سفری به اعماق کانتینرها

کانتینرها چه هستند و چرا به آن‌ها نیاز داریم؟

Container که در زبان فارسی محفظه، نگهدارنده یا کانتینر ترجمه می‌شود، مبحثی است که به‌تازگی اهمیت بیشتری پیدا کرده است. کانتینر یک فناوری است که مشکلات انتقال نرم‌افزار از یک محیط به محیط دیگر را حل می‌کند.

داکر (Docker) یکی از کانتینرهایی است که در سال 2013 به وجود آمد و یکی از جذاب‌ترین مباحث حوزه فناوری اطلاعات از ابتدا تا کنون بوده است. کانتینر که توسط داکر ارائه شد، نحوه به‌کارگیری فناوری مجازی‌سازی را دست‌خوش تغییر ساخت. بر همین اساس، در این مقاله در نظر داریم به 13 پرسش رایجی پاسخ دهیم که درباره کانتینرها مطرح شده است.

کانتینرها چه هستند و چرا به آن‌ها نیاز داریم؟

زمانی که نرم‌افزاری از یک محیط به محیطی دیگر منتقل می‌شود، ممکن است در اجرای آن مشکلاتی به وجود آید. کانتینر راه حلی برای مشکل اجرای نرم‌افزار به‌دلیل تغییر محیط اجرا است. این تغییر ممکن است از لپ‌تاپ یک توسعه‌دهنده به یک محیط آزمایشی، از یک ماشین فیزیکی در یک مرکز داده به یک ماشین مجازی در ابر خصوصی یا عمومی یا مواردی از این دست باشد.

سالومون هایکس سازنده داکر می‌گوید: «مشکل زمانی به وجود می‌آید که محیط نرم‌افزاری فعلی و مرجع با یکدیگر یکسان نباشند. شما از پایتون نسخه 2.7 برای سنجش کارتان استفاده می‌کنید. اما پس از تولید، محصول روی پایتون نسخه 3 اجرا می‌شود و اتفاقات پیش‌بینی‌ناپذیر و عجیب و غریب رخ می‌دهند. همچنین، ممکن است کار شما بر پایه نسخه خاص کتابخانه SSL باشد یا سنجش در لینوکس دبیان باشد، ولی محل اجرای نهایی در لینوکس Red Hat باشد. طبیعی است که ممکن است مشکلات زیادی به وجود آیند.»

وی اضافه کرد: «البته همه مشکلات ممکن است به‌دلیل تفاوت در نرم‌افزارها نباشند. ممکن است توپولوژی شبکه متفاوت باشد یا سیاست‌های امنیتی و ذخیره‌سازی مغایر باشند، ولی نرم‌افزار باید روی آن اجرا شود.»

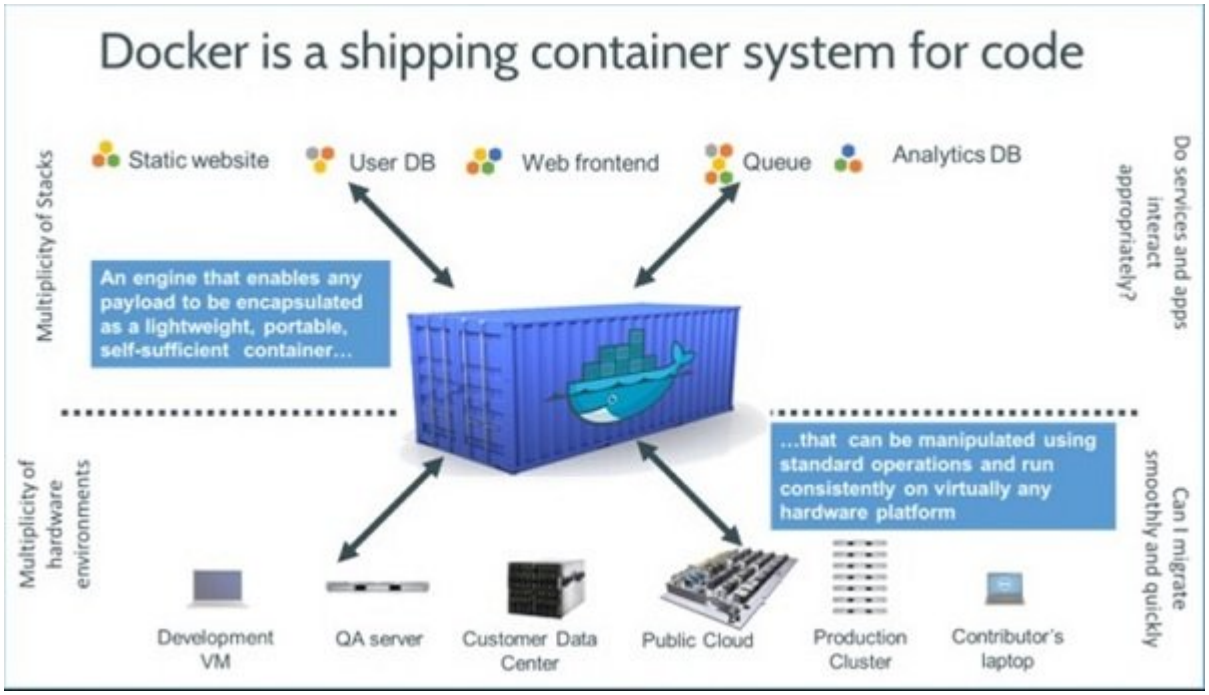
چگونه کانتینرها مشکل ذکر شده را برطرف می‌کنند؟

به صورت ساده، یک کانتینر شامل تمام مواردی است که برای زمان اجرا نیازمند آن‌ها هستیم؛ یک اپلیکیشن و تمام وابستگی‌های آن، کتابخانه‌ها و فایل‌های پیکربندی وغیره. موارد گفته شده به‌عنوان یک پکیج بسته‌بندی می‌شوند. با این کار، دیگر تفاوت در سیستم عامل و زیرساخت‌ها برای اپلیکیشن احساس نمی‌شود.

چه تفاوتی بین مجازی‌سازی و کانتینرها وجود دارد؟

در فناوری مجازی‌سازی پکیج مورد نظر که بدون مشکل قابل انتقال است، یک ماشین مجازی است و شامل تمام سیستم عامل‌ها و برنامه‌ها است. یک سرور فیزیکی که سه ماشین مجازی را اجرا می‌کند، به یک Hypervisor نیاز

دارد که سه سیستم عامل مجزا روی آن اجرا شوند. (Hypervisor یک مدل از مجازی‌سازی سخت‌افزاری است که امکان اجرا و استفاده چند سیستم عامل از یک سخت‌افزار را فراهم می‌کند.)
در مقابل، کانتینرها را داریم که در آن یک سرور می‌تواند سه اپلیکیشن را با استفاده از داکر روی یک سیستم عامل اجرا کند و هر کانتینر هسته سیستم عامل (OS kernel) را با دیگری تقسیم می‌کند. قسمت‌های تقسیم شده سیستم عامل فقط خواندنی (Read only) هستند، در حالی که هر کانتینر برای نوشتن روش دسترسی خود را دارد. یعنی در مقایسه با ماشین مجازی، استفاده از کانتینرها سبک‌تر است و استفاده کمتری از منابع می‌کند. (شکل 1)



کانتینرها چه مزایای دیگری دارند؟

یک کانتینر ممکن است تنها چند ده مگابایت حجم داشته باشد، در حالی که ماشین مجازی با سیستم عاملش ممکن است چند گیگابایت فضا را اشغال کند. به همین دلیل، یک سرور می‌تواند میزبان تعداد بیشتری کانتینر نسبت به ماشین مجازی باشد.
مزیت بزرگ دیگر این است که در یک ماشین مجازی بوت شدن سیستم عامل و شروع به کار اپلیکیشن‌ها ممکن است چند دقیقه به طول انجامد، در حالی که یک اپلیکیشن کانتینر شده خیلی سریع می‌تواند آغاز به کار کند. این به آن معنا است که کانتینرها زمانی که به آن‌ها نیاز داشته باشیم سریع ظاهر می‌شوند و زمانی که نیاز نباشند، در لحظه محو می‌شوند و منابع را آزاد می‌کنند.
سومین مزیت قابلیت ماژولار بودن کانتینر است. به‌جای اینکه تمام اپلیکیشن پیچیده در یک کانتینر قرار گیرد، می‌تواند به چند ماژول تقسیم شود (مانند پایگاه داده، اپلیکیشن front-end و امثال آن). این روش به‌اصطلاح میکروسرویس نامیده می‌شود. اپلیکیشن‌هایی که بدین روش ساخته می‌شوند، به‌راحتی مدیریت می‌شوند. زیرا هر ماژول کوچک‌تر و ساده‌تر است و تغییرات فقط روی یک ماژول انجام می‌شود و نیازی به بازسازی کل اپلیکیشن نیست. به‌دلیل سبک بودن کانتینرها، هر ماژول می‌تواند هر زمان که نیاز باشد سریع به کار گرفته یا غیرفعال شود.

مطلب پیشنهادی

توصیه‌هایی برای توسعه‌دهندگان
اگر تازه قصد استفاده از Container را دارید به این توصیه‌ها توجه کنید

تفاوت بین داکر و کانتینرها در چیست؟

تعریف داکر شباهت زیادی با فناوری کانتینر دارد و بیشترین تأثیر در محبوبیت کانتینرها را خود داکر داشته است. اما فناوری کانتینر یک موضوع جدید نیست و در لینوکس در طی ده سال گذشته به‌شکل LXC ساخته شده است. همچنین، مجازی‌سازی سطح سیستم عامل توسط AIX Workload Partitions، FreeBSD jails و Solaris Containers ارائه شده است.

آیا فرمت و قالب استاندارد برای کانتینر وجود دارد؟

در سال 2015 یک شرکت به‌نام CoreOS یک کانتینر به‌نام ACI با مشخصاتی تولید کرد که با مشخصات داکر متفاوت بود. در آن زمان این ریسک وجود داشت که با استفاده از این کانتینر مشکلاتی با دیگر کانتینرهای لینوکس به وجود آید.

اما در همان سال در یک نوآوری پروژه OCP معرفی شد و بعداً به OCI (سرنام Open Container Initiative) تغییر نام داد. هدف OCI به وجود آوردن استانداردهای صنعتی برای فرمت کانتینر و نرم‌افزار زمان اجرای کانتینر برای تمام سکوها است. نقطه شروع OCP از فناوری داکر شروع شد و داکر 5 درصد از کد منبعش را در اختیار OCP قرار داد تا اطلاعاتش را درون کدها تعبیه کند.

اسپانسرهای این پروژه خدمات وب آمازون، گوگل، IBM، اچ‌پی، مایکروسافت، Red Hat، VMware، اوراکل، توئیتر و همچنین داکر و CoreOS هستند.

چرا تمام این شرکت‌ها درگیر پروژه OCI هستند؟

هدف OCI این است که مطمئن شود ساختارهای بنیادی فناوری کانتینر (مانند فرمت آن) استاندارد هستند و بنابراین همه می‌توانند از مزایای آن استفاده کنند. این بدان معنا است که به‌جای مصرف منابع برای رقابت در توسعه فناوری‌های کانتینر، سازمان‌ها می‌توانند نرم‌افزار مکملی را توسعه دهند که برای حمایت از کانتینرهای استاندارد شده (در سازمان‌ها یا محیط‌های ابری) مورد نیاز است. نرم‌افزارهای مورد نیاز می‌تواند در حوزه سیستم‌های مدیریتی، هماهنگی کانتینر و سیستم‌های امنیتی کانتینر باشد.

آیا سیستم‌های مدیریت کانتینر به‌صورت رایگان و متن باز وجود دارد؟

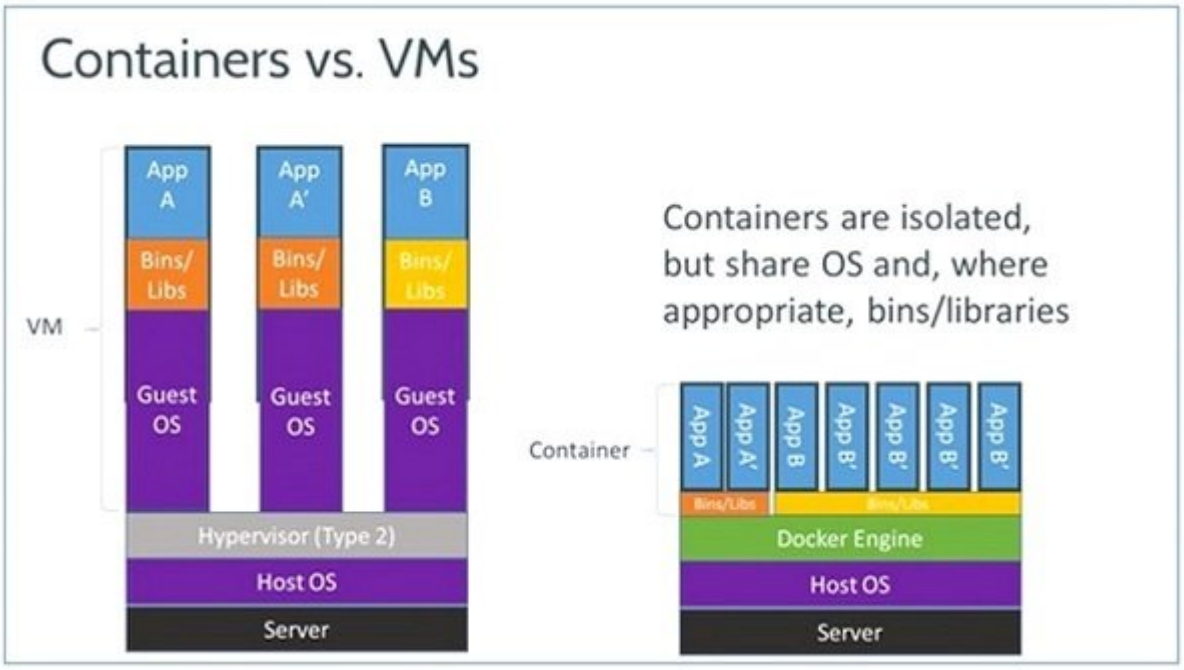
بله، احتمالاً معروف‌ترین و پرکاربردترین سیستم مدیریت کانتینر پروژه نرم‌افزاری Kubernetes است که از گوگل آغاز شد. Kubernetes مکانیسم‌هایی برای توسعه، نگهداری و مقیاس‌پذیری اپلیکیشن‌های کانتینر شده فراهم می‌کند.

چه راه حل‌های تجاری برای مدیریت کانتینر وجود دارند؟

نسخه Enterprise داکر احتمالاً بهترین راه حل مدیریت کانتینر از نوع تجاری است. این مورد یک سکوی یکپارچه، تست شده و تأیید شده برای اپلیکیشن‌هایی ارائه می‌دهد که روی سیسم عامل‌های لینوکس یا ویندوز Enterprise و فراهم‌کنندگان ابر اجرا می‌شوند.

البته تعداد آن‌ها بسیار است و برخی از آن‌ها لایه نرم‌افزاری اختصاصی اطراف Kubernetes در هسته دارند. نمونه‌هایی از این محصولات نرم‌افزاری مدیریتی در زیر آورده شده است:

- **Tectonic** که محصول شرکت CoreOS است که در ابتدا تمام بخش‌های متن باز مورد نیاز برای ایجاد یک زیرساخت به سبک گوگل را بسته‌بندی می‌کند و سپس خصیصه‌های تجاری دیگری اضافه می‌کند مانند یک کنسول مدیریتی، یکپارچگی SSO و همچنین Quay.
- **Open Shift Container Platform** محصول Red Hat یک سکو به‌عنوان سرویس (PaaS) خصوصی است. OpenShift در لینوکس Red Hat از نوع Enterprise ساخته می‌شود و پیرامون کانتینر اپلیکیشنی قرار می‌گیرد که بر پایه داکر است و هماهنگی و مدیریت آن توسط Kubernetes انجام می‌شود.
- **Rancher** محصول Rancher Lab است و یک راه حل متن باز تجاری است. Rancher به این دلیل طراحی شده است که مدیریت و گسترش کانتینرها را در محصولات هر زیرساختی ساده‌تر می‌کند.



کانتینرها چقدر امنیت دارند؟

اغلب مردم اعتقاد دارند که کانتینرها به اندازه ماشین‌های مجازی امن نیستند به دلیل اینکه اگر به هسته میزبان کانتینر نفوذ شود، می‌توان راهی از داخل کانتینر پیدا و آن را به بیرون ارسال کرد. این قضیه درباره Hypervisor هم صادق است، اما به دلیل اینکه Hypervisor امکانات بسیار کمتری نسبت به هسته لینوکس فراهم می‌کند، کمتر در معرض خطر است. (هسته معمولاً فایل سیستم، شبکه‌سازی، کنترل پردازش برنامه وغیره را پیاده‌سازی می‌کند.) در دو سال گذشته تلاش‌های بسیاری صورت گرفته است تا نرم‌افزارهایی گسترش پیدا کنند که امنیت کانتینرها را افزایش دهند. برای مثال، داکر (و دیگر سیستم‌های کانتینر) در حال حاضر یک زیرساخت بر پایه امضا دارند که به ادمین‌ها اجازه می‌دهد کانتینر را امضا کنند و با این کار از گسترش کانتینرهای نامعتبر جلوگیری شود. اما لزوماً همیشه مشکل مربوط به بحث اعتماد و امضا نیست. زیرا ممکن است آسیب‌پذیری‌ها در برخی نرم‌افزارها بعد از امضا کشف شوند. به همین دلیل، داکر و دیگر ارائه‌کنندگان کانتینر به فکر پیدا کردن راه حلی افتادند که ادمین‌ها از وجود آسیب‌پذیری‌ها مطلع شوند.

نرم‌افزارهای خاصی نیز برای امنیت کانتینر گسترش یافته‌اند. برای مثال Twistlock باعث می‌شود نرم‌افزار رفتارهای قابل انتظار، پردازش فهرست سفید، فعالیت‌های شبکه (مانند آی‌پی و پورت مقصد و مبدأ) و حتی فعالیت‌های ذخیره‌سازی را در قالب پروفایل انجام دهد. در نتیجه، هر رفتار بدخواهانه یا غیرمنتظره قابل شناسایی است.

یکی دیگر از کمپانی‌های مخصوص تأمین امنیت کانتینرها به‌نام Polyverse ایده دیگری را به کار گرفته است. این کمپانی از این مزیت کانتینر که اپلیکیشن در کسری از ثانیه مجدد می‌تواند شروع به کار کند، استفاده کرده است. این کار باعث می‌شود هکر فرصت زیادی برای اجرای اپلیکیشن خود در کانتینر نداشته باشد.

سومین مزیت قابلیت ماژولار بودن کانتینر است. به‌جای اینکه تمام اپلیکیشن پیچیده در یک کانتینر قرار گیرد، می‌تواند به چند ماژول تقسیم شود (مانند پایگاه داده، اپلیکیشن front-end و امثال آن). این روش به‌اصطلاح میکروسرویس نامیده می‌شود

کدام توزیع لینوکس به‌عنوان میزبان برای کانتینر مناسب است؟

توزیع‌های لینوکسی که خواهان میزبان کانتینرها هستند باید سبک باشند. به همین دلیل، برخی توزیع‌های مخصوص برای اجرای کانتینرها به وجود آمده است. برای مثال:

- **Container Linux** که قبلاً لینوکس CoreOS نامیده می‌شد، یکی از اولین سیستم عامل‌های سبک بود که برای کانتینرها به وجود آمد.
- **RancherOS** یک توزیع لینوکسی ساده شده است که با هدف اجرای کانتینرها ساخته شده است.
- **Photon OS** یک میزبان لینوکسی برای کانتینر است که برای اجرا روی سکوی VMware بهینه شده است.
- **Project Atomic Host** نام سیستم عامل سبک Red Hat برای کانتینرها است که نسخه‌هایی بر پایه ContOS

و فدورا دارد. همچنین، یک نسخه Enterprise در لینوکس Red Hat Enterprise دارد.
• **Ubuntu Core** کوچک‌ترین نسخه اوبونتو است و هسته آن به‌عنوان سیستم عامل میزبان برای دستگاه‌های اینترنت اشیا و توسعه کانتینر ابری در مقیاس بزرگ طراحی شده است.

آیا کانتینرها برای ویندوز نیز وجود دارند؟

علاوه بر اجرای داکر بر روی توزیع‌های لینوکسی که هسته لینوکس نسخه 3.10 یا بالاتر دارند، داکر روی ویندوز هم اجرا می‌شود. در سال 2016 قابلیتی در ویندوز 10 و ویندوز سرور 2016 ایجاد شد که بتوان کانتینرهای ویندوزی را اجرا کرد. کانتینرهای داکری که برای ویندوز طراحی شده‌اند، قابلیت مدیریت توسط هر مشتری داکر یا PowerShell مایکروسافت را دارند. مایکروسافت کانتینرهای Hyper-V را معرفی کرد که در واقع کانتینرهای ویندوزی هستند که روی ماشین مجازی Hyper-V اجرا می‌شوند.
کانتینرهای ویندوز می‌توانند به‌صورت نصب استاندارد به کار گرفته شوند. (نصب خطی در Server Core یا نصب در نانو سرور که به‌طور خاص برای اجرای اپلیکیشن‌ها در کانتینرها یا ماشین‌های مجازی طراحی شده است.)
علاوه بر لینوکس و ویندوز، داکر روی سکوهای ابری محبوب مانند EC2 آمازون، Compute Engine گوگل، آژور مایکروسافت و Rackspace اجرا می‌شود.

آیا کانتینرها درنهایت به‌طور کامل جایگزین مجازی‌سازی (سرور) می‌شوند؟

طبق پیش‌بینی‌ها این اتفاق به احتمال زیاد و طبق دلایل زیر اتفاق نخواهد افتاد:
اول از همه در حال حاضر توجهات بیشتر به‌سمت ماشین‌های مجازی است، زیرا امنیت بالاتری دارند و سطح ایزوله شدن بالاتری را فراهم می‌کنند. دوم، ابزارهای مدیریتی که برای هماهنگی تعداد زیاد کانتینرها وجود دارند همانند نرم‌افزارهای مدیریتی در زیرساخت مجازی‌سازی (مانند VMware، vCenter یا System Center مایکروسافت) جامع نیستند. شاید فناوری‌های مجازی‌سازی و کانتینرها به وجود آمده‌اند تا مکمل یکدیگر باشند، نه اینکه با یکدیگر رقابت کنند. علت این حرف این است که کانتینرها می‌توانند بر روی ماشین‌های مجازی اجرا شوند تا امنیت و ایزوله شدن بیشتری داشته باشند. در طرف دیگر مجازی‌سازی با پشتیبانی از کانتینرها می‌تواند راحت‌تر زیرساخت سخت‌افزاری (شبکه‌ها، سرورها و ذخیره‌سازی) را مدیریت کند. VMware مشتریان خود را که در زیرساخت مدیریتی ماشین مجازی سرمایه‌گذاری کرده‌اند تشویق می‌کند تا کانتینرها را روی سیستم عامل فوتون در یک ماشین مجازی سبک اجرا کنند و آن را vCenter مدیریت کنند. اما VMware کانتینرهایی تحت عنوان VIC (سرنام vSphere Integrated Containers) ارائه داده است و این کار را استراتژی «کانتینر به‌عنوان ماشین مجازی» می‌داند.
هر دو روش مزایای خود را دارند، اما چیزی که اهمیت دارد این است که به‌جای اینکه کانتینرها را جایگزین ماشین مجازی کنیم، از زیرساخت آن در کنار کانتینرها بهره ببریم

تاریخ انتشار:

31 شهریور 1396

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/9383/%DA%A9%D8%A7%D9%86%D8%AA%DB%8C%D9%86%D8%B1%D9%87%D8%A7-%DA%86%D9%87-%D9%87%D8%B3%D8%AA%D9%86%D8%AF-%D9%88-%DA%86%D8%B1%D8%A7-%D8%A8%D9%87-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7-%D9%86%DB%8C%D8%A7%D8%B2-%D8%AF%D8%A7%D8%B1%DB%8C%D9%85%D8%9F