



专栏：网络新技术

基于容器技术的 PaaS 云平台方案

齐磊, 张海峰, 张天骁, 祝好, 陈旭

(中国移动通信集团设计院有限公司, 北京 100080)

摘要: 随着互联网业务发展及 IaaS 云资源池技术的成熟, IT 支撑系统也在尝试 PaaS 云的建设及应用。分析了 IT 系统如何考虑技术演进, 搭建 PaaS 云平台架构, 实现系统资源的统一管理、监控、共享和调度, 实现应用的统一部署和多数据中心的高可应用性。

关键词: 平台即服务; 容器技术; Docker; Kubernetes

中图分类号: TP319

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017101

PaaS cloud platform based on container technology

QI Lei, ZHANG Haifeng, ZHANG Tianxiao, ZHU Hao, CHEN Xu

China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

Abstract: With the development of internet service and IaaS cloud, the PaaS cloud was discussed in the construction and application of IT support systems. How to take into technological evolution and how to build PaaS architecture, were analyzed. How to implement a system of centralized management, supervision, sharing and scheduling was introduced. How to achieve unity of application deployment and how to achieve high availability for data center were discussed.

Key words: PaaS, container technology, Docker, Kubernetes

1 引言

移动融合业务, 尤其是互联网业务的发展, 对系统水平弹性动态扩展、业务连续性保障、故障迅速恢复提出更高的要求。现有 IT 支撑系统缺乏能使业务能力得以快速扩展的统一技术和平台, 无法适应互联网业务发展带来的剧烈业务波动, 业务快速上线和弹性伸缩能力较差。同时, 伴随 IaaS (infrastructure as a service, 基础设施即服务) 资源池的应用及成熟, IT 系统主机、网络、

存储等资源数量呈现几何级数增长, 传统的运营效率已经无法满足需求, 跨数据中心资源无法共享, 对项目建设、运维开发等各个流程都带来颠覆性挑战。

本文以 IT 系统引入容器技术建设 PaaS (platform as a service, 平台即服务) 云平台的解决方案为例, 分析其如何实现系统资源的集中管理、动态分配、监控、共享和调度, 如何实现应用的统一部署和业务连续性保障, 实现多数据中心的高可用, 推动系统架构及流程的调整, 应对

收稿日期: 2017-02-20; 修回日期: 2017-04-01



云计算时代所带来的变革。

2 PaaS 云平台架构

有着 10 多年发展历史的业务支撑系统，其承载的业务相当复杂，业务和系统架构耦合极其紧密。以承担了全网产品一体化运营及管控能力的某支撑系统为例，该系统承载 170 个全网业务平台，业务服务能力多达 700 个，提供了金融、互联网、客服、业务订购及鉴权等各类业务的聚合。在 IT 系统架构 PaaS 层云化改造设计过程中，如何搭建标准云架构模式以适应传统应用，如何避免架构调整对业务带来的重构冲击，是架构设计首先要考虑解决的问题。

IT 支撑系统主要通过引进 Docker、Kubernetes 等技术和搭建微服务架构模式来减少对现有应用的影响，即将应用程序分割成更小的相互关联的服务，并采用容器化技术进行微服务的封装、部署、管控。这些服务围绕业务能力构建并且可独立部署，方便地为不同类型的微服务提供差异化的管理策略。以容器技术为核心的支撑技术框架，

既满足当前业务支撑系统发展的实际需求，又具有支撑未来业务高速发展的技术先进性。该技术架构主要分为以下几层。

(1) 资源管理层

OpenStack 或裸机资源池，即 IaaS 基础设施层，提供上层获取资源的接口。

(2) 公共服务层

通过基于 Docker 和 Kubernetes 的容器化服务提供平台层服务，在其上部署基础服务和用户自定义的服务，并通过微服务的组合和编排组成对外能力开放平台，提供业务级的服务组合，供应用层通过 REST 接口调用。

(3) 应用层

提供用户访问、运维管理的入口门户，通常以 Web 服务或 REST API 方式提供给客户端（浏览器、智能终端或外部系统）进行访问。

IT 支撑系统 PaaS 平台的整体技术架构如图 1 所示。

Docker 是容器技术的一种，它运行于 Linux 宿主机上，每个运行的容器都使用操作系统的内

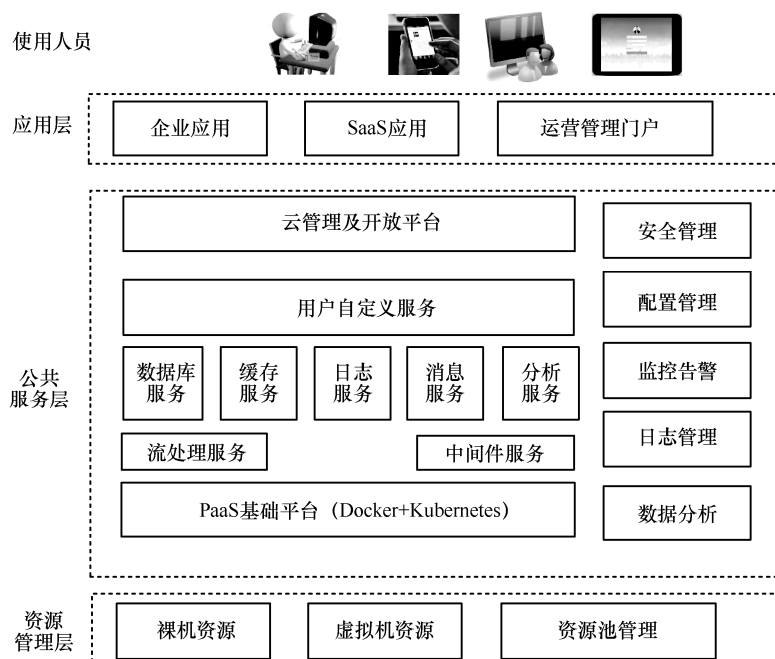


图 1 IT 支撑系统 PaaS 平台的整体技术架构

核隔离功能,是轻量的虚拟技术,更加高效,启动速度更快,且可以屏蔽开发、测试及生产环境的区别,实现更轻松的迁移和扩展,提高开发、测试、部署、升级及维护的效率。Kubernetes 是基于容器技术、采用分布式架构的一种集群管理解决方案,它具有完备的集群管理能力,包括多层次的安全防护和准入机制、多租户应用支撑能力、透明的服务注册和服务发现机制、内建智能负载均衡器、强大的故障发现和自我修复能力、服务滚动升级和在线扩容能力、可扩展的资源自动调度机制以及多粒度的资源配额管理能力。

3 PaaS 云关键技术

3.1 应用拆分和服务部署方式

PaaS 云平台引入微服务架构,并采用容器化技术进行微服务设计、编排、授权和配置,解除应用间的紧耦合和依赖。针对 IT 支撑系统多种多样的应用及业务,本文根据使用频次、服务调用开销不同,采用不同策略进行划分和分布式部署。几种应用拆分方式介绍如下。

(1) 针对 HTTP/soap 应用,采用开源缓存集群部署,将应用和 MySQL 数据库放在一个镜像(image)中,将会话(session)数据放在第三方缓存,实现快速的水平扩张,可满足类似电渠查询类业务的高峰值交易量需求。

(2) 针对纯计算类应用,如不涉及数据库的 DCC 应用模块,通过容器化提供大量计算能力,并通过对主控端(master)的多节点部署保障其高可用性。

(3) 针对 MySQL 类集群进行容器化改造,通过主从复制及共享存储备份解决数据服务的高可靠和安全性,并且可达到裸机的性能和更好的高可用性。

拆分后的微服务粒度小,轻便灵活,可实现复杂多种应用场景的敏捷交付。通过容器技术

进行服务设计、编排、授权、配置,可解除应用间的紧耦合和依赖,为业务系统升级和扩展提供了良好的技术基础,极大地提高运维效率和系统性能。

3.2 多集群资源的统一纳管

PaaS 云平台通过下述方式实现资源统一管理功能。

(1) 经过证书认证之后,通过 Kubernetes API 服务器对集群进行纳管,导入集群的节点数量、配置等信息,并补充机房、机架等信息。

(2) 将所纳入集群和租户进行绑定,把集群分配给不同的指定租户。可为每个业务建立独立的租户,安全隔离不同租户的资源和访问权限。根据业务大小,通过分区或分集群的方式实现安全隔离,既保证各业务的独立性又保障资源的共享。

(3) 租户可以继续对集群资源进行分区,部署不同的应用,实现不同配置的主机共存。租户也可以对集群资源根据应用和业务进行划域隔离,保障安全。如将 Web 类应用和 proxy 应用部署在 DMZ 和互联网域,采用 Kubernetes+Docker 容器技术,具备轻量但弹性扩展需求强的特点;可将包含大量的计算类、服务类、分析类应用部署在核心区,引入 Mesos 技术搭建分布式系统内核,构建巨大的计算集群。

多集群资源统一管理架构如图 2 所示。通过使用 Kubernetes 多集群统一管理,后台运维人员可以很方便地了解资源情况,如系统集群数量、每个集群分配的机器数量及配置、机房条件、资源利用率等。该功能大幅度提升后台运维人员对系统的管理和监控力度,为多集群、多数据中心间的资源调配奠定基础。

3.3 多集群应用的统一部署

考虑 IT 支撑系统的业务及架构特色,PaaS 云平台针对多集群情况下的应用部署需要考虑多种情况:应用需要能支持跨广域网、跨集群统一

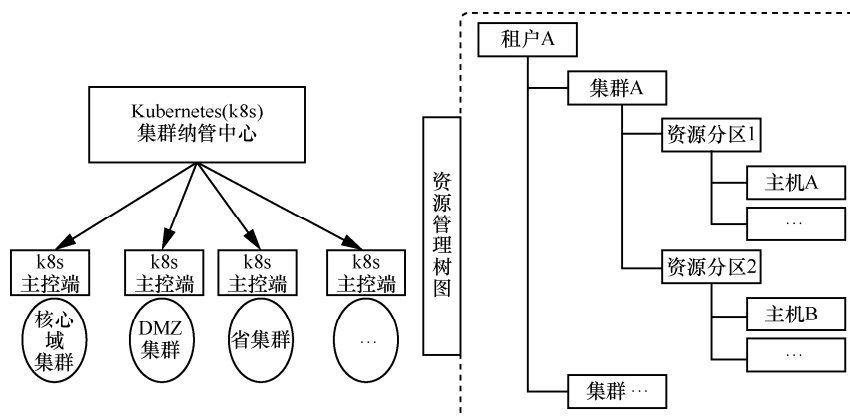


图2 多集群资源统一管理架构

部署；需要能支持部署到不同集群的不同分区上；还需要支持跨集群灰度发布和滚动升级。

针对这些要求，PaaS 云平台对应用部署功能进行了改进。

(1) 通过两级镜像架构实现镜像的统一生命周期的管理。总部统一库集中实现镜像的入库、出库和版本更新，并按照省节点或集群划分子库。子库可以设定同步规则，只同步一部分镜像到子库，并实现镜像的跨地域、跨 IP 承载网同步和更新，支持全量同步和增量同步。

(2) 用户定义完应用并进行部署时，从镜像库获取应用镜像，结合其权限选择应用部署的集群和分区的列表，并通过一键式操作把应用同步部署到多个集群的资源分区上。

(3) 大型的应用都会部署在多个集群或者分区，通过应用的在线灰度发布和升级提高应用的高可用性，并且在升级的时候用户可以选择按集群和分区进行滚动升级。

前期每次全网应用软件版本升级约需要8人/天，通过多集群应用的统一部署，该工作可提升至15 min 部署完成，大幅度提升了 IT 系统新版本的上线效率，保障了业务系统的连续性。

3.4 多集群、多数据中心之间的高可用

PaaS 云平台的多数据中心的高可用场景如下。

(1) 多集群的统一服务部署

由 Kubernetes 管理平台自动化部署模块统一

对各数据中心进行服务自动化安装部署。可以定义同一个服务在不同数据中心的 Kubernetes 集群统一部署，并且可以定义在每个集群部署服务的容器实例的比例，如可按 6:4 的比例在集群 A 和集群 B 上部署服务。

(2) 灰度升级

由 Kubernetes 管理平台自动化部署模块统一对各数据中心自动化进行服务升级。可以实现先在一部分集群部署新版本，稳定之后再平滑升级全部的节点。

(3) 动态集群间业务调整

业务高峰期当一个数据中心容量不足时，由 Kubernetes 管理平台自动进行服务动态扩展，启动容灾数据中心的部分服务来支撑业务。

(4) 业务高可用

当主数据中心发生故障时，由 Kubernetes 管理平台自动进行容灾切换，由容灾数据中心自动接管所有业务服务。

4 PaaS 云的应用

4.1 组网架构及统一管理

仍以运营商某全网性业务支撑系统为例，该系统采用容器技术承载 PaaS 云平台，目前共管理了全网 33 个大集群，目前已包含 1 200 台 x86 服务器组成的多个集群，按照不同的服务提供上万个容器，实现了对系统跨域（核心域、DMZ、接

入域)、跨 31 个省、跨多个数据中心的复杂多集群环境的集中管理。其应用及服务集群架构如图 3 所示。

图 3 通过容器云平台的统一监控管理实现对所有租户、集群、资源、应用的集中数据采集和展示。后台人员不仅可以了解传统的资源情况,还可以从租户或应用角度了解系统集群及配置、资源利用率、主机信息等情况。通过租户视图,每个租户可以查看自己的资源和服务的运行情况,通过基于业务角度的服务视图,可轻松查看每个业务的 Docker 容器对 CPU、内存等关键性能指标的实时占用情况,实现了资源的占用和业务的有效匹配。租户还可结合业务资源使用情况,进行权限范围内的添加/删除资源分区、主机等操作,大幅度提升系统的运管效率和监控力度。

4.2 业务调度及高可用

通过 IT 支撑系统 PaaS 云的建设,可以实现不同集群、不同数据中心间资源的快速共享、服务的动态迁移及扩展,保障系统的高可用。仍以该系统为例,系统承载了全网互联网、金融等各类业务,且业务呈现容量大、实时性强、波动剧烈、增长迅速等特点。如天猫商城“双十一”期

间,系统承载的电子渠道类(校验及查询)业务峰值达到了日均规模的 20 倍,一天提交的订单量更是达到日均规模的 120 倍。针对互联网业务高峰带来的剧烈波动,PaaS 平台采用如下两种方式来实现有效的解决。

- 通过容器的统一监控及弹性伸缩技术,设置 KPI 伸缩策略的阈值。当查询类业务达到 4 万笔交易/min 的阈值时,自动触发在秒级快速增加 100 个容器实例支撑峰值业务量,很好地支撑了业务的波动。
- 借助多集群的动态部署及多数据中心间资源的快速共享,将总部订单类应用指向容灾数据中心及 31 个省的节点进行处理,并借助部分非高峰业务的处理能力,有效解决了总部节点处理能力上限不足的问题,保障了系统灵活的水平扩展和高可靠能力。

5 结束语

基于容器技术的 PaaS 平台,可实现 IT 支撑系统跨多个网络域、跨多个数据中心的复杂多集群环境的集中管理,且通过多集群统一部署可大幅度提升软件新版本的上线效率。通过容

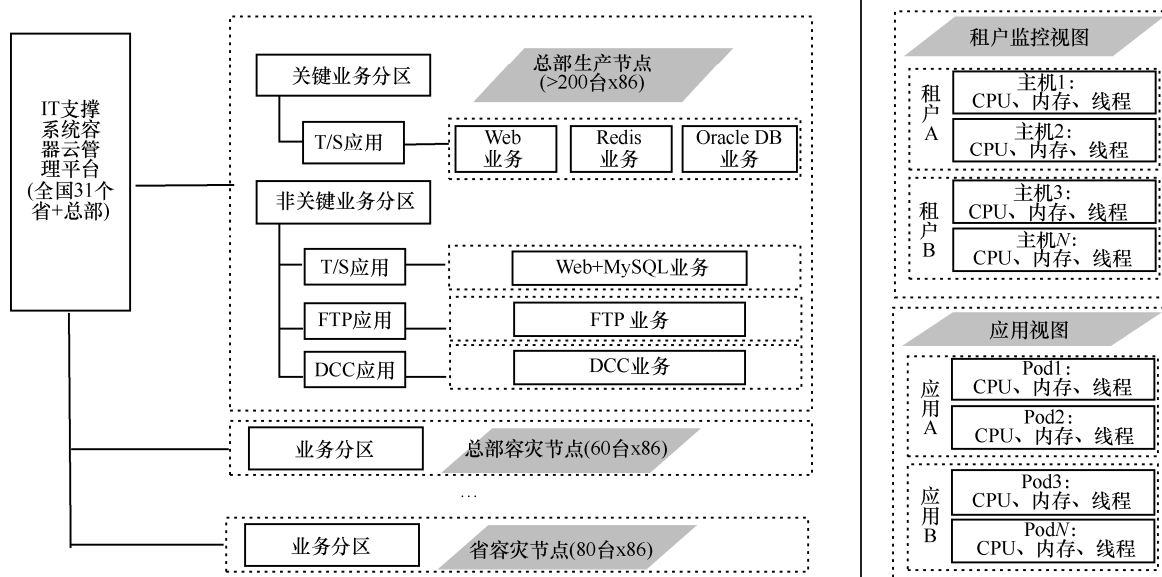


图 3 PaaS 云平台应用集群组网结构及管理视图



器技术和立体化监控,可全方位监控各集群的资源整体利用率,并通过多集群间动态部署容器数量,实现灵活的水平扩展能力。但考虑容器技术作为一个较新的技术,在推动容器技术的标准化和规范化、实现更多应用的重构及统管、构建统一化的服务组件等方面,仍需要持续关注和研究。

参考文献:

- [1] 董昭. NGBOSS 互联技术研究[J].电信工程技术与标准化, 2012, 25(3): 53-58.
DONG Z. Technical of NGBOSS interconnection[J]. Telecom Engineering Technics and Standardization, 2012, 25(3): 53-58.
- [2] 刘昭, 张海峰, 李玮, 等. 运营商发展大数据技术及建设模式展望[J].电信工程技术与标准化, 2015, 28(3): 12-16.
LIU Z, ZHANG H F, LI W, et al. Operators to develop big data technologies and construction mode prospect[J]. Telecom Engineering Technics and Standardization, 2015, 28(3): 12-16.

[作者简介]



齐磊 (1982-), 男, 中国移动通信集团设计院有限公司高级工程师, 主要研究方向为 IT 支撑系统技术及组网。



张海峰 (1980-), 男, 中国移动通信集团设计院有限公司高级工程师, 主要研究方向为 IT 支撑系统技术及组网、大数据平台方案及设计工作。



张天晓 (1988-), 男, 中国移动通信集团设计院有限公司工程师, 主要研究方向为 IT 支撑系统技术及组网、电子渠道系统方案及设计工作。



祝好 (1985-), 女, 中国移动通信集团设计院有限公司工程师, 主要研究方向为 IT 支撑系统技术及组网、运营管理系统方案及设计工作。



陈旭 (1987-), 女, 中国移动通信集团设计院有限公司工程师, 主要研究方向为 IT 支撑系统技术及组网、业务支撑系统方案及设计工作。