



# S'Breaking News

La lettre d'information des bâtisseurs de la défense et de la sécurité de demain

#BuilderException

#139 – 20 novembre 2020

## Les Kata Containers

### Un peu d'histoire...

Apparue dans les années 70s au sein d'IBM, la machine virtuelle, ou **VM** (logiciel affichant le comportement d'une machine physique, exécutant un OS et des applications), est encore massivement utilisée aujourd'hui en milieu professionnel.

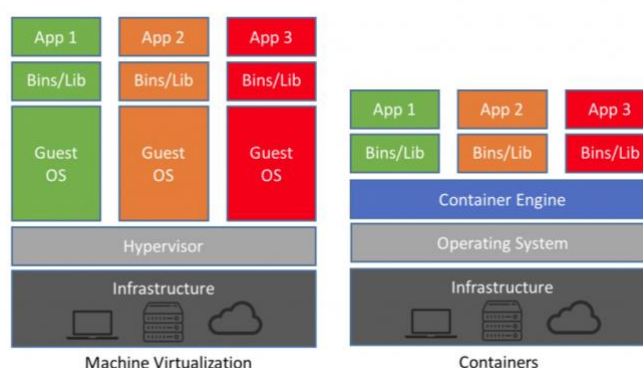
Ce que l'on sait moins, c'est que le concept de **containerisation** (exécution d'une application dans un environnement virtuel), est lui aussi apparu à la fin des années 70s avec l'appel UNIX *chroot*, permettant de fournir un espace disque isolé pour chaque processus. Les containers se sont ensuite progressivement développés et démocratisés, avec notamment l'arrivée des LXC (Linux Containers) en 2008, mais surtout avec l'**émergence de Docker en 2013**.

### VMs vs. Containers

Comme le montre le schéma ci-contre, **chaque VM possède son propre OS**, qui contient lui-même des bibliothèques, qui sont répliquées pour chacune d'entre-elles. L'un des avantages des VMs est qu'elles **peuvent être redimensionnées à tout moment**, en fonction des ressources nécessaires aux applications ou à l'OS invité. De plus, un hyperviseur peut gérer **des dizaines de VMs sur un seul serveur physique**.

Seulement, le problème avec les VMs, c'est qu'elles sont trop **gourmandes** (en ressources :). Chaque VM **exécute une copie complète d'un OS**, mais aussi une **copie virtuelle de tout le matériel** dont l'OS a besoin pour fonctionner.

En revanche, les **containers**, eux, se **partagent l'OS et le noyau de la machine hôte**. De fait, un container sera **plus léger** (il ne contient que les bibliothèques et binaires nécessaires à l'exécution de l'application), et **moins gourmand** en ressources qu'une VM.

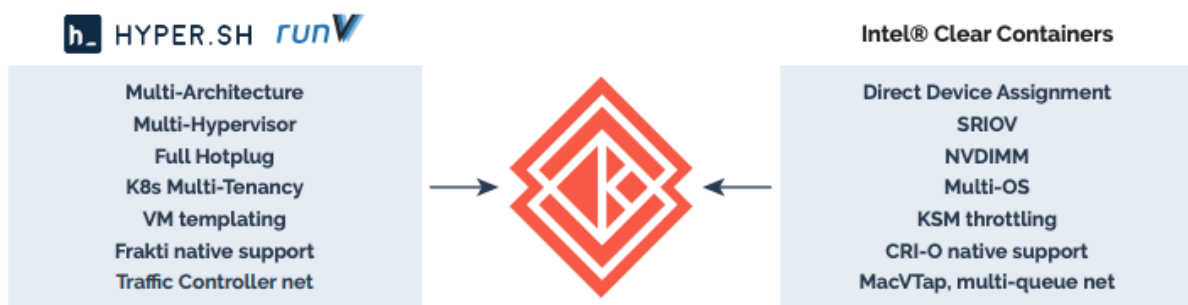
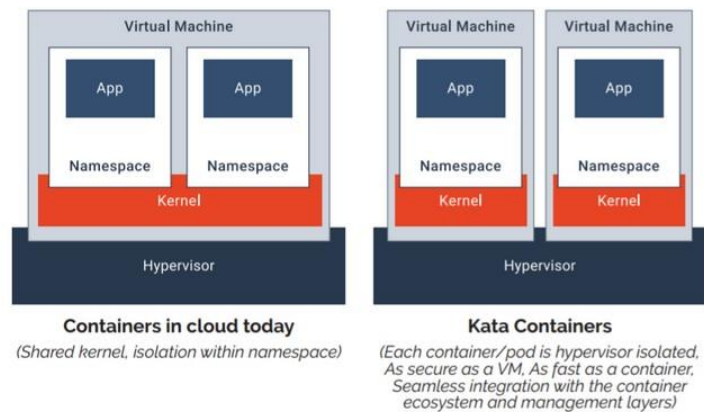


Mais, le problème avec les containers, c'est aussi leur force : leur **isolation au niveau processus**. Les containers partagent tous le noyau de la machine hôte, et **peuvent exposer l'infrastructure sous-jacente**, rendant ainsi **l'environnement plus vulnérable aux attaques**.

### Et si on combinait les deux ?

C'est l'idée derrière **Kata Containers**, un projet open-source à l'initiative de la fondation OpenStack, qui a vu le jour en décembre 2017.





Fusion de deux projets open-source existants, Intel Clear Containers et Hyper runV, Kata Containers rassemble le meilleur des deux technologies et permet ainsi **d'améliorer la sécurité** dans l'écosystème des conteneurs en **ajoutant des VM et des hyperviseurs légers** pour **isoler les charges de travail**.



Le projet, qui s'est rapidement développé, compte désormais parmi ses contributeurs de nombreuses entreprises influentes de la sphère IT, telles que Alibaba, Amazon, Google, Huawei, IBM, Microsoft, Oracle, RedHat, ...

### Et concrètement, ça donne quoi ?

#### Kata Containers Features:

-  **Security** Runs in a dedicated kernel, providing isolation of network, I/O and memory and can utilize hardware-enforced isolation with virtualization VT extensions
-  **Compatibility** Supports industry standards including OCI container format, Kubernetes CRI interface, as well as legacy virtualization technologies
-  **Simplicity** Eliminates the requirement for nesting containers inside full blown VMs
-  **Performance** Delivers consistent performance as standard Linux containers

L'un des principaux avantages des Kata Containers par rapport aux VMs traditionnelles est leur **intégration transparente aux plateformes d'orchestration de containers**, comme Kubernetes.

En effet, l'environnement d'exécution des Kata Containers respecte la **norme OCI** (Open Container Initiative), ce qui les rend **manipulables comme des containers Docker**. Des fonctionnalités telles que la **mise à l'échelle automatique**, ou les **mise à jour progressives**, qui font la force des containers à l'heure actuelle, demeurent donc toujours disponibles.

En somme, les Kata Containers sont **aussi légers et rapides que les containers**, et **s'intègrent parfaitement à leur écosystème**, tout en offrant les **avantages de la sécurité des VMs**.

Bien que l'utilisation des Kata Containers soit encore relativement peu démocratisée en entreprise, le socle technique du projet (Intel Clear Containers & Hyper runV) est lui massivement utilisé.

Baidu, géant de l'Internet chinois, utilise depuis peu Kata Containers en production, à grande échelle (+ de 43 000 cœurs de CPU). Pour les fournisseurs d'infrastructures, et notamment les fournisseurs de Cloud, comme Baidu, l'enjeu est de **garantir à leurs clients qu'ils ne seront pas impactés par les applications infectées d'une autre entreprise**, en **protégeant l'infrastructure hôte**.

---

Il était impératif pour Baidu de trouver comment améliorer l'isolation des conteneurs pour protéger les charges de travail et les données des clients tout en tirant parti de la légèreté et de l'agilité des conteneurs. [...]

Le mode d'isolation parmi les machines virtuelles adopté par Kata Containers garantit non seulement une isolation sûre du conteneur dans un environnement multi-locataire, mais contribue également à rendre l'isolation des machines virtuelles invisible pour les applications et les utilisateurs. [...]

En tant que solution de conteneur sécurisé, Kata Containers joue un rôle essentiel dans les services de conteneur fournis par Baidu en répondant à divers cas d'utilisation des clients [...].

---

Extrait de « The Application of Kata Containers in Baidu AI Cloud »

## Quelques liens

[Le site officiel](#)

[Le dépôt GitHub](#)

[Kata Containers en production – Baidu AI Cloud](#)

Clément LEFEVRE



rm -rf /



CommitStrip.com