Docker – Plateforme de containérisation

Présentation « Systèmes Avancés »
Vendredi 15 Février 2019

Docker est un logiciel libre sorti en **2013** qui permet la **containérisation** d'applications.

→ Il a pour but de faciliter la tâche aux développeurs et des administrateurs système en leur assurant le **même fonctionnement** de leurs applications **dans tout les environnements**.

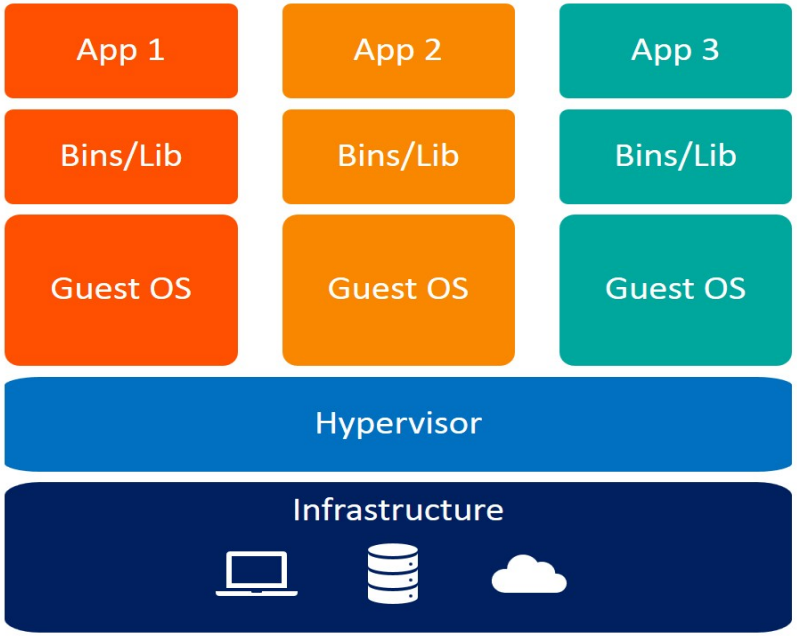
Containérisation

Un **conteneur** est une instance d'une image, c'est-à-dire une **paquet** qui contient tout ce qui est nécessaire pour exécuter une application : le code, les librairies, les variables d'environnement, les fichiers de configuration …

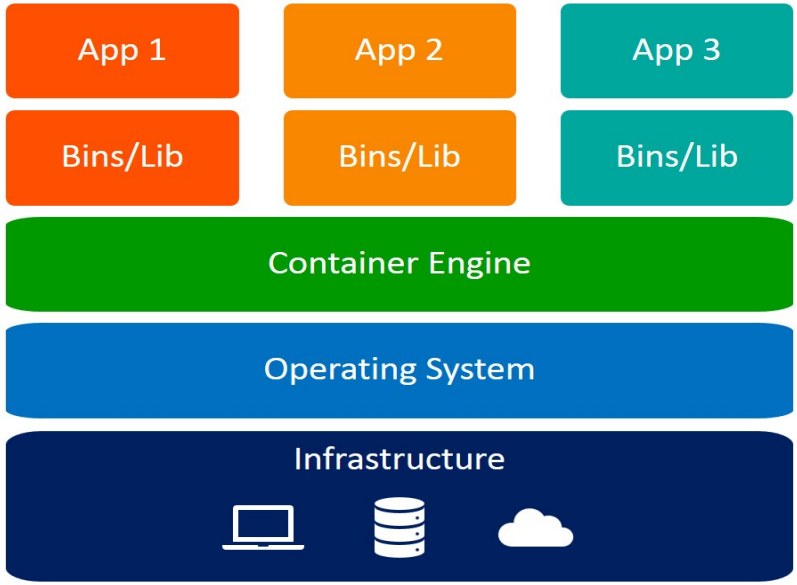
Il permet de **limiter** (et mesurer) **la mémoire** et l'utilisation **CPU** (grâce aux « ***cgroups*** »), et d'isoler l'application (grâce aux « **namespaces** »).

Containérisation VS Virtualisation

Un conteneur **partage** le système d'exploitation de la machine hôte, contrairement à une machine virtuelle, ce qui le rend plus **efficace**.



Virtual Machines



Containers

Controls Group & Namespaces

Les « **cgroups** » sont une fonctionnalité du noyau Linux (tout comme les « namespaces ») qui permet de limiter, mesurer et isoler l'utilisation des ressources (processeur, mémoire, utilisation disque…).

Les « **namespaces** » permettent de limiter ce que peut voir une application de l'environnement. Par exemple : *user, pid, mnt…*

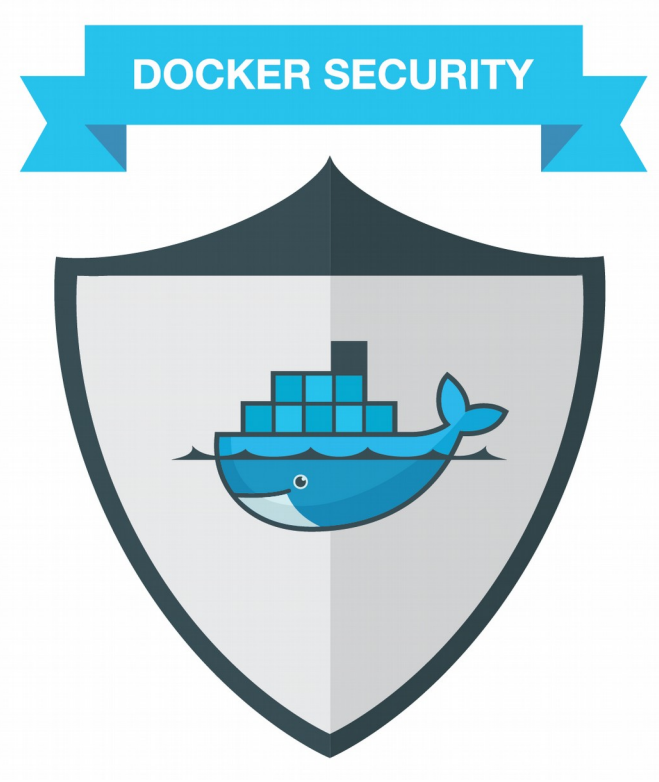
Sécurité

Il y a trois types d'attaques possibles sur Docker :

- une image Docker malveillante
→ *choisir du contenu de confiance*

- une attaque via la machine hôte
→ *maintenir le système à jour*

- une attaque par le réseau
→ *interdire les communications inter-conteneurs.*



Ce qu’il reste à découvrir

- Mieux comprendre comment fonctionnent les conteneurs : comment communiquent-ils avec la machine ? Entre eux ? Et comment sécuriser ces communications ?
- Examiner la librairie *libcontainer* → permet la virtualisation grâce au noyau Linux
- Comment déplacer un conteneur d’une machine à l’autre (en cas de panne d’un serveur par ex.)