大数据与
计算机科学系列

大数据
技术与
应用方向

私有云架构设计与实践

尤永康 梅 磊 刘松涛 蒋 迪 著

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

私有云架构设计与实践

尤永康　梅　磊　刘松涛　蒋　迪　著

上海交通大學出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书通过现状、通用架构与模型、技术实现基础、典型案例与用例等四个部分，阐述基于KVM环境中的私有云构建元素。

通过本书，读者会了解到KVM私有云的主流实现技术，包括架构、模拟器、存储、网络等基础知识等。最后的部分会对VDI的几个典型场景以及运维、测试、调节与优化等有针对性地叙述，读者可以直接将其运用到产品或项目中。

图书在版编目(CIP)数据

私有云架构设计与实践 / 尤永康等著. —上海：
上海交通大学出版社，2019
(电子工程与计算机科学)
ISBN 978-7-313-22087-5

Ⅰ. ①私… Ⅱ. ①尤… Ⅲ. ①云计算 Ⅳ.
①TP393.027

中国版本图书馆CIP数据核字(2019)第227367号

私有云架构设计与实践
SIYOUYUN JIAGOU SHEJI YU SHIJIAN

著　　者：尤永康　梅　磊　刘松涛　蒋　迪
出版发行：上海交通大学出版社
邮政编码：200030
印　　制：上海天地海设计印刷有限公司
开　　本：787 mm×1092 mm　1/16
字　　数：464千字
版　　次：2019年12月第1版
书　　号：ISBN 978-7-313-22087-5
定　　价：88.00元

地　　址：上海市番禺路951号
电　　话：021-64071208
经　　销：全国新华书店
印　　张：20.25
印　　次：2019年12月第1次印刷

“大数据与计算机科学”系列教材

编委会名单

编委会委员

（排名不分先后）

曹珍富　华东师范大学计算机科学与软件工程学院密码与网络安全系主任

崔立真　山东大学计算机科学与技术学院副院长

何钦铭　浙江大学计算机科学与技术学院副院长

黄冬梅　上海海洋大学信息学院院长

江建慧　同济大学软件学院副院长

蒋建伟　上海交通大学软件学院副院长、MOOC 推进办副主任

马　啸　中山大学数据科学与计算机学院副院长

秦磊华　华中科技大学计算机科学与技术学院副院长

陶先平　南京大学计算机科学与技术系副主任

童维勤　上海大学计算机工程与科学学院计算机科学与技术系主任

薛向阳　复旦大学大数据学院副院长

虞慧群　华东理工大学信息科学与工程学院副院长

朱　敏　四川大学计算机学院副院长

前言

本书特色

根据中国信息通信研究院发布的《云计算发展白皮书》，云计算的发展，已经进入到第二个 10 年。全球云计算市场趋于稳定增长，尤其在中国，由于传统 IT 基础设施的发展相对发达国家有一定差距，云计算作为新兴的 IT 基础架构，仍然处于高速增长阶段，预计未来几年市场平均增长率在 22%左右，到 2021 年市场规模将达到 2 461 亿美元。云计算已经深入包括政府、金融、部队、运营商、教育等行业。目前市场上有众多的厂商，基于不同的云计算技术，提供了不同的解决方案。本书将围绕企业云平台建设的场景以及各类技术的落地应用，以及企业云平台的架构设计和实践，帮助读者更好的理解云平台最佳的落地实践。

Linux 下早期有以 Xen 为核心的虚拟化技术，但由于其代码的臃肿导致其未能并入 Linux 内核中，现在由以 Citrix 领导的社区维护。KVM(Kernel Based Virtualization)作为后起之秀在服务器虚拟化应用中已经可以完全替代 Xen，并且在桌面虚拟化中也有替代 Xen 的趋势。所以现在不少公司 IT 部门对 KVM 云平台研发与部署都有比较大的投入，以期构建完整的云平台。

本书的将首先提取私有云平台架构中的基本要素，然后再针对这些基本要素结合私有云的特点，“模型化”地讲解虚拟化技术核心知识，从而让读者能够比较自由且准确地修改架构以满足其需求。在最后，笔者将针对虚拟化中大家较为关心的技术实现细节提出具体的用例，也有关于运维、测试的一些建议。

读者对象

本书主要适合于以下读者：

(1) 云架构师；

（2）虚拟化研发工程师；

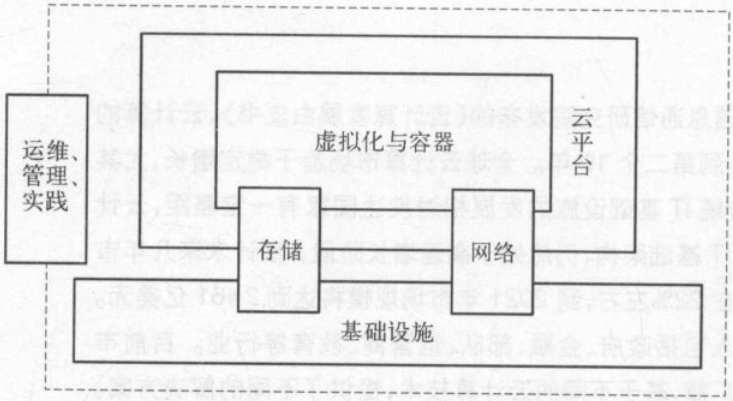
（3）运维工程师；

（4）产品工程师；

（5）云计算初学者；

如何阅读本书

在开始阅读之际，请读者先了解本书的整体结构，以有目的的阅读，每个章节部分都能在下图找到对应位置。



全书分为 4 篇：

第 1 篇以国内当下的私有云环境为背景，讲述各个私有云厂商的发力点，以及在典型客户中遇到的痛点；

第 2 篇从主流云平台中提取其通用架构，并结合私有云的特点阐架构原则，包括基础设施以及软件模型；

第 3 篇将系统地介绍私有云中的包括虚拟化、存储、网络在内的工具，除使用外，也将说明一下其基本原理，从而使读者更加正确地利用这些工具。对于开发者和入门者而言，这些章节也可作手册查询使用；

第 4 篇为笔者在开发、部署、维护私有云平台的实践经验、案例，列举现在私有云行业比较关心的种种问题并提供用例。

笔者期望本书能够帮助私有云从业者少走些弯路，在一些关键性问题上提供原则性指导和建议，由于经验有限，本书并不能事无巨细地涵盖私有云的各个方面，只期能达到“授之以渔”的目的。

目 录

第一篇 私有云现状

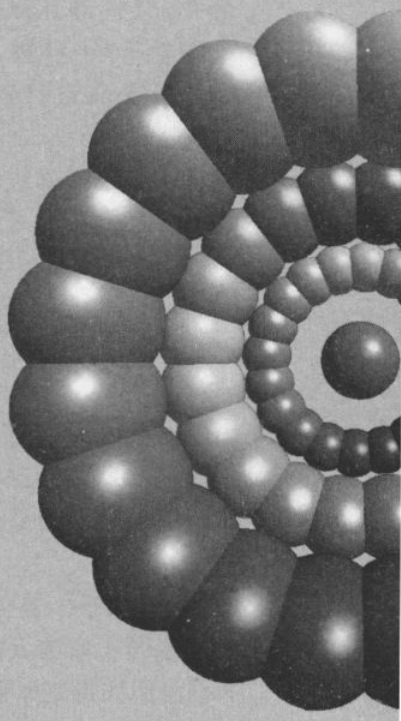
第二篇 架构设计

第三篇 私有云核心技术与应用

第四篇 实践与拓展

第一篇

私有云现状



第1章 私有云行业现状

随着技术的发展，公有云、私有云所提供的业务已经在部分领域互相融合，并且在行业客户方面也有较大突破，不再局限于IT企业而渗入了制造、银行、汽车等诸多行业中。相比公有云，私有云具有本地部署、管理受控、带宽充裕等特点而受到客户青睐。

本章首先将介绍公有云与私有云在通用标准上的区别，然后再通过私有云在一些典型行业落地时遇到的痛点，向读者概述现阶段国内私有云的状况。

1.1 私有云概念

私有云首先属于“云”的范畴，它仍然符合IaaS、PaaS、SaaS分层定义，以及更细化的虚拟化、云存储、CDN、负载均衡、应用程序平台和数据库服务等。近些年来国内外关于“云”的讨论与实践来从未中断，但由于其种类较多、厂家宣传过分渲染、受众群体较为分散等诸多因素，导致大众对“云”的理解存在些许偏颇。

首先，“云”的通用功能是提供某种IT服务，其服务仍然以计算、存储、网络等资源中的某个或某些元素为载体，并可通过量化指标测量其服务质量。这些元素在不同层面的组合即是不同种类的服务，比如IaaS层面提供虚拟机运行环境，PaaS层面提供应用运行环境，SaaS层面则直接提供终端应用。终端用户与服务提供商对“云”的理解有所不同——终端用户认为它是无所不在、随用随取、具有一定安全性和可靠性的服务实体，而服务提供商则将其定义为有弹性、可扩展的、前景广阔的IT基础架构。但不论从哪个角度考虑我们都会有一点共识，那就是“云即服务”。

公有云与私有云有几点关键差别，比如服务对象、基础设施规模等方面。公有云依托其强大的网络基础设施，面向整个互联网提供服务；私有云面向一些团体用户，公共网络资源较少。表1-1是公有云与私有云的在各方面的对比。

在某些情况下两者也存在交叉，比如有厂商会提供私有云下的公有云管理套件，也有公有云下自建私有云的解决方案，而这些也是当前“混合云”的一种存在形式。

表 1-1 公有云与私有云特点对比

	公 有 云	私 有 云
服务对象	互联网服务	企业内部服务
公网资源	充沛	较少
服务种类	丰富	单一/丰富
服务质量	不可控	可控
基础设施规模	极大	小/大

本书的私有云介绍将以提供基础架构的开源 IaaS、PaaS 为主，除特别说明，以后章节提及“私有云”即表示“IaaS”或“PaaS”，不代表其他类型服务。

1.2 多云管理平台

多云管理平台(Cloud management platforms)是一个可以同时提供公有云、私有云管理的平台。

在过去的十几年中，虚拟化和云计算技术已经帮助企业 IT 运维人员可以抽象和整合基础 IT 设施，并帮助企业数据中心实施转型，同时，虚拟化和云计算技术还极大地降低了企业投资 IT 部门的 TCO。过去，数据中心机器的上架、操作系统的安装、应用程序的配置需要耗费大量的人天。而随着虚拟化和云计算技术的发展，这些工作只需要系统管理员点击几下鼠标，然后从模板部署即可以轻松完成。

然而，随着业界公有云和私有云的共同发展，提供的服务也面向不同的场景。企业的业务也会根据不同的服务对象部署在不同的云平台上。通常，一些企业内部的业务，如开发测试环境，ERP，OA 系统，放在私有云上，一些对外提供服务的业务，如网站系统，会员服务系统，会放在公有云上。那么，CMP 在这种场景下就应运而生，CMP 的主要功能体现在以下三个方面。

(1) 提供公有云、私有云的统一管理能力

对企业 IT 人员来说，可以通过一套 Portal 实现不同云平台的统一管理能力。减少操作的复杂性。

(2) 快速地开通整个服务堆栈

企业 IT 人员能够通过 CMP，快速地跨私有云和公有云开通整个服务堆栈，而无需来回切换公有云和私有云的控制台，且可以减少一些复杂的配置操作。CMP 通常会封装各个云平台的 API，提供统一的外部 API，让跨云的自动化业务部署上线能够快速通过 API 实现。

(3) 精准地运营企业的 IT 资源

CMP 需要确保相关业务在不同平台下的运营效率最佳，并通过实时的监控和运营数据确保业务能够达到最佳的运行效率和最佳的性能。让企业 IT 人员能够像运营企业一样

来运营云环境。

CMP 的优势主要体现在以下几个方面。

(1) 选择多样

CMP 作为一个管理平台,允许企业 IT 人员自由选择对应的云平台供应商,企业 IT 人员可以充分满足企业内部用户的不同需求。

(2) 消费透明

对于企业内部的用户,通过 CMP,他们能够更清楚地看到自己的预算消费到了哪里。对于企业 IT 人员,他们能够充分证明自己提供了哪些服务。

(3) 提高跨云运营效率

通过 CMP,企业 IT 人员无需再辗转于各个云平台供应商提供的界面,只需在一套界面下即可完成所有操作。CMP 通常提供的 API 接口,也可以帮助开发测试运维人员快速完成资源的自动化开通和业务上线。

(4) 节约成本

通过 CMP 的运营数据,企业 IT 人员能够快速决定采取何种措施降低 IT 资源的使用成本。

(5) 降低风险

业务通过 CMP 部署在不同的云平台,或通过 CMP 实现业务的跨云备份,可以降低因为单一云平台的故障导致整个业务长时间不可访问的风险。

1.3 边缘计算

CMP 是云计算发展的必然补充,随着客户业务的不断发展,单一的云平台已经无法满足客户业务多样性的要求,为了实现更高效的使用云计算资源,对多个云平台的统一管理、使用和运营催生了 CMP 平台的发展。

而边缘计算是近几年兴起的新概念,目前,业界关于什么是边缘计算,还有着不同认知。

维基百科认为:边缘计算是一种分散式运算的架构,将应用程序、数据资料与服务的运算,由网络中心节点,移往网络逻辑上的边缘节点来处理。边缘运算将原本完全由中心节点处理大型服务加以分解,切割成更小与更容易管理的部分,分散到边缘节点去处理。边缘节点更接近于用户终端装置,可以加快资料的处理与传送速度,减少延迟。在这种架构下,资料的分析与知识的产生,更接近于数据资料的来源,因此更适合处理大数据。

Gartner 认为,边缘计算是一种新兴的拓扑结构,这个结构基于分散式的计算模型,该模型让计算节点尽可能地靠近数据和内容的源头。

边缘计算产业联盟认为,边缘计算是在靠近物或数据源头的网络边缘侧,融合网络、计算、存储、应用核心能力的分布式开放平台,就近提供边缘智能服务,满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。它可以作

为联接物理和数字世界的桥梁，使能智能资产、智能网关、智能系统和智能服务。

虽然主流机构对于边缘计算的精确定义众说纷纭，但是我们仍然能够看到边缘计算有如下几个特征。

分散式部署。边缘计算节点和传统的云计算节点不同，不再集中部署在某一个或多个数据中心内部，而是分散在不同的地域或区域，更加靠近数据的源头。

节约网络流量。因为边缘计算节点更加靠近数据源头，所以大量数据的采集和处理只需要在边缘侧完成，只有部分需要进一步处理的数据、备份的数据或处理的结果需要上传给中心云平台，因此，可以节约大量的网络流量。

提供计算、存储、网络能力。边缘计算节点在不同场景下需要提供不同的服务，但是几乎都需要计算、存储、网络功能，来进行边缘数据的计算处理，对处理后的数据进行存储，以及通过网络功能对外上传。

协同处理。边缘计算节点需要和云端节点进行通信，接受并执行云端资源调度管理策略，并和云端节点实现数据的协同处理和交换。

目前，国际主流的云计算巨头都已经开拓边缘计算业务，推出自己的边缘计算产品。

AWS 推出了 AWS IoT Greengrass，将云功能扩展到本地设备的软件。该软件使设备能够收集和分析更靠近信息源的数据，自主应对本地事件，并在本地网络上相互安全地通信。

微软也发布了 Azure IoT Edge 边缘侧产品，将云分析扩展到边缘设备，支持离线使用，同时聚焦边缘的人工智能应用。

谷歌也在 2018 年推出了硬件芯片 Edge TPU 和软件堆栈 Cloud IoT Edge，可将数据处理和机器学习功能扩展到边缘设备，使设备能够对来自其传感器的数据进行实时操作，并在本地进行结果预测。

阿里云推出了 Link IoT Edge，是阿里云能力在边缘端的拓展。它继承了阿里云安全、存储、计算、人工智能的能力，可部署于不同量级的智能设备和计算节点中，通过定义物模型连接不同协议、不同数据格式的设备，提供安全可靠、低延时、低成本、易扩展、弱依赖的本地计算服务。同时，可以结合阿里云的大数据、AI 学习、语音、视频等能力，打造出云边端三位一体的计算体系。

甚至原先一些主打私有云场景的厂商，也针对边缘计算场景，推出更加轻量级的边缘计算节点。能够以更低的成本，运行在边缘场景，提供计算、网络、存储的虚拟化功能，并提供业务的高可用保证，同时和云端协同工作。

可以看到，边缘计算将会是云计算的一个有益补充，随着物联网技术的发展，边缘计算将会成为未来云发展的一个不可替代的部分。

1.4 国内私有云企业与落地场景

目前国内市场的私有云可以按产品类型和客户群体进行垂直和水平细分。垂直细分

即按照私有云的相关产品进行分类，包括软件平台、服务器设施、接入终端等；水平细分即按照它们所面向行业客户类型进行划分。

1.4.1 企业细分

基础设施软件

根据云平台的服务提供内容，比如虚拟机、应用环境、云存储、计算、数据库、网络等可以将云分为 IaaS、PaaS、SaaS。表 1-2 是各个层次中的主流私有云市场典型项目或公司。

表 1-2 私有云平台典型项目/产品

云平台类型	项目/公司
IaaS	OpenStack、VMWare、ZStack 等
PaaS	Rancher、OpenShift、CloudFoundry 等
SaaS	Salesforce

国内市场中，在各个层次都有公司参与，其中以 IaaS 和 SaaS 最多、PaaS 相对较少。根据笔者的初步统计，国内目前在 IaaS 层拥有私有云产品（软件、硬件）并且有行业案例的公司超过 100 家，其中以桌面云为主要软件产品且运营两年以上的公司有超过 30 家；PaaS 层由于其受众以开发人员为主，所以在国内主要以互联网公司内部使用为主，但随着 Docker 的火热也有公司开始涉足私有云形式的 PaaS 平台，他们目前以中小型互联网公司、理工科学校等有大量软件开发需求的客户为主；SaaS 出现最早，国内电商公司在这方面有丰富的经验积累，并且私有云形式的 SaaS 也是最容易落地的，比如 CRM、OA、ERP 系统等。

基础设施硬件

服务器厂商在国内的私有云行业中处于“大卖家”的地位。首先无论是使用公有云、私有云，总免不了服务器的采购。同时我们可以从这些年来服务器厂商的产品目录中发现，他们中很多都开始以云计算、大数据为关键字准备了各种配置的服务器、存储和网络设备等，某些厂商还推出了类似 OpenRack 的一体化机柜、计算存储一体的超融合架构解决方案等。

比较值得注意的是，当政企、学校等单位的 IT 部门的提出需求时，首先会知道此消息的很可能是各一线集成商代表，又由于服务器采购在政企采购中的比例较大，此时集成商会考虑到价格、风险等因素而就客户需求的相关解决方案优先咨询服务器厂商，所以有一部分私有云平台厂商在进入相关行业领域时又主要依托于服务器厂商。

应用软件

无论是 IaaS 还是 PaaS，应用软件绝大多数情况下都会作为企业客户面向用户提供的服务载体，比如中间件、数据库、业务应用等。而随着云平台的普及，应用软件或多或少都