计算机类专业系统能力培养系列教材

云安全原理与实践

陈兴蜀　葛　龙　主编

罗永刚　曾雪梅　王海舟　王文贤　编著

HZ BOOKS
华章图书

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

云安全原理与实践 / 陈兴蜀，葛龙主编 . —北京：机械工业出版社，2017.7
（计算机类专业系统能力培养系列教材）

ISBN 978-7-111-57468-2

I. 云…　II. ①陈…　②葛…　III. 计算机网络 – 安全技术 – 教材　IV. TP393.08

中国版本图书馆 CIP 数据核字（2017）第 159613 号

本书系统地介绍了云安全的基本概念、原理和技术，主要内容包括云计算的安全风险分析、虚拟化安全、身份管理与访问控制、云数据安全、云运维安全、云服务的安全使用、云安全解决方案以及云计算相关的标准、法规等，并通过产业案例使读者掌握云安全的相关实践技术，从产业发展角度理解云安全的技术发展和趋势。

本书适合作为高等院校信息安全、计算机、电子工程及相关专业云安全课程的教材，也适合作为从事云安全工作的技术人员和研究人员的参考书。

HZ BOOKS
华章图书

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：朱　劼　　责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2017 年 8 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：16.5
书　　号：ISBN 978-7-111-57468-2　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

版权所有 • 侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所　韩光 / 邹晓东

FOREWORD

丛书序言

——计算机专业学生系统能力培养和系统课程设置的研究

未来的 5 ~ 10 年是中国实现工业化与信息化融合，利用信息技术与装备提高资源利用率、改造传统产业、优化经济结构、提高技术创新能力与现代管理水平的关键时期，而实现这一目标，对于高效利用计算系统的其他传统专业的专业人员需要了解和掌握计算思维，对于负责研发多种计算系统的计算机专业的专业人员则需要具备系统级的设计、实现和应用能力。

1. 计算技术发展特点分析

进入本世纪以来，计算技术正在发生重要发展和变化，在 20 世纪个人机普及和 Internet 快速发展基础上，计算技术从初期的科学计算与信息处理进入了以移动互联、物物相联、云计算与大数据计算为主要特征的新型网络时代，在这一发展过程中，计算技术也呈现出以下新的系统形态和技术特征。

（1）四类新型计算系统

1）嵌入式计算系统 在移动互联网、物联网、智能家电、三网融合等行业技术与产业发展中，嵌入式计算系统有着举足重轻和广泛的作用。例如，移动互联网中的移动智能终端、物联网中的汇聚节点、“三网融合”后的电视机顶盒等是复杂而新型的嵌入式计算系统；除此之外，新一代武器装备，工业化与信息化融合战略实施所推动的工业智能装备，其核心也是嵌入式计算系统。因此，嵌入式计算将成为新型计算系统的主要形态之一。在当今网络时代，嵌入式计算系统也日益呈现网络化的开放特点。

2）移动计算系统 在移动互联网、物联网、智能家电以及新型装备中，均以移动通信网络为基础，在此基础上，移动计算成为关键技术。移动计算技术将使计算机或其他信息智能终端设备在无线环境下实现数据传输及资源共享，其核心技术涉及支持高性能、低功耗、无线连接和轻松移动的移动处理机及其软件技术。

3）并行计算系统 随着半导体工艺技术的飞速进步和体系结构的不断发展，多核 / 众核处理机硬件日趋普及，使得昔日高端的并行计算呈现出普适化的发展趋势；多核技术就是在

处理器上拥有两个或更多一样功能的处理器核心，即将数个物理处理器核心整合在一个内核中，数个处理器核心在共享芯片组存储界面的同时，可以完全独立地完成各自操作，从而能在平衡功耗的基础上极大地提高 CPU 性能；其对计算系统微体系结构、系统软件与编程环境均有很大影响；同时，云计算也是建立在廉价服务器组成的大规模集群并行计算基础之上。因此，并行计算将成为各类计算系统的基础技术。

4）基于服务的计算系统 无论是云计算还是其他现代网络化应用软件系统，均以服务计算为核心技术。服务计算是指面向服务的体系结构（SOA）和面向服务的计算（SOC）技术，它是标识分布式系统和软件集成领域技术进步的一个里程碑。服务作为一种自治、开放以及与平台无关的网络化构件可使分布式应用具有更好的复用性、灵活性和可增长性。基于服务组织计算资源所具有的松耦合特征使得遵从 SOA 的企业 IT 架构不仅可以有效保护企业投资、促进遗留系统的复用，而且可以支持企业随需应变的敏捷性和先进的软件外包管理模式。Web 服务技术是当前 SOA 的主流实现方式，其已经形成了规范的服务定义、服务组合以及服务访问。

（2）“四化”主要特征

1）网络化 在当今网络时代，各类计算系统无不呈现出网络化发展趋势，除了云计算系统、企业服务计算系统、移动计算系统之外，嵌入式计算系统也在物联时代通过网络化成为开放式系统。即，当今的计算系统必然与网络相关，尽管各种有线网络、无线网络所具有的通信方式、通信能力与通信品质有较大区别，但均使得与其相联的计算系统能力得以充分延伸，更能满足应用需求。网络化对计算系统的开放适应能力、协同工作能力等也提出了更高的要求。

2）多媒体化 无论是传统 Internet 应用服务，还是新兴的移动互联网服务业务，多媒体化是其面向人类、实现服务的主要形态特征之一。多媒体技术是利用计算机对文本、图形、图像、声音、动画、视频等多种信息进行综合处理、建立逻辑关系和人机交互作用的新技术。多媒体技术使计算机可以处理人类生活中最直接、最普遍的信息，从而使得计算机应用领域及功能得到了极大的扩展，使计算机系统的人机交互界面和手段更加友好和方便。多媒体具有计算机综合处理多种媒体信息的集成性、实时性与交互性特点。

3）大数据化 随着物联网、移动互联网、社会化网络的快速发展，半结构化及非结构化的数据呈几何倍增长。数据来源的渠道也逐渐增多，不仅包括了本地的文档、音视频，还包括网络内容和社交媒体；不仅包括 Internet 数据，更包括感知物理世界的数据。从各种类型的数据中快速获得有价值信息的能力，称为大数据技术。大数据具有体量巨大、类型繁多、

价值密度低、处理速度快等特点。大数据时代的来临，给各行各业的数据处理与业务发展带来重要变革，也对计算系统的新型计算模型、大规模并行处理、分布式数据存储、高效的数据处理机制等提出了新的挑战。

4）智能化 无论是计算系统的结构动态重构，还是软件系统的能力动态演化；无论是传统 Internet 的搜索服务，还是新兴移动互联的位置服务；无论是智能交通应用，还是智能电网应用，无不显现出鲜明的智能化特征。智能化将影响计算系统的体系结构、软件形态、处理算法以及应用界面等。例如，相对于功能手机的智能手机是一种安装了开放式操作系统的手机，可以随意安装和卸载应用软件，具备无线接入互联网、多任务和复制粘贴以及良好用户体验等能力；相对于传统搜索引擎的智能搜索引擎是结合了人工智能技术的新一代搜索引擎，不仅具有传统的快速检索、相关度排序等功能，更具有用户角色登记、用户兴趣自动识别、内容的语义理解、智能信息化过滤和推送等功能，其追求的目标是根据用户的请求从可以获得的网络资源中检索出对用户最有价值的信息。

2. 系统能力的主要内涵及培养需求

（1）主要内涵

计算机专业学生的系统能力的核心是掌握计算系统内部各软件 / 硬件部分的关联关系与逻辑层次；了解计算系统呈现的外部特性以及与人和物理世界的交互模式；在掌握基本系统原理的基础上，进一步掌握设计、实现计算机硬件、系统软件以及应用系统的综合能力。

（2）培养需求

要适应“四类计算系统，四化主要特征”的计算技术发展特点，计算机专业人才培养必须“与时俱进”，体现计算技术与信息产业发展对学生系统能力培养的需求。在教育思想上要突现系统观教育理念，在教学内容中体现新型计算系统原理，在实践环节上展现计算系统平台技术。

要深刻理解系统化专业教育思想对计算机专业高等教育过程所带来的影响。系统化教育和系统能力培养要采取系统科学的方法，将计算对象看成一个整体，追求系统的整体优化；要夯实系统理论基础，使学生能够构建出准确描述真实系统的模型，进而能够用于预测系统行为；要强化系统实践，培养学生能够有效地构造正确系统的能力。

从系统观出发，计算机专业的教学应该注意教学生怎样从系统的层面上思考（设计过程、工具、用户和物理环境的交互），讲透原理（基本原则、架构、协议、编译以及仿真等），强化系统性的实践教学培养过程和内容，激发学生的辩证思考能力，帮助他们理解和掌控数字世界。

3. 计算机专业系统能力培养课程体系设置总体思路

为了更好地培养适应新技术发展的、具有系统设计和系统应用能力的计算机专门人才，

我们需要建立新的计算机专业本科教学课程体系，特别是设立有关系统级综合性课程，并重新规划计算机系统核心课程的内容，使这些核心课程之间的内容联系更紧密、衔接更顺畅。

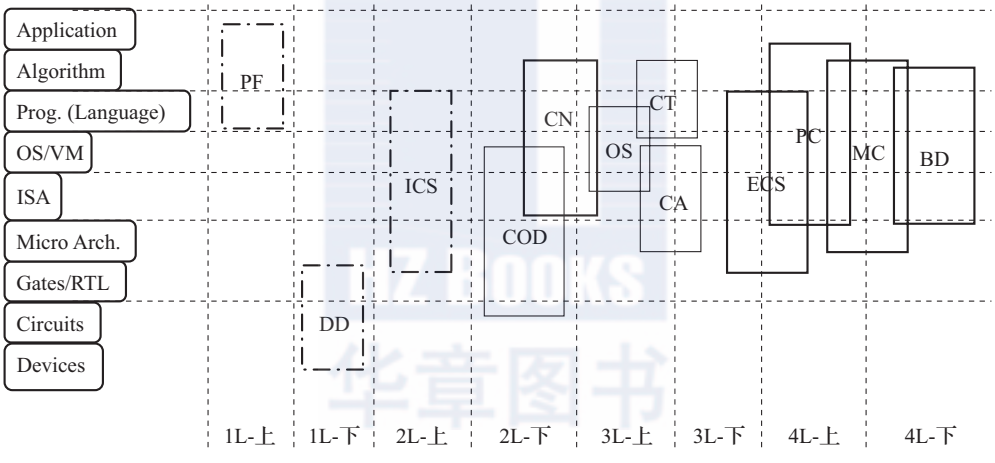
我们建议把课程分成三个层次：计算机系统基础课程、重组内容的核心课程、侧重不同计算系统的若干相关平台应用课程。

第一层次核心课程包括：“程序设计基础（PF）”“数字逻辑电路（DD）”和“计算机系统基础（ICS）”。

第二层次核心课程包括：“计算机组成与设计（COD）”“操作系统（OS）”“编译技术（CT）”和“计算机系统结构（CA）”。

第三层次核心课程包括：“嵌入式计算系统（ECS）”“计算机网络（CN）”“移动计算（MC）”“并行计算（PC）”和“大数据并行处理技术（BD）”。

基于这三个层次的课程体系中相关课程设置方案如下图所示。



图中左边部分是计算机系统的各个抽象层，右边的矩形表示课程，其上下两条边的位置标示了课程内容在系统抽象层中的涵盖范围，矩形的左右两条边的位置标示了课程大约在哪个年级开设。点划线、细实线和粗实线分别表示第一、第二和第三层次核心课程。

从图中可以看出，该课程体系的基本思路是：先讲顶层比较抽象的编程方面的内容；再讲底层有关系统的具体实现基础内容；然后再从两头到中间，把顶层程序设计的内容和底层电路的内容按照程序员视角全部串起来；在此基础上，再按序分别介绍计算机系统硬件、操作系统和编译器的实现细节。至此的所有课程内容主要介绍单处理器系统的相关内容，而计算机体系结构主要介绍各不同并行粒度的体系结构及其相关的操作系统实现技术和编译器实现技术。第三层次的课程没有先后顺序，而且都可以是选修课，课程内容应体现第一和第二

层次课程内容的螺旋式上升趋势，也即第三层次课程内容涉及的系统抽象层与第一和第二层次课程涉及的系统抽象层是重叠的，但内容并不是简单重复，应该讲授在特定计算系统中的相应教学内容。例如，对于“嵌入式计算系统（ECS）”课程，虽然它所涉及的系统抽象层与“计算机系统基础（ICS）”课程涉及的系统抽象层完全一样，但是，这两门课程的教学内容基本上不重叠。前者着重介绍与嵌入式计算系统相关的指令集体系结构设计、操作系统实现和底层硬件设计等内容，而后者着重介绍如何从程序员的角度来理解计算机系统设计与实现中涉及的基础内容。

与传统课程体系设置相比，最大的不同在于新的课程体系中有一门涉及计算机系统各个抽象层面的能够贯穿整个计算机系统设计和实现的基础课程：“计算机系统基础（ICS）”。该课程讲解如何从程序员角度来理解计算机系统，可以使程序员进一步明确程序设计语言中的语句、数据和程序是如何在计算机系统中实现和运行的，让程序员了解不同的程序设计方法为什么会有不同的性能等。

此外，新的课程体系中，强调课程之间的衔接和连贯，主要体现在以下几个方面。

1）“计算机系统基础”课程可以把“程序设计基础”和“数字逻辑电路”之间存在于计算机系统抽象层中的“中间间隔”填补上去并很好地衔接起来，这样，到 2L- 上结束的时候，学生就可以通过这三门课程清晰地建立单处理器计算机系统的整机概念，构造出完整的计算机系统的基本框架，而具体的计算机系统各个部分的实现细节再通过后续相关课程来细化充实。

2）“数字逻辑电路”“计算机组成与设计”“嵌入式计算系统”中的实验内容之间能够很好地衔接，可以规划一套承上启下的基于 FPGA 开发板的综合实验平台，让学生在一个统一的实验平台上从门电路开始设计基本功能部件，然后再以功能部件为基础设计 CPU、存储器和外围接口，最终将 CPU、存储器和 I/O 接口通过总线互连为一个完整的计算机硬件系统。

3）“计算机系统基础”“计算机组成与设计”“操作系统”和“编译技术”之间能够很好地衔接。新课程体系中“计算机系统基础”和“计算机组成与设计”两门课程对原来的“计算机系统概论”和“计算机组成原理”的内容进行了重新调整和统筹规划，这两门课程的内容是相互密切关联的。对于“计算机系统基础”与“操作系统”“编译技术”的关系，因为“计算机系统基础”以 Intel x86 为模型机进行讲解，所以它为“操作系统”（特别是 Linux 内核分析）提供了很好的体系结构基础。同时，在“计算机系统基础”课程中为了清楚地解释程序中的文件访问和设备访问等问题，会从程序员角度简单引入一些操作系统中的相关基础知识。此外，在“计算机系统基础”课程中，会讲解高级语言程序如何进行转换、链接以生成可执行代码的问题；“计算机组成与设计”中的流水线处理等也与编译优化相关，而且

“计算机组成与设计”以 MIPS 为模型机进行讲解，而 MIPS 模拟器可以为“编译技术”的实验提供可验证实验环境，因而“计算机系统基础”和“计算机组成与设计”两门课程都与“编译技术”有密切的关联。“计算机系统基础”“计算机组成与设计”“操作系统”和“编译技术”这四门课程构成了一组计算机系统能力培养最基本的核心课程。

从“计算机系统基础”课程的内容和教学目标以及开设时间来看，位于较高抽象层的先行课（如程序设计基础和数据结构等课程）可以按照原来的内容和方式开设和教学，而作为新的“计算机系统基础”和“计算机组成与设计”先导课的“数字逻辑电路”，则需要对传统的教学内容，特别是实验内容和实验手段方面进行修改和完善。

有了“计算机系统基础”和“计算机组成与设计”课程的基础，作为后续课程的操作系统、编译原理等将更容易被学生从计算机系统整体的角度理解，课程内容方面不需要大的改动，但是操作系统和编译器的实验要以先行课程实现的计算机硬件系统为基础，这样才能形成一致的、完整的计算机系统整体概念。

本研究还对 12 门课程的规划思路、主要教学内容及实验内容进行了研究和阐述，具体内容详见公开发表的研究报告。

4. 关于本研究项目及本系列教材

机械工业出版社华章公司在较早的时间就引进出版了 MIT、UC-Berkeley、CMU 等国际知名院校有关计算机系统课程的多种教材，并推动和组织了计算机系统能力培养相关的研究，对国内计算机系统能力培养起到了积极的促进作用。

本项研究是教育部 2013 ~ 2017 年计算机类专业教学指导委员会“计算机类专业系统能力培养研究”项目之一，研究组成员由国防科技大学王志英、北京航空航天大学马殿富、西北工业大学周兴社、南开大学吴功宜、武汉大学何炎祥、南京大学袁春风、北京大学陈向群、中国科技大学安虹、天津大学张刚、机械工业出版社华章公司温莉芳等组成，研究报告分别发表于中国计算机学会《中国计算机科学技术发展报告》及《计算机教育》杂志。

本系列教材编委会在上述研究的基础上对本套教材的出版工作经过了精心策划，选择了对系统观教育和系统能力培养有研究和实践的教师作为作者，以系统观为核心编写了本系列教材。我们相信本系列教材的出版和使用，将对提高国内高校计算机类专业学生的系统能力和整体水平起到积极的促进作用。

“计算机类专业系统能力培养系列教材”编委会

2014 年 5 月

本书编委会

主编　陈兴蜀（四川大学）

葛　龙（四川大学）

编委　（按拼音顺序排列）

董斌雁（阿里云公司）　　李　俊（阿里云公司）

李兰柱（阿里云公司）　　李妹芳（阿里云公司）

罗永刚（四川大学）　　苏建东（阿里云公司）

王海舟（四川大学）　　王文贤（四川大学）

王晓斐（阿里云公司）　　邬　怡（阿里云公司）

肖　力（阿里云公司）　　杨　宁（阿里云公司）

曾雪梅（四川大学）

特别感谢

肖　力（阿里云公司）

李妹芳（阿里云公司）

HZ BOOKS 华章图书

PREFACE

序

当前，一场科技革命浪潮正席卷全球，这一次，IT 技术是主角之一。云计算、大数据、人工智能、物联网，这些新技术正加速走向应用。很快，它们将渗透至我们生产、生活中的每个角落，并将深刻改变我们的世界。

在这些新技术当中，云计算作为基础设施，将全面支撑各类新技术、新应用。我认为：云计算，特别是公共云，将成为这场科技革命的承载平台，全面支撑各类技术创新、应用创新和模式创新。

作为一种普惠的公共计算资源与服务，云计算与传统 IT 计算资源相比有以下几个方面的优势：一是硬件的集约化；二是人才的集约化；三是安全的集约化；四是服务的普惠化。

公共云计算的快速发展将带动云计算产业进入一个新的阶段，我们可以称之为“云计算 2.0 时代”，云计算对行业演进发展的支撑作用将更加凸显。

云计算是“数据在线”的主要承载。“在线”是我们这个时代最重要的本能，它让互联网变成了最具渗透力的基础设施，数据变成了最具共享性的生产资料，计算变成了随时随地的公共服务。云计算不仅承载数据本身，同时也承载数据应用所需的计算资源。

云计算是“智能”与“智慧”的重要支撑。智慧有两大支撑，即网络与大数据。包括互联网、移动互联网、物联网在内的各种网络，负责搜集和共享数据；大数据作为“原材料”，是各类智慧应用的基础。云计算是支撑网络和大数据的平台，所以，几乎所有智慧应用都离不开云计算。

云计算是企业享受平等 IT 应用与创新环境的有力保障。当前，企业创新，特别是小微企业和创业企业的创新面临 IT 技术和 IT 成本方面的壁垒。云计算的出现打破了这一壁垒，IT 成为唾手可得的基础性资源，企业无须把重点放在 IT 支撑与实现上，可以更加聚焦于擅长的领域进行创新，这对提升全行业的信息化水平以及激发创新创业热情将起到至关重要的作用。

除了发挥基础设施平台的支撑作用外，2.0 时代的云计算，特别是公共云计算对产业的影响将从量变到质变。我认为，公共云将全面重塑整个 ICT 生态，向下定义数据中心、IT 设备，甚至是 CPU 等核心器件，向上定义软件与应用，横向承载数据与安全，纵向支撑人工智能的技术演进与应用创新。

对我国来说，发展云计算产业的战略意义重大。我认为，云计算已不仅仅是“ IT 基础设施”，它将像电网、移动通信网、互联网、交通网络一样，成为“国家基础设施”，全面服务国家多项重大战略的实施与落地。

云计算是网络强国建设的重要基石。发展云计算产业，有利于我国实现 IT 全产业链的自主可控，提高信息安全保障水平，并推动大数据、人工智能的发展。

云计算是提升国家治理能力的重要工具。随着大数据、人工智能、物联网等技术应用到智慧城市、智慧政务建设中，国家及各城市的治理水平和服务能力大幅提升，这背后，云计算平台功不可没。

云计算将全面推动国家产业转型升级。云计算将支撑“中国制造 2025”“互联网 +”战略，全面推动“两化”深度融合。同时，云计算也为创新创业提供了优质土壤，在“双创”领域，云计算已真正成为基础设施。

在 DT 时代，我认为计算及计算的能力是衡量一个国家科技实力和创新能力的重要标准。只有掌握计算能力，才具备全面支撑创新的基础，才有能力挖掘数据的价值，才能在重塑 ICT 生态过程中掌握主导权。

接下来的几年，云计算将成为全球科技和产业竞争的焦点。目前，我国的云计算产业具备和发达国家抗衡的能力，而我们对数据的认知、驾驭能力及对资源的利用开发和人力也是与发达国家等同的。因此，我们正处在一个“黄金窗口期”。

我一直认为，支撑技术进步和产业发展的最主要力量是人才，未来世界各国在云计算、大数据、AI 等领域的竞争，在某种程度上会转变为人才之争。因此，加强专业人才培养将是推动云计算、大数据产业发展的重要抓手。

由于是新兴产业，我国云计算、大数据领域的人才相对短缺。作为中国最大的云计算服务企业，阿里云希望能在云计算、大数据领域的人才培养方面做出努力，将我们在云计算、大数据领域的实践经验贡献到高校的教育中，为高校的课程建设提供支持。

与传统 IT 基础技术理论相比，云计算和大数据更偏向应用，而这方面恰恰是阿里云的优势。因此，我们与高校合作，优势互补，将计算机科学的理论和阿里云的产业实践融合起来，让大家从实战的角度认识、掌握云计算和大数据。

我们希望通过这套教材，把阿里云一些经过检验的经验与成果分享给全社会，让众多计算机相关专业学生、技术开发者及所有对云计算、大数据感兴趣的企业和个人，可以与我们一起推动中国云计算、大数据产业的健康快速发展！

胡晓明

阿里云总裁

HZ BOOKS
华章图书

P R E F A C E

前　言

近几年，云计算（Cloud Computing）迅速发展，从美国的亚马逊到我国的阿里云，国内外的云计算服务提供商提供了类型繁多、性价比高的 IT 服务模式，新的服务类型还在不断推出，并在各行各业得到了广泛应用。云计算是信息技术发展过程中的一次巨大变革，众多国家政府以及大型 IT 企业都制定了云计算发展战略规划，以引领或适应技术变革的趋势。

在云计算发展的同时，其安全问题也日益凸显。CSA（Cloud Security Alliance，云安全联盟）在 2016 年 2 月发布了《2016 年 12 大顶级云计算安全威胁》，指出了包括数据泄露、系统漏洞、拒绝服务、共享技术等在内的 12 项云安全威胁，云计算的安全问题逐渐成为制约其快速应用和发展的重要因素。

为了让读者全面了解云计算中的安全问题，本书从云计算的基本概念入手，由浅入深地分析了云计算中面临的安全威胁、云计算服务应具备的安全能力、如何安全地使用云计算服务，以及云安全的相关标准等。本书强调云计算的技术特点，系统介绍了云计算服务过程中提供方、使用方所关注的安全问题，并将理论与实践紧密结合。在本书撰写过程中，四川大学网络空间安全研究院与阿里云深度合作，共同探讨教材的大纲、内容，并同时面向研究生和高年级本科生授课，探索高校课程和教材建设的创新合作模式。本书是学术研究成果与企业实践的结合，关键技术章节配有基于阿里云平台的实验，“理论 + 实践”的模式使得读者能够更好地理解教材所阐述的关键知识点，通过动手实践让读者加深对理论知识的理解。

本书分为四个部分，包含 11 章，各个部分的内容组织安排如下：

第一部分（包括第 1 章和第 2 章）主要介绍云计算相关的基础知识。其中，第 1 章概述云计算的发展历程以及基本概念，并对云服务中的角色和责任进行了划分和界定，为读者后续的深入学习奠定基础。第 2 章从技术、管理以及法律法规三个方面分析了云计算的安全风险，并给出了进行云计算安全设计时需要考虑的原则。

第二部分（包括第 3~8 章）剖析云计算服务的安全能力、运维安全以及云安全技术的发展。其中，第 3 章讨论主机虚拟化带来的安全问题，详细分析其面临的虚拟机信息窃取、虚拟机逃逸、Rootkit 攻击等安全威胁及其对应的安全解决方案。第 4 章阐释网络虚拟化的安全问题，分析 IaaS 环境下网络安全域的划分与构建，并介绍阿里云的 VPC，最后提出两种针对虚拟网络的安全服务接入机制。第 5 章介绍云计算下的身份认证、授权管理以及操作审计。第 6 章根据云数据安全的生命周期，分析数据从创建到销毁各个阶段面临的安全问题以及对应的关键保护技术。第 7 章介绍云运维的基本内容，分析其相对于传统运维的区别以及应注意的问题。第 8 章结合下一代网络应该考虑的技术，介绍零信任模型、MSSP、APT 攻击防御、大数据安全分析等内容。

第三部分（包括第 9 章和第 10 章）介绍如何安全地使用云计算服务。其中，第 9 章针对云用户控制权弱化的问题，区分了云计算服务的角色并进行了责任划分，然后从用户的角度介绍云计算服务的使用过程。第 10 章结合不同应用场景介绍云安全解决方案。

第四部分（包括第 11 章）介绍当前云计算服务的安全标准和管理机制。第 11 章阐释国内外云计算服务的安全管理、云安全标准以及管理规范。

本书的层次结构清晰，内容循序渐进，可作为高等院校信息安全、计算机及其他信息学科云安全相关课程的教材，也可以作为广大云计算运维人员、云计算安全开发人员以及对云安全感兴趣的读者的参考书籍。作为教材时，可参考第 3 章到第 5 章的最佳实践进行课程实验，包括第 3 章云计算平台中的虚拟化主机安全管理，第 4 章 VPC 的相关实验，第 5 章身份管理、权限管理以及操作审计的实践等。本书为读者提供云安全问题的系统知识，并借助阿里云的实践使读者深入理解关键技术，提升读者对云安全理论的掌握和应用能力。

本书由陈兴蜀主持编写，第 1~2 章和第 11 章由陈兴蜀编写，第 3 章、第 6 章由曾雪梅编写，第 4~5 章和第 8 章由葛龙编写，第 7 章由罗永刚编写，第 9 章由王海舟编写，第 10 章由王文贤编写。本书在写作的过程中得到了四川大学网络空间安全研究院师生的大力支持，王毅桐、金鑫、邵国林、杨露、陈广瑞、苑中梁、车奔、陈佳昕、赵成、陈蒙蒙、赵丹丹、王煜骢、王伟、王小艳、滑强、李敏毓、马晨曦等进行了大量的工作，没有他（她）们的支持与帮助，很难完成本书编写工作。

本书是教育部 – 阿里云产学合作专业综合改革项目的规划教材，同时获得四川大学研究生课程建设项目的支持。

感谢阿里云团队对本书编写给予的大力支持，李妹芳、苏建东、杨宁、李俊、李兰柱、董斌雁、安忍、王晓斐、邬怡、杨宁、肖力等阿里云的专家为本书的编写提供了大量帮助，尤其

在讨论书稿内容、提出重要建议、申请阿里云平台资源、提供参考资料等方面给予了重要支持。

同时还要感谢机械工业出版社华章分社朱劼编辑和出版团队的辛勤工作。

本书仅代表作者及研究团队对于云计算安全的观点，由于水平有限，书中难免存在不准确或不足之处，恳请读者批评指正，以便后续改进和完善。

编者

2017 年 5 月

HZ BOOKS
华章图书

CONTENTS

目　录

HZ BOOKS 华章图书

HZ BOOKS 华章图书

第四部分　云计算的安全标准和管理机制

第 11 章　云计算安全管理和标准 ……212

HZ BOOKS
华章图书

PART I

第一部分

云安全基础

HZ BOOKS
华章图书

CHAPTER 1

第1章

云计算基础

网络基础设施，特别是宽带的普及，使得网络逐渐变得和水、电、煤气一样，成为标准的基础设施。全球经济一体化发展、企业 IT 的成熟和计算能力提升、社会需求的膨胀、商业规模的扩大，以及全球产业从制造型向服务型、创新型转变，推动了云计算的产生与发展。云计算并非来自学术理论，而是直接产生于企业需求，它更关心如何扩展系统、如何方便 IT 管理。云计算的最终目标是将计算、服务和应用作为一种公共设施提供给公众，使人们能够像使用水、电、煤气和电话那样使用计算资源。

时代的需要为云计算提供了良好的发展机遇。云计算从产生到发展仅仅十余年，众多的企业或组织，从全球企业、政府机构、非营利组织到小型初创公司，出于各种原因，都积极地采用了这项技术，通过部署云系统来为客户提供存储、备份、数据、计算、应用等各种服务。

云计算已经成为当前 IT 产业的一个重要热点。那么到底什么是云计算？云计算的产生、发展、概念、模式又是什么？为此，本章将首先介绍云计算的相关基础知识，包括云计算的起源与发展、主要参与的厂商与社区，接下来介绍云计算中的基本概念、术语以及云计算的主要特性、服务模式和部署模式等，使读者对云计算有初步了解。

1.1 云计算的发展历程

云计算的出现是技术和计算模式不断发展和演变的结果。云计算的基础思想可以追溯到半个世纪以前。1961 年，MIT（美国麻省理工学院）的教授 John McCarthy 提出“计算力”的概念，认为可以将计算资源作为像电力一样的基础设施按需付费使用；1966 年，Douglas Parkhill 在《计算机工具的挑战》（The Challenge of the Computer Utility）一书中对现今云计算的几乎所有特点，如作为公共设施供应、弹性供应、实时供应以及具备“无限”供应能力等，甚至云计算的服务模式，如公共模式、私有模式、政府以及社团模式，进行了详尽的讨论。

几十年来，计算模式的发展经历了早期的单主机计算模式、个人计算机普及后的 C/S（客户机 / 服务器）模式、网络时代的 B/S（浏览器 / 服务器）模式的变迁，如今大量的软件以服务的形式通过互联网提供给用户，传统的 IDC（Internet Data Center，互联网数据中心）逐渐不能满足新环境下业务的需求，于是云计算应运而生。

1.1.1　云计算的起源与发展

1996 年，在康柏公司的一份内部文件中首次提到了现代意义上的“云计算”概念，但是云计算概念的流行却是在 10 年之后。2006 年，谷歌推出了“ Google 101 计划”，并正式提出“云”的概念和理论。该计划基于谷歌员工比希利亚的设想，初衷是设置一门课程，着重引导学生们进行“云”系统的程序开发。随着计划的不断发展，2007 年 10 月，谷歌、IBM 联合了美国 6 所知名大学帮助学生在大型分布式计算系统上进行开发，当时的 IBM 发言人就指出这种所谓的“大型分布式计算系统”就是云计算，明确将云计算作为一个新概念提出。由于当年谷歌和 IBM 在信息技术领域处于领军地位，使得云计算的概念刚被提出就立刻有大量的公司、传统 IT 技术人员和媒体追逐，甚至在云计算的概念中提出一系列的 IT 创新。图 1-1 给出了目前已知最早使用“云计算”概念的文件。

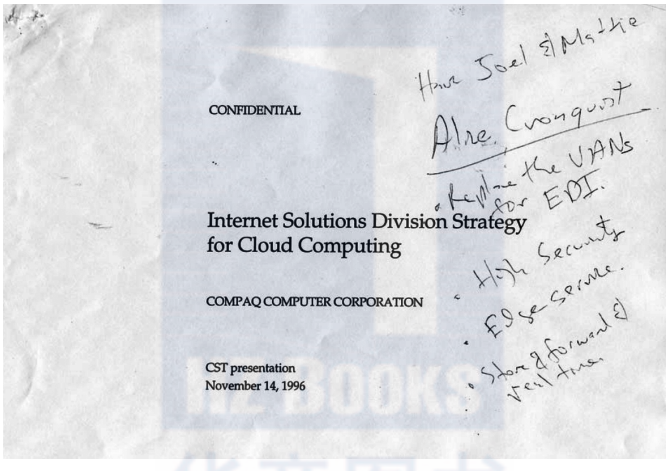


图 1-1　目前已知最早使用的“云计算”概念的文件

相比于谷歌和 IBM，亚马逊在当年的影响力有限，虽然它在 2006 年就发布了云计算产品 Amazon Elastic Compute Cloud（ EC2 ），但在业界并未引发太大的关注，因为 EC2 产品作为商业项目对云计算概念的普及并不像 IBM-Google 的项目那么明显。随着 2007 年 10 月 IBM-Google 并行计算项目的提出让云计算概念迅速普及，客户渴望得到商用云计算服务，EC2 恰逢其时，因为此时 EC2 已是一个相当商业化的云计算产品了，并且拥有完善的云计算服务，于是短时间内亚马逊在云计算乃至信息技术领域声名鹊起，由此奠定了亚马逊在云计算领域的领军位置。

随后进入云计算的飞速发展时期，一大批优秀的 IT 企业积极投入到云计算行业中，带来了一大批优秀的云计算产品和解决方案，如 IBM 的蓝云计划、亚马逊的 AWS、微软的 Azure 等，与此同时也有一批开源项目（如 OpenStack、CloudStack 等）也加入到云计算的“大家庭”，为云计算行业开启了一个百花齐放的新时代。

近几年，中国在云计算领域也有了长足的进步，涌现了如阿里云、青云、华为云、天翼云等优秀的公有云解决方案。由中国信息通信研究院发布的《中国公共云服务发展调查报告》显示，公有云服务市场规模正在以每年 40% 左右的增幅增长，企业的“云”化趋势愈加显著，云计算的大潮正以不可阻挡之势向前推进。

云计算相关技术的具体发展历程及重大标志性事件如下：

1959 年 6 月，Christopher Strachey 发表了有关虚拟化的论文，而虚拟化是现在云计算架构的基石。

1961 年，John McCarthy 提出“计算力”的概念，以及通过公用事业销售计算机应用的思想。

1984 年，Sun 公司的联合创始人 John Gage 将分布式计算技术带来的改变描述为“网络就是计算机”，而现在云计算正在将该理念变成现实。2006 年，该公司推出了基于云计算理论的“ BlackBox”计划，旨在以创新的系统改变整个数据中心环境。2008 年 5 月，Sun 公司又宣布推出“Hydrazine”计划。

1998 年，威睿（VMware）公司成立并首次引入 x86 虚拟化技术。x86 虚拟化技术是指在 x86 的系统中使一个或几个客户操作系统在一个主操作系统下运行的技术。2009 年 4 月，该公司推出 VMware vSphere 4。2009 年 9 月，VMware 又推出 vCloud 计划，以构建全新云服务。

1999 年，Marc Andreessen 创建了第一个商业化的 IaaS 平台——LoudCloud。同年 Salesforce.com 公司成立，它提出云计算和 SaaS 的理念，开创了新的里程碑，宣布“软件终结”革命的开始。2008 年 1 月，Salesforce.com 推出 DevForce 平台，旨在帮助开发人员创建各种商业应用，例如根据需要创建数据库应用、管理用户之间的协作等，Sales force.com 推出的 Force.com 平台是世界上第一个 PaaS 的应用。

2004 年，谷歌发布 MapReduce 论文，MapReduce 是 Hadoop 的主要组成部分。2006 年 8 月，“云计算”的概念由谷歌行政总裁 Eric Schmidt 在搜索引擎大会（SES San Jose 2006）上首次提出。2008 年，Doug Cutting 和 Mike Cafarella 实现了 MapReduce 和 HDFS，在此基础上，Hadoop 成为优秀的分布式系统的基础架构。

2005 年，亚马逊公司宣布推出 AWS（Amazon Web Service）云计算平台。AWS 是一组允许通过程序访问亚马逊的计算基础设施的服务。次年又推出了在线存储服务 S3（Simple Storage Service）和弹性计算云 EC2（Elastic Compute Cloud）等云服务。2007 年 7 月，该公司推出简单队列服务（Simple Queue Service，SQS），SQS 是所有基于 Amazon 网格计算的基础。2008 年 9 月，亚马逊公司与甲骨文公司合作，使得用户可以在云中部署甲骨文软件和备份甲骨文数据库。

2007 年 3 月，戴尔公司成立数据中心解决方案部门，为 Windows Azure、Facebook 和 Ask.com 三家公司提供云基础架构。2008 年 8 月，戴尔公司在美国专利商标局申请“云计算”商标，旨在加强对该术语的控制权。2010 年 4 月，戴尔又推出 PowerEdgeC 系列云计算服务器和相关服务。

2007 年 11 月，IBM 公司推出“蓝云”（Blue Cloud）计划，旨在为客户带来即刻使用的云计算。2008 年 2 月，IBM 公司宣布在中国无锡产业园建立第一个云计算中心，该中心将为

中国新兴软件公司提供接入虚拟计算环境的能力。同年 6 月，IBM 公司宣布成立 IBM 大中华区云计算中心。2010 年 1 月，又与松下公司合作达成了当时全球最大的云计算交易。

2008 年 2 月，EMC 中国研发集团正式成立云架构和服务部，该部门联合云基础架构部和 Mozy、Pi 两家公司，共同形成 EMC 云战略体系。同年 6 月，EMC 中国研发中心加入道里可信基础架构项目，该项目主要研究云计算环境下信任和可靠度保证的全球研究协作，主要成员还有复旦大学、华中科技大学、清华大学和武汉大学四所高校。

2008 年 7 月，云计算试验台 Open Cirrus 推出，它由 HP、Intel 和 Yahoo 三家公司联合创建。

2008 年 9 月，思杰公司公布云计算战略并发布新的思杰云中心产品系列（Citrix Cloud Center，C3），它整合了经云验证的虚拟化产品和网络产品，可支持当时大多数大型互联网和 Web 服务提供商的业务运作。

2008 年 10 月，微软公司的 Windows Azure Platform 公共云计算平台发布，开始了微软公司的云计算之路。2010 年 1 月，与 HP 公司合作一起发布了完整的云计算解决方案。同月，微软公司又发布 Microsoft Azure 云平台服务，通过该平台，用户可以在微软公司管理的数据中心的全球网络中快速生成、部署和管理应用程序。

2008 年，亚马逊、谷歌和 Flexiscale 等公司的云服务相继发生宕机故障，引发业界对云计算安全的讨论。

2009 年 1 月，阿里巴巴集团旗下子公司阿里软件在江苏南京建立首个“电子商务云计算中心”，该中心与杭州总部的数据中心一起协同工作，形成规模能够与谷歌匹敌的服务器集群“商业云”体系。

2009 年 3 月，思科公司发布集存储、网络和计算功能于一体的统一计算系统（Unified Computing System，UCS），又在 5 月推出了云计算服务平台，正式迈入云计算领域。同年 11 月，思科与 EMC、VMware 建立虚拟计算环境联盟，旨在让用户能够快速地提高业务敏捷性。2011 年 2 月，思科系统正式加入 OpenStack，该平台由美国航空航天局（National Aeronautics and Space Administration，NASA）和托管服务提供商 Rackspace Hosting 共同研发，使用该平台的公司还有微软、Ubuntu、戴尔和超微半导体公司（Advanced Micro Devices，AMD）等。

2009 年 11 月，中国移动启动云计算平台“大云”（Big Cloud）计划，并于次年 5 月发布了“大云平台”1.0 版本。“大云”产品包括五部分：分布式海量数据仓库、弹性计算系统、云存储系统、并行数据挖掘工具和 MapReduce 并行计算执行环境。

2010 年 4 月，Intel 公司在 Intel 信息技术峰会（Intel Developer Forum，IDF）上提出互联计算，目的是让用户从 PC（客户端）、服务器（云计算）到移动、车载、便携等所有个性化互联设备获得熟悉且连贯一致的个性化应用体验，Intel 公司此举的目的是试图用 x86 架构统一嵌入式、物联网和云计算领域。

2010 年 7 月，美国太空总署联合 Rackspace、AMD、Intel、戴尔等厂商共同宣布“OpenStack”开源计划。

2011 年 6 月，美国电信工业协会制定了云计算白皮书，分析了一体化的挑战和云服务与传统的美国电信标准之间的机会。

2015 年 10 月，阿里巴巴集团董事局主席马云和 CEO 张勇在年报致投资者的公开信中表示，全球化、农村经济和大数据云计算将成为阿里未来十年的发展大方向。

1.1.2　云计算的主要厂商与社区

云计算的高速发展离不开优秀企业和开源社区的推动，接下来就简单介绍一下参与云计算发展过程的企业和社区。

目前参与云计算的厂商主要包括传统的 IT 硬件厂商、互联网企业转型的云计算服务提供商和拥有强大研发实力的软件厂商，以下将对应介绍三个典型代表企业。

IBM 作为行业中的佼佼者，拥有强大的技术研发力量和商业客户基础，可以为用户提供从底层存储、服务器、交换机等硬件到应用层软件（例如 Lotus Domino，Tivoli Storage，DB2 等应用软件）的整套解决方案，凭借多年硬件研发和运营大型数据中心的经验，IBM 在云计算的潮流中占有了一席之地。

亚马逊一开始是一家互联网服务提供商，但早在 2006 年就建立了自己的弹性计算云 EC2，作为最早提供云计算平台服务的公司，亚马逊积累了大量的云计算技术，在云计算领域异军突起，成为最大的云计算服务提供商。

与上述两家企业不同，VMware 作为全球最大的虚拟化软件提供商，拥有成熟的虚拟化解决方案，而虚拟化技术是云计算发展最关键的技术之一，虽然它自己不提供云服务，但是其提供的 VMware vSphere 是业界领先且可靠的虚拟化平台，为云计算平台提供了可靠的底层保障。

随着企业在云平台项目上的拓展，一些开源云计算项目也不断出现，如 OpenNebula、OpenStack、CloudStack 等。

与后两者相比，OpenNebula 更像是一款为云计算打造的开源工具集，配合 KVM、XEN 或者 ESXi 一起建立和管理私有云，同时也可以与 Amazon EC2 相配合来管理混合云。

OpenStack 是一个开源的云计算管理平台项目，它旨在为云的建设和管理过程提供软件。目前，OpenStack 社区有近 4 万名开发者，近 600 家企业参与到 OpenStack 代码的提交和更新当中，用户只需要将 OpenStack 作为基础设施即服务（IaaS）资源的通用前端即可实现对自己云环境的创建和管理，这大大简化了云环境的部署过程，并为其带来良好的可扩展性。

CloudStack 也是一个开源的云操作系统，它可以帮助用户利用自己的硬件提供类似于 Amazon EC2 的公共云服务，通过协调用户的虚拟化资源为用户搭建一个完整的云计算环境。与此同时，CloudStack 兼容 Amazon API，这使得用户可以在现有的架构上建立自己的云服务并帮助用户协调服务器、存储和网络资源，完成一个 IaaS 平台的构建。

1.2　云计算的基本概念

1.2.1　云计算的定义与术语

云计算本身是一个非常抽象的概念，要准确地为其进行定义并不是一件容易的事。国内外的公司、标准组织和学术机构对它的定义也不尽相同。

1）亚马逊将云计算定义为：通过互联网以按使用量定价方式付费的 IT 资源和应用程序的按需交付。

2）IBM 的定义为：①一种新的用户体验和业务模式。云计算是一种新出现的计算模式，它是一个计算资源池，并将应用、数据及其他资源以服务的形式通过网络提供给最终用户。②一种新的架构管理方法。云计算采用一种新的方式来管理大量的虚拟化资源，从管理的角度来看云计算，它可以是多个小的资源组装成大的资源池，也可以是大型资源虚拟化成多个小型资源，而最终目的都是提供服务。

3）微软的定义为：云计算就是通过标准和协议，以实用工具形式提供的计算功能。

4）美国加州大学伯克利分校在《伯克利云计算白皮书》中对云计算的定义为：云计算是互联网上的应用服务，以及在数据中心提供这些服务的软硬件设施。互联网上的应用服务一直被称作“软件即服务”，而数据中心的软硬件设施就是所谓的“云”。

5）美国国家标准技术研究所 NIST 对云计算的定义是：云计算是一种资源利用模式，它能以方便、友好的方式通过网络按需访问可配置的计算机资源池（例如网络、服务器、存储、应用程序和服务），并以最小的管理代价快速提供服务。

6）我国相关部门在参考了国际组织和其他国家相关标准和法规后，于 2014 年发布国家标准 GB/T 31167—2014《信息安全技术　云计算服务安全指南》，其中对云计算进行了如下定义：

“以按需自助获取、管理资源的方式，通过网络访问可扩展的、灵活的物理或虚拟共享资源池的模式。”（注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。）

该标准也对云计算涉及的相关术语进行了定义：

- **云计算服务**：使用定义的接口，借助云计算提供一种或多种资源的能力。
- **云服务商**：提供云计算服务的参与方。云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。
- **客户**：为使用云计算服务同云服务商建立商业关系的参与方。
- **第三方评估机构**：独立于云计算服务相关方的专业评估机构。
- **云基础设施**：由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。硬件资源指所有的物理计算资源，包括服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链接和接口等）及其他物理计算基础元素。资源抽象控制组件对物理计算资源进行软件抽象，云服务商通过这些组件提供和管理对物理计算资源的访问。
- **云计算平台**：云服务商提供的云基础设施及其上的服务软件的集合。
- **云计算环境**：云服务商提供的云计算平台，及客户在云计算平台之上部署的软件及相关组件的集合。

1.2.2　云计算的主要特性

GB/T 31167—2014《信息安全技术　云计算服务安全指南》中描述了云计算的五个特性。

1. 按需自助服务

在不需或仅需较少云服务商人员参与的情况下，客户能根据需要获得所需计算资源，如自主确定资源占用时间和数量等。比如对于 IaaS 服务，客户可以通过云服务商的网站自助选择需要购买的虚拟机数量、每台虚拟机的配置（包括 CPU 数量、内存容量、磁盘空间、对外网络带宽等）、服务使用时间等。

2. 泛在接入

客户通过标准接入机制，利用计算机、移动电话、平板等各种终端通过网络随时随地使用服务。对客户来讲，云计算的泛在接入特征使客户可以在不同的环境（如工作环境或非工作环境）下访问服务，增加了服务的可用性。

3. 资源池化

云服务商将资源（如计算资源、存储资源、网络资源等）提供给多个客户使用，这些物理的、虚拟的资源根据客户的需求进行动态分配或重新分配。

构建资源池也就是通过虚拟化的方式将服务器、存储、网络等资源组织成一个巨大的资源池。云计算基于资源池进行资源的分配，从而消除物理边界，提升资源利用率。云计算资源在云计算平台上以资源池的形式提供统一管理和分配，使资源配置更加灵活。通常情况下，规划和购置 IT 资源都是满足应用峰值以及五年计划需求的条件，导致实际运行过程中资源无法充分使用、利用率低，而云计算服务则有效地降低了硬件及运行维护成本。同时，客户使用云计算服务时不必了解提供服务的计算资源（如网络带宽、存储、内存和虚拟机）所在的具体物理位置和存在形式。但是，客户可以在更高层面（如地区、国家或数据中心）指定资源的位置。

4. 快速伸缩性

客户可以根据需要快速、灵活、方便地获取和释放计算资源。对于客户来讲，这种资源是“无限”的，能在任何时候获得所需资源量。

云服务商能提供快速和弹性的云计算服务，客户能够在任何位置和任何时间，获取需要数量的计算资源。计算资源的数量没有“界限”，客户可根据需求快速向上或向下扩展计算资源，没有时间限制。从时间代价上来讲，在云计算服务上，可以在几分钟之内实现计算能力的扩展或缩减，可以在几小时之内完成上百台虚拟机的创建。

5. 服务可计量

云计算可按照多种计量方式（如按次付费或充值使用等）自动控制或量化资源，计量的对象可以是存储空间、计算能力、网络带宽或活跃的账户数等。

该特性一方面可以指导资源配置优化、容量规划和访问控制等任务；另一方面可以监视、控制、报告资源的使用情况，让云服务商和客户及时了解资源使用明细，增加客户对云计算服务的可信度。

1.2.3　服务模式

根据云服务商提供的资源类型不同，云计算的服务模式主要分为三类。

1. 软件即服务

软件即服务（Software-as-a-Service，SaaS）是指云服务商将应用软件功能封装成服务，使客户能通过网络获取服务。云服务商负责软件的安装、管理和维护工作，客户可对软件进行有限的配置管理。客户无需将软件安装在自己的电脑或服务器上，而是按某种服务水平协议（SLA）通过网络获取所需要的、带有相应软件功能的云计算服务。例如，客户通过云计算服务向用户提供典型的办公软件或邮件等，终端用户使用软件应用，软件应用的管理者可以配置应用，客户可以按需使用软件和管理软件的数据（如数据备份和数据共享）。如 Saleforce 公司提供的在线客户关系管理（CRM）服务。

SaaS 供应商的主要职责如下：其一，确保提供给客户的软件能获得稳定的技术支持和测试；其二，确保应用是可扩展的，足以满足不断上升的大工作负载；其三，确保软件运行在一个安全的环境中，因为很多客户将有价值的数据存储在云端，这些信息也许是私人或商业机密。

2. 平台即服务

平台即服务（Platform-as-a-Service，PaaS）是指云服务商为客户提供软件开发、测试、部署和管理所需的软硬件资源，能够支持大量客户，处理大数量的数据。在这种服务模式中，PaaS 提供整套程序设计语言关联的 SDK 和测试环境等，包括开发和运行时所需的数据库、Web 服务、开发工具和操作系统等资源，客户利用 PaaS 平台能够快速创建、测试和部署应用和服务。PaaS 提供的工具包和服务可以用于开发各种类型的应用，从而可以支撑对外提供 SaaS 服务。PaaS 的客户包括应用软件的设计者、开发者、测试人员（在云计算环境运行应用）、实施人员（在云计算环境完成应用的发布，管理多版本的应用冲突）、应用管理者（在云计算环境配置、协调和监管应用）。

典型的 PaaS 包括 Google App Engine 和 Microsoft Windows Azure。PaaS 负责资源的动态扩展、容错管理和节点间配合，但用户的自主权会相应地降低，必须使用特定的编程环境并遵照特定的编程模型。例如，Google App Engine 只允许使用 Python 和 Java 语言、基于 Django 的 Web 应用框架、调用 Google App Engine SDK 来开发在线应用服务。

3. 基础设施即服务

基础设施即服务（Infrastructure-as-a-Service，IaaS）是指云服务商将计算、存储和网络等资源封装成服务供客户使用，无论是普通客户、SaaS 提供商还是 PaaS 提供商都可以从基础设施服务中获得所需的计算资源，客户无需购买 IT 硬件。典型的 IaaS 服务有亚马逊的 EC2 和简单存储服务 S3。相比于传统的客户自行购置硬件的使用方式，IaaS 允许客户按需使用硬件资源，并按照具体使用量计费。从客户角度看，IaaS 的计算资源规模大，客户能够申请的资源几乎是“无限的”；从云服务商的角度看，IaaS 能同时为多个客户提供服务，因而具有更高的资源利用率。通常情况下，可以根据 CPU 使用小时数、占用的网络带宽、网络设施（如 IP 地址）使用小时数和是否使用增值服务（如监控、服务自动伸缩）等方式计量费用。

与 SaaS 和 PaaS 客户不同的是，IaaS 的客户承担了更多的责任。客户要管理虚拟机，承担操作系统管理的工作。使用 IaaS 服务的客户更容易实现与传统应用的交互和移植，能够更灵活、高效地租用计算资源。同时，客户也面临很多问题，例如，将传统的应用软件部署到

IaaS 的同时会引发传统软件系统的漏洞所带来的安全威胁；客户可以在 IaaS 上创建和维护多个不同状态的虚拟机（如运行、暂停和关闭），也要负责虚拟机安全的维护更新（原理上，云服务商可以代表客户对非活动态虚拟机进行安全状态的维护更新，而这种类型的更新机制很复杂）等工作。

1.2.4　部署模式

根据使用云计算平台的客户范围的不同，可以将云计算分成私有云、公有云、社区云和混合云等四种部署模式。

1. 私有云

私有云的特点是云基础设施为某个独立的组织或机构运营。云基础设施的建立、管理和运营既可以是客户自己，这种私有云称为场内私有云（或自有私有云），也可以是其他组织或机构，这种私有云称为场外私有云（或外包私有云）。与公有云相比，私有云可以使客户更好地控制基础设施。下面分别对场内私有云场景和场外私有云场景进行分析。

图 1-2 描述了场内私有云的部署场景。为有效控制云基础设施，客户可以控制云基础设施的安全访问边界。边界内的客户可以直接访问，边界外的客户只能通过边界控制器访问云基础设施。

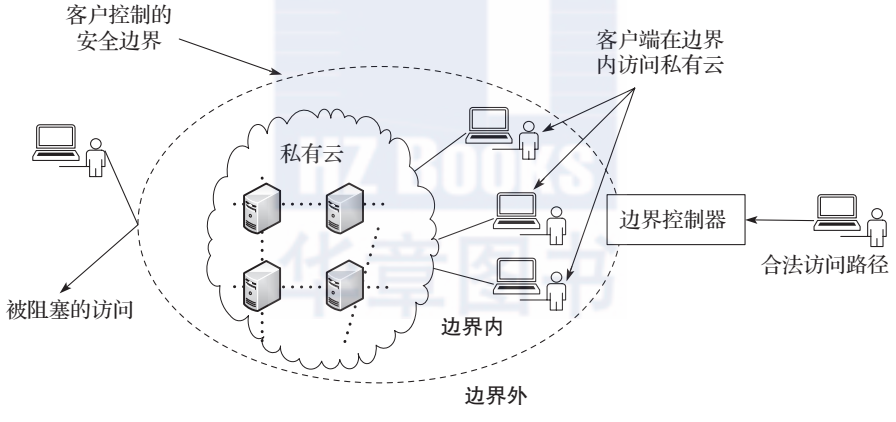


图 1-2　场内私有云

图 1-3 描述了场外私有云的部署场景。场外私有云具有两个安全边界，一个安全边界由云客户实现，另一个安全边界由云服务商实现。云服务商控制访问客户所使用的云基础设施的安全边界，客户控制客户端的安全边界。两个安全边界通过一条受保护的链路互联。场外私有云的数据和处理过程的安全依赖于两个安全边界以及边界之间的链接的强度和可用性。

2. 公有云

公有云是开放式服务，能为所有人提供服务（包括其潜在竞争对手）。公有云是指基础设施和计算资源通过互联网向公众开放的云服务。公有云的所有者和运营者是向客户提供服务的云服务商，而从其定义可以看出，该云服务商独立于客户所在的组织或机构。

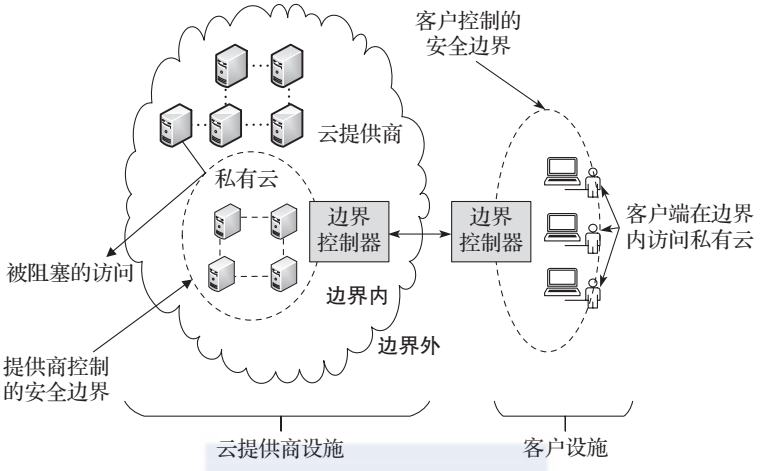


图 1-3　场外私有云

公有云主要分为以下几类：①免费向用户开放并通过广告支撑的服务，众所周知的就是搜索引擎和电子邮件服务。这些服务可能只限个人或非商业用途使用，且可能将用户的注册和使用信息与从其他来源获取的信息结合起来，向用户发送个性化广告。此外，这些服务可能不具备通信加密等保护措施。②需付费的服务。此类服务与第一类服务相似，但可以用低成本的方式为客户提供服务，因为服务提供条款都是没有商量余地的，且只能由云服务商单方面进行修改。此类服务的保护机制要超出第一类服务，且可由客户进行配置。③需付费且服务条款可由客户和云服务商进行协商的云计算服务。

图 1-4 描述了公有云场景，所有客户均能访问任何可用的云基础设施。

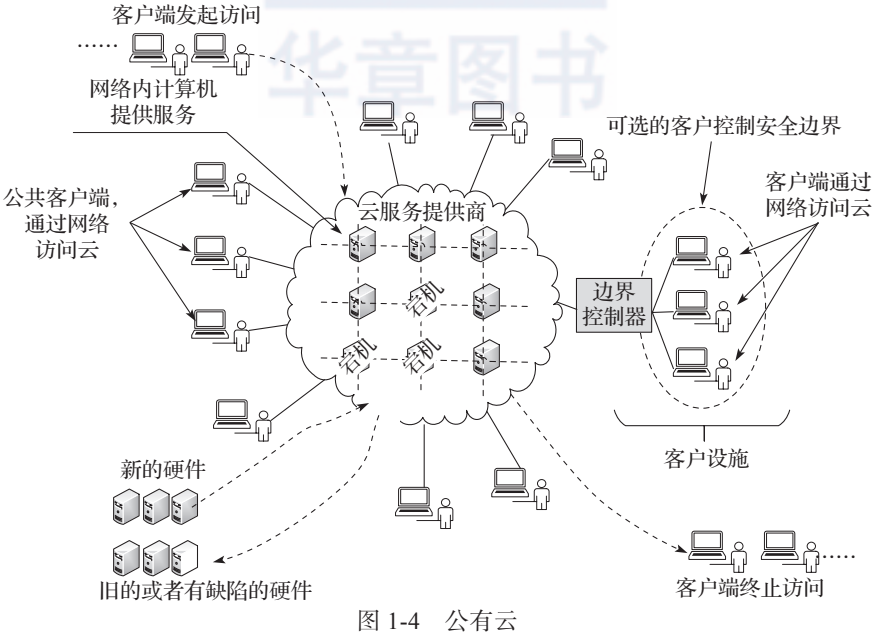


图 1-4　公有云

3. 社区云

社区云的特点是云基础设施由若干特定的客户共享。这些客户具有共同的特性（如任务、安全需求和策略等）。和私有云类似，社区云的云基础设施的建立、管理和运营既可以由一个客户或多个客户实施，也可以由其他组织或机构实施。

图 1-5 描述了场内社区云的部署场景，每个参与组织或机构可以提供云服务、使用云服务，或既提供云服务也使用云服务，但至少有一个社区云成员提供云服务。提供云计算服务的各个成员分别控制了一个云基础设施的安全边界和云计算服务的安全边界。使用社区云的客户可以在接入端建立一个安全边界。

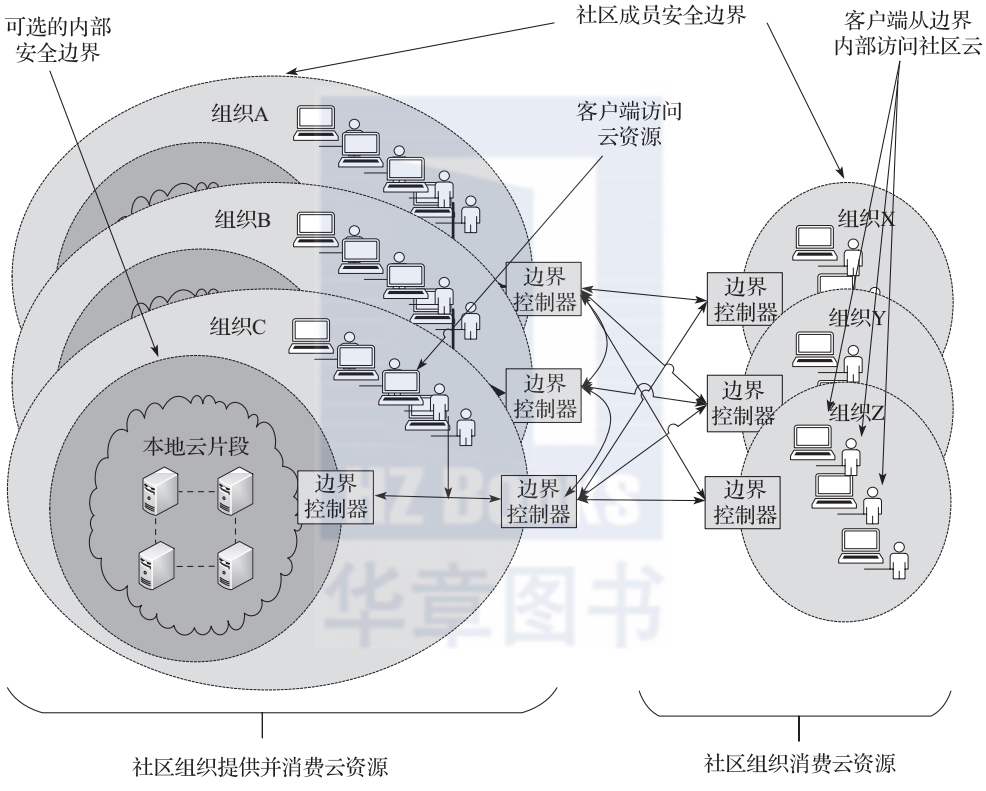


图 1-5　场内社区云

图 1-6 描述的场外社区云由一系列参与组织（包括云服务商和客户）构成，该场景与场外私有云类似：服务端的责任由云服务商管理，云服务商实现了安全边界，防止社区云资源与其他供应商安全边界以外的云资源混合。与场外私有云相比，一个明显的不同之处在于云服务商可能需要在参与组织之间实施恰当的共享策略。

4. 混合云

混合云的特点是云基础设施由两种或者两种以上相对独立的云（私有云、公有云或社区云）组成，并用某种标准或者专用技术绑定在一起，这使数据和应用具有可移植性。因为混

合云由两个或多个云（私有云、社区云或公有云）组成，所以会比其他的部署模型更为复杂。每个成员依然是独立的个体，通过标准技术或专有技术与其他成员绑定，从而实现应用和数据在成员间的可移植性。

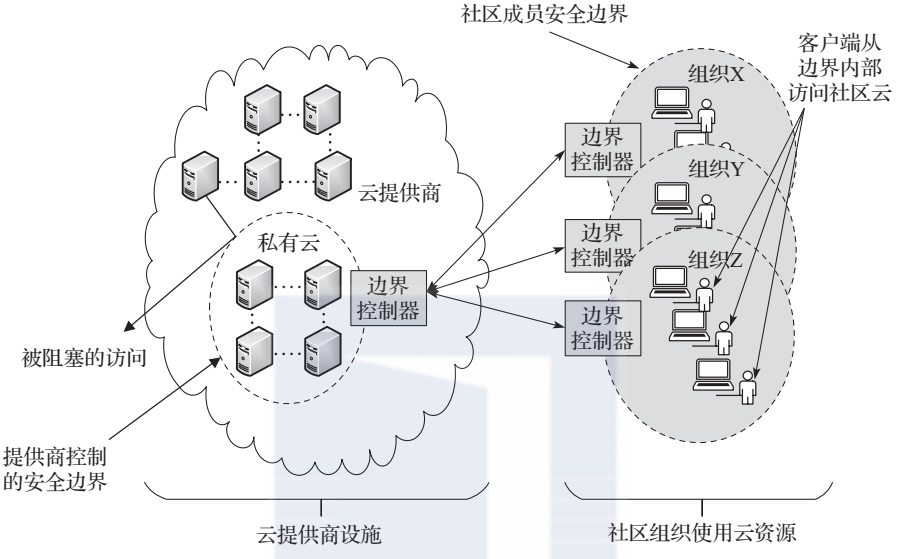


图 1-6　场外社区云

1.3　云计算的应用案例

本节将对政府、金融和医药行业的云计算应用案例进行介绍，分析云计算服务的特点。

1.3.1　政府部门

美国高速公路安全管理局（NHTSA）负责执行汽车补贴置换政策（对旧机动车升级换代进行政府补助）并主持该业务系统的建设，选择在传统数据中心内架设 IT 系统并配备专门设计的商业应用系统。该局预测 4 个月内可能有 25 万交易申请，但从 2009 年 7 月系统投产后仅 90 天该系统就处理了将近 69 万个交易。该系统从第一笔交易受理的三天内就出现超负荷情况，导致大量交易无法处理和多次系统瘫痪情况发生。联邦政府为建设该系统拨付的 10 亿美元专项资金在系统上线后 1 周内几乎用完。为此，两天后联邦政府紧急额外拨款 20 亿美元，用于对该系统按照初期测算交易量 3 倍进行扩容，并耗费众多时日才得以完成。

上面的例子是美国联邦政府当时的 IT 应用环境的写照，由于普遍存在资源利用率低、资源需求分裂、信息系统重复建设、系统环境管理难、采购部署时间过长等问题，影响了联邦政府向公众提供服务的能力。为改变上述局面，美国政府对云计算模式进行研究和规划，发布了《美国联邦政府云计算战略白皮书》（Federal Cloud Computing Strategy），大幅提高了对云计算模式的关注、研究、管理和应用的力度。

美国联邦政府前首席信息官 Vivek Kundra 表示，使用云计算能够提升、恢复首席信息官的本职职能，从“过去的关注数据中心、网络运行、系统安全等工作中解脱出来，转变为关注国家面临的问题，例如健康、教育和信息鸿沟等”。另外，云计算将优化联邦政府数据设施环境配置，可通过对现有 IT 基础设施进行虚拟和整合，使政府部门减少在各自数据中心运行维护 IT 系统的支出。研究显示，云计算拥有巨大潜能来解决政府面临的旧有信息系统建设和应用的弊端，提高政府运行效率，帮助政府机构实现提供高可靠性的、革新的服务方式的需求，不必受制于资源的可用性。从效率、弹性和创新三个方面，云计算具有传统数据中心无法比拟的优势，如表 1-1 所示。

表 1-1　云计算相较于传统数据中心的优势

方　面	优　势
效率	可将资产使用率从低于 30% 提高到 60% ~ 70%
	将割裂的需求和系统建设转变为整合的系统需求和系统建设计划
	降低面向众多系统的管理难度，提高管理效率
弹性	将周期长、投资大的新信息系统建设转变为按需、按量使用和付费的方式
	将系统扩容的时间从数个月降低到近乎实时增减系统容量
	增强对信息系统紧急需求的快速响应能力
创新	将工作重点从管理资产转变为管理服务，减轻进行资产管理的沉重负担
	将较为保守的政府文化转变为鼓励、融合企业和行业创新技术的文化

在 2016 年，经 FedRAMP（The Federal Risk and Authorization Management Program，联邦风险和授权管理项目）认证授权的云服务产品数量以指数方式增长，新增加了 72 项云服务，同比增长 80%；新认证了 345 项操作授权，同比增长 56%。所有的 24 个首席财务官法案机构都正在使用 FedRAMP 认证授权的云服务。截至 2017 年 2 月，美国联邦政府采购使用云计算服务的机构已达 103 家，云计算在美国真正实现了政府层面的应用。

1.3.2　金融行业

怡安集团（AON Corporation）为美国上市公司，是全球 500 强企业。该集团使用云计算来进行客户关系管理，这是对传统计算和云计算的风险进行深入分析和对比后做出的选择。传统计算方式造成的信息竖井和孤立架构所导致的管理困难、信息不一致、实效性低等给企业带来了巨大的操作风险；另一方面，传统方式下信息与数据分布式存储和保存，复杂度高、可用性低，对于信息和数据安全性缺乏统一的、可执行的电子数据安全等级管理体系，电子数据与信息存在潜在外泄风险，内部的安全管理漏洞更加难以防范，导致客户信息与数据更易泄露或不当使用。现在选用云计算方式，通过保密协议与服务等级协议规范云计算服务提供商达到特定的数据信息安全等级要求，实现数据云端存储以及尽量减少人为参与、干预环节，达到对数据特别是敏感数据的安全保护要求。同时，信息的云端集中式存储还有利于隐私保护和遵从反洗钱法案等法律法规的要求，提高信息、数据的合规性。安全认证、授权、加密、数据漂白、审计等安全技术的发展及其在云计算服务特别是在网络传输、云数据处理、

云存储上的应用，提升了客户信息和业务数据的安全性与合规性。

与大家通常认为的恰恰相反，云计算比传统计算在总体上更安全、更可靠、风险更低，更有利于降低企业的运营风险。这也是为什么一家以控制风险为主业的公司，要选择云服务模式而不是传统 CRM 软件包的模式来管理全公司客户关系的原因。

1.3.3　医药行业

创建于 1876 年的礼来公司（Eli Lilly and Company）现已发展成为全球十大制药企业之一，跻身世界 500 强企业。目前，礼来公司使用 Google、Amazon Web Service、Alexa and Drupal 等公司的解决方案实现快速安装、部署新的计算资源。通过转变和整合，礼来公司成倍减少了部署新计算资源的时间，让该公司研发新药品项目的启动时间大幅度减少，进而缩减新药品上市的时间。礼来公司使用 Amazon 的 EC2 集群的情况为：3809 个计算单元，每个计算单元配备 8 核处理器、7GB 内存，整个集群共有 30 472 核处理器、26.7TB 内存、2PB 磁盘空间。使用该集群能够为该公司提供强大的计算能力，而费用为每小时 1279 美元。若公司采用自行建设方式建设上述系统资源和基础设施，巨额的资金投入和耗时的建设周期是企业无法承受的，即使建成，也将面临资源浪费和闲置的问题。相比之下，礼来公司运用云计算服务，将固定支出模式转为浮动支出模式，削减了 IT 固定资产和相关费用的投入，同时满足了及时获取强大计算能力的要求。

1.3.4　12306 网站

2015 年春运火车票售卖量创下历年新高，而铁路 12306 售票网站却并没有出现明显的卡滞，采用云计算技术是关键原因。经分析，余票查询环节的访问量占 12306 网站近乎九成流量，也是往年造成网站拥堵的最主要原因之一。同阿里云合作后，12306 网站把余票查询系统从自身后台分离出来，在云上独立部署了一套余票查询系统。把高频次、高消耗、低转化的余票查询环节放到云端，而将下单、支付这种“小而轻”的核心业务留在 12306 原有的后台系统上，这样的思路为系统减负不少。

1.4　小结

云计算是一种计算资源的新型应用模式，客户以购买服务的方式，通过网络获得计算、存储、软件等不同类型的资源，仅需较少的使用成本即可获得优质的 IT 资源和服务，避免了前期基础设施建设的大量投入。云计算技术已经成为当前的研究热点。通过本章的学习，你可以对云计算的发展、云计算的基本概念有一定的了解。

云计算给客户带来灵活性和经济效益的同时也引入了新的安全风险。在学习和应用云计算技术的同时，了解云计算存在的安全问题和面临的安全风险，以及提高云计算的安全性的相关技术是非常必要的。本书后续的章节将分析云计算面临的安全风险，并从多个角度深入剖析云计算安全技术。

1.5　参考文献与进一步阅读

[1] 蒋永生，彭俊杰，张武 . 云计算及云计算实施标准：综述与探索[J]. 上海大学学报（自然科学版），2013（01）：5-13.
[2] 骆祖莹 . 云计算安全性研究[J]. 信息网络安全，2011（06）：33-35.
[3] 刘黎明 . 云计算起源探析[J]. 电信网技术，2010（09）：8-11.
[4] 马云致投资者公开信：大数据云计算是阿里未来十年核心战略之一[EB/OL]. https://yq.aliyun.com/articles/80931.
[5] 王惠莅，上官晓丽 . SC27 云计算安全国际标准制定进展[J]. 保密科学技术，2015（04）：38-42.
[6] 汪芳，张云勇，房秉毅 . 云计算生态环境和产业监管探讨[J]. 电信网技术，2011（05）：47-51.
[7] 云计算 HOLD 住了谁？[EB/OL]. http://blog.sina.com.cn/s/blog_59e64c8e0102dt9o.html.
[8] 陈康，郑纬民 . 云计算：系统实例与研究现状[J]. 软件学报，2009（05）：1337-1348.
[9] 孙少陵，罗治国，徐萌 . 云计算点亮网络智慧[J]. 世界电信，2009（09）：60-63.
[10] 孙鸿靖，白洁，马海兵 . 计算模式的创新——云计算[J]. 中国科技信息，2010（19）：76-77.
[11] 邵泽云，刘正岐 . 云计算关键技术研究[J]. 信息安全与技术，2014（04）：24-25.
[12] 斯琴其木格 . 云计算概念的产生、定义、原理及前景分析[J]. 赤峰学院学报（自然科学版），2011（12）：30-31.
[13] 刘琦琳 . 区域云计算平台：云计算的落脚点[J]. 互联网周刊，2010（12）：62-63.
[14] 廖志涛 . 云计算环境下面向数据密集型应用的数据布局探究[J]. 数字技术与应用，2011（08）：210.
[15] 冀勇庆 . 云的战争[J]. IT 经理世界，2010（06）：39-41.
[16] 孙定 . 云计算必然性的经典论证[N]. 计算机世界，2011-01-17（002）.
[17] 云计算服务应用案例介绍和分析[J]. 物联网技术，2012（02）：20-24.
[18] 贾一苇，赵迪，蒋凯元，栾国春 . 美国联邦政府云计算战略[J]. 电子政务，2011（07）：2-16.

CHAPTER 2

第2章

云计算安全风险分析

随着云计算的普及，安全问题逐渐成为制约其发展的重要因素。云计算技术将计算资源、存储资源和网络资源等转化成为一种共享的公共资源，这使得 IT 资产透明度和用户对资产的控制性降低，因此用户在采用云计算服务时会产生诸多安全顾虑。因此，要推动云计算技术发展，让用户放心地将数据和业务部署或迁移到社会化云计算平台，并交付给云服务提供商管理，就必须全面分析并着手解决云计算所面临的各种安全风险。本章将从云计算面临的技术风险、管理风险和法律法规风险几个方面分析云计算安全风险，并给出云计算安全设计时需要考虑的原则。

2.1 云计算面临的技术风险

云计算服务模式将硬件、软件甚至应用交给经验丰富的云服务商来管理，客户通过网络来享受云服务商提供的服务，并可按需定制、弹性升缩、降低成本。但是，传统信息技术所面临的安全风险依然威胁着云计算的安全，并且云计算所使用的核心技术在带来诸多新特性的同时也带来了一些新的风险。

2.1.1 物理与环境安全风险

物理与环境安全是系统安全的前提。信息系统所处的物理环境的优劣直接影响信息系统的安全，物理与环境安全问题会对信息系统的保密性、完整性、可用性带来严重的安全威胁。

物理安全是保障物理设备安全的第一道防线。物理安全会导致系统存在风险。例如，环境事故有可能造成整个系统毁灭；电源故障造成的设备断电会造成操作系统引导失败或数据库信息丢失；设备被盗、被毁会造成数据丢失或信息泄露；电磁辐射可能造成数据信息被窃取或偷阅；报警系统的设计不足或失灵可能造成一些事故等。

环境安全是物理安全的基本保障，是整个安全系统不可缺少和忽视的组成部分。环境安全技术主要是指保障信息网络所处环境安全的技术，主要技术规范是对场地和机房的约束，强调对于地震、水灾、火灾等自然灾害的预防措施，包括场地安全、防火、防水、防静电、

防雷击、电磁防护和线路安全等。

2.1.2　主机安全风险

从技术角度来看，云计算平台中的主机系统和传统 IT 系统类似，传统 IT 系统中各个层次存在的安全问题在云计算环境中仍然存在，如系统的物理安全、主机、网络等基础设施安全、应用安全等。云主机面临的安全风险主要包括以下几点，如图 2-1 所示。

（1）资源虚拟化共享风险

云主机中，硬件平台通过虚拟化为多个应用共享。由于传统安全策略主要适用于物理设备，如物理主机、网络设备、磁盘阵列等，而无法管理到每个虚拟机、虚拟网络等，使得传统的基于物理安全边界的防护机制难以有效保护共享虚拟化环境下的用户应用及信息安全。

（2）数据安全风险

用户在使用云主机服务的过程中，不可避免地要通过互联网将数据从其主机移动到云上，并登录到云上进行数据管理。在此过程中，如果没有采取足够的安全措施，将面临数据泄漏和被篡改的安全风险。

（3）平台安全防护风险

云计算应用由于其用户、信息资源的高度集中，更容易成为各类拒绝服务攻击的目标，并且由拒绝服务攻击带来的后果和破坏性将会明显超过传统的企业网应用环境，因此，云计算平台的安全防护更为困难。

2.1.3　虚拟化安全风险

将虚拟化应用于云计算的部署中能带来很多好处，包括成本效益、增加正常运行时间、改善灾难恢复和应用程序隔离等。但它同样也带来了很多安全问题，如图 2-2 所示。

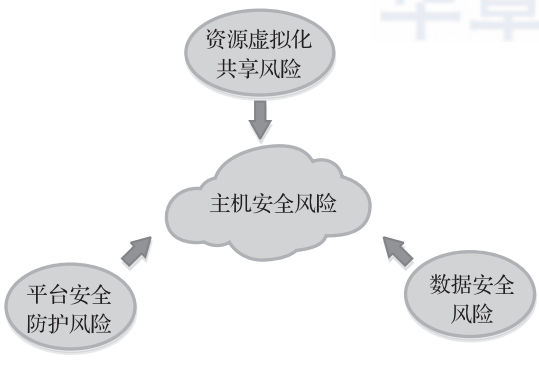


图 2-1　主机安全风险

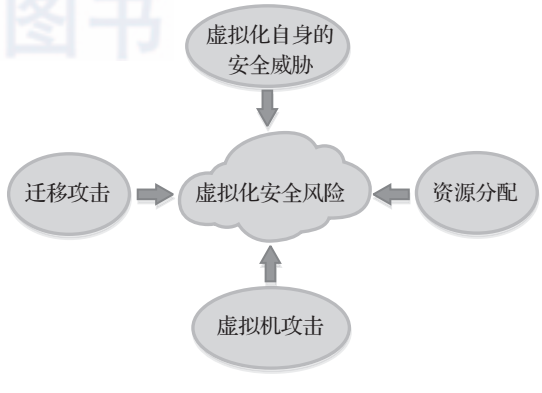


图 2-2　虚拟化安全风险

（1）虚拟化技术自身的安全威胁

Hypervisor（虚拟机管理器）本身的脆弱性不可避免，攻击者可能利用 Hypervisor 存在的

漏洞来获取对整个主机的访问，实施虚拟机逃逸等攻击，从而可以访问或控制主机上运行的其他虚拟机。由于管理程序很少更新，现有漏洞可能会危及整个系统的安全性。如果发现一个漏洞，企业应该尽快修复漏洞以防止潜在的安全事故。

（2）资源分配

当一段被某台虚拟机独占的物理内存空间重新分配给另一台虚拟机时，可能会发生数据泄露；当不再需要的虚拟机被删除，释放的资源被分配给其他虚拟机时，同样可能发生数据泄露。当新的虚拟机获得存储资源后，它可以使用取证调查技术来获取整个物理内存以及数据存储的镜像。而该镜像随后可用于分析，并获取前一台虚拟机遗留下的重要信息。

（3）虚拟机攻击

攻击者成功地攻击了一台虚拟机后，在很长一段时间内可以攻击网络上相同主机的其他虚拟机，如图 2-3 所示。这种跨虚拟机攻击的方法越来越常见，因为云内部虚拟机之间的流量无法被传统的 IDS/IPS 设备和软件检测到，只能通过在虚拟机机内部部署 IDS/IPS 软件进行监测。

（4）迁移攻击

虚拟机迁移时会通过网络被发送到另一台虚拟化服务器，并在其中设置一个相同的虚拟机，如果虚拟机通过未加密的信道来发送，就有可能被执行中间人攻击的攻击者嗅探到。当然，为了做到这一点，攻击者必须获得受感染网络上另一台虚拟机的访问权。

2.1.4　网络安全风险

泛在接入作为云计算服务的五大特征之一，云环境下的网络安全问题也就自然而然地凸显出来。

在网络风险方面，云计算主要面临以下的风险：拒绝服务攻击、中间人攻击、网络嗅探、端口扫描、SQL 注入和跨站脚本攻击，如图 2-4 所示。

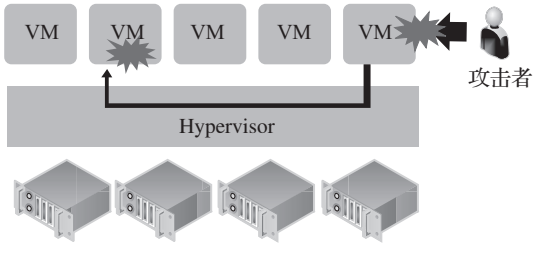


图 2-3　虚拟机攻击

图 2-4　网络安全风险

1）**拒绝服务攻击**：指攻击者想办法让目标服务器停止提供服务甚至导致主机死机。在云计算中，黑客对服务器开展拒绝服务攻击时，会发起成千上万次的访问请求到服务器，导致

服务器无法正常工作，无法响应客户端的合法访问请求。针对这种攻击，主要的防御方式是通过入侵检测、流量过滤和多重验证，将堵塞网络带宽的流量过滤，放行正常的流量。

2）**中间人攻击**：是指攻击者通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而通信的双方却毫不知情。在网络通信中，如果没有正确配置安全套接字层（SSL），那么这个风险就有可能出现。针对这种攻击手段，可以采用的应对措施是正确地安装配置 SSL，并且通信前应由第三方权威机构对 SSL 的安装配置进行检查确认。

3）**网络嗅探**：这原本是网络管理员用来查找网络漏洞和检测网络性能的一种工具，但是到了黑客手中，它变成了一种网络攻击手段，从而造成更为严峻的网络安全问题。例如，在通信过程中，由于数据密码设置过于简单或未设置，导致被黑客破解，那么未加密的数据便被黑客通过网络攻击获取。如果通信双方没有使用加密技术来保护数据安全性。那么攻击者作为第三方便可以在通信双方的数据传输过程中窃取到数据信息。针对这种攻击手段，可以采用的应对策略是通信各方使用加密技术及方法，确保数据在传输过程中安全。

4）**端口扫描**：这也是一种常见的网络攻击方法，攻击者通过向目标服务器发送一组端口扫描消息，并从返回的消息结果中探寻攻击的弱点。针对此类攻击，可以启用防火墙来保护数据信息免遭端口攻击。

5）**SQL 注入**：SQL 注入是一种安全漏洞，利用这个安全漏洞，攻击者可以向网络表格输入框中添加 SQL 代码以获得访问权。在这种攻击中，攻击者可以操纵基于 Web 界面的网站，迫使数据库执行不良 SQL 代码，获取用户数据信息。针对这种攻击，应定期使用安全扫描工具对服务器的 Web 应用进行渗透扫描，这样可以提前发现服务器上的 SQL 注入漏洞，并进行加固处理。另外，针对数据库 SQL 注入攻击，应避免将外部参数用于拼接 SQL 语句，尽量使用参数化查询，同时限制那些执行 Web 应用程序代码的账户权限，减少或消除调试信息。

6）**跨站脚本**（Cross-Site Scripting，XSS）：XSS 是一种网站应用程序的安全漏洞攻击，属于代码注入的一种。它允许用户将恶意代码注入到网页上，其他用户在浏览网页时就会受到影响。这类攻击通常包含 HTML 以及用户端脚本语言。攻击成功后，攻击者可能得到更高的权限、从而窃取私密网页内容、会话和 cookie 等各种信息。针对此类攻击，最主要的应对策略是将用户所提供的内容进行过滤，避免恶意数据被浏览器解析。另外，可以在客户端进行防御，如把安全级别设高，以及只允许信任的站点运行脚本、Java、Flash 等小程序。

2.1.5　安全漏洞

在 ISO/IEC 27005 风险管理标准中，将安全漏洞定义为可被一个或多个威胁利用的资产或资产组的弱点；在 Open Group 的风险分类法中，对安全漏洞进行了一个较为完整、准确的定义：安全漏洞就是威胁能力超过抵御威胁能力的机率。云计算环境所面临的安全漏洞不仅可能存在于云计算所依赖的现有核心技术中，也有可能是某些关键的云计算特性所带来的。

（1）核心技术漏洞

在云计算所依赖的某些现有核心技术中，例如 Web 应用程序和服务、虚拟化和加密技术

等，都存在着一些漏洞。有些是技术本身固有的，而另一些则是普遍存在于该技术的流行实现方式中。这里以其中三个为例进行介绍，包括虚拟机逃逸、会话控制和劫持以及不安全或过时的加密。

首先，虚拟化的本质就决定了存在攻击者从一个虚拟环境中成功逃脱的可能性。因此，我们必须把这个漏洞归类于虚拟化固有的、与云计算高度相关的那一类漏洞。

其次，Web 应用技术必须克服这样一个问题，即从设计的初衷来说，HTTP 协议是无状态协议，而 Web 应用程序则需要一些会话状态的概念。有许多技术能够实现会话处理，而许多会话处理的实现都容易遭受会话控制和劫持。

最后，密码分析学的进步可以使任何加密机制或算法变得不再安全，因为总是能找到新奇的破解方法。而更为普遍的情况是，加密算法的实现被发现具有关键的缺陷，可以让原本的强加密退化成弱加密（有时甚至相当于完全不加密）。在没有加密技术保护云上数据的保密性和完整性的情况下，无法想象云计算能够获得广泛的应用，因而可以说不安全或过时的加密漏洞与云计算有着非常密切的关系。

（2）关键的云计算特性所带来的漏洞

针对国标 GB/T 31167—2014 中描述的五个云计算特性：按需自助服务、泛在接入、资源池化、快速伸缩性、服务可计量，下面列举一些源自上述一种或几种特性的安全漏洞的例子：

1）未经授权的管理界面访问：按需自助服务的云计算特性需要一个管理界面，可以向云服务的用户开放访问。这样，未经授权的管理界面访问对于云计算系统来说就算得上是一个具有特别相关性的漏洞，可能发生未经授权的访问的概率要远远高于传统的系统，在那些系统中只有少数管理员能够访问管理功能。

2）互联网协议漏洞：泛在接入这一云计算特性意味着云服务是通过使用标准协议的网络来访问的。在大多数情况下，这个网络即互联网，必须被看作是不可信的。这样一来，互联网协议漏洞也就和云计算产生了联系，它可能导致中间人攻击等。

3）数据恢复漏洞：资源池化的云特性意味着分配给一个用户的资源将有可能在稍后被重新分配到不同的用户。对于内存或存储资源来说，就有可能从中恢复出前面用户写入的数据。

4）逃避计量和计费：服务可计量的云特性意味着，任何云服务都在某一个适合服务类型的抽象层次（如存储、处理能力以及活跃账户）上具备计量能力。计量数据被用来优化服务交付以及计费，这就有可能出现操纵计量和计费数据，以及逃避计费的漏洞。

综合来看，当前及未来的主要云安全问题将会集中在虚拟机漏洞、Web 漏洞、数据安全等方向上，主要原因如下：

- 云平台上一般是多个用户共用一台服务器，如果利用虚拟机漏洞逃逸出去，进而控制主系统，那么攻击者就可能窃取他人的数据并执行其他恶意的越权操作。
- Web 漏洞相对其他类型的漏洞门槛会低一些，也是外部最容易接触到的层面，此处若发生安全问题可能直接导致服务器被入侵，危害严重。
- 数据加密往往是最后一道防线，即使服务器被入侵，若采用较为坚固的数据加密方案，可以大大地提高免受破解的能力，而若对敏感数据未做加密或采用不安全的加密

方式，则破解数据只是时间问题。

因为上述安全问题，所以现在许多云服务商自身或者第三方安全厂商会提供一些云安全产品，比如云 WAF、云漏洞扫描器、主机入侵防御系统、数据加密系统、DDOS 防御系统等。可以预见未来会有更多的云安全产品出现。

2.1.6　数据安全风险

云计算模型开启了旧数据以及新数据的安全风险。基于其自身的定义，发展云计算意味着允许更加开放的信息访问以及更容易地改进数据共享。数据上传到云并存储在一个数据中心，由数据中心的用户访问，或在完全基于云模型中，在云上创建、存储数据，而通过云访问数据（不是通过数据中心访问数据）。在上述过程中，最明显的风险是数据存储方面的风险。用户上传或创建基于云的数据，这些数据也包括第三方的云服务商（如 Google、Amazon、Microsoft）负责存储以及维护的数据，也会引发一些相关的风险。

一般来说，云服务产生的数据的生命周期可分为六个阶段，如图 2-5 所示，数据安全在这六个阶段中面临着不同方面、不同程度的安全威胁。

（1）数据生成

数据生成阶段即数据刚被数据所有者创建，尚未被存储到云端的阶段。在这个阶段，数据所有者需要为数据添加必要的属性，如数据的类型、安全级别等一些信息；此外，数据的所有者为了防范云端不可信，在存储数据之前可能还需要着手准备对数据的存储、使用等各方面情况进行跟踪审计。在数据生成阶段，云数据面临如下问题：

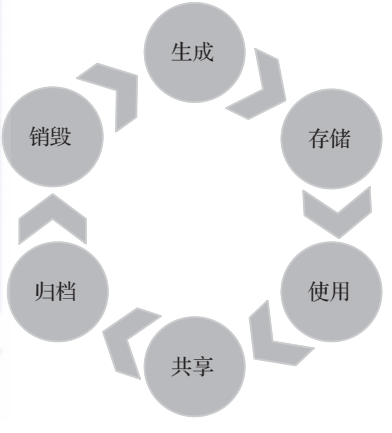


图 2-5　云数据的生命周期

1）数据的安全级别划分：不同的用户类别，如个人用户、企业用户、政府机关、社会团体等对数据安全级别的划分策略可能会不同，同一用户类别之内的不同用户对数据的敏感分类也不同。在云计算环境下，多个用户的数据可能存储在同一个位置，因此，若数据的安全级别划分策略混乱，云服务商就无法针对海量数据制定出切实有效的保护方案。

2）数据的预处理：用户要存储在云端的数据可能是海量的，因此在对数据进行预处理前，用户必须考虑预处理的计算、时间和存储开销，否则会因为过度追求安全性而失去云计算带来的便捷性。

3）审计策略的制定：即使在传统的 IT 架构下，审计人员制定有效的数据审计策略也是很困难的，何况在多用户共享存储、计算和网络等资源的云计算环境下，用户对自己的数据进行跟踪审计更是难上加难。

（2）数据存储

在云计算场景下，用户的数据都存储在云端，云数据面临如下安全风险：

1）数据存放位置的不确定性：在云计算中，用户对自己的数据失去了物理控制权，即用

户无法确定自己的数据存储在云服务商的哪些节点上，更无法得知数据存储的地理位置。

2）数据混合存储：不同用户的各类数据都存储在云端，若云服务提供商没有有效的数据隔离策略，可能造成用户的敏感数据被其他用户或者不法分子获取。

3）数据丢失或被篡改：云服务器可能会被病毒破坏，或者遭受木马入侵；云服务商可能不可信，或管理不当，操作违法；云服务器所在地可能遭受自然灾害等不可抗力的破坏。上述原因都会造成云服务数据丢失或者被篡改，威胁到数据的机密性、完整性和可用性。

（3）数据使用

数据使用即用户访问存储在云端的数据，同时对数据做增删查改等操作。在数据使用的各个阶段，会面临如下问题：

1）访问控制：如果云服务商制定的访问控制策略不合理、不全面，就有可能造成合法用户无法正常访问自己的数据或对自己的数据进行合规的操作，而未授权用户却能非法访问甚至窃取、修改其他用户的数据。

2）数据传输风险：用户通过网络来使用云端数据，若传输信道不安全，数据可能会被非法拦截；网络可能遭受攻击而发生故障，造成云服务不可用；另外，传输时的安全操作不当可能导致数据在传输时丧失完整性和可用性。

3）云服务的性能：用户使用数据时，往往会对数据的传输速度、数据处理请求的响应时间等有一个要求或期望，但云服务的性能受用户所使用的硬件等多因素的影响，因此云服务商可能无法切实保障云服务的性能。

（4）数据共享

数据共享即让处于不同地方使用不同终端、不同软件的云用户能够读取他人的数据并进行各种运算和分析。在数据共享阶段，数据同样面临着风险：

1）信息丢失：不同的数据内容、数据格式和数据质量千差万别，在数据共享时可能需要对数据的格式进行转换，而数据转换格式后可能面临数据丢失的风险。

2）应用安全：数据共享可能通过特定的应用实现，如果该应用本身有安全漏洞，则基于该应用实现的数据共享就可能有数据泄露、丢失、被篡改的风险。

（5）数据归档

数据归档就是将不经常使用的数据转移到单独的存储设备进行长期保存。在本阶段，云数据会面临法律和合规性问题。某些特殊数据对归档所用的介质和归档的时间期限会有专门规定，而云服务商不一定支持这些规定，造成这些数据无法合规地进行归档。

（6）数据销毁

在云计算场景下，当用户需要删除某些数据时。最直接的方法就是向云服务商发送删除命令，依赖云服务商删除对应的数据。但是这同样面临着多种问题：

1）数据删除后可被重新恢复：计算机数据存储基于磁介质形式或电荷形式，一方面可以采用技术手段直接访问这些已删除数据的残留数据；另一方面可以通过对介质进行物理访问，确定介质上的电磁残余所代表的数据。如果不法分子获得这些数据，有可能给用户带来极大隐患。

2）云服务商不可信：一方面，用户无法确认云服务商是否真的删除了数据；另一方面，

云服务商可能留有被删除数据的多个备份，在用户发送删除命令后，云服务商并没有删除备份数据。

2.1.7　加密与密钥风险

在 2016 年最新的 CSA(云安全联盟）云安全威胁排名中，“弱身份、凭证和访问管理”威胁位居第二位，如图 2-6 所示，说明在云环境下，传统的加密与密钥管理的方案向云环境的迁移和演变遇到了很大的挑战。

No	威胁
T1	数据泄露
T2	弱身份、凭证和访问管理
T3	不安全的接口和 API
T4	系统、应用漏洞
T5	账号劫持
T6	恶意内部员工
T7	APT 攻击
T8	数据丢失
T9	没有足够的尽职调查
T10	滥用云服务
T11	拒绝服务（DDOS）
T12	共享技术问题

图 2-6　CSA 2016 最新的威胁列表

传统的数据安全一直强调数据的完整性、机密性和可用性，因此产生了传统的对称加密和非对称加密的方案用于保护数据的这些安全特性。由于虚拟化技术的发展，云计算兴起，云环境上数据的安全防护显得越来越重要，传统的加密和密钥的方案向云计算环境的迁移受到了云计算环境的各种挑战，不仅有传统的加密与密钥风险，而且也产生了云环境下特有的加密和密钥风险，大体分为加密方案和密钥管理两方面。

对于加密方案的挑战主要是：

1）虚拟化技术使得单个物理主机可以承载多个不同的操作系统，导致传统的加密方案的部署环境逐步向虚拟机、虚拟网络演变。

2）云平台及其存储数据在地域上的不确定性。

3）访问控制与认证机制的有效性与可靠性。

4）单一物理主机上的多个客户操作系统之间的信息泄露。

5）海量敏感数据在单一的云计算环境中高度集中。

6）根据数据的存储位置、关键程度、当前状态（静止或传送中）决定加密等级。

对于密钥管理的挑战主要是：

1）本地密钥管理，主要是针对于在云基础设施外部的用户端的密钥管理，与传统的密钥管理风险相似。

2）云端密钥管理，云服务商必须保证密钥信息在传输与存储过程中的安全防护，由于云的多租户的特性，存在着密钥信息泄露的风险。

2.1.8　API 安全风险

在云环境下，API 提供了对应功能的访问权限，这无疑增加了云平台的攻击面，攻击者可能会滥用或寻找流行 API 代码中的漏洞，来实现对云用户和云服务的攻击，因此，云安全联盟也指出不安全的 API 是云计算面临的最大威胁之一。

1. API 签名安全

API 签名主要用于解决任意调用带来的风险，系统从外部获取数据时，一般都采用 API 接口调用的方式来实现，请求方和接口提供方在通信的过程中，主要需要考虑以下几

个问题：

- 请求参数是否被篡改。
- 请求来源是否合法。
- 请求是否具有唯一性。

比如，在阿里云的最佳实践中，每个 API 服务都属于一个 API 分组，每个 API 分组有不同的域名，域名的格式为：

www.[独立域名].com/[Path]?[HTTPMethod]

域名是由服务端绑定的独立域名，API 网关通过域名来寻址定位 API 分组，API 网关通过域名定位到一个唯一的分组，通过 Path + HTTPMethod 确定该分组下唯一的 API。

2. API 防重放攻击

虽然 API 接口传输采用了 HTTPS 进行加密传输，但是一部分接口仍旧存在重放攻击的风险。在阿里云实践中，防重放的规则是请求唯一标识，15 分钟内 AppKey+API+Nonce 不能重复，并且要与时间戳结合使用才能起到防重放作用。AppKey 在 API 网关控制台生成，只有获得 API 授权后才可以调用，通过云市场等渠道购买的 API 默认已经给 APP 授过权，阿里云所有云产品共用一套 AppKey 体系，删除 ApppKey 时应谨慎，以免影响到其他已经开通服务的云产品。时间戳的值为当前时间的毫秒数，也就是从 1970 年 1 月 1 日起至今的时间转换为毫秒，时间戳有效时间为 15 分钟。

3. API 流量控制

流量控制策略和 API 是各自独立管理的，两者绑定后，流量控制策略会对已绑定的 API 起作用。在已有的流量控制策略上，可以额外配置特殊用户和特殊应用（APP），这些特例只是针对当前策略已绑定的 API 生效。流量控制策略可以配置对 API、用户、应用三个对象的流控值，流控的单位可以是分钟、小时、天。

流量控制策略可以涵盖表 2-1中的维度。

表 2-1　流量限制策略

API 流量限制	该策略绑定的 API 在单位时间内被调用的次数不能超过设定值，单位时间可选分钟、小时、天，如 5000 次 / 分钟
APP 流量限制	每个 APP 对该策略绑定的任何一个 API 在单位时间内的调用次数不能超过设定值，如 50 000 次 / 小时
用户流量限制	每个云账号对该策略绑定的任何一个 API 在单位时间内的调用次数不能超过设定值。一个云账号可能有多个 APP，所以对云账号的流量限制就是对该账号下所有 APP 的流量总和的限制。如 50 万次 / 天

在 API 网关控制台，可以完成对流量控制策略的创建、修改、删除、查看等基本操作，以及流量控制策略与 API 的绑定 / 解绑等操作。

4. API 授权管理

将 API 发布到线上环境后，需要给客户的 APP 授权，客户才能用该 APP 进行调用，建立或者解除某个 API 与某个 APP 的授权关系，API 网关会对权限关系进行验证。

2.1.9　安全风险案例分析

1. 配置错误

2014 年 11 月，某公司云服务出现大面积服务中断现象，但其服务健康仪表控制板却显示一切应用正常运行。此次事故造成的影响波及美国、欧洲和部分亚洲地区，导致其相关应用和网站等无法使用。故障时长近 11 个小时，原因为存储组件在更新时产生错误，导致 Blob 前端进入死循环状态，从而造成流量故障。当技术维护团队发现问题后，恢复了之前配置，但由于 Blob 前端已经无法更新配置，因此只能采取系统重启模式，使得恢复过程消耗了相当长的时间。该公司技术团队在事故发生后采取了一系列改进措施，包括改变灾备恢复方法，最大限度减少恢复时间；修复 Blob 前端关于 CPU 无限循环的漏洞；改进服务健康仪表控制板基础设施和协议。

2015 年 2 月，另一公司的实例出现外部流量丢失现象，导致大量应用程序无法使用。事后经过调查，流量损失时间长度为 2 小时 40 分钟，从 18 日晚上 22:40 至 23:55，其外部流量损失由 10% 增长到 70%，在 19 日凌晨 1:20，流量恢复了正常。此次事件发生的原因为虚拟机实例的内部网络系统停止更新路由信息，虚拟机的外部流量数据被视为过期而遭到删除。为防止类似事件再度发生，工程师们将路由项的到期时间由几个小时延长到了一个星期，并添加了路由信息的监控和预警系统。

2. 宕机事件

2011 年 4 月，某公司的云计算数据中心宕机，导致其数千家商业客户受到影响，故障时间持续 4 天之久，此次事件可以说是一场严重的宕机事件。经调查，造成此次事故的主要原因是在修改网络设置进行主网络升级扩容的过程中，工程师不慎将主网的全部数据切换到备份网络上，由于备份网络带宽较小，承载不了所有数据造成网络堵塞，所有块存储节点通信全部中断，导致存储数据的 MySQL 数据库宕机。事故发生后，该公司重新审计了网络设置修改流程，加强了自动化运维手段并改进了灾备架构以避免该类事故再次发生。

2015 年 5 月，某公司系统出现大规模瘫痪，国内很多在线支付用户在 PC 端和移动端均无法使用，这一事故持续了差不多两小时。此次事故是由于市政施工导致光缆被挖断，进而导致该公司一个主要机房受影响而造成的。

2015 年 5 月，某公司的部分服务器遭不明攻击，导致官网及 APP 暂时无法正常使用。经技术排查已确认，此次事件是由于员工错误操作，删除了生产服务器上的执行代码导致。

3. 隐私泄露

2014 年 9 月，黑客攻击了某公司的云存储服务账户，导致大量用户私密照片和视频泄露。该公司发表声明称，本次泄露事件黑客并没有利用此前受怀疑的服务漏洞，而是因为用户账户在用户名、密码以及安全问题的设置上存在重大隐患导致的，也就是说，部分受害者设置的密码太过简单。另外，调查结果显示，泄漏照片的拍摄设备并非来自同一品牌，并且一部分照片明显经过通信软件的处理，通过某款通信 APP 发送或接收。据技术专家判定，本次泄露并非全部来自同一公司的云服务应用，或者某些通信 APP 的聊天记录，这很有可能是受害者在多

个网络服务中使用了相似甚至相同的密码导致的。因此，该信息泄露事件的原因并非是云服务器端的泄露，而是黑客针对性地攻击得到用户账号的密码，或者是密码保护问题的详细资料，然后冒充用户身份登录窃取到云端数据，本质上采用的是身份欺骗的手段。攻击者利用的缺陷是云端对用户的身份认证只通过用户名密码方式，认证强度不够而导致资料被盗取。

4. 恶意攻击

DDoS 是 Distributed Denial of Service 的缩写，即分布式拒绝服务。DDoS 攻击就是指以分散攻击源来非法进入指定网站的黑客方式。DDoS 的攻击方式有很多种，最基本的攻击就是利用合理的服务请求来占用过多的服务器资源，从而使合法用户无法得到服务器响应。

2013 年 3 月，欧洲反垃圾邮件机构 Spamhaus 曾遭遇 300G DDoS 攻击，导致全球互联网大堵塞。

2014 年 2 月，针对 Cloudflare 的一次 400G 攻击造成 78.5 万个网站安全服务受到影响。

2014 年 12 月，部署在阿里云上的一家知名游戏公司，遭遇了全球互联网史上最大的一次 DDoS 攻击，攻击时长 14 个小时，攻击峰值流量达到每秒 453.8G。阿里云称，第一波 DDoS 从 12 月 20 日 19 点左右开始，一直持续到 21 日凌晨，第二天黑客又再次组织大规模攻击，共持续了 14 个小时。阿里云安全防护产品“云盾”，结合该游戏公司的“超级盾防火墙”，帮助用户成功抵御了此次攻击。

2.2　云计算面临的管理风险

数据的所有权与管理权分离是云服务模式的重要特点，用户并不直接控制云计算系统，对系统的防护依赖于云服务商。在这种情况下，云服务商的管理规范程度、双方安全边界划分是否清晰等将直接影响用户应用和数据的安全。

2.2.1　组织与策略风险

1. 服务中断

云计算的优势在于提供资源的优化和 IT 服务的便捷性。在缩减 IT 成本的前提下，如何保证业务运营的连续性一直是备受业界关心的问题之一。即使时间再短的云计算服务中断也会让企业陷入困境，而云计算服务的长时间中断甚至可能使一个企业面临倒闭。因此，对于云服务商而言，确保业务不中断是一个关键问题。可能引起业务中断的安全风险如 2-7 所示。

1）**技术故障**：技术故障主要由于以下两个原因造成：①由于云计算数据中心的硬件故障、云计算平台的软件故障、通信链路故障等，可能导致服务计划外中断。②由于数据中心未进行有效的安全保护、监控、定期维护、没有制定切实有效的应急响应方案等，从而导致服务计划外中断。

2）**环境风险**。由于水灾、火灾、大气放电、太阳引起的地磁风暴、风力灾害、地震、海啸、爆炸、核事故、火山爆发、生化威胁、民事骚扰、泥石流、地壳活动等引起的数据中心基础设施受损、水电供应不稳定、通信链路中断等情况，进而导致云服务计划外中断。

3）**操作失误**：由于云租户管理员操作不当、配置错误等导致云服务计划外中断。

4）**恶意攻击**：由于敌手的恶意攻击造成云服务计划外中断、勒索、破坏。

2．供应链风险

云服务商在构建云平台时往往需要购买第三方的物理设施、产品（如物理服务器，交换机等）和服务（水、电、网服务和第三方外包服务等），与此同时相关的开发人员也是云服务商供应链的重要环节。从供应链层面来看，风险主要有以下几类，如图 2-8 所示。

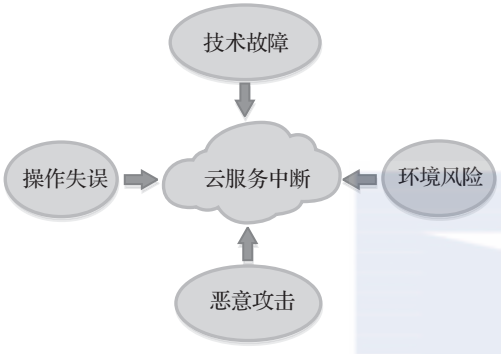


图 2-7　云服务中断

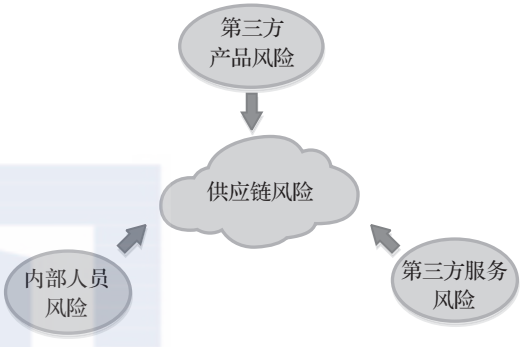


图 2-8　供应链风险

1）第三方产品风险：由于云服务商要购买大量物理计算设备和网络设备，如果供应商产品不符合国内法律政策的标准或云服务商安全需求，甚至采用假冒伪劣的设备，将会对云服务商造成难以估量的巨大损失。

2）第三方服务风险：云服务商需要的第三方服务主要包括基础设施服务（如水、电和网络服务等）和外包服务（如加密服务等）。对于基础设施服务，如果服务供应商未经过相关资质认证，出现停电、停水等事故将会影响云服务商的正常服务；外包服务则要评估外包信息系统的安全性和稳定性，其开发人员是否有安全开发能力等，以避免自身云服务不稳定的威胁。

3）内部人员风险：云服务商内部人员主要包括云开发人员和云运维人员。对于云开发人员，风险主要在于其开发的信息系统是否安全；设计是否遵循了安全的设计规范；最终的代码中是否存在相关漏洞；其开发人员是否存在泄密风险等。云平台运维人员主要完成云平台的运维工作，其风险主要包括运维方式是否科学合理、运维目的是否规范、盗窃运维数据等。

因此，无论是云平台开发人员还是运维人员都应该对其进行相应的背景审查、专业的安全培训，云服务商也需要定期对内部人员进行权限审批、操作行为审查及审计、入侵识别评估和安全风险关联分析，将内部人员风险降到最低。

2.2.2　数据归属不清晰

在云计算时代，数据将成为最有价值的资产。在云环境下，不同用户的数据都存储在共享的云基础设施之上，当用户的数据存储与数据维护工作都是由云服务商来完成时，就很难分清到底是谁拥有使用这些数据的权利并对这些数据负责。目前，大多数云商都通过职责划

分、用户协议、访问控制等多种方式来限制内部人员接触数据并且尽可能与用户达成共识。比如，在 2015 年 7 月，阿里云曾发起“数据保护协议”自律公约，明确“数据是客户资产，云平台不得擅自移做他用”。

2.2.3　安全边界不清晰

在传统网络中，通过物理上或者逻辑上的安全域定义将物理资源进行区域划分，在不同的区域边界可以通过引入边界防护设备（如防火墙、IPS 等）进行边界防护，但是在云环境下，随着虚拟化技术的引入，租户的资源更多以虚拟机的形式呈现，由于云计算环境中服务器、存储设备、网络设备的高度整合，租户的资源往往是跨主机甚至是跨数据中心的部署，传统的物理防御边界被打破，租户的安全边界模糊，因此需要进一步发展传统意义上的边界防御手段来适应云计算的新特性。

2.2.4　内部窃密

由于云服务商在为用户提供云服务的过程中不可避免地会接触到用户的数据，因此云服务商内部窃密是一个重大的安全隐患。事实上，内部窃密可分为内部工作人员无意泄露内部特权信息或者有意和外部敌手勾结窃取内部敏感信息两种情况。在云计算环境下，内部人员不再是以往我们所说云服务商的内部人员，也包括为云服务商提供第三方服务的厂商的内部人员，这也增加了内部威胁的复杂性。此时需要采用更严格的权限访问控制来限制不同级别内部用户的数据访问权限。

2.2.5　权限管理混乱

云服务商内部需要完善的权限管理机制来避免数据泄露的问题，但是由于云计算自身具有易扩展、多租户、弹性化等诸多有别于传统模型的特征，在传统模型下的一些权限模型（如 DAC、MAC、RBAC）并不完全适用于目前的云平台组织结构复杂、权限变更频繁的场景，因此在云环境中权限管理还没有成熟的解决方案，各大厂商采用的方案都还存在一定缺陷，导致目前云中的权限管理混乱。

2.3　云计算面临的法律法规风险

为了保障云上的服务健康良好地发展，更好地助力企业理性上云、安全上云，建立良好的法律法规体系是重要的一环。但是，云计算作为一种新的服务模型，其本身的特性又决定了其法律制定与传统法律制定的差别与冲突。

2.3.1　数据跨境流动

数据跨境流动（Data Transborder Flow）首先出现在个人数据保护立法中，用于管理个人

数据向第三国的转移。随着云计算的出现，其泛在的网络接入导致了数据流动性大的特征，大规模的政府数据、商业数据以及个人数据跨境更加频繁，因此各国开始重新审视数据跨境流动的制度规范，特别是政府部门和公共部门的数据跨境流动制度规范。

当前针对数据跨境流动，在国际上并没有统一的定义和明确的界定。联合国跨国公司中心指出了“跨越国界对存储在计算机中的机器可读的数据进行处理、存储和检索”属于数据跨境流动的范畴；经济合作与发展组织（Organization for Economic Co-operation and Development，OECD）对数据跨境流动的定义是个人数据跨越国界流动；澳大利亚在联邦个人隐私原则中对“数据的跨境流动”进行了规定，要求机构向海外组织或信息主体以外的某人传送信息应该受到一定的制约。由此可见，通常对于数据跨境的流动有两层含义：一方面是对数据跨越国界的存储、传输和处理；另一方面则是数据并没有跨越国界，但是能够被第三方国家的主体访问。

虽然就数据的跨境流动尚未形成统一的框架，但是从国外针对不同类型数据的管理模式来看，主要分为三个级别。

1. 禁止重要的数据跨境流动

对于一些威胁到国家安全的数据信息，禁止其跨境的流动具有相当的必要性，一些国家也逐渐意识到重要数据在本地存储的重要性。例如，美国虽然没有相关的法律规定禁止数据的跨境流动，但是在外资安全审查机制中，针对国外的网络运营商，会要求其与电信企业签订相关的协议，要求国内的通信基础设施应位于美国境内，并且通信数据、交易数据、用户信息等也只能在美国境内存储；印度的电信许可协议中明确禁止各类电信企业将用户的账户信息、个人信息转移至境外；意大利、匈牙利等国家也有相关法律法规禁止将政府数据交由国外的 IaaS 服务提供商存储。除此之外，印度尼西亚、澳大利亚、韩国等国家都有相关的法律法规明确指出禁止重要的数据跨境流动。

2. 有条件的限制数据跨境流动

对于政府部门和公共部门的一般数据、行业相关的技术数据等，部分国家针对这类型的数据实施了条件限制的管理模式来控制其跨境的流动。例如，在澳大利亚《政府信息外包、离岸存储和处理 ICT 安排政策与风险管理指南》中规定，把政府部门的信息进行分级，对于非保密的信息，要求必须通过安全风险评估之后才能实施外包。

3. 允许普通个人数据的跨境流动

对于普通用户的个人数据，国际上通用的观点是允许其自由跨境流动，但是必须满足安全的管理要求。出于对个人数据的安全考虑，一般采用问责制、合同干预等形式来进行管理。问责制一般是通过责任的界定，要求采集和处理数据的实体对数据进行安全管理，并要求其承担数据在跨境的整个过程中的审查和监督；合同干预则是由政府来规定跨境数据的安全管理相关内容。例如，在欧盟，根据数据保护法的原则，由数据保护主管部门来制定相关的合同条款，指明数据保护的要求。

针对国际范围内的数据流动，目前还处于发展中，部分国家出台了各自的法律法规来要求是否允许本国的数据跨境存储和传输。美国于 1974 年通过《隐私法》，由于美国在全球范

围内有大量跨国公司，因而其倾向于信息的自由流通，对数据的跨境流动不做专门限制；英国在 1984 年通过《数据保护法》，其规定数据跨境流动时，需要向相关机构进行登记；德国在 20 世纪 70 年代通过《个人数据保护法》，规定数据跨境的流动要按照相关协定来进行管理；欧盟在《关于个人数据处理保护与自由流动指令》和《有关个人数据处理和电子通信领域隐私保护的指令》明确指出对数据跨境流动的相关规定；澳大利亚的《政府信息外包、离岸存储和处理 ICT 安排政策与风险管理指南》中对于安全分类数据的存储进行了相关规定；韩国的《信息通信网络的促进利用与信息保护法》规定，为了防止任何有关工业、经济、科学、技术等重要信息的跨境流动，信息通信提供商可采取必要手段；加拿大在《个人信息保护和电子文件法》中规定，传输、拥有或保管个人信息的机构应该对这些信息负责。

就目前国外针对跨境数据流动的管理趋势而言，可以从三个层面来分析：第一，从管理范围上，重点关注政府部分和公共部门的数据跨境流动管理。一些国家已经制定了专门的管理制度。例如，上文提到的澳大利亚《政府信息外包、离岸存储和处理 ICT 安排政策与风险管理指南》中对政府数据进行分级管理，并规定了政府数据的离岸存储和风险管理；加拿大在《关于解决美国爱国者法案和跨境数据流动问题的联邦战略》向联邦政府提出了 160 条关于数据安全管理的建议；第二，从管理对象上，加强对数据跨境流动的监管。数据的跨境流动主要依托于互联网，因此，各国在新签署自由贸易协定或双边投资协定时，对电信业务的跨境服务承诺开始变得极为谨慎；第三，从管理机制上，增强各国的跨境执法合作，加强各国用户对跨境数据流动的信任。由于各国不同的管理机制限制了数据跨境流动的发展，因此一些国际组织尝试从国际层面来建立协调机制。例如，APEC 建立了跨境隐私执法协作机制（Cross-border Privacy Enforcement Arrangement，CPEA）来协调数据跨境流动。

在我国，随着国外公司陆续进入到我国的云服务市场，我国的数据跨境流动的相关管理机制的建立与完善日益受到重视。从国外的经验来看，一方面，可以在相关法律法规中明确数据跨境流动的相关概念和管理模式，另一方面，可以建立针对数据跨境流动的多元化管理手段，例如分级分类管理、合同管理、安全风险评估等都是可取的手段措施。

2.3.2　集体诉讼

集体诉讼起源于英国，但是却在美国开花结果，它指个人或部分成员为了全体成员的共同利益，代表整个团体成员提出的诉讼。在现实中，一些企业遭遇的集体诉讼的案例也对后来的公司或企业产生了深远的警示意义。

2.3.3　个人隐私保护不当

在云计算、大数据孕育的时代，社会的发展取得了巨大的进步，但与此同时，个人隐私的问题也浮现出来。近年来，侵犯个人隐私的案件时有发生，之前被曝光的用户信息泄露事件严重侵犯了用户的合法权益。因此，建立云环境下的个人隐私保护制度刻不容缓。

在云计算、大数据环境下，个人隐私的安全风险表现在以下几个方面：

1）数据存储过程中对个人隐私造成侵犯：在云服务商给用户提供云服务的时候，数据的

存储对用户来说是透明的，用户无法得知数据确切的存储位置，更无法对其个人数据的采集、存储、使用的过程进行有效控制。

2）数据传输过程中对个人隐私造成侵犯：云环境下的数据传输具有开放性和多元化的特征，传统的物理区域的隔离方法和技术无法适应云环境下数据的远距离传输，更加无法保证数据传输过程中的安全性。

3）数据处理过程中对个人隐私造成侵犯：云服务的部署引入大量的虚拟化技术，基础设施的脆弱性或加密措施的失效引入了新的安全风险，大规模的数据处理需要完备的访问控制、身份认证管理，而云计算的资源动态性增加了管理的难度，账户劫持、攻击、认证失效等都将成为数据处理过程中的安全威胁。

4）数据销毁过程中对个人隐私造成侵犯：单纯对数据的删除并不能彻底的销毁数据，再加之云服务商可能对数据进行备份，进一步增加了数据销毁不彻底的可能性。

由此可见，在云计算的时代，我们需要切实加强个人隐私的保护，主要可以从如下几个方面着手：

（1）从国家的战略层面来保护个人信息

在云计算大数据时代，个人隐私构成了网络社会运行的基石。在我国，从网络系统、设备到操作系统、应用软件等核心技术依然面临巨大的安全风险，这不仅对国家的安全造成了威胁，同时对用户的个人隐私也造成了风险，因此需要从国家层面来建立针对个人隐私的保护战略和机制。

（2）加快完善个人隐私的立法保护

在云计算大数据的背景下，对于个人隐私，从技术层面保护远远不够，必须建立完善的法律法规，用法律的武器打击不法分子，保障用户权益。

（3）加强对个人隐私保护的行政监管

在信息网络的环境下，个人信息和个人隐私等具有了财产属性，部分不良的企业可能对其进行商业化利用以达到盈利的目的，因此，政府的有效监管、个人隐私方面的测评机制和标准就显得尤为必要。

（4）加强对个人隐私的技术保护

技术手段是法律措施的重要补充，应积极进行隐私保护技术的研发和创新，从技术层面来保障个人隐私的安全。

2.4　云计算安全设计原则

云计算作为一种新兴的信息服务模式，尽管会带来新的安全风险与挑战，但其与传统 IT 信息服务的安全需求并无本质区别，核心需求仍是对应用及数据的机密性、完整性、可用性和隐私性的保护。因此，云计算安全设计原则应从传统的安全管理角度出发，结合云计算自身的特点，将现有成熟的安全技术及机制延伸到云计算安全设计中，满足云计算的安全防护需求。

2.4.1　最小特权

最小特权原则是云计算安全中最基本的原则之一，它指的是在完成某种操作的过程中，赋予网络中每个参与的主体必不可少的特权。最小特权原则一方面保证了主体能在被赋予的特权之中完成需要完成的所有操作；另一方面保证了主体无权执行不应由它执行的操作，即限制了每个主体可以进行的操作。

在云计算环境中，最小特权原则可以减少程序之间潜在的相互影响，从而减少、消除对特权无意的、不必要的或者不适当的使用。另外，能够减少未授权访问敏感信息的机会。

在利用最小特权原则进行安全管理时，对特权的分配、管理工作就显得尤为重要，所以需要定期对每个主体的权限进行审计。通过定期审核来检查权限分配是否正确，以及不再使用的账户是否已被禁用或删除。

2.4.2　职责分离

职责分离是在多人之间划分任务和特定安全程序所需权限的概念。它通过消除高风险组合来限制人员对关键系统的权力与影响，从而降低个人因意外或恶意而造成的潜在破坏。这一原则被应用于云的开发和运行的职责划分上，同样也应用于云软件开发生命周期中。一般情况下，云的软件开发为分离状态，确保在最终交付物内不含有未授权的后门，确保不同人员管理不同的关键基础设施组件。

此外，职责分离还伴随着岗位轮换，如图 2-9 所示。管理层应给重要岗位的员工安排假期，并在该员工休假期间进行目标岗位的工作审计。因为职责轮换一般都涉及放假，所以职责轮换也通常成为强制放假。职责轮换除了可以进一步防止重要岗位的欺诈之外，也可以让人员熟悉本来不属于他负责的其他工作，为业务流程的岗位安排带来人员备份和协调工作能力提升的好处。

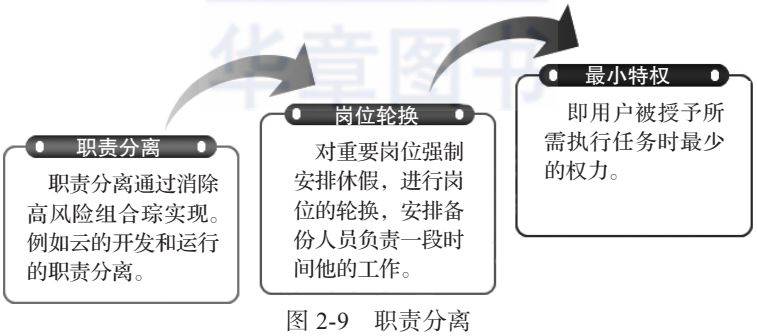


图 2-9　职责分离

2.4.3　纵深防御

在云计算环境中，原有的可信边界日益削弱，攻击平面也在增多，过去的单层防御已经难以维系安全性，纵深防御是经典信息安全防御体系在云计算环境中的必然发展趋势。云计算环境由于其结构的特殊性，攻击平面较多，在进行纵深防御时，需要考虑的层面也较多，从底至上主要包括：物理设施安全、网络安全、云平台安全、主机安全、应用安全和数据安全等方面，如图 2-10 所示。

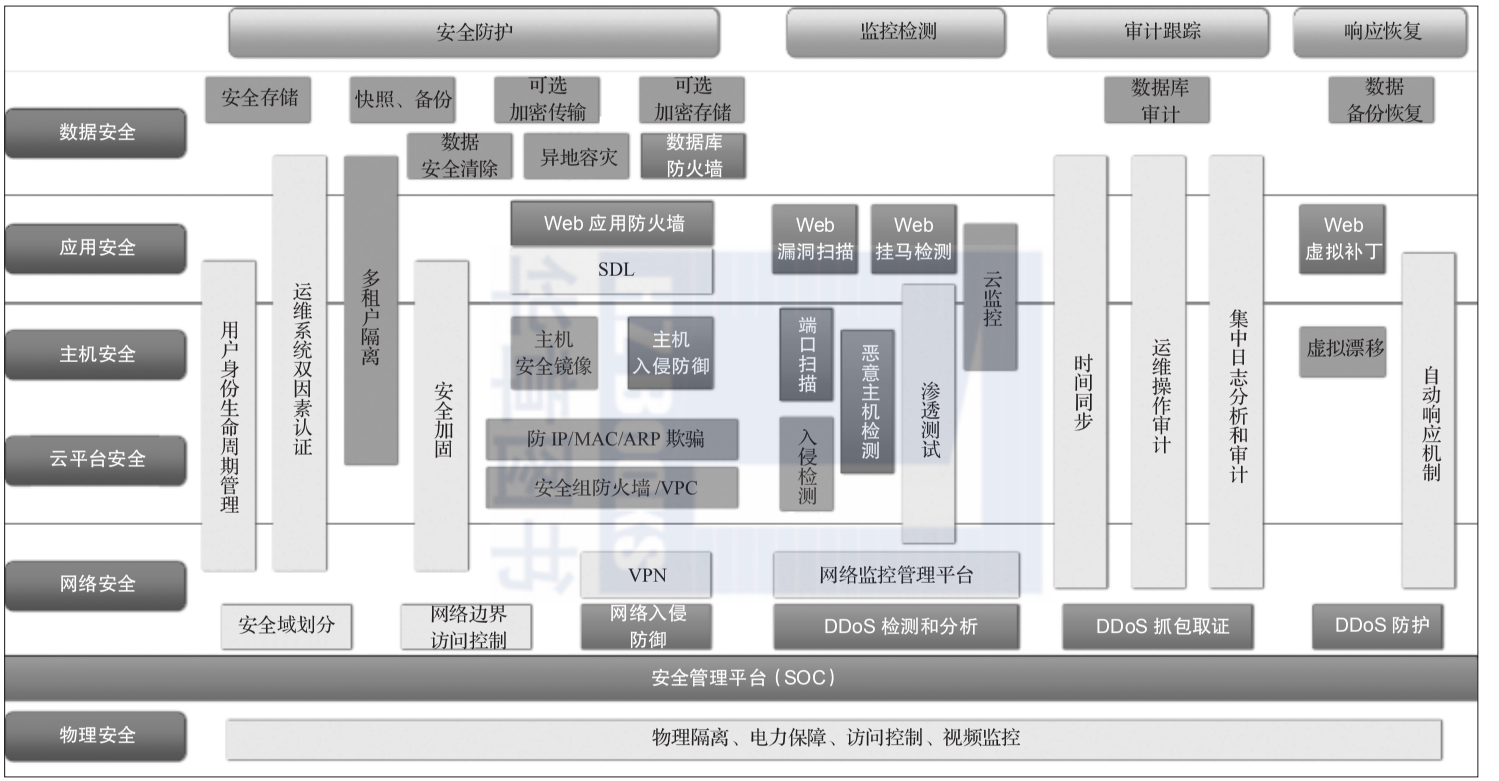

安全防护
监控检测
审计跟踪
响应恢复
数据安全
应用安全
主机安全
云平台安全
网络安全
物理安全
安全存储
快照、备份
可选加密传输
可选加密存储
数据安全清除
异地容灾
数据库防火墙
数据库审计
数据备份恢复
Web 应用防火墙
SDL
Web 漏洞扫描
Web 挂马检测
云监控
Web 虚拟补丁
虚拟漂移
用户身份生命周期管理
运维系统双因素认证
多租户隔离
安全加固
主机安全镜像
主机入侵防御
端口扫描
恶意主机检测
渗透测试
时间同步
运维操作审计
集中日志分析和审计
自动响应机制
防 IP/MAC/ARP 欺骗
安全组防火墙 /VPC
入侵检测
VPN
网络监控管理平台
安全域划分
网络边界访问控制
网络入侵防御
DDoS 检测和分析
DDoS 抓包取证
DDoS 防护
安全管理平台（SOC）
物理隔离、电力保障、访问控制、视频监控

图 2-10　纵深防御

另外，云计算环境中的纵深防御还具有多点联动防御和入侵容忍的特性。在云计算环境中，多个安全节点协同防御、互补不足，会带来更好的防御效果。入侵容忍则是指当某一攻击面遭遇攻击时，可以通过安全设计手段将攻击限制在这一攻击层面，使攻击不能持续渗透下去。

根据木桶原理，系统的安全性取决于整个系统中安全性最低的部分，这个原理在云计算环境下同样适用。针对某一方面、采取某种单一手段增强系统的安全性，无法真正解决云计算环境下的安全问题，也无法真正提高云计算环境的安全性。云计算的安全需要从整个系统的安全角度出发进行考虑。

2.4.4　防御单元解耦

将防御单元从系统中解耦，使云计算的防御模块和服务模块在运行过程中不会相互影响，各自独立工作。这一原则主要体现在网络模块划分和应用模块划分两个方面。可以将网络划分成 VPC（Virtual Private Cloud）模式，保证各模块的网络之间进行有效的隔离。另一方面，将云服务商的应用和系统划分为最小的模块，这些模块之间保持独立的防御策略。另外，对某些特殊场景的应用还可以配置多层沙箱防御策略，如图 2-11 所示。

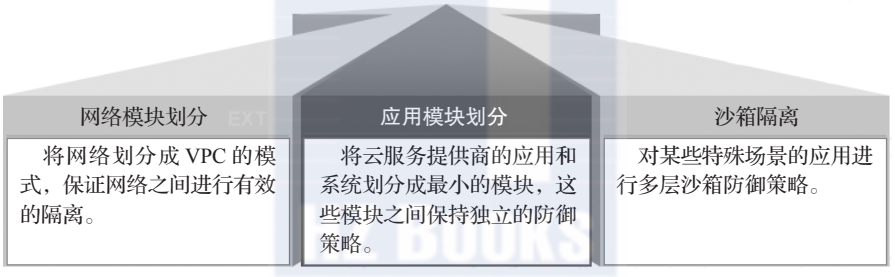


图 2-11　防御单元解耦

2.4.5　面向失效的安全设计

面向失效的安全设计原则与纵深防御有相似之处。它是指在云计算环境下的安全设计中，当某种防御手段失效后，还能通过补救手段进行有效防御；一种补救手段失效，还有后续补救手段。这种多个或多层次的防御手段可能表现在时间或空间方面，也可能表现在多样性方面。

2.4.6　回溯和审计

云计算环境因其复杂的架构导致面临的安全威胁更多，发生安全事故的可能性更大，对安全事故的预警、处理、响应和恢复的效率要求也更高。因此，建立完善的系统日志采集机制对于安全审计、安全事件追溯、系统回溯和系统运行维护等方面来说就变得尤为重要。在云计算环境下，应该建立完善的日志系统和审计系统，实现对资源分配的审计、对各角色授权的审计、对各角色登录后的操作行为的审计等，从而提高系统对安全事故的审查和恢复能力。

2.4.7　安全数据标准化

由于目前的云计算解决方案很多，且不同的解决方案对相关数据、调用接口等的定义不同，导致目前无法定义一个统一的流程来对所有的云计算服务的安全数据进行采集和分析。目前已经有相关的组织对比进行了研究，如云安全联盟 CSA 提出的 CTP（云可信协议）协议以及动态管理工作组 DMTF 提出的 CADF（云审计数据互联）模型。

2.5　小结

云计算的灵活性和经济性吸引着越来越多的客户，但也有大量潜在客户因为担心云计算面临的安全风险而驻足不前。因此，在云计算建设和应用时采用多种安全设计，可以大大降低这些风险，逐渐消除客户的疑虑。解决了云计算的安全问题，云计算的发展前景将更为广阔，更好地为我们的工作、生活服务。

2.6　参考文献与进一步阅读

[1] 徐蓉 . 理解云计算漏洞 [J]. 网络安全技术与应用，2015（08）：79-80.
[2] 周勇 . 移动网络中的云计算及其安全问题探讨 [J]. 信息通信，2015（07）：229-230.
[3] 王冉晴，范伟 . 云计算安全威胁研究初探 [J]. 保密科学技术，2015（04）：13-18.
[4] 贾创辉，韦勇，颜颀 . 基于 Xen 架构的桌面云安全研究 [J]. 网络安全技术与应用，2014（09）：127-128.
[5] 李峰 . 基于云计算的计算机系统面临的风险与对策 [J]. 中国西部科技，2014（03）：87-88.
[6] 李亚方，俞国红 . 云计算安全防范及对策研究 [J]. 电脑知识与技术，2013（36）：46-48.
[7] 姚平，李洪 . 浅谈云计算的网络安全威胁与应对策略 [J]. 电信科学，2013（08）：90-93.
[8] 沈军，樊宁 . 电信 IDC 云计算应用与安全风险分析 [J]. 信息安全与通信保密，2012（11）：95-97.
[9] 别玉玉，林果园 . 云计算中基于信任的多域访问控制策略 [J]. 信息安全与技术，2012（10）：39-45.
[10] 白璐 . 信息系统安全等级保护物理安全测评方法研究 [J]. 信息网络安全，2011（12）：89-92.
[11] 何明，沈军，金涛 . 云主机安全运营技术探析 [J]. 电信技术，2011（11）：9-11.
[12] 黄虹 . 基于等级保护的网络物理安全建设 [J]. 科技广场，2010（01）：226-228.
[13] 在云计算中使用虚拟化面临的安全问题 [EB/OL]. http://chengfei.blog.51cto.com/503939/1532984.
[14] 针对 SSL 的中间人攻击 [EB/OL]. http://blog.csdn.net/ztclx2010/article/details/6891682.

PART 2

第二部分

云计算服务的安全能力与运维

CHAPTER 3

第3章

主机虚拟化安全

虚拟化技术起源于20世纪60年代，是指将一个高性能物理服务器划分为多个独立的“虚拟机”，在用户看来，在虚拟机上操作和物理服务器上操作没什么区别。虚拟化是云计算的基础，云计算的重要特性（如动态伸缩、按需分配等）都需要虚拟化技术来提供支撑。虚拟化带来了IT资源整合以及访问终端的变革，但也引入了一些新的安全问题。本章将针对主机虚拟化技术及其面临的安全威胁展开讨论，并给出有针对性的主机虚拟化安全加固方案。

3.1 主机虚拟化技术概述

虚拟化技术经过半个多世纪的发展，已日趋成熟并逐渐得到广泛的应用，成为云计算的基础技术。

1959年，在国际信息处理大会上，著名科学家克里斯托弗（Christopher Strachey）发表了一篇名为“大型高速计算机中的时间共享”（Time Sharing in Large Fast Computers）的学术报告。在该报告中，他提出了虚拟化的基本概念，同时这篇文章也被认为是对虚拟化技术的最早的论述。

1965年，IBM公司发布IBM7044，它被认为是最早在商业系统中实现的虚拟化。它通过在一台大型主机上运行多个操作系统，形成若干个独立的虚拟机，让每一个用户可以充分利用整个大型机资源，有效解决了大型机资源利用率不足的问题。

1999年，由于X86平台已具备高效的处理能力，VMware公司在X86平台上推出了商用的虚拟化软件。这也标志着虚拟化技术从大型机时代走向了PC服务器的时代。

现在，随着云计算技术的快速发展，作为与云计算密不可分的虚拟化技术也得到了进一步的发展。越来越多的厂商，包括VMware、Citrix、微软、Intel、Cisco等都加入了虚拟化技术的市场竞争，虚拟化技术在未来将具有广阔的应用前景。

3.1.1 主机虚拟化的概念

有很多标准组织对**虚拟化**（virtualization）进行了定义。维基百科对于虚拟化的描述是：

在计算机技术中，虚拟化技术或虚拟技术是一种资源管理技术，是将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等）予以抽象、转换后呈现出来，并可供分区、组合为一个或多个电脑配置环境。由此，打破实体结构间的不可切割的障碍，使用户可以比原本的配置更好的方式来应用这些电脑硬件资源。这些资源的新虚拟部分是不受现有资源的架设方式、地域或物理配置所限制。虚拟化资源一般包括计算能力和数据存储。开放网格服务体系（Open Grid Services Architecture，OGSA）对虚拟化的定义是：虚拟化是对一组类似资源提供的通用抽象接口集，进而隐藏了属性和操作间的差异。IBM 则认为，虚拟化是资源的逻辑表示，它不受物理限制的约束。

尽管不同的组织机构对虚拟化有不同的定义，但总的来说，我们可以这样理解虚拟化：虚拟化是对各种物理资源和软件资源的抽象利用。这里所说的资源包括硬件资源（如 CPU、内存、网络等），也包括软件资源（如操作系统、应用程序等）。对于用户来说，他只需要利用虚拟化环境来完成自己的工作，而不需要了解虚拟化逻辑资源的内部细节；在虚拟化环境下，用户可以在其中实现与在真实环境下相同的功能或部分功能。

主机虚拟化作为一种虚拟化实现方案，旨在通过将主机资源分配到多台虚拟机，在同一企业级服务器上同时运行不同的操作系统，从而提高服务器的效率，并减少需要管理和维护的服务器数量。与传统服务器相比，主机虚拟化在成本、管理、效率和灾备等方面，具有显著的优势。通过主机虚拟化实现方案，企业能够极大地增强 IT 资源的灵活性，降低管理成本并提高运营效率。

如图 3-1 所示，主机虚拟化架构通常由物理主机、虚拟化层软件和运行在虚拟化层上的虚拟机组成。物理主机是由物理硬件（包括 CPU、内存、I/O 设备）所组成的物理机器；虚拟化层软件又被称作 Hypervisor 或者虚拟机监视器（Virtual Machine Monitor，VMM），它的主要功能是将物理主机的硬件资源进行调度和管理，并将其分配给虚拟机，管理虚拟机与物理主机之间资源的访问和交互。虚拟机则是运行在虚拟化层软件之上的各个客户机操作系统，用户可以像使用真实计算机一样使用它们来完成工作。对于虚拟机上的各个应用程序来说，虚拟机就是一台真正的计算机。

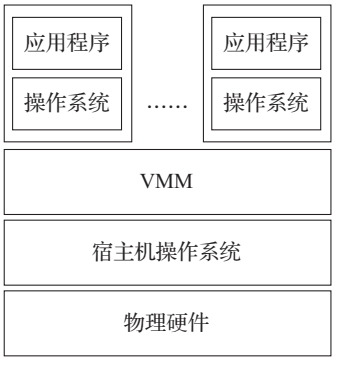


图 3-1　主机虚拟化架构示意图

3.1.2　主机虚拟化实现方案

在基本遵循主机虚拟化架构的前提下，业界主流公司都提出了其主机虚拟化解决方案，其典型代表有：VMware Workstation、Microsoft Virtual PC、Xen、KVM 等。

1. VMware Workstation

VMware Workstation 是一个基于主机的虚拟机产品，可以在 Windows、Linux 和 Macintosh 等主流操作系统上运行。它包含内核 VMM、虚拟机扩展驱动 VMX 和 VMware 应用程序三个模块，VMM 负责虚拟机的创建管理等核心工作；VMX 驱动运行在 Ring0 特权级，辅

助 VMM 完成虚拟机操作系统触发的 I/O 操作；VMware 应用程序运行在 Ring3 特权级，是 VMware Workstation 的人机界面。当启动 VMware 应用程序时，VMX 驱动将 VMM 加载到核心区域，并赋予 VMM 和 VMX 驱动 Ring0 特权级，虚拟机操作系统能够探测到 VMX 和 VMware 应用程序，但是无法感知到 VMM。VMM 可以直接控制处理器内存，或者管理 VM 与主机通信来完成虚拟机 I/O 等特殊指令。

当虚拟机操作系统或在其之上运行的应用程序执行计算时，虚拟机可以获得处理器的控制权，程序直接在处理器硬件上执行。当虚拟机需要执行 I/O 操作或者执行敏感指令时，VMM 模块就会捕获这些指令并将处理器切换到 VMM 控制模式，在主机环境中由 VMX 模块或 VM 应用模拟执行 I/O，必要时由主机操作系统触发真实 I/O。由于 I/O 是由虚拟机操作系统引发，因此执行结果将通过 VMM 传递回虚拟机。虚拟机的处理器和内存调用基本是靠硬件实现，执行效率高，而 I/O 操作虚拟环境切换，导致虚拟机 I/O 性能较低。

2. Microsoft Virtual PC

微软公司的 Virtual PC 是一款基于主机操作系统的虚拟化产品，与 VMware Workstation 非常类似。Virtual PC 可以运行于 Windows 操作系统和 Macintosh 操作系统上，在操作系统上支持多个 Windows 操作系统实例及其应用程序的运行。与 VMware 相比，Virtual PC 有很多不足，如不支持 Windows 以外的操作系统（Linux、FreeBSD、Solaris 等）；Virtual PC 虚拟机不能修改已经赋予虚拟机使用的虚拟硬件设备，不支持 SCSI 设备，因此局限性比较大。Virtual PC 有一项特殊的功能，允许用户撤销在虚拟磁盘中所做的操作，使虚拟机恢复先前的状态，这在测试中非常有用。

3. Xen

Xen 采用半虚拟化技术，需要对操作系统进行修改才能与虚拟机监视器协同工作，这也就使得 Xen 无需硬件支持就能以较高效率实现虚拟化。在 Xen 中，虚拟机被称为域（Domain），其中，Domain 0 是一个管理域，它作为一个特殊域，可直接访问硬件资源，协助虚拟机监视器完成虚拟机的管理工作，为虚拟机监视器提供扩展服务。与 Domain 0 相比，普通虚拟机只能访问虚拟硬件资源，我们称之为普通域。虚拟机监视器运行在 Ring 0 特权级上，Domain 0 的内核运行在 Ring 1 上，它拥有系统 I/O 等硬件设备，负责向其他域提供虚拟硬件资源。Domain 0 作为整个系统的管理平台，可以通过超级调用（Hypercalls，是一种对 Hypervisor 的调用申请，类似于操作系统中的系统调用）来创建、保存、恢复、移植和销毁普通虚拟机。

Xen 普通虚拟机（Domain U）不能访问自身之外的任何硬件资源，包括虚拟机监视器拥有的硬件资源，但是可以通过 Hypercalls 向虚拟机监视器申请各种硬件服务，如内存更新、Domain 0 支持、处理器状态等，并且 Hypercalls 支持批处理调用，即能将 Hypercalls 集中在一个队列中统一处理，提高系统处理速度。

4. KVM

KVM 和 Xen 是两个比较接近的开源虚拟化实现方案，但是它们依然有很多不同。KVM 作为一个 Linux 内核核心模块，已经成为 Linux 的一个组成部分。KVM 虚拟化实现方案充

分利用了 Linux 进程调度算法和内存管理技术，任何 Linux 内核性能的改进或版本提升均可直接应用于 KVM 虚拟化实现方案中，从而使 KVM 虚拟机获得性能上的提高。KVM 充分利用了 Linux 内核模块简单而高效的特点，修改 KVM 模块无需重新编译 Linux 内核，只需在 Linux 中重新加载修改后的 KVM 模块即可。

3.1.3　主机虚拟化的特性

在高性能的物理硬件产能过剩以及老旧硬件产能过低的情况下，为了实现硬件资源的合理分配和使用，虚拟化技术应运而生。不同类型的虚拟化技术使软件资源和硬件资源、底层资源和上层资源之间的耦合度降低，资源的利用方式也发生变化。以单个主机资源的利用方式为例，虚拟化前后，主机资源的利用方式发生的变化如图 3-2 及表 3-1 所示。

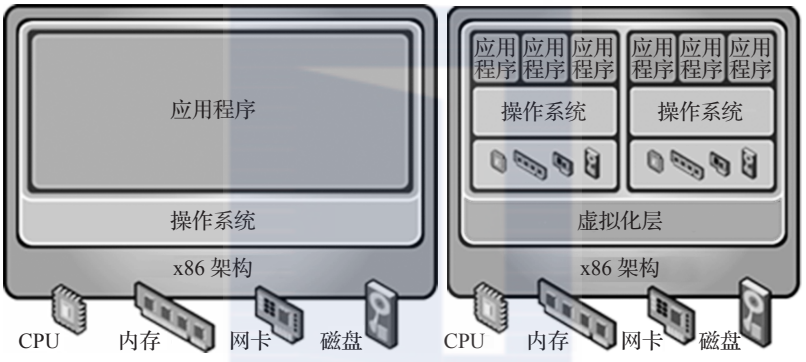


图 3-2　虚拟化前后的主机资源的利用方式

表 3-1　虚拟化前后对比

虚拟化前	虚拟化后
每台主机运行一个操作系统	一台主机可以运行多个操作系统
软硬件紧密结合，尤其是操作系统和硬件间的依赖度高	打破了操作系统和硬件的互相依赖，通过虚拟机封装技术，使操作系统和应用程序成为一个整体
在同一主机上运行多个应用程序通常会遭遇冲突	强大的安全和故障隔离
系统资源利用率低，尤其是 CPU 的利用率，一般保持在 10% 以下	系统资源利用率比较高，以 CPU 资源为例，一般保持在 70% 左右
硬件成本高昂而不够灵活	虚拟机可独立于硬件运行

主机虚拟化带来便利的同时也带来了新的挑战，主要体现在如何合理地分配一台物理主机的资源给多个虚拟机、如何确保多个虚拟机的运行不发生冲突、如何管理一个虚拟机和其拥有的各种资源、如何使虚拟化系统不受硬件平台的限制。这些与传统的资源利用的不同正是主机虚拟化技术的特性所在，同时也是服务器虚拟化（主机虚拟化在物理服务器上的实现）在实际环境中进行有效运用需要具备的特性，分别是：多实例、隔离性、封装性和高性能。

1）**多实例**　通过服务器虚拟化技术，实现了从“一个物理服务器一个操作系统实例”到“一个物理服务器多个操作系统实例”的转变。在一个物理服务器上虚拟出多台虚拟机，支持多个操作系统实例，这样就可以把服务器的物理资源进行逻辑整合，供多个虚拟机实例使用；可以根据实际需要把处理器、内存等硬件资源动态分配给不同的虚拟机实例；可以根据虚拟机实例的功能划分资源比重，对物理资源进行可控调配。与单服务器单操作系统的传统的服务器管理模式相比，多实例特性既可以利用有限的资源进行最大化的管理，又可以节省人力资源。

2）**隔离性**　虚拟机之间可以采用不同的操作系统，因此每个虚拟机之间是完全独立的。在一台虚拟机出现问题时，这种隔离机制可以保障其他虚拟机不会受其影响。其数据、文档、资料等集合不会丢失。也就是说，既方便系统管理员进行对每一台虚拟机进行管理，又能使虚拟机之间不受干扰，独立工作。而每个虚拟机内互访问，又可以通过所部署的网络进行通信，就如同在同一网域内每台计算机之间的数据通信一样。

3）**封装性**　采用了服务器虚拟化后，每台虚拟机的运行环境与硬件无关。通过虚拟化进行硬件资源分配，每台虚拟机就是一台独立的个体，可以实现计算机的所有操作。封装使不同硬件间的数据迁移、存储、整合等变得易于实现。在同一台物理服务器上运行的多个虚拟机会通过统一的逻辑资源管理接口来共用底层硬件资源，这样就可以将物理资源按照虚拟机不同的应用需求进行分配。将硬件封装为标准化的虚拟硬件设备，提供给虚拟机内的操作系统和应用程序使用，也可以保证虚拟机的兼容性。

4）**高性能**　服务器虚拟化是将服务器划分为不同的虚拟管理区域。其中的虚拟化抽象层通过虚拟机监视器或者虚拟化平台来实现，这会产生一定的开销，这些开销即为服务器虚拟化的性能损耗。服务器虚拟化的高性能是指虚拟机监视器的开销应控制在可承受的范围之内。

3.1.4　主机虚拟化的关键技术

在 x86 体系结构下，主机虚拟化的主要技术包括 CPU 虚拟化、内存虚拟化、I/O 虚拟化以及虚拟机的实时迁移。

1. CPU 虚拟化

CPU 虚拟化是 VMM 的核心部分，由于内存和 I/O 操作的指令都是敏感指令，因此对于内存虚拟化和 I/O 虚拟化的实现都是依赖于 CPU 虚拟化而完成的。所谓敏感指令，是指原本需要在操作系统最高特权级下执行的指令，这样的指令不能在虚拟机内直接执行，而是交由 VMM 处理，并将结果重新返回给虚拟机。CPU 虚拟化的目的就是让虚拟机中执行的敏感指令能够触发异常而陷入到 VMM 中，并通过 VMM 进行模拟执行。在 x86 体系结构当中，处理器拥有 4 个特权级，分别是 Ring 0、Ring 1、Ring 2、Ring 3。运行级别依次递减。其中位于用户态的应用程序运行在 Ring 3 特权级上，而位于内核态的代码需要对 CPU 的状态进行控制和改变，需要较高的特权级，所以其运行在 Ring 0 特权级上。

在 x86 体系结构中实现虚拟化时，由于虚拟化层需要对虚拟机进行管理和控制，如果

虚拟化层运行在 Ring 0 特权级上，则客户机操作系统只能够运行在低于 Ring 0 的特权级别。但由于在客户机操作系统中的某些特权指令，如中断处理和内存管理指令，如果没有运行在 Ring 0 特权级，则可能会出现语义冲突导致指令不能够正常执行。针对这样的问题，研究者们提出了两种解决方案，分别是全虚拟化（Full-virtualization）和半虚拟化（Para-virtualization），两者的区别如图 3-3 所示。

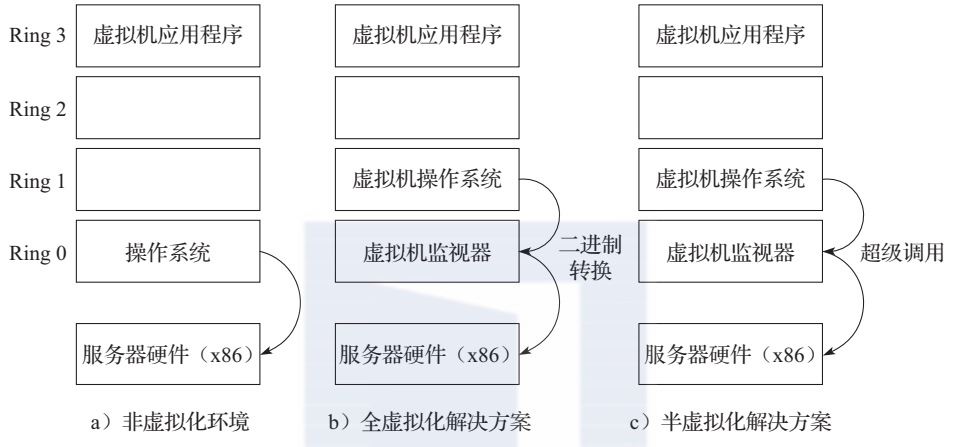


图 3-3　非虚拟化、全虚拟化、半虚拟化环境解决方案

全虚拟化采用了二进制动态代码翻译技术（Dynamic Binary Translation），这种方法在敏感指令之前插入陷入指令。当虚拟机需要执行这些敏感指令时，会先通过陷入指令陷入到虚拟机监视器中。虚拟机监视器将需要执行的敏感指令动态转换为具有相同功能的指令序列，再交由虚拟机执行。通过这样的方法，非敏感指令由虚拟机直接处理执行，而敏感指令则通过陷入虚拟机监视器进行指令转换后再执行。全虚拟化解决方案的优点是不需要对客户机操作系统进行修改，因此可以适配多种类型的操作系统，但缺点在于指令的动态转换需要一定的性能开销。

半虚拟化解决方案则通过对客户机操作系统进行修改来解决虚拟机敏感指令不能正常执行的问题。在半虚拟化中，被虚拟化平台托管的客户机操作系统通过修改其操作系统，将所有敏感指令替换成对底层虚拟化平台的超级调用。虚拟化平台也为这些敏感的特权指令提供了调用接口。形象地说，半虚拟化中的客户机操作系统被修改后，知道自己处在虚拟化环境中，从而主动配合虚拟机监视器，在需要的时候对虚拟化平台进行调用来完成相应指令的执行。半虚拟化解决方案的优点是其性能开销小于全虚拟化解决方案。但缺点在于，由于对客户机操作系统进行了修改，使得客户机操作系统能够感知到自己处在虚拟化环境中，不能够保证虚拟机监视器对虚拟机的透明性。而且半虚拟化对客户机操作系统版本有一定的限制，降低了客户机操作系统与虚拟化层之间的兼容性。

上述的全虚拟化与半虚拟化解决方案都属于通过软件方式来完成的虚拟化，但由于两者都存在一定的性能开销或者是增加了系统开发维护的复杂性。为了解决以上问题，产生

了通过硬件来辅助完成 CPU 虚拟化的方式，即硬件辅助虚拟化技术。当今两大主流的硬件厂商 Intel 公司和 AMD 公司分别推出了各自的硬件辅助虚拟化技术 Intel VT 和 AMD-V。以 Intel VT 技术为例，它在处理器中增加了一套虚拟机扩展指令集（Virtual Machine Extensions，VMX）用于虚拟化环境的相关操作。Intel VT 技术将处理器运行模式分为根模式（root）和非根模式（non-root）。对于虚拟化层而言，它运行在根模式下。对于客户机操作系统而言，它运行在非根模式下。由于两种运行模式都具备从 Ring 0 到 Ring 3 的四个特权级，所以很好地保留了全虚拟化和半虚拟化的优点，同时又弥补了两者的不足。

2. 内存虚拟化

物理机的内存是一段连续分配的地址空间，虚拟机监视器上层的各个虚拟机共享物理机的内存地址空间。由于虚拟机对于内存的访问是随机的，并且又需要保证虚拟机内部的内存地址是连续的，因此虚拟机监视器就需要合理映射虚拟机内部看到的内存地址到物理机上的真实内存地址。虚拟机监视器对物理机上的内存进行管理，并根据每个虚拟机对内存的需求对其进行合理分配。所以，从虚拟机中看到的“内存”不是真正意义上的物理内存，而是经过虚拟机监视器进行管理的“虚拟”物理内存。在内存虚拟化当中，存在着虚拟机逻辑内存、虚拟机看到的物理内存以及真实物理主机上的内存三种类型，这三种内存地址空间也分别称为虚拟机逻辑地址、虚拟机物理地址以及机器地址，如图 3-4 所示。

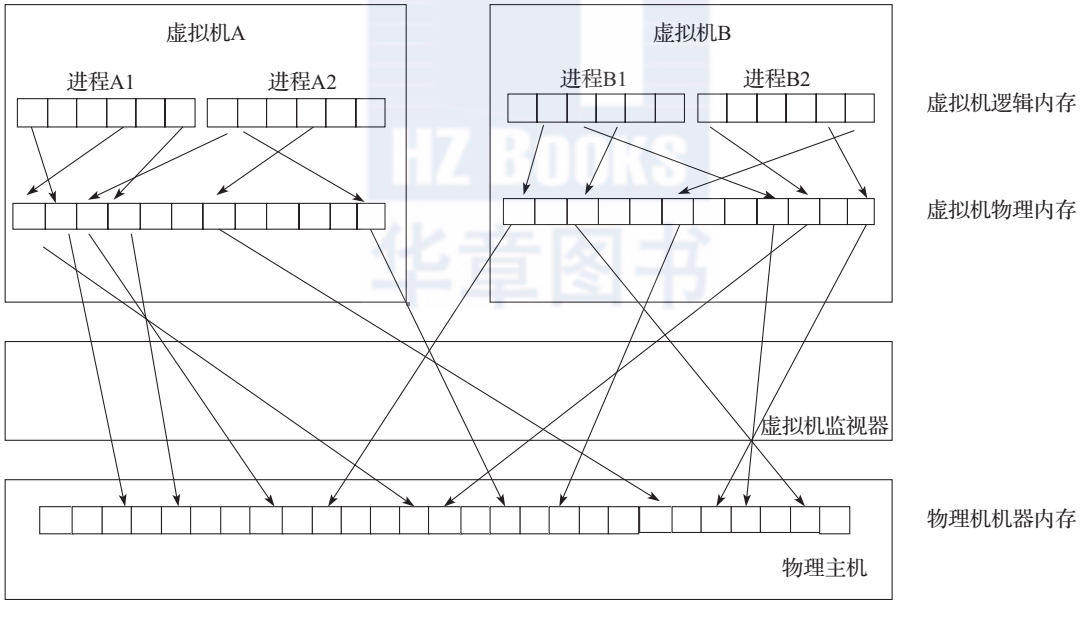


图 3-4　内存虚拟化

在内存虚拟化中，虚拟机逻辑地址与真实物理主机上的机器地址之间的映射是通过内存虚拟化中的内存管理单元来完成的。现阶段，内存虚拟化的实现方法主要有两种，分别是影子页表法和页表写入法，如图 3-5 所示。

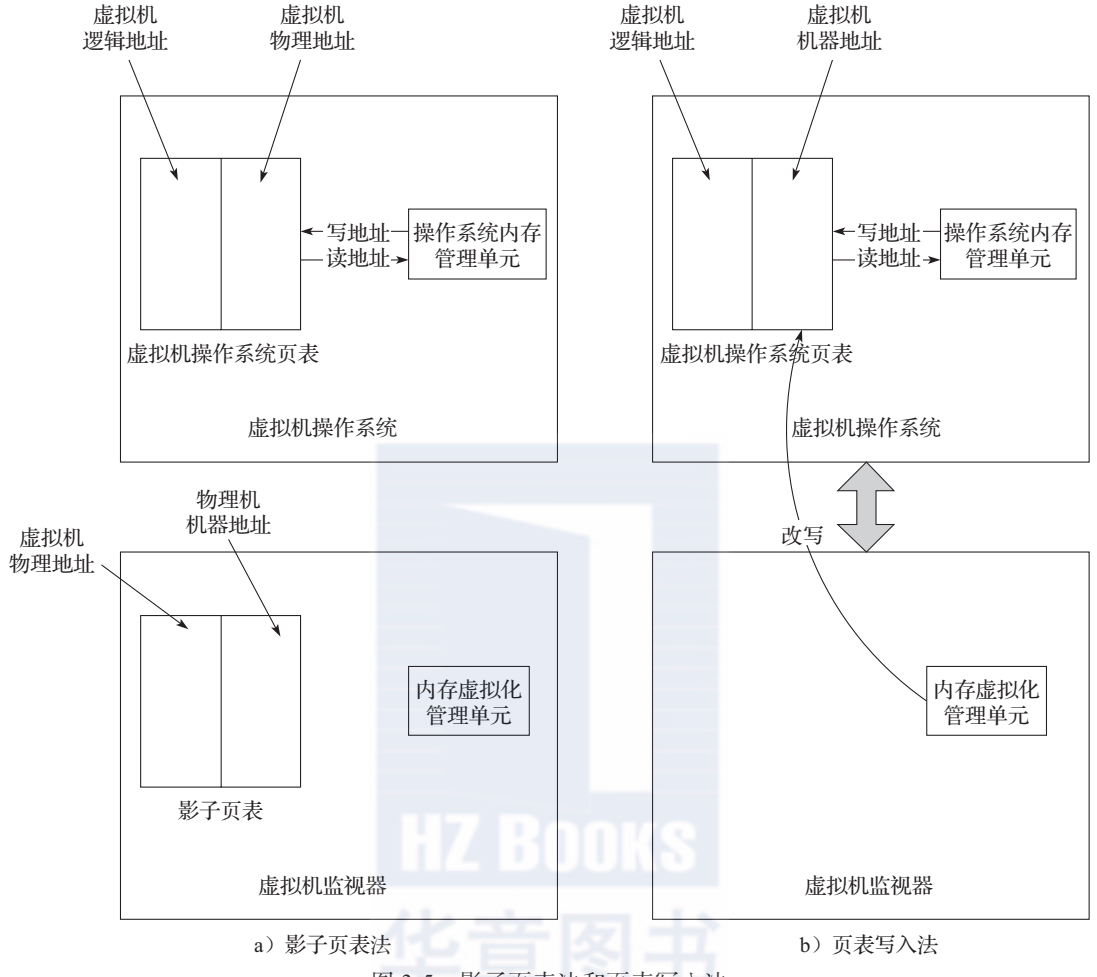


图 3-5　影子页表法和页表写入法

影子页表法是指在客户机操作系统中维护了虚拟机自己的页表。该页表中保存的是虚拟机逻辑地址到虚拟机物理地址的映射关系，而在虚拟机监视器当中，为每一台虚拟机也都维护了一套页表，该页表中保存的是当前客户机操作系统页表物理地址到真实物理机机器地址的映射关系。在客户机操作系统页表发生改变时，在虚拟机监视器中维护的页表也会随之更新，如同它的影子，所以被称作“影子页表”（Shadow Page Table）。

页表写入法是指每当客户机操作系统新创建一个页表时，虚拟机监视器也创建一套与当前页表相同的页表，这个页表中保存的是虚拟机物理地址与物理机机器地址之间的映射关系。在客户机操作系统对它自身所维护的这套页表进行写操作时，将会产生敏感指令并由虚拟机监视器剥夺客户机操作系统对其页表的写操作权限，然后由虚拟机监视器对客户机操作系统页表进行更新，使得客户机操作系统能直接从它自己的页表当中读取到真实物理主机的机器地址。

总的来说，影子页表法是一个从虚拟机逻辑地址到虚拟机物理地址再到物理机机器地址的二级映射关系，而页表写入法是一个从虚拟机逻辑地址到物理机机器地址的一级映射关系。但由于页表写入法在虚拟机监视器中需要对每一套虚拟机页表都维护一套页表，因此对系统性能的消耗比较大。

3. I/O 虚拟化

真实物理主机上的外设资源是有限的，为了使多台虚拟机能够复用这些外设资源，就需要虚拟机监视器通过 I/O 虚拟化来对这些资源进行有效地管理。虚拟机监视器通过截获客户机操作系统对外部设备的访问请求，再通过软件模拟的方式来模拟真实外设资源，从而满足多台虚拟机对外设的使用要求，如图 3-6 所示。

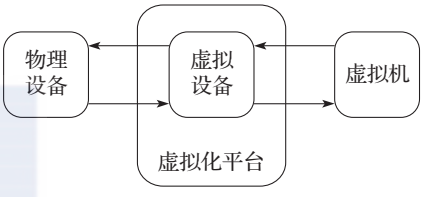


图 3-6　I/O 虚拟化

虚拟机监视器通过软件的方式模拟出来的虚拟设备可以有效地模拟物理设备的动作，并将虚拟机的设备操作转译给物理设备，同时将物理设备的运行结果返回给虚拟机。对于虚拟机而言，它只能够察觉到虚拟化平台提供的模拟设备，而不能直接对物理外设进行访问，所以这种方式所带来的好处就是，虚拟机不会依赖于底层物理设备的实现。

I/O 虚拟化的实现主要有全设备模拟、半虚拟化和直接 I/O 三种方式。

1）**全设备模拟**：该方法可以模拟一些主流的 I/O 设备，在软件实现中对一个设备的所有功能或者总线结构（例如设备枚举、识别、中断和 DMA）进行复制。该软件位于虚拟机监视器中，每当客户机操作系统执行 I/O 访问请求时，将会陷入到虚拟机监视器中，与 I/O 设备进行交互。这种方式的体系结构如图 3-7 所示。

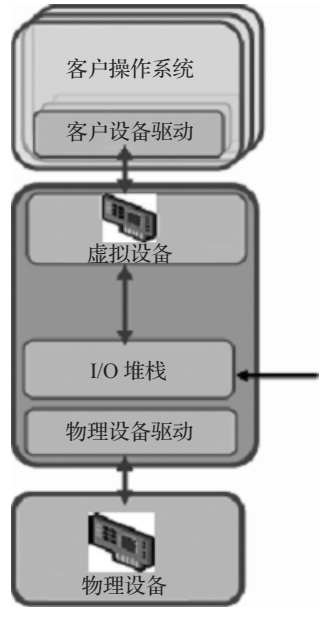


图 3-7　全设备模拟结构图

如图 3-7 所示，从上往下依次有客户设备驱动、虚拟设备、I/O 堆栈、物理设备驱动和物理设备。其中 I/O 堆栈主要用于提供虚拟机 I/O 地址到物理主机地址的地址转换，处理虚拟机之间的通信，复用从虚拟机到物理设备的 I/O 请求，提供企业级的 I/O 特性。

2）**半虚拟化**：半虚拟化中具有代表性的是 Xen 虚拟化解决方案中实现 I/O 虚拟化的方式。它由前端驱动和后端驱动两部分构成。前端驱动运行在 Domain U（其他虚拟机）中，后端驱动运行在 Domain 0（特权域）中，它们通过一块共享内存交互。前端驱动管理客户机操作系统的 I/O 请求，后端驱动负责管理真实的 I/O 设备并复用不同虚拟机的 I/O 数据。尽管与全虚拟化设备模拟相比，半 I/O 虚拟化的方法可以获得更好的设备性能，但其 I/O 虚拟化的运行机制也会带来更高的 CPU 开销。

3）**直接 I/O 虚拟化**：这是指让虚拟机直接访问设备硬件，它能获得近乎宿主机访问设备硬件的性能，并且 CPU 开销不高。目前，直接 I/O 虚拟化主要集中在大型主机的网络虚拟化方面，通过直接 I/O 虚拟化来为虚拟机分配独立的物理网络接口设备，以提高其网络交互能力。但是直接 I/O 虚拟化成本要求高，在商业大规模推广方面仍面临许多挑战。

4. 虚拟机实时迁移

虚拟机实时迁移是指在保证虚拟机上服务正常运行的同时，使虚拟机在不同的物理主机上进行迁移。整个迁移过程需要保证虚拟机是可用的，并且整个迁移过程是快速且平滑的，迁移过程对用户透明，即用户几乎不会察觉到在虚拟机使用过程中产生的任何差异。

整个实时迁移的过程需要虚拟机监视器的配合来完成虚拟机从源物理主机到目标物理主机上内存和其他数据信息的拷贝。在实时迁移开始时，虚拟机的内存页面和数据信息将不断从源物理主机拷贝到目标物理主机，直到最后一部分位于源物理主机中的虚拟机内存和数据被拷贝进目标物理主机后，目标物理主机上的虚拟机将开始运行，整个迁移过程不会影响源物理主机中虚拟机的工作，如图 3-8 所示。

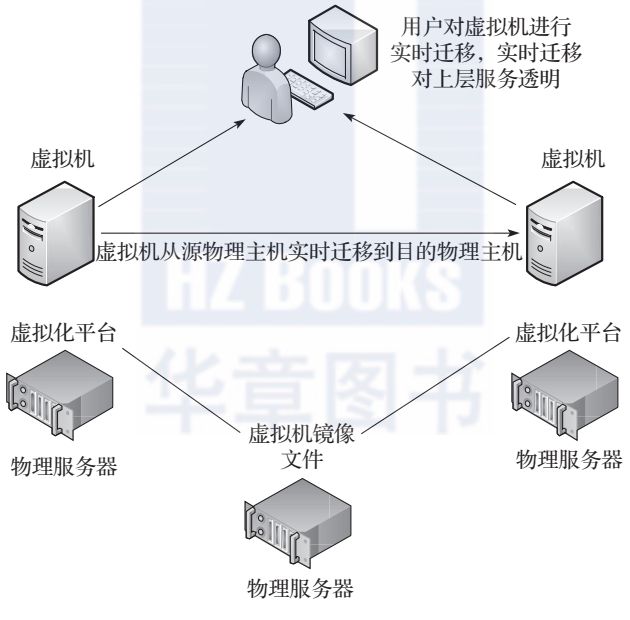


图 3-8　虚拟机实时迁移

利用虚拟机实时迁移技术，可以实现服务器的在线维护、在线升级和动态负载均衡，因此在云计算领域有着广阔的应用前景。

3.1.5　主机虚拟化的优势

虚拟化是基础设施整合中的重要技术。有了虚拟化技术，一些基础设施（如服务器、网络、存储等）可以被资源池化，并且经过抽象后提供给上层的计算单元，使上层的计算单元

以为自己运行在独立的内存空间中，享有独立的网络、存储资源用于服务。同时，虚拟化技术的分区特性使得各种硬件资源被合理、高效地划分给不同的虚拟机；隔离特性使得多个不同虚拟机在同一主机上互不影响计算的效果；封装特性使得虚拟机更方便地迁移和备份；独立于硬件的特性使得虚拟机的配置更加方便。

由图 3-9 可以看出，目前虚拟化的市场还处于起步阶段，是 IT 行业新兴发展方向之一。图中，虚拟化的市场发展被分为了四个阶段，即降低成本、提高使用率、提高灵活性与更好地使 IT 配合业务。

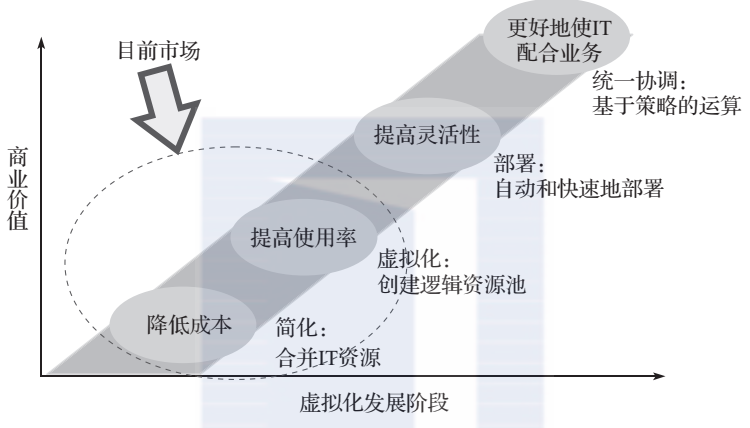


图 3-9　虚拟化的市场发展图

总而言之，主机虚拟化的优势主要体现在两方面：增加硬件的利用率以及提高生产率。

（1）增加硬件的利用率

以 CPU 的利用率为例，如图 3-10 所示，在宿主机进行虚拟化之前，主机上 CPU 的利用率一般在 10% 以下，偶尔会出现 CPU 的利用高峰，但是也没有超过 30%；在宿主机进行虚拟化之后，宿主机上的 4 个 CPU 的利用率均维持在 55% ~ 80%，最低利用率也没有小于 50%。可见，相较于传统主机而言，主机虚拟化技术极大提高了 CPU 的利用率。

（2）提高生产率

主机虚拟化在提高生产率方面的作用可通过以下几个例子来说明：

【例 3.1】 部署一个新的服务器。若采用传统的服务器架构，需要 3 ~ 10 天进行硬件采购，1 ~ 4 小时进行系统部署；采用虚拟化架构后，只需要 5 ~ 10 分钟的时间即可采用模板和部署向导初步完成一个系统的部署。

【例 3.2】 硬件的维护。若采用传统的服务器架构，需要 1 ~ 3 小时进行窗口维护，数天乃至数周进行变更管理准备；采用虚拟化架构后，可以通过虚拟化技术实现零宕机的硬件升级。

【例 3.3】 迁移集成服务器。采用传统的服务器架构，需要数天甚至数周进行变更管理准备，有时候，迁移能否成功还会受到其他环境因素的影响；采用虚拟化架构后，采用 P2V

（Physical To Virtual）技术，只需要一个小时左右便可以实现服务器的迁移。

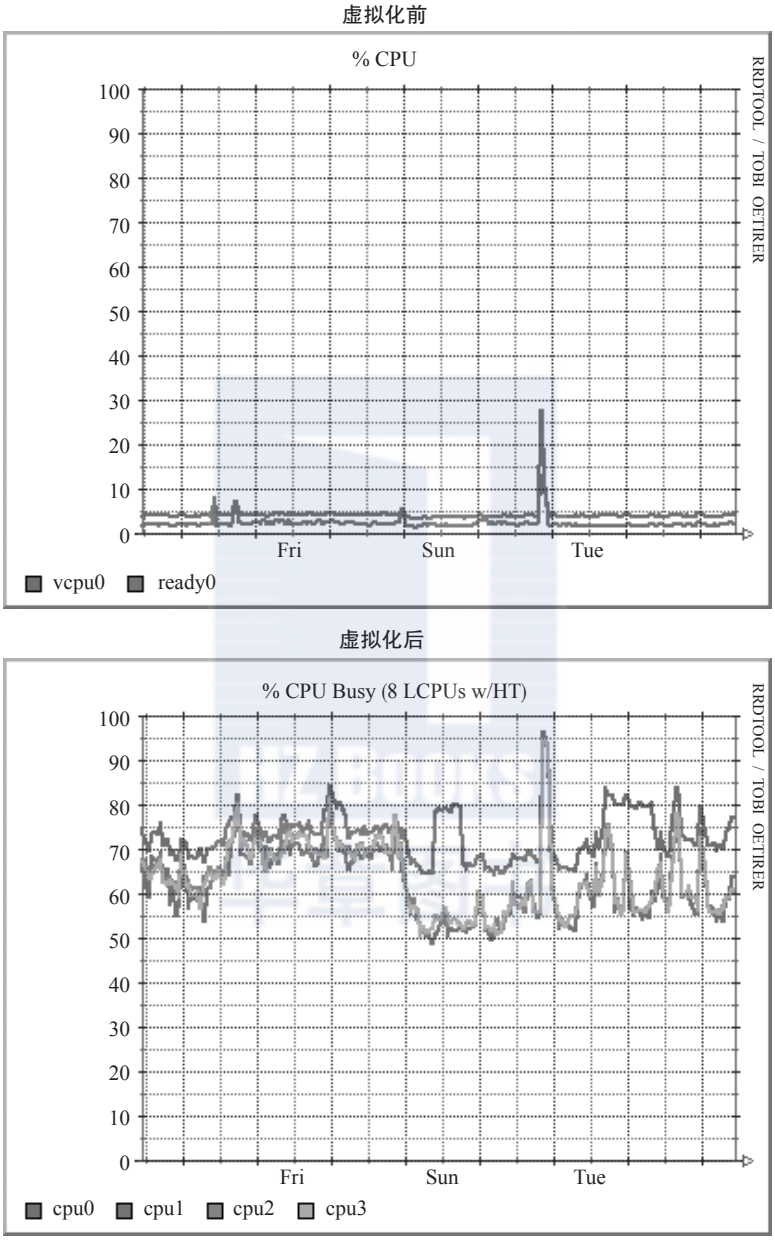


图 3-10　CPU 利用率对比图

【例 3.4】 移动服务器优化负载。采用传统的服务器架构，迁移过程大约需要 4 ~ 6 小时，所有的维护窗口中的服务全部中断，并且需要数天甚至数周的变更准备时间；采用虚拟

化架构后，利用虚拟机实时迁移技术，可以在 2 ~ 5 分钟内实现无服务中断的迁移。

服务器虚拟化是虚拟化技术中出现时间最早的技术分支，也是虚拟化技术中最为成熟的领域。服务器虚拟化是将虚拟化技术应用于服务器上，将一个服务器虚拟化成若干个服务器使用。服务器虚拟化技术的多实例、强隔离、高性能、封装好等特性保证了它能有效地运用在实际的环境中，独特的优势使其受到很多大型企业的青睐。服务器虚拟化的主要优点可总结如下：

1）降低运营成本：服务器虚拟化厂商都提供了功能强大的虚拟化环境管理工具，可降低人工干预的频率，降低 IT 基础设施的运营成本。

2）提高应用兼容性：服务器虚拟化技术所具有的封装和隔离特性使管理员仅需构建一个应用版本，即可将其发布到被虚拟化封装后的不同类型的平台上。

3）加速应用部署：采用服务器虚拟化后，部署一个应用通常只需要几分钟至十几分钟的时间，且不需要人工干预，极大地缩短了部署时间，降低了部署成本。

4）提高服务可用性：服务器虚拟化技术可以方便地对运行中的服务器进行快照并备份成虚拟机镜像文件，支持虚拟机的动态迁移和恢复，提高了服务的可用性。

5）提升资源利用率：服务器虚拟化技术将原有的多台服务器整合到一台服务器上，提高了物理服务器的利用率。

6）动态调度资源：服务器虚拟化支持实时迁移，方便资源的整合和动态调度。同时，数据中心统一的资源池，使数据中心管理员可以灵活地调整分配资源。

7）降低能源消耗：服务器虚拟化可以将原来运行在各个服务器上的应用整合到少数几台服务器上，通过减少运行的服务器的数量，降低了能源消耗。

这些优势加速了服务器虚拟化技术的普及，使其应用领域越来越广泛。服务器虚拟化技术开启了基础硬件利用方式的全新时代，尤其为构建云计算基础架构奠定了重要的技术基础。在当今云计算盛行的 IT 时代，服务器虚拟化技术必将大行其道。

3.1.6　主机虚拟化上机实践

1. 单主机虚拟化上机实践

（1）实验目的

学习主机虚拟化环境的搭建过程和利用虚拟化管理软件对虚拟机进行可视化管理。

（2）实验环境

① Linux 操作系统（以 Ubuntu Desktop 操作系统为例）。

②可连通互联网的主机。

③ KVM、QEMU、虚拟机操作系统安装文件等。

（3）实验步骤

1）配置环境：配置环境的步骤如下。

①查看 CPU 是否支持硬件虚拟化，因为 KVM 需要硬件虚拟化功能支持。

```
Intel CPU :
grep vmx /proc/cpuinfo
AMD CPU :
grep svm /proc/cpuinfo
```

如果查询的信息中有“vmx”或“svm”字段，说明 CPU 可支持硬件虚拟化。

②配置安装源：Linux 默认安装源下载及安装速度较慢，因此需要修改软件安装源为适合本地环境的安装源以提高速度。修改 /etc/apt/sources.list 文件，此处将安装源改为“ mirrors.ustc.edu.cn”（中国科技大学）。

```
$sudo vi /etc/apt/sources.list
//在 vi 编辑环境中，将软件源替换为“mirrors.ustc.edu.cn”，在命令模式下使用以下命令行：
:1,$s/cn.archive.ubuntu.com/mirrors.ustc.edu.cn/g     //根据操作系统版本不同
                                                      //此处安装源为“cn.archive.
                                                      //ubuntu.com”，不同 Ubuntu
                                                      //版本可能有所不同
:1,$s/security.ubuntu.com/mirrors.ustc.edu.cn/g       //根据操作系统版本不同
                                                      //此处安装源为“security.
                                                      //ubuntu.com”，不同 Ubuntu
                                                      //版本可能有所不同
:wq                                                   //保存退出 vi 环境

$sudo apt-get update
$sudo apt-get upgrade
```

③安装 KVM、QEMU 及配套软件。

```
$sudo apt-get install kvm qemu libvirt-bin virtinst virt-manager virt-viewer
xtightvncviewer

//查看 KVM 是否安装成功

# virsh -c qemu:/// system list
 Id    Name                           State
----------------------------------------------------
//如果显示以上信息，则说明 KVM、QEMU 安装成功!
```

④使用命令行建立虚拟机，安装操作系统，使用虚拟机。

```
# qemu-img create -f qcow2 ubuntu.img 10G

# qemu-system-x86_64 -hda ubuntu.img  -cdrom <虚拟机操作系统安装文件> -boot d -m 1024

# qemu-system-x86_64 -hda ubuntu.img  -m 1024
//启动完成后，系统会提示如下信息：
VNC server running on‘127.0.0.1:5901’  //不同环境下，端口号会有所不同

//在 Ubuntu 桌面上新开一个 Terminal，在命令行输入：
#vncviewer :5901
```

之后，就可以在新窗口中查看和操作普通操作系统一样操作虚拟机，显示效果如图 3-11 所示：

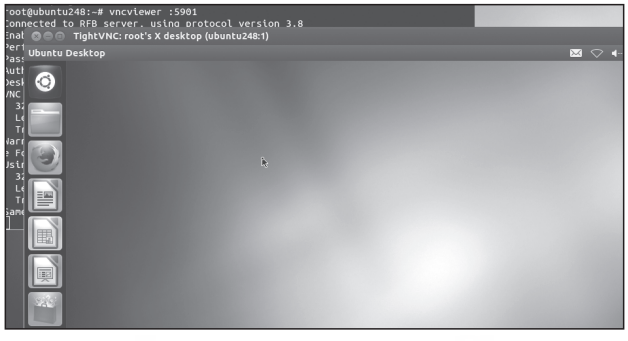


图 3-11　Ubuntu 虚拟机桌面

⑤通过 virt-manager 管理虚拟机。在用户界面上，打开 Terminal 终端，输入以下命令：

```
#virt-manager
```

系统弹出如图 3-12 所示的窗口：

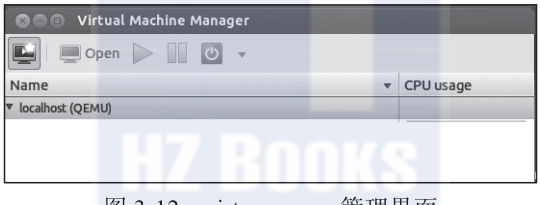


图 3-12　virt-manager 管理界面

后续的操作都在这个环境下进行。

a）将已有的虚拟机镜像文件加入到 virt-manager 中。点击界面上侧工具栏第一个图标，弹出“新增虚拟机”窗口，在“安装选项”中选择“导入有磁盘镜像”，之后选择第④步创建的虚拟机镜像，按照提示进行操作，完成虚拟机镜像的导入操作。

b）在 virt-manager 中新建虚拟机。在 virt-manager 中，点击界面上侧工具栏第一个图标，弹出“新增虚拟机”窗口，在“安装选项”中选择“本地安装媒介”，之后选择虚拟机操作系统的安装镜像所在位置，之后按照提示进行操作，完成虚拟机操作系统的导入操作。如图 3-13 所示。

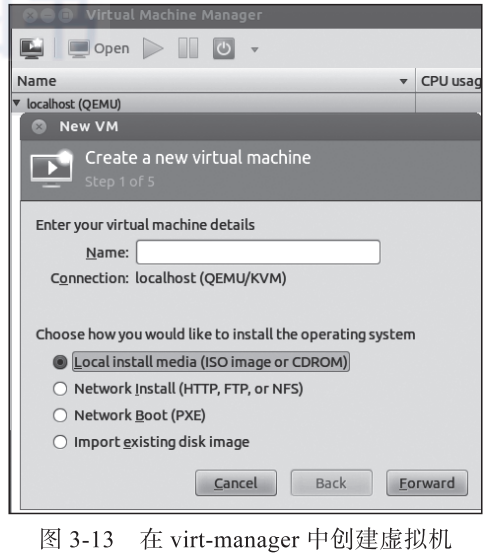


图 3-13　在 virt-manager 中创建虚拟机

c）在 virt-manager 中拷贝现有虚拟机。在 virt-manager 中现有的虚拟机实例上单击右键，在右键菜单上选择“Clone”，如图 3-14 所示。

之后，按照系统提示完成虚拟机克隆操作，就能够以现有虚拟机为模板创建新的虚拟机。如图 3-15 所示。

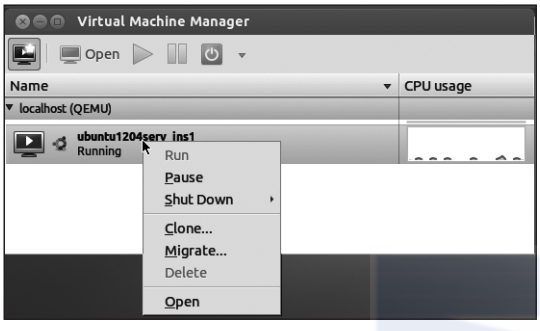


图 3-14　在 virt-manager 中拷贝现有虚拟机

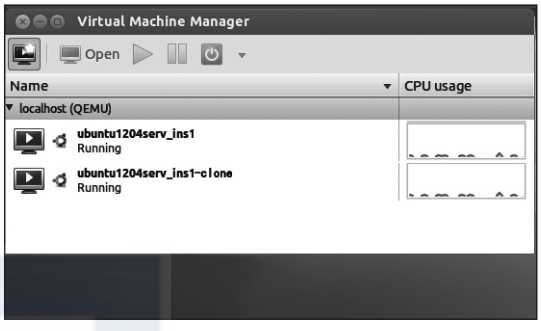


图 3-15　拷贝虚拟机完成

2. 阿里云虚拟化上机实践

（1）实验目的

使用阿里云进行虚拟机的创建与管理。

（2）实验环境

阿里云平台

（3）实验步骤

步骤 1：配置选型

阿里云推荐以下几种配置组合方案，能够满足大部分用户的需求。

- **入门型**：1vCPU+1GB+1MB，适用于访问量较小的个人网站。
- **进阶型**：1vCPU+2GB+1MB，适用于流量适中的网站、简单开发环境、代码存储库等。
- **通用型**：2vCPU+4GB+1MB，能满足 90% 云计算用户，适用于企业运营活动、并行计算应用、普通数据处理。
- **理想型**：4vCPU+8GB+1MB，用于对计算性能要求较高的业务，如企业运营活动、批量处理、分布式分析、APP 应用等。

注意　这些推荐配置只是作为开始使用云服务器 ECS 的参考。阿里云提供了灵活、可编辑的配置修改方式。如果在使用过程中，发现配置过高或过低，可以随时修改配置。

步骤 2：创建 Linux 实例

这里只介绍新购实例。如果已有镜像，可以使用自定义镜像创建实例。新购实例的操作步骤如下：

①登录云服务器管理控制台。如果尚未注册，单击免费注册。

②定位到云服务器 ECS →实例。单击“创建实例”。如图 3-16 所示。

图 3-16　阿里云中创建 Linux 实例

③选择付费方式，有包年包月或按量付费。关于两种付费方式的区别，请参见计费模式。如果选择“按量付费”，请确保账户余额至少有 100 元。如无余额，请进入充值页面充值后再开通。注意：对于按量付费的实例，即使停止实例，也会继续收费。如果不再需要该按量付费的实例，请及时释放实例。如图 3-17 所示。

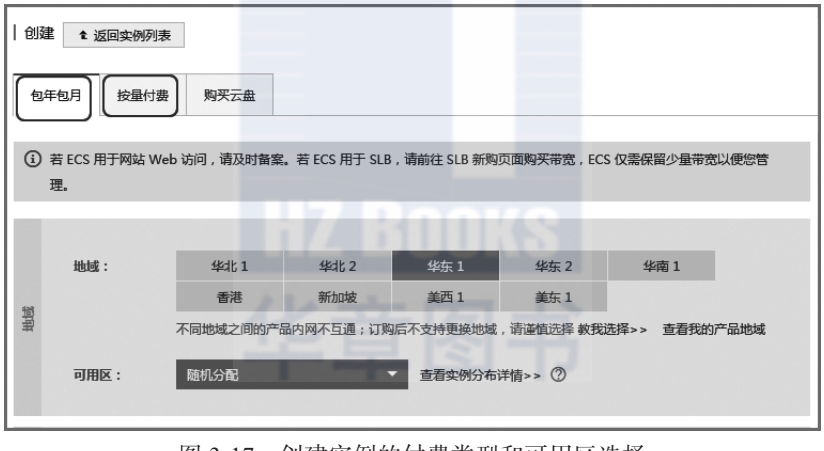


图 3-17　创建实例的付费类型和可用区选择

④选择地域。所谓地域，是指实例所在的地理位置。可以根据用户所在的地理位置选择地域。与用户距离越近，延迟相对越少，下载速度相对越快。例如，如果用户都分布在杭州地区，则可以选择华东 1。

在这里需要注意：

- 不同地域间的内网不能互通。
- 实例创建完成后，不支持更换地域。
- 不同地域提供的可用区数量、实例系列、存储类型、实例价格等也会有所差异，请根据业务需求进行选择。

⑤选择网络类型。目前，大部分地域提供两种网络类型。网络类型一旦选择后，不能更

改，因此请慎重选择。

如果想使用经典网络，选择“经典网络”。然后点击“选择安全组”。如图 3-18 所示。

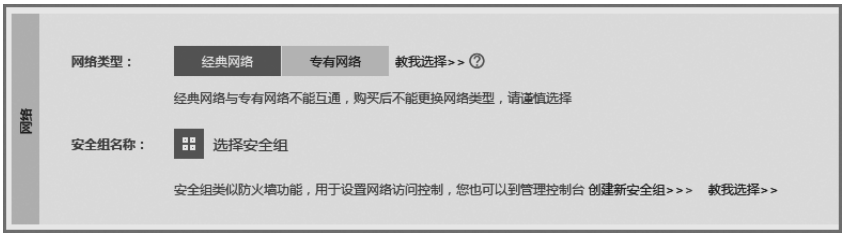


图 3-18　创建实例的网络和安全组选择

如果需要使用逻辑隔离的专有网络，选择“专有网络”。如图 3-19 所示。

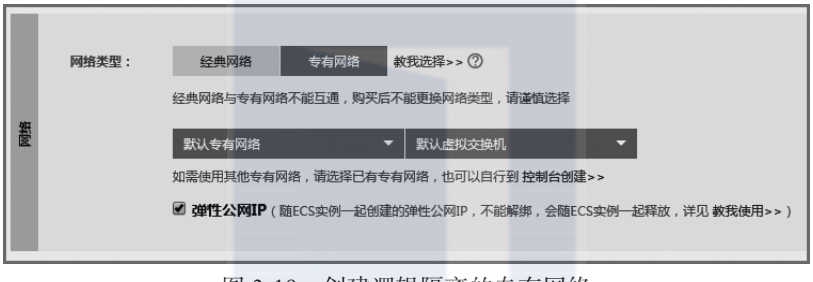


图 3-19　创建逻辑隔离的专有网络

⑥选择实例，包括实例系列、I/O 优化实例和实例规格。关于实例规格的详细介绍，请参考实例规格族。其中，实例系列 II 是实例系统 I 的升级版，能提供更高的性能，推荐使用。推荐选择 I/O 优化，挂载后可以获得 SSD 云盘的全部性能。如图 3-20 所示。

图 3-20　创建实例的规模和系列

⑦选择网络带宽。如果选择 0MB，则不分配外网 IP，该实例将无法访问公网。如果选择了按量付费，同时选择 0MB 固定带宽，则同样不分配外网 IP，而且不支持 0MB 带宽升级，因此请谨慎选择。

按固定带宽付费如图 3-21 所示。

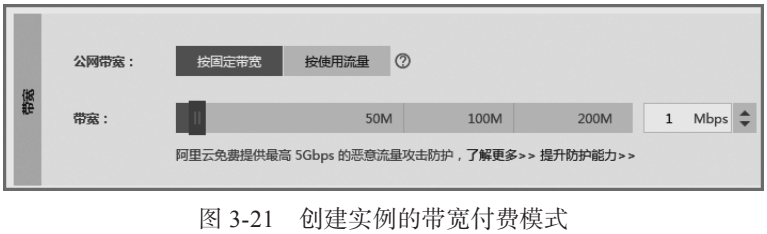


图 3-21　创建实例的带宽付费模式

按使用流量付费如图 3-22 所示。

图 3-22　创建实例的带宽峰值设定

⑧选择镜像。可以选择公共镜像，包含正版操作系统，购买完成后再手动安装部署软件；也可以选择镜像市场提供的镜像，其中集成了运行环境和各类软件。公共镜像中的操作系统 License 无须额外费用（海外地域除外）。如图 3-23 所示。

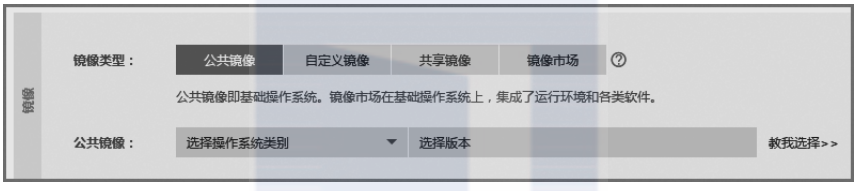


图 3-23　创建实例的操作系统来源选择

⑨选择操作系统。选择操作系统的时候，应注意以下几个问题：

- 最流行的服务器端操作系统，强大的安全性和稳定性。
- 免费且开源，轻松建立和编译源代码。
- 通过 SSH 方式远程访问您的云服务器。
- 一般用于高性能 Web 等服务器应用，支持常见的 PHP/Python 等编程语言，支持 MySQL 等数据库（需自行安装）。
- 推荐使用 CentOS。

⑩选择存储，如图 3-24 所示。系统盘为必选，用于安装操作系统。可以根据业务需求，选择添加最多 4 块数据盘，每块数据盘最大 32TB。用户还可以选择用快照创建磁盘，把快照的数据直接复制到磁盘中。

图 3-24　创建实例的存储选择

⑪设置实例的登录密码和实例名称，如图 3-25 所示。请务必牢记密码。也可以在创建完成后再设置密码。

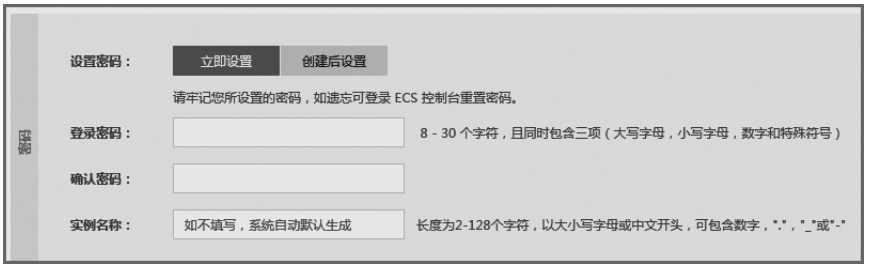


图 3-25　创建实例的系统密码

⑫设置购买的时长和数量。

⑬单击页面右侧价格下面的“立即购买”。

⑭确认订单并付款。

至此，实例创建完成，你会收到短信和邮件通知，告知实例名称、公网 IP 地址、内网 IP 地址等信息。之后，就可以使用这些信息登录和管理实例。

步骤 3：登录 Linux 实例

根据使用的本地操作系统，可以从 Windows、Linux、Mac OS X 等操作系统登录 Linux 实例。

步骤 4：格式化和挂载数据盘

如果在创建实例时选择了数据盘，那么在登录实例后，系统需要先格式化数据盘，然后挂载数据盘。另外，还可以根据业务需要，对数据盘进行多分区配置。建议使用系统自带的工具进行分区操作。

注意：云服务器 ECS 仅支持对数据盘进行二次分区，而不支持对系统盘进行二次分区（不管是 Windows 还是 Linux 系统）。如果强行使用第三方工具对系统盘进行二次分区操作，可能引发未知风险，如系统崩溃、数据丢失等。

本操作适用于非 I/O 优化 +SSD 云盘 Linux（Redhat、CentOS、Debian、Ubuntu）实例。

①使用管理终端或远程连接工具，输入用户名 root 和密码登录到实例。

②运行 fdisk -l 命令查看数据盘。注意：在没有分区和格式化数据盘之前，使用 df -h 命令是无法看到数据盘的。在下面的示例中，有一个 5GB 的数据盘需要挂载。如图 3-26 所示。

③如果执行了 fdisk -l 命令后，没有发现 /dev/xvdb，则表示你的实例没有数据盘，因此无需挂载。

④运行 fdisk/dev/xvdb，对数据盘进行分区。根据提示，依次输入 n、p、1，两次按回车，wq，分区就开始了。如图 3-27 所示。

⑤运行 fdisk -l 命令，查看新的分区，可以看到新分区 xvdb1 已经创建好。如下面示例中的 /dev/xvdb1。如图 3-28 所示。

```
[root@AY11092611360929c66a0 ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda1              62G  467M   62G   1% /
tmpfs                 753M     0  753M   0% /dev/shm
[root@AY11092611360929c66a0 ~]# fdisk -l

Disk /dev/hda: 68.7 GB, 68719476736 bytes
255 heads, 63 sectors/track, 8354 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1   *           1        8094    65015023+  83  Linux
/dev/hda2            8095        8351     2064352+  82  Linux swap / Solaris

Disk /dev/xvdb: 96.6 GB, 96636764160 bytes
255 heads, 63 sectors/track, 11748 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

图 3-26　实例的磁盘情况

```
[root@AY11092611360929c66a0 ~]# fdisk /dev/xvdb
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.


The number of cylinders for this disk is set to 11748.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-11748, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-11748, default 11748):
Using default value 11748

Command (m for help): wq
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

图 3-27　对实例的数据盘进行分区操作

```
[root@AY11092611360929c66a0 ~]# fdisk -l

Disk /dev/hda: 68.7 GB, 68719476736 bytes
255 heads, 63 sectors/track, 8354 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1   *           1        8094    65015023+  83  Linux
/dev/hda2            8095        8351     2064352+  82  Linux swap / Solaris

Disk /dev/xvdb: 96.6 GB, 96636764160 bytes
255 heads, 63 sectors/track, 11748 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

    Device Boot      Start         End      Blocks   Id  System
/dev/xvdb1               1       11748    94365778+  83  Linux
```

图 3-28　查看创建好的分区

⑥运行 mkfs.ext3 /dev/xvdb1，对新分区进行格式化。格式化所需时间取决于数据盘大小。也可自主决定选用其他文件格式，如 ext4 等。如图 3-29 所示。

```
[root@AY110926113609 29c66a0 ~]# mkfs.ext3 /dev/xvdb1
mke2fs 1.39 (29-May-2006)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
11796480 inodes, 23591444 blocks
1179572 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
720 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 24 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

图 3-29　格式化新分区

⑦运行 echo /dev/xvdb1 /mnt ext3 defaults 0 0>>/etc/fstab 写入新分区信息。完成后，可以使用 cat /etc/fstab 命令查看写入的信息，如图 3-30 所示。

```
[root@AY110926113609 29c66a0 ~]# cat /etc/fstab
LABEL=/                 /                       xfs     defaults        1 1
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
LABEL=SWAP              swap                    swap    defaults        0 0
/dev/xvdb1              /mnt                    ext3    defaults        0 0
```

图 3-30　写入新分区信息

注意　Ubuntu 12.04 不支持 barrier，所以对该系统正确的命令是：echo /dev/xvdb1 /mnt ext3 defaults 0 0>>/etc/fstab。

如果需要把数据盘单独挂载到某个文件夹，比如单独用来存放网页，可以修改以上命令中的 /mnt 部分。

运行 mount /dev/xvdb1 /mnt 挂载新分区，然后执行 df -h 查看分区。如果出现数据盘信息，说明挂载成功，可以使用新分区了。

```
# mount /dev/xvdb1 /mnt
# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       40G  1.5G   36G   4% /
tmpfs           498M     0  498M   0% /dev/shm
/dev/xvdb1      5.0G  139M  4.6G   3% /mnt
```

3.2　主机虚拟化的主要安全威胁

主机虚拟化提供给用户使用的不是物理意义上的服务器，而是虚拟服务层中的一个操作系统实例。通过主机虚拟化，管理员不仅可以在物理服务器上部署多个虚拟服务器，并为其安装操作系统，还可以根据不同业务需求定制虚拟机的内存、CPU、存储容量等。这样不但提高了服务器的利用率，还降低了硬件成本，缩短了服务器的配置时间，并能保持业务的连续性等。与物理服务器一样，虚拟服务器上同样存在安全风险。因此，在部署、使用、分配、管理虚拟服务器时必须加强安全风险防范意识。

1. 虚拟机之间的安全威胁

传统网络是从客户端发起访问到服务器的纵向流量结构，纵向流量必然要经过外置的硬件安全防护机制，如防火墙等。即使在虚拟化后，传统的安全防护设备也可以实现对纵向流量的安全防护和业务隔离。与传统的安全防护不同，在虚拟化环境下可能存在多租户服务模型。多个虚拟机可在同一台物理主机上交互数据从而产生横向流量，这些数据不经过外置的硬件安全防护机制，管理员无法对这些横向流量进行有效监控或者实施高级的安全策略，例如，入侵防御规则或防火墙规则，如图 3-31 所示。在服务器的虚拟化过程中，一些虚拟化厂商通过在服务器 Hypervisor 层集成虚拟交换机的特性。也可以实现一些基本的访问允许或拒绝规则，但是很难集成更高级的安全检测防护引擎来检测虚拟机之间的流量漏洞攻击行为。当多个虚拟机共享硬件资源，且虚拟机横向流量又不被外部感知的情况下，一台虚拟机受到攻击后，宿主机乃至整个网络都会遭受严重威胁。

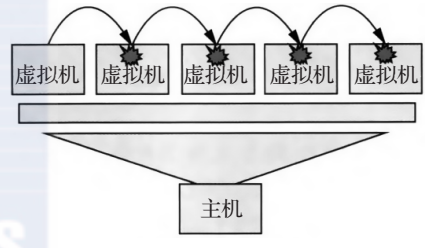


图 3-31　虚拟机之间的攻击面

2. 虚拟机与宿主机之间的安全威胁

宿主机是虚拟机的物理基础，虚拟机存在于宿主机中，且与宿主机共享硬件。宿主机的运行是虚拟机运行的前提与基础，因此宿主机的安全至关重要。一旦宿主机被控制，利用宿主机的高特权极，攻击者可以对同一宿主机上的虚拟机进行攻击（如图 3-32 所示）。攻击者甚至可以通过提升重要的访问权限，以使其可以访问宿主机的本地网络和相邻系统。

3. 虚拟机控制中心的安全威胁

通过虚拟机控制中心，管理员可以管理部署在不同位置上的虚拟机，并应用自动化策略执行和快速部署等功能使日常工作变得简单、快捷、高效，从而使数据中心的虚拟化环境更加易于管理，并能大大降低相关成本。因为虚拟机控制中心对其管理的所有虚拟机拥有高级别访问控制权限，所以确保虚拟机控制中心的安全非常重要。否则，一旦虚拟机控制中心被入侵，那么所有虚拟机乃至数据中心都会面临极大威胁。

4. 虚拟机蔓延（泛滥）及管理疏漏的隐患

导致虚拟机蔓延（泛滥）的因素有很多，如僵尸虚拟机。这些虚拟机在完成工作后被丢弃，不会被关闭，也不会被删除，但它们继续消耗资源。由于长期处于无人看管状态，虚拟

机一旦形成蔓延趋势，就会造成巨大浪费。同时，口令的时限、漏洞的出现等问题都会成为虚拟机管理的安全隐患。

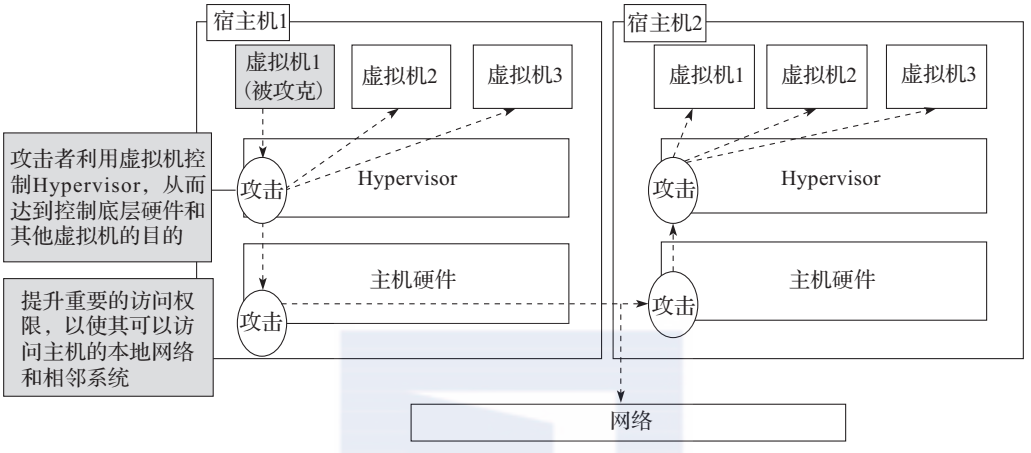


图 3-32　虚拟机与宿主机之间的安全威胁

在虚拟机出现后，安全管理上会变得更为繁琐。虚拟机口令、宿主机口令、虚拟机控制中心口令、虚拟机漏洞、宿主机漏洞等每个细节都不容忽视。同样，在部署虚拟机时使用连续 IP 地址，主机、虚拟机管理口令相同等这些看似方便的管理方式，会在未来带来较大麻烦。总之，虚拟机如管理不善，很可能会演变为整个数据中心的灾难。

虚拟机是主机虚拟化的基础运算单元，一旦虚拟机被劫持或攻陷，造成的损失是无法估量的。通常对虚拟机攻击方式是以下一种或多种方式的结合：

- **社会工程**：攻击者可通过各种社交渠道获得有关目标的结构、使用情况、安全防范措施等有用信息从而提高攻击成功率。
- **口令破解**：攻击者可通过获取口令文件，然后运用口令破解工具获得口令，也可通过猜测或窃听等方式获取口令。
- **地址欺骗**：攻击者可通过伪装成被信任的 IP 地址等方式来骗取目标的信任。
- **连接盗用**：在合法的通信连接建立后，攻击者可通过阻塞或摧毁通信的一方来接管已经过认证建立起来的连接，从而假冒被接管方与对方通信。
- **网络窃听**：网络的开放性使攻击者可通过直接或间接窃听获取所需信息。
- **数据篡改**：攻击者可通过截获并修改数据或重放数据等方式破坏数据的完整性。
- **恶意扫描**：攻击者可编制或使用现有扫描工具发现目标的漏洞，进而发起攻击。
- **破坏基础设施**：攻击者可通过破坏 DNS 或路由信息等基础设施，使目标陷于孤立。
- **数据驱动攻击**：攻击者可通过施放病毒、特洛伊木马、数据炸弹等方式破坏或遥控目标。
- **服务拒绝**：攻击者可直接发动攻击，也可通过控制其他主机发起攻击，使目标瘫痪，如发送大量的数据洪流阻塞目标。

本节将重点分析目前主流的主机虚拟化面临的安全威胁，包括虚拟机信息窃取及篡改、虚拟机逃逸、Rootkit 攻击、拒绝服务攻击和侧信道攻击等。

3.2.1　虚拟机信息窃取和篡改

虚拟机信息主要通过镜像文件及快照来保存的。虚拟机镜像无论在静止还是运行状态都有被窃取或篡改的脆弱漏洞，另外，包含重要敏感信息的虚拟机镜像和快照以文件形式存在，能够轻易通过网络传输到其他位置。

建立客户机镜像文件及快照不会影响客户机的脆弱性。然而，对于镜像和快照来说，最大的安全性问题就是它们像物理硬盘一样包含敏感数据（例如，密码、个人数据等）。因为镜像文件和快照与硬盘相比更易移动，所以更应重视在镜像或快照是的数据的安全性。快照比镜像具有更大风险，因为快照包含在快照生成时的 RAM 内存数据，甚至包含从没存在硬盘上的敏感信息。

我们可以将系统或应用程序部署到镜像文件中，然后通过这个镜像文件进行分发部署，这样可以节省大量的时间。增加镜像文件保护能力，能够提高业务系统的安全性、连续性和健壮性。由于镜像文件易于分发和存储，需要防止其未经授权的访问、修改和重置。

随着在组织机构内的服务器和桌面虚拟化工作的不断推进，管理镜像文件成为一个巨大的挑战。一个镜像文件越长时间没运行，就会在它再一次加载时出现越多的脆弱点。因此，应检查所有的镜像以确保长时间未运行的镜像文件也定期更新。当用户和管理者可以创建自己的镜像文件时，跟踪这些镜像文件也是一个麻烦的问题。这些镜像可能没有做到适当的防护，尤其在没有可参照的安全基线的时候（例如，提供一个不同的预安全地镜像），这会增加被攻陷的风险。

伴随着虚拟化工作推进，另一个潜在的问题是镜像文件的增殖，也叫无序蔓延。创建一个镜像只需要几分钟，如果没有任何安全性的考虑，就会创建很多没必要的镜像文件。多余的镜像文件会成为攻击者另一个潜在的攻击点。另外，每一个镜像都需要独立的安全性维护工作，加大了安全维护的工作量。因此，组织机构应该减少建造、存储和使用不必要的镜像，实施完善的镜像管理流程，通过管理流程来管理镜像尤其是服务器镜像的创建、安全性、分发、存储、使用、退役和销毁工作。

同样，也需要考虑快照的管理。某些情况下，组织机构会规定不允许存储快照，因为被恶意软件感染的系统在后期恢复快照时有可能重新加载恶意软件。

3.2.2　虚拟机逃逸

利用虚拟机，用户能够分享宿主机的资源并实现相互隔离。理想情况下，一个程序运行在虚拟机里，应该无法影响其他虚拟机。但是，由于技术的限制和虚拟化软件的一些 bug，在某些情况下，虚拟机里运行的程序会绕过隔离限制，进而直接运行在宿主机上，这叫做虚拟机逃逸。由于宿主机的特权地位，出现虚拟机逃逸会使整个安全模型完全崩溃。当虚拟机逃逸攻击成功之后，对于 Hypervisor 和宿主机都具有极大的威胁。对于 Hypervisor 而言，攻击者有可能获得 Hypervisor 的所有权限。此时，攻击者可以截获该宿主机上其他虚

拟机的 I/O 数据流，并加以分析获得用户的相关数据，之后进行更进一步的针对用户个人敏感信息的攻击，更有甚者，倘若该宿主机上的某个虚拟机作为基本运行，攻击者便可以通过 Hypervisor 的特权，对该虚拟机进行强制关机或删除，造成基本服务的中断；对于宿主机而言，攻击者有可能获得宿主机操作系统的全部权限。此时，攻击者可以对宿主机的共享资源进行修改或替换，使得该宿主机上的所有虚拟机访问到虚假或篡改后的资源，从而对其他虚拟机进行攻击。由于攻击者获得了最高权限，则可以修改默认用户的基本信息，并降低虚拟机监视器的稳健性，从而对整个虚拟化平台造成不可恢复的灾难，使得其上的所有虚拟机都丢失重要信息。

目前对于虚拟机逃逸攻击，尚没有很好的安全对策，主要是针对云计算服务角色给出一些安全防范建议。例如，及时发现漏洞、开发漏洞补丁、使用强制访问控制措施限制客户虚拟机的资源访问权限、及时度量 Hypervisor 完整性等。

但这些安全防范建议均不能真正解决虚拟机逃逸攻击带来的危害。针对虚拟机逃逸漏洞，还是应该采用纵深防御的安全防护方法，从攻击检测、预防、避免攻击蔓延和 Hypervisor 完整性防护等多个方面，并结合可信计算技术，建立一个多层次的安全防护框架。

3.2.3　Rootkit 攻击

“ Rootkit”中 Root 一词来自 UNIX 领域。由于 UNIX 主机系统管理员账号为 root，该账号拥有最小的安全限制，完全控制主机并拥有了管理员权限被称为“ root”了主机。然而，能够“ root”一台主机并不意味着能持续地控制它，因为管理员完全可能发现主机遭受入侵并采取应对措施。因此 Rootkit 的初始含义就是“能维持 root 权限的一套工具”。

简单地说，Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，持久并毫无察觉地驻留在目标计算机中，对系统进行操纵，并通过隐秘渠道收集数据。Rootkit 的三要素就是：隐藏、操纵、收集数据。Rootkit 通常和木马、后门等其他恶意程序结合使用。

Rootkit 并不一定是用于获得系统 root 访问权限。实际上，Rootkit 是攻击者用来隐藏自己的踪迹和保留 root 访问权限的工具。通常，攻击者通过远程攻击获得 root 访问权限，或者首先通过密码猜测或者密码强制破译的技术获得系统的访问权限。进入系统后，如果还未获得 root 权限，再通过某些安全漏洞获得系统的 root 权限。接着，攻击者会在侵入的主机中安装 Rootkit 后门，然后将通过后门检查系统中是否有其他用户登录，如果只有自己，攻击者便开始着手清理日志中的有关信息，隐藏入侵踪迹。通过 Rootkit 的嗅探器获得其他系统的用户和密码之后，攻击者就会利用这些信息侵入其他系统。

在发现系统中存在 Rootkit 之后，能够采取的补救措施也较为有限。由于 Rootkit 可以将自身隐藏起来，因此可能无法知道它们已经在系统中存在了多长的时间，也不知道 Rootkit 已经对系统中的哪些信息造成了损害。对于找出的 Rootkit，最好的应对方法便是擦除并重新安装系统。虽然这种手段很严厉，但是这是得到证明的唯一可以彻底删除 Rootkit 的方法。

3.2.4　分布式拒绝服务攻击

分布式拒绝服务攻击（DDoS）是目前黑客经常采用而难以防范的攻击手段。

DoS（Denial of Service，拒绝服务攻击）有很多攻击方式，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一的方式，当攻击目标的各项性能指标（CPU 速度低、内存小或者网络带宽小等）不高时，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速提高，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度大大增加，分布式拒绝服务攻击（DDoS）便应运而生。高速广泛连接的网络在给大家带来方便的同时，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少、效果好；而现在电信骨干节点之间的连接都是以 G 为级别，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以分布在更大的范围，选择起来更加灵活。因此，现在的 DDoS 能够利用更多的傀儡机，以比从前更大的规模来攻击受害者主机。

DDos 攻击的后果有很多。例如，被攻击主机上存在大量等待的 TCP 连接；网络中充斥着大量无用的数据包，且源 IP 地址为假；制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信；利用受害主机提供的服务或传输协议上的缺陷，反复高速地发出特定的服务请求，使受害主机无法及时处理所有的正常请求；严重时会造成系统死机等。

3.2.5　侧信道攻击

基于虚拟化环境提供的逻辑隔离，采用访问控制、入侵检测等方法可以增强云计算环境的安全性，但是底层硬件资源的共享却容易面临侧信道攻击的威胁。

侧信道攻击是一个经典的研究课题，由 Kocher 等人于 1996 年首先提出。侧信道攻击是针对密码算法实现的一种攻击方式，当密码算法具体执行时，执行过程中可能泄露与内部运算紧密相关的多种物理状态信息，比如声光信息、功耗、电磁辐射以及运行时间等。这些通过非直接传输途径泄露出来的物理状态信息被研究人员称为侧信道信息（Side-Channel Information，SCI）。攻击者通过测量采集密码算法执行期间产生的侧信道信息，再结合密码算法的具体实现，就可以进行密钥的分析与破解。而这种利用侧信道信息进行密码分析的攻击方法则被称为侧信道攻击。

针对侧信道攻击，安全芯片可以提供大量的解决方案。安全芯片可以采用混淆时序、能耗随机等手段使黑客无从辨别，也就难以解密。

3.3　主机虚拟化安全的解决方案

针对主机虚拟化面临的安全风险，本节将从不同层面有针对性地采取安全加固方案，制