 2022 13:15:26.210 * DB saved on disk
	source
	centos7.localdomain