Bogdan Roxana, sg 1.1

TEMA 2 DATC

Container orchestration. Docker.

Ce sunt containerele?

Containerele software îndeplinesc un rol similar într-o aplicație ca și containerele de tansport. Inițial sunt transportate de un camion într-un port, apoi înglobate cu mii de alte containere de transport maritim pe o navă de containere, însă în niciun moment al călătoriei, conținutul acestui container nu trebuie să fie reambalat sau modificat în nici un fel.

Conținutul fiecărui container este păstrat izolat de cel al celorlalte; recipientul plin de Mentos poate sta în siguranță lângă rezervorul plin de sifon, fără nici un risc de reacție. Odată ce un loc de pe vas a fost rezervat, puteți avea încredere că există spațiu pentru toate încărcăturile ambalate, nu există nici un risc ca un container învecinat să ocupe mai mult decât spațiu decât îi este alocat.

Într-o aplicatie software, ambalarea containerului implică definirea a ceea ce trebuie să fie acolo pentru ca aplicația să funcționeze: sistemul de operare, bibliotecile, fișierele de configurare, binarele de aplicațe și alte părți din stiva de tehnologie. Odată ce containerul a fost definit, acea * imagine* este utilizată pentru a crea containere care rulează în orice mediu, de la laptop-ul dezvoltatorului până la platforma de testare, la centrul de date de producție, local sau în cloud.

Ce este orchestrarea containerelor?

Orchestrarea containerelor este procesul de implementare a containerelor pe un cluster de computere format din noduri multiple. Este un proces care automatizeaza implimentarea prin numeroase caracteristici, incluzând:

- furnizarea de gazed
- instanțiarea unui set de containere
- relansarea containerelor eșuate
- conectarea containerelor prin interfețe
- furnizarea serviciilor la mașinile din afara clusterului
- scalarea clusterului prin adăugarea sau eliminarea containerelor

Aspecte funcționale principale ale orchestrării containerelor:

Gestionarea serviciilor: etichete, grupuri, namespace-uri, verificari de disponibilitate sau încărcare.

Gestionarea resurselor: CPU, memorie, volume, porturi, IP-uri.

La ce foloseste orchestrare containerelor?

DevOps și livrare continuă. Într-o aplicatie ce constă în mai multe containere cu interfețe între ele bine definite este mult mai usor de actualizat un container sau de revenit la o vesiune mai veche. Orchestrare ne scutește de replicarea environment-ului, configuratia completă a aplicatiei se intanțiază în container. De asemeanea, faciliteaza testarea. Mediul de testare este identic cu cel de implementare - până la versiunea exactă a fiecărei biblioteci.

Un alt aspect important ar fi izolarea. Fiecare container care rulează pe aceeași gazdă este independent și izolat de ceilalți, precum și de gazda însăși. Același echipament poate găzdui simultan versiuni de dezvoltare, suport, testare și producție ale aplicației, chiar dacă rulează diferite versiuni de tool-uri, limbaje de programare, baze de date și biblioteci, fără riscul ca un mediu să aibă un impact asupra celuilalt.

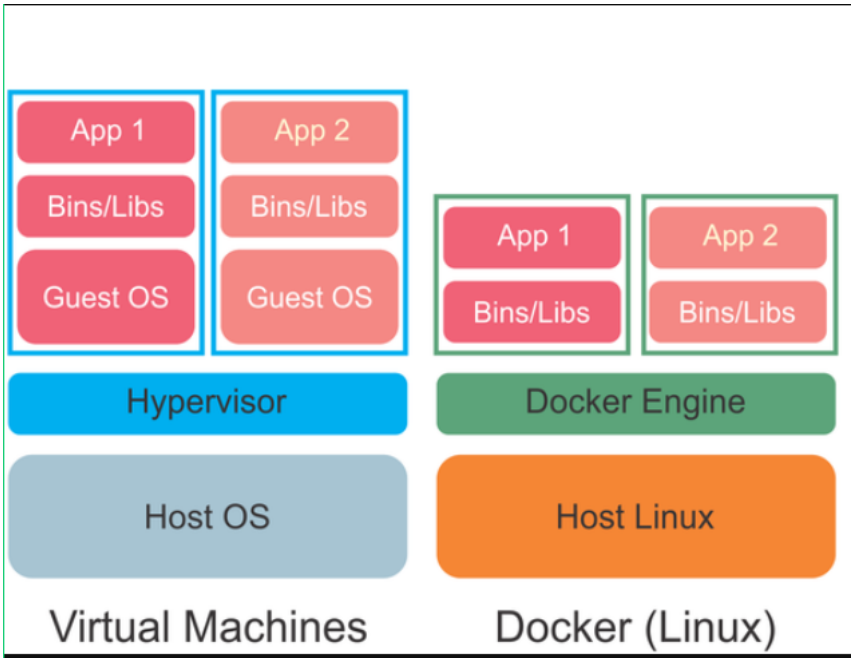
Există multe instrumente de orchestrare disponibile, unele dintre cele mai comune sunt:

- Docker Swarm: Produce o singură gazdă virtuală Docker prin gruparea mai multor gazde Docker împreună. Acesta prezintă același API Docker; permițându-i să se integreze cu orice instrument care funcționează cu o singură gazdă Docker.
- Docker Compose: Efectuează un fișier care definește o aplicație multi-container (inclusiv dependențe) și implementează aplicația descrisă prin crearea containerelor necesare. Este destinată în principal mediilor de dezvoltare, testare și staționare.
- Kubernetes: a fost creat de Google și este unul dintre cadrele de orchestrație bogate în funcții și cele mai utilizate

Ce este docker?

Docker este cea mai populară tehnologie când vine vorba de containere. Docker este un tool open source ce oferă funcționalitate nativă de grupare a containerelor.

Într-un fel, Docker este un fel de mașină virtuală. Dar spre deosebire de o mașină virtuală, Docker permite aplicațiilor să utilizeze același kernel Linux ca și sistemul pe care rulează și cere doar ca aplicațiile să fie livrate cu lucruri care nu se execută deja pe computerul gazdă, fapt ce ofera un plus de performanță si reduce dimensiunea aplicației.



Containerele Docker specifice sunt create din imagini care au fost proiectate pentru a oferi o anumită capacitate. Imaginile Docker sunt construite din sisteme de fișiere cu straturi, astfel încât acestea să poată partaja fișiere comune, reducând utilizarea memoriei și accelerând descărcarea imaginilor.

Este Docker sigur?

Deși trebuie să există problemele legate de utilizarea containerelor în siguranță, dacă acestea sunt utilizate în mod corespunzător, pot oferi un sistem mai sigur și mai eficient decât utilizarea mașinilor virtuale (VM).

Potențiale breșe în securitatea Docker:

- Orice utilizator care are drepturi de root într-un container, are drepturi de root pe gazdă.
- Secretele precum parole, nume de utilizatori sau cheii de API pot fi compromise.
- Imaginile pot fi compromise.
- Expolatarea kernel-ului; spre deosebire de un VM, kernelul este împărțit între toate containerele și gazdă, crescând amploarea oricăror vulnerabilități ce ar putea aparea la nivelui acestuia. În cazul în care un container provoacă o panică a kernel-ului, acesta va elimina întreaga gazdă.
- Dacă un container poate monopoliza accesul la anumite resurse - inclusiv memorie și ID-urile utilizatorilor (UID) - alte containere de pe gazdă pot rămane fără resurse, ducând la o negare a serviciului (DoS).