COURS DOCKER

5ème année Génie Informatique, Ecole Polytechnique Yaoundé

Présenté par : Ing MASSAGA Aristide

Phd student in software engineering

Master 2 in microservice architecture

Software engineer, devops, microservice architect

https://m-aristide.github.io

[Virtualisation et conteneur 2](#_Toc49132214)

[Virtualisation 2](#_Toc340960289)

[Conteneur 2](#_Toc1215385310)

[Présentation de docker plateforme 3](#_Toc504299934)

[Exécution image docker à partir du docker hub 5](#_Toc902899144)

[docker hub 5](#_Toc1116825380)

[docker pull 6](#_Toc304291610)

[docker image 6](#_Toc180859509)

[docker ps 7](#_Toc913591233)

[docker container 8](#_Toc236957802)

[Persistance des données d’un container 9](#_Toc1681313777)

[docker volume 9](#_Toc367320975)

[docker bind mounts 10](#_Toc1925767743)

[Création d’un réseau et exécution de 2 containers dans le réseau 11](#_Toc1789058800)

[Construction image docker 12](#_Toc937372300)

[Publier une image docker 12](#_Toc605200205)

[docker-compose 13](#_Toc1660302761)

[Références 14](#_Toc1862854002)

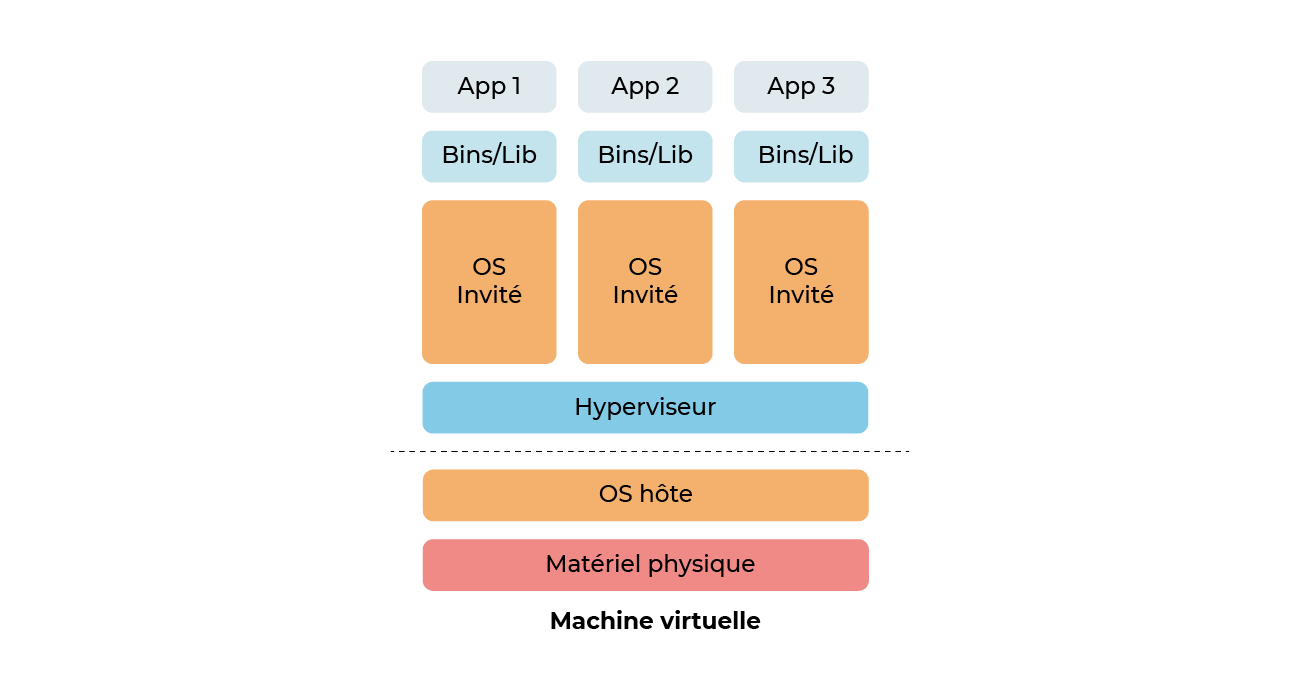
# Virtualisation et conteneur

## Virtualisation

La virtualisation hardware consiste à faire fonctionner sur une même machine physique, plusieurs systèmes comme s’ils fonctionnaient sur des machines physiques distinctes.

Un serveur est composé de plusieurs “couches” :

* Applications (Ce sont les apps tel que Spotify, gmail, word... qui vont “tourner” sur la machine.)
* OS (Operating System ou système d’exploitation : c’est le premier programme à s'exécuter lors du démarrage de la machine et il assure le lien entre les ressources matériel (hardware) de la machine et les applications qui “tournent” dessus. Par exemple, on parle de MacOs,Windows, iOs...)
* Hardware (machine physique peut être autant un téléphone portable, qu’un ordinateur...)



Lorsqu’on utilise une machine virtuelle (VM), ce qu’on appelle de la virtualisation lourde. En effet, vous recréez un système complet dans le système hôte, pour qu’il ait ses propres ressources.

L'isolation avec le système hôte est donc totale ; cependant, cela apporte plusieurs contraintes :

* une machine virtuelle prend du temps à démarrer ;
* une machine virtuelle réserve les ressources (CPU/RAM) sur le système hôte.

Mais cette solution présente aussi de nombreux avantages :

* une machine virtuelle est totalement isolée du système hôte ;
* les ressources attribuées à une machine virtuelle lui sont totalement réservées ;
* vous pouvez installer différents OS (Linux, Windows, BSD, etc.).

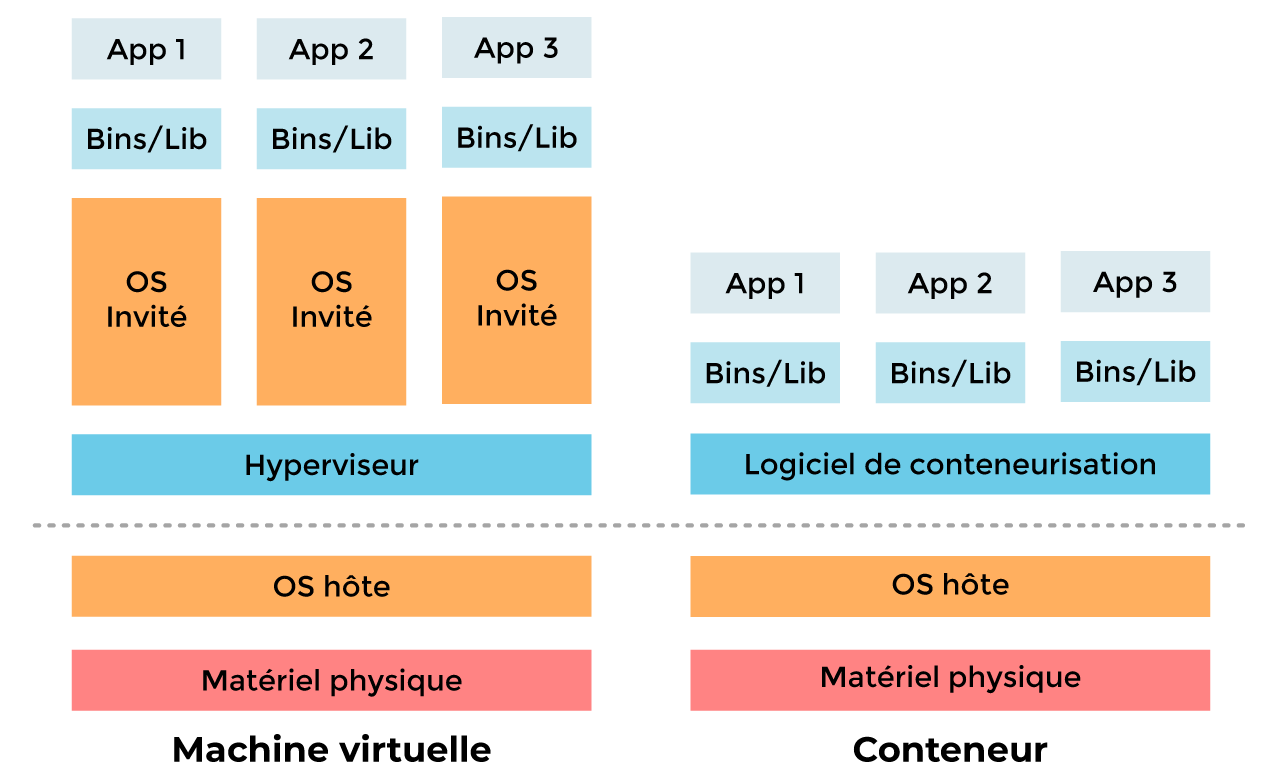
Mais il arrive très souvent que l'application qu'elle fait tourner ne consomme pas l'ensemble des ressources disponibles sur la machine virtuelle.

## Conteneur

Les machines virtuelles et les conteneurs sont proches, car ce sont toutes les deux des technologies de virtualisation.

Un conteneur Linux est un processus ou un ensemble de processus isolés du reste du système, tout en étant légers.

Le conteneur permet de faire de la virtualisation légère, c'est-à-dire qu'il ne virtualise pas les ressources, il ne crée qu'une isolation des processus. Le conteneur partage donc les ressources avec le système hôte.



Les conteneurs, au sens d'OpenVZ et LXC, apportent une isolation importante des processus systèmes ; cependant, les ressources CPU, RAM et disque sont totalement partagées avec l'ensemble du système. Les conteneurs partagent entre eux le kernel Linux ; ainsi, il n'est pas possible de faire fonctionner un système Windows ou BSD dans celui-ci.

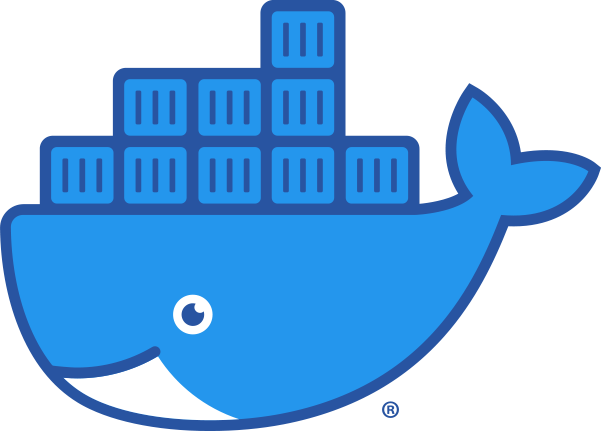
Ainsi l’utilisation de conteneur comme système de virtualisation apporte :

* Réduction de l'utilisation des ressources RAM et CPU
* Démarrez rapidement vos conteneurs
* Faible isolation entre les conteneurs et l'OS

# Présentation de docker plateforme

Docker est un projet open source (Apache 2.0) écrit en GO et hébergé sur GitHub:

<https://github.com/docker>. Docker, c’est donc à la fois le nom d’une technologie, les conteneurs, et celui d’une entreprise américaine créée par Solomon Hykes.



Contrairement aux systèmes de conteneur existant tels LXC ou OpenVZ, Docker apporte une notion importante dans le monde du conteneur. Dans la vision Docker, un conteneur ne doit faire tourner qu'un seul processus.

Docker Inc distribue 3 versions de Docker différentes :

* Docker Community Edition (Linux seulement) ;
* Docker Desktop (Mac ou Windows) ;
* Docker Enterprise (Linux seulement).

Docker est composé de trois éléments :

* le daemon Docker qui s’exécute en arrière-plan et qui s’occupe de gérer les conteneurs (Containerd avec runC)
* une API de type REST qui permet de communiquer avec le daemon
* Le client en CLI (command line interface) : commande docker

Par défaut, le client communique avec le daemon Docker via un socket Unix (/var/run/docker.sock) mais il est possible d’utiliser un socket TCP.

Dans docker nous allons manipuluer deux concepts principaux :

* Image : template de conteneur en read-only contenant un systeme de base et une application.
* Conteneur : Image exécutable d’un environnement complet incluant code, librairies, outils et configuration.

Avantages de Docker :

* Légèreté : Du fait que les conteneurs n'incluent pas la logique de l'OS mais uniquement ce qui est nécessaire au bon fonctionnement de l'applications
* Portabilité : Il est possible de créer, déployer et démarrer des conteneurs sur n’importe quel ordinateur ou serveur distant.
* Performance : Docker permet une montée en charge facile des applications car il va pouvoir les multiplier sur tout un ensemble d’OS, et fournir de la haute disponibilité.

Le problème principal lié à l’utilisation de conteneur est la sécurité :

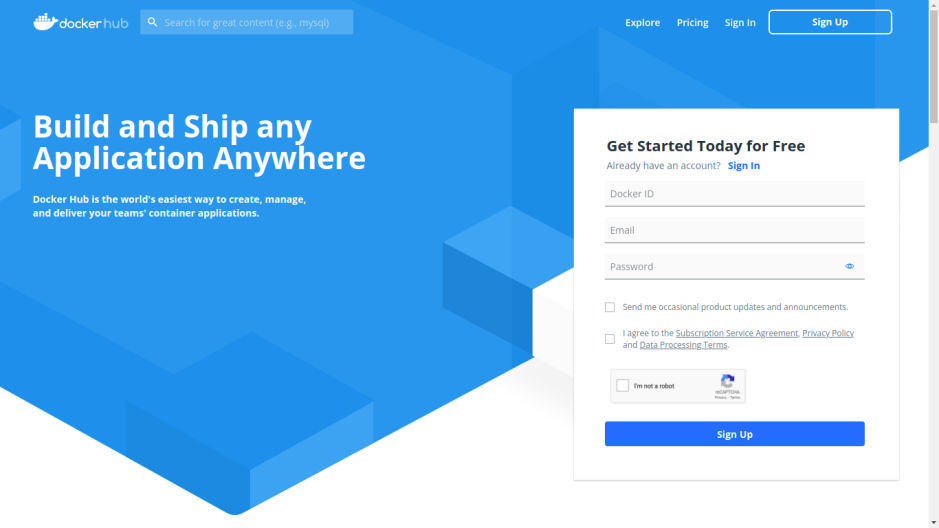
* Il facile pour un pirate de passer du conteneur vers le système d’exploitation hôte
* Attention aux applications déjà conteneurisées : vous aller peut-être faire entrer un cheval de Troie dans votre serveur.

# Exécution image docker à partir du docker hub

## docker hub

<https://hub.docker.com/>

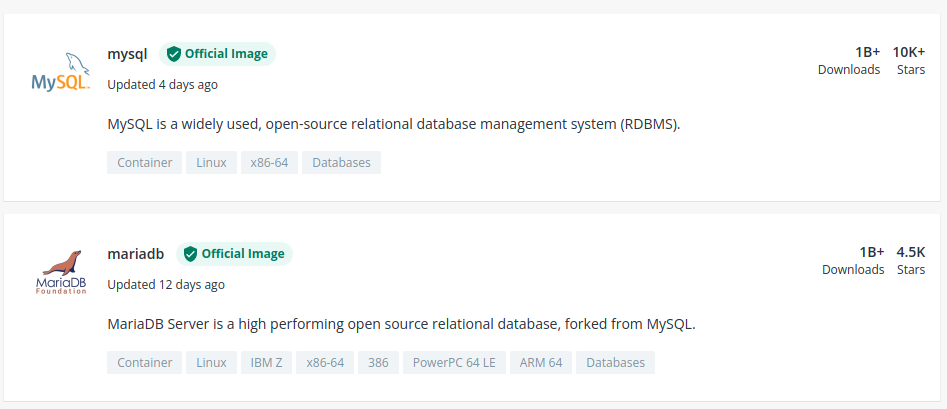
C’est un repository d’images docker



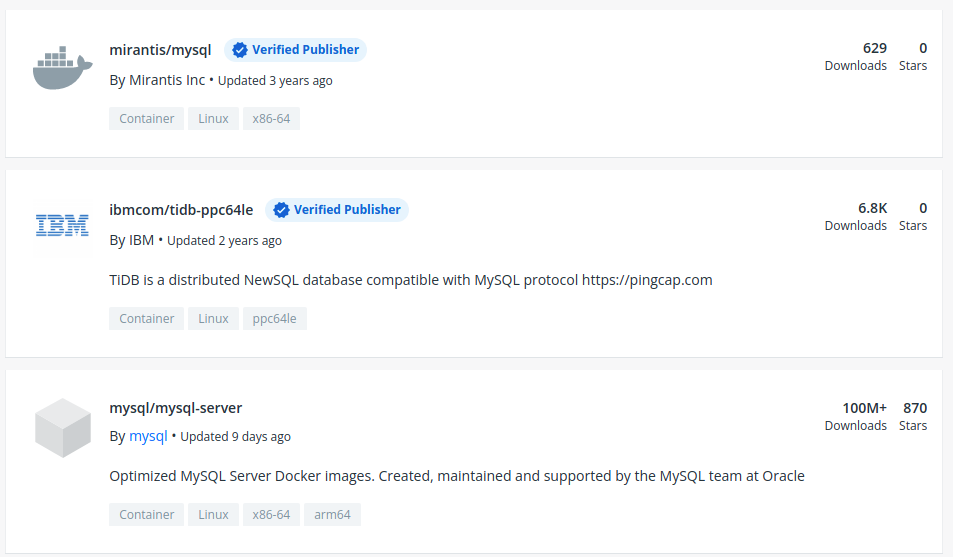
Ce qui nous intérèsse ici c’est de comprendre les informations que nous donne docker hub sur les images docker.

Sur le hub il existe 3 catégories d’images :

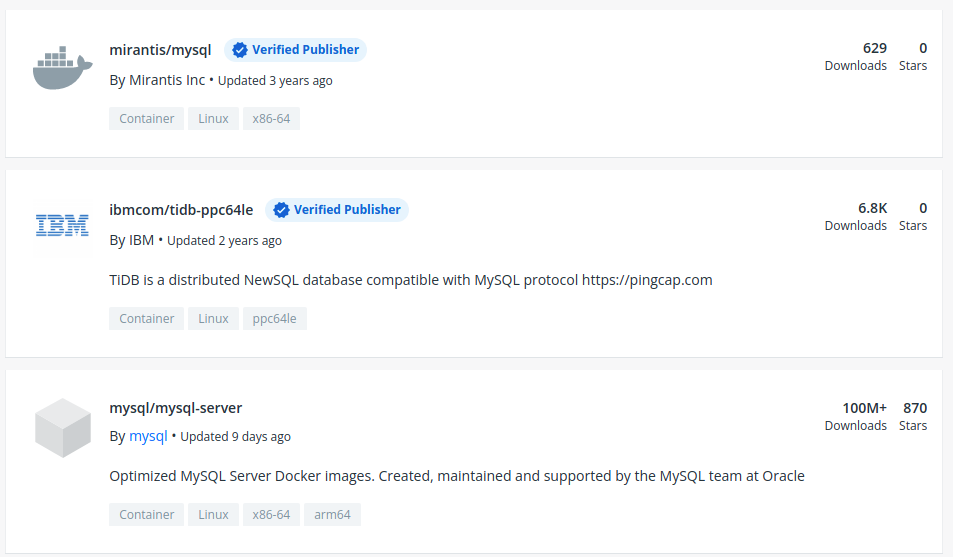
* les images officielles (Official image)



* les images dont l’auteur a été vérifié (Verified Publisher)

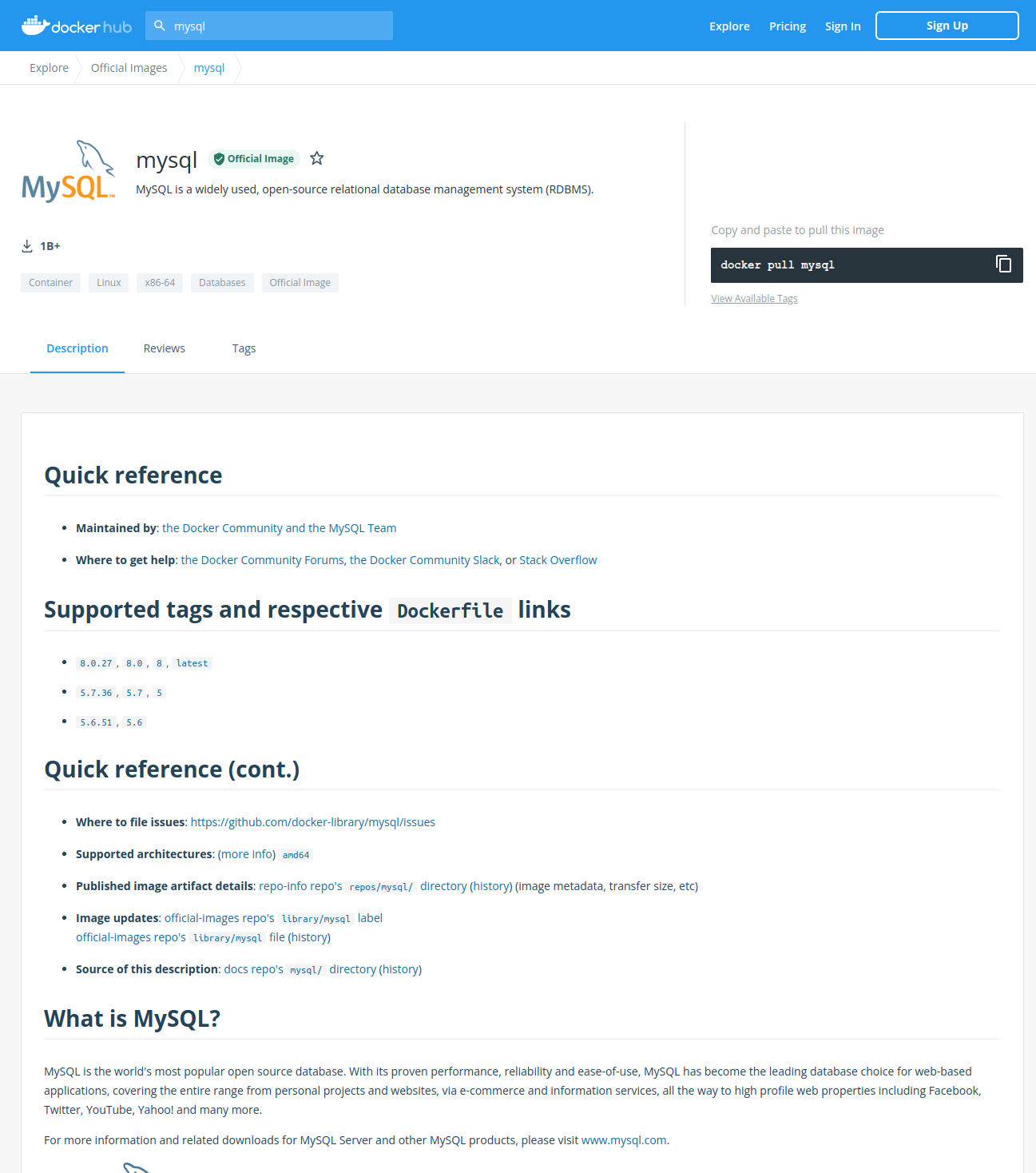


* les images tiers, car tout le monde peut publier une image



Le images officielles et les images vérifiées apportent de la sécurité quant à l’origine de l’image docker.

Chaque image docker a une page où, les informations sur l’image, son utilisation, etc sont données



## docker pull

* docker pull hello-world

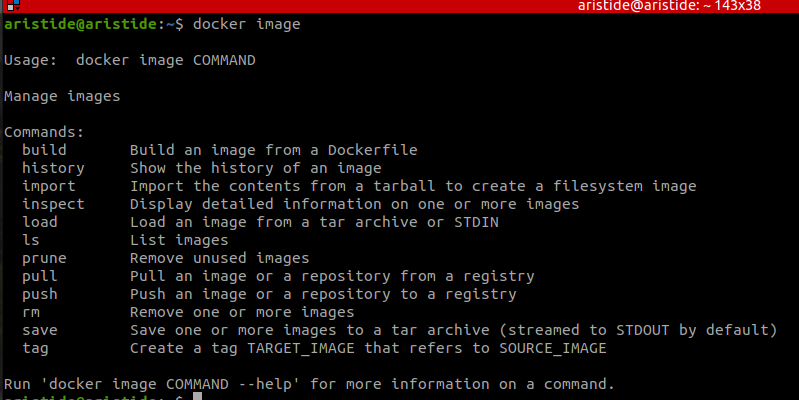
cette commande ira télécharger un l’image docker depuis le docker hub

* docker pull masscorp-dev.win:5000/hello-world

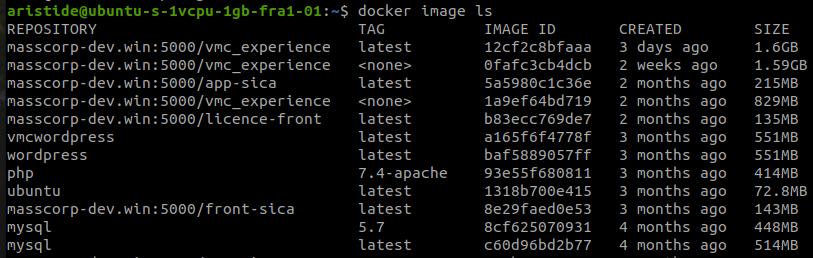
cette commande ira télécharger l’image docker sur le repository dont l’adresse est masscorp-dev.win:5000

## docker image

La liste des commandes disponibles applicables aux images

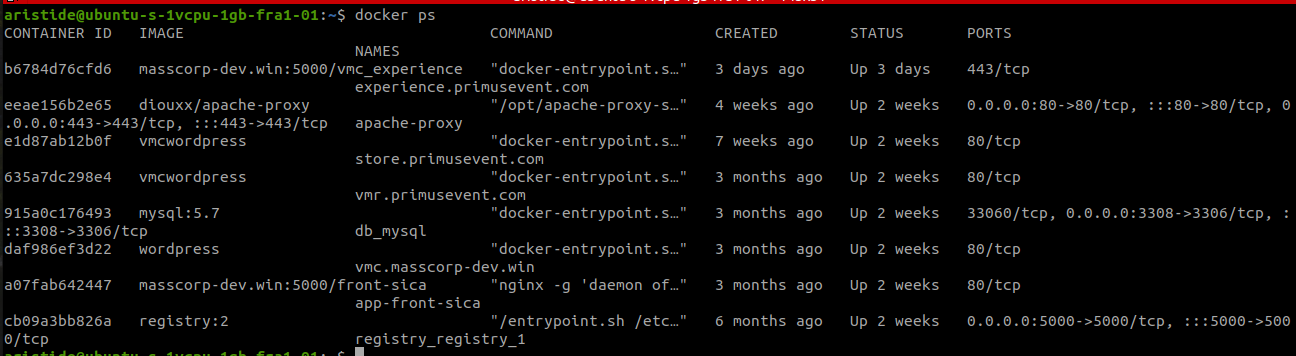


* docker image ls



* REPOSITORY : indique le nom de l’image en incluant l’origine de l’image
* TAG : c’est la version de l’image
* latest : c’est la version par défaut. Lorsqu’une image est construite sans y mettre de version
* <none> : signie qu’on a construit une nouvelle image avec la même version qu’une image qui existait déjà
* 5.7 : c’est une version spécifique
* IMAGE ID : l’identifiant unique de chaque image
* CREATED : la date de création de l’image
* SIZE : le poids de l’image

## docker ps



* CONTAINER ID : c’est l’identifiant unique du container
* IMAGE : c’est l’image d’origine
* NAMES : c’est le nom du container et c’est particulièrement dans le réseau
* COMMAND : c’est le processus que le docker exécute
* CREATED : c’est la date de lancement du container
* STATUS : il indique l’état d’exécution du container
* up : le container est démarré
* exited : le container est arrêté mais présent
* restarting : le container est en train de redémarré
* etc
* PORTS : ce sont les ports déclarrés lors de la construction de l’image et les ports que auxquels ces ports sont mapés sur la machine physique.

Exemple :

docker pull httpd

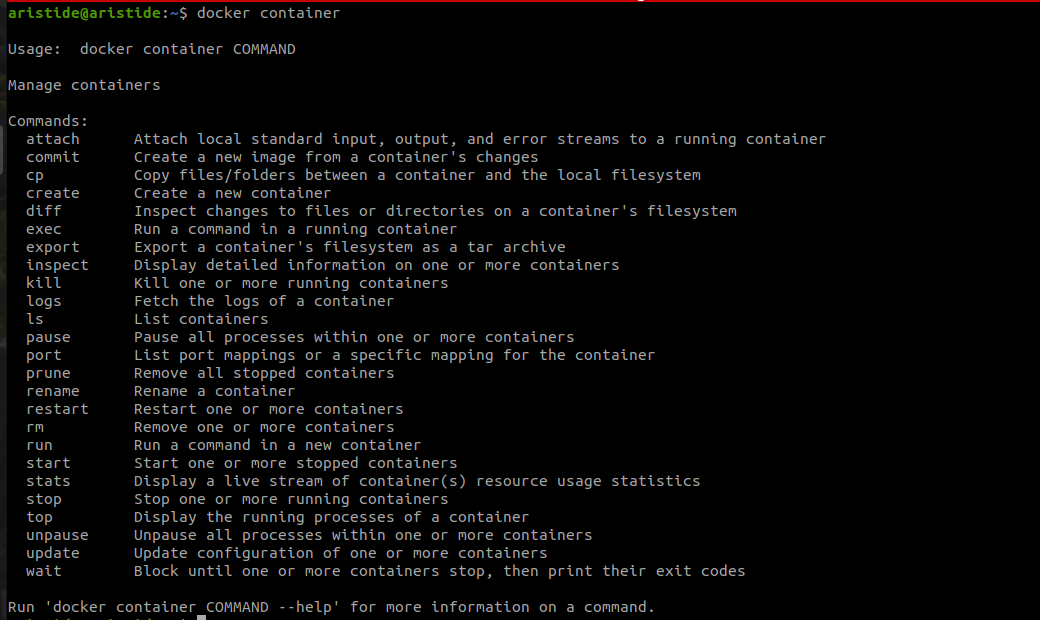
docker run -p 8080:80 httpd

docker run -p 8080:80 -d httpd

docker ps

htop

## docker container



* docker inspect name\_container

Permet d’obtenir les informations sur le container en cours d’exécution. Les informations sont énromes :

* Les informations sur la configuration réseau du container : NetworkSettings
* Les variables d’environnement passées au container
* Les informations sur les volumes

Exemple: docker inspect name\_container

* docker start name\_container

Permet de démarrer un container existant. Le container est démarré avec toute sa configuration de lorsqu’il a été créé.

Exemple :

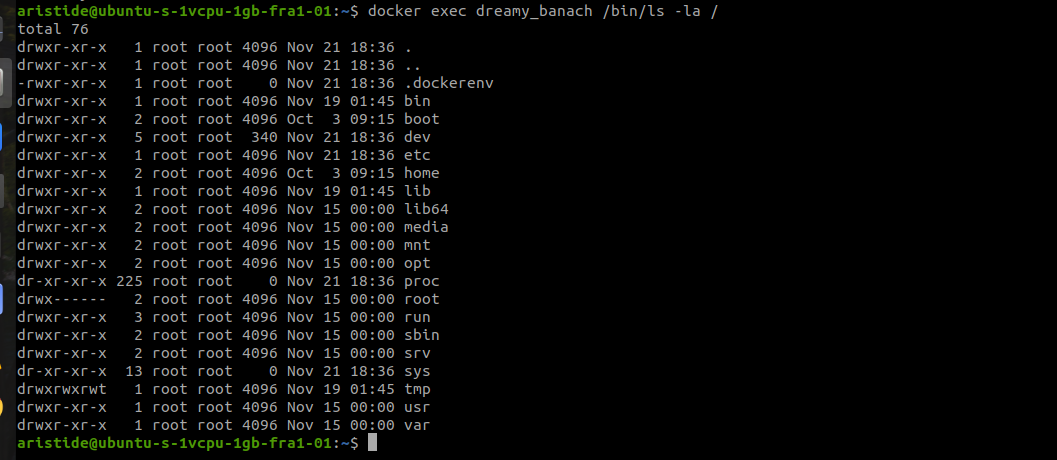
docker stop name\_container

docker start name\_container

* docker exec

Permet d’exécuter une commande à l’intérieur du container

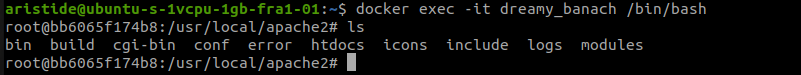
docker exec name\_container /bin/ls -la /



Des options intéressantes avec la commande exec ce sont les options -i et -t

docker exec -it name\_container /bin/bah

Cette commande permet d’ouvrir un terminal dans le docker



Devoir :

- démarrer un container docker apache (httpd)

- modifier la page d’accueil par défaut d’apache pour qu’elle affiche son nom.

- le docker doit être exposé sur le port 6907

Donc en tapant dans le navigateur <http://localhost:6907,> je vois voir s’afficher votre nom.

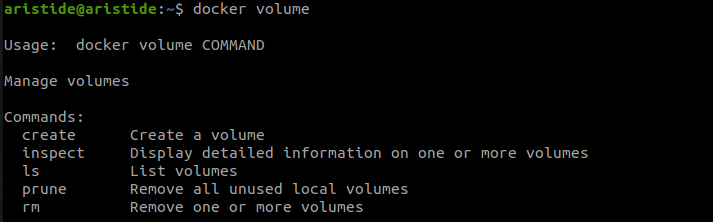
# Persistance des données d’un container

Docker offre plusieurs mécanismes de persistance des données d’un container en cours d’exécution : volume et bind mounts

## docker volume

Ce sont des espaces de stockage créés, gérés et controlés par docker qui sont utilisable par les container. Les volumes sont le mécanisme privilégié pour la persistance des données générées et utilisées par les conteneurs Docker. Les volumes présentent plusieurs avantages par rapport aux montages liés :

* Les volumes sont plus faciles à sauvegarder ou à migrer que les montages bind.
* Vous pouvez gérer les volumes à l'aide des commandes Docker CLI ou de l'API Docker.
* Les volumes fonctionnent sur les conteneurs Linux et Windows.
* Les volumes peuvent être partagés de manière plus sûre entre plusieurs conteneurs.
* Les pilotes de volume vous permettent de stocker des volumes sur des hôtes ou des fournisseurs de clouds distants, de chiffrer le contenu des volumes ou d'ajouter d'autres fonctionnalités.
* Les nouveaux volumes peuvent avoir leur contenu pré-rempli par un conteneur.
* Les volumes sur Docker Desktop sont beaucoup plus performants que les montages liés à partir d'hôtes Mac et Windows.

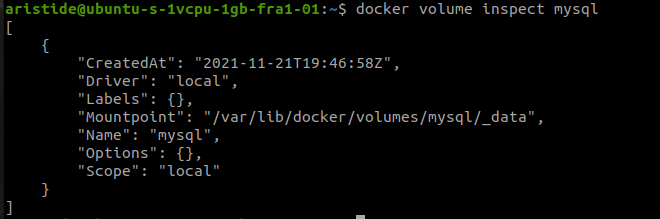


Exemple de volume avec mysql :

docker volume create mysql

docker volume ls

docker volume inspect mysql



docker pull mysql

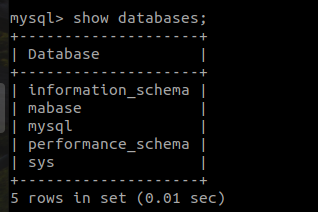
docker run --name myserver -e MYSQL\_ROOT\_PASSWORD=my-secret-pw -d -v mysql:/var/lib/mysql mysql

docker exec -it myserver /bin/bash

mysql -pmy-secret-pw

CREATE DATABASE mabase;

show databases;



exit

exit

docker rm -f myserver

docker run --name newmyserver -e MYSQL\_ROOT\_PASSWORD=my-secret-pw -d -v mysql:/var/lib/mysql mysql

docker exec -it newmyserver /bin/bash

show databases;

## docker bind mounts

Il consiste à faire correspondre un dossier/fichier à l’intérieur du container avec un dossier/fichier dans le système de fichier de la machine hôte. Ils dépendent de la structure des répertoires et du système d'exploitation de la machine hôte. Le fichier ou le répertoire est référencé par son chemin absolu sur la machine hôte.

Il n'est pas nécessaire que le fichier ou le répertoire existe déjà sur l'hôte Docker. Il est créé à la demande s'il n'existe pas encore. Les montages liés sont très performants, mais ils dépendent du fait que le système de fichiers de la machine hôte dispose d'une structure de répertoire spécifique.

Exemple de volume avec mysql :

mkdir -p ~/volumes/mysql

docker run --name myserver -e MYSQL\_ROOT\_PASSWORD=my-secret-pw -d -v ~/volumes/mysql:/var/lib/mysql mysql

ou

docker run --name myserver -e MYSQL\_ROOT\_PASSWORD=my-secret-pw -d --mount type=bind,source=~/volumes/mysql,target=/var/lib/mysql mysql mysql

# Création d’un réseau et exécution de 2 containers dans le réseau

L'une des raisons pour lesquelles les conteneurs et services Docker sont si puissants est que vous pouvez les connecter entre eux, ou les connecter à des systèmes non Docker.

Cette rubrique n'entre pas dans les détails spécifiques aux systèmes d'exploitation concernant le fonctionnement des réseaux Docker. Vous ne trouverez donc pas d'informations sur la façon dont Docker manipule les règles iptables sur Linux ou sur la façon dont il manipule les règles de routage sur les serveurs Windows, et vous ne trouverez pas d'informations détaillées sur la façon dont Docker forme et encapsule les paquets ou gère le cryptage.

Docker offre plusieurs manières de mettre des containers en réseau :

* **User-defined bridge networks** : Les réseaux de pont définis par l'utilisateur sont les meilleurs lorsque vous avez besoin que plusieurs conteneurs communiquent sur le même hôte Docker.
* **Host networks** : Les réseaux d'hôtes sont plus adaptés lorsque la pile réseau ne doit pas être isolée de l'hôte Docker, mais que vous souhaitez que d'autres aspects du conteneur soient isolés.
* **Overlay networks** : Les réseaux superposés sont idéaux lorsque vous souhaitez que les conteneurs s'exécutant sur différents hôtes Docker communiquent, ou lorsque plusieurs applications travaillent ensemble à l'aide de services swarm.
* **Macvlan networks** : Les réseaux Macvlan sont les plus adaptés lorsque vous migrez à partir d'une configuration VM ou lorsque vous souhaitez que vos conteneurs ressemblent à des hôtes physiques sur votre réseau, chacun ayant une adresse MAC unique.
* **Third-party network plugins** : Des plugins réseau tiers vous permettent d'intégrer Docker à des piles réseau spécialisées.

**User-defined bridge networks**

Ce sont des réseaux bridge créés par l’utilisateur. En effet, il existe un réseau bridge par défaut dans docker dans lequel tout nouveau container est ajouté lorsqu’un réseau n’a pas été spécifié.

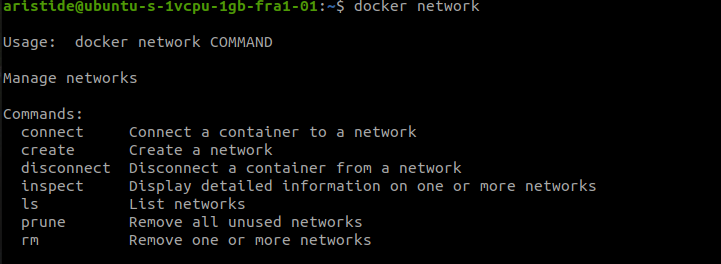
Les User-defined bridge networks ont les caractéristiques suivantes :

* Fournissent une résolution DNS automatique entre les conteneurs.
* Assurent une meilleure isolation.
* Les conteneurs peuvent être attachés et détachés des réseaux définis par l'utilisateur à la volée.
* Chaque réseau défini par l'utilisateur crée un pont configurable.
* Les conteneurs liés sur le réseau pont par défaut partagent des variables d'environnement.

Exemple :

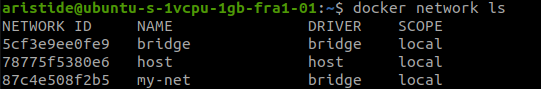
Pour cet exemple nous allons mettre déployer phpmyadmin et mysql dans un même réseau et désormais c’est par phpmyadmin que nous allons manipuler notre base de données.

docker network



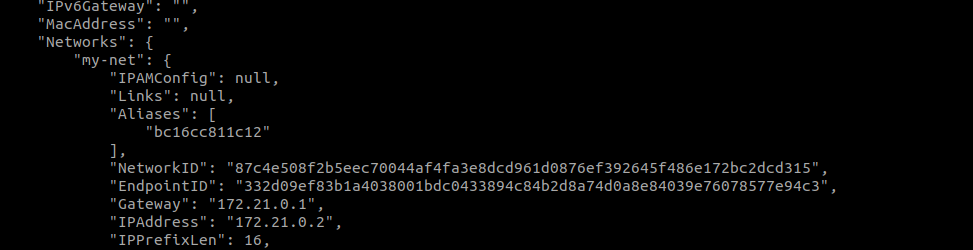
docker network create my-net

docker network ls



docker run --name myserver -e MYSQL\_ROOT\_PASSWORD=my-secret-pw -v mysql:/var/lib/mysql --network my-net -d mysql

docker inspect myserver



docker pull phpmyadmin

docker run --name myadmin -d --link myserver:db -p 8080:80 --network my-net -d phpmyadmin

Devoir :

Déployer un container wordpress utilisant la base de données mysql pour son fonctionnement

# Construction image docker

# Publier une image docker

# docker-compose

# Références