# 容器技术

代东洋 1251368

2016 年 6 月 6 日

## 目录

# 1 云计算与虚拟化技术

随着互联网、移动互联网的高速发展，传统 IT 企业加速向云计算转型。其中，投入速度快、成本低和系统迭代更新是企业转向云计算技术的三个主要原因。

虚拟化技术是通过虚拟机监视器（virtural machinemonitor, VMM) 对底层硬件资源进行管理，支持多个操作系统实例同时运行。虚拟化技术的目标是实现资源利用率的最大化，同时将底层的物理设备和上层的操作系统应用软件分离，从而实现计算资源的灵活性。对于大型的实验或软件设备，使用虚拟化技术能充分利用高性能的硬件资源，而且有利于设备的综合管理和维护。目前，主流的虚拟化技术分为两种——完全虚拟化（硬件虚拟化技术）和基于容器的虚拟化（容器技术)。

# 2 容器技术简介

容器技术本质上是虚拟化技术的一种，属于操作系统级别的虚拟化。同传统硬件虚拟化技术不同，容器技术并不模拟硬件，而是在特定的操作系统内核的支持下对主机系统的 CPU、内存、磁盘、网络等资源进行分配，形成一个容器，每人容器被视为独立的操作系统实例，从而实现不同操作系统实例上应用程序之间的隔离，并共享主机资源，达到类似硬件虚拟化的效果。同传统的硬件虚拟化相比，容器技术具有系统架构简单高效、存储和内存需求小、部署启动速度快和运行性能好等特点。

# 3 容器技术的实现

不同的容器技术的隔离方法也有所区别，概括起来有以下几种:

## 3.1 chroot 方式

在 Linux 系统和 UNIX 系统中，文件系统拥有唯一的根目录”/”，系统中所有的运行时库和应用程序都是从根目录派生出来的。chroot 工具可以针对不同的用户改变根目录的实际位置，从而实现运行环境和文件资源的隔离。FreeBSD Jail 基本是基于 chroot 方式实现的。

### 3.2 容器虚拟层方式

在内核之上建立一个容器虚拟层，将整个操作系统环境容器化，利用命名空间和标记等方式对进程、用户、CPU 时间片、内存页面、网络流量、系统文件等系统资源进行划分和过滤，使不同的容器内的进程只能是使用被分配给容器的系统资源，只能对容器内部的文件进行操作，从而实现容器间的资源隔离与安全隔离。

### 3.3 基于操作系统内核功能的方式

Linux 内核通过 namespace 功能实现进程隔离，通过 cgroup 功能实现资源的隔离和统计。LXC 是基于操作系统内核功能实现的容器技术。

## 4 云计算中的安全技术

安全一直是云计算面临的重大问题，如何通过技术实现云服务的信息安全、隐私保护、服务稳定性，抵御 DDos 攻击，降低数据泄露风险，一直是科研机构和企业着力研究的范畴。2014 年，两项技术突破为云安全防护带来了曙光。云计算企业 Cloudflare 发明了一种方法，允许企业将加密数据分布式存储到云中，但将私钥存储在一个单独的安全服务器中。当用户访问网站时，Cloudflare 会签发一个临时的“会话密钥”，与用户的设备一一对应，从而让密钥从公众视野中消失。IBM 的密码学者 Graig Gentry 研发了一种加密算法，在云计算环境中对数据加密，使得云服务商无法获取数据内容，仅限于用户合法正式的用户能够访问。

## 5 容器技术的的挑战

### 5.1 容器技术和容器生态仍需要持续发展

容器技术的流行是进几年的事情，一般来说，会把 Docker 技术诞生的 2013 年作为容器技术流行的元年。当 Docker 过分地曝光在众人注目之下时，它固有的缺点就暴露出来了。举个例子，Docker 的网络和存储管理带有天然的缺陷，成为大部分生产环境实践的障碍。另外，Docker 集群管理工具 (Kubernetes, Swarm 等) 也需要更多的大规模线上实战来历练和验证。

### 5.2 云安全仍是个大问题

容器技术本身非但没有提升应用的安全性，反而在一定程度上降低了安全性。因为容器与宿主机共享操作系统内核，只要同一个宿主机上任一容器存在漏洞，或者宿主机本身存在安全漏洞，都有可能导致上面的所有容器安全性受到影响。再加上公有镜像市场中的容器镜像鱼龙混杂、恶意镜像的传播途径更是不可控的，使得单独容器对容器云平台的安全性造成很大的威胁。如何有效防止外部攻击和内部渗透把危害带给云平台和业务，也是各容器云平台厂商需要思考并且解决的。

## 6 容器技术与复用

### 6.1 应用程序的打包、复用

云计算对于简化部署、缩短上线周期和应用自动伸缩有着强烈的需求，因此容器技术越来越炙手可热。基于 Linux 的容器技术为应用程序的开发、测试和发布提供了一个简单易用的打包工具。

容器的设计初衷旨在让开发者更简单更快地创建一个完整的应用运行环境。传统的应用部署方式要求开发者检查系统是否满足部署的最低要求，容器技术将开发者从这些繁杂的过程中解脱出来。

除了给开发者带来方便外，容器还有很多优势。Linux 容器打包技术适用于任何类型的服务端应用，并且不受环境限制，它可以运行在桌面机器上、云上，或者任何有 Linux 的地方，开发者也无需关心 Linux 发行版的内核版本。

容器技术的“一次构建，到处运行”特点，实现了应用程序级别的复用，降低了开发成本，提高了开发效率。

### 6.2 选取什么样的容器技术方案

容器技术的选择应该结合自身业务特点、自身系统构架、成本、该技术的流行程度、发展趋势、以及相关资料的多少综合考量。

# 7 参考资料

*容器技术日渐火热 - 赛迪智库*

*云计算中使用容器技术的信息安全风险与对策 - 张楠*

*基于* Docker *技术的容器隔离性研究 - 刘思尧、李强、李斌*