

# La plateforme Docker

Baptiste Bauer

Version v2.0.0, 2022-12-08 17:23:43

# Table des matières

1. Introduction .....	1
1.1. Pour qui ? pourquoi ? .....	1
1.2. Quelques concepts utiles pour les Développeurs .....	4
1.2.1. Un container Linux, c'est quoi ? .....	4
1.2.2. Containers Linux : Les Namespaces .....	4
1.2.3. Containers Linux : Control Groups (cgroups) .....	4
1.2.4. Containers Linux : VM/Container .....	4
1.2.5. Architecture micro-services .....	5
1.2.6. Questionnaire de synthèse .....	9
1.3. Le modèle client/serveur .....	10
1.3.1. Le serveur : Dockerd .....	10
1.3.2. Le client : docker .....	10
1.3.3. Concepts essentiels .....	11
1.3.4. Docker Hub .....	11
1.3.5. Cluster Swarm .....	12
1.4. Installation de Docker .....	13
1.5. Installation sur un poste élève .....	14
1.6. Installation pour Windows 10 ou MacOS .....	21
1.7. Installation pour Linux .....	21
1.8. Vérification de l'installation .....	22
2. Les containers avec Docker .....	24
2.1. Hello World .....	24
2.2. Ubuntu sous docker .....	25
2.3. Un conteneur dans un mode interactif .....	26
2.4. Publication de port .....	28
2.5. Bind-mount .....	29
2.5.1. Exemple : Monter un dossier 'www' .....	29
2.5.2. Exemple: Interagir avec le Docker Daemom .....	30
2.5.2.1. LINUX UNIQUEMENT .....	30
2.5.3. Ecouter les actions demandées au Docker Daemon .....	31
2.5.4. Limitation des ressources .....	31
2.5.5. Les droits dans un conteneur .....	32
2.5.6. Des options utiles .....	33
2.5.7. Les commandes de base avec Docker .....	33
2.6. En pratique : .....	37
2.7. Exercices : .....	39
2.7.1. Exercice 2 : Shell interactif .....	39
2.7.2. Exercice 3 : foreground / background .....	39

2.7.3. Exercice 4 : Publication de port .....	40
2.7.4. Exercice 5 : Liste des containers .....	40
2.7.5. Exercice 6 : Inspection d'un container .....	40
2.7.6. Exercice 7 : exec dans un container .....	40
2.7.7. Exercice 8 : cleanup .....	41
2.8. En résumé .....	41
3. Les images Docker .....	42
3.1. Union Filesystem .....	42
3.2. Exercices .....	43
3.2.1. Exercice 1 : Container's layer .....	43
3.3. DockerFile .....	46
3.4. Création d'images .....	50
3.5. Mise en pratique .....	50
3.6. Exercices : Création d'images .....	54
3.6.1. Exercice 1 : Création d'une image à partir d'un container .....	54
3.6.2. Exercice 2 : Dockerizez un serveur web simple .....	55
3.6.3. Exercice 3 : ENTRYPOINT et CMD .....	55
3.6.3.1. Format .....	55
3.6.3.2. Ré-écriture à l'exécution d'un container .....	55
3.6.3.3. Instruction ENTRYPOINT utilisée seule .....	56
3.6.3.4. Instructions CMD utilisée seule .....	57
3.6.3.5. Instructions ENTRYPOINT et CMD .....	58
3.6.4. Pour aller plus loin : où est stockée mon image ? .....	59
3.6.4.1. Stockage d'une image .....	59
3.7. Multi-Stages Build .....	63
3.8. Mise en pratique .....	64
3.8.1. Un serveur http écrit en Go .....	64
3.8.1.1. Dockerfile traditionnel .....	65
3.8.1.2. Dockerfile utilisant un build multi-stage .....	65
3.9. Prise en compte du cache .....	66
3.9.1. Exercice : Prise en compte du cache .....	69
3.10. Le contexte de Build .....	69
3.11. Les commandes de base avec docker image .....	71
3.12. Exercice : Analyse du contenu d'une image .....	73
4. Registry .....	75
5. Stockage .....	76
5.1. Volume .....	76
5.2. Démo : Volume avec MongoDB .....	78
5.3. Exercice : Utilisation des volumes .....	80
5.3.1. Prérequis .....	80
5.3.2. Persistance des données dans un conteneur .....	81

5.3.3. Définition d'un volume dans un Dockerfile .....	83
5.3.4. Définition d'un volume au lancement d'un container .....	85
5.3.5. Utilisation des volumes via la CLI .....	86
5.4. Drivers de volumes .....	88
5.4.1. Démo : Plugin de volume .....	90
5.4.1.1. Installation et configuration de OPENSSH SERVER sur Windows 10.....	90
5.4.1.1.1. Installation .....	90
5.4.1.1.2. Démarrer et configurer OpenSSH Server .....	91
5.4.1.1.3. Se connecter à OpenSSH Server .....	92
5.4.1.1.4. Installation du plugin et du volume sur la machine hôte:.....	92
6. Docker Machine .....	94
7. Docker Compose .....	95
7.1. Structure du fichier <code>docker.compose.yml</code> .....	95
7.2. Le binaire <code>docker-compose</code> .....	97
7.3. Service discovery .....	97
7.4. Mise en œuvre d'une application microservice : Voting App.....	98
7.5. Voting App Installation sur <code>Play Docker</code> .....	103
7.6. Voting App Installation en <code>local</code> . .....	107
7.6.1. Vue d'ensemble .....	107
7.6.2. Récupération des repos.....	108
7.6.3. Installation du binaire <code>docker-compose</code> .....	108
7.6.4. Le format de fichier <code>docker-compose.yml</code> .....	109
7.6.5. Lancement de l'application .....	111
7.6.6. Containers lancés .....	111
7.6.7. Les volumes créés .....	112
7.6.8. Les networks créés .....	112
7.6.9. Utilisation de l'application .....	112
7.6.10. 8.6.10 Scaling du service worker.....	113
7.6.11. Suppression de l'application .....	114
8. Docker Swarm .....	116
8.1. Swarm mode .....	116
8.1.1. Présentation .....	116
8.1.2. Les primitives .....	116
8.1.3. Vue d'ensemble .....	116
8.1.4. Les commandes de base .....	117
8.2. Raft : Algorithme de consensus distribué .....	118
8.3. Node .....	118
8.3.1. Les états d'un Node (availability) .....	118
8.3.2. Node : Initialisation du Swarm .....	119
8.3.3. Node : Ajout d'un worker .....	119
8.3.4. Node : Ajout d'un manager .....	119

8.3.5. Node : promotion / destitution .....	120
8.3.6. Node : Availability .....	120
8.3.7. Node : Label .....	120
8.4. [DEMO] Création d'un Swarm .....	121
8.5. [Exercice] Création en local .....	123
8.5.1. Quelques rappels sur Docker Swarm .....	123
8.5.2. Crédit des hôtes avec Docker Machine .....	125
8.5.2.1. Docker machine .....	125
8.5.2.2. Docker Desktop (Windows) .....	125
8.5.2.3. Docker Desktop (Mac) .....	126
8.5.2.4. Docker for Ubuntu .....	127
8.5.3. Crédit du swarm .....	128
8.5.3.1. Initialisation à partir de node1 .....	128
8.5.3.2. Ajout des workers .....	129
8.5.4. Inspection d'un hôte .....	130
8.5.5. Mise à jour d'un node .....	133
8.5.5.1. Promotion de node2 .....	133
8.5.5.2. Destitution du node2 .....	133
8.5.6. Résumé .....	134
8.6. [DEMO] Crédit d'un Service .....	134
8.7. Crédit d'un service .....	134
8.7.1. Pré-requis .....	135
8.7.2. Crédit d'un service .....	135
8.7.3. Ajout du service de visualisation .....	137
8.7.4. Passage du node2 en drain .....	139
8.7.5. En résumé .....	139
9. Network .....	140
10. Sécurité .....	141
11. Gestion des logs .....	142
12. Mise en pratique .....	143
12.1. Serveur HTTP avec Docker .....	143
12.2. Serveur HTTPS avec Docker .....	145
12.3. Crédit d'un Dockerfile .....	153
12.4. CICD dans un Swarm, avec GitLab et Portainer .....	159
13. Les étapes .....	160
14. 1ère étape: Crédit d'un serveur web .....	161
14.1. NodeJs .....	161
14.1.1. Installation .....	161
14.1.2. Code source .....	161
14.1.3. Installation de expressjs .....	162
14.2. Lancement du serveur .....	162

14.3. Test . . . . .	162
14.4. Python . . . . .	162
14.4.1. Installation . . . . .	162
14.4.2. Code source . . . . .	162
14.4.3. Installation des dépendances . . . . .	163
14.4.4. Lancement du serveur . . . . .	163
14.4.5. Test . . . . .	163
14.5. Ruby . . . . .	163
14.5.1. Installation . . . . .	163
14.5.2. Code source . . . . .	163
14.5.3. Installation des dépendances . . . . .	163
14.5.4. Lancement du serveur . . . . .	163
14.5.5. Test . . . . .	164
14.6. Go . . . . .	164
14.6.1. Installation . . . . .	164
14.6.2. Code source . . . . .	164
14.6.3. Lancement du serveur . . . . .	164
14.6.4. Test . . . . .	164
14.7. Java / Spring . . . . .	165
14.7.1. Installation . . . . .	165
14.7.2. Packaging de l'application . . . . .	165
14.7.3. Lancement du serveur . . . . .	165
14.7.4. Test . . . . .	165
14.8. DotNetCore . . . . .	165
14.8.1. Création du projet . . . . .	165
14.8.2. Compilation . . . . .	165
14.8.3. Lancement du serveur . . . . .	165
14.8.4. Test . . . . .	166
14.9. 2ème étape : Création d'une image Docker . . . . .	166
14.9.1. Ajout d'un fichier Dockerfile . . . . .	166
14.9.1.1. Exemple de Dockerfile pour un serveur web écrit en Java . . . . .	166
14.9.1.2. Exemple de Dockerfile pour un serveur web écrit en Python . . . . .	166
14.9.1.3. Exemple de Dockerfile pour un serveur web écrit en Node.js . . . . .	166
14.9.1.4. Exemple de Dockerfile pour un serveur web écrit en Go . . . . .	167
14.9.2. Construction de l'image . . . . .	167
14.9.3. Lancement d'un container . . . . .	167
14.10. 3ème étape: repository GitLab . . . . .	167
14.10.1. 1. GitLab.com . . . . .	168
14.10.2. 2. Création d'un projet . . . . .	168
14.10.3. 3. Envoi du code de l'application . . . . .	169
14.11. 4ème étape: Cluster Swarm . . . . .	169

14.11.1. Cr�ation d'un h�te Docker . . . . .	169
14.11.2. Initialisation d'un cluster Swarm . . . . .	169
14.11.3. Installation de Portainer . . . . .	170
14.12. 5�me (et derni�re) �tape: CICD . . . . .	171
14.12.1. Utilisation de GitLab CI . . . . .	172
14.12.2. Ajout d'un test d'int�gration . . . . .	173
14.12.3. Creation d'un service . . . . .	175
14.12.4. Webhook Portainer . . . . .	175
14.12.5. D�ploiement automatique . . . . .	177
14.13. En r�sum� . . . . .	178

# 1. Introduction

Ce cours est découpé en différents chapitres et permet un apprentissage progressif des différents concepts Docker et de leur mise en pratique. On commencera par donner quelques exemples de ce qu'il est possible de faire avec Docker dans la section **Pour qui ? pourquoi ?**. Nous ferons références à des concepts utiles comme les **containers** Linux, les Micro services, le Dev Ops.etc.

Nous aurons un chapitre sur la **plateforme Docker**, son architecture, son fonctionnement et sa mise en place. Nous verrons comment Docker rend très simple la manipulation des **conteneurs**. Nous parlerons de la notion d'images qui permet de **packager** une application et ses dépendances. Dans le chapitre sur le stockage, nous apprendrons à utiliser **Docker** pour que les données puissent persister dans les conteneurs.

**Thèmes abordé dans ce cours :**

- **Docker Machine** pour créer des hôtes Docker.
- **Docker compose** qui permet de créer des applications en multi container.
- **Docker Swarm**, la solution d'orchestration de **Docker** qui permet de gérer des applications qui tournent dans des containers.
- Le **réseau** dans Docker.
- La **sécurité**.

## 1.1. Pour qui ? pourquoi ?

Très souvent le premier contact que l'on a avec **Docker** s'effectue via le **Docker Hub** accessible sur <https://hub.docker.com>.

The screenshot shows the Docker Hub homepage with a search bar at the top. Below the search bar, there are navigation links for Docker, Containers, and Plugins. A sidebar on the left contains filters for Images (Verified Publisher, Official Images) and Categories (Analytics, Application Frameworks, etc.). The main content area displays a list of 8,559,349 available images. Each item in the list includes a thumbnail, the image name (e.g., ubuntu, couchbase, alpine), the official status (Official Image with a checkmark), the last update time, download and star counts, and a detailed description. The first three items shown are:

- ubuntu** (Official Image) - Updated 21 days ago. Description: Ubuntu is a Debian-based Linux operating system based on free software. Tags: Container, Linux, riscv64, PowerPC 64 LE, ARM 64, x86-64, IBM Z, ARM, 386, Base Images, Operating Systems.
- couchbase** (Official Image) - Updated 2 months ago. Description: Couchbase Server is a NoSQL document database with a distributed architecture. Tags: Container, Linux, x86-64, Storage, Application Frameworks.
- alpine** (Official Image) - Updated 7 days ago. Description: A minimal Docker image based on Alpine Linux with a complete package index and only 5 MB in size! Tags: Container, Linux, ARM 64, PowerPC 64 LE, IBM Z, x86-64, riscv64, 386, ARM, Featured Images, Base Images, Operating Systems.

Il s'agit d'un **registre** (ou **registry**) dans lequel nous retrouvons beaucoup d'applications packagées dans des images **Docker**. Cette notion d'image est la base de ce qu'apporte **Docker**. Voici un exemple de services qui peuvent être contenu dans une image **Docker** :



Par exemple, grâce à **Docker** nous pouvons lancer un interpréteur interactif (**REPL**) pour des langages de programmation comme le **Python**, le **Ruby On Rail** ou le **Javascript**.

#### Exemple : REPL

```
# Environment Python
$ docker container run -ti python:3
Python 3.7.0 (default, Sep 12 2018, 02:07:10)
[GCC 6.4.0] on linux
Type "help", "copyright", "credits" or
"license" for more information.
>>>
Permet de lancer un conteneur
```

```
# Environment Node
docker container run -ti node:8.12-alpine
>
```

Contenant Python Version 3.  
":3" est appelé un Tag

Nous avons alors accès à un environnement **Python** en interactif et c'est le flag **-ti** qui permet l'interactivité avec le processus du conteneur.

De la même manière, nous pouvons lancer un environnement **NodeJs**, ici contenant le Tag **8.12-alpine**. **8.12** est la version de **NodeJs** et **alpine** est le nom de la distribution Linux utilisée dans le conteneur.

Par exemple si nous avons besoin d'une base de données **MongoDB** dans la version 4.0. Nous n'avons qu'à trouver une image disponible dans le **Docker Hub**.

## Exemple: base de données MongoDB

# Lancement du container basé sur mongo 4.0  
\$ docker container run -p 27017:27017 -d mongo:4.0

MongoDB disponible sur le port 27017 de la machine en local.

Application en tâche de fond

MongoDB Compass Beta - localhost:27017

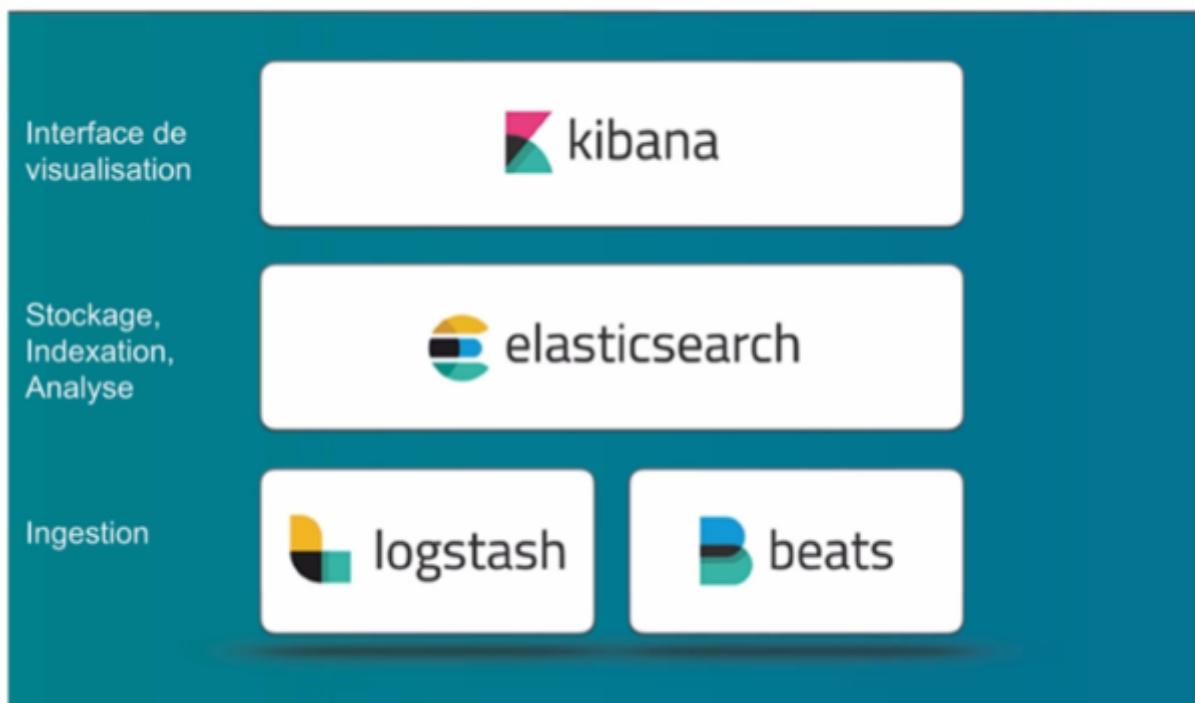
Database Name	Storage Size	Collections	Indexes
admin	4.0KB	0	1
local	4.0KB	1	1

Connexion via MongoDB Compass

On peut imaginer avoir besoin de lancer plusieurs containers **MongoDB** avec des versions différentes. Cela peut être utile pour tester une différence de comportement entre deux versions par exemple.

### ==Des Stacks complètes

Une application fonctionne rarement seule et est souvent constituée d'un ensemble de services. Cet ensemble constitue une **Stack applicative**. Par exemple, prenons le cas de la Stack **Elastic**, qui est souvent utilisée pour la gestion des log. Elle est constituée de **BEATS** et **LOGSTASH** qui est là pour l'ingestion des logs, de **ELASTICSEARCH** pour l'analyse et le stockage des logs et **KIBANA** qui permet de visualiser tout cela.



Il existe une multitude d'applications prêtent à être utilisée avec Docker, accessible en ligne de commande. Nous verrons rapidement comment Docker permet de créer notre propre package d'application pour faciliter : l'installation, l'utilisation et le déploiement.

## 1.2. Quelques concepts utiles pour les Développeurs

### 1.2.1. Un container Linux, c'est quoi ?

Un **container** est simplement un **processus** particulier qui tourne sur le système. Il est isolé des autres **processus**. Il possède sa **propre vision** du système sur lequel il tourne, on appelle cela les **Namepaces**. On peut limiter les ressources utilisées par ce processus en utilisant les **Controls Groups** (ou **Cgroups**). Le même système peut exécuter plusieurs containers en même temps, c'est d'ailleurs ce qui constitue l'avantage de cette technologie. Le noyau Linux de la machine hôte est **partagé** entre tous ses conteneurs.

### 1.2.2. Containers Linux : Les Namepaces

Les **Namepaces** sont des technologies Linux qui servent à isoler un processus. Cela permet de limiter ce qu'un processus peut voir. Il existe **6 NameSpaces** différents :

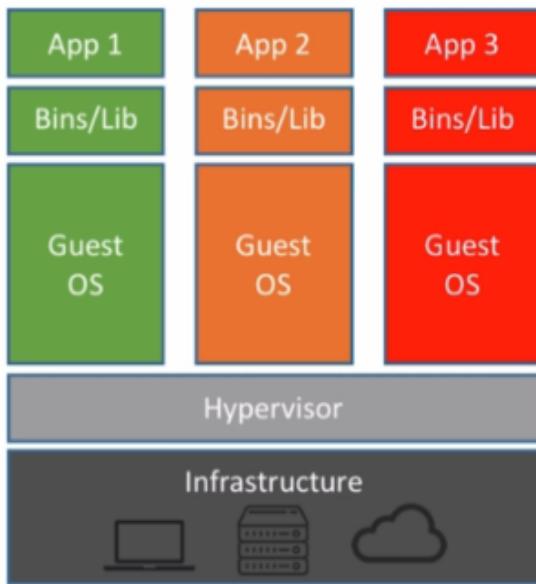
1. **Pid** : Permet de donner à un processus la vision de lui-même et de ses processus enfant.
2. **Net** : Permet de donner au processus son propre réseau privé.
3. **Mount** : Permet de donner au processus un système de fichiers privé.
4. **Uts** : Permet la gestion du nom de l'hôte.
5. **Ipc** : Isole les communications inter processus.
6. **User** : permet de faire un mapping entre les utilisateurs de l'hôte et les conteneurs.

### 1.2.3. Containers Linux : Control Groups (cgroups)

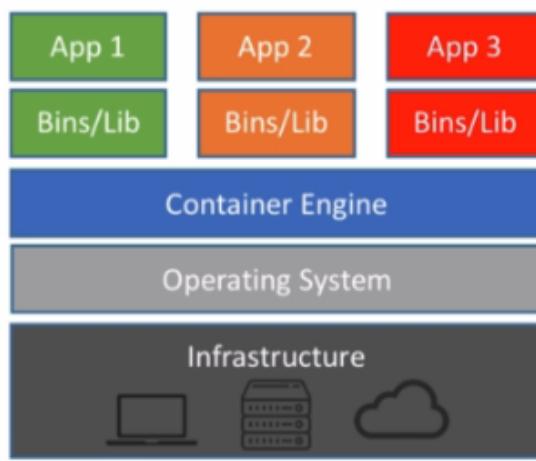
Les **cgroups** sont une autre technologie Linux qui va permettre de limiter les ressources qu'un processus va utiliser. Par exemple, pour limiter l'utilisation :

- **RAM**
- **CPU**
- des **I/O** (périphériques d'entrées et de sorties)
- du **Réseau**

### 1.2.4. Containers Linux : VM/Container



- Nécessite un hyperviseur
- Chaque VM a son OS
- Overhead RAM / CPU



- Processus
- Partage le Kernel de la machine hôte

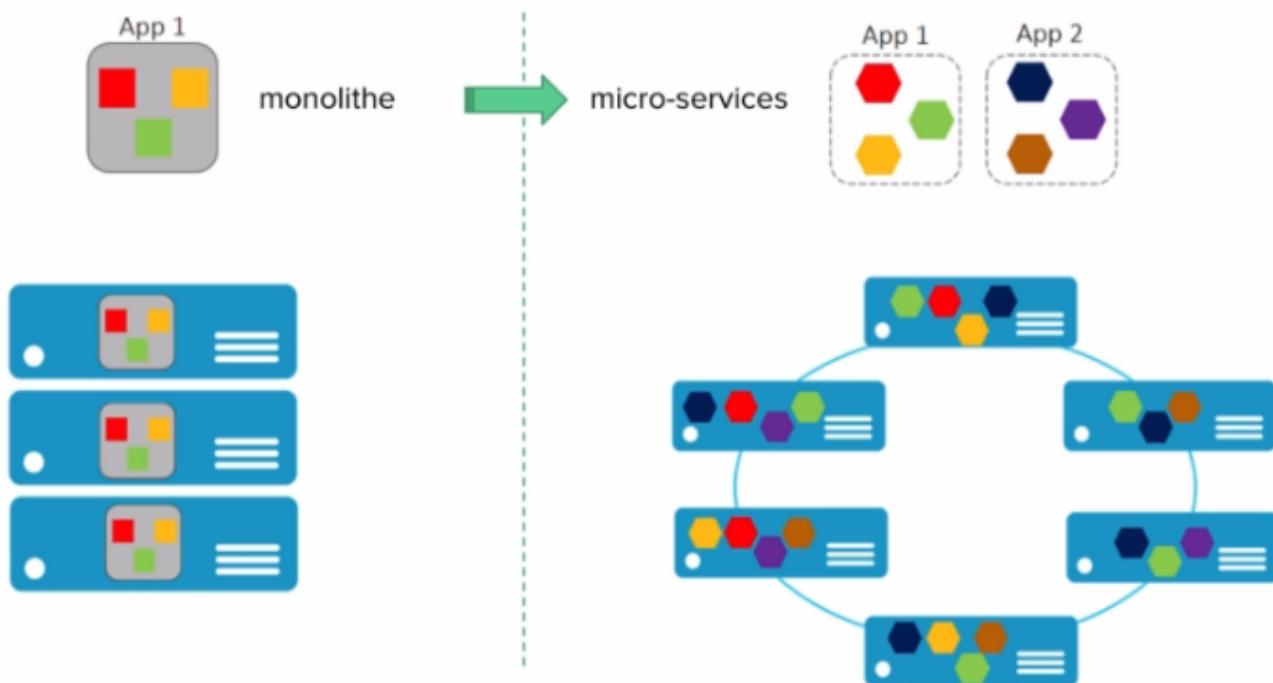
On compare souvent les containers à des machines virtuelles, car elles permettent d'exécuter des applications de manière isolée.

Mais la virtualisation nécessite un **hyperviseur** qui s'exécute sur le **système d'exploitation de l'hôte** et nécessite également que **chaque machine virtuelle** ait son propre système d'exploitation. Alors que l'approche du container est **beaucoup plus légère** car chacun partage le **Kernel Linux de la machine hôte**.

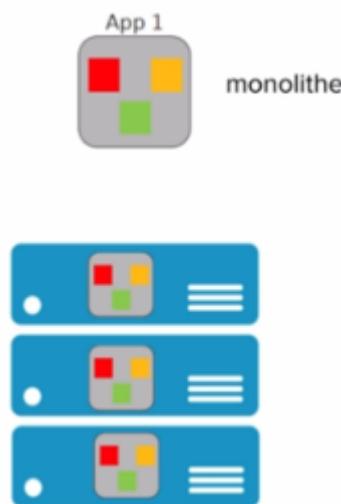
La machine virtuelle consomme plus de disque mémoire et de ram que les containers. **Cela implique que beaucoup plus de containers peuvent fonctionner sur une même machine hôte.**

### 1.2.5. Architecture micro-services

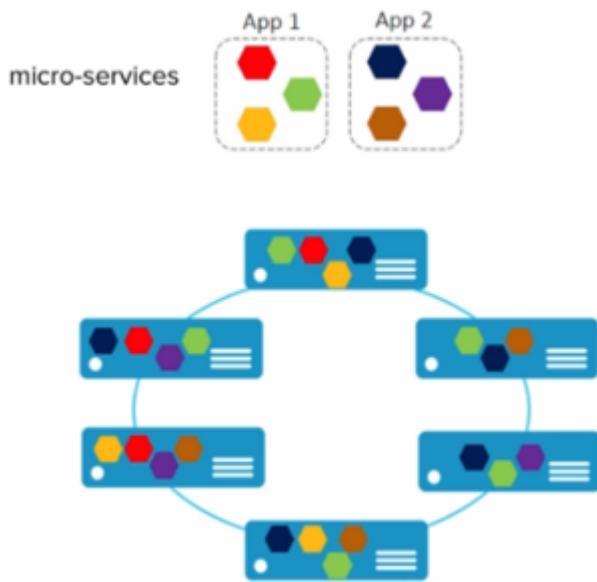
Depuis quelques années, les applications sont développées autour d'une architecture appelée **micro-services**. Alors qu'avant une application était souvent un gros bloc unique **monolithique**.



Aujourd'hui, une application est constituée de **plusieurs petits composants** qui sont des services qui ont leur propre rôle et fonctionnalité. Et c'est l'**interconnexion** de l'ensemble de ces services qui permettent de définir l'application globale.

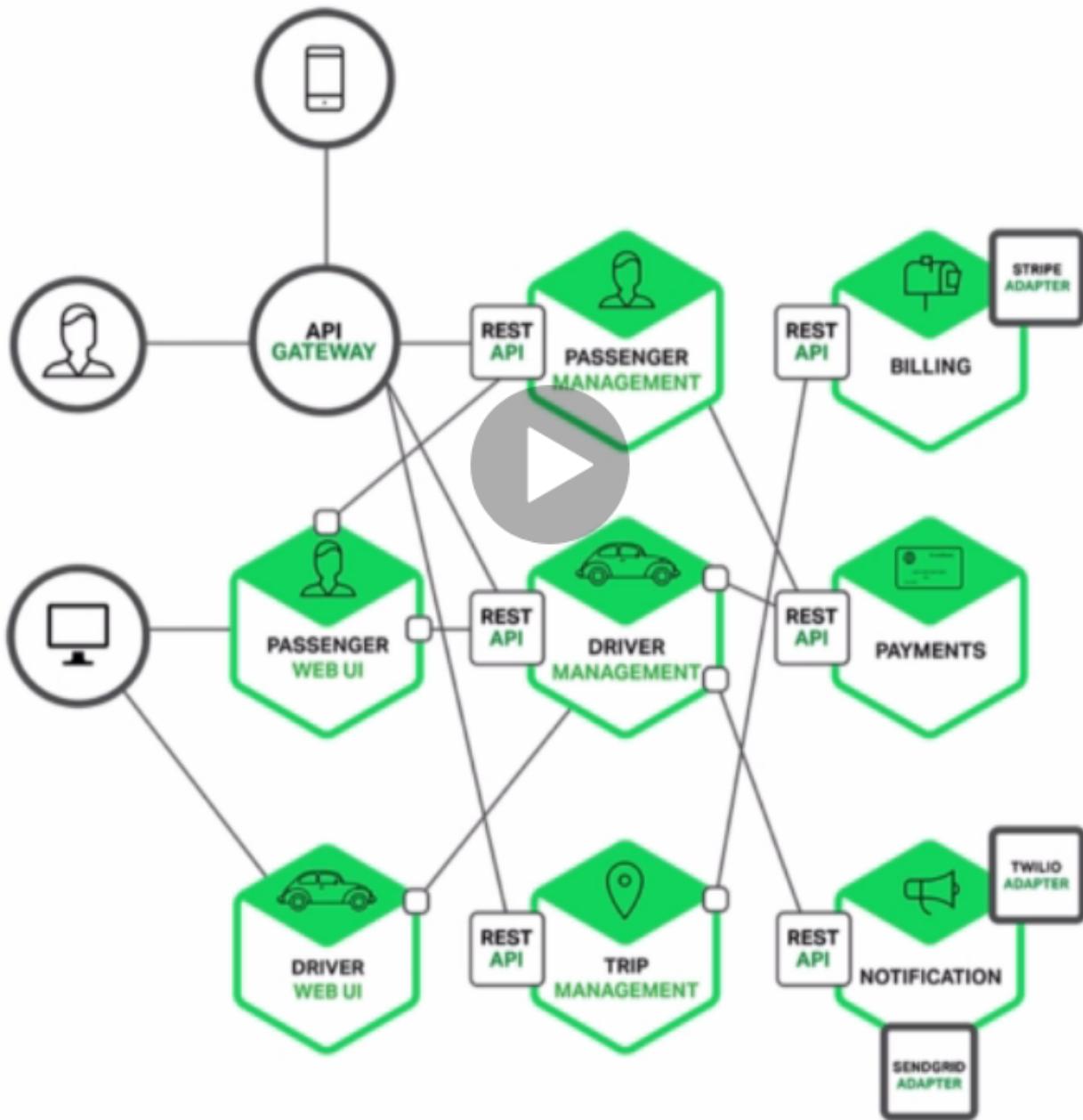


Dans une **application monolithique**, si l'on veut que plusieurs instances de l'application soient déployées il faut créer plusieurs machines virtuelles contenant l'application dans son entiereté.



Alors que dans le contexte d'une application micro-services chaque service peut être déployé indépendamment des autres services, nous avons plusieurs machines virtuelles sur lesquelles les services des différentes applications sont dispatchées.

#### Exemple d'architecture micro-services : l'application UBER



<https://www.nginx.com/blog/introduction-to-microservices/>

Chaque processus métier est isolé dans un service :

- Paiement
- Notification
- Facturation

Avantages de l'architecture micro-services :

- Découpage de l'application en **processus** (services) indépendants.
- Chacun a sa propre **responsabilité métier**.
- **Equipe dédiée** pour chaque service.
- Plus de **liberté** de choix de langage.

- **Mise à jour.**
- Containers très adaptés pour les micro-services.

*Inconvénients :*

- Nécessite des interfaces bien définies.
- Focus sur les tests d'intégration.
- Déplace la complexité dans l'orchestration de l'application globale. (Docker SWARM ou Kubernetes).

## APPLICATION CLOUD NATIVE

On entend de plus en plus parler d'applications **Cloud Native** définies par plusieurs critères :

- Applications qui suivent une architecture **microservices**.
- Utilisant la **technologie des containers**.
- L'orchestration est faite **dynamiquement**.

Il existe une branche de la **Linux Foundation** : la **CNCF** ( Cloud Native Computing Foundation ) qui porte de nombreux projets **Cloud Native** comme :

- **Kubernetes**
- **Prometheus**
- **Fluentd**

[Site de la cncf](#)

### 1.2.6. Questionnaire de synthèse

#### 1. Quels sont les éléments permettant la création d'un container sous Linux ?

- Le kernel Linux et le système de fichiers.
- Les namespaces et les control groups.
- Les control groups et le système de fichiers.

#### 2. Les cgroups permettent :

- De limiter la vision d'un processus
- De limiter les ressources que peut utiliser un processus
- D'isoler le système de fichiers d'un processus
- De faire un chroot

#### 3. Un container c'est

- Une mini machine virtuelle
- Un répertoire sur le système de fichiers
- Un processus qui tourne de manière isolée des autres processus

- Une technologie créée par Docker = La plateforme Docker

**Docker** apporte une facilité de développement, de packaging et de déploiement d'applications **quelque soit le langage de programmation**. Un développeur peut **tester une application** sur sa machine en **imitant** les conditions de l'environnement de **production** tout en nécessitant une **configuration minimale**. Si l'application est soumise à un **fort stresse**, **Docker** peut orchestrer l'allocation d'autres containers. La **scalabilité** s'effectue très rapidement car un container peut être lancé en quelques secondes.



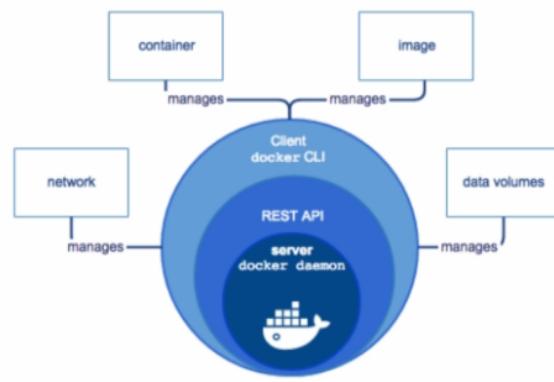
Cherchez la définition du terme **scalabilité**.

Docker permet également d'**augmenter** le rythme de **mise à jour** des logiciels.

## 1.3. Le modèle client/serveur

The screenshot shows a browser window with the URL <https://docs.docker.com/engine/api/v1.37/>. The page displays the Docker Engine API documentation for the 'List containers' endpoint. It includes a sidebar with navigation links like 'CONTAINERS', 'IMAGES', 'NETWORKS', and 'VOLUMES'. The main content area has sections for 'PARAMETERS' (with fields for 'all', 'since', and 'size') and 'Filters' (with a JSON example). To the right, there is a 'RESPONSE SAMPLE' section showing a JSON array of container objects.

<https://docs.docker.com/engine/api/v1.37/>



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

**Docker** utilise un modèle **client/serveur**. D'une part nous avons le client **Docker**, un fichier binaire écrit en **GO**. Et d'autre part nous avons le **Docker Daemon** (appelé **dockerd**), écrit aussi en GO, et qui expose une **API REST** consommée par le client. Le client envoie des commandes au **Docker Daemon** pour gérer les containers, les images entre autres.

### 1.3.1. Le serveur : Dockerd

#### Processus : dockerd

- Gestion des images, networks, volumes, cluster, ...
- Délègue la gestion des containers à containerd.
  - Expose une **API Rest**.
  - Ecoute sur le **socket unix** `/var/run/docker.sock` par défaut.
  - Peut-être configuré pour écouter sur un socket tcp.

### 1.3.2. Le client : docker

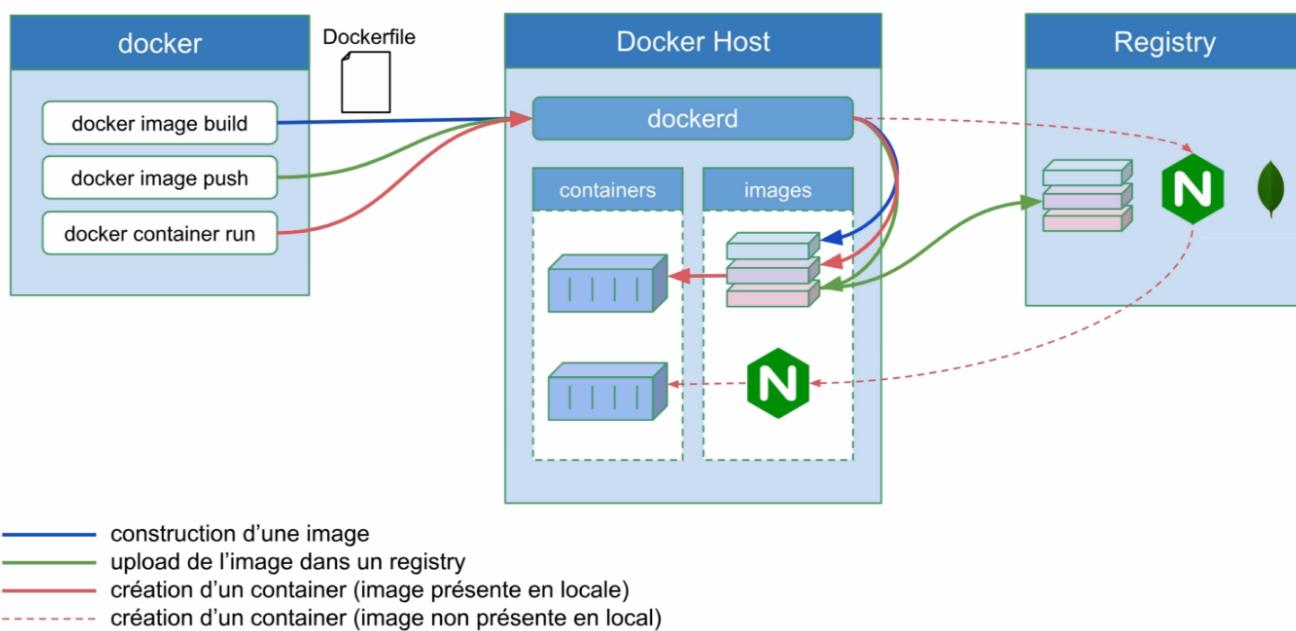
- Installé en même temps que **dockerd**.
- Communique avec le **daemon local** par défaut via `/var/run/docker.sock`.

- Peut être configuré pour communiquer avec un **daemon distant**.

### 1.3.3. Concepts essentiels

- **Docker** facilite la manipulation des **containers Linux**. Et cache la complexité sous-jacente.
- Introduction de la **notion d'image** : Format d'un package qui contient une application.
- Une image est un **template** qui sert pour la création d'un container.
- Pour créer une image on utilise un **Dockerfile**. Un fichier texte qui contient une liste d'instructions.
- La distribution de ces images se fait par l'intermédiaire d'un **Registry**.
- Docker permet de lancer des containers sur une machine unique ou sur un ensemble d'hôtes regroupées en un **cluster Swarm**.

Voici un schéma qui montre le **fonctionnement global des composants de base de Docker**.

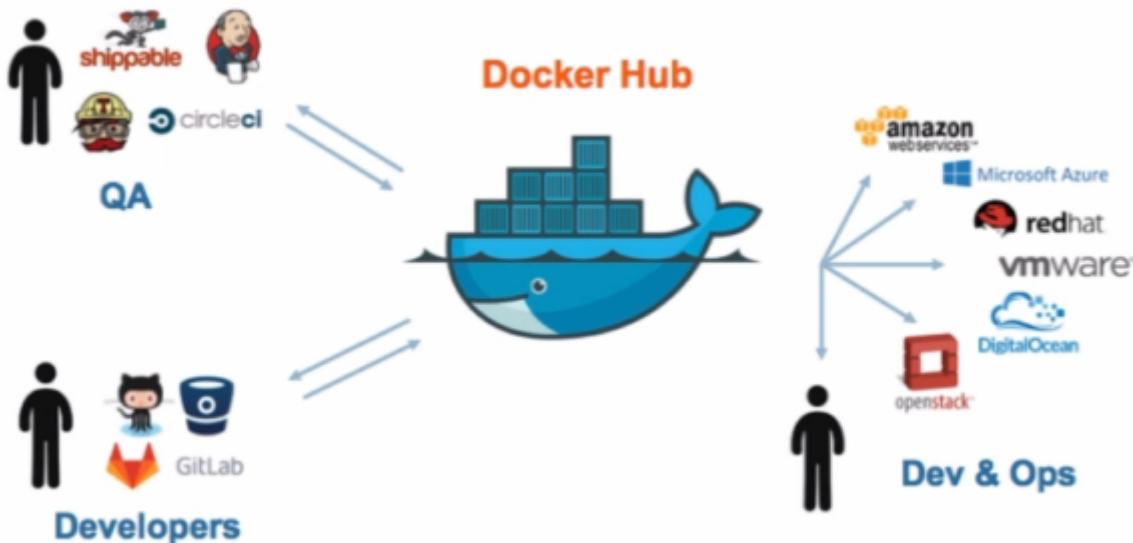


Quand on installe la plateforme Docker nous avons donc : un client et un serveur (ou daemon) qui tourne constamment et qui est responsable de la gestion des containers et des images.

### 1.3.4. Docker Hub

Par défaut le **daemon Dockerd** communique avec le **Docker Hub**, qui est le **Registry** officiel de Docker disponible à l'adresse : <https://hub.docker.com>

Il existe bien entendu beaucoup d'autres Registry que l'on peut utiliser si on le souhaite.

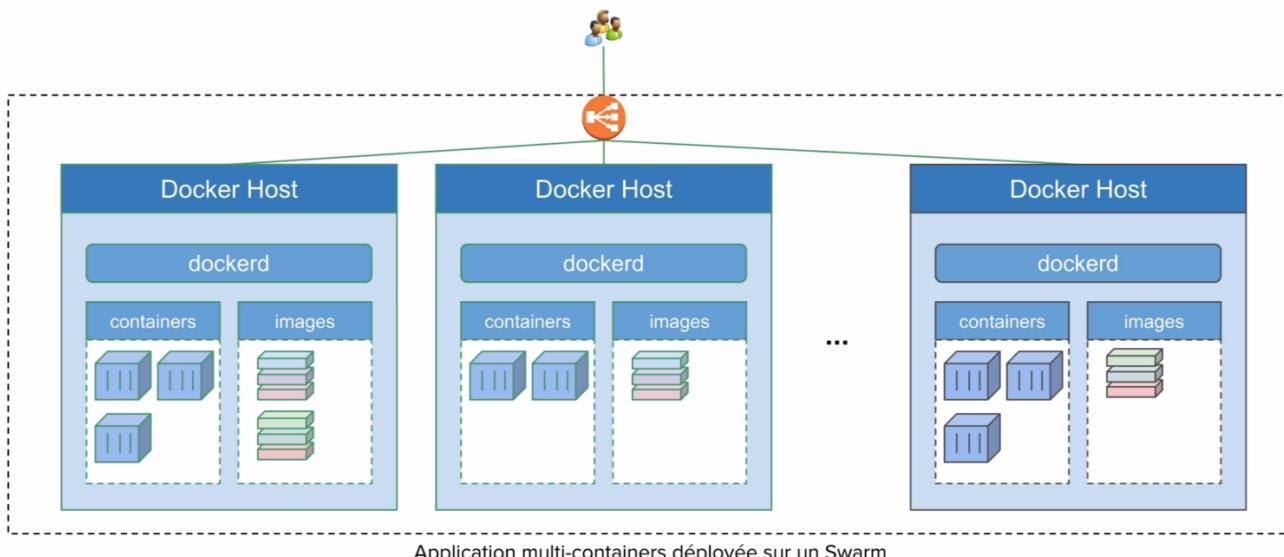


Les images du Docker Hub peuvent être classées en plusieurs catégories.

- Les images officielles qui sont validées et que l'on peut utiliser avec confiance.
- Les images publiques à utiliser avec précaution.
- Les images privées dédiées qu'aux utilisateurs autorisés (partage d'images au sein d'une entreprise par exemple).

### 1.3.5. Cluster Swarm

Un Cluster Swarm est un ensemble de **Docker Host**, c'est-à-dire un ensemble de machines sur lesquelles le **Docker Démon** est installé.

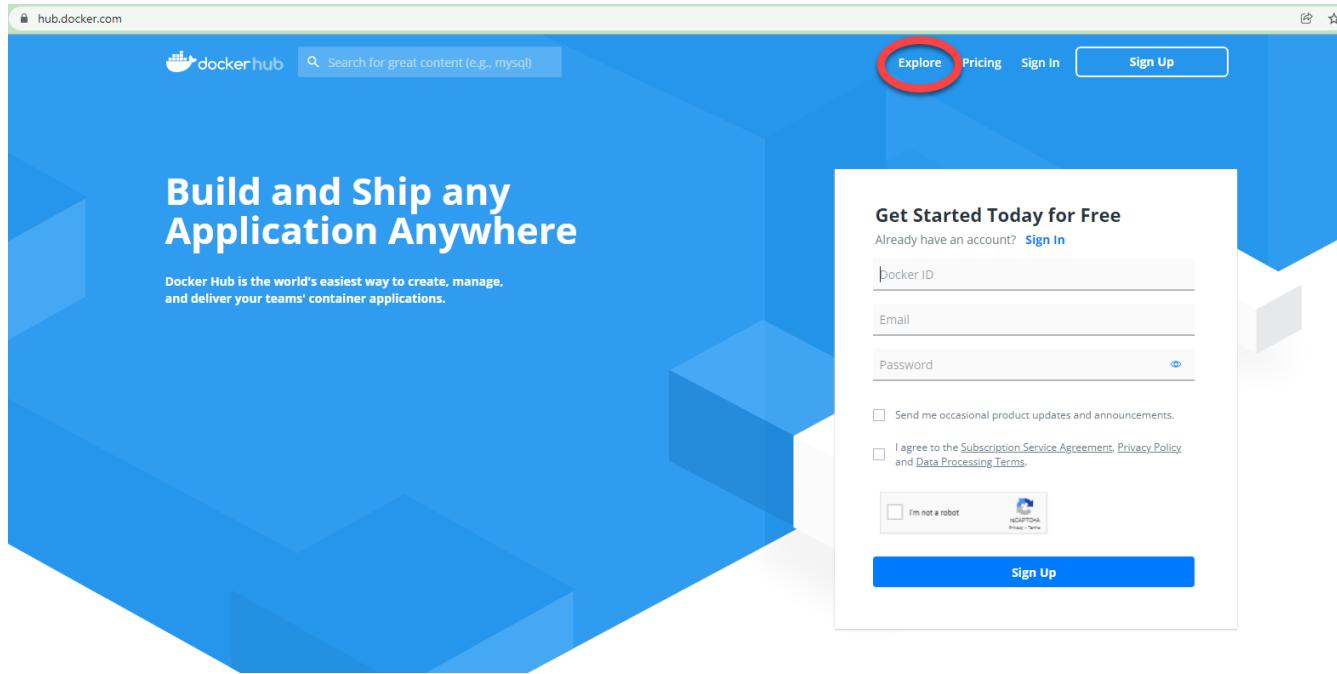


Ses machines vont communiquer entre elles afin d'orchestrer des applications et d'assurer qu'elles fonctionnent de la manière voulue.

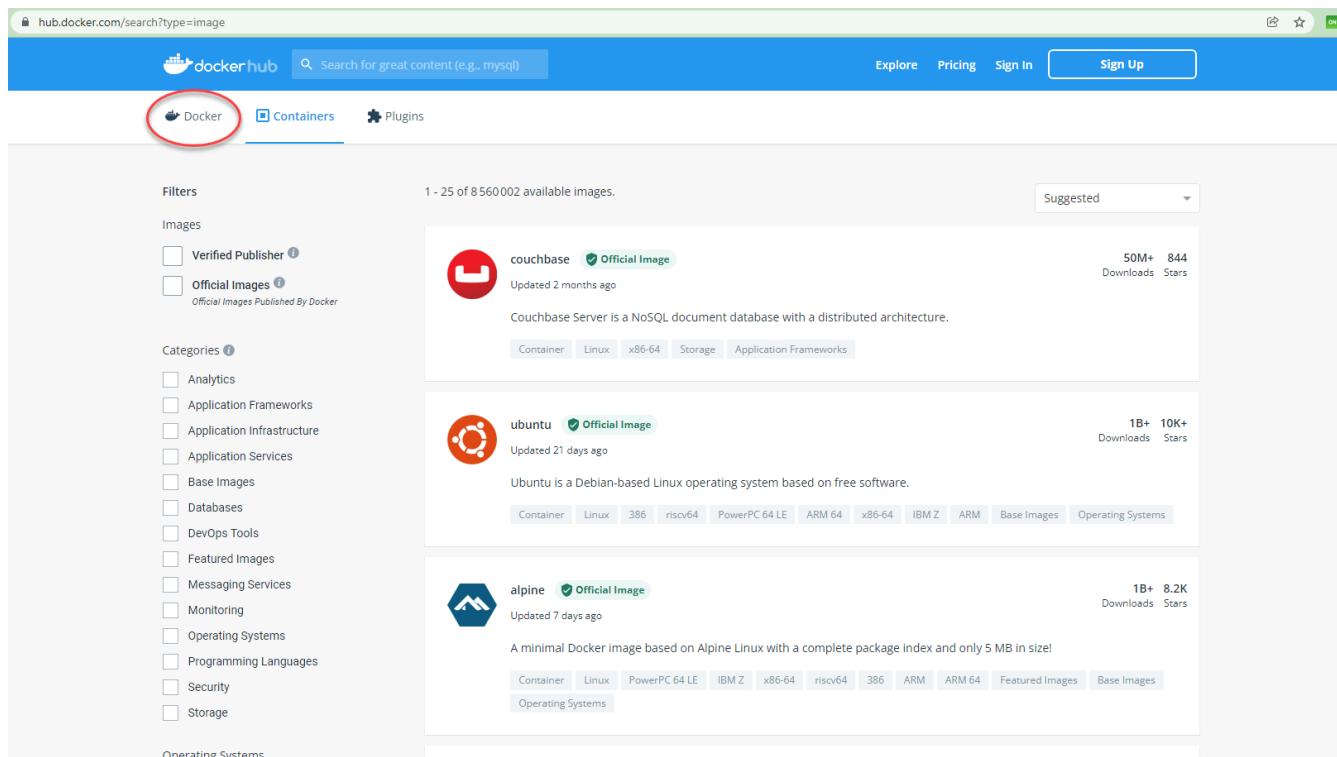
## 1.4. Installation de Docker

Nous allons voir ici comment installer **Docker** sur votre environnement.

Rendez-vous tout d'abord dans le [Docker hub](#) puis sélectionner l'onglet **Explore**:



Sélectionnez ensuite l'onglet **Docker** dans le sous menu:



Sur la gauche vous verrez alors un menu vous permettant de sélectionner différents éléments :

- plateforme
- système d'exploitation

- architecture

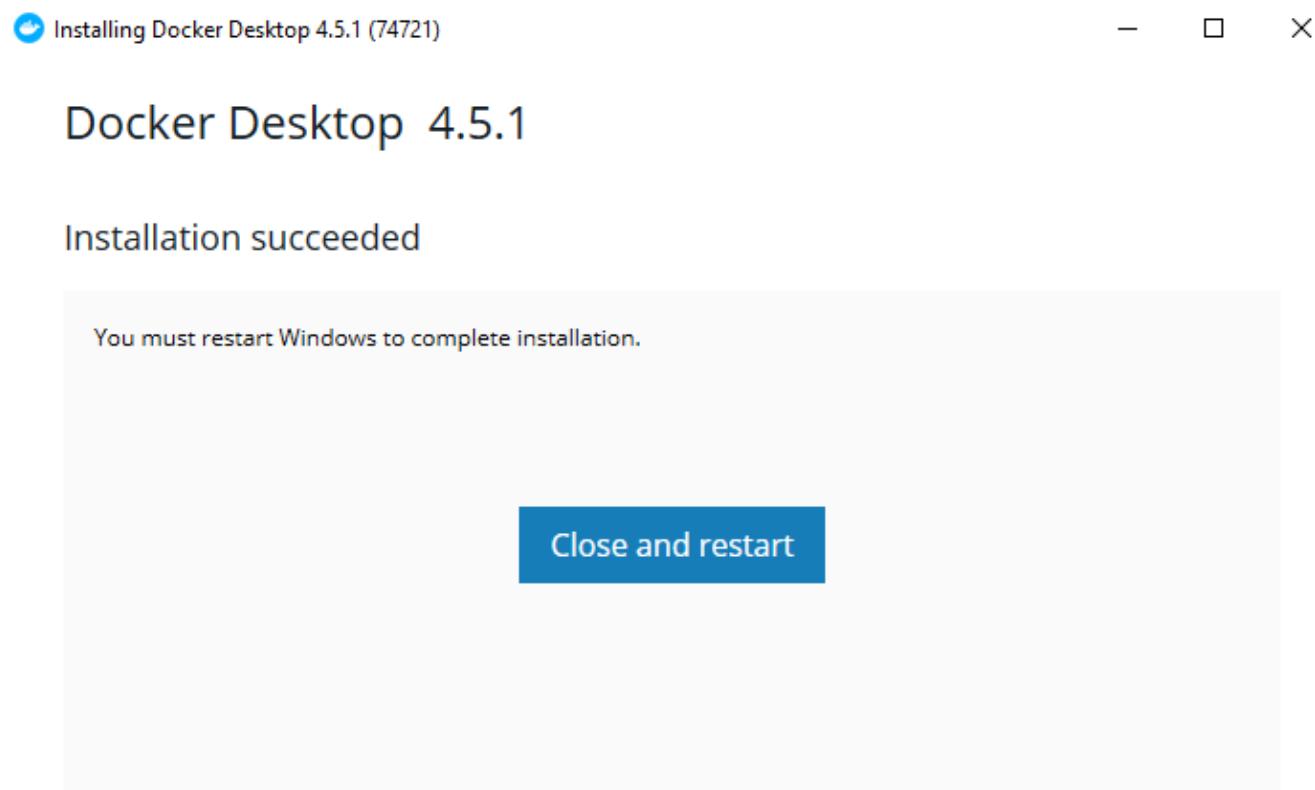
Comme nous pouvons le constater, Docker peut être installé sur des systèmes divers: machine de développement, l'infrastructure d'un cloud provider, et même des devices de type Raspberry PI.

## 1.5. Installation sur un poste élève

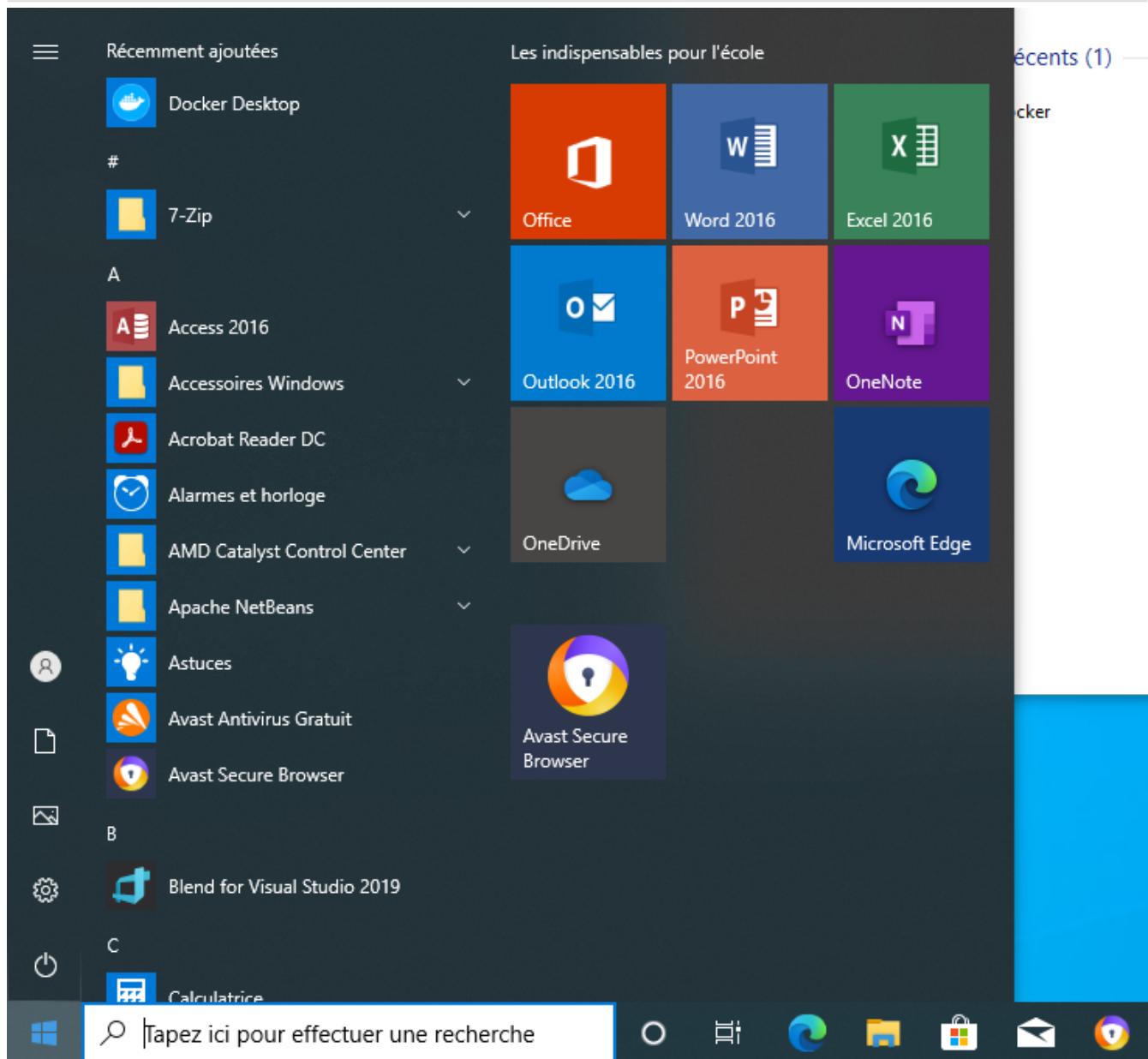
Normalement, il faudrait télécharger [Docker Desktop](#) depuis le site officiel. Mais pour économiser la bande passante, utilisez le fichier d'installation présent dans le répertoire `\COMMUN\BAUER\Docker\`.

Double cliquez sur l'installateur et laissez les options d'installation cochées par défaut. **WSL 2** est nécessaire pour faire fonctionner **DOCKER**.

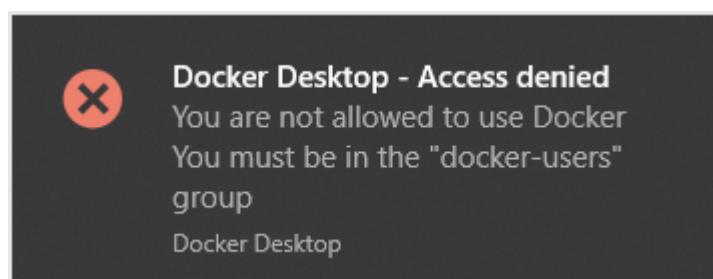
Si tout se passe bien vous devriez avoir cet écran vous invitant à redémarrer la machine :



- Lancer l'application : Docker Desktop\*\*



Si vous tentez d'exécuter l'application, il est fort probable que vous ayez un message d'erreur vous indiquant :

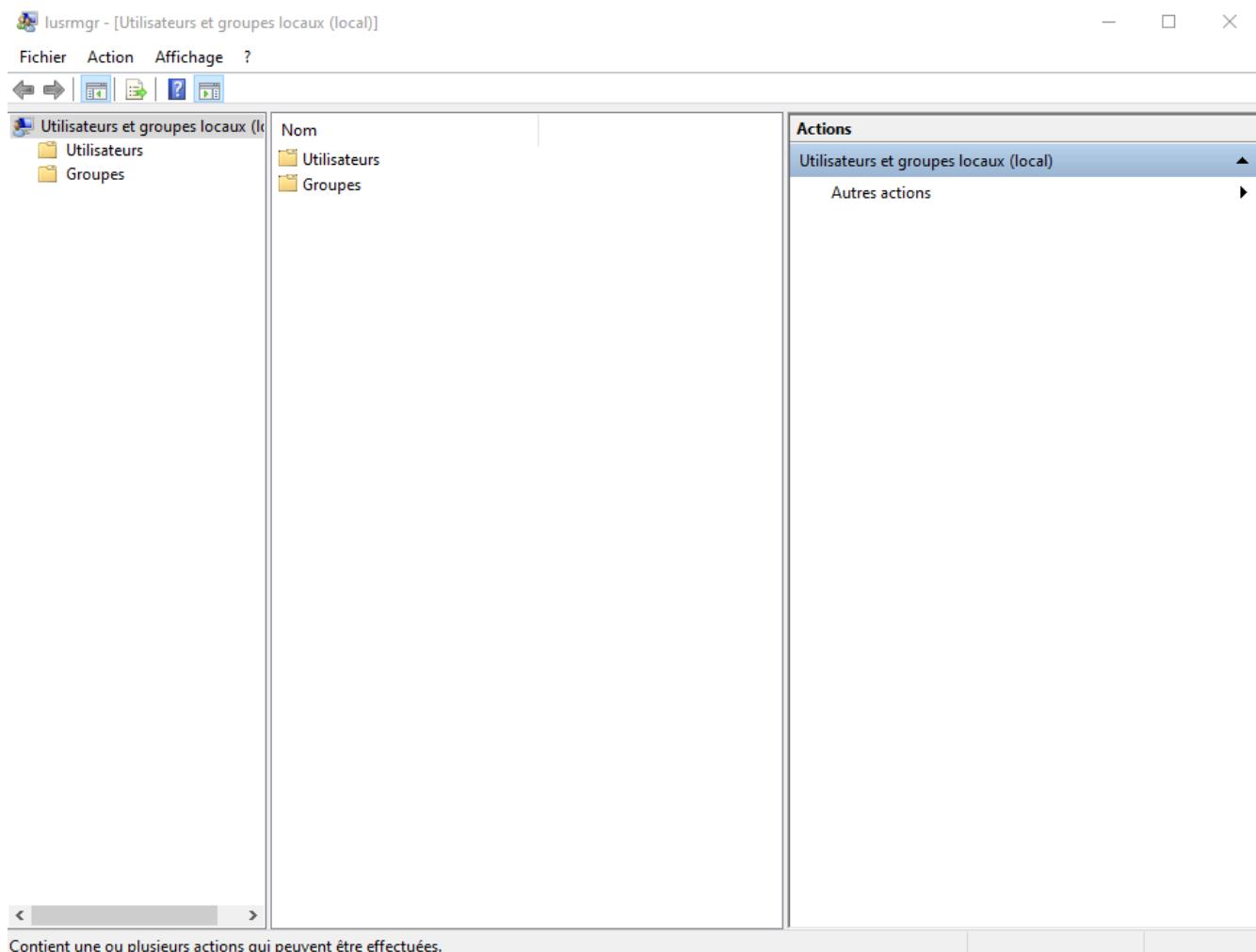


Pour résoudre ce problème, nous avons besoin d'ajouter les utilisateurs de la machine au groupe **docker-users** nouvellement créé par l'installation.

Ouvrez une session en **administrateur** de la machine locale : compte **INFO/INFO**. Dans **WINDOWS 10**, tapez dans le champ de recherche situé en bas à gauche :

### « modifier les utilisateurs et les groupes locaux »

Cette fenêtre devrait s'ouvrir :

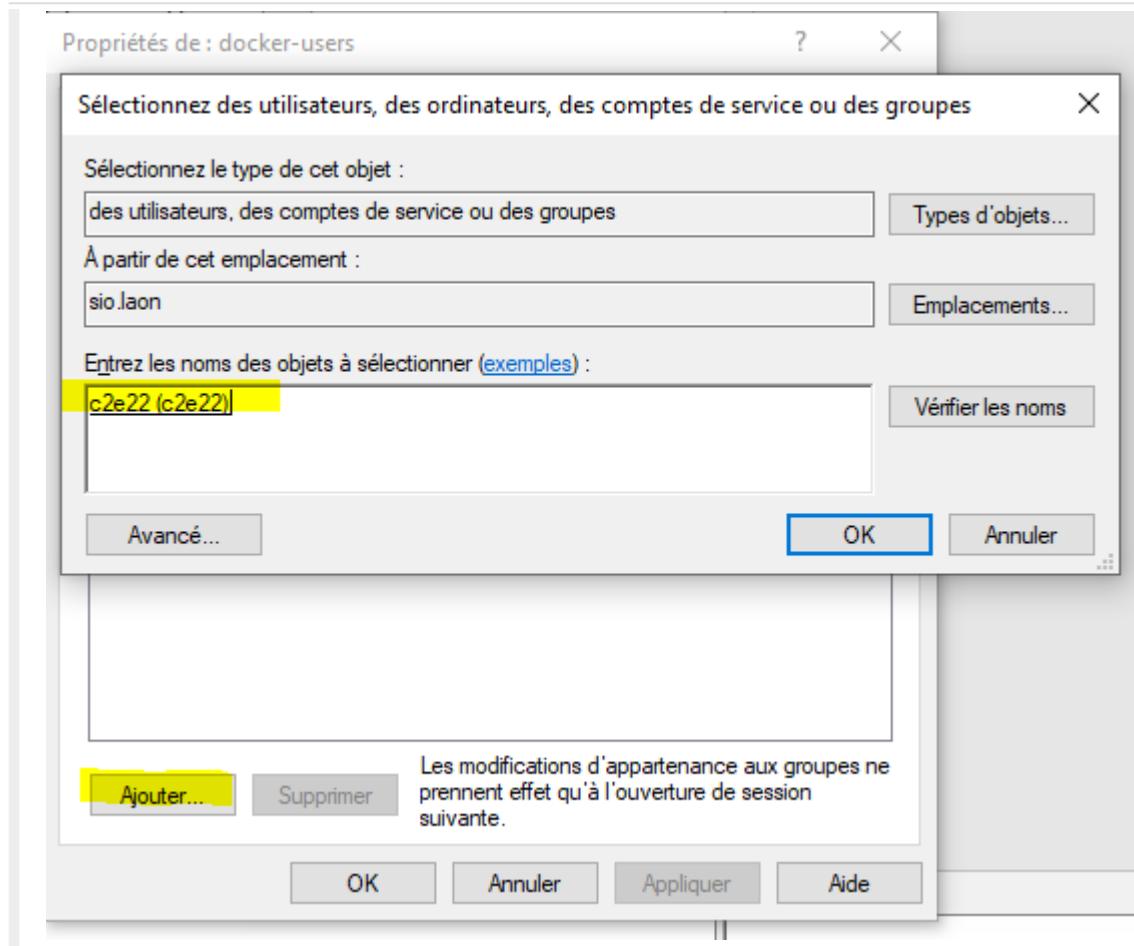


The screenshot shows the Windows Local Users and Groups snap-in. The left pane displays a tree view with 'Utilisateurs et groupes locaux (local)' expanded, showing 'Utilisateurs' and 'Groupes'. The right pane lists groups with columns for 'Nom' (Name) and 'Description'. A sidebar on the right shows 'Actions' with 'Groupes' selected. The 'docker-users' group is highlighted with a yellow background.

Nom	Description
Administrateurs	Les membres du groupe Administrateurs
Administrateurs Hypervisor	Les membres de ce groupe disposent d'autorisations supplémentaires pour les fonctionnalités de l'hyperviseur.
Duplicateurs	Prend en charge la réplication des groupes.
IS_IUSRS	Groupe intégré utilisé par les services intégrés.
Invités	Les membres du groupe Invités disposent d'autorisations limitées.
Lecteurs des journaux	Des membres de ce groupe peuvent lire les journaux.
Opérateurs d'assistan...	Les membres de ce groupe peuvent effectuer toutes les opérations administratives.
Opérateurs de chiffre...	Les membres sont autorisés à effacer les données.
Opérateurs de config...	Les membres de ce groupe peuvent configurer les paramètres système.
Opérateurs de sauveg...	Les membres du groupe Opérateurs de sauvegarde peuvent effectuer une sauvegarde.
Propriétaires d'appareils	Les membres de ce groupe peuvent modifier les propriétés des appareils.
System Managed Acc...	Les membres de ce groupe sont gérés par le système.
Utilisateurs	Les utilisateurs ne peuvent pas effectuer d'opérations administratives.
Utilisateurs avec pouvoirs	Les utilisateurs avec pouvoir ont accès à toutes les fonctionnalités.
Utilisateurs de gestion...	Les membres de ce groupe ont accès à l'interface de gestion.
Utilisateurs de l'Analyse	Les membres de ce groupe peuvent utiliser l'outil d'analyse.
Utilisateurs du Bureau	Les membres de ce groupe disposent d'autorisations supplémentaires pour le bureau.
Utilisateurs du journal	Les membres de ce groupe peuvent consulter les journaux.
Utilisateurs du modèle	Les membres sont autorisés à lancer des modèles.
AMD FUEL	Members of this group can change the AMD FUEL settings.
<b>docker-users</b>	<b>Users of Docker Desktop</b>

Double-cliquez sur le groupe **docker-users**.

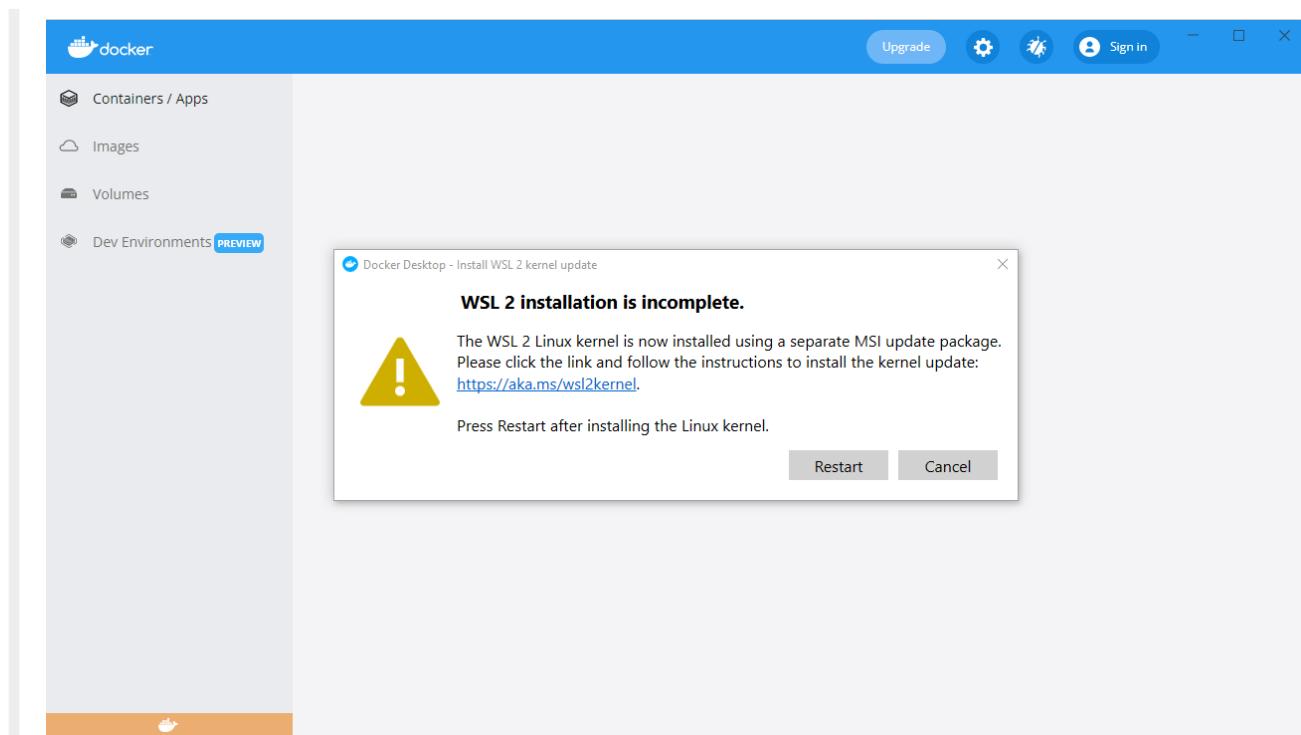
Et ajoutez un nouvel utilisateur : votre compte issu du domaine **sio**



Le système vous demandera de saisir l'identifiant et le mot de passe du compte à intégrer à ce groupe.

Redémarrer la machine et reconnectez-vous maintenant à votre compte WINDOWS standard.

Lancez L'application **Docker Desktop** et validez les conditions d'utilisation. Vous devriez avoir ce message d'erreur :



Fermez alors la fenêtre et rendez-vous sur ce site :

[Étapes d'installation manuelle pour les versions antérieures de WSL | Microsoft Docs](#)

Suivez les étapes d'installation :

Vous allez installer **WSL2** qui est un sous-système **Linux** pour **WINDOWS**. Cela va permettre d'utiliser des commandes **Linux** dans un terminal Windows.

Tapez ensuite la commande :

```
wsl.exe --set-default-version 2
```

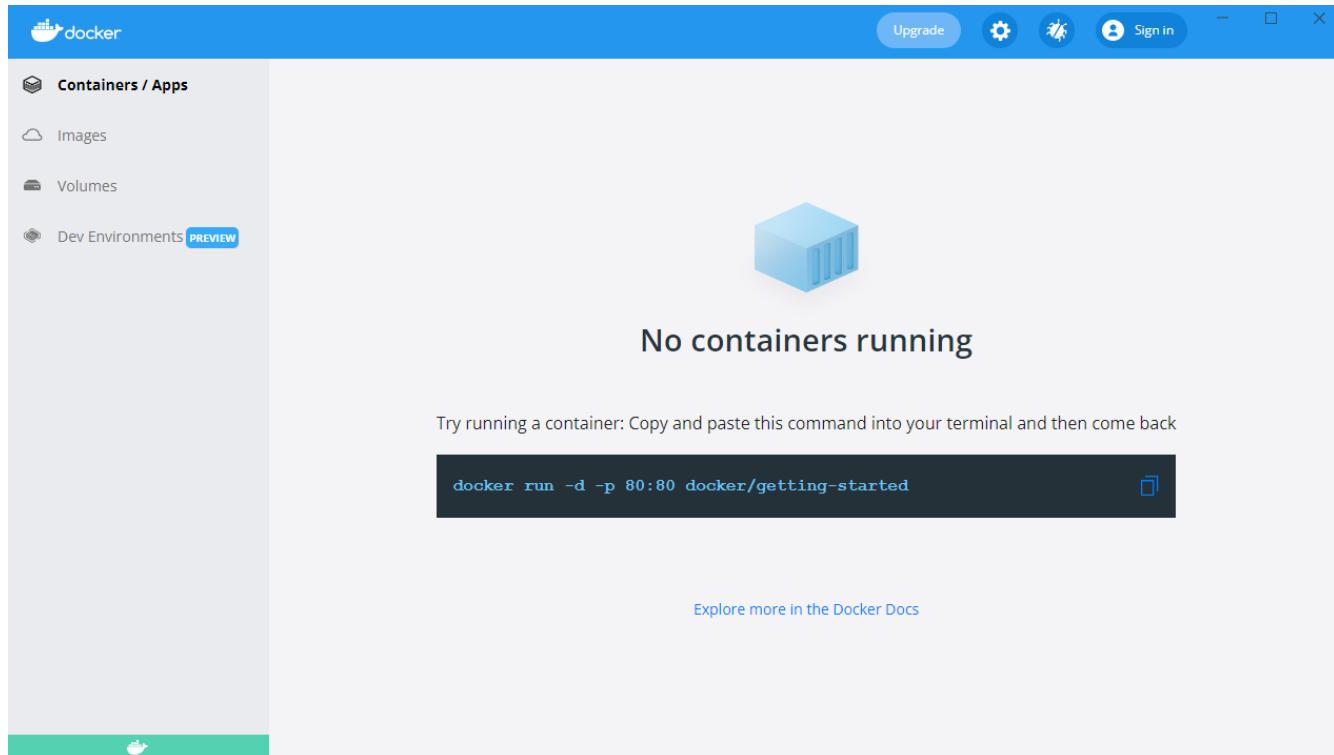
Nous pouvons en profiter pour installer le nouveau **Terminal de Windows**. Cela va apporter plus de confort durant la pratique de ce cours.

[Lien vers la page Terminal Windows](#)

Il faut un compte « **Microsoft** ».

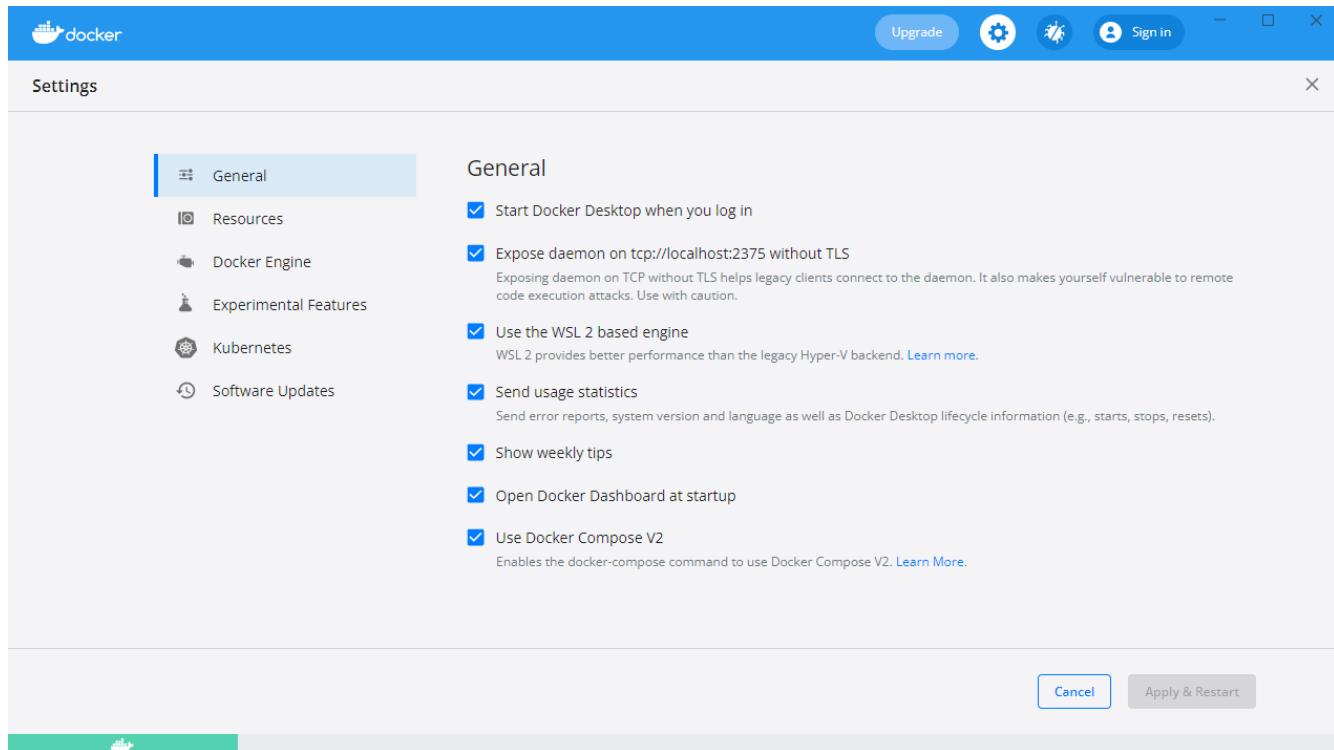
Redémarrez la machine encore une fois pour que **WSL2** soit pris en compte.

**Docker** devrait maintenant pouvoir démarrer :



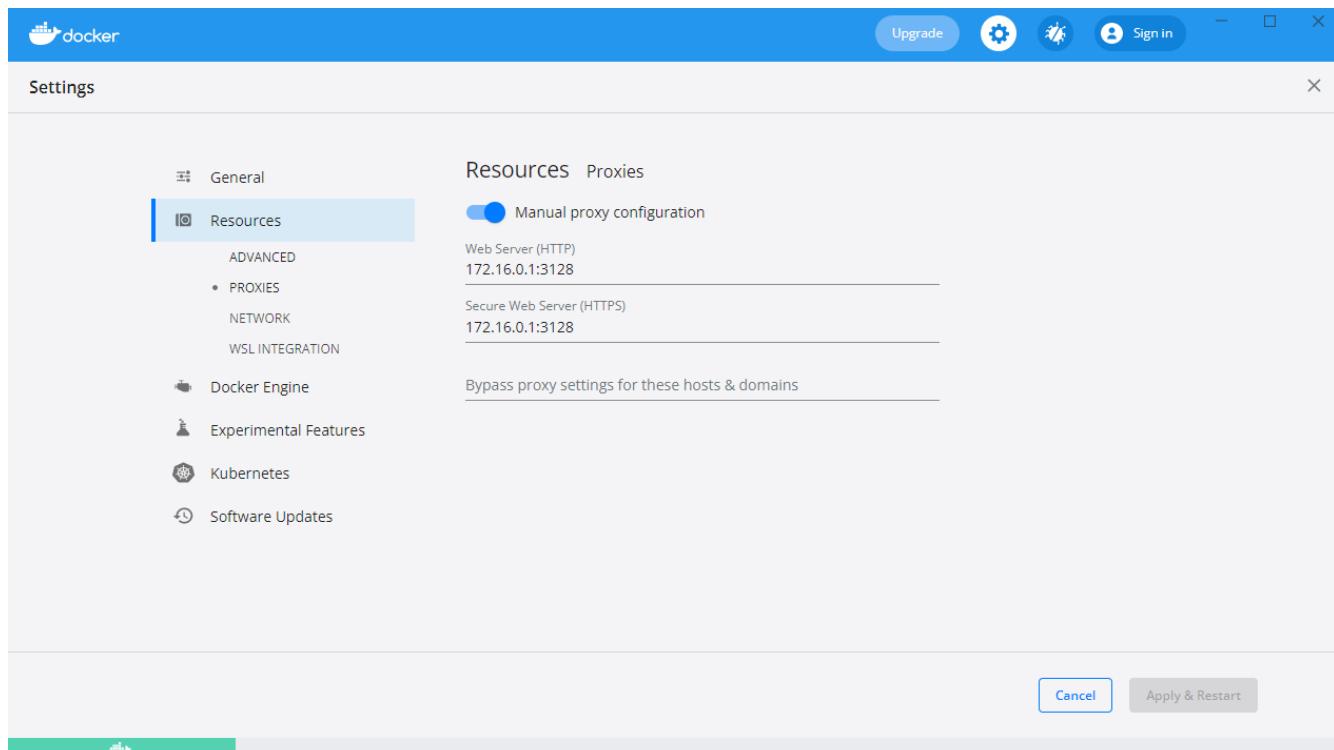
Il faut maintenant configurer le client en cliquant sur l'engrenage en haut à droite.

Cochez les options comme sur la capture d'écran :

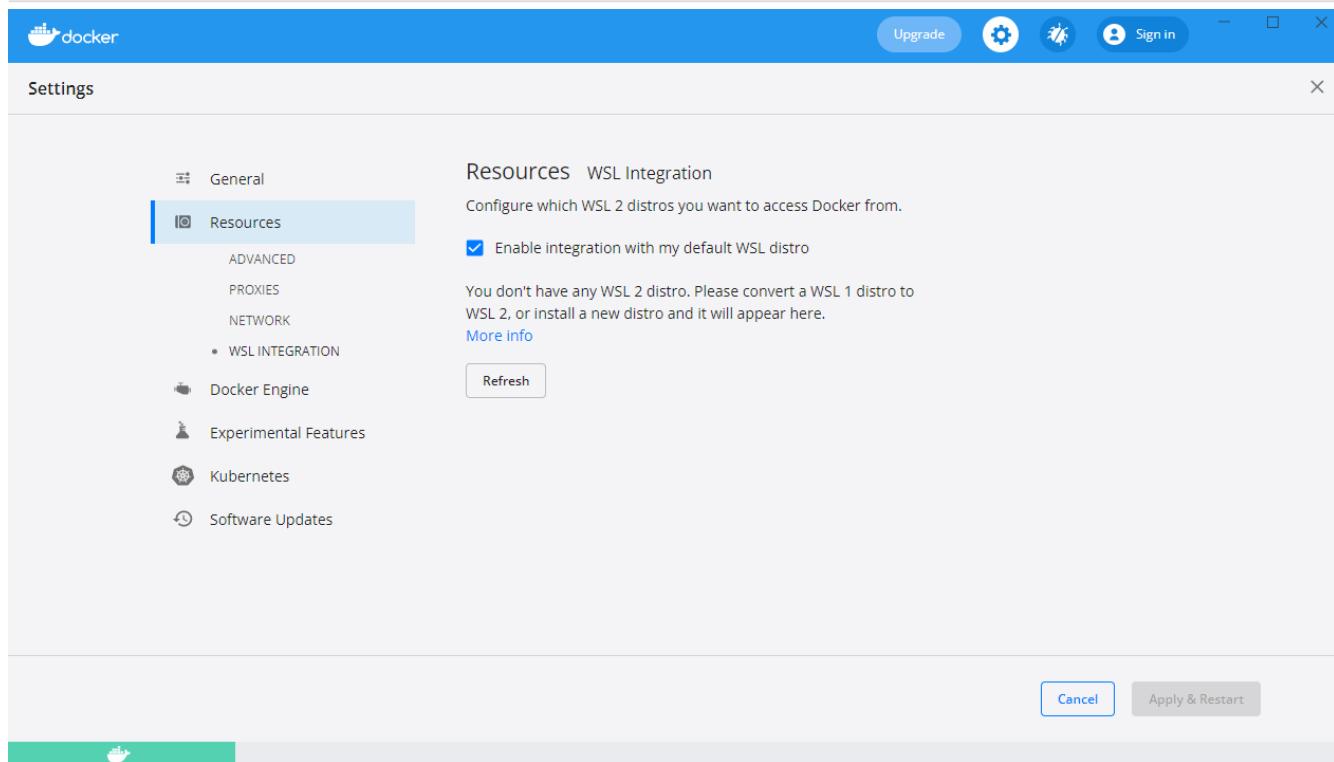


N'oubliez pas de cliquer sur « **Apply & Restart** »

## Configurez le PROXY



Si vous allez dans l'onglet WSL intégration :



**Vous êtes maintenant prêt !**

**Bienvenue dans le monde de DOCKER.**

Passez directement à la partie : **Vérification de l'installation**

## 1.6. Installation pour Windows 10 ou MacOS

Si vous êtes sur **MacOS** ou **Windows 10 (Entreprise ou Pro)** vous pouvez installer **Docker Desktop**, un environnement compatible pour chacune de ces plateformes

- [Docker Desktop for Windows](#)
- [Docker Desktop for Mac](#)

## 1.7. Installation pour Linux

Si vous êtes sur **Linux**, vous pouvez sélectionner la distribution que vous utilisez (**Fedora, CentOS, Ubuntu, Debian**) et vous obtiendrez alors un lien vers la documentation à suivre pour installer **Docker** sur la distribution en question.

Pour aller un peu plus vite, vous pouvez également lancer la commande suivante (compatible avec les principales distribution **Linux**) :

```
curl -sSL https://get.docker.com | sh
```

En quelques dizaines de secondes, cela installera **la plateforme Docker** sur votre distribution. Il sera ensuite nécessaire **d'ajouter votre utilisateur** dans le **groupe docker** afin de pouvoir interagir avec le **daemon** sans avoir à utiliser **sudo** (il faudra cependant lancer un nouveau **shell**

afin que ce changement de groupe soit pris en compte.)

```
sudo usermod -aG docker <UTILISATEUR>
```

*Note*



Il est également possible d'installer **Docker** sur d'autres types d'**architecture infrastructure**.

## 1.8. Vérification de l'installation

Une fois installé, lancez la commande suivante afin de vérifier que tout est fonctionnel :

```
docker info
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\baptiste> docker info
Client:
  Context:    default
  Debug Mode: false
  Plugins:
    buildx: Build with BuildKit (Docker Inc., v0.6.3)
    compose: Docker Compose (Docker Inc., v2.1.1)
    scan: Docker Scan (Docker Inc., 0.9.0)

Server:
  Containers: 0
  Running: 0
  Paused: 0
  Stopped: 0
  Images: 0
  Server Version: 20.10.10
  Storage Driver: overlay2
    Backing Filesystem: extfs
    Supports d_type: true
    Native Overlay Diff: true
    userxattr: false
  Logging Driver: json-file
  Cgroup Driver: cgroupfs
  Cgroup Version: 1
  Plugins:
    Volume: local
    Network: bridge host ipvlan macvlan null overlay
    Log: awslogs fluentd gcplogs gelf journalctl json-file local logentries splunk syslog
  Swarm: inactive
  Runtimes: io.containerd.runc.v2 io.containerd.runtime.v1.linux runc
  Default Runtime: runc
  Init Binary: docker-init
  containerd version: 5b46e404f6b9f661a205e28d59c982d3634148f8
  runc version: v1.0.2-0-g52b36a2
  init version: de40ad0
  Security Options:
    seccomp
      Profile: default
  Kernel Version: 5.4.72-microsoft-standard-WSL2
  Operating System: Docker Desktop
  OSType: linux
  Architecture: x86_64
  CPUs: 4
  Total Memory: 18.71GiB
  Name: docker-desktop
  ID: YLBX:Q5HX:KIWS:PRRS:FZJE:K6WA:TEEW:SBRK:XPD2:IPNB:KQWR:IZJI
  Docker Root Dir: /var/lib/docker
  Debug Mode: false
  Registry: https://index.docker.io/v1/
  Labels:
  Experimental: false
  Insecure Registries:
    127.0.0.0/8
  Live Restore Enabled: false

WARNING: No blkio throttle.read_bps_device support
WARNING: No blkio throttle.write_bps_device support
WARNING: No blkio throttle.read_iops_device support
WARNING: No blkio throttle.write_iops_device support
PS C:\Users\baptiste> |
```

## 2. Les containers avec Docker

Après avoir présenté la **plateforme Docker**, nous allons voir comment créer **des conteneurs** en ligne de commande afin de lancer des services en tâche de fond et/ou rendre disponible des répertoires de la **machine hôte** dedans.

Nous verrons comment lancer un conteneur dans un mode d'**accès privilégié**, ainsi que les commandes de bases pour la gestion de son cycle de vie.

Avant la **1.13**, lancer un **conteneur** s'effectuait avec la commande : `Docker Run` sans le mot clé **container**.

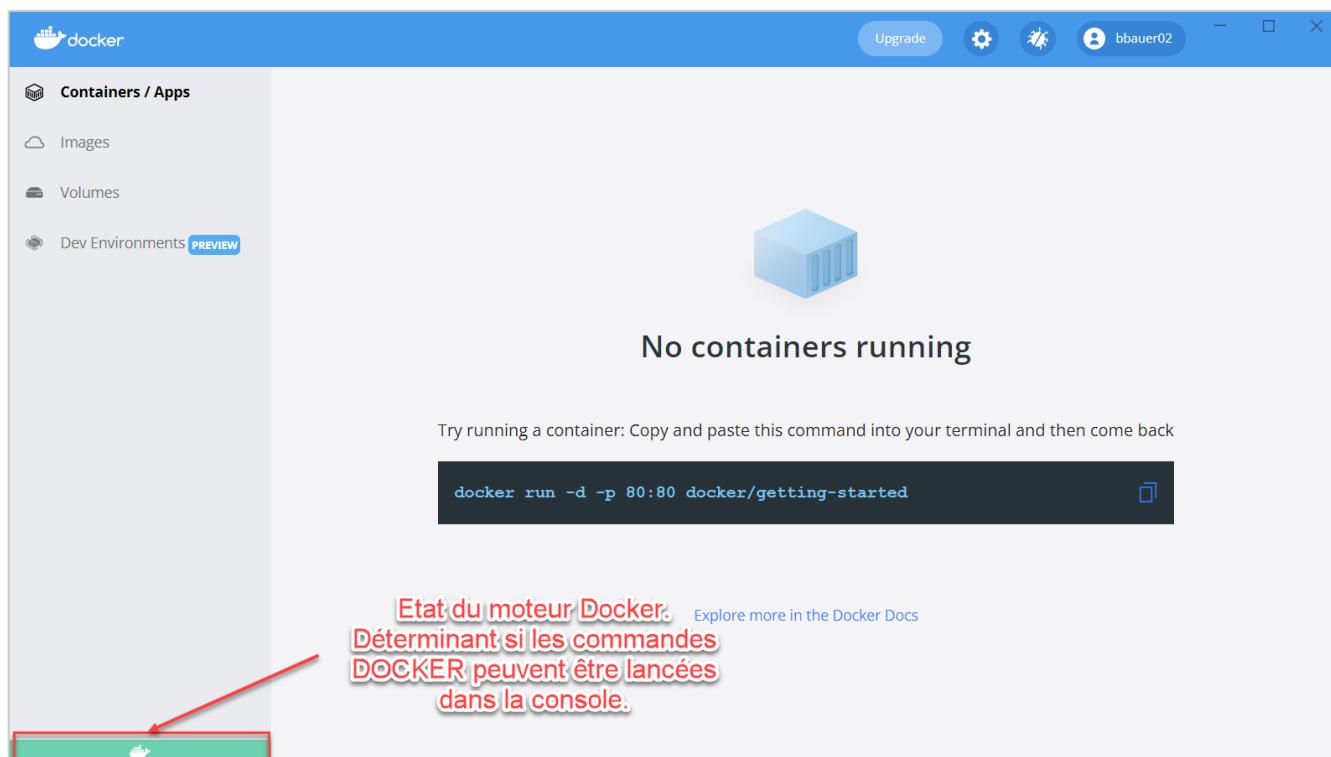
Il est toujours possible de le faire. Mais maintenant les commandes ont été regroupées aux composants auxquels elles se rapportent. C'est la raison pour laquelle le mot clé **container** a été rajouté pour les commandes relatives à la gestion du conteneur.

`docker container run [OPTIONS] IMAGE [COMMAND] [ARG]`

D'autres groupes de commandes existent et nous les étudierons plus tard.

### 2.1. Hello World

Lançons notre premier conteneur **Hello-World**.



Ouvrez un **terminal** et tapez :

```
docker container run hello-world
```

The screenshot shows a Windows command prompt window titled "Invite de commandes". The command entered is "Docker container run hello-world". The output indicates that Docker is unable to find the image locally and is pulling it from the Docker Hub. Once pulled, it creates a new container and runs the "hello-world" executable, which outputs "Hello from Docker!" and a message stating that the installation appears to be working correctly. Below this, a series of numbered steps explain the process: 1. Docker client contacted the Docker daemon. 2. Docker daemon pulled the "hello-world" image from the Docker Hub (amd64). 3. Docker daemon created a new container from that image which runs the executable. 4. Docker daemon streamed the output to the Docker client. A note at the bottom suggests running an Ubuntu container with "docker run -it ubuntu bash". It also provides links to Docker Hub and documentation.

```
Microsoft Windows [version 10.0.19044.1466]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\baptiste>Docker container run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:507ecde44b8eb741278274653120c2bf793b174c06ff4eaa672b713b3263477b
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

C:\Users\baptiste>
```

Téléchargement de l'image depuis le registry (Docker Hub)

Exécution de la commande définie dans l'image.

Le client demande au **daemon** (*processus*) de lancer un **conteneur** basé sur l'image **Hello-World**.

Cette image, n'étant pas disponible en local, est téléchargée et le **processus** présent dans cette image est automatiquement exécuté.

Et dans le cas de notre **Hello-world**, il s'agit seulement d'écrire du texte sur la sortie standard : **Hello from Docker** suivi d'un texte.

Cet exemple est simple, mais il met en avant le mécanisme sous-adjacent. À la fin du texte, on nous demande d'essayer un exemple plus ambitieux, c'est ce que nous allons faire par la suite.

**Activité 1 :** Expérimitez la commande sur votre machine :

```
docker container run hello-world
```

## 2.2. Ubuntu sous docker

Nous pouvons lancer un autre conteneur basé sur l'image d'**Ubuntu** et lui demander d'afficher **Hello** dans le contexte de cette image.

```
docker container run ubuntu echo hello
```

```
PS C:\Users\baptiste> docker container run ubuntu echo hello
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
08c01a0ec47e: Pull complete
Digest: sha256:669e010b58baf5beb2836b253c1fd5768333f0d1dbc834f7c07a4dc93f474be
Status: Downloaded newer image for ubuntu:latest
hello
PS C:\Users\baptiste>
```

Activité 2 : Analyser le contenu des cadres ci-dessus. A quelles actions correspondent-ils ?

## 2.3. Un conteneur dans un mode interactif

Le mode **interactif** permet d'avoir accès à un **shell** depuis le client local qui tourne dans le **contexte du conteneur**.

Pour cela il faut rajouter **deux options** à notre commande :



**-t** qui permet d'allouer un pseudo terminal à notre container.

**-i** qui va permettre de laisser l'entrée standard du container ouverte.

Nous allons utiliser l'image **Ubuntu** qui contient les binaires et les bibliothèques du système d'exploitation **Ubuntu**.

Le processus du **conteneur** dans le **système de fichier** qui est amené par le système **Ubuntu**.

```
docker container run -t -i ubuntu bash
```

ou

```
docker container run -ti ubuntu bash
```

Résultat :

```
PS C:\Users\baptiste> docker container run -t -i ubuntu bash
root@99bc74dab5c9:/# ls /
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@99bc74dab5c9:/# Nous avons accès à un Shell
```

Nous voyons que nous avons accès à un **shell** (*coquille* en anglais soit *interface système* dans le jargon informatique).

Nous reconnaissons sans peine le Prompt **Ubuntu/Linux** dans lequel nous pouvons écrire par exemple une commande Linux : **ls**

Activité 3 :

Tapez dans le **shell**, la commande : `cat /etc/issue`.

- Quelle information obtenez-vous ?

Pour sortir du conteneur, nous allons tuer le processus via la commande : `exit`

Nous aurions pu faire la même chose en utilisant une autre image que celle d'Ubuntu.

Lançons par exemple un conteneur basé sur la distribution **Linux Alpine** qui est distribution légère et sécurisée.

```
docker container run -t -i alpine
```

ou

```
docker container run -ti alpine
```

```
PS C:\Users\baptiste> docker container run -ti alpine
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
59bf1c3509f3: Pull complete
Digest: sha256:21a3deaa0d32a8057914f36584b5288d2e5ecc984380bc0118285c70fa8c9300
Status: Downloaded newer image for alpine:latest
/ # cat /etc/issue
Welcome to Alpine Linux 3.15
Kernel \r on an \m (\l)

/ # |
```

Vous savez maintenant lancer un **shell** interactif dans un conteneur.



Quand un **conteneur** est lancé seulement avec la commande `docker container run`, il est exécuté par défaut en **foreground**, mais si l'on veut l'exécuter en **background**, c'est-à-dire, en tâche de fond, il faudra utiliser l'option `-d` et la commande retournera alors l'**identifiant** du conteneur que l'on pourra utiliser par la suite pour effectuer différentes actions.

Par exemple nous pouvons lancer un conteneur basé sur l'image **nginx**, un **serveur http**.

*Exemple 1. Container NGINX en foreground*

Le conteneur est lancé et occupe notre console. Nous n'avons plus la main.

```
docker container run nginx
```

```
PS C:\Users\baptiste> docker container run nginx
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
5eb5b503b376: Pull complete
1ae07ab881bd: Pull complete
78091884b7be: Pull complete
091c283c6a66: Pull complete
55de5851019b: Pull complete
b559bad762be: Pull complete
Digest: sha256:2834dc507516af02784808c5f48b7cbe38b8ed5d0f4837f16e78d00deb7e7767
Status: Downloaded newer image for nginx:latest
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: Enabled listen on IPv6 in /etc/nginx/conf.d/default.conf
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Configuration complete; ready for start up
2022/02/09 11:00:30 [notice] 1#1: using the "epoll" event method
2022/02/09 11:00:30 [notice] 1#1: nginx/1.21.6
2022/02/09 11:00:30 [notice] 1#1: built by gcc 10.2.1 20210110 (Debian 10.2.1-6)
2022/02/09 11:00:30 [notice] 1#1: OS: Linux 5.4.72-microsoft-standard-WSL2
2022/02/09 11:00:30 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2022/02/09 11:00:30 [notice] 1#1: start worker processes
2022/02/09 11:00:30 [notice] 1#1: start worker process 32
2022/02/09 11:00:30 [notice] 1#1: start worker process 33
2022/02/09 11:00:30 [notice] 1#1: start worker process 34
2022/02/09 11:00:30 [notice] 1#1: start worker process 35
```

### Exemple 2. Container NGINX en background

Le conteneur est lancé et nous récupérons la main sur la console.

```
docker container run -d nginx
```

```
PS C:\Users\baptiste> docker container run -d nginx
6a54b3bae3345f6caf3aead71329e4cb40ea6b34d99910a2b3980920b8cd1081
PS C:\Users\baptiste> |
```

NGINX tourne en tâche de fond et nous pourrons accéder à ce conteneur par la suite grâce à son **identifiant**.



Nous pourrions aussi accéder à ce serveur web depuis un **navigateur**. Cela n'est actuellement pas possible car nous n'avons pas publié de **port**.

## 2.4. Publication de port.

La publication d'un port est utilisée pour qu'un **conteneur** puisse être accessible depuis l'extérieur. Afin de publier un port nous utilisons l'option **-p HOST\_PORT:CONTAINER\_PORT**.

Cela permet de publier un **port du conteneur** sur un **port de la machine hôte**.

L'option **-P** quant à elle laisse le choix du port au **docker démon**.

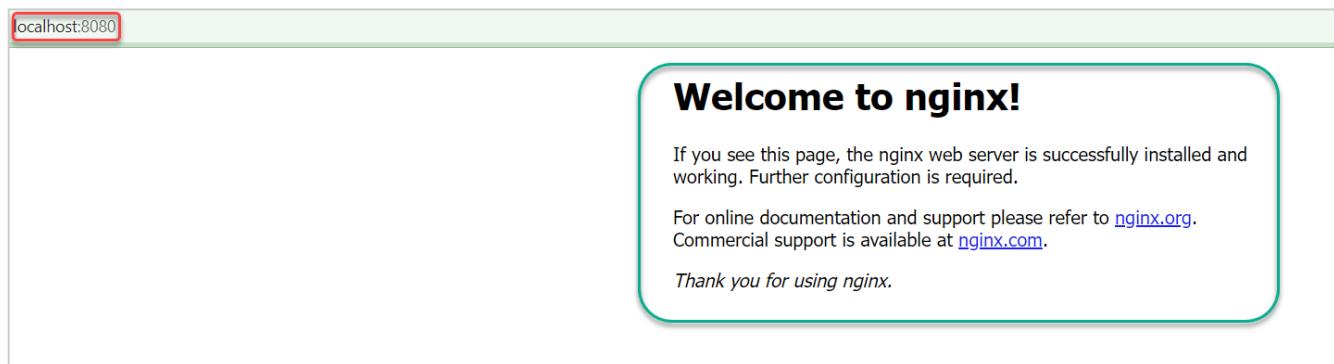
Reprendons notre conteneur **NGINX** qui est un serveur **http**. Par défaut, **NGINX** est un processus qui se lance sur le **port 80** dans le conteneur.

Si nous souhaitons accéder à notre conteneur depuis **un navigateur de la machine hôte** sur le **port 8080** de la machine hôte, nous lancerons le conteneur **nginx** avec la commande suivante :

```
docker container run -d -p 8080:80 nginx
```

```
PS C:\Users\baptiste> Docker container run -d -p 8080:80 nginx
f37a9ffd84ca3b07430c03693061a1e968381636cec27e0bf307401903713cf2
```

Maintenant, nous pouvons ouvrir notre navigateur sur l'adresse : <http://localhost:8080>



## 2.5. Bind-mount

Nous allons maintenant voir comment **monter un répertoire de la machine hôte** dans un conteneur.

Cela s'effectue grâce à l'option `-v <HOST_PATH>:<CONTAINER_PATH>`

Il existe une autre notation avec l'option `--mount type=bind, src=<HOST_PATH>, dst=<CONTAINER_PATH>`

Cela permet de partager, par exemple, le code source d'un programme présent sur une **machine hôte** avec un **conteneur** ou de monter le **socket Unix** du **daemon Docker** (`/var/run/docker.sock`) pour permettre à un conteneur de dialoguer avec le **daemon**.

### 2.5.1. Exemple : Monter un dossier 'www'

Quand vous développez une application et que vous modifiez le code source, il peut être intéressant que cela soit pris en compte dans le conteneur.

C'est le cas lors du développement d'une **application web**. Nos **fichiers sources** sont sur une **machine locale**, et dans **un conteneur**, nous avons un serveur **WEB** avec **NGINX** par exemple. Nous allons alors monter le dossier **www** local dans le **conteneur**.

```
docker container run -v $PWD/www:/usr/share/nginx/html -d -p 80:80 nginx
```

ou

```
docker container run -mount type=bind,src=$PWD/www,dst=/usr/share/nginx/html -d -p
```

80:80 nginx

\$PWD est une variable d'environnement qui va être créée par le SHELL et prendra comme valeur le chemin du répertoire courant dans lequel la commande a été lancé.

```
PS C:\Users\baptiste> docker container run -v $PWD/www:/usr/share/nginx/html -d -p 80:80 nginx  
a859ae3cb7f8926c18bbbed0e0888h066faa290201a372a16ad98e1b1eb51de78
```

PS C:\Users\baptiste> \$PWD

On affiche le contenu de la variable \$PWD

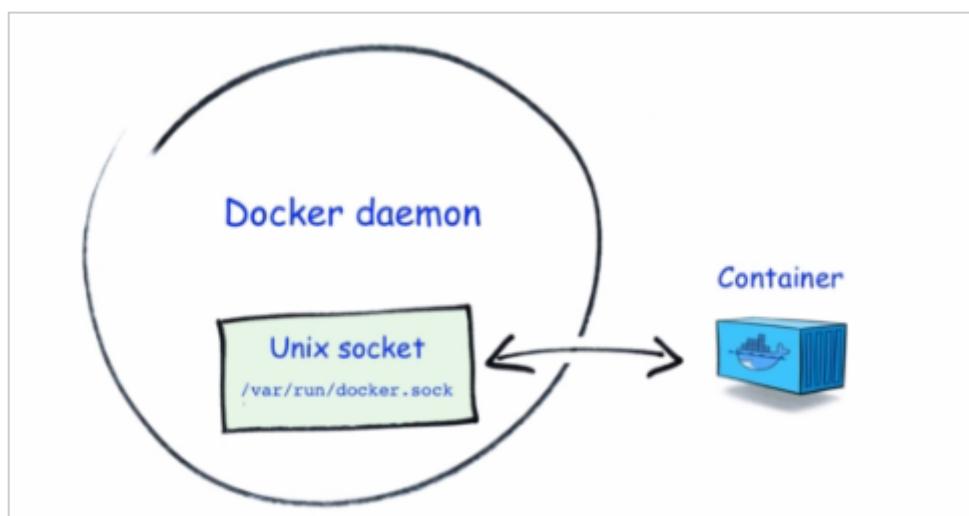
Path

C:\Users\baptiste La réponse ...

PS C:\Users\baptiste> |

## 2.5.2. Exemple: Intéragir avec le Docker Daemon

Dans cet exemple nous allons voir comment lier(bind) /var/run/docker.sock. Ce qui nous permettra d'interagir avec le Docker Daemon directement depuis le conteneur et cela nous donnera accès à l'API du Daemon.



### 2.5.2.1. LINUX UNIQUEMENT

Créons donc un simple conteneur : avec l'image d' Alpine.

```
docker container run --rm -it --name admin -v  
/var/run/docker.sock:/var/run/docker.sock alpine
```

Maintenant que le conteneur est monté et branché au Docker Daemon, nous pouvons lui envoyer des requêtes.

Depuis le Shell:

Installons CURL :

apk add curl pour ajouter l'utilitaire CURL.

Nous allons lancer une requête **http POST** sur le **Docker Daemon** :

```
curl -X POST \unix-socket /var/run/docker.sock -d '{"Image":"nginx:1.12.2"}' -H 'Content-Type: application/json' http://localhost/containers/create
```

Cela aura pour effet de demander au **Docker Daemon** de créer un nouveau conteneur avec l'image **NGINX version 1.12.2**.

Le paramètre **-X POST** permet d'effectuer quel type de requête **http** ? Sous quel format sont envoyés les instructions de configuration de l'image **Docker** à créer ?

Pour lancer le conteneur depuis le conteneur **ADMIN** :

```
curl -XPOST \unix-socket /var/run/docker.sock  
http://localhost/containers/6b24...283b/start
```

**Question 1 : Dans cette commande, à votre avis à quoi correspond la chaîne de caractère : 6b24...283b ?**

### 2.5.3. Ecouter les actions demandées au Docker Daemon

Nous allons lancer un autre conteneur dans lequel le **socket** est monté. Puis nous écouterons les actions demandées sur le **Docker Daemon**.



Même ceux provenant d'autre conteneur

```
docker container run \name admin -ti -v /var/run/docker.sock:/var/run/docker.sock  
alpine
```

```
curl \unix-socket /var/run/docker.sock http://localhost/events
```

### 2.5.4. Limitation des ressources

Nous avons dit que le lancement d'un **conteneur** revient en fait à exécuter un **processeur**, et par défaut, il n'y a pas de limite de consommation des ressources matériels.

Par exemple, Un conteneur pourra utiliser toute la RAM et impacter tous les autres conteneurs qui tournent sur la même machine hôte.

Nous pouvons toutefois imposer des limites à un conteneur.

Lançons un conteneur avec l'image **estesp/hogit** qui a pour objectif de consommer de la ram.

```
docker container run --memory 32m estesp/hogit
```

Avec `--memory 32m`, nous avons fixé une limite : quand le processus aura atteint la limite de **32M** de **RAM** consommée, il sera tué par **Docker**.

Nous pouvons limiter l'utilisation du **CPU** également.

Lançons un conteneur avec l'image `progrium/stress` qui va se charger de stresser les coeurs du **CPU**.

```
docker container run -it --rm progrium/stress -cpu 4
```

Ici les 4 coeurs du **CPU** serons utilisés car nous n'avons pas imposé de limite.

Maintenant lançons la même commande avec le flag `--cpus 0.5` pour limiter l'utilisation du **CPU à la moitié d'un cœur**. (12% d'utilisation)

```
docker container run -it --rm progrium/stress -cpu 4 --cpus 0.5
```

En utilisant la valeur du flag : `--cpus 2`, nous limitons l'utilisation à 2 coeurs seulement. (50% d'utilisation)

### 2.5.5. Les droits dans un conteneur

Dans un conteneur, s'il n'est pas précisé explicitement, l'utilisateur `root` sera utilisé comme propriétaire. L'utilisateur `root` du conteneur correspond à l'utilisateur `root` de la machine hôte.



**Une bonne pratique** est d'utiliser un autre utilisateur pour lancer le conteneur.

Il y a plusieurs façons de le définir :

- Soit à la création de l'image,
- Soit en utilisant l'option `--user`,
- Soit en changeant l'utilisateur dans le processus du conteneur (`gosu`).

Lançons un conteneur basé sur l'image **Alpine** et exécutons l'instruction `sleep 10000`.

```
docker container run -d alpine sleep 10000
```

Nous allons vérifier le `owner` du processus depuis la machine hôte :

**Pour LINUX :**

```
ps aux | grep sleep
```

**Pour WINDOWS :**

Sous Windows, nous n'avons pas accès aux commandes LINUX nativement. Il faut utiliser les

commandes Docker natives pour avoir accès aux informations liées aux processus des conteneurs par l'intermédiaire de leur identifiant ou nom et via la commande `top`.

Récupérez l'identifiant ou le nom du conteneur obtenu avec la commande précédente puis :

```
docker container top <identifiant ou nom du container>
```

Identifiant du container si on a pas précisé de --name

```
PS C:\Users\baptiste> docker container run -d alpine sleep 10000
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
59bf1c13509f: Already exists
Digest: sha256:21a3deaa0d32a8057914f36584b5288d2e5ecc984380bc0118285c70fa8c9300
Status: Downloaded newer image for alpine:latest
a692cbd9f9972cadaf27e84292e24e2de478ae6fa15167a74978b81002fca9d0
PS C:\Users\baptiste> docker container top a692cbd9f9972cadaf27e84292e24e2de478ae6fa15167a74978b81002fca9d0
UID          PID    la commande
TIME        OWNER   CMD
root        1401   SLEEP 1380
00:00:00
```

Faisons la même manipulation, mais cette fois avec l'image officielle de **MongoDB**

a. code-block::

```
docker container run -d mongo
```

```
PS C:\Users\baptiste> docker container top 9f53f705b1cd158173b1aa4c2208d646789d9aec4ca19a7a126af727c882bf99
UID          PID    PPID   C      STIME   TTY      TIME             CMD
999         1557   1537   4      19:51   ?       00:00:00  mongod --bind_ip_all
```

On constate que le processus est la propriété d'un `owner` qui possède un `UID` de **999**. Nous verrons par la suite comme il est possible de configurer le `owner` d'un processus lors du montage de **container**.

## 2.5.6. Des options utiles



- `--name` qui permet de donner un nom au container.
- `--rm` pour supprimer le container quand il est stoppé.
- `--restart=on-failure` pour relancer le container en cas d'erreur.

## 2.5.7. Les commandes de base avec Docker

```
docker container <command>
```

### 1. Résumé des commandes de base avec Docker.

Commande	Description
<code>run</code>	Création d'un conteneur
<code>ls</code>	Liste des conteneurs
<code>inspect</code>	Détails d'un conteneur
<code>logs</code>	Visualisation des logs

Commande	Description
exec	Lancement d'un processus dans un conteneur existant
stop	Arrêt d'un conteneur
rm	Suppression d'un container

- La commande `ls` :

La commande `docker container ls` montre les containers qui sont en cours d'execution.

```
bauer@DESKTOP-9ML085I:~$ docker container ls
CONTAINER ID   IMAGE      COMMAND       CREATED          STATUS        PORTS     NAMES
5305cda41c82   alpine     "sleep 1000"   8 minutes ago   Up 8 minutes
                                                              

```

Pour lister tous les conteneurs actifs et stoppés :

```
docker container ls -a
```

```
bauer@DESKTOP-9ML085I:~$ docker container ls -a
CONTAINER ID   IMAGE      COMMAND       CREATED          STATUS        PORTS     NAMES
5305cda41c82   alpine     "sleep 1000"   9 minutes ago   Up 9 minutes
a37b0c664066   alpine     "sleep 1000"   23 minutes ago  Exited (0) 6 minutes ago
f0dab6b381f0    mongo:4.0  "docker-entrypoint.s..."  25 minutes ago  Exited (0) 24 minutes ago
c1cc9f763a86   alpine     "sleep 1000"   28 minutes ago  Exited (137) 24 minutes ago
243c4a3ad725   mongo:4.0  "docker-entrypoint.s..."  33 minutes ago  Exited (0) 24 minutes ago
c231d84d9ea3   alpine     "sleep 1000"   36 minutes ago  Exited (137) 24 minutes ago
                                                              

```

Pour lister les identifiants des containers actifs et stoppés : `docker container ls -a -q`.

```
bauer@DESKTOP-9ML085I:~$ docker container ls -a -q
5305cda41c82
a37b0c664066
f0dab6b381f0
c1cc9f763a86
243c4a3ad725
c231d84d9ea3
```

A partir d'un nom ou identifiant d'un container on peut l'inspecter :

```
bauer@DESKTOP-9ML085I:~$ docker container inspect clever_kilby
[
  {
    "Id": "5305cda41c82dfbea49919a2aaaf8752f6b75542cba6f9273e1eec9597ac1e086",
    "Created": "2022-02-21T10:57:14.8917367Z",
    "Path": "sleep",
    "Args": [
      "1000"
    ],
    "State": {
      "Status": "running",
      "Running": true,
      "Paused": false,
      "Restarting": false,
      "OOMKilled": false,
      "Dead": false,
      "Pid": 1909,
      "ExitCode": 0,
      "Error": "",
      "StartedAt": "2022-02-21T10:57:15.3015127Z",
      "FinishedAt": "0001-01-01T00:00:00Z"
    },
    "Image": "sha256:c059bfaa849c4d8e4aecab3a10c2d9b3d85f5165c66ad3a4d937758128c4d18",
    "Config": {
      "Image": "sha256:c059bfaa849c4d8e4aecab3a10c2d9b3d85f5165c66ad3a4d937758128c4d18",
      "Cmd": [
        "sleep"
      ],
      "ExposedPorts": {}
    }
  }
]
```

La commande renvoie une multitude d'information de configuration du container. On peut utiliser des templates (**Go Template**) pour formater les données reçues et même extraire seulement des informations nécessaires : par exemple : **Obtenir l'IP**

a. code-block::

```
docker container inspect --format '{{ .NetworkSettings.IPAddress }}' clever_kilby
* La commande 'logs' :
```

Cette commande, nous permet de visualiser les logs d'un container , l'option **-f** permet de les lire en temps réel.

Créons un container sous une image **alpine** qui exécutera une commande **ping 8.8.8.8** et qui sera nommé : **ping**

```
docker container run --name ping -d alpine ping 8.8.8.8
```

Puis, écoutons en temps réel les **logs** du container nommé **ping**

```
docker container logs -f ping
```

```
PS C:\Users\baptiste> docker container run --name ping -d alpine ping 8.8.8.8
b23e5c4c3c4078fc1e3c30044606643539060d29fe27f80679c06e14fb69da70
PS C:\Users\baptiste> docker container logs -f ping
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=37 time=16.148 ms
64 bytes from 8.8.8.8: seq=1 ttl=37 time=17.334 ms
64 bytes from 8.8.8.8: seq=2 ttl=37 time=17.132 ms
64 bytes from 8.8.8.8: seq=3 ttl=37 time=16.003 ms
64 bytes from 8.8.8.8: seq=4 ttl=37 time=15.244 ms
64 bytes from 8.8.8.8: seq=5 ttl=37 time=15.405 ms
64 bytes from 8.8.8.8: seq=6 ttl=37 time=14.706 ms
```

- La commande **exec** :

Cette commande permet de lancer un processus dans un container existant pour faire du débug par exemple. Dans ce cas nous utiliserons les options **-t** et **-i** pour obtenir un **shell** interactif.

**Exemple** : lançons un container qui attend 100000 secondes, et demandons ensuite d'ouvrir un shell pour lister les processus de ce container.

```
docker container run -d --name debug alpine sleep 100000
```

On lance le container avec l'option **-d** pour le mettre en tâche de fond et récupérer la main sur le terminal et on lui donne le nom **debug** pour le manipuler facilement.

Ensuite nous utilisons la commande **exec** qui injectera dans notre container une commande, à savoir ici, la demande d'ouverture d'un **shell**.

```
docker container exec -ti debug sh
```

```
PS C:\Users\baptiste> docker container run -d --name debug alpine sleep 100000
45ccd4f2abd682490666e15a9fb6f8d78c367dd0bb1d6b200fcf59a6377262ab
PS C:\Users\baptiste> docker container exec -ti debug sh
/ # ps aux
PID  USER      TIME  COMMAND
  1 root      0:00 sleep 100000
  8 root      0:00 sh
 15 root      0:00 ps aux
/ # |
```

Sur la capture d'écran : Dans le shell, nous avons exécuté la commande **ps aux**. Qui permet de lister les processus et leur **owner**. On constate que le processus de **PID 1**, correspond à la commande **sleep**. Et le processus de PID 15 correspond à notre **ps aux**.

#### *Warning*



Si l'on **kill** le processus de **PID 1**, le container s'arrêtera, car un container n'est actif que tant que son processus de **PID 1** spécifié au lancement est en cours d'exécution.

- La commande **stop** :

Cette commande permet de stopper un ou plusieurs containers.

```
docker container stop <ID>
```

```
docker container stop <NAME>
```

Nous pouvons combiner des commandes !

**Rappel :** Obtenir la liste des containers en cours d'exécution :

```
docker container ls -q
```

Donc pour stopper les containers en cours d'exécution :

```
docker container stop $(docker container ls -q)
```

Les containers stoppés existent toujours :

```
docker container ls -a
```

- La commande `rm` :

Pour supprimer un container.

```
docker container rm <ID>
docker container rm <NAME>
```

Donc, par combinaison de commande, nous pouvons supprimer définitivement un ou plusieurs containers qui sont déjà stoppé.

```
docker container rm $(docker container ls -aq)
```

Avec l'option `-f` nous pouvons forcer l'arrêt d'un container et le supprimer dans la foulée.

## 2.6. En pratique :

Lançons quelques containers pour pratiquer, vous devez être en mesure de comprendre maintenant la finalité de ces 3 commandes :

```
docker container run -d -p 80:80 --name www nginx
```

```
docker container run -d --name ping alpine ping 8.8.8.8
```

```
docker container run hello-world
```

Listons les containers :

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
6f94e474cab6	alpine	"ping 8.8.8.8"	About a minute ago	Up About a minute		ping
40c3e10088aa	nginx	"/docker-entrypoint..."	3 minutes ago	Up 3 minutes	0.0.0.0:80→80/tcp	www

Nous voyons les 2 premiers containers avec le statut **UP**. Nous ne voyons pas le 3 ième container pour la simple raison qu'une fois qu'il a effectué son action : `echo hello world`, il s'est arrêté automatiquement. Par contre avec un : `docker container ls -a` celui-ci est visible.

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
599ddf847b4b	hello-world	"/hello"	3 minutes ago	Exited (0) 3 minutes ago		fervent_napier
6f94e474cab6	alpine	"ping 8.8.8.8"	4 minutes ago	Up 4 minutes		ping
40c3e10088aa	nginx	"/docker-entrypoint..."	5 minutes ago	Up 5 minutes	0.0.0.0:80→80/tcp	www

Son statut est **exited**, indiquant qu'il n'est pas démarré.

Nous pouvons inspecter les containers et en particulier extraire une information comme l'**adresse IP** de notre serveur web **NGINX** :

```
docker container inspect --format '{{ .NetworkSettings.IPAddress }}' www
```

```
PS C:\Users\baptiste> docker container inspect --format '{{ .NetworkSettings.IPAddress }}' www
172.17.0.2
```

Nous pouvons lancer une commande dans un container en cours : par exemple nous voulons lister la liste des processus en cours dans le container **ping** :

```
docker container exec -ti ping sh
```

Un **shell** est alors disponible, et dedans nous pouvons taper la commande : `ps aux`

```
PS C:\Users\baptiste> docker container exec ping sh
/ # ps aux
PID  USER      TIME  COMMAND
  1 root      0:00  ping 8.8.8.8
  7 root      0:00  sh
 14 root      0:00  ps aux
/ # |
```

Tapez : `exit` pour sortir du **shell**.

Stoppons les containers : **ping** et **www**

```
docker container stop ping www
```

faites ensuite : `docker container ls`

Que constatez vous ? Pourquoi ?

Même question avec : `docker container ls -a`

Supprimons maintenant les containers créés :

```
docker container rm $(docker container ls -a -q)
```

## 2.7. Exercices :

==Exercice 1 : Hello From Alpine

Le but de ce premier exercice est de lancer des containers basés sur l'image **alpine**.

1. Lancez un container basé sur alpine en lui fournissant la commande echo hello
2. Quelles sont les étapes effectuées par le docker daemon ?
3. Lancez un container basé sur alpine sans lui spécifier de commande. Qu'observez-vous ?

### 2.7.1. Exercice 2 : Shell interactif

Le but de cet exercice est lancer des containers en mode **interactif**.

1. Lancez un container basé sur alpine en mode **interactif** sans lui spécifier de commande
2. Que s'est-il passé ?
3. Quelle est la commande par défaut d'un container basé sur **alpine** ?
4. Naviguez dans le **système de fichiers**
5. Utilisez le gestionnaire de package d'alpine (**apk**) pour ajouter un package : **apk update** et **apk add curl**.

### 2.7.2. Exercice 3 : foreground / background

Le but de cet exercice est de créer des containers en **foreground** et en **background**.

1. Lancez un container basé sur alpine en lui spécifiant la commande **ping 8.8.8.8**.
2. Arrêter le container avec **CTRL-C**

Le container est t-il toujours en cours d'exécution ?

*Note*

 Vous pouvez utiliser la commande **docker ps** que nous détaillerons prochainement, et qui permet de lister les containers qui tournent sur la machine.

1. Lancez un container en mode interactif en lui spécifiant la commande **ping 8.8.8.8**.
2. Arrêter le container avec **CTRL-P CTRL-Q**

Le container est t-il toujours en cours d'exécution ?

1. Lancez un container en **background**, toujours en lui spécifiant la commande **ping 8.8.8.8**.

Le container est t-il toujours en cours d'exécution ?

### 2.7.3. Exercice 4 : Publication de port

Le but de cet exercice est de créer un container **en exposant un port** sur la machine **hôte**.

1. Lancez un container basé sur **nginx** et publiez le **port 80** du container sur le **port 8080** de l'hôte.
2. Vérifiez depuis votre navigateur que la page par défaut de **nginx** est servie sur <http://localhost:8080>.
3. Lancez un second container en publiant le même port.

Qu'observez-vous ?

### 2.7.4. Exercice 5 : Liste des containers

Le but de cet exercice est de montrer les différentes options pour lister les containers du système.

1. Listez les containers en cours d'exécution.

Est ce que tous les containers que vous avez créés sont listés ?

1. Utilisez l'option **-a** pour voir également les containers qui ont été stoppés.
2. Utilisez l'option **-q** pour ne lister que les IDs des containers (en cours d'exécution ou stoppés).

### 2.7.5. Exercice 6 : Inspection d'un container

Le but de cet exercice est l'inspection d'un container.

1. Lancez, en **background**, un nouveau container basé sur **nginx** en publiant le **port 80** du container sur le **port 3000** de la machine host.

Notez l'identifiant du container retourné par la commande précédente.

1. Inspectez le container en utilisant son identifiant.
2. En utilisant le **format Go template**, récupérez le nom et l'**IP** du container.
3. Manipuler les **Go template** pour récupérer d'autres information.

### 2.7.6. Exercice 7 : exec dans un container

Le but de cet exercice est de montrer comment lancer un processus dans un container existant.

1. Lancez un container en background, basé sur l'image alpine. Spécifiez la commande **ping 8.8.8.8** et le nom ping avec l'option **--name**.
2. Observez les logs du container en utilisant l'ID retourné par la commande précédente ou bien le nom du container.

Quittez la commande de logs avec **CTRL-C**.

1. Lancez un shell **sh**, en mode **interactif**, dans le container précédent.
2. Listez les processus du container.

Qu'observez vous par rapport aux identifiants des processus ?

### 2.7.7. Exercice 8 : cleanup

Le but de cet exercice est de stopper et de supprimer les containers existants.

1. Listez tous les containers (**actifs** et **inactifs**)
2. Stoppez tous les containers encore actifs en fournissant la liste des IDs à la commande **stop**.
3. Vérifiez qu'il n'y a plus de containers actifs.
4. Listez les containers arrêtés.
5. Supprimez tous les containers.
6. Vérifiez qu'il n'y a plus de containers.

## 2.8. En résumé

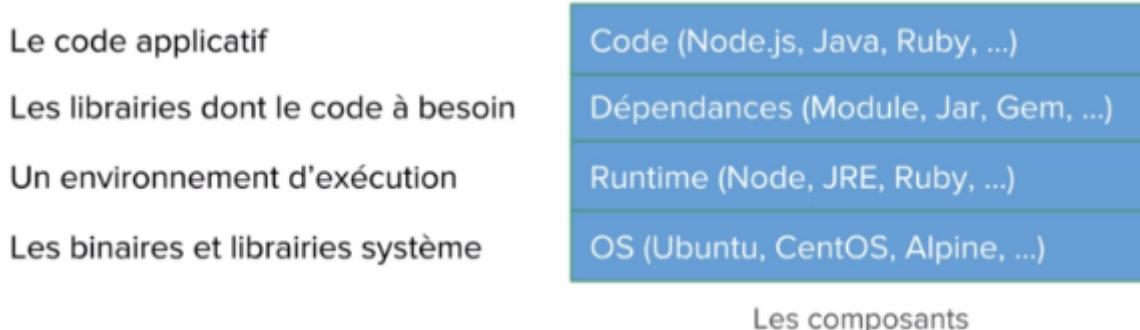
Nous avons commencé à jouer avec les containers et vu les commandes les plus utilisées pour la gestion du cycle de vie des containers (**run**, **exec**, **ls**, **rm**, **inspect**). Nous les utiliserons souvent dans la suite du cours.

C'est parfois utile d'avoir un **Shell** directement sur la machine hôte. C'est-à-dire la machine sur laquelle le **Docker Daemon** tourne. Si l'on est sur **linux**, le client et le **daemon** tournent sur la **même machine**. Par contre le **docker daemon** va tourner sur une **machine virtuelle** sous Windows alors que le client sera lui sur une machine locale.

## 3. Les images Docker

Nous allons parler des images **Docker**. Une image est un système de fichier qui contient une application et l'ensemble des éléments nécessaires pour la faire tourner. On peut voir une image comme étant un **template** permettant la création d'un container. L'image est portable sur n'importe quel environnement où tourne **Docker** et est composée de **couches (layers)** qui peuvent être réutilisé par d'autres images. On distribue une image via un **registry** ( ex : Docker Hub)

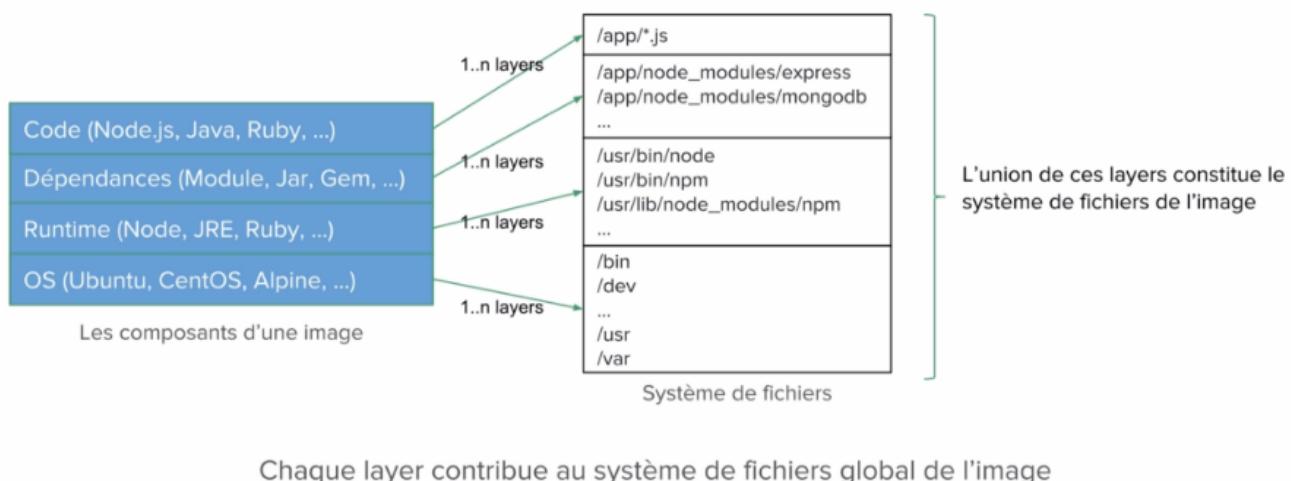
Contenu d'une image :



La construction du fichier image, se fait dans l'ordre inverse du contenu d'une image que l'on vient de lister.

On part d'un OS de base qui va ajouter une ou plusieurs couches comme le système de fichiers. A cet OS on va ajouter une ou plusieurs couches liées à l'environnement de notre application puis de la même façon les dépendances et le code applicatifs.

Et l'ensemble de ses couches forment l'image.



### 3.1. Union Filesystem

Une image est donc constituée d'un ensemble de **layers** ou **couches** et chacune d'elles est en **lectures seules**. Et c'est le rôle du **storage/graph driver** de constituer le système de fichier global de l'instance du container.

Le **Graph driver** ajoute en plus une couche qui est en **lecture/écriture** pour permettre au processus de modifier le filesystem sans que les modifications ne soient persistées dans les layers de l'image. Il existe plusieurs **filesystem** et le choix du système dépend principalement du **filesystem hôte**. Par default, toutes les layers sont installées dans le répertoire `/var/lib/docker` sur la machine hôte et c'est à cette endroit que sont stockées toutes les layers des images.

Sur windows 10, docker s'exécute sur une VM. Ressources à consulter pour comprendre comment Docker fonction sous Windows :



1. <https://docs.docker.com/desktop/windows/>
2. <https://forums.docker.com/t/the-location-of-images-in-docker-for-windows/19647>

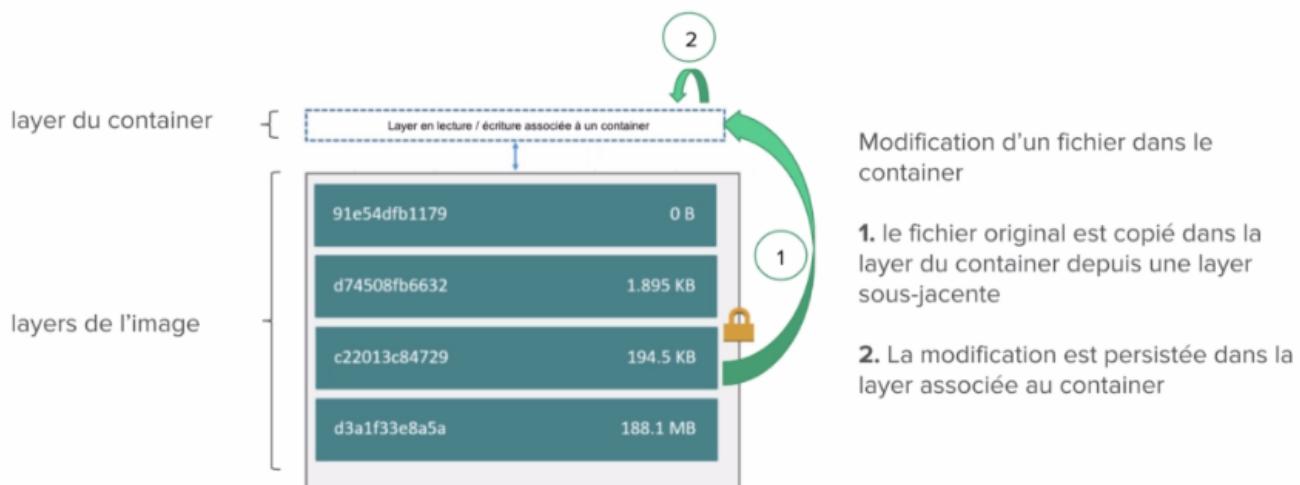
Pour accéder à ce dossier sous Windows, il faut alors créer un container et le lier avec Docker :

```
docker run -it --privileged --pid=host debian nsenter -t 1 -m -u -i sh
```

Nous pouvons alors lister le dossier `/var/lib/docker` dans le shell.

```
ls /var/lib/docker
```

Il est possible de modifier des fichiers qui sont apportés par une layer ; cela s'appelle : **copy-On-Write**. Le fichier original est alors copier dans la layer qui est en **lecture / écriture** et la modification peut être **persistée**.



## 3.2. Exercices

### 3.2.1. Exercice 1 : Container's layer

La layer d'un container, est la layer **read-write** créé lorsqu'un container est lancé. C'est la layer dans laquelle tous les changements effectués dans le container sont sauvegardés. Cette layer est supprimée avec le container et ne doit donc pas être utilisée comme un stockage persistant.

## Lancement d'un container

Utilisez la commande suivante pour lancer un **shell interactif** dans un container basé sur l'image **ubuntu**.

```
docker container run -ti ubuntu
```

## Installation d'un package

**figlet** est un package qui prend un texte en entrée et le formatte de façon amusante. Par défaut ce package n'est pas disponible dans l'image ubuntu.

Vérifiez le avec la commande suivante:

```
figlet
```

La commande devrait donner le résultat suivant :

```
bash: figlet: command not found
```

Installez le package **figlet** avec les commandes suivantes:

```
apt-get update -y  
apt-get install figlet
```

Vérifiez que le binaire fonctionne :

```
figlet Hola
```

Ce qui devrait donner le résultat suivant

Sortez du container.

```
exit
```

## Lancement d'un nouveau container

Lancez un nouveau container basé sur **ubuntu**.

```
docker container run -ti ubuntu
```

Vérifiez si le package **figlet** est présent :

```
figlet
```

Vous devriez obtenir l'erreur suivante:

```
bash: figlet: command not found
```

Comment expliquez-vous ce résultat ? Chaque container lancé à partir de l'image **ubuntu** est différent des autres. Le second container est différent de celui dans lequel **figlet** a été installé. Chacun correspond à une instance de l'image ubuntu et a sa propre **layer**, ajoutée au dessus des layers de l'image, et dans laquelle tous les changements effectués dans le container sont sauvegardés.

Sortez du container.

```
exit
```

## Redémarrage du container

Listez les containers (en exécution ou non) sur la machine hôte.

```
docker container ls -a
```

Depuis cette liste, récuperez l'ID du container dans lequel le package **figlet** a été installé et redémarrez le avec la commande suivante.

**Note:** la commande **start** permet de démarrer un container se trouvant dans l'état **Exited**.

```
docker container start <CONTAINER_ID>
```

Lancez un **shell interactif** dans ce container en utilisant la commande **exec**.

```
docker container exec -ti <CONTAINER_ID> bash
```

Vérifiez que **figlet** est présent dans ce container.

```
figlet Hola
```

Résultat :



Vous pouvez maintenant sortir du container.

```
exit
```

## Nettoyage

Listez les containers (en exécution ou non) sur la machine hôte

```
docker container ls -a
```

Pour supprimer tous les containers, nous pouvons utiliser les commandes `rm` et `ls -aq` conjointement. Nous ajoutons l'option `-f` afin de forcer la suppression des containers encore en exécution. Il faudrait sinon arrêter les containers et les supprimer.

```
docker container rm -f $(docker container ls -aq)
```

Tous les containers ont été supprimés, vérifiez le une nouvelle fois avec la commande suivante:

```
docker container ls -a
```

## 3.3. DockerFile

Le **DockerFile** est un fichier texte qui est utilisé pour la construction d'**une image DOCKER**. Il contient des instructions pour la construction du système de fichier d'une image. Nous allons partir d'un fichier de base qui sera enrichie par notre application et l'ensemble de ses dépendances.

- Exemple d'un **Docker File** dans laquelle est packagée une application **NODEJS**.

```

# Image de base
FROM node:8.11.1-alpine

# Copie de la liste des dependances
COPY package.json /app/package.json

# Installation / compilation des dependances
RUN cd /app && npm install

# Copie du code applicatif
COPY . /app/

# Exposition du port HTTP
EXPOSE 80

# Positionnement du répertoire de travail
WORKDIR /app

# Commande exécutée au lancement d'un container
CMD ["npm", "start"]

```

Exemple de Dockerfile utilisé pour une application Node.js

Avec l'instruction **FROM** nous définissons une image de base dans laquelle l'application **NODEJS** sera packagée.

- **COPY** qui permet d'ajouter la liste des dépendances.
- **RUN** permet de définir la commande d'installation des dépendances.
- **EXPOSE** défini le port utilisé par l'application.
- **WORKDIR** nous positionnes dans le répertoire de travail.
- **CMD** défini la commande à lancer lorsqu'un container sera lancer à partir de cette image.

Voici la liste des principales instructions à utiliser dans un **DockerFile**.

FROM	Image de base
ENV	Définition de variables d'environnement
RUN	Exécution d'une commande, construction du filesystem de l'image
COPY / ADD	Copie de ressources depuis la machine local dans le filesystem de l'image
EXPOSE	Expose un port de l'application
HEALTHCHECK	Vérifie l'état de santé de l'application
VOLUME	Définition d'un volume pour la gestion des données
WORKDIR	Définition du répertoire de travail
USER	Utilisateur auquel appartient le processus du container
ENTRYPOINT	Définie la commande exécutée au lancement du container
CMD	

### L'instruction FROM.

Il s'agit de la première instruction dans un DOckerFile. Elle permet de spécifier l'image à partir de laquelle nous allons créer une nouvelle image. On peut partir d'une image d'un OS, ou d'une image contenant déjà des applications comme un serveur web, ou un environnement d'exécution

enveloppé dans une image contenant un OS de base.

Nous pouvons utiliser également une image particulière qui s'appelle **SCRATCH**, c'est une image au sens **DOCKER** même si elle est vide, et peut être utilisé par exemple dans une application écrite en langage GO qui n'a pas besoin d'être packagé dans un système de fichier.

### L'instruction ENV.

Cette instruction nous permet de définir des variables d'environnement. Et pourront être utilisées dans les instructions suivantes lors de la construction de l'image. On les retrouvera dans l'environnement des containers lancés à partir de cette image.

```
FROM nginx:1.14.0
ENV path /usr/share/nginx/html/
WORKDIR ${path}
COPY . $path
```

Dans cet exemple, nous construisons une image basée sur NGINX et on définit une variable **path** que l'on pourra utiliser dans les instructions suivantes : **WORKDIR** et **COPY**.

### L'instruction COPY / ADD.

Permet de copier des ressources locales vers le système de fichier de l'image que l'on créé.

Et cela engendre la création d'une nouvelle layer pour l'image.

Avec l'option **chown** on peut définir les droits sur ces fichiers qu'auront les utilisateurs de l'image.

**ADD** permet des actions supplémentaires comme récupérer des ressources à partir d'une URL. Ou de Dézipper des fichiers.

Il est préférable d'utiliser **COPY** par rapport à **ADD** car l'on maîtrise davantage comment la copie est faite.

### L'instruction RUN.

**RUN** est une instruction qui va engendrer la construction d'une nouvelle **layer** pour l'image.

Elle permet d'exécuter une commande dans le système de fichier de l'image comme l'installation d'un package. Il y a 2 formats pour définir la commande. Le format **SHELL** qui va lancer la commande dans le contexte d'un **shell**. Et le format **Exec** qui va définir la commande comme une liste de **string** et qui n'est pas lancée dans le contexte d'un **shell**.

- Shell : lancé dans un shell avec "/bin/sh -c" par défaut

```
RUN apt-get update -y && apt-get install
```

- Exec : non lancé dans un shell

```
RUN ["/bin/bash", "-c", "echo hello"]
```

### L'instruction EXPOSE.

Permet de spécifier les ports sur lesquels l'application écoute au lancement du container. Mais cela peut être modifié par l'option : **-p** lors de la création du container. Nous pouvons utiliser aussi un mapping comme vu précédemment : **-p HOST\_PORT:CONTAINER\_PORT**.

On peut aussi utiliser l'option **P** dans ce cas le démon **DOCKER** va publier l'ensemble des ports en attribuant à chacun un port de la machine hôte.

```
...
EXPOSE 27017
CMD ["mongod"]
```

Extrait du Dockerfile de MongoDB

```
...
EXPOSE 80
CMD ["nginx", "-g", "daemon off;"]
```

Extrait du Dockerfile de Nginx

### L'instruction VOLUME.

Permet de définir un répertoire dont les données sont découplées du cycle de vie du container. Les fichiers ne seront pas stockés dans la layer **lecture/écriture** du container mais dans le système de fichier de la machine hôte. Et si le container est supprimé, les données de ce répertoire seront toujours là.

Si on reprend l'exemple du **dockerfile de MongoDB**.

```
...
RUN mkdir -p /data/db /data/configdb \
&& chown -R mongodb:mongodb /data/db /data/configdb
VOLUME /data/db /data/configdb

COPY docker-entrypoint.sh /usr/local/bin/
ENTRYPOINT ["docker-entrypoint.sh"]

EXPOSE 27017
CMD ["mongod"]
```

L'instruction **VOLUME** est utilisée pour créer 2 volumes. Au lancement de cette image, deux répertoires seront créés sur la machine hôte.

### L'instruction USER.

Si on ne définit pas l'utilisateur, par défaut se sera **ROOT** qui sera utilisé. Ce qui pose des problèmes de sécurité évident.

### L'instruction HEALTHCHECK.

Vérifie l'état de santé du processus qui tourne dans un container. On peut définir des options comme la fréquence d'inspection.

```
FROM node:8.11-alpine
RUN apk update && apk add curl
HEALTHCHECK --interval=5s --timeout=3s --retries=3 CMD curl -f http://localhost:8000/health || exit 1
COPY package.json /app/package.json
WORKDIR /app
RUN npm install
COPY . /app
CMD [ "npm", "start" ]
```

### L'instruction ENTRYPPOINT / CMD.

Spécifie la commande qui sera exécuté lorsque l'on lancera un container basé sur cette image. Les instruction **CMD** et **ENTRYPOINT** sont les dernières instructions du fichier **DOCKERFILE**.

On précise souvent le binaire de l'application dans **ENTRYPOINT** et les paramètres dans **CMD**.

La commande alors exécuté correspondra à la concaténation de **ENTRYPOINT** et **CMD**.

On peut modifier ses paramètres au lancement du container si besoin avec l'annotation **Shell** ou **Exec** vu précédemment.

```
ENTRYPOINT ["curl"]
CMD ["--help"]
```

## 3.4. Crédit d'images

Il est temps maintenant de créer notre image. Dans un premier temps il faut : créer un fichier **DockerFile** qui contiendra les instructions nécessaires. Ensuite il faut utiliser la commande :

```
docker image build [OPTIONS] PATH | URL | -
```

Des options courantes :

- **-f** : spécifie le fichier à utiliser pour la construction (**DockerFile** par défaut)
- **--tag / -t** : spécifie le nom de l'image ([registry/]user/repository :tag)
- **--label** : ajout de métadonnées à l'image.

## 3.5. Mise en pratique

Nous allons créer une simple application **NODEJS** qui renverra la date et l'heure. Tout l'environnement nécessaire à l'exécution de ce script sera intégré dans une image que nous allons créer.

Dans un dossier, créez le fichier **index.js**:

```
var express = require('express');
var util = require('util');
```

```
var app = express();

app.get('/', function(req, res) {
  res.setHeader('Content-Type', 'text/plain');
  res.end(util.format('%s - %s\n', new Date(), 'Got Request'));
});

app.listen(process.env.PORT || 8080);
```

Puis créez le fichier `package.js` dans le même dossier :

```
{
  "name": "testnode",
  "version": "0.0.1",
  "main": "index.js",
  "scripts": {
    "start": "node index.js"
  },
  "dependencies": {
    "express": "^4.14.0"
  }
}
```

Dans une console, placez vous dans le dossier dans lequel vous avez déposé les fichiers et tapez :

```
npm install
```

puis

```
npm start
```

Ouvrez un navigateur à l'adresse : <http://localhost:8080>

Si tout se passe comme prévu alors vous devriez avoir ceci :



2022-02-21T16:14:04.366Z - Got Request

Notre application fonctionne, mais cela est lourd pour l'utilisateur :

1. Il doit avoir NODEJS d'installé sur sa machine.
2. Il doit installer les dépendances du projet, ici `express`.
3. Il doit lancer le serveur Nodejs.

Il faudrait donc créer une image réalisant ces étapes !!

Nous allons créer un **DockerFile**.

Il nous faut trouver une image de base sur : [Docker Hub](#)

**Cochez : « Official Images »** pour n'avoir que des images officielles. Nous voyons que nous avons une multitude de possibilité pour concevoir notre image.

The screenshot shows the Docker Hub search interface. On the left, there are filters for 'Images' and 'Categories'. Under 'Categories', 'Official Images' is checked. The search results show three official images:

- alpine**: Alpine Linux image, updated 3 months ago, with 1B+ downloads and 8.5K stars. It's a minimal Docker image based on Alpine Linux with a complete package index and only 5 MB in size! It supports Container, Linux, IBM Z, 386, riscv64, PowerPC 64 LE, ARM 64, ARM, x86-64, Featured Images, Base Images, and Operating Systems.
- ubuntu**: Ubuntu image, updated 20 days ago, with 1B+ downloads and 10K+ stars. Ubuntu is a Debian-based Linux operating system based on free software. It supports Container, Linux, riscv64, IBM Z, 386, x86-64, ARM, ARM 64, PowerPC 64 LE, Base Images, and Operating Systems.
- busybox**: Busybox base image, updated 17 days ago, with 1B+ downloads and 2.5K stars. It's a Busybox base image. It supports Container, Linux, ARM 64, PowerPC 64 LE, IBM Z, ARM, riscv64, x86-64, 386, mips64le, and Base Images.

Nous pouvons partir sur une image **LINUX : UBUNTU, ALPINE ...Etc** mais aussi une image où le runtime **NODEJS** est déjà packagé. C'est ce que nous allons choisir.

The screenshot shows the details page for the **node** Docker image. It's an official image, last updated 10 days ago, with 1B+ downloads and 10K+ stars. Node.js is a JavaScript-based platform for server-side and networking applications. It supports Container, Linux, x86-64, ARM, ARM 64, PowerPC 64 LE, IBM Z, 386, and Application Infrastructure.

En cliquant dessus, sélectionnez l'onglet **TAGS**.

The screenshot shows the 'Tags' section for the node Docker image. It lists several tags, with 'alpine3.15' being the most recent one.

Description	Reviews	Tags
		alpine3.15, latest, v12.18.3, v12.18.2, v12.18.1, v12.18.0, v12.17.3, v12.17.2, v12.17.1, v12.17.0, v12.16.3, v12.16.2, v12.16.1, v12.16.0, v12.15.3, v12.15.2, v12.15.1, v12.15.0, v12.14.3, v12.14.2, v12.14.1, v12.14.0, v12.13.3, v12.13.2, v12.13.1, v12.13.0, v12.12.3, v12.12.2, v12.12.1, v12.12.0, v12.11.3, v12.11.2, v12.11.1, v12.11.0, v12.10.3, v12.10.2, v12.10.1, v12.10.0, v12.9.3, v12.9.2, v12.9.1, v12.9.0, v12.8.3, v12.8.2, v12.8.1, v12.8.0, v12.7.3, v12.7.2, v12.7.1, v12.7.0, v12.6.3, v12.6.2, v12.6.1, v12.6.0, v12.5.3, v12.5.2, v12.5.1, v12.5.0, v12.4.3, v12.4.2, v12.4.1, v12.4.0, v12.3.3, v12.3.2, v12.3.1, v12.3.0, v12.2.3, v12.2.2, v12.2.1, v12.2.0, v12.1.3, v12.1.2, v12.1.1, v12.1.0, v12.0.3, v12.0.2, v12.0.1, v12.0.0, v11.14.3, v11.14.2, v11.14.1, v11.14.0, v11.13.3, v11.13.2, v11.13.1, v11.13.0, v11.12.3, v11.12.2, v11.12.1, v11.12.0, v11.11.3, v11.11.2, v11.11.1, v11.11.0, v11.10.3, v11.10.2, v11.10.1, v11.10.0, v11.9.3, v11.9.2, v11.9.1, v11.9.0, v11.8.3, v11.8.2, v11.8.1, v11.8.0, v11.7.3, v11.7.2, v11.7.1, v11.7.0, v11.6.3, v11.6.2, v11.6.1, v11.6.0, v11.5.3, v11.5.2, v11.5.1, v11.5.0, v11.4.3, v11.4.2, v11.4.1, v11.4.0, v11.3.3, v11.3.2, v11.3.1, v11.3.0, v11.2.3, v11.2.2, v11.2.1, v11.2.0, v11.1.3, v11.1.2, v11.1.1, v11.1.0, v11.0.3, v11.0.2, v11.0.1, v11.0.0, v10.19.3, v10.19.2, v10.19.1, v10.19.0, v10.18.3, v10.18.2, v10.18.1, v10.18.0, v10.17.3, v10.17.2, v10.17.1, v10.17.0, v10.16.3, v10.16.2, v10.16.1, v10.16.0, v10.15.3, v10.15.2, v10.15.1, v10.15.0, v10.14.3, v10.14.2, v10.14.1, v10.14.0, v10.13.3, v10.13.2, v10.13.1, v10.13.0, v10.12.3, v10.12.2, v10.12.1, v10.12.0, v10.11.3, v10.11.2, v10.11.1, v10.11.0, v10.10.3, v10.10.2, v10.10.1, v10.10.0, v10.9.3, v10.9.2, v10.9.1, v10.9.0, v10.8.3, v10.8.2, v10.8.1, v10.8.0, v10.7.3, v10.7.2, v10.7.1, v10.7.0, v10.6.3, v10.6.2, v10.6.1, v10.6.0, v10.5.3, v10.5.2, v10.5.1, v10.5.0, v10.4.3, v10.4.2, v10.4.1, v10.4.0, v10.3.3, v10.3.2, v10.3.1, v10.3.0, v10.2.3, v10.2.2, v10.2.1, v10.2.0, v10.1.3, v10.1.2, v10.1.1, v10.1.0, v10.0.3, v10.0.2, v10.0.1, v10.0.0, v9.18.3, v9.18.2, v9.18.1, v9.18.0, v9.17.3, v9.17.2, v9.17.1, v9.17.0, v9.16.3, v9.16.2, v9.16.1, v9.16.0, v9.15.3, v9.15.2, v9.15.1, v9.15.0, v9.14.3, v9.14.2, v9.14.1, v9.14.0, v9.13.3, v9.13.2, v9.13.1, v9.13.0, v9.12.3, v9.12.2, v9.12.1, v9.12.0, v9.11.3, v9.11.2, v9.11.1, v9.11.0, v9.10.3, v9.10.2, v9.10.1, v9.10.0, v9.9.3, v9.9.2, v9.9.1, v9.9.0, v9.8.3, v9.8.2, v9.8.1, v9.8.0, v9.7.3, v9.7.2, v9.7.1, v9.7.0, v9.6.3, v9.6.2, v9.6.1, v9.6.0, v9.5.3, v9.5.2, v9.5.1, v9.5.0, v9.4.3, v9.4.2, v9.4.1, v9.4.0, v9.3.3, v9.3.2, v9.3.1, v9.3.0, v9.2.3, v9.2.2, v9.2.1, v9.2.0, v9.1.3, v9.1.2, v9.1.1, v9.1.0, v9.0.3, v9.0.2, v9.0.1, v9.0.0, v8.17.3, v8.17.2, v8.17.1, v8.17.0, v8.16.3, v8.16.2, v8.16.1, v8.16.0, v8.15.3, v8.15.2, v8.15.1, v8.15.0, v8.14.3, v8.14.2, v8.14.1, v8.14.0, v8.13.3, v8.13.2, v8.13.1, v8.13.0, v8.12.3, v8.12.2, v8.12.1, v8.12.0, v8.11.3, v8.11.2, v8.11.1, v8.11.0, v8.10.3, v8.10.2, v8.10.1, v8.10.0, v8.9.3, v8.9.2, v8.9.1, v8.9.0, v8.8.3, v8.8.2, v8.8.1, v8.8.0, v8.7.3, v8.7.2, v8.7.1, v8.7.0, v8.6.3, v8.6.2, v8.6.1, v8.6.0, v8.5.3, v8.5.2, v8.5.1, v8.5.0, v8.4.3, v8.4.2, v8.4.1, v8.4.0, v8.3.3, v8.3.2, v8.3.1, v8.3.0, v8.2.3, v8.2.2, v8.2.1, v8.2.0, v8.1.3, v8.1.2, v8.1.1, v8.1.0, v8.0.3, v8.0.2, v8.0.1, v8.0.0, v7.16.3, v7.16.2, v7.16.1, v7.16.0, v7.15.3, v7.15.2, v7.15.1, v7.15.0, v7.14.3, v7.14.2, v7.14.1, v7.14.0, v7.13.3, v7.13.2, v7.13.1, v7.13.0, v7.12.3, v7.12.2, v7.12.1, v7.12.0, v7.11.3, v7.11.2, v7.11.1, v7.11.0, v7.10.3, v7.10.2, v7.10.1, v7.10.0, v7.9.3, v7.9.2, v7.9.1, v7.9.0, v7.8.3, v7.8.2, v7.8.1, v7.8.0, v7.7.3, v7.7.2, v7.7.1, v7.7.0, v7.6.3, v7.6.2, v7.6.1, v7.6.0, v7.5.3, v7.5.2, v7.5.1, v7.5.0, v7.4.3, v7.4.2, v7.4.1, v7.4.0, v7.3.3, v7.3.2, v7.3.1, v7.3.0, v7.2.3, v7.2.2, v7.2.1, v7.2.0, v7.1.3, v7.1.2, v7.1.1, v7.1.0, v7.0.3, v7.0.2, v7.0.1, v7.0.0, v6.14.3, v6.14.2, v6.14.1, v6.14.0, v6.13.3, v6.13.2, v6.13.1, v6.13.0, v6.12.3, v6.12.2, v6.12.1, v6.12.0, v6.11.3, v6.11.2, v6.11.1, v6.11.0, v6.10.3, v6.10.2, v6.10.1, v6.10.0, v6.9.3, v6.9.2, v6.9.1, v6.9.0, v6.8.3, v6.8.2, v6.8.1, v6.8.0, v6.7.3, v6.7.2, v6.7.1, v6.7.0, v6.6.3, v6.6.2, v6.6.1, v6.6.0, v6.5.3, v6.5.2, v6.5.1, v6.5.0, v6.4.3, v6.4.2, v6.4.1, v6.4.0, v6.3.3, v6.3.2, v6.3.1, v6.3.0, v6.2.3, v6.2.2, v6.2.1, v6.2.0, v6.1.3, v6.1.2, v6.1.1, v6.1.0, v6.0.3, v6.0.2, v6.0.1, v6.0.0, v5.13.3, v5.13.2, v5.13.1, v5.13.0, v5.12.3, v5.12.2, v5.12.1, v5.12.0, v5.11.3, v5.11.2, v5.11.1, v5.11.0, v5.10.3, v5.10.2, v5.10.1, v5.10.0, v5.9.3, v5.9.2, v5.9.1, v5.9.0, v5.8.3, v5.8.2, v5.8.1, v5.8.0, v5.7.3, v5.7.2, v5.7.1, v5.7.0, v5.6.3, v5.6.2, v5.6.1, v5.6.0, v5.5.3, v5.5.2, v5.5.1, v5.5.0, v5.4.3, v5.4.2, v5.4.1, v5.4.0, v5.3.3, v5.3.2, v5.3.1, v5.3.0, v5.2.3, v5.2.2, v5.2.1, v5.2.0, v5.1.3, v5.1.2, v5.1.1, v5.1.0, v5.0.3, v5.0.2, v5.0.1, v5.0.0, v4.13.3, v4.13.2, v4.13.1, v4.13.0, v4.12.3, v4.12.2, v4.12.1, v4.12.0, v4.11.3, v4.11.2, v4.11.1, v4.11.0, v4.10.3, v4.10.2, v4.10.1, v4.10.0, v4.9.3, v4.9.2, v4.9.1, v4.9.0, v4.8.3, v4.8.2, v4.8.1, v4.8.0, v4.7.3, v4.7.2, v4.7.1, v4.7.0, v4.6.3, v4.6.2, v4.6.1, v4.6.0, v4.5.3, v4.5.2, v4.5.1, v4.5.0, v4.4.3, v4.4.2, v4.4.1, v4.4.0, v4.3.3, v4.3.2, v4.3.1, v4.3.0, v4.2.3, v4.2.2, v4.2.1, v4.2.0, v4.1.3, v4.1.2, v4.1.1, v4.1.0, v4.0.3, v4.0.2, v4.0.1, v4.0.0, v3.13.3, v3.13.2, v3.13.1, v3.13.0, v3.12.3, v3.12.2, v3.12.1, v3.12.0, v3.11.3, v3.11.2, v3.11.1, v3.11.0, v3.10.3, v3.10.2, v3.10.1, v3.10.0, v3.9.3, v3.9.2, v3.9.1, v3.9.0, v3.8.3, v3.8.2, v3.8.1, v3.8.0, v3.7.3, v3.7.2, v3.7.1, v3.7.0, v3.6.3, v3.6.2, v3.6.1, v3.6.0, v3.5.3, v3.5.2, v3.5.1, v3.5.0, v3.4.3, v3.4.2, v3.4.1, v3.4.0, v3.3.3, v3.3.2, v3.3.1, v3.3.0, v3.2.3, v3.2.2, v3.2.1, v3.2.0, v3.1.3, v3.1.2, v3.1.1, v3.1.0, v3.0.3, v3.0.2, v3.0.1, v3.0.0, v2.13.3, v2.13.2, v2.13.1, v2.13.0, v2.12.3, v2.12.2, v2.12.1, v2.12.0, v2.11.3, v2.11.2, v2.11.1, v2.11.0, v2.10.3, v2.10.2, v2.10.1, v2.10.0, v2.9.3, v2.9.2, v2.9.1, v2.9.0, v2.8.3, v2.8.2, v2.8.1, v2.8.0, v2.7.3, v2.7.2, v2.7.1, v2.7.0, v2.6.3, v2.6.2, v2.6.1, v2.6.0, v2.5.3, v2.5.2, v2.5.1, v2.5.0, v2.4.3, v2.4.2, v2.4.1, v2.4.0, v2.3.3, v2.3.2, v2.3.1, v2.3.0, v2.2.3, v2.2.2, v2.2.1, v2.2.0, v2.1.3, v2.1.2, v2.1.1, v2.1.0, v2.0.3, v2.0.2, v2.0.1, v2.0.0, v1.13.3, v1.13.2, v1.13.1, v1.13.0, v1.12.3, v1.12.2, v1.12.1, v1.12.0, v1.11.3, v1.11.2, v1.11.1, v1.11.0, v1.10.3, v1.10.2, v1.10.1, v1.10.0, v1.9.3, v1.9.2, v1.9.1, v1.9.0, v1.8.3, v1.8.2, v1.8.1, v1.8.0, v1.7.3, v1.7.2, v1.7.1, v1.7.0, v1.6.3, v1.6.2, v1.6.1, v1.6.0, v1.5.3, v1.5.2, v1.5.1, v1.5.0, v1.4.3, v1.4.2, v1.4.1, v1.4.0, v1.3.3, v1.3.2, v1.3.1, v1.3.0, v1.2.3, v1.2.2, v1.2.1, v1.2.0, v1.1.3, v1.1.2, v1.1.1, v1.1.0, v1.0.3, v1.0.2, v1.0.1, v1.0.0, v0.13.3, v0.13.2, v0.13.1, v0.13.0, v0.12.3, v0.12.2, v0.12.1, v0.12.0, v0.11.3, v0.11.2, v0.11.1, v0.11.0, v0.10.3, v0.10.2, v0.10.1, v0.10.0, v0.9.3, v0.9.2, v0.9.1, v0.9.0, v0.8.3, v0.8.2, v0.8.1, v0.8.0, v0.7.3, v0.7.2, v0.7.1, v0.7.0, v0.6.3, v0.6.2, v0.6.1, v0.6.0, v0.5.3, v0.5.2, v0.5.1, v0.5.0, v0.4.3, v0.4.2, v0.4.1, v0.4.0, v0.3.3, v0.3.2, v0.3.1, v0.3.0, v0.2.3, v0.2.2, v0.2.1, v0.2.0, v0.1.3, v0.1.2, v0.1.1, v0.1.0, v0.0.3, v0.0.2, v0.0.1, v0.0.0

Et dans la liste, nous allons nous intéresser à une version de **NODEJS** sous Alpine3.15.

TAG	DIGEST	OS/ARCH	COMPRESSED SIZE
current-alpine3.15	1ea32da58dd6	linux/amd64	49.02 MB
	0043bb44b001	linux/arm/v6	47.97 MB
	282d94d9edee	linux/arm/v7	47.3 MB
+3 more...			

Et conservons en mémoire le tag de cette version de node : current-alpine3.15

Maintenant dans le dossier contenant notre application, créons un fichier : **Dockerfile**. Sans extension.

### Fichier : Dockerfile

```
# Nous renseignons dans l'instruction FROM le Tag de notre image qui servira de base à
# notre application
FROM node:current-alpine3.15

# Nous allons copier nos fichiers sources du répertoire courant du fichier Dockerfile
# dans le répertoire /app/.
# C'est un répertoire qui sera créé dans l'image lorsque l'on va faire le build
COPY . /app/
RUN cd /app && npm install
EXPOSE 8080
WORKDIR /app
CMD ["npm", "start"]
```

A partir de ce **Dockerfile**, nous allons pouvoir créer une **image**.

```
docker image build -t appbts:0.1 .
```



```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> docker image build -t appbts:0.1 .
[+] Building 12.0s (10/10) FINISHED
⇒ [internal] load build definition from Dockerfile
⇒ ⇒ transferring dockerfile: 47B
⇒ [internal] load .dockerignore
⇒ ⇒ transferring context: 2B
⇒ [internal] load metadata for docker.io/library/node:current-alpine3.15
⇒ [auth] library/node:pull token for registry-1.docker.io
⇒ [internal] load build context
⇒ ⇒ transferring context: 1.78MB
⇒ [1/4] FROM docker.io/library/node:current-alpine3.15@sha256:0e83c81025bc29e614189acf3d419e3c09881cef9f7a170fdcf3e15bbfd5
⇒ ⇒ resolve docker.io/library/node:current-alpine3.15@sha256:0e83c810225bc29e614189acf3d6419e3c09881cef9f7a170fdcf3e15bbfd5
⇒ ⇒ sha256:c6a2764d974bd4282296a11650b126e912159874a75809619b6fee0ed142dfa 6.53kB / 6.53kB
⇒ ⇒ sha256:47b63b511936c7feff2a2e2af5e33b015231fed160c11036e9b891661212e17e3 46.25MB / 46.25MB
⇒ ⇒ sha256:0e83c810225bc29e614189acf3d419e3c09881cef9f7a170fdcf3e15bbfd5 1.43kB / 1.43kB
⇒ ⇒ sha256:1ea32da58dd6d3ed50163f7e1add4ba7cbe62ae6fabef24139c8349778f6ec2 1.16kB / 1.16kB
⇒ ⇒ sha256:99fc5a6cadcc483a47220bae86a1037fb85a1bb0414af81673f46d2eb04e0e0dd 451B / 451B
⇒ ⇒ sha256:acce0d11a36090fc0d068694eb3cf0c403853713da2f4e81c8dd2bcd036d4ef 2.34MB / 2.34MB
⇒ ⇒ extracting sha256:47b63b511936c7feff2a2e2af5e33b015231fed160c11036e9b891661212e17e3
⇒ ⇒ extracting sha256:acce0d11a36090fc0d068694eb3cf0c403853713da2f4e81c8dd2bcd036d4ef
⇒ ⇒ extracting sha256:99fc5a6cadcc483a47220bae86a1037fb85a1bb414aaaf81673f46d2eb04e0e0dd
⇒ [2/4] COPY . /app/
⇒ [3/4] RUN cd /app && npm install
⇒ [4/4] WORKDIR /app
⇒ exporting to image
⇒ ⇒ writing image sha256:7c68d3cfdd1de77fe10e51153bd335e56fdfce0f7375afdf404d6b90ad81cd77f
⇒ ⇒ naming to docker.io/library/appbts:0.1
```

Nous voyons que pour chaque instruction nous avons une étape.

Si nous allons dans **Docker Desktop**, onglet « **Images** » :

NAME ↑	TAG	IMAGE ID	CREATED	SIZE
alpine	latest	c059bfaa849c	3 months ago	5.59 MB
appbts	0.1	7c68d3cfdd1d	less than a minute ago	174.9 MB
debian	<b>IN USE</b>	04fbda87a6a	27 days ago	123.89 MB
hello-world	latest	feb5d9fea6a5	5 months ago	13.26 KB
mongo	4.0	e70e486406ef	21 days ago	430.28 MB
nginx	latest	c316d5a335a5	26 days ago	141.5 MB
ubuntu	latest	54c9d81cbb44	20 days ago	72.78 MB

Nous voyons notre image, avec son nom et son numéro de version. Nous pouvons maintenant créer un conteneur avec notre application, en précisant que nous utiliserons le **port 8080** du container sur le **port 8080** de ma machine hôte.

```
docker container run -p 8080:8080 appbts:0.1
```

Et je peux maintenant utiliser mon navigateur à l'adresse : <http://localhost:8080>

## 3.6. Exercices : Création d'images

### 3.6.1. Exercice 1 : Création d'une image à partir d'un container

1. Lancez une container basé sur une image **alpine**, en mode **interactif**, et en lui donnant le nom **c1**.
2. Lancez la commande `curl google.com`.

Qu'observez-vous ?

1. Installez `curl` à l'aide du gestionnaire de package `apk`.
2. Quittez le container avec **CTRL-P CTRL-Q** (pour ne pas killer le processus de **PID 1**).
3. Créez une image, nommée `curly`, à partir du container **c1**.

Utilisez pour cela la commande `commit` (`docker commit --help` pour voir le fonctionnement de cette commande).

1. Lancez un **shell** interactif dans un container basée sur l'image `curly` et vérifiez que `curl` est présent.

### 3.6.2. Exercice 2 : Dockerizez un serveur web simple

1. Créez un nouveau répertoire et développez un serveur HTTP qui expose le endpoint `/ping` sur le **port 80** et répond par **PONG**. Inspirez vous de l'exemple du cours ci-dessus.
2. Dans le même répertoire, créez le fichier **Dockerfile** qui servira à construire l'image de l'application. Ce fichier devra décrire les actions suivantes :
  - spécification d'une image de base.
  - installation du runtime correspondant au langage choisi.
  - installation des dépendances de l'application.
  - copie du code applicatif.
  - exposition du port d'écoute de l'application.
  - spécification de la commande à exécuter pour lancer le serveur.
3. Construire l'image en la taguant `pong:v1.0`.
4. Lancez un container basé sur cette image en publiant le `port 80` sur le `port 8080` de la machine hôte.
5. Tester l'application.
6. Supprimez le container.

### 3.6.3. Exercice 3 : ENTRYPPOINT et CMD

Nous allons illustrer sur plusieurs exemples l'utilisation des instructions **ENTRYPPOINT** et **CMD**. Ces instructions sont utilisées dans un **Dockerfile** pour définir la commande qui sera lancée dans un container.

#### 3.6.3.1. Format

Dans un **Dockerfile**, les instructions **ENTRYPPOINT** et **CMD** peuvent être spécifiées selon 2 formats:

- le format `shell`, ex: `ENTRYPOINT /usr/bin/node index.js`. Une commande spécifiée dans ce format sera exécutée via un shell présent dans l'image. Cela peut notamment poser des problématiques car les signaux ne sont pas forwardés aux processus forkés.
- le format `exec`, ex: `CMD ["node", "index.js"]`. Une commande spécifiée dans ce format ne nécessitera pas la présence d'un shell dans l'image. On utilisera souvent le format exec pour ne pas avoir de problème si aucun shell n'est présent.

#### 3.6.3.2. Ré-écriture à l'exécution d'un container

**ENTRYPPOINT** et **CMD** sont 2 instructions du Dockerfile, mais elles peuvent cependant être écrasées au lancement d'un container:

- pour spécifier une autre valeur pour l'**ENTRYPPOINT**, on utilisera l'option `--entrypoint`, par exemple: `docker container run --entrypoint echo alpine hello`.
- pour spécifier une autre valeur pour **CMD**, on précisera celle-ci après le nom de l'image, par exemple: `docker container run alpine echo hello`.

### 3.6.3.3. Instruction ENTRYPPOINT utilisée seule

L'utilisation de l'instruction **ENTRYPPOINT** seule permet de créer un wrapper autour de l'application. Nous pouvons définir une commande de base et lui donner des paramètres supplémentaires, si nécessaire, au lancement d'un container.

Dans ce premier exemple, vous allez créer un fichier **Dockerfile-v1** contenant les instructions suivantes:

```
FROM alpine
ENTRYPOINT ["ping"]
```

Créez ensuite une image, nommée **ping:1.0**, à partir de ce fichier.

```
docker image build -f Dockerfile-v1 -t ping:1.0 .
```

Lancez maintenant un container basé sur l'image **ping:1.0**

```
docker container run ping:1.0
```

La commande **ping** est lancée dans le container (car elle est spécifiée dans **ENTRYPPOINT**), ce qui produit le message suivant:

```
BusyBox v1.26.2 (2017-05-23 16:46:25 GMT) multi-call binary.
Usage: ping [OPTIONS] HOST
Send ICMP ECHO_REQUEST packets to network hosts
  -4,-6           Force IP or IPv6 name resolution
  -c CNT          Send only CNT pings
  -s SIZE         Send SIZE data bytes in packets (default:56)
  -t TTL          Set TTL
  -I IFACE/IP    Use interface or IP address as source
  -W SEC          Seconds to wait for the first response (default:10)
                  (after all -c CNT packets are sent)
  -w SEC          Seconds until ping exits (default:infinite)
                  (can exit earlier with -c CNT)
  -q              Quiet, only display output at start
                  and when finished
  -p              Pattern to use for payload
```

Par défaut, aucune machine hôte n'est ciblée, et à chaque lancement d'un container il est nécessaire de préciser un **FQDN** ou une **IP**. La commande suivante lance un nouveau container en lui donnant l'adresse IP d'un DNS Google (**8.8.8.8**), nous ajoutons également l'option **-c 3** pour limiter le nombre de ping envoyés.

```
docker container run ping:1.0 -c 3 8.8.8.8
```

Nous obtenons alors le résultat suivant :

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=37 time=8.731 ms
64 bytes from 8.8.8.8: seq=1 ttl=37 time=8.503 ms
64 bytes from 8.8.8.8: seq=2 ttl=37 time=8.507 ms
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0%
round-trip min/avg/max = 8.503/8.580/8.731 ms
```

La commande lancée dans le container est donc la concaténation de l'**ENTRYPOINT** et de la commande spécifiée lors du lancement du container (tout ce qui est situé après le nom de l'image). Comme nous pouvons le voir dans cet exemple, l'image que nous avons créée est un wrapper autour de l'utilitaire **ping** et nécessite de spécifier des paramètres supplémentaires au lancement d'un container.

### 3.6.3.4. Instructions CMD utilisée seule

De la même manière, il est possible de n'utiliser que l'instruction **CMD** dans un **Dockerfile**, c'est d'ailleurs très souvent l'approche qui est utilisée car il est plus simple de manipuler les instructions **CMD** que les **ENTRYPOINT**. Créez un fichier **Dockerfile-v2** contenant les instructions suivantes:

```
FROM alpine
CMD ["ping"]
```

Créez une image, nommée **ping:2.0** , à partir de ce fichier.

```
docker image build -f Dockerfile-v2 -t ping:2.0 .
```

Si nous lançons maintenant un nouveau container, il lancera la commande ping comme c'était le cas avec l'exemple précédent dans lequel seul l'ENTRYPOINT était défini.

```
$ docker container run ping:2.0
BusyBox v1.26.2 (2017-05-23 16:46:25 GMT) multi-call binary.
Usage: ping [OPTIONS] HOST
Send ICMP ECHO_REQUEST packets to network hosts
  -4,-6      Force IP or IPv6 name resolution
  -c CNT      Send only CNT pings
  -s SIZE     Send SIZE data bytes in packets (default:56)
  -t TTL      Set TTL
  -I IFACE/IP Use interface or IP address as source
  -W SEC      Seconds to wait for the first response (default:10)
               (after all -c CNT packets are sent)
  -w SEC      Seconds until ping exits (default:infinite)
               (can exit earlier with -c CNT)
```

-q	Quiet, only display output at start and when finished
-p	Pattern to use for payload

Nous n'avons cependant pas le même comportement que précédemment, car pour spécifier la machine à cibler, il faut redéfinir la commande complète à la suite du nom de l'image.

Si nous ne spécifions que les paramètres de la commande ping, nous obtenons un message d'erreur car la commande lancée dans le container ne peut pas être interprétée.

```
docker container run ping:2.0 -c 3 8.8.8.8
```

Vous devriez alors obtenir l'erreur suivante:

```
container_linux.go:247: starting container process caused "exec: \"-c\": executable  
file not found in $PATH"  
docker: Error response from daemon: oci runtime error: container_linux.go:247:  
starting container process ca  
used "exec: \"-c\": executable file not found in $PATH".  
ERRO[0000] error getting events from daemon: net/http: request canceled
```

Il faut redéfinir la commande dans sa totalité, ce qui est fait en la spécifiant à la suite du nom de l'image.

```
$ docker container run ping:2.0 ping -c 3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8): 56 data bytes  
64 bytes from 8.8.8.8: seq=0 ttl=37 time=10.223 ms  
64 bytes from 8.8.8.8: seq=1 ttl=37 time=8.523 ms  
64 bytes from 8.8.8.8: seq=2 ttl=37 time=8.512 ms  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 8.512/9.086/10.223 ms
```

### 3.6.3.5. Instructions ENTRYPPOINT et CMD

Il est également possible d'utiliser ENTRYPPOINT et CMD en même temps dans un Dockerfile, ce qui permet à la fois de créer un wrapper autour d'une application et de spécifier un comportement par défaut.

Nous allons illustrer cela sur un nouvel exemple et créer un fichier Dockerfile-v3 contenant les instructions suivantes:

```
FROM alpine  
ENTRYPOINT ["ping"]  
CMD ["-c3", "localhost"]
```

Ici, nous définissons ENTRYPOINT et CMD, la commande lancée dans un container sera la concaténation de ces 2 instructions: ping -c3 localhost. Créez une image à partir de ce Dockerfile, nommez la ping:3.0, et lancez un nouveau container à partir de celle-ci.

```
$ docker image build -f Dockerfile-v3 -t ping:3.0 .
$ docker container run ping:3.0
```

Vous devriez alors obtenir le résultat suivant:

```
PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.102 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.048 ms
--- localhost ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.048/0.070/0.102 ms
```

Nous pouvons écraser la commande par défaut et spécifier une autre adresse IP

```
docker container run ping:3.0 8.8.8.8
```

Nous obtenons alors le résultat suivant:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=38 time=9.235 ms
64 bytes from 8.8.8.8: seq=1 ttl=38 time=8.590 ms
64 bytes from 8.8.8.8: seq=2 ttl=38 time=8.585 ms
```

Il faut alors faire un CTRL-C pour arrêter le container car l'option -c3 limitant le nombre de ping n'a pas été spécifiée. Cela nous permet à la fois d'avoir un comportement par défaut et de pouvoir facilement le modifier en spécifiant une autre commande.

### 3.6.4. Pour aller plus loin : où est stockée mon image ?

#### 3.6.4.1. Stockage d'une image

Dans un exercice précédent, nous avons créé une image nommée ping:1.0, nous allons voir ici où cette image est stockée.

Reprenons le Dockerfile de l'exercice :

```
FROM ubuntu:16.04
RUN apt-get update -y && apt-get install -y iputils-ping
ENTRYPOINT ["ping"]
```

```
CMD ["8.8.8.8"]
```

A partir de ce Dockerfile, l'image est buildée avec la commande suivante :

```
$ docker image build -t ping:1.0 .  
Sending build context to Docker daemon 2.048kB  
Step 1/4 : FROM ubuntu:16.04  
--> 5e8b97a2a082  
Step 2/4 : RUN apt-get update -y && apt-get install -y iputils-ping  
--> Using cache  
--> 4cd5304ad0fb  
Step 3/4 : ENTRYPOINT ["ping"]  
--> Using cache  
--> d2846bbd30e8  
Step 4/4 : CMD ["8.8.8.8"]  
--> Using cache  
--> 00a905f2bd5a  
Successfully built 00a905f2bd5a  
Successfully tagged ping:1.0
```

Pour lister les images présentes localement on utilise la commande `docker image ls` (on reverra cette commande un peu plus loin). Pour ne lister que les images qui ont le nom `ping` on le précise à la suite de `ls`.

```
$ docker image ls ping
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
ping	1.0	00a905f2bd5a	4 weeks ago	159MB

Notre image est constituée d'un ensemble de layers, il faut voir chaque layer comme un morceau de système de fichiers. L'ID de l'image (dans sa version courte) est `00a905f2bd5a`, nous allons voir à partir de cette identifiant comment l'image est stockée sur la machine hôte (la machine sur laquelle tourne le daemon Docker).

Tout se passe dans le répertoire `/var/lib/docker`, c'est le répertoire au Docker gère l'ensemble des primitives (containers, images, volumes, networks, ...). Et plus précisément dans `/var/lib/docker/image/overlay2/`, overlay2 étant le driver en charge du stockage des images.

**Note:** si vous utilisez **Docker for Mac** ou **Docker for Windows**, il est nécessaire d'utiliser la commande suivante pour lancer un `shell` dans la machine virtuelle dans laquelle tourne le daemon Docker. On pourra ensuite explorer le répertoire `/var/lib/docker` depuis ce shell.

```
docker run -it --privileged --pid=host debian nsenter -t 1 -m -u -n -i sh
```

Plusieurs **fichiers / répertoires** ont un nom qui contient l'ID de notre image comme on peut le voir

ci-dessous :

```
/var/lib/docker/image/overlay2 # find . | grep 00a905f2bd5a  
.imagedb/content/sha256/00a905f2bd5aa3b1c4e28611704717679352a619bcd  
c4f8f6851cf459dc05  
816  
.imagedb/metadata/sha256/00a905f2bd5aa3b1c4e28611704717679352a619bcd  
c4f8f6851cf459dc05  
816  
.imagedb/metadata/sha256/00a905f2bd5aa3b1c4e28611704717679352a619bcd  
c4f8f6851cf459dc05  
816/lastUpdated  
.imagedb/metadata/sha256/00a905f2bd5aa3b1c4e28611704717679352a619bcd  
c4f8f6851cf459dc05  
816/parent
```

- **Content** : le premier fichier contient un ensemble d'information concernant cette image, notamment les paramètres de configuration, l'historique de création (ensemble des commandes qui ont servi à construire le système de fichiers contenu dans l'image), et également l'ensemble des layers qui la constituent. Une grande partie de ces informations peuvent également être retrouvées avec la commande :

```
docker image inspect ping:1.0
```

Parmi ces éléments, on a donc les identifiants de chaque layer :

```
"rootfs": {  
  "type": "layers",  
  "diff_ids": [  
    "sha256:644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2",  
    "sha256:d7ff1dc646ba52a02312b535446d6c9b72cd09fda0480524e4828554ef  
b2f748",  
    "sha256:686245e78935e73b737c9a82111c3c7df35f5529d06ce8c2f9a7cd32ec  
90b456",  
    "sha256:d73dd9e652956dcbbef716de4b172cc15fff644cc92fc69d221cc3a1cb  
89a39",  
    "sha256:2de391e51d731ba02b708038a7f98b7103061b916727bcd165e9ee6402f4cd  
de",  
    "sha256:3045bfad4cfefecabc342600d368863445b12ed18188f5f2896c5389b0e84b  
66"  
  ]  
}
```

Si l'on considère la première layer (celle dont l'ID est 6448...), on voit dans [/var/lib/docker/image/overlay2](#) qu'il y a un répertoire dont le nom correspond à l'ID de cette layer, celui-ci contient plusieurs fichiers :

```
/var/lib/docker/image/overlay2 # find . | grep '644879075e24394fefef8a7dddefbc133aad42'  
.layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2  
.layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2/size  
.layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2/tar-  
split.json.gz  
.layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2/diff  
.layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cac  
f98bd1e3d5ddde2/cach  
e-id
```

```
./distribution/v2metadata-by-
diffid/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cacf98bd1e3d
```

Ceux-ci contiennent différentes informations sur la layer en question. Parmi celles-ci, le fichier **cache-id** nous donne l'identifiant du cache qui a été généré pour cette layer.

```
/var/lib/docker/image/overlay2 # cat
./layerdb/sha256/644879075e24394fefef8a7dddefbc133aad42002df6223cacf98bd1e3d5ddde2/cach
e-id
49908d07e177f9b61dc273ec7089efed9223d3798ad1d86c78d4fe953e227668
```

Le système de fichier construit dans cette layer est alors accessible dans le répertoire :

```
/var/lib/docker/overlay2/49908d07e177f9b61dc273ec7089efed9223d3798ad1d86c78d4fe953e227
668/diff/
```

**LastUpdated** : ce fichier contient la date de dernière mise à jour de l'image

```
/var/lib/docker/image/overlay2 # cat
./imagedb/metadata/sha256/00a905f2bd5...459dc05816/lastUpdated
2018-07-31T07:32:04.6840553Z
```

- **parent** : ce fichier contient l'identifiant du container qui a servi à créer l'image.

```
/var/lib/docker/image/overlay2 # cat
./imagedb/metadata/sha256/00a905f2bd5459dc05816/parent
sha256:d2846bbd30e811ac8baaf759fc6c4f424c8df2365c42dab34d363869164881ae
```

On retrouve d'ailleurs ce container dans l'avant dernière étape de création de l'image.

```
Step 3/4 : ENTRYPOINT ["ping"]
---> Using cache
---> d2846bbd30e8
```

Ce container est celui qui a été commité pour créer l'image finale.

**En résumé** : il est important de garder en tête qu'une image est constituée de plusieurs layers. Chaque layer est une partie du système de fichiers de l'image finale. C'est le rôle du driver de stockage de stocker ces différentes layers et de construire le système de fichiers de chaque container lancé à partir de cette image.

## 3.7. Multi-Stages Build

Depuis la version **17.05** de Docker, nous pouvons découper le Build d'une image en plusieurs étapes.

Un cas d'usage courant :

**Etape 1** : Avoir une image de base contenant l'ensemble des librairies et binaires nécessaires pour la création d'artéfacts.

**Etape 2** : Utiliser une image de base plus light et d'y copier les artéfacts générés à l'étape précédente.

**Exemple :**

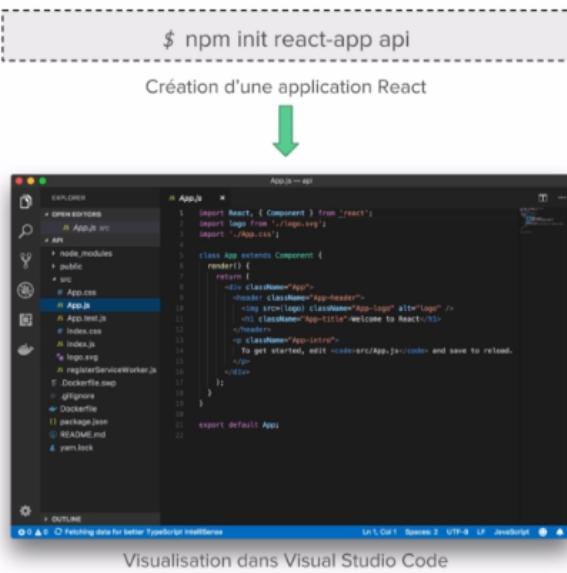
Considérons une application **ReactJs**. Pour créer le squelette d'un projet React nous utilisons la commande :

```
npm init react-app api
```

un dossier **api** est créé.

```
cd api
```

En utilisant le **multistage build** nous allons construire des artéfacts Web. Et nous aurons seulement besoin de copier ces artefacts dans un serveur **WEB NGINX** dans un second temps.



```
FROM node:8.11-alpine as build
WORKDIR /app
COPY package.json ./package.json
RUN npm install
COPY . .
RUN npm run build

FROM nginx:1.14.0
COPY --from=build /app/build/ /usr/share/nginx/html/
EXPOSE 80
CMD ["nginx", "-g", "daemon off;"]
```

Dockerfile avec multi stage build

**Dans le DockerFile** : La première instruction **FROM** utilise une image **NODE** dans laquelle les dépendances de l'application seront installées. Et le code applicatif Buildé.

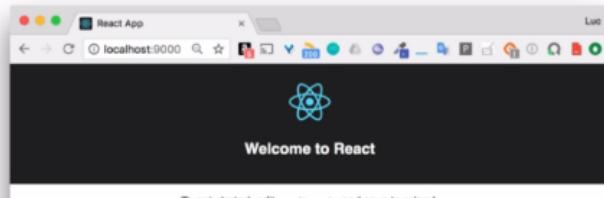
Et la seconde instruction **FROM** utilise une image **NGINX** dans laquelle les assets web buildés précédemment sont copiés. Et au final nous avons une seule image qui contient notre application.

Cela peut être vérifié en faisant le Build de l'image :

```
$ docker image build -t app:1.0 .
Sending build context to Docker daemon 116.8MB
Step 1/10 : FROM node:8.11-alpine as build
--> ca148a52ea10
Step 2/10 : WORKDIR /app
--> ac238d1a666d
...
Step 8/10 : COPY --from=build /app/build/
/usr/share/nginx/html/
--> Using cache
--> a8028d66c9f9
Step 9/10 : EXPOSE 80
--> Running in 2f47dc17484
Removing intermediate container 2f47dc17484
--> a87f7038dbb3
Step 10/10 : CMD ["nginx", "-g", "daemon off;"]
--> Running in 5aa44388a837
Removing intermediate container 5aa44388a837
--> b4f80ee7f075
Successfully built b4f80ee7f075
Successfully tagged app:1.0
```

Création d'un container à partir de l'image app:1.0

```
$ docker run -p 9000:80 app:1.0
```



## 3.8. Mise en pratique

Dans cette mise en pratique, nous allons illustrer le multi stage build.

### 3.8.1. Un serveur http écrit en Go

Prenons l'exemple du programme suivant écrit en Go.

Dans un nouveau répertoire, créez le fichier http.go contenant le code suivant. Celui-ci définit un simple serveur http qui écoute sur le port 8080 et qui expose le endpoint /whoami en GET. A chaque requête, il renvoie le nom de la machine hôte sur laquelle il tourne.

```
package main
import (
    "io"
    "net/http"
    "os"
)
func handler(w http.ResponseWriter, req *http.Request) {
    host, err := os.Hostname()
    if err != nil {
        io.WriteString(w, "unknown")
    } else {
        io.WriteString(w, host)
    }
}
func main() {
    http.HandleFunc("/whoami", handler)
    http.ListenAndServe(":8080", nil)
}
```

### 3.8.1.1. Dockerfile traditionel

Afin de créer une image pour cette application, créez tout dabord le fichier Dockerfile avec le contenu suivant (placez ce fichier dans le même répertoire que http.go):

```
FROM golang:1.17
WORKDIR /go/src/app
COPY http.go .
RUN go mod init
RUN CGO_ENABLED=0 GOOS=linux go build -o http .
CMD ["./http"]
```

Note: dans ce Dockerfile, l'image officielle golang est utilisée comme image de base, le fichier source http.go est copié puis compilé.

Vous pouvez ensuite builder l'image et la nommer whoami:1.0:

```
docker image build -t whoami:1.0 .
```

Listez les images présentes et notez la taille de l'image whoami:1.0

```
$ docker image ls whoami
REPOSITORY      TAG          IMAGE ID      CREATED       SIZE
whoami           1.0          16795cf36deb  2 seconds ago  962MB
```

L'image obtenue a une taille très conséquente car elle contient l'ensemble de la toolchain du langage Go. Or, une fois que le binaire a été compilé, nous n'avons plus besoin du compilateur dans l'image finale.

### 3.8.1.2. Dockerfile utilisant un build multi-stage

Le multi-stage build, introduit dans la version 17.05 de Docker permet, au sein d'un seul Dockerfile, d'effectuer le process de build en plusieurs étapes. Chacune des étapes peut réutiliser des artefacts (fichiers résultant de compilation, assets web, ...) créés lors des étapes précédentes. Ce Dockerfile aura plusieurs instructions FROM mais seule la dernière sera utilisée pour la construction de l'image finale.

Si nous reprenons l'exemple du serveur http ci dessus, nous pouvons dans un premier temps compiler le code source en utilisant l'image golang contenant le compilateur. Une fois le binaire créé, nous pouvons utiliser une image de base vide, nommée scratch, et copier le binaire généré précédemment.

Remplacer le contenu du fichier Dockerfile avec les instructions suivantes:

```
FROM golang:1.17 as build
WORKDIR /go/src/app
COPY http.go .
```

```
RUN go mod init  
RUN CGO_ENABLED=0 GOOS=linux go build -o http .  
  
FROM scratch  
COPY --from=build /go/src/app .  
CMD ["../http"]
```

L'exemple que nous avons utilisé ici se base sur une application écrite en Go. ce langage a la particularité de pouvoir être compilé en un binaire static, c'est à dire ne nécessitant pas d'être "linké" à des librairies externes. C'est la raison pour laquelle nous pouvons partir de l'image scratch. Pour d'autres langages, l'image de base utilisée lors de la dernière étape du build pourra être différente (alpine, ...)

Buildez l'image dans sa version 2 avec la commande suivante.

```
docker image build -t whoami:2.0 .
```

Listez les images et observez la différence de taille entre celles-ci:

```
$ docker image ls whoami  
REPOSITORY      TAG          IMAGE ID      CREATED       SIZE  
whoami           2.0          0a97315aeaaa  6 seconds ago  6.07MB  
whoami           1.0          16795cf36deb  2 minutes ago  962MB
```

Lancez un container basé sur l'image whoami:2.0

```
docker container run -p 8080:8080 whoami:2.0
```

A l'aide de la commande curl, envoyez une requête GET sur le endpoint exposé. Vous devriez avoir, en retour, l'identifiant du container qui a traité la requête.

```
$ curl localhost:8080/whoami  
7562306c6c5e
```

Pour cette simple application, le multistage build a permis de supprimer les binaires et librairies dont la présence est inutile dans l'image finale. L'exemple d'une application écrite en go est extrême, mais le multistage build fait partie des bonnes pratiques à adopter pour de nombreux langages de développement.

## 3.9. Prise en compte du cache

Quand on écrit un Dockerfile, on doit prendre en compte le mécanisme de cache.

Pour optimiser le temps nécessaire pour construire l'image.

Quand une image est créée chaque instruction crée une layer et en fonction de la complexité du Dockerfile, le premier build peut prendre un peu de temps mais les suivant seront très rapide parce que les layers existantes seront réutilisés.

Un Dockerfile qui est créé doit s'assurer que le cache est bien utilisé.

On peut l'utiliser pour reconstruire une image après qu'un changement ait été effectué, dans un fichier de configuration par exemple de sorte qu'il empêche le code source d'être compilé à nouveau si cela n'est pas nécessaire.

Il y a plusieurs façons de forcer la recréation des layers d'une image si besoin. Notamment par la modification de la valeur d'une variable d'environnement ou si on modifie le code source qui est pris en compte dans les instructions ADD ou COPY.

Si une instruction invalide le cache, alors toutes les instructions après ne l'utiliseront pas.

A partir de l'exemple de l'application NODEJS vue précédemment :

- Chaque instruction utilise le cache créé lors du build précédent
- Création de l'image quasi immédiate

```
FROM node:8.11-alpine
COPY package.json /app/package.json
RUN cd /app && npm install
COPY . /app/
WORKDIR /app
EXPOSE 80
CMD ["npm", "start"]
```



```
$ docker image build -t app:1.0 .
Sending build context to Docker daemon 4.096kB
Step 1/7 : FROM node:8.11-alpine
--> 8adf3c3eb26c
Step 2/7 : COPY package.json /app/package.json
--> Using cache
--> 1d0614163d62
Step 3/7 : RUN cd /app && npm install
--> Using cache
--> de7ac239b6b5
Step 4/7 : COPY . /app/
--> Using cache
--> 812921ed8643
Step 5/7 : WORKDIR /app
--> Using cache
--> ea7c2d576e53
Step 6/7 : EXPOSE 80
--> Using cache
--> 202601df911a
Step 7/7 : CMD ["npm", "start"]
--> Using cache
--> 24f42e7ed5ea
Successfully built 24f42e7ed5ea
Successfully tagged app:1.0
```

Si on lance une nouvelle fois le build de l'image on voit que pour chaque instruction le cache est utilisé. Cela signifie que pour chaque instruction la layer qui a déjà été créé, la première version, est réutilisé. Lorsque que l'image est créée pour la première fois, cela prend un peu de temps car il faut récupérer les dépendances et l'image. Mais à l'aide du cache cela prend quelque seconde.

Faites l'expérience : Dans le dossier contenant l'application NODEJS, tapez la commande :

```
Docker image build -t app :0.1 .
```

```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> docker image build -t appbts:0.1 .
[+] Building 1.8s (10/10) FINISHED
  => [internal] load build definition from Dockerfile
  => => transferring dockerfile: 32B
  => [internal] load .dockerignore
  => => transferring context: 2B
  => [internal] load metadata for docker.io/library/node:current-alpine3.15
  => [auth] library/node:pull token for registry-1.docker.io
  => [internal] load build context
  => => transferring context: 20.98kB
  => [1/4] FROM docker.io/library/node:current-alpine3.15@sha256:0e83c810225bc29e614189acf3d6419e3c09881cefb9f7a170fdcf3e15bbfd5
  => CACHED [2/4] COPY . /app/
  => CACHED [3/4] RUN cd /app && npm install
  => CACHED [4/4] WORKDIR /app
  => exporting to image
  => => exporting layers
  => => writing image sha256:1cab61d3de9b52003b3dc2950fd5a93b19f57bf74fb89bd53974b2033724f0ec
  => => naming to docker.io/library/appbts:0.1
```

**Utilisation du cache**

Nous allons maintenant modifier le code de l'application. Ouvrons : index.js et modifions le label

```
var express = require('express');
var util = require('util');
var app = express();
app.get('/', function(req, res) {
  res.setHeader('Content-Type', 'text/plain');
  res.end(util.format('%s - %s\n', new Date(), '==> Test Modification'));
});
app.listen(process.env.PORT || 8080);
```

et rebuildons l'image

```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> docker image build -t appbts:0.1 .
[+] Building 3.6s (9/9) FINISHED
  => [internal] load build definition from Dockerfile
  => => transferring dockerfile: 32B
  => [internal] load .dockerignore
  => => transferring context: 2B
  => [internal] load metadata for docker.io/library/node:current-alpine3.15
  => [internal] load build context
  => => transferring context: 21.28kB
  => CACHED [1/4] FROM docker.io/library/node:current-alpine3.15@sha256:0e83c810225bc29e614189acf3d6419e3c09881cefb9f7a170fdcf3e15bbfd5
  => [2/4] COPY . /app/ Docker Daemon détecte que les fichiers ont été modifiés.
  => [3/4] RUN cd /app && npm install Alors le cache n'est pas utilisé pour les étapes 2 à 4
  => [4/4] WORKDIR /app
  => exporting to image
  => => exporting layers
  => => writing image sha256:7b68a4b2a8d48bde9e7b5e793db1e5c9a652577ea46b7fcf06f8d2d96a3e4fc5
  => => naming to docker.io/library/appbts:0.1
```

Lorsque l'on a changé le code source, cela a entraîné la reconstruction des dépendances de package.json. Ici ce n'est pas très long car nous n'avons que le package Express mais dans des applications plus lourdes cela peut impacter les performances.

Pour éviter ce problème nous allons modifier le DockerFile.

Nous allons faire en sorte de séparer le COPY en deux.

Dans le premier nous ne copierons que le fichier PACKAGE.JSON. Puis nous déplacerons l'instruction RUN de façon à récupérer les dépendances.

Ensuite nous copierons le code applicatif.

```
FROM node:current-alpine3.15
COPY package.json /app/package.json
RUN cd /app && npm install
COPY . /app/
```

```
EXPOSE 8080
WORKDIR /app
CMD ["npm", "start"]
```

Nous rebuildons ensuite notre image. Le cache n'est pas utilisé car le DOCKERFILE a été modifié alors tout est reconstruit.

Remodifions le code source.

```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> docker image build -t appbts:0.1 .
[+] Building 1.3s (10/10) FINISHED
  => [internal] load build definition from Dockerfile
  => => transferring dockerfile: 32B
  => [internal] load .dockerignore
  => => transferring context: 2B
  => [internal] load metadata for docker.io/library/node:current-alpine3.15
  => [1/5] FROM docker.io/library/node:current-alpine3.15@sha256:0e83c810225bc29e614189acf3d6419e3c09881cef9f7a170fdccfe3e15bbfd5
  => [internal] load build context
  => => transferring context: 21.28kB
  => CACHED [2/5] COPY package.json /app/package.json
  => CACHED [3/5] RUN cd /app && npm install
  => [4/5] COPY . /app/
  => [5/5] WORKDIR /app
  => exporting to image
  => => exporting layers
  => => writing image sha256:05cb03980b25bedbe7d0b3cbcd335dc612ad8021f291b95b0e6fb8b4b3d375d8
  => naming to docker.io/library/appbts:0.1
```

Package.json est bien utilisé en cache ici

Le code source est rechargé sans avoir à reconstruire les dépendances.

### 3.9.1. Exercice : Prise en compte du cache

1. Modifiez le code du serveur pong de l'exercice précédent. Vous pouvez par exemple ajouter une instruction qui loggue une chaîne de caractère.
2. Construisez une nouvelle image en la taguant pong:1.1
3. Qu'observez-vous dans la sortie de la commande de build ?
4. Modifiez le Dockerfile pour faire en sorte que les dépendances ne soient pas rebuildées si un changement est effectué dans le code. Créez l'image pong:1.2 à partir de ce nouveau Dockerfile.
5. Modifiez une nouvelle fois le code de l'application et créez l'image pong:1.3. Observez la prise en compte du cache

## 3.10. Le contexte de Build

Quand on construit une image Docker avec la commande Docker image build. La première chose que le client Docker fait, c'est d'envoyer au Daemon, sous forme d'une archive Tar, l'ensemble des fichiers nécessaire pour construire le système de fichier de l'image. Cet ensemble constitue le Build Context. Par défaut, c'est tout les fichiers qui sont envoyés. Cela peut être dangereux si l'on a des informations sensibles. D'où l'intérêt d'utiliser un fichier .DOCKERRUNIGNORE pour filtrer les fichiers et les répertoires qui ne doivent pas être répertorié par le contexte de build.

C'est le même principe que le fichier .gitignore sur GIT par exemple.

Reprenons l'exemple de notre application NODEJS.

Refaisons un build :

```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> docker image build -t appbts:0.1 .
[+] Building 1.3s (10/10) FINISHED
  => [internal] load build definition from Dockerfile
  => => transferring dockerfile: 32B
  => [internal] load .dockerignore
  => => transferring context: 2B
  => [internal] load metadata for docker.io/library/node:current-alpine3.15
  => [1/5] FROM docker.io/library/node:current-alpine3.15@sha256:0e83c810225bc29e614189acf3d6419e3c09881cef9f7a170fdcfe3e15bbfd5
  => [internal] load build context
  => => transferring context: 21.28kB
  => CACHED [2/5] COPY package.json /app/package.json
  => CACHED [3/5] RUN cd /app && npm install
  => [4/5] COPY . /app/
  => [5/5] WORKDIR /app
  => exporting to image
  => => exporting layers
  => => writing image sha256:05cb03980b25bedbe7d0b3cbcd335dc612ad8021f291b95b0e6fb8b4b3d375d8
  => => naming to docker.io/library/appbts:0.1
```

Durant le build nous constatons qu'avant de transférer le context de build au Daemon Docker, on essaie de charger le fichier .dockerignore.

Le contexte ici, correspond au répertoire courant symbolisé par le « . » à la fin de la commande docker image build.

On ne veut pas forcement que certains fichiers arrivent au Docker Daemon, comme un historique GIT ou de données sensibles comme des mots de passe stockés dans un fichier ENV ..ETC

Testons cela, en créant un dépôt git :

Dans le répertoire du projet NODEJS :

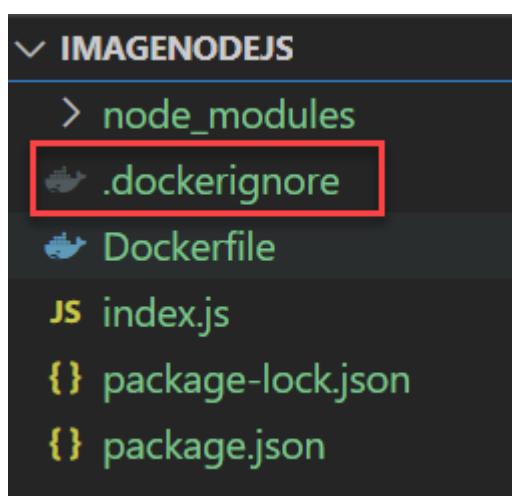
Git init

```
PS C:\Users\baptiste\Documents\docker\imageNodeJs> git init
Initialized empty Git repository in C:/Users/baptiste/Documents/docker/imageNodeJs/.git/
```

Et relançons le build :

Et constatons que le context transféré passe de : 21.28 Kb à 46.15kb. Cela signifie que l'ensemble des répertoires de git ont été transféré dans le Docker Daemon.

Créons donc un fichier .dockerignore et ajoutons le dossier .git.





Relançons le build et constatons la taille du context :

⇒ ⇒ transferring context: 21.02kB

Le .GIT n'est plus envoyé dans le context.

Dans une application NODEJS, nous pourrions aussi ajouter le répertoire node\_module qui contient les dépendances de l'application dans le .dockerignore.

## 3.11. Les commandes de base avec docker image.

### La commande PULL.

Permet de télécharger une image à partir d'un registry, par défaut : Docker Hub.

```
$ docker image ls
REPOSITORY          TAG      IMAGE ID      CREATED       SIZE
$ docker image pull alpine
Using default tag: latest
latest: Pulling from library/alpine
0a8490d0dfd3: Pull complete
Digest: sha256:dfbd4a3a8ebca874ebd2474f044a0b33600d4523d03b0df76e5c5986cb02d7e8
Status: Downloaded newer image for alpine:latest
$ docker image ls
REPOSITORY          TAG      IMAGE ID      CREATED       SIZE
alpine              latest   88e169ea8f46   2 weeks ago   3.98 MB
```

Format de nommage : USER/IMAGE :VERSION

Si l'on ne précise pas de numéro de version, par défaut c'est « latest » qui est retenu.

### La commande : push

La commande Push permet d'uploader une image dans un registry. Pour cela il faut avoir les droits sur ses images. Mais avant il faut avoir précisé ses identifiants de connexion au registry avec docker login.

### La commande : Inspect

Permet de voir la liste des layer qui composent une image. On peut utiliser ici aussi le formaliste Go Template.

```
$ docker image inspect alpine
[
  {
    "Id": "sha256:88e169ea8f46ff0d0df784b1b254a15ecfaf045aee1856dca1ec242fdd231ddd",
    "RepoTags": ["alpine:latest"],
    ...
    "Architecture": "amd64",
    "Os": "linux",
    "Size": 3983615,
    "VirtualSize": 3983615,
    "GraphDriver": {
      "Name": "aufs",
      "Data": null
    },
    "RootFS": {
      "Type": "layers",
      "Layers": [
        "sha256:60ab55d3379d47c1ba6b6225d59d10e1f52096ee9d5c816e42c635ccc57a5a2b"
      ]
    }
  }
]

$ docker image inspect -f '{{ .Architecture }}' alpine
Amd64

$ docker inspect --format '{{ .ContainerConfig.Cmd }}' mongo:3.2
[/bin/sh -c #(nop) CMD ["mongod"]]
```

## La commande : History

Permet de voir l'historique d'une image.

## La commande : ls

Permet d'énumérer les images localement.

\$ docker image ls				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
node	6.9.4	c5667be18e4e	2 days ago	655 MB
alpine	latest	88e169ea8f46	3 weeks ago	3.98 MB
<none>	<none>	d02c4d04476c	11 hours ago	653.2 MB

\$ docker image ls -a				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
<none>	<none>	dcb9d60b5a87	About a minute ago	653.2 MB
<none>	<none>	9a77011f0d01	About a minute ago	653.2 MB
node	6.9.4	c5667be18e4e	2 days ago	655 MB
alpine	latest	88e169ea8f46	3 weeks ago	3.98 MB
<none>	<none>	d02c4d04476c	11 hours ago	653.2 MB

\$ docker image ls node				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
node	6.9.4	06b984afb149	9 days ago	655 MB

\$ docker image ls --filter dangling=true				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
<none>	<none>	d02c4d04476c	11 hours ago	653.2 MB

\$ docker image prune				
Total reclaimed space: 653.2 MB				

Images créées ou téléchargées

Liste les images temporaires créées lors du build

Filtre des images par nom

Les images “dangling” ne sont plus référencées

Suppression des images “dangling”

## Les commandes Save et Load.

Save permet de sauvegarder une image et Load permet de charger une image à partir d'une sauvegarde.

```
$ docker images
REPOSITORY      TAG          IMAGE ID       CREATED        SIZE
alpine          latest        88e169ea8f46   3 weeks ago   3.98 MB

$ docker save -o alpine.tar alpine

$ ls
alpine.tar

$ docker image rm alpine
Untagged: alpine:latest
Untagged: alpine@sha256:dfbd4a3a8ebca874ebd2474f044a0b33600d4523d03b0df76e5c5986cb02d7e8
Deleted: sha256:88e169ea8f46ff0d0df784b1b254a15ecfaf045aee1856dca1ec242fdd231ddd
Deleted: sha256:60ab55d3379d47c1ba6b6225d59d10e1f52096ee9d5c816e42c635ccc57a5a2b

$ docker images
REPOSITORY      TAG          IMAGE ID       CREATED        SIZE
$ docker load < alpine.tar
60ab55d3379d: Loading layer [=====] 4.226 MB/4.226 MB
Loaded image: alpine:latest

$ docker image ls
REPOSITORY      TAG          IMAGE ID       CREATED        SIZE
alpine          latest        88e169ea8f46   3 weeks ago   3.98 MB
```

## La commande : rm

Supprime une image avec l'ensemble de ses layers. Plusieurs images peuvent être supprimées en même temps.

```
$ docker image ls
REPOSITORY      TAG          IMAGE ID       CREATED        SIZE
ubuntu          latest        f49eec89601e   16 hours ago  129 MB
mhart/alpine-node 6.9.4       d448eac1cfdb   2 weeks ago   49 MB
alpine          latest        88e169ea8f46   3 weeks ago   3.98 MB

$ docker image rm ubuntu
Untagged: ubuntu:latest
Untagged: ubuntu@sha256:71cd81252a3563a03ad8daee81047b62ab5d892ebbfb71cf53415f29c130950
Deleted: sha256:f49eec89601e8484026a8ed97be00f14db75339925fad17b440976cffcb88a
Deleted: sha256:3e2d12b23fafef176cf40429fb25be6572212807f27455b8e3e114c397324446f
Deleted: sha256:88a37465e211da3c72acbd999b158ee31c6c7239131f6308f000dcf52d622a7b
Deleted: sha256:99be185bee70b39c64096b8d39b96153d28d3caa7764961a9285ad4d189cd536
Deleted: sha256:fc7e2c65ec42780443f87ae7d9621cd6fcdb371e2127dd461b449d9e50b7ab7b
Deleted: sha256:4f03495a4d7de505ccb8b8e4cf0a8ac201491e1f67ae54b65584e0012aaab9c

$ docker image ls -q
d448eac1cfdb
88e169ea8f46

$ docker image rm $(docker image ls -q)
```

## 3.12. Exercice : Analyse du contenu d'une image

1. Télécharger l'image **mongo:3.6** en local
2. Quelles sont les différentes étapes de constructions de l'image

Comparez ces étapes avec le contenu du Dockerfile utilisé pour builder cette image.

1. Inspectez l'image
2. En utilisant la notation Go template, listez les ports exposés
3. Exportez l'image mongo:3.6 dans un tar
  - Extrayez le contenu de cette archive avec la commande **tar -xvf**, qu'observez-vous ?

- Extrayez le contenu d'une des layers, qu'observez-vous ?
4. Supprimez l'image mongo:3.6

## 4. Registry

En cours de rédaction ...

# 5. Stockage

Dans ce chapitre nous verrons comment une application peut persister ses données au sein d'un container.

## 5.1. Volume

Si un processus modifie ou créé un fichier , cette modification sera enregistrée dans le layer du container. Pour rappel, cette layer est créé au lancement du container et est en lecture/écriture. Elle est superposée aux layers qui sont en lecture de l'image.

Quand le container est supprimé, cette layer et tout les fichiers qu'elle contient sont également supprimés.

Donc pour persister des données, il faut les stocker à l'extérieur de la layer du container de manière à ne pas dépendre de son cycle de vie.

Pour cela il va falloir monter des **volumes** pour persister des données grâce à :

- L'instruction **VOLUME** dans le **Dockerfile**.
- L'option **-v** ou **--mount** à la création d'un container.
- La commande **docker create volume** de la CLI.

On utilise la persistance des données dans le cas de l'utilisation d'une base de données par exemple ou des fichiers de log.

Par exemple, si nous montons une image basée sur MongoDB :

```
docker container run -d --name mongo mongo:4.0
```

Et que nous inspectons le container :

```
docker container inspect -f '{{json .Mounts}}' mongo | python -m json.tool
```

```

[{"Type": "volume", "Name": "f460ce00574a9379e86fcfd6441442a6e0cc", "Source": "/var/lib/docker/volumes/f460ce00574a9379e86fcfd6441442a6e0cc", "Destination": "/data/configdb", "Driver": "Local", "Mode": "", "RW": true, "Propagation": ""}, {"Type": "volume", "Name": "efc5758d9491150ad17a652e4d4f2f", "Source": "/var/lib/docker/volumes/efc5758d9491150ad17a652e4d4f2f", "Destination": "/data/db", "Driver": "Local", "Mode": "", "RW": true, "Propagation": ""}]
  
```

```

17 /bin/sh -c echo "deb [ DockerFile de l'image
18   E MongoDB4.0
19   /bin/sh -c set -x &&
20   /bin/sh -c mkdir -p /data/db
21 VOLUME [/data/db /data/configdb]
22 COPY file:ff519c7454e20e6f14c42932b8d6eaee066e1
23 ENTRYPOINT ["docker-entrypoint.sh"]
24 EXPOSE 27017
25 CMD ["mongod"]
  
```

Nous voyons que pour chacun des volumes montés, il y a un répertoire qui a été créé sur la machine hôte.

Si l'on supprime le container, tout les fichiers créés dans ce volume persisteront dans la machine hôte.

Nous avons vu comment utiliser l'option `-v CONTAINER_PATH` dans les chapitre précédent. Elle permet de créer un lien symbolique entre un dossier de la machine hôte vers un container.

Le Docker Daemon fournit une API pour manipuler les volumes. Voici les commandes de base :

```

PS C:\Users\baptiste> docker volume --help
Usage: docker volume COMMAND

Manage volumes

Commands:
  create      Create a volume
  inspect     Display detailed information on one or more volumes
  ls          List volumes
  prune       Remove all unused local volumes
  rm          Remove one or more volumes
  
```

Il est possible de créer, inspecter, lister, supprimer des volumes. Grâce à la commande `docker volume prune`, il est possible de supprimer les volumes qui ne sont plus utilisés afin de libérer de la place sur la machine hôte.

**Créons un volume nommé : db-data :**

```
docker volume create --name db-data
```

En listant nos volumes, nous retrouvons **db-data**, et nous voyons que c'est le driver local de Docker par défaut qui a été utilisé pour la création de ce volume.

```
PS C:\Users\baptiste> docker volume ls
DRIVER      VOLUME NAME
local        db-data
local        efc5758d9491150ad17a652e4d4f2f469146ef9b397f4189ad467d0fbe944bd2
local        f460ce00574a9379e86fcfd6441442a6e0cd2b6bdc08a1d0900a737c0ce978cde
```

Lorsque nous consultons la liste des volumes disponibles sur notre machine hôte, nous comprenons facilement pourquoi il est intéressant de leur donner un nom. Sinon le nom sera généré automatiquement et sera difficilement exploitable.

Et si nous inspectons ce volume :

```
docker volume inspect db-data
```

```
PS C:\Users\baptiste> docker volume inspect db-data
[
  {
    "CreatedAt": "2022-03-10T14:50:20Z",
    "Driver": "local",
    "Labels": {},
    "Mountpoint": "/var/lib/docker/volumes/db-data/_data",
    "Name": "db-data",
    "Options": {},
    "Scope": "local"
  }
]
```

Nous constatons que le volume est bien monté, et que son emplacement est autogéré par le driver **local**.

Maintenant que notre volume est créé. Nous allons pouvoir facilement le monter dans un container grâce à son nom.

```
docker container run -d --name db -v db-data:/data/db mongo
```

## 5.2. Démo : Volume avec MongoDB

Nous allons illustrer la notion de volume dans cette partie.

Examinons les commandes à disposition pour gérer le cycle de vie des volumes :

```
PS C:\Users\baptiste> docker volume --help

Usage: docker volume COMMAND

Manage volumes

Commands:
  create      Create a volume
  inspect     Display detailed information on one or more volumes
  ls          List volumes
  prune      Remove all unused local volumes
  rm          Remove one or more volumes

Run 'docker volume COMMAND --help' for more information on a command.
PS C:\Users\baptiste> |
```

Listons les volumes existant avec la commande :

```
docker volume ls
```

Lançons un conteneur basé sur MongoDB

```
docker container run -d mongo
```

Puis listons de nouveau la liste des volumes :

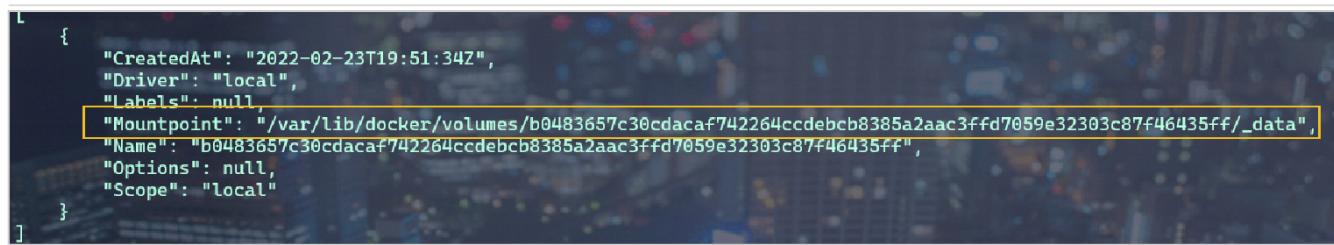
```
docker volume ls
```

```
PS C:\Users\baptiste> docker container run -d mongo
9ddbb45cae18ee3d430d9b316ef55b2864bd00d758af8b42d4fe7b4d0bbebde
PS C:\Users\baptiste> docker volume ls
DRIVER      VOLUME NAME
local      22d3830f7f483d13e7683b4d8555f506f7ebf3ca92c2ec0e392a3a14bca31ad8
local      6960cfe06cedea0dde3b0b8ab84e78fc5f6eeb4fa3263a4a7f61eb1a30f4b827
local      abd632c1f90b61fd96bd13bc3a4c395f776a429682a2a137c87016a39f87b60b
local      b0483657c30cdacaf742264ccdebc8385a2aac3ffd7059e32303c87f46435ff
PS C:\Users\baptiste> |
```

Récupérons un identifiant de volume et inspectons le :

```
docker inspect b0483657c30cdacaf742264ccdebc8385a2aac3ffd7059e32303c87f46435ff
```

La clé **Mountpoint** nous indique le répertoire dans lequel est stocké le volume sur la machine hôte, c'est-à-dire l'ensemble des bases, des collections de MongoDB par exemple.



```
[{"CreatedAt": "2022-02-23T19:51:34Z", "Driver": "local", "Labels": null, "Mountpoint": "/var/lib/docker/volumes/b0483657c30cdacaf742264ccdebcb8385a2aac3ffd7059e32303c87f46435ff/_data", "Name": "b0483657c30cdacaf742264ccdebcb8385a2aac3ffd7059e32303c87f46435ff", "Options": null, "Scope": "local"}]
```



Les données sont toujours présentes dans la machine hôte même si le conteneur est supprimé. Car le volume est stocké dans la machine hôte.

Si l'on regarde le contenu du **Dockerfile** de MongoDB ( voir Docker Hub), nous constatons que deux volumes sont créés.



```
10 /bin/sh -c set -x &&
11
12 VOLUME [ /data/db /data/configdb ]
13
14 ENV HOME=/data/db
```

- Comment créer nos propres volumes ?

```
docker container run -d --name mongo -v <data>:/data/db mongo
```

On peut alors monter un conteneur Mongo avec des données existantes. Ainsi, les deux volumes par default ne seront pas créé lors du montage du conteneur.

L'intérêt de créer des volumes est de pouvoir s'interfacer avec des solutions de stockage qui existent.



Par défaut, on utilise un driver "local" sur la machine hôte. Mais l'on peut utiliser un autre driver qui pourrait nous permettre de créer un volume sur des stockages distribués ou différentes solutions.

## 5.3. Exercice : Utilisation des volumes

Nous allons illustrer la notion de volume. Nous verrons notamment comment définir un volume:

- Dans un Dockerfile
- Au lancement d'un conteneur en utilisant l'option **-v**
- En utilisant la ligne de commande

### 5.3.1. Prérequis

- Installation de **jq**

Pour certaines commandes vous aurez besoin de l'utilitaire **jq** qui permet de manipuler des

structures json très facilement. Vous pouvez l'installer depuis <https://stedolan.github.io/jq/download/>

- Si vous utilisez Docker for Mac ou Docker for Windows

la plateforme Docker est installée dans une machine virtuelle tournant sur un hyperviseur léger (*xhyve* pour macOS, *Hyper-V* pour Windows). Pour effectuer cet exercice il vous faudra utiliser la commande suivante pour accéder à un **shell** dans cette machine virtuelle.

```
$ docker run -it --privileged --pid=host debian nsenter -t 1 -m -u -n -i sh
```

Comme nous l'avons évoqué dans le cours, cette commande permet de lancer un shell dans un conteneur basé sur `debian`, et faire en sorte d'utiliser les namespaces de la machine hôte (la machine virtuelle) sur laquelle tourne le daemon Docker.

Une fois que vous avez lancé ce conteneur, vous pourrez naviguer dans le *filesystem* de la machine sur laquelle tourne le daemon Docker, c'est-à-dire l'endroit où les images sont stockées.

### 5.3.2. Persistance des données dans un conteneur



Nous allons illustrer pourquoi, par défaut, un conteneur ne doit pas être utilisé pour persister des données.

En utilisant la commande suivante, lancez un shell interactif dans un conteneur basé sur l'image `alpine:3.8`, et nommé le `c1`.

```
docker container run --name c1 -ti alpine:3.8 sh
```

Dans ce conteneur, créez le répertoire `/data` et dans celui-ci le fichier `hello.txt`.

```
mkdir /data && touch /data/hello.txt
```

Sortez ensuite du conteneur.

```
exit
```

Lors de la création du container, une **layer read-write** est ajoutée au-dessus des layers **read-only** de l'image sous-adjacente.

C'est dans cette **layer** que les changements que nous avons apportés dans le container ont été persistés (création du fichier `/data/hello.txt`).

Nous allons voir comment cette **layer** est accessible depuis la machine hôte (celle sur laquelle tourne le daemon Docker) et vérifier que nos modifications sont bien présentes. Utilisez la command **inspect** pour obtenir le path de la layer du container `c1`.

La clé qui nous intéresse est **GraphDriver**.

```
docker container inspect c1
```

Nous pouvons scroller dans l'output de la commande suivante jusqu'à la clé **GraphDriver** ou bien nous pouvons utiliser le format **Go templates** et obtenir directement le contenu de la clé.

Lancez la commande suivante pour n'obtenir que le contenu de **GraphDriver**.

```
docker container inspect -f "{{ json .GraphDriver }}" c1 | jq .
```

Vous devriez obtenir un résultat proche de celui ci-dessous.

```
{
  "Data": {
    "LowerDir": "/var/lib/docker/overlay2/d0ffe7...1d66-
init/diff:/var/lib/docker/overlay2/acba19...b584/diff",
    "MergedDir": "/var/lib/docker/overlay2/d0ffe7...1d66/merged",
    "UpperDir": "/var/lib/docker/overlay2/d0ffe7...1d66/diff",
    "WorkDir": "/var/lib/docker/overlay2/d0ffe7...1d66/work"
  },
  "Name": "overlay2"
}
```

Avec la commande suivante, vérifiez que le fichier **hello.txt** se trouve dans le répertoire référencé par **UpperDir**.

```
COUNTAINER_LAYER_PATH=$(docker container inspect -f "{{ json .GraphDriver.Data.UpperDir }}"
} c1 | tr -d '')
```

```
find $COUNTAINER_LAYER_PATH -name hello.txt
/var/lib/docker/overlay2/d0ffe7...1d66/diff/data/hello.txt
```

Supprimez le container **c1** et vérifiez que le répertoire spécifié par **UpperDir** n'existe plus.

```
docker container rm c1
```

```
ls $COUNTAINER_LAYER_PATH
```

```
ls: cannot access '/var/lib/docker/overlay2/d0ffe7...1d66/diff': No such file or
directory
```

Cela montre que les données créées dans le conteneur ne sont pas persistées et sont supprimées avec lui.

### 5.3.3. Définition d'un volume dans un Dockerfile

Nous allons maintenant voir comment les volumes sont utilisés pour permettre de remédier à ce problème et permettre de persister des données en dehors d'un container.

Nous allons commencer par créer un Dockerfile basé sur l'image alpine et définir /data en tant que volume. Tous les éléments créés dans /data seront persistés en dehors de l'union filesystem comme nous allons le voir.

Créez le fichier *Dockerfile* contenant les 2 instructions suivantes:

```
FROM alpine:3.8
VOLUME ["/data"]
```

Construisez l'image *imgvol* à partir de ce Dockerfile.

```
$ docker image build -t imgvol .
Sending build context to Docker daemon 2.048kB
Step 1/2 : FROM alpine:3.8
 --> 3f53bb00af94
Step 2/2 : VOLUME ["/data"]
 --> Running in 7ee2310fca60
Removing intermediate container 7ee2310fca60
 --> d8f6d5332181
Successfully built d8f6d5332181
Successfully tagged imgvol:latest
```

Avec la commande suivante, lancez un shell interactif dans un container, nommé *c2*, basé sur l'image *imgvol*.

```
$ docker container run --name c2 -ti imgvol
```

Depuis le container, créez le fichier */data/hello.txt*

```
# touch /data/hello.txt
```

Sortons ensuite du container avec la commande **CTRL-P** suivie de **CTRL-Q**, cette commande permet de passer le process en tache de fond, elle n'arrête pas le container. Pour être sur que *c2* tourne, il doit apparaître dans la liste des containers en execution. Vérifiez le avec la commande suivante:

```
$ docker container ls
```

Utilisez la commande *inspect* pour récupérer la clé **Mounts** afin d'avoir le chemin d'accès du volume sur la machine hôte.

```
$ docker container inspect -f "{{ json .Mounts }}" c2 | jq .
```

Vous devriez obtenir un résultat similaire à celui ci-dessous (aux ID prêts).

```
[  
 {  
   "Type": "volume",  
   "Name": "d071337...3896",  
   "Source": "/var/lib/docker/volumes/d071337...3896/_data",  
   "Destination": "/data",  
   "Driver": "local",  
   "Mode": "",  
   "RW": true,  
   "Propagation": ""  
 }  
]
```

Le volume */data* est accessible, sur la machine hôte, dans le path spécifié par la clé **Source**.

Avec la commande suivante, vérifiez que le fichier *hello.txt* est bien présent sur la machine hôte.

```
VOLUME_PATH=$(docker container inspect -f "{{ (index .Mounts 0).Source }}" c2)
```

```
find $VOLUME_PATH -name hello.txt  
/var/lib/docker/volumes/cb5...f49/_data/hello.txt
```

Supprimez maintenant le container *c2*.

```
docker container stop c2 && docker container rm c2
```

Vérifier que le fichier *hello.txt* existe toujours sur le filesystem de l'hôte.

```
$ find $VOLUME_PATH -name hello.txt  
/var/lib/docker/volumes/cb5...f49/_data/hello.txt
```

Cet exemple nous montre qu'un volume permet de persister les données en dehors de l'union filesystem et ceci indépendamment du cycle de vie d'un container.

### 5.3.4. Définition d'un volume au lancement d'un container

Précédemment nous avons défini un volume dans le *Dockerfile*, nous allons maintenant voir comment définir des volumes à l'aide de l'option **-v** au lancement d'un container.

Lancez un container avec les caractéristiques suivantes:

- basé sur l'image *alpine:3.8* - nommé *c3* - exécution en background (option **-d**)
- définition de */data* en tant que volume (option **-v**) - spécification d'une commande qui écrit dans le volume ci-dessus.

Pour ce faire, lancez la commande suivante:

```
docker container run --name c3 -d -v /data alpine sh -c 'ping 8.8.8.8 > /data/ping.txt'
```

Inspectez le container et repérez notamment le chemin d'accès du volume sur la machine hôte.

```
docker inspect -f "{{ json .Mounts }}" c3 | jq .  
[  
  {  
    "Type": "volume",  
    "Name": "2ba36b...3ef2",  
    "Source": "/var/lib/docker/volumes/2ba36b...3ef2/_data",  
    "Destination": "/data",  
    "Driver": "local",  
    "Mode": "",  
    "RW": true,  
    "Propagation": ""  
  }  
]
```

Le volume est accessible via le filesystem de la machine hôte dans le path spécifié par la clé **Source**.

En utilisant la commande suivante, vérifiez ce que ce répertoire contient.

```
VOLUME_PATH=$(docker container inspect -f "{{ (index .Mounts 0).Source }}" c3)
```

```
tail -f $VOLUME_PATH/ping.txt
```

```
64 bytes from 8.8.8.8: seq=34 ttl=37 time=0.462 ms  
64 bytes from 8.8.8.8: seq=35 ttl=37 time=0.436 ms  
64 bytes from 8.8.8.8: seq=36 ttl=37 time=0.512 ms  
64 bytes from 8.8.8.8: seq=37 ttl=37 time=0.487 ms  
64 bytes from 8.8.8.8: seq=38 ttl=37 time=0.409 ms
```

```
64 bytes from 8.8.8.8: seq=39 ttl=37 time=0.438 ms
64 bytes from 8.8.8.8: seq=40 ttl=37 time=0.477 ms
```

Le fichier *ping.txt* est mis à jour régulièrement par la commande ping qui tourne dans le container.

Si nous stoppons et supprimons le container, le fichier *ping.txt* sera toujours disponible via le volume, cependant il ne sera plus mis à jour.

Supprimez le container *c3* avec la commande suivante.

```
$ docker container rm -f c3
```

### 5.3.5. Utilisation des volumes via la CLI



Les commandes relatives aux volumes ont été introduites dans Docker 1.9.

Elles permettent de manager le cycle de vie des volumes de manière très simple.

La commande suivante liste l'ensemble des sous-commandes disponibles.

```
docker volume --help
```

La commande *create* permet de créer un nouveau volume. Créez un volume nommé *html* avec la commande suivante.

```
docker volume create --name html
```

Lister les volumes existants et vérifiez que le volume *html* est présent.

```
docker volume ls
```

DRIVER	VOLUME NAME
local	html

Comme pour les containers et les images (et d'autres primitives Docker), la commande *inspect* permet d'avoir la vue détaillée d'un volume. Inspectez le volume *html*

```
$ docker volume inspect html
[
  {
    "Driver": "local",
    "Labels": {},
    "Mountpoint": "/var/lib/docker/volumes/html/_data",
```

```
        "Name": "html",
        "Options": {},
        "Scope": "local"
    }
]
```

La clé **Mountpoint** définie ici correspond au chemin d'accès de ce volume sur la machine hôte. Lorsque l'on crée un volume via la CLI, le path contient le nom du volume et non pas un identifiant comme nous l'avons vu plus haut.

Utilisez la commande suivante pour lancer un container basé sur *nginx* et monter le volume *html* sur le point de montage */usr/share/nginx/html* du container. Cette commande publie également le port **80** du container sur le port **8080** de l'hôte.



*/usr/share/nginx/html* est le répertoire servi par défaut par *nginx*, il contient les fichiers *index.html* et *50x.html*.

```
docker run --name www -d -p 8080:80 -v html:/usr/share/nginx/html nginx:1.16
```

Depuis l'hôte, regardez le contenu du volume *html*.

```
$ ls -al /var/lib/docker/volumes/html/_data
total 16
drwxr-xr-x 2 root root 4096 Jan 10 17:07 .
drwxr-xr-x 3 root root 4096 Jan 10 17:07 ..
-rw-r--r-- 1 root root 494 Dec 25 09:56 50x.html
-rw-r--r-- 1 root root 612 Dec 25 09:56 index.html
```

Le contenu du répertoire */usr/share/nginx/html* du container a été copié dans le répertoire **/var/lib/docker/volumes/html/\_data** de l'hôte.

Accédez à la page d'accueil en lançant un *curl* sur <http://localhost:8080>

```
$ curl localhost:8080
```

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
}
```

```
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Depuis l'hôte, nous pouvons modifier le fichier *index.html*.

```
cat<<END >/var/lib/docker/volumes/html/_data/index.html
HELLO !!!
END
```

Utilisez une nouvelle fois la commande *curl* pour vérifier que le container sert le fichier *index.html* modifié.

```
curl localhost:8080
HELLO !!!
```

## 5.4. Drivers de volumes

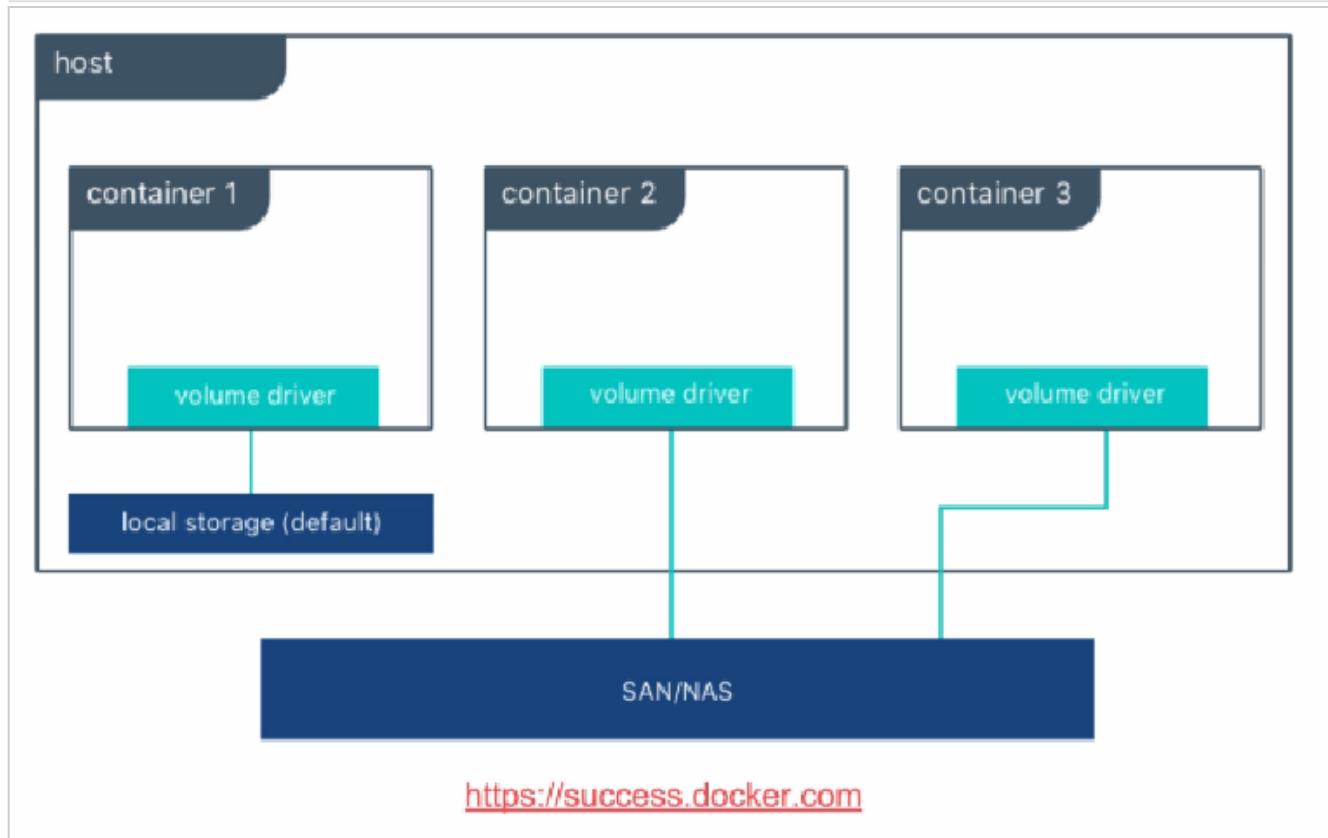
Un driver de volume permet de persister des données au travers différentes solutions de stockage.

Par défaut, le driver est **local** et si on monte un volume avec ce driver, les données seront stockées dans un répertoire dédié sur la machine hôte :

```
/var/lib/docker/volume/<ID DU VOLUME>
```

Mais l'on peut ajouter des drivers de volume supplémentaire par l'intermédiaire de plugin pour utiliser AWS, AZURE ...Etc

Ce schéma illustre 3 conteneurs utilisant des drivers de stockage différent sur la même machine hôte.



### Exemple : Plugin `sshfs`

- Stockage sur un système de fichier via ssh.

<https://github.com/vieux/docker-volume-sshfs>

```
# Installation du plugin
$ docker plugin install vieux/sshfs
Plugin "vieux/sshfs" is requesting the following privileges:
- network: [host]
- mount: [/var/lib/docker/plugins/]
- mount: []
- device: [/dev/fuse]
- capabilities: [CAP_SYS_ADMIN]
Do you grant the above permissions? [y/N] y
latest: Pulling from vieux/sshfs
52d435ada6a4: Download complete
Digest: sha256:1d3c3e42c12138da5ef7873b97f7f32cf99fb6edde75fa4f0bcf9ed277855811
Status: Downloaded newer image for vieux/sshfs:latest
Installed plugin vieux/sshfs
```

} téléchargement depuis le Docker Hub

Une fois que le plugin est installé :

- Création du répertoire sur le serveur ssh

```
ssh USER@HOST mkdir /tmp/data
```

- Création du volume avec le driver `vieux/sshfs`

```
docker volume create -d vieux/sshfs -o sshcmd=USER@HOST:/tmp/data -o password=PASSWORD
data
```

- Liste des volumes

```
docker volume ls
```

- Utilisation du volume dans un conteneur.

```
docker run -it -v data:/data alpine
# touch /data/test
```

- Vérification sur le serveur SSH

```
ssh USER@HOST ls /tmp/data
```

### 5.4.1. Démo : Plugin de volume

Nous allons installer un plugin de volume et l'utiliser dans un conteneur pour faire de la persistance de données.

Dans DockerHub, nous allons rechercher "un volume".

Le plugin `vieux/sshfs` permet de créer un volume dans un dossier distant à travers une connexion ssh.

<https://hub.docker.com/r/vieux/sshfs>

Préparation d'une machine distante avec une connexion SSH

#### 5.4.1.1. Installation et configuration de OPENSSH SERVER sur Windows 10.

##### 5.4.1.1.1. Installation

The screenshot shows the Windows Settings interface under the 'Applications et fonctionnalités' section. A modal window titled 'Ajouter une fonctionnalité facultative' is open, showing the 'Serveur OpenSSH' feature with a checked checkbox. The background shows a list of installed optional features.

Les deux composants **OpenSSH** peuvent être installés à l'aide des Paramètres Windows sur les appareils Windows Server 2019 et Windows 10.

Pour installer les composants OpenSSH :

Ouvrez Paramètres, sélectionnez **Applications > Applications et fonctionnalités**, puis **Fonctionnalités facultatives**.

Parcourez la liste pour voir si OpenSSH est déjà installé. Si ce n'est pas le cas, sélectionnez Ajouter une fonctionnalité en haut de la page, puis :

- Recherchez **OpenSSH Client** et cliquez sur Installer.
- Recherchez **OpenSSH Server** et cliquez sur Installer.

Une fois l'installation terminée, revenez à **Applications > Applications et fonctionnalités** et **Fonctionnalités facultatives**.

Vous devriez voir **OpenSSH** dans la liste.

#### 5.4.1.1.2. Démarrer et configurer OpenSSH Server

Pour démarrer et configurer **OpenSSH Server** pour une première utilisation, ouvrez **PowerShell en tant qu'administrateur**, puis exécutez les commandes suivantes pour démarrer **sshd service** :

```
# Start the sshd service
Start-Service sshd

# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'
```

```
# Confirm the Firewall rule is configured. It should be created automatically by
setup. Run the following to verify
if !(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue
| Select-Object Name, Enabled) {
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist, creating
it..."
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName 'OpenSSH Server
(sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and exists."
}
```

#### 5.4.1.1.3. Se connecter à OpenSSH Server

Une fois l'installation terminée, vous pouvez vous connecter à OpenSSH Server à partir d'un appareil Windows 10 ou Windows Server 2019 avec OpenSSH Client installé à l'aide de PowerShell, comme suit. Veillez à exécuter PowerShell en tant qu'administrateur :

```
ssh <login windows>@<server name>
```

Une fois connecté, vous recevez un message semblable à celui-ci :

```
The authenticity of host 'servername (10.00.00.001)' can't be established.
ECDSA key fingerprint is SHA256:<a large string>.
Are you sure you want to continue connecting (yes/no)?
```

Si vous sélectionnez Oui, ce serveur est ajouté à la liste des hôtes SSH connus sur votre client Windows.

Vous êtes alors invité à entrer le mot de passe. Par mesure de sécurité, votre mot de passe n'est pas affiché lorsque vous l'entrez.

Une fois connecté, vous voyez l'invite de l'interpréteur de commandes Windows :

```
domain\username@SERVERNAME C:\Users\username>
```



Créez un dossier **data** sur votre serveur SSH/

#### 5.4.1.1.4. Installation du plugin et du volume sur la machine hôte:

- Installation du plugin

```
docker plugin install vieux/sshfs # or docker plugin install vieux/sshfs DEBUG=1
```

Pour lister les plugins installés sur la machine :

```
docker plugin ls
```

- Création du volume

```
docker volume create -d vieux/sshfs -o sshcmd=<user>@<host>:<path du volume> -o  
password=<password> data
```

```
docker container run -ti -v data:/data alpine
```

```
# touch /data/hello.txt
```

Nous constatons que le fichier a bien été créé coté serveur SSH.



Il existe d'autres drivers à disposition !

## 6. Docker Machine

En cours de rédaction ...

## 7. Docker Compose

Docker Compose permet de gérer des applications complexes, c'est-à-dire par exemple des applications qui dialoguent les unes avec les autres. Très simplement nous pouvons utiliser **Docker Compose** : Grâce à une configuration sous forme de fichier **YAML** dont le nom par défaut est `docker-compose.yml` par défaut.

### 7.1. Structure du fichier `docker.compose.yml`

Dans ce fichier nous définirons l'ensemble des éléments d'une application :

- Les services.
- Les volumes.
- Les Networks qui permettent d'isoler les services.
- Les secrets (donnés sensibles nécessaires au fonctionnement de l'application, pris en compte seulement dans un cluster Swarm).
- Les configs (configuration sensibles nécessaires au fonctionnement de l'application, pris en compte seulement dans un cluster Swarm).

Examinons maintenant une application web branchée à une API configurée dans le fichier `docker-compose.yml` :

```
version: '3.9'
volumes:
  data:
networks:
  frontend:
  backend:
services:
  web:
    images: org/web:2.3
    networks:
      - frontend
    ports:
      - 80:80
  api:
    image: org/api
    networks:
      - backend
      - frontend
  db:
    image: mongo
    volumes:
      - data:/data/db
    networks:
      - backend
```

Analysons les principales clés de notre fichier :

- **Version** correspond à la version du format **Compose** à mettre en relation avec la version du **Docker Daemon** de la machine hôte qui va être utilisée pour déployer notre application. Si on utilise la dernière version de **compose** avec un Daemon plus ancien, il y a certaines options écrites dans le `docker-compose.yml` qui ne seront pas prises en compte.
- **Volumes** permet de définir un volume, que l'on appelle ici, **data** et qui sera utilisé dans un service par la suite. Par défaut, ce volume utilise le driver local, qui va donc créer un répertoire sur la machine hôte.
- **Networks** permet de créer des réseaux qui serviront à isoler des groupes de services.
- **Services** contient la définition des services nécessaires au fonctionnement de notre application. Ici, nous avons nos 3 services : **WEB**, **API**, **DB**.

Pour chaque service on spécifie l'image utilisée, les volumes pour la persistance des données. Le service **DB** est le seul à persister les données et montera le volume **data** dans le répertoire `/data/db` du container qui sera lancé.

Pour chaque service, on définit aussi les réseaux attachés avec la clé **Networks**. Dans notre exemple : le service **API** doit pouvoir communiquer avec le service **WEB** et **DB**. Donc, il faut lui donner accès aux deux réseaux attachés à ces services : **backend** et **frontend**.

En isolant ainsi les services, on s'assure qu'ils ne puissent pas avoir accès à des services dont ils n'ont pas l'utilité directement. Comme le service **WEB**, qui ne doit pas pouvoir accéder au service **DB** directement. Cela ajoute un niveau de sécurité au cas où l'un des services serait compromis.

La clé **ports** publie les ports nommés vers l'extérieur pour le service qui a besoin d'être joint, comme le serveur **Web** et son port 80.

De nombreuses options sont encore disponibles pour la définition d'un service dans le format **compose**.

Voici une liste des plus utilisées :

- Image utilisée par le container du service.
- Nombre de répliques, c'est à dire le nombre de container identique qui sera lancé pour le service. En augmentant le nombre de container, on pourra traiter les piques de charge par exemple.
- Les ports publiés à l'extérieur par les services qui ont besoin d'être accessible par l'extérieur.
- La définition d'un Health check pour vérifier l'état de santé d'un service.
- Les stratégies de redémarrage de façon à définir que faire si un container a planté par exemple.
- Contraintes de déploiement (dans un contexte de SWARM uniquement), par exemple pour imposer qu'un container doit tourner sur une machine contenant un disque SSD.
- Contraintes des mises à jour (dans un contexte de SWARM uniquement).

Un des avantages qu'il y a à déployer une application à travers le fichier `docker-compose.yml`, c'est qu'elle peut être déployé sur n'importe quel environnement. En utilisant le binaire **compose**, un développeur peut installer sur une machine son application, avec son environnement de

## 7.2. Le binaire docker-compose

Le binaire **docker-compose** est utilisé pour gérer une application qui est gérée selon le format **docker-compose.yml**. Cet outil est indépendant du **docker daemon** qui est souvent livré en même temps (Docker for Mac, Docker for Windows).

```
docker-compose [-f <arg>...] [options] [COMMAND] [ARGS...]
```

Il y a plusieurs éléments qui peuvent être fournis au binaire :

- Le chemin d'accès aux fichiers dans lesquels est définie l'application. ( Par défaut il s'agit du fichier : **docker-compose.yml** du répertoire courant)
- Des options, comme des chemins d'accès à des certificats et clés TLS ou l'adresse de l'hôte à contacter.
- Une commande pour gérer l'application.
- Des arguments pour cette commande.

On peut avoir plusieurs fichiers pour spécifier une configuration différente par environnement de développement.

Commande	Utilisation
up / down	Création / Suppression d'une application (services, volumes, réseaux)
start / stop	Démarrage / arrêt d'une application
build	Build des images des services (si instruction build utilisée)
pull	Téléchargement d'une image
logs	Visualisation des logs de l'application
scale	Modification du nombre de container pour un service
ps	Liste les containers de l'application

## 7.3. Service discovery

Une application définie par **docker-compose** est en général constituée de plusieurs services dont certains communiquent avec d'autres. Nous sommes souvent dans un environnement **microservice**.

Pour permettre la résolution du service, le **dns** intégré dans le **docker daemon** est utilisé. Ainsi nous pouvons résoudre l'IP d'un service à partir de son nom.

Voyons un exemple :

```
version: '3'  
services:  
  db:  
    image: mongo:3.4  
    volumes:  
      - data:/data/db  
    restart: always  
  api:  
    image: org/api:1.2  
    restart: always  
    volumes:  
      data:
```

Extrait d'un fichier docker-compose.yml

Le service **api** utilise le service de base de données par son nom

```
// Mongodb connection string  
url = 'mongodb://db/todos';  
  
// Connection to database  
MongoClient.connect(url, (err, conn) => {  
  if(err){  
    return callback(err);  
  } else {  
    return callback(null, conn);  
  }  
});
```

Extrait d'un code Node.js: connexion à la base de données

Sur la gauche, nous avons un extrait d'une application **docker-compose** composée de deux services.

Un service est utilisé pour la base de données, **db** et un pour l'`**api**` qui utilise ce service **db**`.

Nous voyons aussi qu'il y a un volume qui se nomme **data** et qui est monté dans le service **db**.

À droite, nous avons une partie du code **nodeJs** de l'**api** qui montre comment la connexion à la base de données est réalisée. Il suffit juste de donner le nom du service de base de données dans la chaîne de connexion.

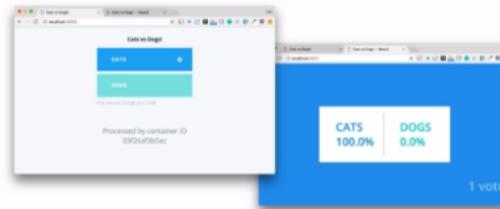
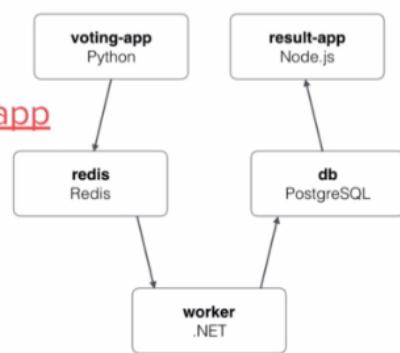
C'est quelque chose de très pratique. Toutefois, il faudra ajouter un mécanisme qui permette d'attendre que la **db** soit disponible ou éventuellement renouveler la tentative de connexion.

**Docker-compose** permet d'indiquer les dépendances entre les services, mais il ne permet pas de savoir qu'un service est disponible avant de lancer un service qui en dépend.

## 7.4. Mise en œuvre d'une application microservice : Voting App.

# Voting App

- <https://github.com/dockersamples/example-voting-app>
- Application Open Source maintenue par Docker
- Utilisée pour des démos / présentations
- 5 services
  - différents langages
    - Node.js / Python / .NET
  - différentes bases de données
    - Redis / Postgres



L'application **Voting App** est développée et maintenue par **Docker**. Elle est beaucoup utilisée pour des présentations ou des démos. Nous pouvons la récupérer en local en clonant [le répository GitHub](#).

C'est une application très pratique pour illustrer le concept de microservices.

Elle est composée de :

- 5 services :
  - 2 bases de données : **redis** et **postgres**
  - 3 services développés chacun dans un environnement différent : **Python**, **NodeJs** et **.NET**

Un utilisateur **vote** depuis l'interface web, par défaut l'utilisateur doit choisir entre "cat" et "dog". Le vote est stocké dans la base de données **Redis**.

Le service **Worker**, va récupérer le vote depuis **Redis** et va l'enregistrer dans la base de données **PostGres** et les utilisateurs pourront consulter les résultats via l'interface **Web** fournie par le service **Result**.

Si nous visitons le dépôt **GitHub** de l'application, nous constatons qu'il existe plusieurs fichiers **docker-compose** qui illustrent différente utilisation de l'application :

Pour la production, on aura le fichier **docker-stack** alors que pour le développement nous aurons plutôt **docker-compose**. Il est possible de choisir différents langages comme **java** ou **.NET** pour le **worker**. Ainsi que différents **OS** : **Linux** ou **Windows**.

docker-compose-javaworker.yml	Set an explicit username/password for Postgres in the other Compose f...	2 years ago
docker-compose-k8s.yml	Version Was invalid, Fix to Version3 docker-compose	17 months ago
docker-compose-simple.yml	Set an explicit username/password for Postgres in the other Compose f...	2 years ago
docker-compose-windows-1809.yml	Update images for Windows 1809	3 years ago
docker-compose-windows.yml	Pin to Nano Server SAC 2016 images	4 years ago
docker-compose.seed.yml	adding data seeding	14 months ago
docker-compose.yml	healthchecks! move to compose spec version!	14 months ago
docker-stack-simple.yml	Set an explicit username/password for Postgres in the swarm and k8s f...	2 years ago
docker-stack-windows-1809.yml	Add Windows 1809 support	4 years ago
docker-stack-windows.yml	Pin to Nano Server SAC 2016 images	4 years ago
docker-stack.yml	Set an explicit username/password for Postgres in the swarm and k8s f...	2 years ago

Ouvrons le fichier `docker-compose-simple.yml`

```
version: "3"

services:
  vote:
    build: ./vote
    command: python app.py
    volumes:
      - ./vote:/app
    ports:
      - "5000:80"

  redis:
    image: redis:alpine
    ports: ["6379"]

  worker:
    build: ./worker

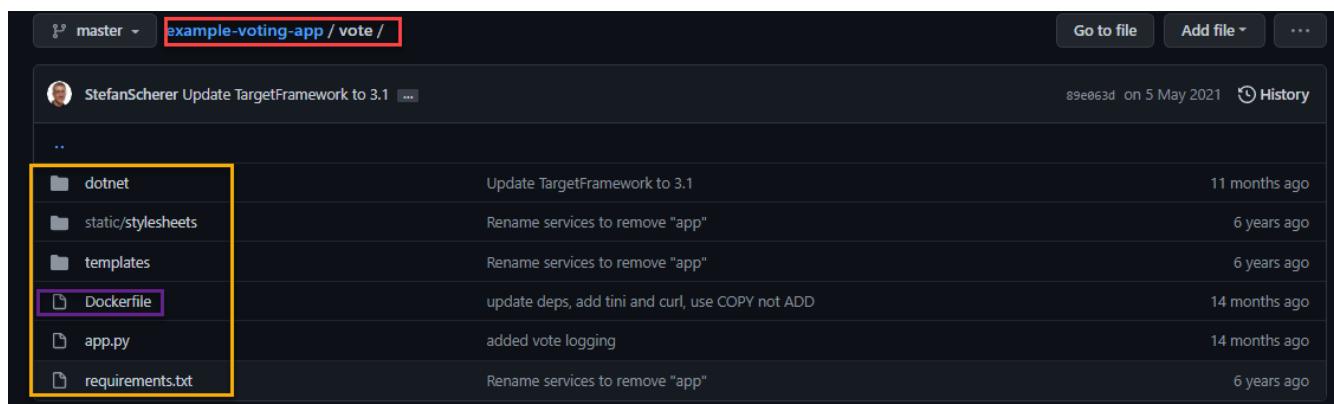
  db:
    image: postgres:9.4
    environment:
      POSTGRES_USER: "postgres"
      POSTGRES_PASSWORD: "postgres"

  result:
    build: ./result
    command: nodemon server.js
    volumes:
      - ./result:/app
    ports:
      - "5001:80"
```

```
- "5858:5858"
```

L'instruction **build** sert à définir l'emplacement du contexte de construction du service : le **dockerfile** ainsi que les autres fichiers nécessaires à la construction de l'image.

Pour le service **vote**, nous voyons que nous avons bien les fichiers de l'application et le **Dockerfile** dans le dossier **vote**.



A screenshot of a GitHub repository interface. The repository name is 'example-voting-app / vote /'. The 'Dockerfile' file is highlighted with a yellow box. The commit history shows several commits from 'StefanScherer':

- Update TargetFramework to 3.1 (11 months ago)
- Rename services to remove "app" (6 years ago)
- Rename services to remove "app" (6 years ago)
- update deps, add tini and curl, use COPY not ADD (14 months ago)
- added vote logging (14 months ago)
- Rename services to remove "app" (6 years ago)

Pour les services **vote** et **result**, nous définissons dans l'instruction **volume** le **bindmount** du code applicatif depuis la machine hôte vers le répertoire **/app** dans le container. Cela permet de rendre le code source présent sur la machine de développement directement accessible dans le container.

Et une approche qui est souvent utilisée avec **Docker-compose** en développement est de redéfinir la commande qui est normalement lancée dans le container.

On utilise pour cela le mot clé **command** comme nous pouvons le voir dans les services **vote** et **result**.

Par contre si nous ouvrons le fichier **docker-stack.yml**, nous avons une définition de l'application prête à être déployé sur un cluster **Swarm** de production.

```
version: "3"
services:

  redis:
    image: redis:alpine
    networks:
      - frontend
    deploy:
      replicas: 1
      update_config:
        parallelism: 2
        delay: 10s
      restart_policy:
        condition: on-failure
  db:
    image: postgres:9.4
    environment:
      POSTGRES_USER: "postgres"
      POSTGRES_PASSWORD: "postgres"
```

```
volumes:
  - db-data:/var/lib/postgresql/data
networks:
  - backend
deploy:
  placement:
    constraints: [node.role == manager]
vote:
  image: dockersamples/examplevotingapp_vote:before
  ports:
    - 5000:80
  networks:
    - frontend
  depends_on:
    - redis
  deploy:
    replicas: 2
    update_config:
      parallelism: 2
    restart_policy:
      condition: on-failure
result:
  image: dockersamples/examplevotingapp_result:before
  ports:
    - 5001:80
  networks:
    - backend
  depends_on:
    - db
  deploy:
    replicas: 1
    update_config:
      parallelism: 2
      delay: 10s
    restart_policy:
      condition: on-failure

worker:
  image: dockersamples/examplevotingapp_worker
  networks:
    - frontend
    - backend
  depends_on:
    - db
    - redis
  deploy:
    mode: replicated
    replicas: 1
    labels: [APP=VOTING]
    restart_policy:
      condition: on-failure
```

```
delay: 10s
max_attempts: 3
window: 120s
placement:
  constraints: [node.role == manager]

visualizer:
  image: dockersamples/visualizer:stable
  ports:
    - "8080:8080"
  stop_grace_period: 1m30s
  volumes:
    - "/var/run/docker.sock:/var/run/docker.sock"
deploy:
  placement:
    constraints: [node.role == manager]

networks:
  frontend:
  backend:

volumes:
  db-data:
```

Si l'on regarde dans le service **vote** par exemple. On peut voir que contrairement au fichier [docker-compose-simple](#), nous n'avons pas l'instruction **build** mais **image**. Ce qui est logique puisqu'en production nous déployons les images des services et non pas les codes applicatifs dans les containers.

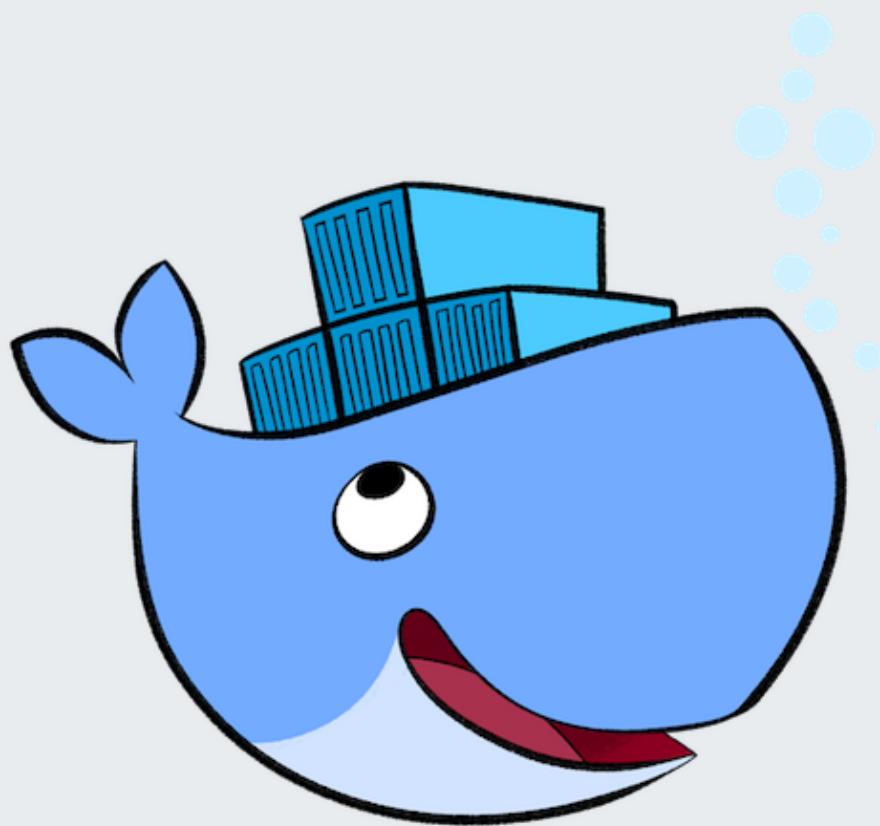
Nous trouvons également l'instruction **deploy** qui permet de spécifier un ensemble de propriétés dans le cadre d'un déploiement sur un cluster **Swarm** comme le nombre de **replicas**, c'est-à-dire le nombre de container identique qui seront lancés par le service.

Des contraintes de **placement**, qui indique le type de machine du cluster sur lequel le service sera déployé. On peut également spécifier des conditions de redémarrage, **restart\_policy** ou la façon dont la mise à jour d'un service sera effectuée avec **update\_config**. Par exemple, si un service a deux replicas, on peut vouloir mettre à jour le premier, se donner quelques secondes pour être certain qu'il fonctionne correctement avant de faire la mise à jour du second. C'est le mécanisme de **rolling update** que l'on verra dans le chapitre sur **Swarm**.

Dans un contexte de production, on s'assurera également d'isoler des groupes de services par l'intermédiaire de **networks**. Ici, tout en bas du fichier nous voyons que deux **networks** sont définis : **frontend** et **backend**.

## 7.5. Voting App Installation sur Play Docker.

Nous allons installer l'application dans un environnement temporaire dans un premier temps : [Play With Docker](#)



# Play with Docker

A simple, interactive and fun playground to learn Docker

[Start](#)

Cela permet de créer une session Docker dans un environnement de test en ligne.

Cliquez sur : **Add New Instance**



Clonez le dépôt git : <https://github.com/dockersamples/example-voting-app.git>

```
git clone https://github.com/dockersamples/example-voting-app.git
```

```
#####
#           WARNING!!!!
# This is a sandbox environment. Using personal credentials
# is HIGHLY! discouraged. Any consequences of doing so are
# completely the user's responsibilites.
#
# The PWD team.
#####
[node1] (local) root@192.168.0.8 ~
$ git clone https://github.com/dockersamples/example-voting-app.git
Cloning into 'example-voting-app'...
remote: Enumerating objects: 975, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 975 (delta 0), reused 0 (delta 0), pack-reused 971
Receiving objects: 100% (975/975), 992.51 KiB | 14.81 MiB/s, done.
Resolving deltas: 100% (355/355), done.
[node1] (local) root@192.168.0.8 ~
$ ls
example-voting-app
[node1] (local) root@192.168.0.8 ~
$ █
```

Naviguez dans le dossier example-voting-app.

```
cd example-voting-app
```

Et lançons maintenant l'application avec **Docker-compose**. Nous lui indiquons le nom du fichier avec l'option **-f**. Le paramètre **up** indique qu'il faut monter l'application et **-d** qu'il faut rendre la main de la console une fois monté.

```
docker-compose -f docker-compose-simple.yml up -d
```

```
$ docker-compose -f docker-compose-simple.yml up -d
Creating network "example-voting-app_default" with the default driver
Building vote
Step 1/8 : FROM python:3.9-slim
3.9-slim: Pulling from library/python
c229119241af: Pull complete
5a3ae98ea812: Pull complete
46d5c684ee5f: Extracting [=====] 10.62MB/11.58MB
fdb2b484fc86: Download complete
bbf0e1f27c8a: Download complete
```

Après le déploiement de l'application, il apparaît dans **Play with Docker** des boutons portant les numéros des ports des applications.

Si l'on regarde le contenu du fichier `docker-compose-simple`, nous lisons que :

Le service `vote` publie son port `80` sur le port `5000` de la machine hôte. Et que le service `result` publie son port `80` sur le port `5001` de la machine hôte.

The screenshot shows a container named 'c9709tk3\_c970bmp4lkkg00a13eeg'. It displays various metrics: IP (192.168.0.8), Memory (48.15% / 3.906GiB), and CPU (3.69%). It features an 'OPEN PORT' button and four ports listed: 5001 (circled in red), 5858, 49153, and 5000 (also circled in red). Below these are SSH and DELETE/EVENTOR buttons. A terminal window at the bottom shows command-line activity related to node.js and npm.

Si l'on clique dessus, nous pourrons avoir accès aux applications ciblées :

Service de vote :



Résultats des votes :



Essayez en local !

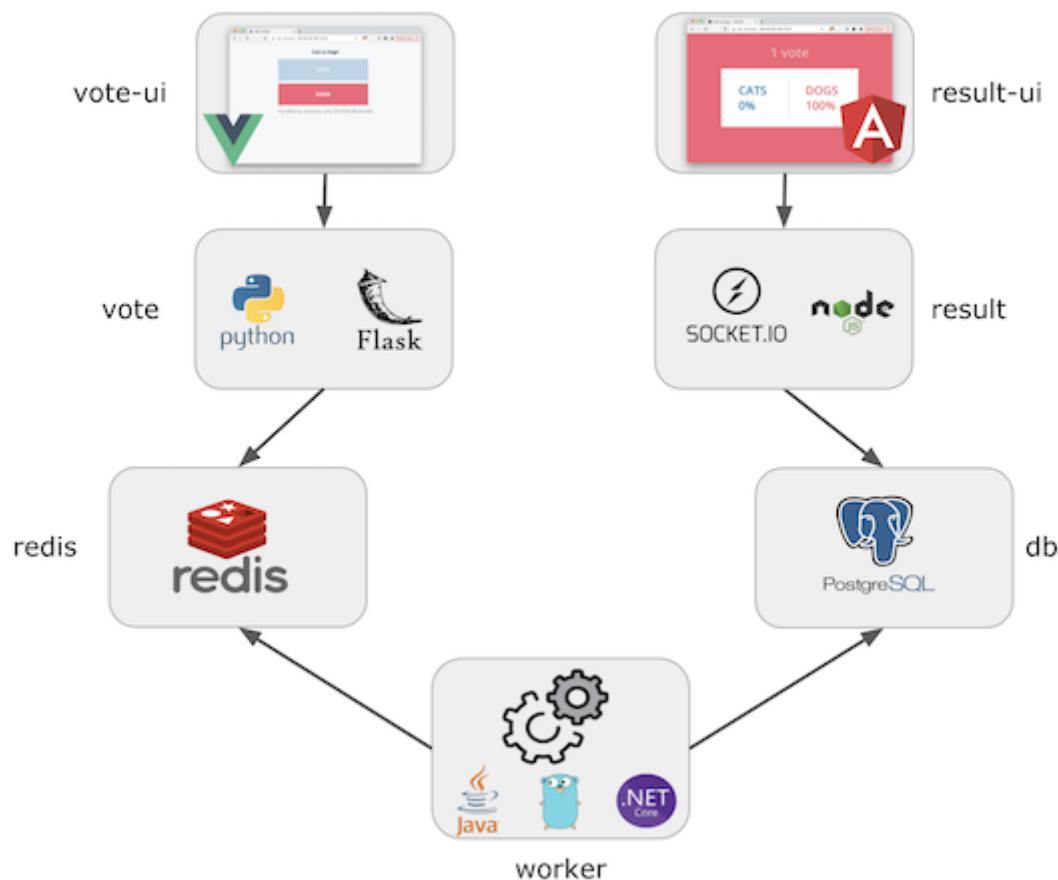
Essayez d'installer cette application en local sur votre propre machine!

## 7.6. Voting App Installation en local.

Nous allons illustrer l'utilisation de [Docker Compose](#) et lancer l'application [Voting App](#). Cette application est très utilisée pour des présentations et démos, c'est un bon exemple d'application micro-services simple.

### 7.6.1. Vue d'ensemble

L'application [Voting App](#) est composée de plusieurs micro-services, ceux utilisés pour la version 2 sont les suivants :



- **vote-ui**: front-end permettant à un utilisateur de voter entre 2 options
- **vote**: back-end réceptionnant les votes
- **result-ui**: front-end permettant de visualiser les résultats
- **result**: back-end mettant à disposition les résultats
- **redis**: database redis dans laquelle sont stockés les votes
- **worker**: service qui récupère les votes depuis redis et consolide les résultats dans une database postgres
- **db**: database postgres dans laquelle sont stockés les résultats

### 7.6.2. Récupération des repos

```
mkdir VotingApp && cd VotingApp  
git clone https://gitlab.com/voting-application/$project
```

### 7.6.3. Installation du binaire docker-compose

- Si vous utilisez **Docker for Mac** ou **Docker for Windows**, le binaire **docker-compose** est déjà installé.

## 7.6.4. Le format de fichier docker-compose.yml

Plusieurs fichiers, au format **Docker Compose**, sont disponibles dans [config/compose](#). Ils décrivent l'application pour différents environnements. Le fichier qui sera utilisé par défaut est le fichier [docker-compose.yml](#) dont le contenu est le suivant:

```
services:  
  vote:  
    build: ../../vote  
    # use python rather than gunicorn for local dev  
    command: python app.py  
    depends_on:  
      redis:  
        condition: service_healthy  
    ports:  
      - "5002:80"  
    volumes:  
      - ../../vote:/app  
    networks:  
      - front-tier  
      - back-tier  
  
  vote-ui:  
    build: ../../vote-ui  
    depends_on:  
      vote:  
        condition: service_started  
    volumes:  
      - ../../vote-ui:/usr/share/nginx/html  
    ports:  
      - "5000:80"  
    networks:  
      - front-tier  
    restart: unless-stopped  
  
  result:  
    build: ../../result  
    # use nodemon rather than node for local dev  
    command: nodemon server.js  
    depends_on:  
      db:  
        condition: service_healthy  
    volumes:  
      - ../../result:/app  
    ports:  
      - "5858:5858"  
    networks:  
      - front-tier  
      - back-tier
```

```
result-ui:
  build: ../../result-ui
  depends_on:
    result:
      condition: service_started
  ports:
    - "5001:80"
  networks:
    - front-tier
  restart: unless-stopped

worker:
  build:
    context: ../../worker
    dockerfile: Dockerfile.${LANGUAGE:-dotnet}
  depends_on:
    redis:
      condition: service_healthy
    db:
      condition: service_healthy
  networks:
    - back-tier

redis:
  image: redis:6.2-alpine3.13
  healthcheck:
    test: ["CMD", "redis-cli", "ping"]
    interval: "5s"
  ports:
    - 6379:6379
  networks:
    - back-tier

db:
  image: postgres:13.2-alpine
  environment:
    POSTGRES_USER: "postgres"
    POSTGRES_PASSWORD: "postgres"
  volumes:
    - "db-data:/var/lib/postgresql/data"
  healthcheck:
    test: ["CMD", "pg_isready", "-U", "postgres"]
    interval: "5s"
  ports:
    - 5432:5432
  networks:
    - back-tier

volumes:
  db-data:
```

```
networks:  
  front-tier:  
  back-tier:
```

Ce fichier est très intéressant, car il définit également des **volumes** et **networks** en plus des **services**. Ce n'est cependant pas un fichier destiné à être lancé en production notamment **parce qu'il utilise le code local et ne fait pas référence à des images existantes pour les services vote-ui, vote, result-ui, result et worker**.

### 7.6.5. Lancement de l'application

Depuis le répertoire **config/compose**, lancez l'application à l'aide de la commande suivante (le fichier **docker-compose.yml** sera utilisé par défaut):

```
>>> docker-compose up -d
```

Les étapes réalisées lors du lancement de l'application sont les suivantes:

- création des networks front-tier et back-tier
- création du volume db-data
- construction des images pour les services *vote-ui*, *vote*, *result-ui*, *result*, *worker* et récupération des images *redis* et *postgres*
- lancement des containers pour chaque service

### 7.6.6. Containers lancés

Avec la commande suivante, listez les containers qui ont été lancés.

```
>>> docker-compose ps
```

Name	Command	State	
<b>Ports</b>			
<hr/>			
compose_db_1	docker-entrypoint.sh postgres	Up (healthy)	0.0.0.0:5432->5432/tcp, :::5432->5432/tcp
compose_redis_1	docker-entrypoint.sh redis ...	Up (healthy)	0.0.0.0:6379->6379/tcp, :::6379->6379/tcp
compose_result-ui_1	/docker-entrypoint.sh nginx ...	Up	0.0.0.0:5001->80/tcp, :::5001->80/tcp
compose_result_1	docker-entrypoint.sh nodejs ...	Up	0.0.0.0:5858->5858/tcp, :::5858->5858/tcp, 80/tcp
compose_vote-ui_1	/docker-entrypoint.sh nginx ...	Up	0.0.0.0:5000->80/tcp, :::5000->80/tcp
compose_vote_1	python app.py	Up	0.0.0.0:5002-

```
>80/tcp,:::5002->80/tcp  
compose_worker_1      dotnet Worker.dll          Up
```

### 7.6.7. Les volumes créés

Listez les volumes avec la CLI, et vérifiez que le volume défini dans le fichier docker-compose.yml est présent.

```
docker volume ls
```

Le nom du volume est prefixé par le nom du répertoire dans lequel l'application a été lancée.

DRIVER	VOLUME NAME
local	compose_db-data

Par défaut ce volume correspond à un répertoire créé sur la machine hôte.

### 7.6.8. Les networks créés

Listez les networks avec la CLI. Les deux networks définis dans le fichier `docker-compose.yml` sont présents.

```
docker network ls
```

De même que pour le volume, leur nom est préfixé par le nom du répertoire.

NETWORK ID	NAME	DRIVER	SCOPE
71d0f64882d5	bridge	bridge	local
409bc6998857	compose_back-tier	bridge	local
b3858656638b	compose_front-tier	bridge	local
2f00536eb085	host	host	local
54dee0283ab4	none	null	local



Comme nous sommes dans le contexte d'un hôte unique (et non dans le contexte d'un cluster Swarm), le driver utilisé pour la création de ces networks est du type bridge. Il permet la communication entre les containers tournant sur une même machine.

### 7.6.9. Utilisation de l'application

Nous pouvons maintenant accéder à l'application : nous effectuons un choix entre les 2 options depuis l'interface de vote à l'adresse <http://localhost:5000>. Si vous avez lancé cette application sur un autre hôte que votre machine, vous aurez accès à cette interface à l'adresse <http://HOST:5000>



## Cats vs Dogs!

CATS

DOGS

Handled by container 1aa3692b62b2

Nous visualisons le résultat depuis l'interface de résultats à l'adresse <http://localhost:5001>. Si vous avez lancé cette application sur un autre hôte que votre machine, vous aurez accès à cette interface à l'adresse <http://HOST:5001>



1 vote

CATS  
100%

DOGS  
0%

### 7.6.10. 8.6.10 Scaling du service worker

Par défaut, un container est lancé pour chaque service. Il est possible, avec l'option `--scale`, de changer ce comportement et de scaler un service une fois qu'il est lancé. Avec la commande suivante, augmenter le nombre de worker à 2.

```
$ docker-compose up -d --scale worker=2
compose_db_1 is up-to-date
compose_redis_1 is up-to-date
compose_result_1 is up-to-date
compose_vote_1 is up-to-date
compose_result-ui_1 is up-to-date
compose_vote-ui_1 is up-to-date
Creating compose_worker_2 ... done
```

Les 2 containers relatifs au service worker sont présents:

Name	Command	State	Ports
compose_db_1	docker-entrypoint.sh postgres	Up (healthy)	0.0.0.0:5432->5432/tcp,:::5432->5432/tcp
compose_redis_1	docker-entrypoint.sh redis ...	Up (healthy)	0.0.0.0:6379->6379/tcp,:::6379->6379/tcp
compose_result-ui_1	/docker-entrypoint.sh nginx ...	Up	0.0.0.0:5001->80/tcp,:::5001->80/tcp
compose_result_1	docker-entrypoint.sh nodem ...	Up	0.0.0.0:5858->5858/tcp,:::5858->5858/tcp, 80/tcp
compose_vote-ui_1	/docker-entrypoint.sh nginx ...	Up	0.0.0.0:5000->80/tcp,:::5000->80/tcp
compose_vote_1	python app.py	Up	0.0.0.0:5002->80/tcp,:::5002->80/tcp
compose_worker_1	dotnet Worker.dll	Up	
compose_worker_2	dotnet Worker.dll	Up	

 il n'est pas possible de scaler les services **vote-ui** et **result-ui** car ils spécifient tous les 2 un port, plusieurs containers ne peuvent pas utiliser le même port de la machine hôte

```
$ docker-compose up -d --scale vote-ui=3
...
ERROR: for vote-ui  Cannot start service vote-ui: driver failed programming external connectivity on endpoint compose_vote-ui_2
(6274094570a329e3a4d9bdcdf4d31b7e3a8e3e7e78d3cc362ad56e14341913da): Bind for 0.0.0.0:5000 failed: port is already allocated
```

## 7.6.11. Suppression de l'application

Avec la commande suivante, stoppez l'application. Cette commande supprime l'ensemble des

éléments créés précédemment à l'exception des volumes (afin de ne pas perdre de données)

```
$ docker-compose down
Stopping compose_result-ui_1 ... done
Stopping compose_vote-ui_1 ... done
Stopping compose_result_1 ... done
Stopping compose_vote_1 ... done
Stopping compose_worker_1 ... done
Stopping compose_redis_1 ... done
Stopping compose_db_1 ... done
Removing compose_vote-ui_3 ... done
Removing compose_vote-ui_2 ... done
Removing compose_result-ui_1 ... done
Removing compose_vote-ui_1 ... done
Removing compose_result_1 ... done
Removing compose_vote_1 ... done
Removing compose_worker_1 ... done
Removing compose_redis_1 ... done
Removing compose_db_1 ... done
Removing network compose_back-tier
Removing network compose_front-tier
```

Afin de supprimer également les volumes utilisés, il faut ajouter le flag `-v`:

```
>>> docker-compose down -v
```

Cet exemple illustre l'utilisation de **Docker Compose** sur l'exemple bien connu de la **Voting App** dans le cadre d'un hôte unique. Pour déployer cette application sur un environnement de production, il faudrait effectuer des modifications dans le fichier **docker-compose**, par exemple:

- Utilisation d'images pour les services
- Ajout de service supplémentaire (aggrégateur de logs, terminaison ssl, ...)
- Contraintes de déploiement
- ...

# 8. Docker Swarm

Nous allons aborder la solution d'orchestration développée par Docker : **SWARM**.

## 8.1. Swarm mode

### 8.1.1. Présentation

Lorsque l'on initialise un **Cluster Swarm**, on met donc à disposition les fonctionnalités d'orchestration du Docker Daemon.

Swarm est un **orquestrateur**, comme Kubernetes. Cela permet de gérer et déployer des applications qui tournent dans des conteneurs.

On définit une application dans le Docker Compose que l'on déploie dans le Cluster.

Dans Swarm, il y a une boucle de réconciliation qui compare l'état désiré de chaque service avec l'état actuel, et s'assure qu'il soit tel que défini dans le fichier **Docker Compose**.

Il y a une gestion des mises à jour de l'application, appelé **rolling update**.

Le **Swarm Mode** utilise une notion de **vIP**, une adresse **IP virtuelle** pour chaque service. Ainsi, quand un service est appelé par son nom, c'est le serveur DNS embarqué dans le Docker Daemon qui va retourner cette **vIP**. Et quand une requête arrive sur cette **vIP**, on a un mécanisme de **load balancing** qui entre en action et qui va rediriger le traffic vers un des conteneurs du service en question.

Swarm, permet de sécuriser les échanges au sein du cluster et d'encrypter les données.

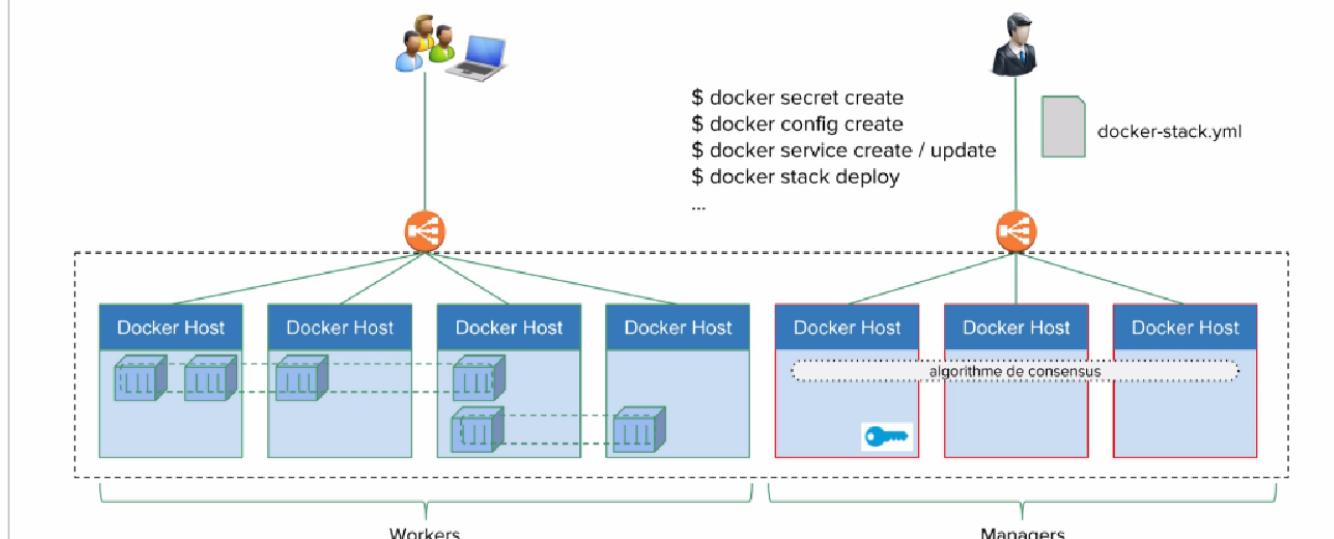
### 8.1.2. Les primitives

Il existe plusieurs primitives qui ont été introduites dans le contexte d'un cluster Swarm.

- **Node** : Une machine membre d'un cluster Swarm.
- **Service** : Qui permet de spécifier la façon dont on veut lancer les conteneurs d'une application.
- **Stack** : Un groupe de service. Par exemple, quand on déploie une application définie dans un format **Docker Compose**, on crée une Stack.
- **Secret** : Un objet secret permet de conserver de façon sécurisée les données sensibles d'une application : Clé privée, mots de passe..Etc
- **Config** : Cet objet permet de gérer la configuration des applications.

### 8.1.3. Vue d'ensemble

## Swarm mode : vue d'ensemble



Nous constatons qu'il y a ici plusieurs **Docker Host**, appelée : **Nodes**. Les 2 Nodes de droites sont les managers du cluster, ils participent à l'algorithme de consensus.

Les Nodes, Workers, sont destinés à déployer les applications sur le cluster.

### 8.1.4. Les commandes de base

```
$ docker swarm --help
```

```
Usage: docker swarm COMMAND
Manage Swarm
Options:
  --help      Print usage
Commands:
  init        Initialize a swarm
  join        Join a swarm as a node and/or manager
  join-token  Manage join tokens
  leave       Leave the swarm
  unlock     Unlock swarm
  unlock-key Manage the unlock key
  update      Update the swarm
```

Pour créer un Swarm :

```
docker swarm init
```

Pour ajouter un Node :

```
docker swarm join
```

L'API permet également d'ajouter une clé de cryptage offrant une couche de sécurité en plus dans le cluster.

## 8.2. Raft : Algorithme de consensus distribué

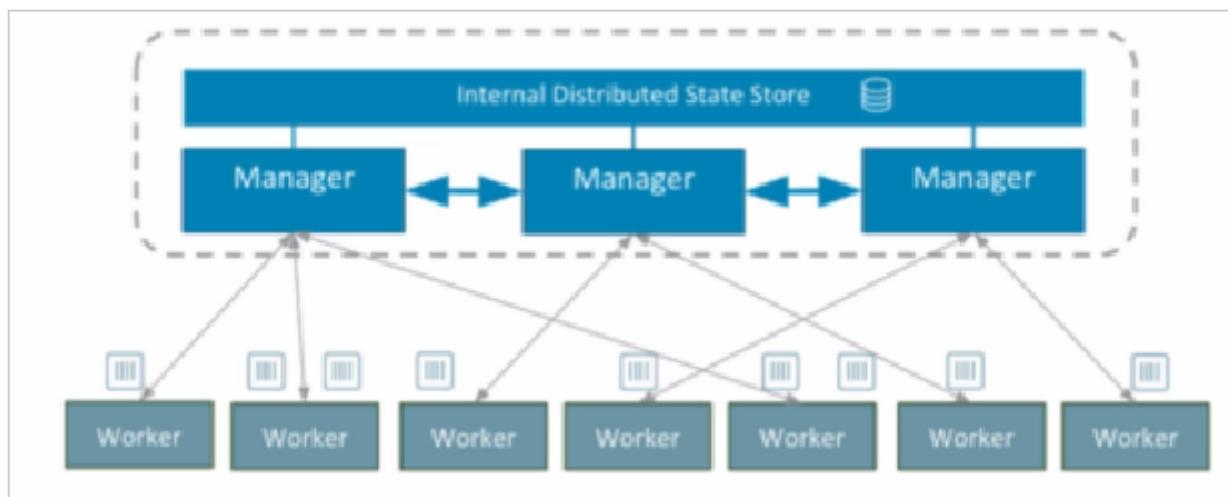
Animation en anglais permettant d'illustrer le fonctionnement de cet algorithme.

<http://thesecretlivesofdata.com/raft/>

## 8.3. Node

Dans le contexte de Swarm, nous avons des Nodes, qui sont simplement des machines sur laquelle tourne un Docker Daemon et qui font partie du Swarm.

Un Node peut être une machine virtuelle ou physique et peut être soit Manager, soit Worker.



S'il est Manager, il peut être Leader, c'est-à-dire responsable de la gestion du Swarm et des décisions d'orchestration. Ou bien, il peut être un manager non-leader et peut participer au consensus Raft.

Si le leader devient non disponible, il pourra être élu comme leader.

Un Node de type Worker, ne va pas participer au consensus Raft, mais va recevoir des instructions du leader et exécute des tâches.

### 8.3.1. Les états d'un Node (availability)

- **Active** : Peut recevoir des tâches.
- **Pause** : Ne peut pas recevoir des tâches. Les tâches en cours ne peuvent pas être modifiées.
- **Drain** : Ne peut pas recevoir des tâches. Les tâches en cours sont stoppées et relancées sur d'autres Nodes.

Les commandes de base pour la primitive Node :

```
$ docker node --help

Usage:docker node COMMAND

Manage Docker Swarm nodes

Options:
    --help      Print usage

Commands:
  demote      Demote one or more nodes from manager in the swarm
  inspect     Display detailed information on one or more nodes
  ls          List nodes in the swarm
  promote     Promote one or more nodes to manager in the swarm
  rm          Remove one or more nodes from the swarm
  ps          List tasks running on a node
  update     Update a node

Run 'docker node COMMAND --help' for more information on a command.
```

### 8.3.2. Node : Initialisation du Swarm



Le Node sur lequel le Swarm est initialisé devient Leader.

```
docker@node1:~$ docker swarm init --advertise-addr 192.168.99.100
Swarm initialized: current node (3gd0odtwxxp6nvomf3xfv05ww) is now a manager.
To add a worker to this swarm, run the following command:
  docker swarm join \
    --token SWMTKN-1-07990ineggmmqgp2zdh7w85y26wd494wwa0f0hjqckim1jq11x-78dzw3pq8drzgq5b1377rsre4 \
    192.168.99.100:2377
To add a manager to this swarm, run 'docker swarm join-token manager' and follow the instructions.

docker@node1:~$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS
3gd0odtwxxp6nvomf3xfv05ww *  node1     Ready   Active        Leader
```

option obligatoire si plusieurs interfaces réseau

### 8.3.3. Node : Ajout d'un worker

- Machine pouvant communiquer avec le manager du Swarm.
- Les commandes Docker doivent être lancées sur un manager.

```
docker@node2:~$ docker swarm join --token
SWMTKN-1-07990ineggmmqgp2zdh7w85y26wd494wwa0f0hjqckim1jq11x-78dzw3pq8drzgq5b1377rsre4 192.168.99.100:2377
This node joined a swarm as a worker.

docker@node1:~$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS
lf2kfkj0442vplsxmgr05lxjq *  node1     Ready   Active        Leader
pes38pa6w8xteze6dbj9lxx54  node2     Ready   Active

docker@node2:~$ docker node ls
Error response from daemon: This node is not a swarm manager. Worker nodes can't be used to view or modify cluster state. Please run this command on a manager node or promote the current node to a manager.
```

### 8.3.4. Node : Ajout d'un manager

- Récupération d'un token depuis le manager
- Un manager non Leader a le statut Reachable

```
docker@node1:~$ docker swarm join-token manager
To add a manager to this swarm, run the following command:
  docker swarm join \
    --token SWMTKN-1-07990ineggmmqgp2zdh7w85y26wd494wwa0f0hjqckim1jq11x-auytk3hyxqijes0mpanl5yax1 \
    192.168.99.100:2377

docker@node3:~$ docker swarm join --token
SWMTKN-1-07990ineggmmqgp2zdh7w85y26wd494wwa0f0hjqckim1jq11x-auytk3hyxqijes0mpanl5yax1 192.168.99.100:2377
This node joined a swarm as a manager.

docker@node1:~$ docker node ls
ID          HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS
1m9rdh9hlkktiwaz3svweeppp  node3    Ready   Active        Reachable
lf2kfkj0442vplsxmgr05lxjq * node1    Ready   Active        Leader
pes38pa6w8xteze6dbj9lxx54  node2    Ready   Active
```

### 8.3.5. Node : promotion / destitution

- Commandes lancées depuis un manager

```
# Destitution d'un node manager en worker
docker@node1:~$ docker node demote node1
Manager node1 demoted in the swarm.

# Promotion d'un node worker en manager
docker@node3:~$ docker node promote node2
Node node2 promoted to a manager in the swarm.

# Etat du Swarm
docker@node2:~$ docker node ls
ID          HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS
1m9rdh9hlkktiwaz3svweeppp  node3    Ready   Active        Leader
lf2kfkj0442vplsxmgr05lxjq * node1    Ready   Active
pes38pa6w8xteze6dbj9lxx54  node2    Ready   Active        Reachable
```

### 8.3.6. Node : Availability

- Une valeur parmi : Active / Pause / Drain
- Contrôle le déploiement des tâches sur un node

```
# Le node2 ne pourra plus recevoir de nouvelles tâches
docker@node1:~$ docker node update --availability pause node2

# Les tâches du node2 seront schédulees sur d'autres node du cluster
docker@node1:~$ docker node update --availability drain node2

# Le node2 repasse en mode actif et pourra recevoir de nouvelles tâches
docker@node1:~$ docker node update --availability active node2
```

### 8.3.7. Node : Label

- Permet l'organisation des nodes
- Peut-être utilisé dans les contraintes de déploiement d'un service

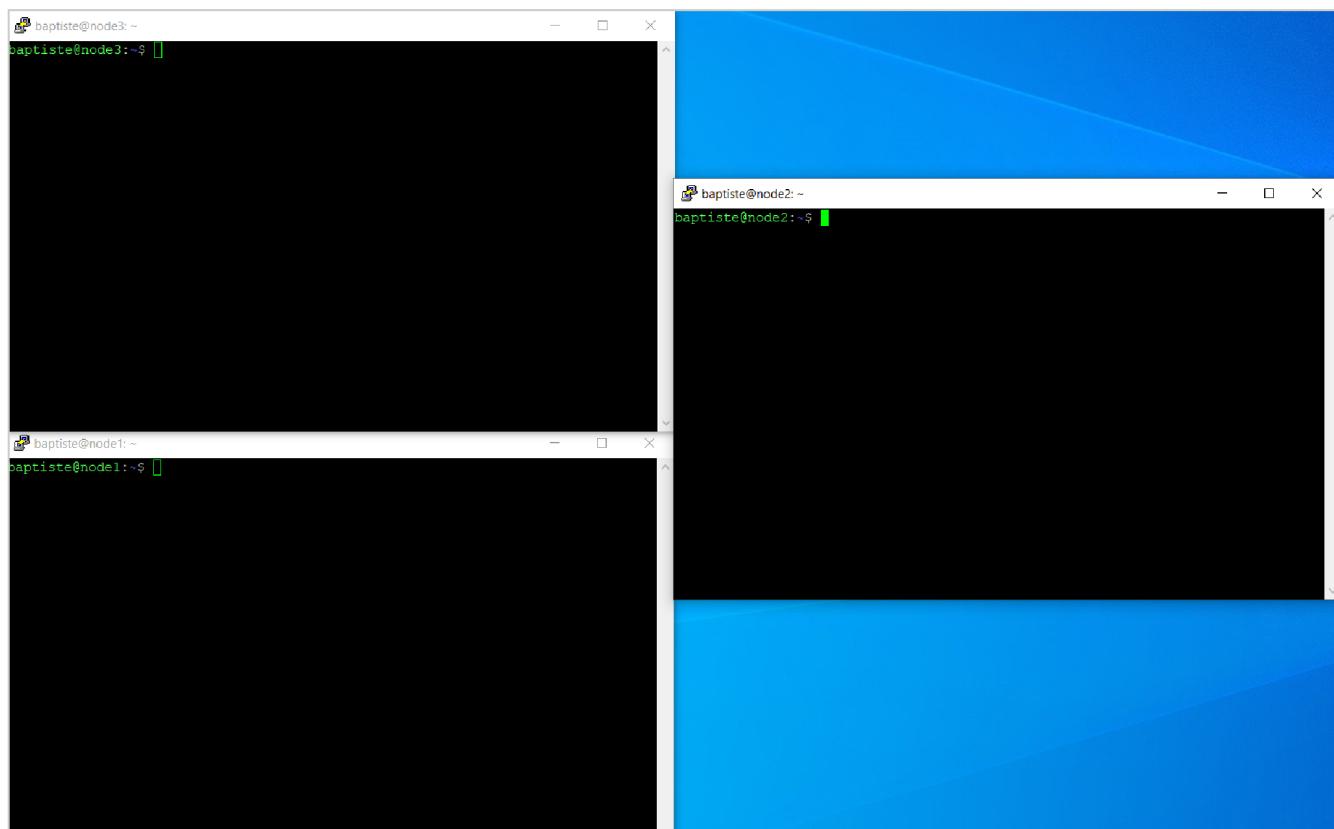
```
# List des labels du node1
$ docker node inspect -f '{{ json .Spec.Labels }}' node1
{}

# Ajout du label Memcached avec la valeur true
$ docker node update --label-add Memcached=true node1
node1

# Liste des labels du node1
$ docker node inspect -f '{{ json .Spec.Labels }}' node1 | jq .
{
  "Memcached": "true"
}
```

## 8.4. [DEMO] Création d'un Swarm

Avec Virtual Box nous avons créé 3 machines virtuelles sous Ubuntu avec Docker Daemon d'installé dessus.



Dans un premier temps nous allons initialiser notre **swarm** avec la commande :

```
docker swarm init
```

```
baptiste@node1:~$ sudo docker swarm init
[sudo] password for baptiste:
Swarm initialized: current node (rbfdhjnmhqdkygdq17h9sewk) is now a manager.

To add a worker to this swarm, run the following command:

    docker swarm join --token SWMTKN-1-509t8pkd49j00hd4hosa1r04ta9v2ci0x42nhviezthuq21z2v-8u9se8xwm
    hkv5n04necsk16p 192.168.1.18:2377

To add a manager to this swarm, run 'docker swarm join-token manager' and follow the instructions.
```

Nous pouvons lister la liste des Node présent :

```
docker node ls
```

ID	HOSTNAME	STATUS	AVAILABILITY	MANAGER STATUS	ENGINE VERSION
obj74c283mce9ikbigezzfu4r2 *	node1	Ready	Active	Leader	20.10.17

Le **node** qui a initialisé le **swarm** devient automatiquement le **Leader**. À partir de lui nous pourrons ajouter un **Worker** grâce à la commande qui est fournie lors de l'initialisation.

- Allons maintenant sur le **Node2** afin d'exécuter cette commande dessus et en faire un **Worker** pour notre **Swarm**.

```
docker swarm join --token SWMTKN-1-  
4mu3p23ebeu30ghysb0bqaynse691bcjz0rqr60jsrshta27ld-76lagmzkiy07ltf0cqjk5w6r9  
192.168.1.18:2377
```

Maintenant, sur **Node1** regardons la liste des Nodes présent sur le Swarm :

```
docker node ls
```

ID	HOSTNAME	STATUS	AVAILABILITY	MANAGER STATUS	ENGINE VERSION
obj74c283mce9ikbigezzfu4r2 *	node1	Ready	Active	Leader	20.10.17
dnbfm3bj64ew11ics27rrii4v	node2	Ready	Active		20.10.17

Nous avons deux nœuds, un **Worker** et un **Leader Manager**.

- Ajoutons donc **Node3** dans notre **Swarm** avec un status de **Manager** :

Dans un premier temps, il faut exécuter la commande suivante sur le **Node1** afin de récupérer un **token** qui permettra à **Node3** de joindre le **Swarm**.

```
docker swarm join-token manager
```

Nous avons obtenu en réponse la commande à saisir dans le **Node3** :

```
docker swarm join --token SWMTKN-1-  
4mu3p23ebeu30ghysb0bqaynse691bcjz0rqr60jsrshta27ld-1fxsub3o4e0cxec0ovf2s3vw0  
192.168.1.18:2377
```

```
baptiste@node3:~$ sudo docker swarm join --token SWMTKN-1-4mu3p23ebeu30ghysb0b  
qaynse691bcjz0rqr60jsrshta27ld-1fxsub3o4e0cxec0ovf2s3vw0 192.168.1.18:2377  
This node joined a swarm as a manager.
```

À partir du Node1, listons la liste des Nodes.

```
docker node ls
```

ID	HOSTNAME	STATUS	AVAILABILITY	MANAGER STATUS	ENGINE VERSION
oj74c283mce9ikbigzzfu4r2 *	node1	Ready	Active	Leader	20.10.17
dnbfm3bj64ew11ics27rrii4v	node2	Ready	Active		20.10.17
e8aempal5891swv1fl6rh74b7	node3	Ready	Active	Reachable	20.10.17

Dans un node Manager, nous pouvons aussi inspecter un autre noeud par exemple et obtenir des informations précises.

```
docker node inspect node1
```

Nous pouvons rétrograder un **Node**, par exemple, le **Node3**, nommons le maintenant comme étant un simple **Worker**.

```
docker node demote node3
```

Et inversement, pour promouvoir :

```
docker node promote node2
```

## 8.5. [Exercice] Crédation en local

### 8.5.1. Quelques rappels sur Docker Swarm

Swarm est la solution de clustering de Docker et permet entre autres:

- le management d'un cluster d'hôtes Docker
- l'orchestration de services sur ce cluster

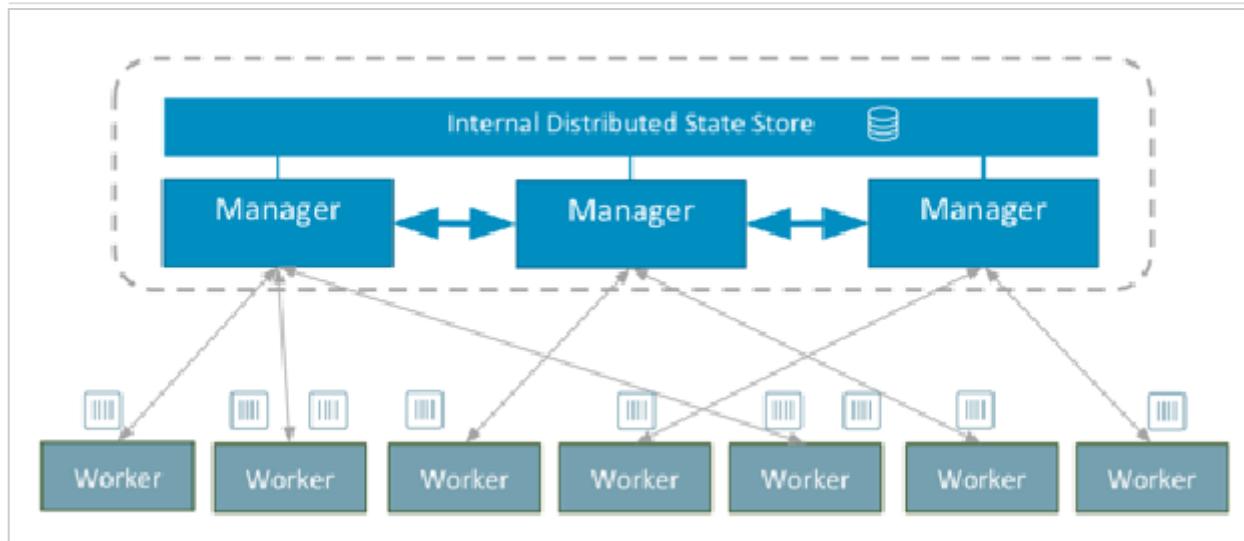
Un cluster Swarm est composé de 2 types de nodes:

- Les managers dont le rôle est de maintenir l'état du cluster. En interne, une implémentation de l'algorithme de consensus Raft est utilisée pour assurer cette fonction.
- Les workers dont le rôle est d'exécuter des tasks (= lancer des containers)



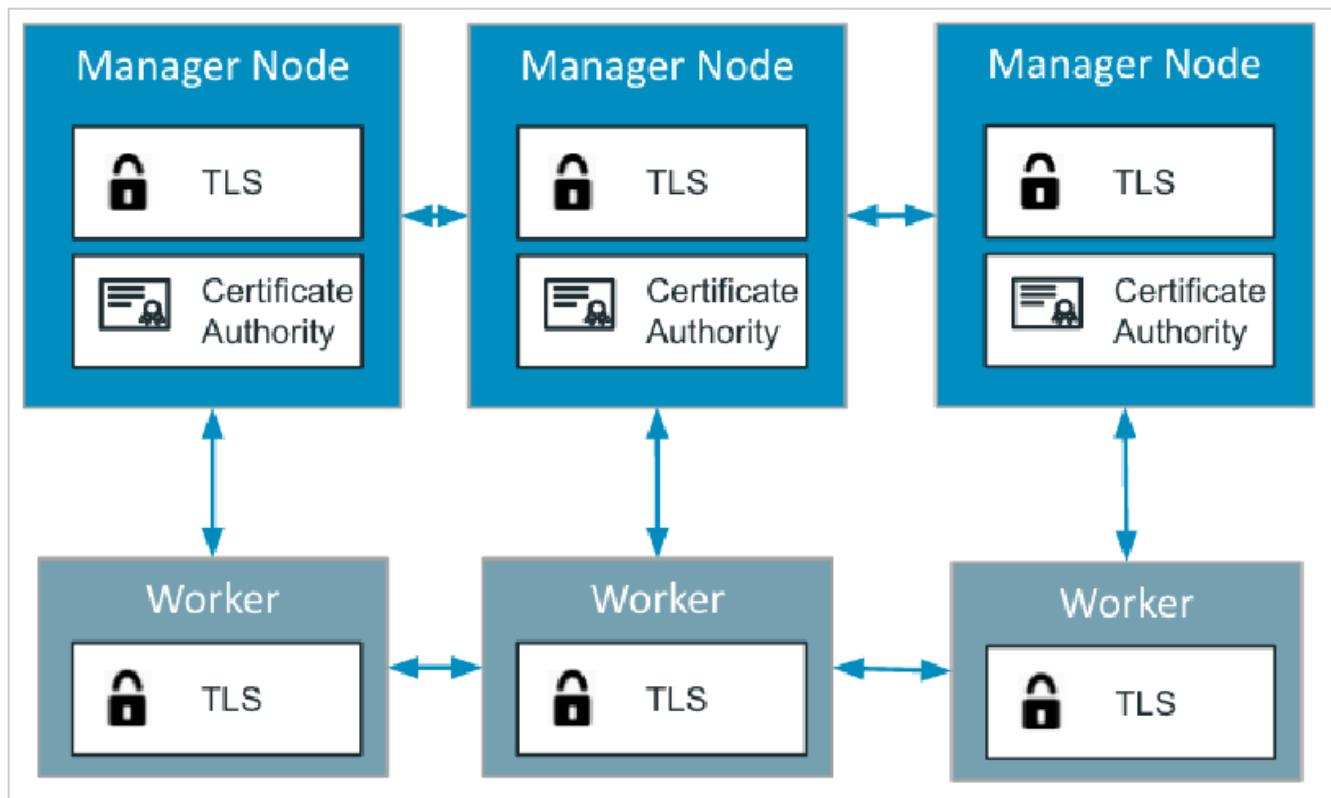
Par défaut, un manager est également un worker.

Le schéma suivant montre la vision haut niveau d'un cluster Swarm.



Par défaut, un Swarm est sécurisé:

- encryption des logs nécessaires à la gestion du cluster
- communication TLS entre les différents nodes
- auto-rotation des certificats



Dans la suite, nous allons créer un cluster swarm en local composé d'un manager et de 2 workers. Nous allons envisager différents cas de figure en fonction de la version de Docker:

- Docker Desktop (Mac), anciennement Docker for Mac
- Docker Desktop (Windows), anciennement Docker for Windows
- Docker for Ubuntu (ou pour d'autres distributions Linux)

Pour effectuer cela, nous utiliserons Docker Machine afin de créer 3 hôtes

## 8.5.2. Création des hôtes avec Docker Machine

### 8.5.2.1. Docker machine

Docker Machine est un utilitaire qui permet de créer une machine virtuelle et d'installer Docker, le client et le daemon, sur celle-ci. Il permet également de gérer le cycle de vie de ces hôtes Docker.

La commande suivante permet d'obtenir la liste des opérations qu'il est possible de faire avec docker-machine.

```
$ docker-machine --help
```

Si vous utilisez Docker Desktop ou Docker Toolbox, le binaire docker-machine est déjà disponible sur votre environnement. Dans les autres cas, il faudra l'installer, c'est un process très simple dont les instructions sont détaillées à l'adresse <https://docs.docker.com/machine/install-machine/> )

En fonction de l'environnement sur lequel vous êtes, il faudra utiliser le driver approprié ci-dessous.

### 8.5.2.2. Docker Desktop (Windows)

L'édition Windows de Docker Desktop utilise l'hyperviseur **Hyper-V**, il faudra dans un premier temps créer un switch virtuel depuis l'interface de Hyper-V, puis ensuite utiliser le driver "hyperv" de docker-machine en précisant le nom de ce switch.

Dans l'exemple ci dessous on utilise un switch virtuel nommé **DMSwitch**.

```
PS C:\WINDOWS\system32> docker-machine create --driver hyperv --hyperv-virtual-switch
"DMSwitch" node1
Running pre-create checks...
Creating machine...
(node1) Copying C:\Users\luc\.docker\machine\cache\boot2docker.iso to
C:\Users\luc\.docker\machine\machines\node1\boot2docker.iso...
(node1) Creating SSH key...
(node1) Creating VM...
(node1) Using switch "DMSwitch"
(node1) Creating VHD
(node1) Starting VM...
(node1) Waiting for host to start...
Waiting for machine to be running, this may take a few minutes...
Detecting operating system of created instance...
Waiting for SSH to be available...
Detecting the provisioner...
Provisioning with boot2docker...
Copying certs to the local machine directory...
Copying certs to the remote machine...
Setting Docker configuration on the remote daemon...
Checking connection to Docker...
Docker is up and running!
```

```
To see how to connect your Docker Client to the Docker Engine running on this virtual machine, run: C:\Program Files\Docker\Resources\bin\docker-machine.exe env node1
```

De la même façon nous créons les 2 autres hôtes, node2 et node3.

```
PS C:\WINDOWS\system32> docker-machine create --driver hyperv --hyperv-virtual-switch "DMSwitch" node2
PS C:\WINDOWS\system32> docker-machine create --driver hyperv --hyperv-virtual-switch "DMSwitch" node3
```

La commande suivante permet de lister les hôtes que nous venons de créer

```
PS C:\WINDOWS\system32> docker-machine ls
NAME      ACTIVE     DRIVER      STATE      URL
ERRORS
node1      -          hyperv      Running    tcp://192.168.1.25:2376
node2      -          hyperv      Running    tcp://192.168.1.26:2376
node3      -          hyperv      Running    tcp://192.168.1.27:2376
SWARM      DOCKER
v18.09.1
v18.09.1
v18.09.1
```

### 8.5.2.3. Docker Desktop (Mac)

Pour Docker for Mac, nous utilisons [Virtualbox](<https://www.virtualbox.org/>) afin d'instantier 3 machines virtuelles.

La commande suivante permet de créer un hôte nommé **node1**

```
$ docker-machine create --driver virtualbox node1
Running pre-create checks...
Creating machine...
(node1) Copying /Users/luc/.docker/machine/cache/boot2docker.iso to
/Users/luc/.docker/machine/machines/node1/boot2docker.iso...
(node1) Creating VirtualBox VM...
(node1) Creating SSH key...
(node1) Starting the VM...
(node1) Check network to re-create if needed...
(node1) Waiting for an IP...
Waiting for machine to be running, this may take a few minutes...
Detecting operating system of created instance...
Waiting for SSH to be available...
Detecting the provisioner...
Provisioning with boot2docker...
Copying certs to the local machine directory...
Copying certs to the remote machine...
Setting Docker configuration on the remote daemon...
Checking connection to Docker...
Docker is up and running!
```

To see how to connect your Docker Client to the Docker Engine running on this virtual machine, run: docker-machine env node1

De la même façon nous créons les 2 autres hôtes, node2 et node3.

```
$ docker-machine create --driver virtualbox node2
$ docker-machine create --driver virtualbox node3
```

Nous pouvons alors nous assurer que nos 3 hôtes sont en état de marche en lançant la commande suivante:

\$ docker-machine ls						
NAME	ACTIVE	DRIVER	STATE	URL	SWARM	DOCKER
ERRORS						
node1	-	virtualbox	Running	tcp://192.168.99.100:2376		v18.09.1
node2	-	virtualbox	Running	tcp://192.168.99.101:2376		v18.09.1
node3	-	virtualbox	Running	tcp://192.168.99.102:2376		v18.09.1

#### 8.5.2.4. Docker for Ubuntu

De la même façon que pour Docker Desktop, dans un environnement Linux nous utiliserons [Virtualbox](<https://www.virtualbox.org/>) afin d'instantier 3 machines virtuelles.

```
$ docker-machine create --driver virtualbox node1
Running pre-create checks...
(node1) Default Boot2Docker ISO is out-of-date, downloading the latest release...
(node1) Latest release for github.com/boot2docker/boot2docker is v18.09.1
(node1) Downloading /home/luc/.docker/machine/cache/boot2docker.iso from
https://github.com/boot2docker/boot2docker/releases/download/v18.09.1/boot2docker.iso.
.
(node1) 0%....10%....20%....30%....40%....50%....60%....70%....80%....90%....100%
Creating machine...
(node1) Copying /home/luc/.docker/machine/cache/boot2docker.iso to
/home/luc/.docker/machine/machines/node1/boot2docker.iso...
(node1) Creating VirtualBox VM...
(node1) Creating SSH key...
(node1) Starting the VM...
(node1) Check network to re-create if needed...
(node1) Waiting for an IP...
Waiting for machine to be running, this may take a few minutes...
Detecting operating system of created instance...
Waiting for SSH to be available...
Detecting the provisioner...
Provisioning with boot2docker...
Copying certs to the local machine directory...
Copying certs to the remote machine...
Setting Docker configuration on the remote daemon...
```

```
Checking connection to Docker...
Docker is up and running!
To see how to connect your Docker Client to the Docker Engine running on this virtual
machine, run: docker-machine env node1
```

Nous répétons alors la procédure pour créer 2 autres hôtes Docker

```
$ docker-machine create --driver virtualbox node2
$ docker-machine create --driver virtualbox node3
```

De la même façon que précédemment, la commande suivante permet de s'assurer que les 3 hôtes sont en état de marche:

```
$ docker-machine ls
NAME ACTIVE DRIVER STATE URL SWARM DOCKER
ERRORS
node1 - virtualbox Running tcp://192.168.99.100:2376 v18.09.1
node2 - virtualbox Running tcp://192.168.99.101:2376 v18.09.1
node3 - virtualbox Running tcp://192.168.99.102:2376 v18.09.1
```

## 8.5.3. Création du swarm

Maintenant que nous avons créé les 3 hôtes Docker, nous allons les mettre en cluster en créant un swarm.

### 8.5.3.1. Initialisation à partir de node1

La commande suivante permet de nous connecter en ssh sur node1

```
$ docker-machine ssh node1
```

Nous pouvons ensuite initialiser le swarm

```
$ docker swarm init
Swarm initialized: current node (preife0qe9vjyum4rv13qm33l) is now a manager.
```

To add a worker to this swarm, run the following command:

```
docker swarm join \
--token SWMTKN-1-0jo31iectxf4uo4airmn1cepphe9mbg4j8j6276as56i6gi82c-
8gggnqa3165gb0x8idf8tqs68p \
10.0.107.3:2377
```

To add a manager to this swarm, run 'docker swarm join-token manager' and follow the instructions.

Attention, lors de l'initialisation il est possible que vous obteniez une erreur semblable au message suivant

```

Error response from daemon: could not choose an IP address to advertise since this system has multiple addresses on different > interfaces (10.0.2.15 on eth0 and 192.168.99.100 on eth1) - specify one with --advertise-addr  
```

Il faudra dans ce cas préciser l'adresse IP sur laquelle le manager sera accessible. On pourra initialiser le swarm avec la commande suivante:

```
$ docker swarm init --advertise-addr 192.168.99.100
```

Le daemon Docker du node1 est maintenant en Swarm mode, nous pouvons lister les nodes de notre cluster.

```
$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS  ENGINE
VERSION
tntzagkqg9uchatr8hzh8alio *  node1    Ready   Active        Leader
18.09.1
```

### 8.5.3.2. Ajout des workers

Depuis les 2 autres terminaux, nous lançons la commande **docker swarm join...** obtenue lors de l'initialisation du Swarm.

```
$ docker swarm join \
--token SWMTKN-1-0jo31iectxf4uo4airmn1cepphe9mbg4j8j6276as56i6gi82c-
8gggnqa3165gb0x8idf8tqs68p \
192.168.99.100:2377
```

Nous obtenons alors la réponse suivante

```
This node joined a swarm as a worker.
```

Depuis le node1 (seul manager de notre swarm), nous pouvons alors lister les nodes présents dans notre cluster.

```
$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS  ENGINE
VERSION
```

tntzagkqg9uchatr8hzh8alio *	node1	Ready	Active	Leader
18.09.1				
7avuhgyf15ia91kyoteefzxf	node2	Ready	Active	
18.09.1				
ua03a3x0rtgrbnbnq2nifdtm2	node3	Ready	Active	
18.09.1				

Le node1 est l'unique manager du cluster, node2 et node3 sont des workers.



Toutes les commandes du client Docker doivent être envoyées sur un manager, si nous lançons la commande précédente sur node2 ou node3, nous obtenons l'erreur suivante.

```
$ docker node ls
Error response from daemon: This node is not a swarm manager. Worker nodes can't be
used to view or modify cluster state. Please run this command on a manager node or
promote the current node to a manager.
Inspection d'un node
```

#### 8.5.4. Inspection d'un hôte

Comme pour les autres primitives de la plateforme (containers, images, volumes, networks), la commande inspect permet d'obtenir la vue détaillée d'un node.

```
$ docker node inspect node1
[
  {
    "ID": "jrqb09bsa47xb23pyrw0fgah4",
    "Version": {
      "Index": 9
    },
    "CreatedAt": "2017-11-03T14:00:17.670877138Z",
    "UpdatedAt": "2017-11-03T14:00:18.278047861Z",
    "Spec": {
      "Labels": {},
      "Role": "manager",
      "Availability": "active"
    },
    "Description": {
      "Hostname": "node1",
      "Platform": {
        "Architecture": "x86_64",
        "OS": "linux"
      },
      "Resources": {
        "NanoCPUs": 1000000000,
        "MemoryBytes": 1044123648
      }
    }
  }
]
```

```
"Engine": {
    "EngineVersion": "17.10.0-ce",
    "Labels": {
        "provider": "virtualbox"
    },
    "Plugins": [
        {
            "Type": "Log",
            "Name": "awslogs"
        },
        {
            "Type": "Log",
            "Name": "fluentd"
        },
        {
            "Type": "Log",
            "Name": "gcplogs"
        },
        {
            "Type": "Log",
            "Name": "gelf"
        },
        {
            "Type": "Log",
            "Name": "journald"
        },
        {
            "Type": "Log",
            "Name": "json-file"
        },
        {
            "Type": "Log",
            "Name": "logentries"
        },
        {
            "Type": "Log",
            "Name": "splunk"
        },
        {
            "Type": "Log",
            "Name": "syslog"
        },
        {
            "Type": "Network",
            "Name": "bridge"
        },
        {
            "Type": "Network",
            "Name": "host"
        }
    ]
}
```

```

        "Type": "Network",
        "Name": "macvlan"
    },
    {
        "Type": "Network",
        "Name": "null"
    },
    {
        "Type": "Network",
        "Name": "overlay"
    },
    {
        "Type": "Volume",
        "Name": "local"
    }
]
},
"TLSInfo": {
    "TrustRoot": "-----BEGIN CERTIFICATE-----
MIIBBaTCCARCgAwIBAgIUIDgi01oBB7DgxX0wYvAaHBj8z14wCgYIKoZIzj0EAwIw\nEzERMA8GA1UEAxMIC3
dhcm0tY2EwHhcNMTcxMTAzMTM1NTAwWhcNMzcxMDI5MTM1\nnNTAwWjATMREwDwYDVQQDEwhzd2FybS1jYTBZMB
MGByqGSM49AgEGCCqGSM49AwEH\nnA0IABOOT4AHM48JwGIp0aiFDHRtXSVQm9yJoaM3awlok7zwVJfVcLWES
VT7B9u\nn4LQtjT5S1+ZUDa1UjQELWQtGaHajQjBAMA4GA1UdDwEB/wQEAvIBBjAPBgNVHRMB\nnAf8EBTADAQH/
MB0GA1UdDgQWBBDfFvLG+hSDdP+AFSL0ZiSEjetnWDAKBggqhkJ0\nnPQQDAgNHADBEAiB9atr7uP0eclaq06Z9
1kyOH8IYxXW9jxInIfNu37BtXgIgfqWu\nnQ51iyG4tNLodPgyxfMEpQrFS/pfDGDU2Timi4=\n-----END
CERTIFICATE-----\n",
    "CertIssuerSubject": "MBMxETAPBgnVBAMTCHN3YXJtLWNh",
    "CertIssuerPublicKey": "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE845PgAcQzjwnAYinRqIUMdG1dJVcb3ImhozdrCWiT
vPBUl9VwtYRJVPsH27gtC2NP1LX5lQNrVSNAQtZC0Zodg=="
}
},
"Status": {
    "State": "ready",
    "Addr": "192.168.99.100"
},
"ManagerStatus": {
    "Leader": true,
    "Reachability": "reachable",
    "Addr": "192.168.99.100:2377"
}
}
]

```

Cette commande retourne entre autres: - le status du node - son rôle (manager vs worker) - les plugins disponibles - le certificat TLS

Nous pouvons utiliser les Go template afin d'obtenir une information précise contenue dans cette structure json. Par exemple, la commande suivante permet de récupérer l'adresse IP du node directement.

```
$ docker node inspect -f "{{ .Status.Addr }}" node1
```

### 8.5.5. Mise à jour d'un node

Une fois les nodes créés, il est possible de changer leur rôle et de: - promouvoir un worker en manager - destituer un manager en worker

#### 8.5.5.1. Promotion de node2

La commande suivante permet de changer le node2 et d'en faire un manager

```
$ docker node promote node2
Node node2 promoted to a manager in the swarm.
```

Les commandes Docker peuvent maintenant être lancées depuis node1 ou node2 puisque tous 2 sont des managers.

```
$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS  ENGINE
VERSION
tntzagkqg9uchatr8hzh8alio *  node1     Ready   Active        Leader
18.09.1
7avuhhygf15ia91kyotee6zxf    node2     Ready   Active        Reachable
18.09.1
ua03a3x0rtgrbnbnq2nifdtm2    node3     Ready   Active
18.09.1
```

Le node2 a l'entrée Reachable dans la colonne MANAGER STATUS, ce qui signifie qu'il est du type manager, mais pas Leader.

#### 8.5.5.2. Destitution du node2

Depuis node1 ou node2, nous pouvons destituer le node2 et le repasser en worker.

```
$ docker node demote node2
Manager node2 demoted in the swarm.
```

Si nous listons une nouvelle fois les nodes du cluster, nous pouvons voir que le node2 n'a plus d'entrée dans la colonne MANAGER STATUS.

```
$ docker node ls
ID                  HOSTNAME  STATUS  AVAILABILITY  MANAGER STATUS  ENGINE
VERSION
tntzagkqg9uchatr8hzh8alio *  node1     Ready   Active        Leader
18.09.1
```

7avuhgyf15ia91kyoteefzxf 18.09.1	node2	Ready	Active
ua03a3x0rtgrbnbnq2nifdtm2 18.09.1	node3	Ready	Active

### 8.5.6. Résumé

Nous avons vu dans cet exercice la façon de créer un swarm en local, soit en utilisant VirtualBox, soit en utilisant l'hyperviseur Hyper-V.

## 8.6. [DEMO] Crédation d'un Service

Nous allons créer un nouveau service basé sur l'image `nginx`.

```
docker service create --name www -p 80:80 --replicas 3 nginx
```

Listons les services de notre Swarm :

```
docker service ls
```

```
baptiste@node1:~$ sudo docker service ls
ID          NAME      MODE      REPLICAS      IMAGE      PORTS
n4smgvts5i8f    www      replicated    3/3        nginx:latest *:80->80/tcp
```

Nous pouvons rajouter des réplicats

```
docker service scale www=5
```

Listons les services `www` :

```
docker service ps www
```

```
baptiste@node1:~$ sudo docker service ps www
ID          NAME      IMAGE      NODE      DESIRED STATE      CURRENT STATE      ERROR
S
q9cznmc49m2s    www.1      nginx:latest    node2      Running      Running 6 minutes ago
od0zptwai3nr    www.2      nginx:latest    node3      Running      Running 6 minutes ago
zf16a2ruqcy4    www.3      nginx:latest    node1      Running      Running 6 minutes ago
kidpuinuuygr    www.4      nginx:latest    node2      Running      Running 45 seconds ago
a71pdml4dy7s    www.5      nginx:latest    node1      Running      Running 45 seconds ago
```

Nous constatons que les services se répartissent sur les nodes du Swarm.

## 8.7. Crédation d'un service

Dans cette partie, nous allons créer un service simple, le déployer et le scaler (c'est à dire modifier le nombre de containers instanciés pour celui-ci). Nous changerons également la disponibilité d'un

node pour voir l'impact sur les tâches en cours.

### 8.7.1. Pré-requis

Vous pouvez utiliser un Swarm que vous avez créé lors des exercices précédent, ou bien en créer un nouveau. N'hésitez pas à vous reporter aux cours ou bien aux exercices précédents si vous avez besoin de revoir le process de création.

### 8.7.2. Crédation d'un service

Utilisez la commande suivante pour créer le service nommé **vote** ayant les spécifications ci-dessous:

- basé sur l'image **instavote/vote:latest**
- publication du 80 sur le port 8080 des nodes du Swarm
- 6 répliques

Le nombre de répliques correspond au nombre de tâches qui seront instanciées pour ce service. Chaque tâche lancera un container basée sur l'image définie dans le service.

Lancez cette commande depuis un node qui a le status de manager.

```
$ docker service create \
  --name vote \
  --publish 8080:80 \
  --replicas 6 \
  instavote/vote
```

Après quelques secondes, le temps que l'image **instavote/vote:latest** soit téléchargée sur chaque node, les 6 tâches du services sont lancées.

```
iloiyvba6uensc6bzvhvbxv93
overall progress: 6 out of 6 tasks
1/6: running  [=====>]
2/6: running  [=====>]
3/6: running  [=====>]
4/6: running  [=====>]
5/6: running  [=====>]
6/6: running  [=====>]
verify: Service converged
```

Utilisez la commande suivante pour lister les tâches du service **vote**.

```
$ docker service ps vote
```

Vous devriez obtenir un résultat proche du résultat suivant (aux identifiants près), indiquant qu'il y

a 2 tâches par node.

ID	NAME	IMAGE	NODE	DESIRED STATE	CURRENT STATE
ERROR PORTS					
xnon20jonsfd ago	vote.1	instavote/vote:latest	node2	Running	Running 13 minutes
rghanh2g8y8b7 ago	vote.2	instavote/vote:latest	node3	Running	Running 13 minutes
on8oog1833yq ago	vote.3	instavote/vote:latest	node1	Running	Running 13 minutes
hmp2wtvojxro ago	vote.4	instavote/vote:latest	node2	Running	Running 13 minutes
vdizjy291q4t ago	vote.5	instavote/vote:latest	node3	Running	Running 13 minutes
mjp0ybsg6pj ago	vote.6	instavote/vote:latest	node1	Running	Running 13 minutes

Le service publie le port 80 sur le port 8080 du swarm via le mécanisme de routing mesh. Cela signifie que le service sera accessible depuis le port 8080 de chaque node du cluster. Nous pouvons vérifier le routing mesh en envoyant une requête sur le port 8080 de node1, node2 ou node3. Quelque soit le node sur lequel la requête est envoyée, nous aurons accès à l'interface de l'application. Nous reviendrons en détails sur le routing mesh un peu plus tard dans le cours.

The screenshot shows a web browser window with the following details:

- Address Bar:** Non sécurisé | 192.168.99.100:8080
- Toolbar:** Includes icons for back, forward, search, and refresh.
- Content Area:**
  - Title:** Cats vs Dogs!
  - Buttons:** Two large buttons labeled "CATS" (blue) and "DOGS" (teal).
  - Text:** (Tip: you can change your vote)
  - Footer:** Processed by container ID a459fe8aab1f



Seule la partie front-end est disponible sur cet exemple, il n'y a pas le backend permettant de prendre en compte la sélection.

Les requêtes envoyées sur le port 8080 d'un node du Swarm sont traitées selon un algorithme de round-robin entre les différents containers intanciés pour le service. Cela signifie que chacun des containers recevra une requête à tour de rôle.

Nous pouvons l'observer en lançant plusieurs requêtes à la suite et observer l'identifiant ID du container depuis l'interface web

### 8.7.3. Ajout du service de visualisation

Utilisez la commande suivante pour lancer un service qui servira à la visualisation des containers sur le cluster.

```
$ docker service create \
--name visualizer \
--mount type=bind,source=/var/run/docker.sock,destination=/var/run/docker.sock \
--constraint 'node.role == manager' \
--publish "8000:8080" dockersamples/visualizer:stable
```

Ce service a la spécification suivante: - il est nommé **visualizer** - il fait un bind-mount de la socket **/var/run/docker.sock** afin de permettre au container du visualizer de dialoguer avec le daemon Docker sur lequel il tourne - il utilise une contrainte de déploiement pour que le replica du service tourne sur le node qui a le rôle manager - il publie le port **8080** sur le port **8000** sur chaque hôte du Swarm

Nous pouvons alors voir la répartition des containers sur les nodes via l'interface du visualiseur. Cette interface donne le même résultat que lorsque l'on liste les service en ligne de commande, mais c'est une façon assez ludique de visualiser les containers.

The screenshot shows a Docker Swarm interface with three nodes:

- node1 manager**: 0.966G RAM. Contains:
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, 3de313d6888fb11591aa6f469746da, state : running
  - visualizer**: image : visualizer:stable@sha256:bc680132f772c, tag : stable@sha256:bc680132f772c, updated : 10/1 21:26, 19222b9588c03ba7b07d21b43a044, state : running
- node2 worker**: 0.966G RAM. Contains:
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, e4c3ca759fa34aecc3845bdd55e0c03, state : running
- node3 worker**: 0.966G RAM. Contains:
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, a459fe8aab1f6ab08eb766ad606a13, state : running
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, 0b72cc119724224962e8caf97c2031, state : running
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, 9cb1df114b108535e8b59f1950c9f33, state : running
  - vote**: image : vote:latest@sha256:744fb4b71488d, tag : latest@sha256:744fb4b71488d, updated : 10/1 21:9, fe6d37555deacf1e43b746ccb32f9f3, state : running

Note: le visualizer tourne sur le node master mais il est possible d'y accéder depuis n'importe quel node du Swarm grâce au mécanisme de routing mesh

## 8.7.4. Passage du node2 en drain

Un node est dans l'un des états suivants: - active, il peut recevoir des nouvelles tâches - pause, il ne peut pas recevoir de nouvelles tâches mais les tâches en cours restent inchangées - drain, il ne peut plus recevoir de nouvelles tâches et les tâches en cours sont re-schédulées sur d'autres nodes

Avec la commande suivante, changez l'availability du **node2** en lui donnant la valeur **drain**.

```
$ docker node update --availability drain node2
```

Depuis le visualizer, regardez comment la répartition des tâches précédentes a été modifiée.

Nous pouvons voir qu'il n'y a plus de tâche sur le node2. Elles ont été stoppées et reschédulées sur les autres nodes.

La commande suivante change l'availability du node2 en le repositionnant dans l'état active. Les tâches existantes sur node1 et node3 restent inchangées mais de nouvelles tâches pourront de nouveau être schédulées sur node2.

```
$ docker node update --availability active node2
```

## 8.7.5. En résumé

Nous avons vu dans cette mise en pratique comment créer des services très simples. Nous avons également vu l'influence de la propriété **availability** d'un node par rapport à la répartition des tâches des services.

# 9. Network

En cours de rédaction ...

# 10. Sécurité

En cours de rédaction ...

# 11. Gestion des logs

En cours de rédaction ...

# 12. Mise en pratique

Cette série de travaux reprend les concepts de base de Docker et vous guides dans leur mise en pratique.

## 12.1. Serveur HTTP avec Docker

[image]

Nous allons vous guider à chaque étape de la mise en place d'un serveur **WEB APACHE** sous **DOCKER**.

Une équipe d'**ESPORT : NECROMANCERS**, a confié la création de son site web à une agence de communication dont la maquette HTML est disponible dans le fichier **esport.zip**.

- **Créez** un dossier « **docker** » dans « **mes documents** » et créez un autre dossier à l'intérieur nommé « **www** ».
- **Téléchargez** ce fichier sur votre disque dur, et **dézippez** l'archive. Vous obtenez un dossier qui se nomme : « **esport** ».
- **Déplacez** le dossier « **esport** » dans le dossier.

Votre première mission sera de mettre en place un serveur **WEB** sous **Apache** avec **Docker**.

- Nous avons plusieurs possibilités qui s'offrent à nous :
  - Soit nous téléchargeons une image d'une distribution Linux puis nous installons et configurons nous-même Apache.
  - Soit nous trouvons une image contenant déjà Apache.

La force de Docker est de posséder une sorte de « **AppStore** », un « **Hub** » appelé le « **dockerHub** » qui regroupe des images officielles et non officielles utilisables. Recherchons donc une image correspondant à notre besoin : [Docker Hub](#)

[image]

Examinons les distributions **Linux** qui accompagnent **Apache** en cliquant dessus. Nous constatons qu'**Alpine** est la distribution par défaut. C'est un bon choix, car c'est une distribution **Linux Légère**.

[image]

En parcourant la page dédiée de l'image **Apache** nous trouvons le sous-titre « **How to use this image** » qui nous permettra de comprendre comment utiliser ce container.

Nous l'installerons grâce au nom de l'image : **httpd**.

Nous allons avoir besoin de dire au container **Apache** où trouver les fichiers de la maquette pour les interpréter. Nous savons qu'ils sont stockés sur notre machine ,appelée la **machine hôte**, au chemin suivant dans mon cas : **C:\Users\baptiste\Documents\docker\td\www\esport**. Le container Apache, (*lire la documentation*) est configuré pour aller lire les fichiers Web dans son dossier

interne : `/usr/local/apache2/htdocs/`.

Il faut donc **monter** notre répertoire de la **machine hôte** dans le dossier **htdocs** de Apache2. Cela est possible grâce à l'option : `-v <HOST_PATH>:<CONTAINER_PATH>`

Apache, le serveur Web, écoute par défaut sur le **port 80** du container. Il faut donc lier un port de la machine hôte avec le port 80 du container. Nous décidons arbitrairement de publier le **port 80 du container** sur le **port 2000 de notre machine hôte**. Grâce à l'option `-p HOST_PORT:CONTAINER_PORT`.

Une fois que notre container est lancé, nous voulons continuer à avoir la main sur notre terminal. Par conséquent il faudra donc utiliser l'option `-d` pour lancer le container en **background** (tâche de fond).

Nous nommerons ce container avec l'option : `--name serveur_http`.

Au final, la commande pour installer et lancer notre container sera :

```
docker container run -d --name serveur_http -v  
$PWD/Documents/docker/td/www/esport:/usr/local/apache2/htdocs -p 2000:80 httpd
```

[image]

Pour tester, ouvrez votre navigateur et saisissez l'adresse : <http://localhost:2000/>

[image]

Nous allons ouvrir un **shell** dans le container pour consulter le contenu du dossier : `/usr/local/apache2/htdocs`

Tapez la commande :

```
docker container exec -ti serveur_http sh
```

`docker container exec` permet de donner l'ordre à notre container de lancer une commande et l'option `-ti` permet de garder la main sur le **shell**.

À partir du shell, plaçons-nous donc dans le répertoire `htdocs`. .. code-block:

```
cd /usr/local/apache2/htdocs
```

et listons les fichiers le contenant :

```
ls
```

[image]

Nous voyons que le dossier **HTDOCS** de notre container contient les fichiers de notre application

provenant de notre dossier **esport**.

Avec un éditeur de code comme **Visual Studio Code**, ouvrez le fichier [/www/esport/index.html](#) à partir de la machine hôte.

Ajoutez le code suivant entre les lignes 250 et 251 et actualisé le navigateur :

```
<h4 class="text-white landing-title">mode dev</h4>
```

[image]

*Note*



Nous constatons que les fichiers de notre application ne sont pas réellement dans le container. Nous l'avons prouvé en modifiant le fichier à partir de la machine hôte et en observant que la modification a été prise en compte par le navigateur. Nous n'avons créé qu'un **lien symbolique** de nos fichiers locaux dans le container.

**Notre site, est accessible !!! Nous avons rempli notre première mission !**

## 12.2. Serveur HTTPS avec Docker

Dans la partie 13.1, nous avons mis en place un container Apache permettant d'accéder à notre site web par l'intermédiaire de l'adresse : <http://localhost:2000> Mais la connexion **http** n'est pas sécurisée. Pour cela, il faut que le protocole soit **https**.

### Rappel : Création des certificats SSL

Les applications Web utilisent le protocole **HTTPS** pour s'assurer que les communications entre les clients et le serveur soient cryptées et ne puissent pas être interceptées. De plus, **Google** pénalise le contenu des sites web qui utilisent le protocole **HTTP** seul dans le référencement. Il est donc obligatoire de configurer notre serveur pour lui permettre d'être accessible via le protocole **HTTPS**.

Pendant le développement local, les développeurs utilisent :

- Soit le protocole **HTTP**.

Cela signifie alors que les versions du projet en local ou en production sont développées dans un environnement différent. Cela peut être plus difficile pour repérer les problèmes.

- Soit un (faux) certificat **SSL Autosigné**.

L'environnement de développement est alors proche de l'environnement de production, mais le navigateur continue de traiter les requêtes différemment. Par exemple, les fausses requêtes SSL ne sont pas mis en cache.

Toutes les communications clients/serveurs ont besoin d'être sécurisés avec un protocole. Nous utiliserons SSL (Secure Socket Layer).

Les communications sécurisées entre des applications se font grâce à des certificats (CERT)

distribués par une autorité certifiante (CA) qui est mutuellement agréé par le client et le serveur.

## Le format CERT

La plupart des certificats ont pour extension `.pem`, `.cer`, `.crt`, `.key`. Les clients (navigateurs) communiquant avec le serveur vont garder le fichier `.pem` (PRIVACY ENHANCED MAIL) ou `.CER` (extension pour les certificats SSL) pour établir une connexion sécurisée.

[image]

L'algorithme RSA (*Rivest Shamir Adleman*) est utilisé pour crypter et décrypter les messages dans une communication où une clé est gardée publique et l'autre clé est privée. C'est le concept de chiffrage asymétrique.

1. Le client demande une ressource protégée au serveur.
2. Le client présente les informations cryptées avec sa clé publique au serveur.
3. Le serveur évalue la requête avec sa clé privée (disponible seulement côté serveur) et répond en retour en rapport avec la ressource demandée par le client.

Cela fonctionnerait de la même manière pour l'authentification mutuelle où le client et le serveur fournissent tous deux leurs clés publiques et déchiffrent leurs messages avec leurs propres clés privées disponibles de leur côté.

### Note

Nous avons déjà configuré `HTTPS` sur un serveur `apache` sous `Ubuntu` lors de d'exercices précédents avec des machines virtuelles. Aujourd'hui nous allons donc travailler sur cette distribution, revoir les étapes de création d'un certificat SSL auto-signé et l'intégration dans une image Docker. Bien entendu, il existe déjà des images toutes prêtes sur `Docker Hub` ... mais nous n'apprendrons rien de nouveau aujourd'hui si nous nous contenterions d'utiliser un existant.



Maintenant, construisons notre container.

Comme nous sommes en local, il nous faudra **autosigner** nos certificats **SSL**.

Stoppons d'abord le container `serveur_http` précédent qui utilise le port `2000` :

```
docker container stop serveur_http
```

Nous allons installer un container avec une image `Ubuntu` et mapper les `ports 80` et `443` de la machine hôte avec les mêmes ports du container.

```
docker run -it -p 80:80 -p 443:443 --name serveur_https ubuntu /bin/sh;
```

Installons un éditeur de texte `nano`, `apache2` notre serveur `http` et `opennss` qui permettra de générer des certificats.

```
apt update  
apt install nano apache2 openssl &y
```

Il faut maintenant démarrer le serveur **Apache**:

```
service apache2 start
```

Testons dans le navigateur : <http://localhost>

Nous voulons un site pour notre équipe de **Esport** : Les *Necromancers* !

Créons donc un dossier spécialement pour eux!

```
mkdir /var/www/html/esport
```

Et créons dedans un fichier **index.html** qui contiendra le code suivant :

```
<h1>Page de test des NECROMANCERS !!</h1>
```

Pour cela nous utiliserons notre éditeur de texte **nano** :

```
nano /var/www/html/esport/index.html
```

Rappel : Pour sauvegarder, tapez au clavier sur les touches **CTRL + O** et **Entrée** et pour quitter **CTRL + X**

Nous allons maintenant modifier notre fichier HOSTS sur la machine hôte afin de forcer la redirection du domaine [necromancers.esport](http://necromancers.esport) sur notre serveur local en cours de conception.

Ouvrez Visual Studio Code ou un autre éditeur comme NotePad++ avec des droits d'administrateur, et éditez le fichier :

```
C:\Windows\System32\drivers\etc\hosts
```

Ajoutez la ligne suivante :

```
127.0.0.1 necromancers.esport
```

Puis modifiez les paramètres du proxy comme suit :

## Configuration manuelle du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Utiliser un serveur proxy



Activé

Adresse

172.16.0.1

Port

3128

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

necromancers.esport;www.necromancers.  
esport

Ne pas utiliser le serveur proxy pour les adresses (intranet) locales

Enregistrer

Ainsi, nous ne passerons pas par le proxy, ni par le DNS pour accéder à notre site avec l'url [necromancers.esport](http://necromancers.esport), mais sur le serveur local d'adresse IP directement: [127.0.0.1](http://127.0.0.1).

Maintenant, il faut configurer **Apache** dans notre container pour que notre URL pointe vers le dossiers WEB du serveur.

**Apache** permet de faire des redirections de connexions entrantes sur un de ses ports vers un dossier de notre choix. Cela se fait grâce aux **VirtualHost**. Copions le fichier **VirtualHost** de base nommé **000-default.conf** et appelons cette copie **esport.conf**.

```
cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/esport.conf
```

Modifions maintenant ce nouveau fichier :

```
nano /etc/apache2/sites-available/esport.conf
```

[image]

Profitons-en aussi pour modifier le fichier [/etc/apache2/apache2.conf](#). Et lui rajouter une ligne : **ServerName localhost**. Cela va permettre de nommer notre serveur local, et d'éviter d'avoir des avertissements au redémarrage.

Le fichier **esport.conf** est prêt ! Il faut le charger dans la configuration du serveur **Apache2**.

```
a2ensite esport
```

Pour que les modifications soient prise en compte, redémarrons le serveur.

```
service apache2 restart
```

Maintenant que notre serveur **Apache** est configuré pour que l'adresse : [necromancers.esport](http://necromancers.esport) pointe vers notre dossier web. ( Testez ! )

Il nous faut installer un certificat pour obtenir une connexion sécurisée en **HTTPS**.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/esport.key -out /etc/ssl/certs/esport.crt
```

Cette commande va créer 2 certificats dans les emplacements : </etc/ssl/private/esport.key> et </etc/ssl/certs/esport.crt>.

Il faut maintenant installer les certificats sur le serveur et les associés à notre domaine.

Copions le fichier de base **default-ssl.conf** et renommons le en **esport-ssl.conf**.

```
cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/esport-ssl.conf
```

Il s'agit simplement d'un **VirtualHost** qui est chargé de rediriger les connexions entrantes provenant du port 443, le port dédié au protocole **HTTPS**.

Editons ce fichier :

```
nano /etc/apache2/sites-available/esport-ssl.conf
```

[image]

Pour tester notre configuration, il faut executer la commande :

```
apachectl configtest
```

Et si tout ce passe bien, la réponse devrait être :

```
# apachectl configtest
Syntax OK
```

Chargeons le module SSL dans apache pour qu'il puisse prendre en compte les connexions HTTPS et les certificats.

```
a2enmod ssl
```

Chargeons aussi le nouveau **VirtualHost** :

```
a2ensite esport-ssl
```

En test l'adresse <https://necromancers.esport> depuis votre navigateur,  
Vous devriez avoir cela :

[image]

Il faut autoriser la connexion au site :

[image]

*Note*

Pourquoi nous avons ce message d'alerte ?



Tout simplement parce que le navigateur a détecté que nous sommes connecté avec le protocole **HTTPS**. Notre serveur lui a fourni un certificat ... qui est ... **autosigné ! Cela alerte donc le navigateur.**

Nous voulons que si l'utilisateur tape **HTTP** dans l'adresse au lieu de **HTTPS** le serveur puisse le rediriger automatiquement.

Activons le mode **rewrite** de Apache qui permet à Apache de réécrire/reformater les URL captées :

```
a2enmod rewrite
```

Et éditons le fichier

```
nano /etc/apache2/sites-available/esport.conf
```

Ajoutons cette règle de réécriture d'url :

```
RewriteEngine On  
RewriteRule ^(.*)$ https:// %{HTTP_HOST} $1 [R=301,L]
```

Redémarrons Apache :

```
service apache2 restart
```

Notre serveur est maintenant correctement configuré !

*Note*



Vous pouvez être fier du travail accompli jusqu'alors ! Et pourquoi ne pas créer une image basée sur cette configuration ? Afin de pouvoir créer une infinité de container avec les même caractéristiques. Cela évitera de recommencer toutes les étapes que nous avons suivies jusqu'alors.

## Création d'une image Docker

Nous avons jusqu'alors créé des containers à partir d'images de bases que nous avons modifié. Il temps de créer notre propre image qui servira de "moule" pour des containers ayant besoin des caractéristiques que nous avons paramétrées.

Mais avant faisons un peu de ménage dans notre container. Supprimons le fichier `index.html` du dossier `/var/www/html/esport`

```
rm /var/www/html/esport/index.html
```

La commande pour créer une nouvelle image à partir d'un container est :

```
docker commit <CONTAINER_ID> <NOM_DE_L_IMAGE>
```

Il nous faut donc récupérer l'identifiant de notre container dans un premier temps :

```
docker ps -a
```

[image]

`Serveur_https` possède bien l'identifiant : `00e15c9f63ea`

Maintenant, nous pouvons créer une nouvelle image à partir de cet identifiant. Nous respecterons les conventions de nommage : `<Nom du constructeur>/<Nom de l'image>:<Numéro de version>`.

Notre image s'appellera alors : `siolaon/https:1.0`.

Lançons la création de l'image avec l'option `-a` pour définir le nom de l'auteur, mettez le votre car vous l'avez bien mérité:

```
docker commit -a Bauer 00e15c9f63ea siolaon/https:1.0
```

Vérifions si l'image a bien été créée en listant les images disponibles sur notre machine hôte.

```
docker images
```

PS C:\Users\p02\Documents\Cours\cours-sio> docker images				
REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
siolaon/https	1.0	5194fd6495e9	45 seconds ago	220MB

Nous pouvons retrouver l'image également dans l'application Docker Desktop, onglet "Images".

Image	Tag	ID	Created	Size
alpine	3.13	6b7b3256dabe	4 months ago	5.62 MB
alpine	3.14	0a97eee8041e	4 months ago	5.61 MB
docker/getting-started	latest	3ba8f2ff0727	12 months ago	27.94 MB
nginx	latest	c316d5a335a5	about 1 month ago	141.5 MB
python	3	70aa8983ec5c	10 months ago	885.71 MB
siolaon/https	1.0	5194fd6495e9	less than a minute ago	220.47 MB
ubuntu	IN USE	7e0aa2d69a15	10 months ago	72.7 MB
ubuntussh	latest	ad162da9cf56	10 months ago	226.06 MB

Stoppons maintenant notre container `serveur_https` :

```
docker container stop serveur_https
```

Maintenant, voici venu le grand moment tant attendu ! Celui de monter notre image, dans un nouveau container avec le dossier web esport !

Positionnons nous dans le répertoire contenant notre dossier `www`, pour ma part:

```
cd C:\Users\baptiste\Documents\docker\td\www
```

```
docker container run -itd --name server_esport -v $PWD/esport:/var/www/html/esport -p 80:80 -p 443:443 siolaon/https:1.0
```

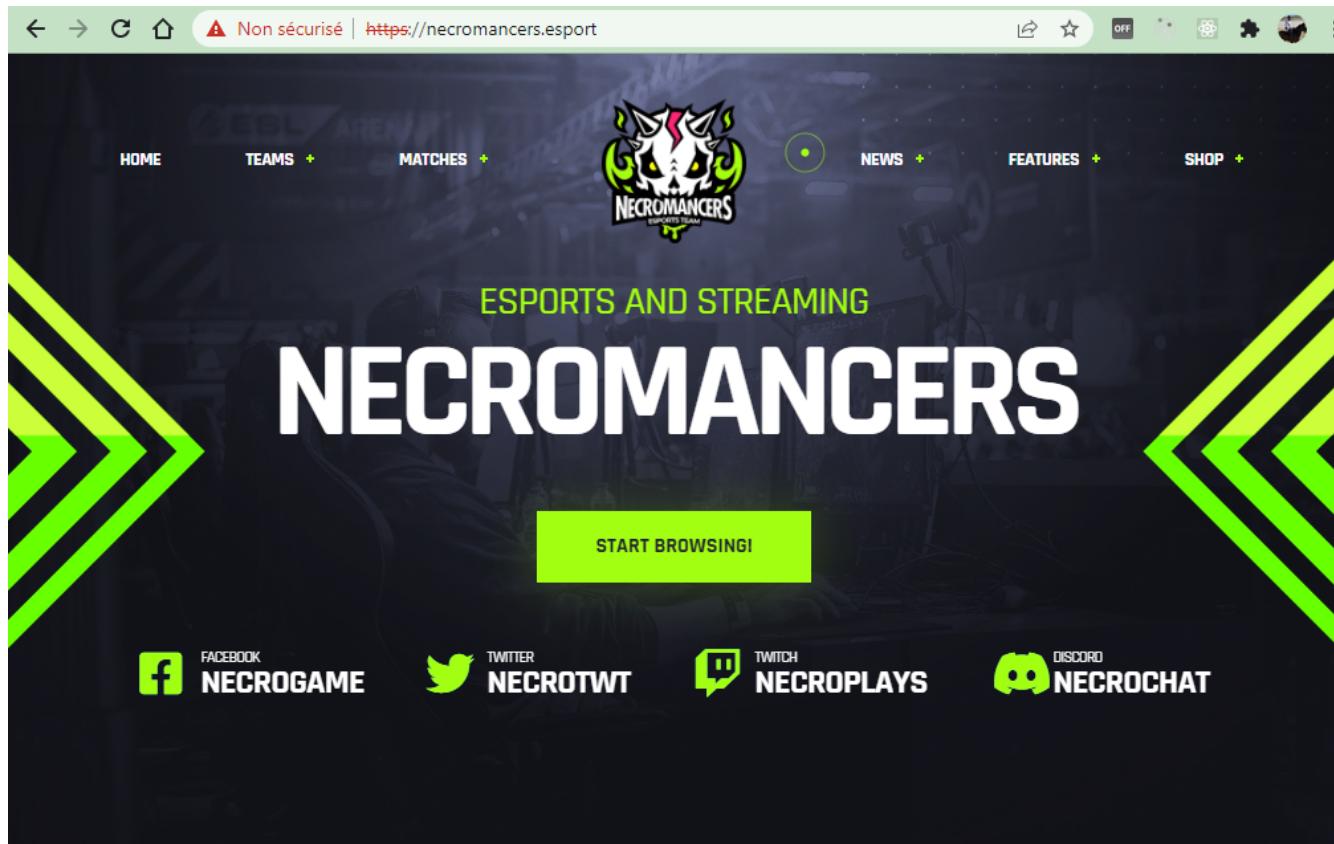
Maintenant il faut lancer le serveur apache2 manuellement depuis le serveur :

```
docker container exec -ti server_esport sh
```

et dans le `shell` lancer la commande :

```
service apache2 start
```

Ouvrez le navigateur et contemplez votre oeuvre :



## 12.3. Crédit à la partie 12

Nous sommes satisfaits du résultat, mais il reste un goût d'inachevé, n'est-ce pas ?

Créer un container à partir de notre image, et devoir lancer la commande `service apache2 start` à partir de son `shell`, demande une manipulation dont on aimerait pouvoir se passer ...

Cela va être possible en créant un fichier `Dockerfile`. Ce fichier contient une liste de commandes à exécuter pour concevoir notre propre image.

Listons les actions effectuées dans la partie 12.2

- Création d'un container avec une image `Ubuntu`.
- Nous avons mis à jour les dépôts `Ubuntu`.
- Nous avons installé `Apache2`.
- Nous avons installé `Nano`.
- Nous avons installé `OpenSSL` et récupéré 2 fichiers : `esport.key` et `esport.crt`.
- Nous avons créé 2 fichiers `VirtualHost` `esport` et `vesport-ssl` pour le site en `http` et `https`.
- Nous avons activé les modules `ssl` et `rewrite` dans `Apache`.
- Nous avons chargé les `VirtualHost` `esport` et `esport-ssl` dans `Apache`.

- Nous avons redémarré **Apache** pour que les modifications soient prises en compte.
- Nous avons lancé **Apache**.

Il va falloir créer un dossier nommé par exemple : **esport\_image**, qui contiendra :

 <b>esport</b>	03/03/2022 15:02	Dossier de fichiers
 <b>Dockerfile</b>	04/03/2022 08:52	Fichier 1 Ko
 <b>esport.conf</b>	03/03/2022 15:06	Fichier CONF 1 Ko
 <b>esport-ssl.conf</b>	03/03/2022 17:04	Fichier CONF 1 Ko

- Notre dossier **esport**, avec dedans les pages html.
- Nos fichiers **VirtualHost** déjà rédigés qui seront ensuite copiés dans **Apache** automatiquement : **esport.conf** et **esport-ssl.conf**.
- Un fichier **Dockerfile**, fichier spécial composé des commandes à envoyer au **Daemon Docker** afin de générer une nouvelle image **Docker** conforme à nos objectifs.



#### *Warning*

Le fichier **Dockerfile** n'a pas d'extension.

Créez 2 fichiers : **esport.conf** et **esport-ssl.conf**. Dont le contenu est :

Fichier : **esport.conf**

```
<VirtualHost *:80>
    ServerName necromancers.esport
    ServerAlias www.necromancers.esport
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/esport
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    RewriteEngine On
    RewriteRule ^(.*)$ https:// %{HTTP_HOST} $1 [R=301,L]
</VirtualHost>
```

Fichier : **esport-ssl.conf**

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName necromancers.esport
    ServerAlias www.necromancers.esport
    DocumentRoot /var/www/html/esport
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/esport.crt
    SSLCertificateKeyFile /etc/ssl/private/esport.key
```

```
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>
</VirtualHost>
```

Maintenant nous allons pouvoir rédiger notre fichier **Dockerfile** :

La première ligne doit contenir l'instruction **FROM** qui définie l'image qui servira de référence. Nous allons construire notre projet autour de la distribution linux **Ubuntu** dans sa dernière version.

```
FROM ubuntu:latest
```

La dernière ligne contiendra l'instruction **CMD**. Il s'agit de la commande à exécuter dès que notre container sera lancé. Nous voulons lancer apache par la commande : **service apache2 start**.

```
CMD ["service", "apache2", "start"]
```

Entre les deux, il faut maintenant programmer la mise en place de notre serveur WEB avec un certificat SSL autosigné et les fichiers de notre projet dedans.

L'instruction **RUN** permet d'établir une liste de commandes à exécuter. Chaque instruction **RUN** créé une couche (layer) dans notre container. Donc au lieu de lancer une instruction **RUN** par commandes, nous allons les chaîner, grâce à l'opérateur logique **&&**.

#### Note

Chainer 2 ou 3 ou 4 commandes peut vite créer une ligne extrêmement longue. Par soucis de lisibilité, il est bien de pouvoir sauter une ligne entre chaque commande. Mais le compilateur qui va se charger de créer l'image ne va pas comprendre, pour l'aider, il faut ajouter un \ après notre opérateur logique.

Exemple : .. code-block:



```
RUN apt install apache2 -y && apt install openssl -y
```

deviendra sur 2 lignes :

```
RUN apt install apache2 -y && \
apt install openssl -y
```

Donc nous aurons une instruction **RUN** qui contiendra toutes les commandes que nous avons saisi.

```
ENV DEBIAN_FRONTEND=noninteractive
RUN apt update && \
    apt install apache2 -y && \
    echo 'ServerName localhost' >> /etc/apache2/apache2.conf && \
    apt install openssl -y && \
    openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/esport.key -out /etc/ssl/certs/esport.crt -subj
"/C=FR/ST=AISNE/L=LAON/O=BTS SIO/OU=IT Department/CN=necromancers.esport" && \
    mkdir /var/www/html/esport
```

Si vous vous rappelez, lorsque nous avons créé nos certificats SSL, il y a eu une série de questions qui nous a été posée. Lors de la création de notre image, nous ne pourrons pas y répondre avec notre clavier, mais seulement grâce au paramètre saisie directement dans la commande : **-subj** **"/C=FR/ST=AISNE/L=LAON/O=BTS SIO/OU=IT Department/CN=necromancers.esport"**.

De même, Apache demande aussi durant son installation de lui donner des informations comme le continent et le pays dans lequel nous sommes. Pour éviter cette question, et nous bloquer durant la création de l'image, nous utiliserons la variable d'environnement **ENV DEBIAN\_FRONTEND=noninteractive**. Grâce à elle, notre système d'exploitation Ubuntu cessera de nous poser des questions, et nous aurons la configuration par défaut des applications que nous installerons.

L'instruction **echo 'ServerName localhost' >> /etc/apache2/apache2.conf** ajoute au fichier de configuration d'Apache la ligne **ServerName localhost** afin de nommer le serveur par défaut.

L'instruction **COPY** va se charger de copier : les fichiers de configuration Apache et HTML dans les bons emplacements du futur container.

```
COPY esport/ ${path}/esport
COPY esport.conf esport-ssl.conf /etc/apache2/sites-available/
```

Il faut maintenant activer les modes **Rewrite** et **SSL** d'Apache, et lui injecter nos fichiers **VirtualHost**.

```
RUN a2enmod ssl && \
    a2enmod rewrite && \
    a2ensite esport && \
    a2ensite esport-ssl
```

L'instruction **EXPOSE** nous permettra de définir les ports utilisés par défaut par le container.

```
EXPOSE 80 443
```

Ainsi, notre fichier **Dockerfile** complet sera ainsi :

```
FROM ubuntu:latest
```

```
ENV DEBIAN_FRONTEND=noninteractive
ENV path /var/www/html/
RUN apt update && \
    apt install apache2 -y && \
    echo 'ServerName localhost' >> /etc/apache2/apache2.conf && \
    apt install openssl -y && \
    openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/esport.key -out /etc/ssl/certs/esport.crt -subj
"/C=FR/ST=AISNE/L=LAON/O=BTS SIO/OU=IT Department/CN=necromancers.esport" && \
mkdir ${path}/esport

COPY esport/ ${path}/esport
COPY esport.conf esport-ssl.conf /etc/apache2/sites-available/

RUN a2enmod ssl && \
    a2enmod rewrite && \
    a2ensite esport && \
    a2ensite esport-ssl

EXPOSE 80
CMD ["service", "apache2", "start"]
```

Nous avons rajouté une variable `ENV` nommée `path` qui nous permet de définir un chemin qui est utilisé plusieurs fois. Cette variable est utilisée grâce à cette notation  `${path}` .

Il est temps maintenant, de créer notre image à partir de notre fichier `Dockerfile`.

Placez vous dans le dossier contenant ce fichier :

Pour ma part mon fichier `Dockerfile`, se trouve dans le dossier :  
`C:\Users\p02\Documents\Cours\docker`

```
cd C:\Users\p02\Documents\Cours\docker
```

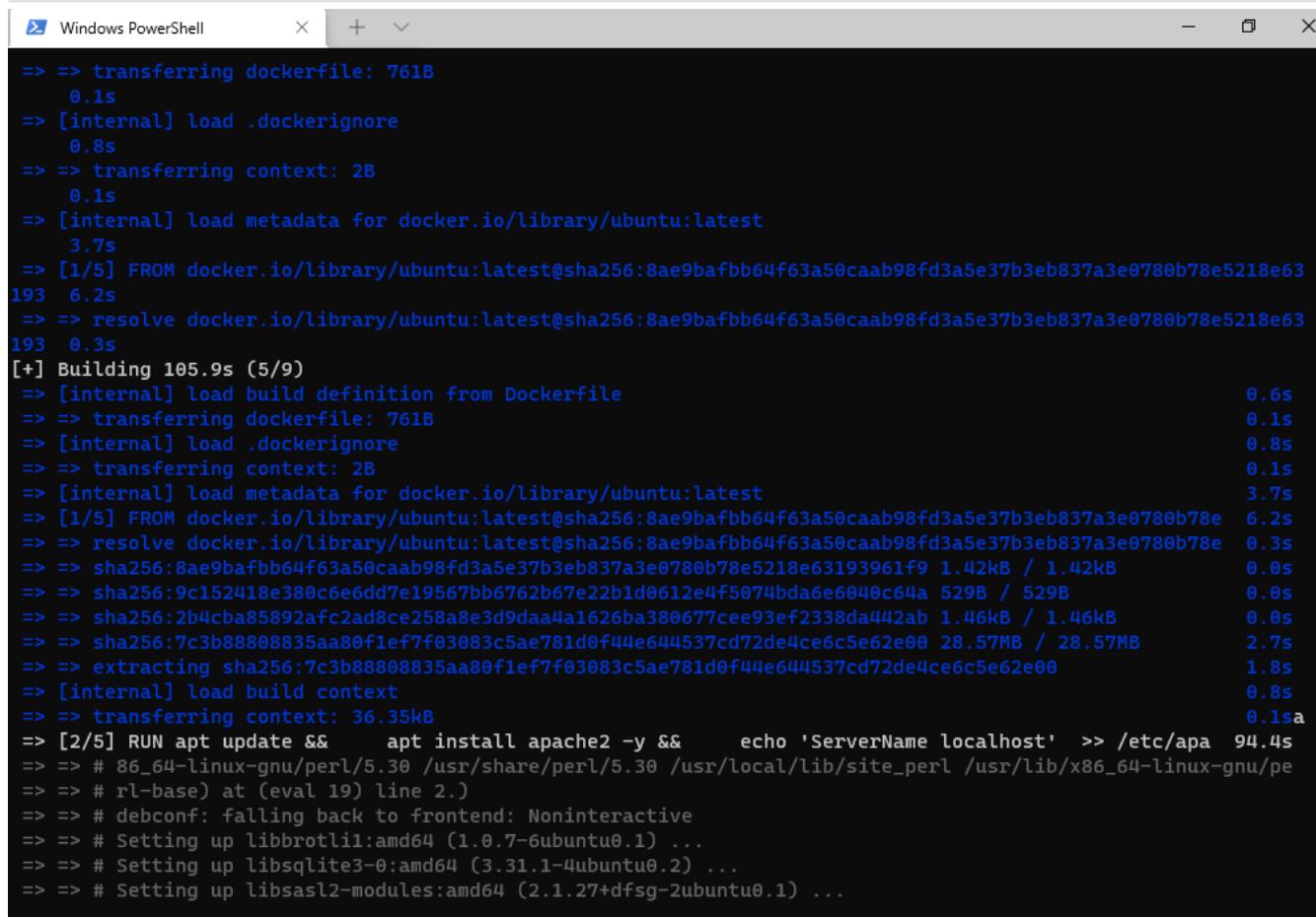
Créons maintenant notre image nommée `esport` dans sa version 1.0. La création peut prendre un certain temps.



*Warning*

N'oubliez pas le ":" !

```
docker image build -t esport:1.0 .
```

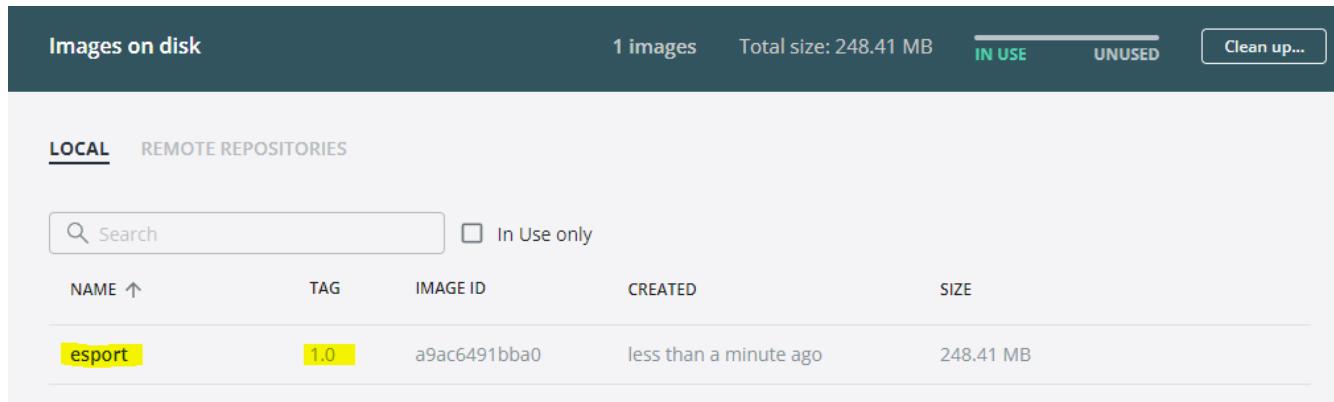


```

>> => transferring dockerfile: 761B
  0.1s
=> [internal] load .dockerignore
  0.8s
=> => transferring context: 2B
  0.1s
=> [internal] load metadata for docker.io/library/ubuntu:latest
  3.7s
=> [1/5] FROM docker.io/library/ubuntu:latest@sha256:8ae9bafbb64f63a50caab98fd3a5e37b3eb837a3e0780b78e5218e63
193  6.2s
=> => resolve docker.io/library/ubuntu:latest@sha256:8ae9bafbb64f63a50caab98fd3a5e37b3eb837a3e0780b78e5218e63
193  0.3s
[+] Building 105.9s (5/9)
=> [internal] load build definition from Dockerfile
=> => transferring dockerfile: 761B
=> [internal] load .dockerignore
=> => transferring context: 2B
=> [internal] load metadata for docker.io/library/ubuntu:latest
=> [1/5] FROM docker.io/library/ubuntu:latest@sha256:8ae9bafbb64f63a50caab98fd3a5e37b3eb837a3e0780b78e 6.2s
=> => resolve docker.io/library/ubuntu:latest@sha256:8ae9bafbb64f63a50caab98fd3a5e37b3eb837a3e0780b78e 0.3s
=> => sha256:8ae9bafbb64f63a50caab98fd3a5e37b3eb837a3e0780b78e5218e63193961f9 1.42kB / 1.42kB 0.0s
=> => sha256:9c152418e380c6e6dd7e19567bb6762b67e22b1d0612e4f5074bda6e6040c64a 529B / 529B 0.0s
=> => sha256:2b4cba85892afc2ad8ce258a8e3d9daa4a1626ba380677cee93ef2338da442ab 1.46kB / 1.46kB 0.0s
=> => sha256:7c3b88808835aa80f1ef7f03083c5ae781d0f44e644537cd72de4ce6c5e62e00 28.57MB / 28.57MB 2.7s
=> => extracting sha256:7c3b88808835aa80f1ef7f03083c5ae781d0f44e644537cd72de4ce6c5e62e00 1.8s
=> [internal] load build context
=> => transferring context: 36.35kB 0.8s
=> [2/5] RUN apt update && apt install apache2 -y && echo 'ServerName localhost' >> /etc/apache2 94.4s
=> => # 86_64-linux-gnu/perl/5.30 /usr/share/perl/5.30 /usr/local/lib/site_perl /usr/lib/x86_64-linux-gnu/pe
=> => # rl-base) at (eval 19) line 2.0
=> => # debconf: falling back to frontend: Noninteractive
=> => # Setting up libbrotli1:amd64 (1.0.7-6ubuntu0.1) ...
=> => # Setting up libssqlite3-0:amd64 (3.31.1-4ubuntu0.2) ...
=> => # Setting up libsasl2-modules:amd64 (2.1.27+dfsg-2ubuntu0.1) ...

```

Notre image apparait bien dans Docker Desktop.



NAME	TAG	IMAGE ID	CREATED	SIZE
esport	1.0	a9ac6491bba0	less than a minute ago	248.41 MB

Maintenant, montons un container basée sur cette image.

Stoppez tout les containers en cours d'exécution afin d'éviter que le port 80 soit déjà utilisé.

```
docker container stop $(docker container ls -q)
```

Puis :

```
docker container run -tid --name site_necroteam -p 80:80 esport:1.0 sh
```

## 12.4. CICD dans un Swarm, avec GitLab et Portainer

Dans cette activité, vous allez mettre en place un pipeline d'intégration continue / déploiement continu en utilisant différents composants : Docker Swarm, GitLab, Portainer



Pour faire cet exercice dans sa totalité, il sera nécessaire de créer une VM accessible depuis internet (étape 4). Pour l'ensemble des cloud providers (Google Compute Engine, Amazon AWS, Packet, Rackspace, DigitalOcean, Scaleway, ...) l'instantiation de VMs est payante (peu cher pour un test de quelques heures cependant). Si vous ne souhaitez pas réaliser la manipulation jusqu'au bout, n'hésitez pas à suivre cet exercice sans l'appliquer, l'essentiel étant de comprendre le flow global.

## 13. Les étapes

Vous allez suivre les différentes étapes ci-dessous :

1. Création, dans le langage de votre choix, d'un serveur web très simple
  2. Ajouter un Dockerfile et création d'une image de l'application
  3. Création d'un répository sur GitLab
  4. Mise en place d'un cluster Swarm
  5. Mise en place d'un pipeline d'intégration continue et déploiement continu
-

# 14. 1ère étape: Crédation d'un serveur web

En utilisant le langage de votre choix, développez un serveur web simple ayant les caractéristiques suivantes: - écoute sur le port 8000 - expose le endpoint / en GET - retourne la chaîne 'Hi!' pour chaque requête reçue.



vous pouvez utiliser l'un des templates ci-dessous, réalisé dans différents langages:

- NodeJs
- Python
- Ruby
- Go
- Java
- .net core

## 14.1. NodeJs

### 14.1.1. Installation

Suivez les instructions suivantes pour installer l'interpréteur NodeJS: [<https://nodejs.org/>](<https://nodejs.org/>)

### 14.1.2. Code source

- index.js

```
var express = require('express');
var app = express();
app.get('/', function(req, res) {
    res.setHeader('Content-Type', 'text/plain');
    res.end("Hi!");
});
app.listen(8000);
```

- package.json

```
{
  "name": "www",
  "version": "0.0.1",
  "main": "index.js",
  "scripts": {
    "start": "node index.js"
  },
  "dependencies": {
    "express": "^4.14.0"
  }
}
```

```
    }  
}
```

### 14.1.3. Installation de expressjs

```
$ npm install
```

## 14.2. Lancement du serveur

```
$ npm start
```

### 14.3. Test

```
$ curl localhost:8000  
Hi!
```

## 14.4. Python

### 14.4.1. Installation

Suivez les instructions suivantes pour installer l'interpréteur Python: <https://www.python.org/downloads/>

### 14.4.2. Code source

- app.py

```
from flask import Flask  
app = Flask(__name__)  
  
@app.route("/")  
def hello():  
    return "Hi!"  
  
if __name__ == "__main__":  
    app.run(host='0.0.0.0', port=8000)
```

- requirements.txt

```
Flask==2.0.2
```

#### 14.4.3. Installation des dépendances

```
$ pip install -r requirements.txt
```

#### 14.4.4. Lancement du serveur

```
$ python app.py
```

#### 14.4.5. Test

```
$ curl localhost:8000  
Hi!
```

### 14.5. Ruby

#### 14.5.1. Installation

Suivez les instructions suivantes pour installer l'interpréteur Ruby:

<https://www.ruby-lang.org/fr/documentation/installation/>

#### 14.5.2. Code source

- app.rb

```
require 'sinatra'  
set :port, 8000  
get '/' do  
  'Hi!'  
end
```

- Gemfile

```
source :rubygems  
gem "sinatra"
```

#### 14.5.3. Installation des dépendances

```
$ bundle install
```

#### 14.5.4. Lancement du serveur

```
$ ruby app.rb -s Puma
```

### 14.5.5. Test

```
$ curl localhost:8000  
Hi!
```

## 14.6. Go

### 14.6.1. Installation

Suivez les instructions suivantes pour installer le compilateur GO: <https://golang.org/doc/install>

### 14.6.2. Code source

- main.go

```
package main

import (
    "io"
    "net/http"
)

func handler(w http.ResponseWriter, req *http.Request) {
    io.WriteString(w, "Hi!")
}

func main() {
    http.HandleFunc("/", handler)
    http.ListenAndServe(":8000", nil)
}
```

### 14.6.3. Lancement du serveur

```
$ go run main.go
```

### 14.6.4. Test

```
$ curl localhost:8000  
Hi!
```

## 14.7. Java / Spring

### 14.7.1. Installation

Suivez les instructions suivantes pour installer le compilateur Java: <https://java.com>

L'application de test est générée depuis [](<https://start.spring.io/>) en utilisant les options suivantes:

![Spring generator](./images/spring-generator.png)

### 14.7.2. Packaging de l'application

```
$ ./mvnw package
```

### 14.7.3. Lancement du serveur

```
$ java -jar target/demo-0.1.jar
```

### 14.7.4. Test

```
$ curl http://localhost:8080/  
hello World
```

## 14.8. DotNetCore

### 14.8.1. Création du projet

Générez un squelette de projet DotNetCore avec la commande suivante:

```
$ dotnet new webapi -o webapi
```

### 14.8.2. Compilation

```
$ cd webapi  
$ dotnet restore  
$ dotnet publish -c Release -o out
```

### 14.8.3. Lancement du serveur

```
$ dotnet out/webapi.dll
```

#### 14.8.4. Test

```
$ curl https://localhost:5000/api/values  
["value1", "value2"]
```

Dans la partie suivante, vous allez packager l'application dans une image Docker.

## 14.9. 2ème étape : Création d'une image Docker

### 14.9.1. Ajout d'un fichier Dockerfile

Ajoutez un Dockerfile à la racine du répertoire contenant le code source du serveur web. Vous servirez ensuite de ce Dockerfile pour créer une image contenant le code de votre application et l'ensemble des dépendances qui sont nécessaires pour la faire tourner.

Vous trouverez ci-dessous des exemples de Dockerfile pour un serveur web écrit dans différents langages.

Important: essayez tout d'abord d'écrire votre propre version du Dockerfile avant d'utiliser l'un de ceux ci-dessous :)

#### 14.9.1.1. Exemple de Dockerfile pour un serveur web écrit en Java

```
FROM openjdk:8-jdk  
COPY . /  
RUN ./mvnw --batch-mode package  
  
FROM openjdk:8-jdk  
COPY --from=0 target/*.jar app.jar  
ENV SERVER_PORT=8000  
ENTRYPOINT ["java", "-Djava.security.egd=file:/dev/.urandom", "-jar", "/app.jar"]  
EXPOSE 8000
```

#### 14.9.1.2. Exemple de Dockerfile pour un serveur web écrit en Python

```
FROM python:3  
COPY . /app  
WORKDIR /app  
RUN pip install -r requirements.txt  
EXPOSE 8000  
CMD python /app/app.py
```

#### 14.9.1.3. Exemple de Dockerfile pour un serveur web écrit en Node.js

```
FROM node:12-alpine
COPY . /app
WORKDIR /app
RUN npm i
EXPOSE 8000
CMD ["npm", "start"]
```

#### 14.9.1.4. Exemple de Dockerfile pour un serveur web écrit en Go

```
FROM golang:1.12-alpine as build
WORKDIR /app
COPY main.go .
RUN CGO_ENABLED=0 GOOS=linux go build -a -installsuffix cgo -o main .

FROM scratch
COPY --from=build /app/main .
CMD ["/main"]
```

#### 14.9.2. Construction de l'image

Une fois que vous avez créé votre Dockerfile, construisez une image, nommé **api** en utilisant la commande suivante:

```
$ docker build -t api .
```

#### 14.9.3. Lancement d'un container

Vérifiez à présent que l'application tourne correctement lorsqu'elle est lancée dans un container (en publiant le port 8000).

```
$ docker run -ti -p 8000:8000 api
```

Vérifiez ensuite que le serveur web est accessible sur le port **8000** depuis la machine locale.

```
$ curl http://localhost:8000
```

Vous pouvez ensuite stopper le container et passer à l'étape suivante.

## 14.10. 3ème étape: repository GitLab

## 14.10.1. 1. GitLab.com

Créez un compte depuis <https://gitlab.com>, ou bien utilisez votre propre compte si vous en avez déjà un.

The screenshot shows the GitLab.com login page. At the top right, there are "Sign in" and "Register" buttons. Below them is a "Username or email" input field and a "Password" input field. There is also a "Remember me" checkbox and a "Forgot your password?" link. A large green "Sign in" button is at the bottom. Below this, there is a "Sign in with" section featuring "Google" and "Twitter" buttons.

GitLab.com offers free unlimited (private) repositories and unlimited collaborators.

- [Explore projects on GitLab.com \(no login needed\)](#)
- [More information about GitLab.com](#)
- [GitLab.com Support Forum](#)
- [GitLab Homepage](#)

By signing up for and by signing in to this service you accept our:

- [Privacy policy](#)
- [GitLab.com Terms](#).

Important: assurez-vous de copier votre clé publique ssh dans la configuration de votre compte GitLab. Dans la suite, cela permettra d'uploader le code de votre serveur sans avoir à renseigner votre login et mot de passe à chaque fois.

## 14.10.2. 2. Création d'un projet

Une fois que vous êtes connecté sur <https://gitlab.com>, créez un nouveau projet en lui donnant le nom que vous souhaitez.

Assurez vous de sélectionner **Public** dans la rubrique **Visibility Level**.

Please ensure your account's recovery settings are up to date.

### New project

A project is where you house your files (repository), plan your work (issues), and publish your documentation (wiki), [among other things](#).

All features are enabled for blank projects, from templates, or when importing, but you can disable them afterward in the project settings.

To only use CI/CD features for an external repository, choose [CI/CD for external repo](#).

Information about additional Pages templates and how to install them can be found in our [Pages getting started guide](#).

**Tip:** You can also create a project from the command line. [Show command](#)

**Blank project**    Create from template    Import project    CI/CD for external

**Project name**: luc-python

**Project URL**: https://gitlab.com/

**Project slug**:

Want to house several dependent projects under the same namespace? [Create a group](#).

**Project description (optional)**

**Description format**

**Visibility Level**

- Private  
Project access must be granted explicitly to each user.
- Public  
The project can be accessed without any authentication.

**Initialize repository with a README**  
Allows you to immediately clone this project's repository. Skip this if you plan to push up an existing repository.

**Create project**

### 14.10.3. 3. Envoi du code de l'application

Suivez les instructions détaillées dans la section **Push an existing folder** afin d'envoyer le code de votre application dans le projet que vous venez de créer.

Dans l'étape suivante, vous allez mettre en place un cluster Docker Swarm dans lequel vous déployerez votre serveur.

## 14.11. 4ème étape: Cluster Swarm

### 14.11.1. Crédation d'un hôte Docker

Vous aurez besoin dans cette partie d'une machine virtuelle accessible depuis Internet. Pour quelques euros vous pourrez par exemple en créer une sur un cloud provider tel que DigitalOcean, OVH, Scaleway, Google Compute Plateform, Amazon AWS, ...

Une fois la VM mise en place, connectez vous sur celle-ci en ssh et installer Docker avec la commande suivante:

```
$ curl https://get.docker.com | sh
```

### 14.11.2. Initialisation d'un cluster Swarm

Initialisez ensuite un Docker Swarm avec la commande suivante:

```
$ docker swarm init
```

Note: si vous obtenez une erreur similaire à: "Error response from daemon: could not choose an IP address to advertise since this system has multiple addresses on interface eth0 (178.62.15.73 and 10.16.0.7) - specify one with --advertise-addr", relancez la commande d'Initialisation en donnant l'adresse IP externe de la VM

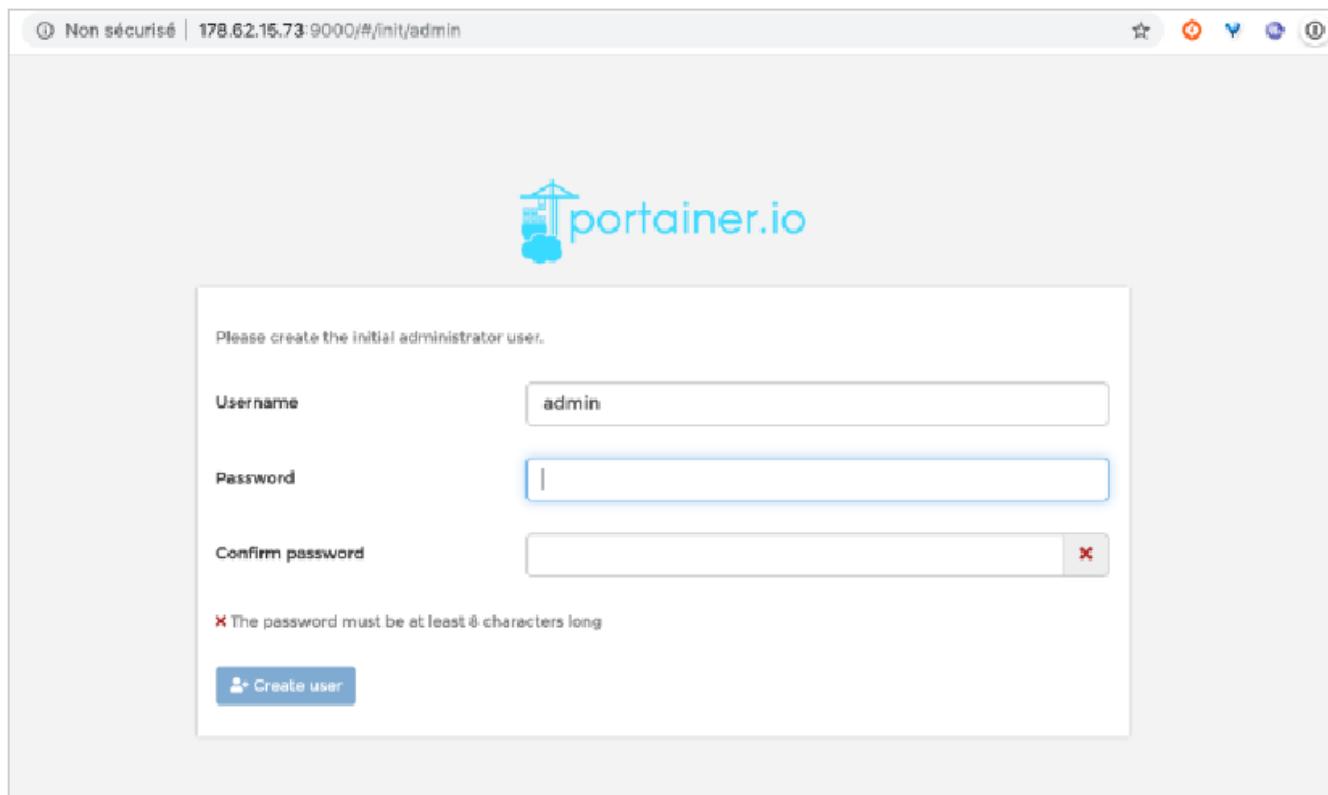
### 14.11.3. Installation de Portainer

Toujours depuis le shell précédent, installez l'outils Portainer en tant que Docker Stack sur le Swarm. Portainer vous permettra de gérer votre Swarm avec une interface web très intuitive.

```
$ curl -L https://downloads.portainer.io/portainer-agent-stack.yml -o portainer-agent-stack.yml  
$ docker stack deploy --compose-file=portainer-agent-stack.yml portainer
```

Vérifiez ensuite que Portainer est bien disponible en lançant un navigateur sur l'adresse suivante:

[http://VM\\_IP\\_ADDRESS:9000](http://VM_IP_ADDRESS:9000)



Suivez les instructions et définissez un mot de passe pour l'utilisateur **admin**. Vous aurez ensuite accès au dashboard de Portainer.

Non sécurisé | 178.62.15.73:9000/#/home

portainer.io

Home

SETTINGS

Extensions

Users

Endpoints

Registries

Settings

portainer.io 1.22.2

Home

Endpoints

Refresh

Search by name, group, tag, status, URL...

primary up 2019-11-17 20:04:34

1 stack 2 services 3 containers - 2 1 1 volume 2 images

No tags

Group: Unassigned

Swarm 19.03.5 + Agent tasks.agent:9001

Items per page 10

Cliquez sur le cluster qui est présenté, vous verrez alors l'ensemble des éléments qui tournent dans le Swarm (seul Portainer est présent pour le moment)

portainer.io

Home

PRIMARY

Dashboard

App Templates

Stacks

Services

Containers

Images

Networks

Volumes

Configs

Secrets

Swarm

SETTINGS

Extensions

Users

Endpoints

Registries

Settings

portainer.io 1.22.2

Dashboard

Endpoint summary

Cluster information

Nodes in the cluster 1

Go to cluster visualizer

1 Stack	2 Services
3 Containers	2 Images
1 Volume	6 Networks

2 running  
1 stopped

94.7 MB

Dans l'étape suivante, vous allez mettre en place un pipeline de CICD

## 14.12. 5ème (et dernière) étape: CICD

### 14.12.1. Utilisation de GitLab CI

A la racine du répertoire contenant les sources de votre projet, créez un fichier `.gitlab-ci.yml` contenant les instructions suivantes:

```
stages:
  - package

push image docker:
  image: docker:stable
  stage: package
  services:
    - docker:18-dind
  script:
    - docker build -t $CI_REGISTRY_IMAGE .
    - docker login -u gitlab-ci-token -p $CI_BUILD_TOKEN $CI_REGISTRY
    - docker push $CI_REGISTRY_IMAGE
```

Ce fichier définit une étape nommée **package** contenant un ensemble d'instructions permettant de builder une image de l'application et de la pusher dans le registry disponible dans GitLab.

Committez votre code et envoyez le dans le repository GitLab:

```
$ git add .gitlab-ci.yml
$ git commit -m 'Add GitLab pipeline'
$ git push origin master
```

Rendez-vous ensuite dans l'interface de GitLab et vérifiez, dans le menu **CI / CD**, qu'un premier pipeline est en train de tourner.

Pipelines

All	1	Pending	0	Running	1	Finished	0	Branches	Tags
Status	Pipeline	Triggerer	Commit	Stages					
<span style="background-color: #00A0A0; color: white; padding: 2px;">running</span>	#966521049	Master - <span style="background-color: #00A0A0; color: white; padding: 2px;">latest</span>	Master - <span style="background-color: #00A0A0; color: white; padding: 2px;">aaef171f6</span>	Add GitLab pipeline	<span style="color: #00A0A0;">●</span>				

Une fois celui-ci terminé, allez dans le menu **Packages** → **Container Registry** et vérifiez que la première image de votre application a bien été construite et qu'elle est disponible dans le registry.

Container Registry

With the Docker Container Registry integrated into GitLab, every project can have its own space to store its Docker images. [More Information](#)

<input type="checkbox"/>	Tag	Tag ID	Size	Last Updated
<input type="checkbox"/>	Latest	e14795f51	337.23 MB	2 minutes ago

![GitLab pipeline](./images/gitlab\_registry\_1.png)

## 14.12.2. Ajout d'un test d'intégration

Dans le fichier `.gitlab-ci.yml`, ajouter une entrée **integration** sous la clé **stage**.

```
stages:  
  - package  
  - integration
```

A la fin du fichier, ajoutez également une nouvelle étape **integration test**:

```
integration test:  
  image: docker:stable  
  stage: integration  
  services:  
    - docker:18-dind  
  script:  
    - docker run -d --name myapp $CI_REGISTRY_IMAGE  
    - sleep 10s  
    - TEST_RESULT=$(docker run --link myapp lucj/curl -s http://myapp:8000)  
    - echo $TEST_RESULT  
    - $([ "$TEST_RESULT" == "Hello World!" ])
```

Cette étape définit un test qui sera effectué sur l'image créée dans l'étape précédente. Ce test très simple s'assure que la chaîne de caractères renvoyée est "Hello World!".

Committez une nouvelle fois le code et envoyez le dans le repository GitLab.

```
$ git add .gitlab-ci.yml  
$ git commit -m 'Add integration step'  
$ git push origin master
```

Depuis l'interface de GitLab, vérifiez qu'un nouveau pipeline a été déclenché. Au bout de quelques dizaines de secondes, vous devriez voir que l'étape **integration** a échoué.

Status	Pipeline	Triggerer	Commit	Stages	Duration	Created At
<span style="color: red;">✖ failed</span>	#96521437	Latest	master => 60482413 Add integration step	<span style="color: green;">✓</span> <span style="color: red;">✖</span>	00:03:38	just now
<span style="color: green;">✔ passed</span>	#96521049		master => aaf171f6 Add GitLab pipeline	<span style="color: green;">✓</span>	00:02:57	3 minutes ago

Vérifiez le contenu des logs de l'étape d'intégration, cela vous permettra de corriger le code. Vous pourrez ensuite commiter ce changement puis l'envoyer dans GitLab. Assurez-vous que le nouveau pipeline déclenché se déroule cette fois-ci sans erreur.

### 14.12.3. Creation d'un service

Vous allez à présent déployer votre application en tant que Service Docker. Utilisez pour cela la commande suivante en remplaçant: - GITLAB\_USER par votre identifiant GitLab - GITLAB\_REPO par le nom de votre projet GitLab

```
$ docker service create \
--name hi \
--publish 8080:8000 \
registry.gitlab.com/GITLAB_USER/GITLAB_REPO:latest
```

Note: le port 8000 du service est publié sur le port 8080 sur le node du cluster Swarm car le port 8000 est déjà utilisé par Portainer.

### 14.12.4. Webhook Portainer

Depuis l'interface de Portainer, assurez-vous que le Service est actif:

Depuis la page de détails du Service, activez le radio button **Service webhook**. Cela va générer une URL sur laquelle pourra être envoyé une requête HTTP POST afin de mettre à jour le Service.

Copiez cette URL et utilisez cette valeur pour la variable **PORTAINER\_WEBHOOK** que vous pourrez créer depuis le menu **Settings > CI / CD**.

The screenshot shows the GitLab interface for managing CI/CD settings. On the left sidebar, under the 'CI / CD' section, the 'Variables' option is selected. The main content area displays two environment variables:

Type	Key	Value	State	Masked	Scope
Variable	PORTAINER_WEBHOOK	b83e-94a705e03fa5	Protected	Masked	All environments
Variable	Input variable key	Input variable value	Protected	Masked	All environments

Below the table are two buttons: 'Save variables' and 'Hide values'. To the right of the table, there is an 'Expand' button. Further down, sections for 'Pipeline triggers' and 'License Compliance' are visible, each with its own expandable sections.

## 14.12.5. Déploiement automatique

L'étape suivante est d'ajouter une phase de déploiement, nommée **deploy** dans le fichier **.gitlab-ci.yml**. Ajoutez cette nouvelle entrée dans la liste **stages**:

```
stages:
  - package
  - integration
  - deploy
```

A la fin du fichier, ajoutez également l'étape **deploy-swarm** qui sera exécutée dans le contexte de cette phase **deploy**:

```
deploy-swarm:
  stage: deploy
  image: alpine:3.9
  script:
    - apk add --update curl
    - curl -XPOST $PORTAINER_WEBHOOK
```

La seule action de cette étape est d'appeler le webhook défini par Portainer en envoyant une requête POST sur l'URL associée au service.

Faites ensuite un changement dans le code de votre application, modifiez par exemple la chaîne de caractères renvoyée (assurez-vous de modifier la description du test en même temps). Commitez ces changements et envoyez le code sur GitLab.

Vérifiez enfin que la nouvelle version de votre application a été correctement déployée.

## 14.13. En résumé

Cet exercice détaille les étapes que l'on peut suivre pour mettre en place un pipeline simple d'intégration continue / déploiement continu (CI/CD). De nombreux éléments pourraient être ajoutés afin d'améliorer ce pipeline...