

La conteneurisation



Introduction

Les conteneurs sont une solution au problème de la façon dont les logiciels peuvent fonctionner de manière fiable lorsqu'ils sont déplacés d'un environnement informatique à l'autre. Voici ce que vous devez savoir sur cette technologie populaire.

Docker a explosé sur scène en 2013, et cela a causé de l'excitation dans les cercles informatiques depuis. La technologie de conteneur d'application fournie par Docker promet de changer la façon dont les opérations informatiques sont réalisées de la même manière que la technologie de virtualisation quelques années auparavant.

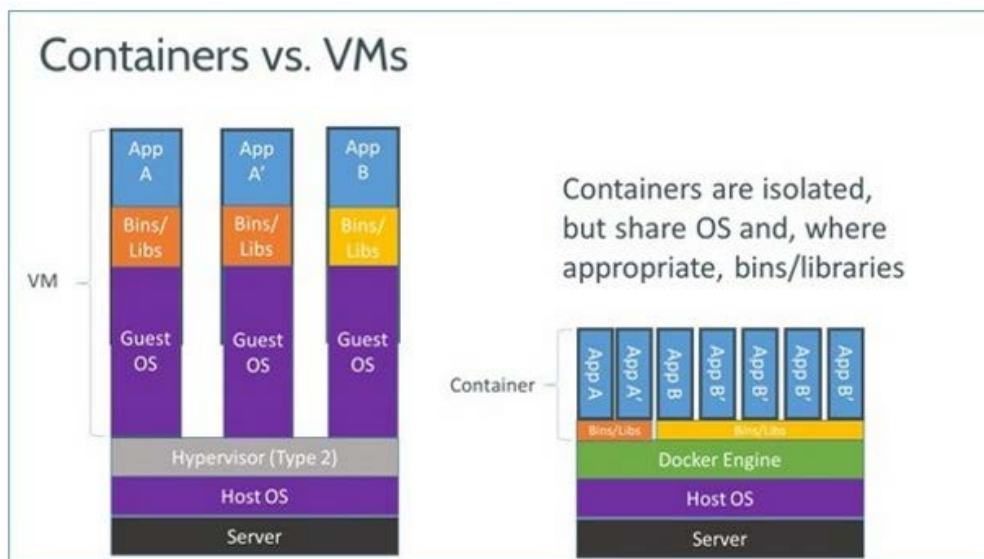
Définition : Les conteneurs

Les conteneurs sont une solution au problème de la façon dont les logiciels peuvent fonctionner de manière fiable lorsqu'ils sont déplacés d'un environnement informatique à l'autre. Cela pourrait être du portable du développeur à un environnement de test, d'un environnement de test à la production, et peut-être d'une machine physique dans un centre de données à une machine virtuelle dans un cloud privé ou public.

Simplement, un conteneur consiste en un environnement d'exécution complet : une application, plus toutes ses dépendances, ses bibliothèques et autres fichiers binaires, ainsi que les fichiers de configuration nécessaires pour l'exécuter, regroupés dans un seul package. En conteneurisant la plate-forme d'application et ses dépendances, les différences dans les distributions du système d'exploitation et l'infrastructure sous-jacente sont abstraites.

Différence entre les conteneurs et la virtualisation

Avec la technologie de virtualisation, le package qui peut être transmis est une machine virtuelle, et comprend un système d'exploitation complet ainsi que l'application. Un serveur physique exécutant trois machines virtuelles aurait un hyperviseur et trois systèmes d'exploitation distincts.



En revanche, un serveur exécutant trois applications conteneurisées avec Docker exécute un seul système d'exploitation et chaque conteneur partage le noyau du système d'exploitation avec les autres conteneurs. Les parties partagées du système d'exploitation sont lues, tandis que chaque conteneur possède son propre support (c'est-à-dire un moyen d'accéder au conteneur) pour l'écriture. Cela signifie que les conteneurs sont beaucoup plus légers et utilisent beaucoup moins de ressources que les machines virtuelles.

Les autres avantages offerts par les conteneurs

Un conteneur peut avoir seulement des dizaines de mégaoctets de taille, alors qu'une machine virtuelle avec son système d'exploitation complet peut avoir plusieurs gigabytes de taille. Pour cette raison, un seul serveur peut accueillir beaucoup plus de conteneurs que les machines virtuelles.

Un autre avantage majeur est que les machines virtuelles peuvent prendre plusieurs minutes pour démarrer leurs systèmes d'exploitation et commencer à exécuter les applications qu'ils hébergent, tandis que les applications conteneurisées peuvent être démarrées presque instantanément. Cela signifie que les conteneurs peuvent être instanciés de manière « juste à temps » lorsqu'ils sont nécessaires et peuvent disparaître lorsqu'ils ne sont plus nécessaires, libérant des ressources sur leurs hôtes.

Un troisième avantage est que la conteneurisation permet une plus grande modularité. Plutôt que d'exécuter une application complexe entière dans un seul conteneur, l'application peut être divisée en modules (tels que la base de données, l'interface avant de l'application, etc.). C'est l'approche dite micro services. Les applications créées de cette manière sont plus faciles à gérer car chaque module est relativement simple et des modifications peuvent être apportées aux modules sans avoir à reconstruire l'application entière. Étant donné que les conteneurs sont si légers, les modules individuels (ou micro services) ne peuvent être instanciés que lorsqu'ils sont nécessaires et sont disponibles presque immédiatement.

Les conteneurs sont-ils sécurisés ?

Beaucoup de personnes pensent que les conteneurs sont moins sécurisés que les machines virtuelles, car s'il existe une vulnérabilité dans le noyau de l'hôte de conteneur, il pourrait fournir une solution aux conteneurs qui le partagent. Cela vaut également pour un hyperviseur, mais comme un hyperviseur offre beaucoup moins de fonctionnalités qu'un noyau Linux, il présente une surface d'attaque beaucoup plus petite.

Mais au cours des deux dernières années, beaucoup d'efforts ont été consacrés au développement de logiciels pour améliorer la sécurité des conteneurs. Par exemple, Docker comprend maintenant une infrastructure de signature permettant aux administrateurs de signer des images de conteneur pour empêcher les conteneurs non approuvés d'être déployés.

Cependant, ce n'est pas nécessairement le cas pour lequel un conteneur approuvé et signé est sécurisé pour être exécuté, car des vulnérabilités peuvent être découvertes dans certains logiciels du conteneur après sa signature. Pour cette raison, Docker offre des solutions de numérisation de sécurité contenant des conteneurs qui peuvent informer les administrateurs si les images contenant des conteneurs présentent des vulnérabilités qui pourraient être exploitées.

Un logiciel de sécurité des conteneurs plus spécialisé a également été développé. Par exemple, Twistlock offre un logiciel qui analyse les comportements attendus d'un conteneur et les processus de « listes blanches », les activités de réseau, telles que les adresses IP et les ports source et destination et même certaines pratiques de stockage, de sorte que tout comportement malveillant ou inattendu peut être signalé.



Une autre société spécialisée dans la sécurité des conteneurs appelée Polyverse prend une approche différente. Il profite du fait que les conteneurs peuvent être démarrés en une fraction de seconde pour relancer les applications conteneurisées dans un bon état connu toutes les quelques secondes afin de minimiser le temps que le pirate exploite une application exécutée dans un conteneur.

Pourquoi les grandes organisations utilisent les conteneurs ?

Plutôt que de dépenser des ressources pour développer des technologies de conteneurs concurrentes, les organisations peuvent se concentrer sur le développement de logiciels supplémentaires nécessaires pour supporter l'utilisation de conteneurs normalisés dans un environnement d'entreprise ou de cloud. Le type de logiciel nécessaire comprend les systèmes d'administration et de gestion des conteneurs et les systèmes de sécurité des conteneurs.

Solutions gratuites de gestion de conteneurs

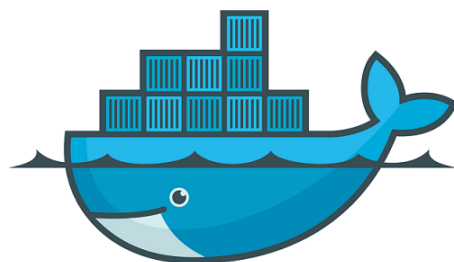
Les systèmes de gestion de conteneurs libres et open source les plus connus et les plus utilisés sont Kubernetes, un projet logiciel issu de Google. Kubernetes fournit des mécanismes de déploiement, de maintenance et de mise à l'échelle des applications conteneurisées.



kubernetes

Solutions commerciales de gestion de conteneurs

Docker Enterprise Edition est peut-être la solution de gestion de conteneurs commerciale la plus connue. Il fournit une plate-forme intégrée, testée et certifiée pour les applications exécutées sur les systèmes d'exploitation Linux ou Windows et les fournisseurs de cloud.



docker

Mais il y en a beaucoup d'autres, et plusieurs d'entre eux ont une couche de logiciel propriétaire construit autour de Kubernetes au noyau. Des exemples de ce type de produit logiciel de gestion comprennent :

- La Tectonic de CoreOS prépare tous les composants open source requis pour construire une infrastructure de style Google et ajoute des fonctionnalités commerciales supplémentaires telles qu'une console de gestion, une intégration SSO d'entreprise et Quay, un registre de contenants prêts à l'entreprise.
- La Plate-forme de conteneur Open Shift de Red Hat est une plate-forme privée sur site comme produit de service, construite autour d'un noyau de conteneurs d'applications alimentés par Docker, avec l'orchestration et la gestion fournies par Kubernetes, sur la base de Red Hat Enterprise Linux.
- Rancher Labs Rancher est une solution open source commerciale conçue pour faciliter le déploiement et la gestion des conteneurs en production sur n'importe quelle infrastructure.

Vers une disparition de la virtualisation ?

C'est peu probable dans un avenir prévisible pour un certain nombre de raisons importantes.

Tout d'abord, il existe toujours une vision largement répandue selon laquelle les machines virtuelles offrent une meilleure sécurité que les conteneurs en raison de l'augmentation du niveau d'isolement qu'elles fournissent.

Deuxièmement, les outils de gestion disponibles pour organiser un grand nombre de conteneurs ne sont pas aussi complets que les logiciels de gestion de l'infrastructure virtualisée, tels que VMware vCenter ou System Center de Microsoft. Il est peu probable que les entreprises qui ont réalisé des investissements importants dans ce type de logiciels souhaitent abandonner leur infrastructure virtualisée sans très bonne raison.

Plus important encore, la virtualisation et les conteneurs sont également considérés comme des technologies complémentaires plutôt que des concurrents. C'est parce que les conteneurs peuvent être exécutés dans des machines virtuelles légères pour accroître l'isolation et donc la sécurité, et parce que la virtualisation matérielle facilite la gestion de l'infrastructure matérielle (réseaux, serveurs et stockage) nécessaire pour supporter les conteneurs.

VMware encourage les clients qui ont investi dans son infrastructure de gestion de machine virtuelle à exécuter des conteneurs sur son distributeur Linux de Photon OS dans des machines virtuelles légères qui peuvent être gérées depuis vCenter. Il s'agit de la stratégie "conteneur dans VM" de VMware.

Mais VMware a également introduit ce qu'il appelle vSphere Integrated Containers (VIC). Ces conteneurs peuvent être déployés directement sur un hôte ESXi autonome ou déployés sur vCenter Server comme s'ils étaient des machines virtuelles. Il s'agit de la stratégie « conteneur en VM » de VMware.

Les deux approches ont leurs avantages, mais ce qui est important, c'est que, plutôt que de remplacer les machines virtuelles, il est souvent utile d'utiliser des conteneurs dans une infrastructure virtualisée.