【Container讲师专访】CloudStack＋Docker构建云端信息安全实验场，i 春秋的容器落地实践...

原创

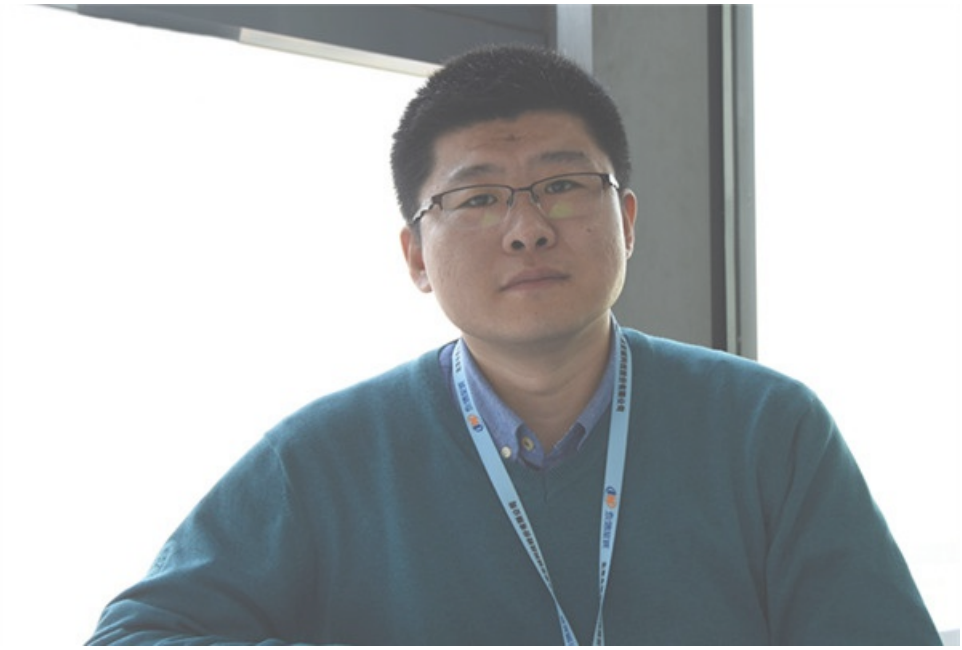
陈晨luminous 于 2016-04-28 11:08:58 发布 1114 收藏

文章标签： 中国云计算大会 CCTC 容器 Docker

> 2016年5月13日-15日，由CSDN重磅打造的2016中国云计算技术大会（CCTC 2016）将于5月13日-15日在北京举办，今年大会特设“中国Spark技术峰会”、“Container技术峰会”、“OpenStack技术峰会”、“大数据核心技术与应用实战峰会”四大技术主题峰会，以及“云计算核心技术架构”、“云计算平台构建与实践”等专场技术论坛。大会讲师阵容囊括Intel、微软、IBM、AWS、Hortonworks、Databricks、Elastic、百度、阿里、腾讯、华为、乐视、京东、小米、微博、迅雷、国家电网、中国移动、长安汽车、广发证券、民生银行、国家超级计算广州中心等60+顶级技术讲师，CCTC必将是中国云计算技术开发者的顶级盛会。

在今年的Container峰会上，除了可以了解到知名互联网公司的顶级容器专家带来的技术分享，另外一个看点就是我们邀请到了广发证券、长安汽车、民生银行等垂直领域的容器使用案例，他们将为我们带来在Docker使用过程中的经验和填过的坑。

为了让大家对本次峰会有个更加全面的认识，我们在峰会召开之前，特别采访到了，北京永信至诚科技股份有限公司副总裁，CTO张凯，他将在本次峰会上发表《CloudStack＋Docker构建云端信息安全实验场》的演讲，欢迎到场聆听。



> 张凯：永信至诚CTO、副总裁。2003年入行的信息安全老兵，先后供职于启明星辰ADLab、中国移动研究院、中国电力科学研究院和永信至诚从事信息安全技术的研究和开发工作。安全技术方面专长于恶意代码研究及防御方向，2013年开始专职从事信息安全人才实训平台和仿真靶场平台的团队组建及研发，主导了i 春秋学院CloudStack、Docker以及自主的e春秋信息安全实验室平台云的架构、产品设计及研发，并负责i春秋学院的运维和运营工作。热衷于虚拟化技术、可视化技术等在信息安全实训方面的实践。

1.你们是什么时候开始使用Docker的？能介绍下目前的一些应用情况吗？

张凯:我们团队从2013年开始接触虚拟化技术，由于我们的业务要求我们实用虚拟化的方式来构建信息安全实验场景，所以最开始接触的还是vmware、kvm这样的虚拟化技术，并成功的研发了i 春秋信息安全学院和e春秋信息安全实验室平台。在去年的时候，Docker容器技术走进了我们的视野，并开始根据我们的业务需求进行一些研究和积累。

我们使用Docker容器主要是搭建我们的信息安全实验场景，之所以要使用“场景”这个概念，是因为在我们的每一个实验中，我们不仅需要设定好一个实验环境，还要设定好剧本以及剧本中可以和用户进行交互和联系的各种东西。简单点说，我们提供的每一个场景就像是一个小型的实验室模版，这个模版定义了实验室的建筑（虚拟机和网络）、建筑中每间屋子之间的联通关系（网络访问策略）、每间屋子开放的门和提供的服务（端口和应用服务）、每间屋子内部的陈设（虚拟机内部的操作系统、各类软件的安装和设定等）、每间房间里藏着的一个或多个“宝藏”（安全漏洞、FLAG为标志的珍贵信息等）以及这些“宝藏”作为线索时候的相互关系等等。因此可以看到我们所面临的主要问题包括：

- 如何快速的构建这样的一个场景模版，释放场景编剧的创造力
- 如何根据场景模版快速的进行克隆，在服务器资源有限的情况下为每个用户准备实验环境
- 如何把每个用户的实验场景相互隔离开而不互相影响

根据我们需要搭建的场景的复杂程度和安全性要求，我们会选择使用虚拟机还是Docker容器来完成这个“房间”的搭建。

我们的另一个特点是，我们的用户有很大一部分并不是技术人员，因此如果仅提供字符界面给用户显然是不够的，我们需要为每一个互联网用户提供一个在云端的发起实验操作“个人计算机”，这个计算机可能是windows或linux，同时我们还要在这个实验机内提供进行实验的各种实验工具等便利措施。为了让用户在互联网的任何地方都可以进行实验，我们开发了我们自己的可视化“虚拟云桌面”，这样用户只要有浏览器，就可以安全的操作我们在云端的实验计算机了。为了操作的便利，在我们场景模版中的一些docker中安装了xwindows和vnc server，并通过我们专有的云桌面代理建立用户与操作计算机之间的操作通道。

2.贵公司的业务为什么选择Docker？Docker在这样的业务中有什么优势，发挥什么样的价值？

张凯:Docker是一个轻量级的虚拟化解决方案，并且容器具有快速启动、占用计算资源少等特性。相比我们以往一直使用的虚拟机构建场景的方式，通过有选择的将容器组建场景或将容器与虚拟机混合组建场景可以在保证安全性的前提下节约时间、减少场景下发时间、节约云端资源等优势。

我们的i春秋产品专注于在线网络安全教育，并给学员提供仿真实验室环境。Docker容器的快速启动特性正好满足我们对快速搭建仿真实验室的需要；占用资源少的特性利于我们缩小计算集群规模，节约资源；轻量级的虚拟化解决方案减小了我们对虚拟化的研究成本，使我们对虚拟化技术的扩展也变得相对容易。

鉴于Docker以上特性在我们公司业务上体现的优越性，我们选择了Docker虚拟化技术，Docker将在未来对我们公司扩大虚拟化集群规模和业务发展发挥重要作用。

3.Docker在你们公司的应用场景有哪些，能否介绍一些关键的技术栈？

张凯:目前Docker在我们公司的应用场景主要包括：内部测试和开发环境部署、虚拟实验场景构建及动态调整、i春秋网络实验室搭建、i春秋闪电实验室搭建、信息安全竞赛赛题搭建等。

我们在使用Docker的过程中，为了让Docker更好的满足我们的业务需要，对Docker做了如下一些改进：

- 配置开机启动项

由于Docker容器并不包含操作系统内核，在系统设置方面的改动都无法保存，因此不能使用配置linux系统开机自启动项的方法来配置Docker容器中的自启动项。

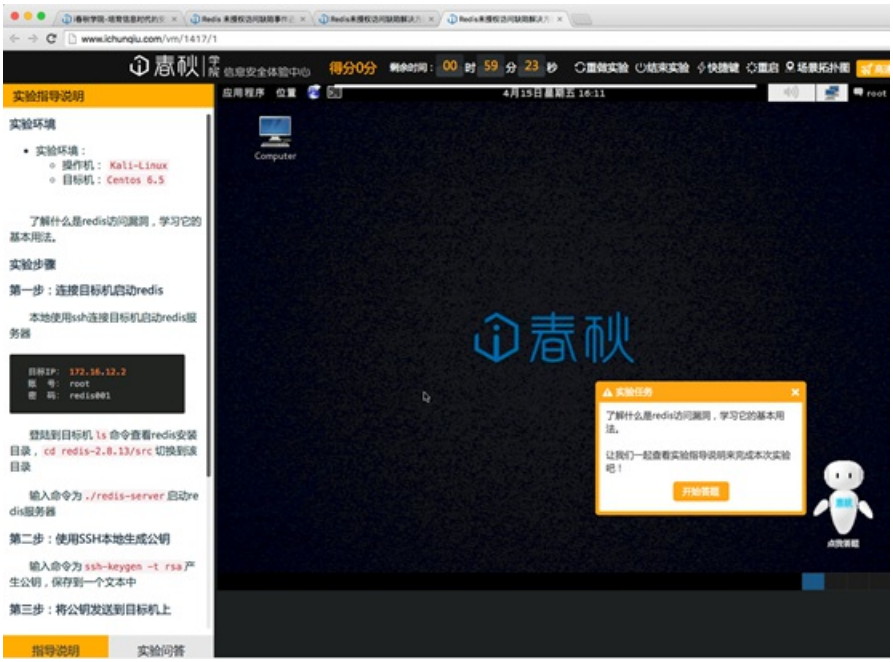
最佳实践是使用build + supervisor（linux下监控进程的工具，通过supervisor启动所有服务）来构建支持开机自启动的镜像，例如开机自启动ssh和apache服务，具体方法如下：

1. 创建supervisord.conf
2. 创建Dockerfile
3. 创建镜像
4. 启动supervisor容器

可以使用这个方法创建一个支持supervisor的基础镜像，之后可以使用这个镜像为基础来创建镜像并配置自启动服务。

- 支持VNC远程桌面

由于所有Linux系统上的应用都可以在Docker容器中运行，因此可以通过在安装了Xwindow的容器中安装vnc server来对外提供可视化的计算机操作服务，再利用平台的虚拟云桌面代理服务器将vnc协议转化为专有的协议将数据传输到用户的浏览器，用户在浏览器上无需安装任何插件即可进行虚拟化桌面的操作。



- 自定义网络配置

Docker本身不支持自定义容器的IP地址，默认选择bridge网络模式的情况下，容器启动后会通过DHCP从docker0网络获取一个地址。可以使用第三方网络配置工具如Pipework、Flannel、Kubernetes、Weave、opencontrail等来配置容器IP，并利用场景中的虚拟路由器来逻辑上将场景中的不同虚拟机和容器进行逻辑隔离、端口的隔离等等。

- 自定义存储池

Docker默认会使用 /var/lib/docker 作为镜像和容器的存储位置，/var分区一般来说容量都分配得较小，当镜像和容器数目较多时会导致默认的存储区容量不足。
在安装完Docker之后应当配置Docker的默认存储路径，一般来说可以使用网络存储。例如将提供NFS服务的存储服务器挂载到Docker宿主机，并配置Docker使用挂载的网络存储。

- 集群控制

一般来说在一台服务器上可以布署100~1000个Docker容器，但是在云环境下这是远远不够的，因此需要部署多台服务器做分布式Docker宿主机，并采用合适的负载均衡调度算法选择运行容器的宿主机。

Swarm是Docker公司在2014年12月初发布的一套较为简单的工具，用来管理Docker集群，它将一群Docker宿主机变成一个单一的，虚拟的主机。Swarm使用标准的Docker API接口作为其前端访问入口，换言之，各种形式的Docker Client(docker client in go, docker_py, docker等)均可以直接与Swarm通信。Swarm几乎全部用Go语言来完成开发，并支持与Docker相同的命令以及集群驱动。

Swarm deamon只是一个调度器（Scheduler）加路由器(router)，Swarm自己不运行容器，它只是接受docker客户端发送过来的请求，调度适合的节点来运行容器，这意味着，即使Swarm由于某些原因挂掉了，集群中的节点也会照常运行，当Swarm重新恢复运行之后，它会收集重建集群信息。

4.企业在应用Docker技术时，需要做哪些改变吗？

张凯:总结我们目前对Docker的使用经验，企业在应用Docker时可根据业务需要做以下几点改进：

- 重新配置Docker使用的存储路径，尽量采用网络存储方案提高扩展性。
- 鉴于目前从Docker官方镜像仓库拉取镜像的不稳定性，使用国内的镜像仓库（比如阿里云镜像仓库），或者搭建自己的私有镜像仓库，用来分享常用的镜像。
- 使用Docker的build命令创建自己的Docker镜像
  安装supervisor（linux下监控进程的工具，通过supervisor启动所有服务）并将supervisor配置成开机自启动，使用supervisor工具管理容器开机自启动项
- 手动配置宿主机防火墙NAT

当业务需要在宿主机上配置到容器的NAT（docker run -p）时，Docker会自动配置宿主机的防火墙NAT规则，但是这些规则并不会持久化到防火墙配置文件，重启防火墙后这些规则都将消失，这对系统维护很不友好。

因此建议：

1）不使用docker run -p参数配置NAT，而是通过手动配置防火墙NAT规则来实现。
2）使用docker run -p参数配置NAT，容器启动之后使用iptables-save（centos）将防火墙规则同步到防火墙配置文件。

- 固定容器IP地址

Docker容器在我们的实验场景中都会运行某些服务，比如nginx、httpd、mysql、dns等，作为承载服务的容器必须要求IP地址固定。然而Docker并不支持自定义容器IP地址功能，在容器重启之后IP地址可能发生变化（容器停止之后会将占用的IP回收，启动之后会重新分配IP），这是不允许的。因此我们使用第三方网络配置工具如Pipework、Flannel、Kubernetes、Weave、opencontrail等来给容器配置固定的IP地址。

5.您所在的企业在应用Container/Docker或者k8s技术时遇到了哪些问题？是如何解决的？

张凯:我们在使用Docker的过程中大概遇到了以下几个问题：

- Docker官方镜像仓库不稳定

在我们从Docker官方镜像仓库拉取镜像到本地的过程中，经常遇到网络中断导致镜像拉取失败的情况。

原因：由于Docker的官方镜像仓库位于国外，网络不是很通畅，偶尔还需要翻墙才能访问。

解决方案：使用阿里云镜像仓库，或者搭建自己的私有镜像仓库。

- 重启防火墙后容器NAT失败

使用docker run -p参数在容器运行后将容器内的端口映射到宿主机，当重启宿主机防火墙（centos iptables）后发现端口映射失效。

原因：docker run -p参数只是临时配置了防火墙NAT规则，并不会把规则持久化到防火墙配置文件，在防火墙重启后导致临时规则失效。

解决方案：不使用docker run -p参数配置容器到宿主机的端口映射，而是采用手动在防火墙配置文件中添加NAT规则，并同时设置临时NAT规则的方式。这种处理方式既能将规则持久化到配置文件，也能达到不重启防火墙就能使规则立即生效的目的。

- 无法自定义容器多个网卡

我们在启动容器的时候禁用容器默认的网络，并使用第三方工具pipework配置容器固定IP，但是不能配置容器多个IP。

- Swarm集群服务发现不准确

我们使用Docker官方提供的集群管理工具Swarm来管理Docker计算节点集群，服务发现使用Docker Hub内置的服务发现功能时，始终有一台服务器无法成功加入集群，也没有报任何错误信息。

解决方案：使用静态IP列表作为Swarm服务发现方案。创建Swarm容器时使用-v参数挂载本地静态IP列表文件到容器（-v /root/clouster:/tmp/cluster），并使用manage file:///tmp/cluster（静态IP文件在容器中的路径）参数设置使用静态IP列表文件作为服务发现方案。

6.作为当前最流行的Container技术，您认为Docker还有哪些方面需要改进？

张凯:我们在使用Docker的过程中觉得以下几点使用上不方便，可以加以改进：

- 重启防火墙后容器NAT失败，可以将防火墙NAT规则持久化到防火墙配置文件
- 容器网络配置很不灵活（例如：无法固定容器IP地址、无法指定容器使用的网络接口）
- Docker不支持以宿主机VNC方式访问容器

7.您在本次演讲中将分享哪些话题？

- 信息安全人才培养中遇到的困难以及我们的解决方案
- 云和虚拟化技术为信息安全人才教育变革提供的机遇
- 我们是如何在互联网上为用户搭建信息安全的“专属实验室”的
- 虚拟化技术和Docker容器技术在我们业务实践中的应用

8.哪些听众最应该了解这些话题？您所分享的主题可以帮助听众解决哪些问题？

张凯:对信息安全人才在线教育、虚拟化技术、容器技术有兴趣的听众、希望利用相似的技术来进行系统研发和实践的研发人员应该会对这些话题感兴趣。

通过这些主题，将能够：

- 了解i春秋学院在信息安全人才教育方面的理念和技术架构
- 了解我们在近三年来的虚拟化和容器技术实践过程中遇到的难题和解决方法，并进行探讨
- 了解实战和动手能力对信息安全人才教育的重要性，并了解我们是如何通过在云端搭建虚拟实践场景的方式解决这个问题的，能够了解我们在这个过程中对现有技术的突破和实践方法，以及我们未来的研究方向。
