HZ BOOKS
华章科技

CLOUD SERVICE
SECURITY

云服务安全

邹德清 代炜琦 金海 著

机械工业出版社
China Machine Press

云服务安全

CLOUD SERVICE SECURITY

邹德清 代炜琦 金海 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

云服务安全 / 邹德清，代炜琦，金海著 . —北京：机械工业出版社，2018.7
（网络空间安全技术丛书）

ISBN 978-7-111-60508-9

I. 云… II. ①邹… ②代… ③金… III. 计算机网络 - 网络安全 IV. TP393.08

中国版本图书馆 CIP 数据核字（2018）第 154832 号

本书主要介绍云服务安全的基础理论和关键技术，系统、全面地对云服务的基本概念、云服务可信构建、云服务安全监控、虚拟域安全保障和云服务高可靠机制等内容进行深入剖析和系统介绍，并给出若干实际例子和思路，具备很强的实践性。

本书可作为高等院校网络空间安全相关专业本科生和研究生教材，也可供信息安全从业人员、云计算安全研究人员和技术人员参考。

云服务安全

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：余　洁　　责任校对：李秋荣
印　　刷：中国电影出版社印刷厂　　版　　次：2018 年 8 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：22
书　　号：ISBN 978-7-111-60508-9　　定　　价：79.00 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

前　言

近年来，云计算技术发展迅速，其凭借服务整合、动态扩展、按需供给等特点引起了产业界、学术界和政府部门的高度关注，已成为越来越多企业与用户部署服务的首要选择。伴随着云计算的快速发展，云服务暴露出的安全问题也日益增多。不同于传统的IT环境，在云计算环境中，云服务将资源的所有权、管理权及使用权进行了分离，租户失去了对物理基础设施的直接控制，因此传统的安全技术手段无法保障云服务的安全性。如今，云安全问题已成为限制云计算发展的关键因素，许多云服务安全问题亟待解决。例如，如何应对虚拟化特性带来的新的安全挑战、如何保护云租户的应用与数据安全，以及如何保障云服务的可靠性等，针对这些问题进行的云服务安全关键技术研究对于推动云计算技术快速发展具有重大意义。

本书主要介绍云服务安全的基础理论和关键技术。全书共7章，主要内容如下。第1章简要阐述云计算的发展概况、体系结构与面临的安全威胁，并给出全书的组织结构。第2章重点探讨云计算的虚拟化技术、可信计算技术、安全监控技术和容错技术等关键技术。第3章从全局角度分析云服务可信构建存在的安全问题，结合云服务的安全需求重点讨论云平台动态可信度量机制、云平台透明信任链机制和可信云服务构建机制。第4章概要论述当前云服务安全监控技术上存在的不足，并针对这些不足介绍云平台通用监控机制、基于数据流分析的主动监控机制和云平台可信监控框架。第5章从虚拟域安全控制、可信构建和可信回滚的角度出发，对虚拟域安全保障手段进行了全面分析。第6章介绍云服务高可靠机制，阐述为实现云服务高可靠性所采用的各种技术解决方案，包括云服务分层故障检测机制、基于日志分析的故障诊断机制、云环境软件故障容忍机制、面向云计算的动态软件升级机制和虚拟机镜像离线更新机制。第7章对全书的内容进行归纳总结，并对云服务安全未来的发展趋势进行展望。

本书的部分内容来自国家重点基础研究发展计划（973）项目子课题“云计算安全基础理论与方法研究”的研究成果，同时也参考了大量的业界研究成果和相关技术资料。感谢陈刚、程戈、项国富、袁劲枫、章文荣、王圣兰、王凤伟、刘凯、秦昊等人为本书贡献的研究成果和技术资料，感谢夏妍就本书的组织和修订做出的辛苦努力。最后，本书得以成功出版，要感谢机械工业出版社华章公司的大力支持，在此表示深深的谢意。

本书代表作者及其研究团队对于云服务安全的观点，由于水平有限，书中难免存在不足之处，恳请读者批评指正。

作者

2018年6月

目　录

第1章

引　言

近年来，云计算已成为当前信息技术领域的热门话题之一，引起了产业界、学术界、政府等各界的广泛关注。以虚拟化技术为支撑的云计算技术通过网络将分散的资源（包括存储、网络、计算、软件和应用运行环境等）集中起来，实现了资源整合，并允许用户以动态、按需、可度量的方式使用。

本章将首先介绍云计算的发展规模，以及云安全对云计算技术发展的重要性；其次介绍云服务的体系结构，包括基础设施即服务、平台即服务和软件即服务；然后强调云服务安全当前面临的重要挑战；最后给出本书的组织结构。

1.1　云计算的发展概述

作为一种新兴的资源使用和交付模式，云计算为资源的使用者提供按需使用和随时扩展的服务[1]。以虚拟化技术为支撑的云平台能够充分利用其优势来进行资源聚合和服务迁移[2]，从而使云平台更加具有灵活性。云租户将服务部署在“云”中，云管理员对所有服务进行统一管理。这种模式能够帮助企业IT管理者从繁重的基础设施管理和维护工作中解放出来，从而更加关注自身核心业务的发展。云计算技术带来的服务整合和按需供给可大大提高当前计算资源的使用率，降低每服务的能耗量，并且有效屏蔽计算资源可能出错的问题[3]。IT产业界普遍认为，云计算是继互联网经济之后的又一个重要的产业增长点，具有广阔的市场发展前景。同时，云计算为大数据、人工智能的高速发展提供了强有力的支持。云计算提供了针对海量数据的强大计算、存储能力，人工智能可依托云计算的强大计算能力进行训练、推理和预测。

云服务凭借其高扩展性、便利性、经济的优势获得越来越多的企业租户的青睐。据中国信息通信研究院发布的《云计算关键行业应用报告（2017年）》[4]显示，2016年全球以IaaS、PaaS和SaaS为代表的典型云服务市场规模达到654.8亿美元，预计2020年将达到1435.3亿美元，而2016年我国云计算整体市场规模达514.9亿元。图1-1为全球云计算市场规模。国外很多公司或企业，如亚马逊、Google、IBM、微软、HP、Dell等都在大力支

持和推广云服务，其中亚马逊、Google、微软、Rackspace 等云服务的企业用户数均已达到 10 万量级。亚马逊的 AWS 2016 年收入达 122 亿美元，增长速度超过 54%，数据中心遍布美国、欧洲、巴西、新加坡、日本和澳大利亚等地，服务全球 190 个国家和地区；微软作为云计算领域的后发力者，其 Azure 云服务的增长率相比同期增长了 93%，是 AWS 云服务的 1.7 倍，同时，微软在云计算数据中心的巨额投入使其在全球的数据中心数量达到 38 家。在国内，腾讯、百度、新浪、搜狐、阿里巴巴、曙光、华为等 IT 企业也将云计算作为发展的重点。据阿里云和腾讯云发布的数据显示，阿里云市场 2017 年第一季度申请合作服务商近千家、商品超过 1000 款。腾讯云已经有超过 200 家各种类型的开发合作伙伴，通过与神马、东华、东软、长亮、思迪、中科大洋等行业领军企业合作，为交通、政务、扶贫、公安、旅游、保险、证券、工业等各行各业的客户提供解决方案。

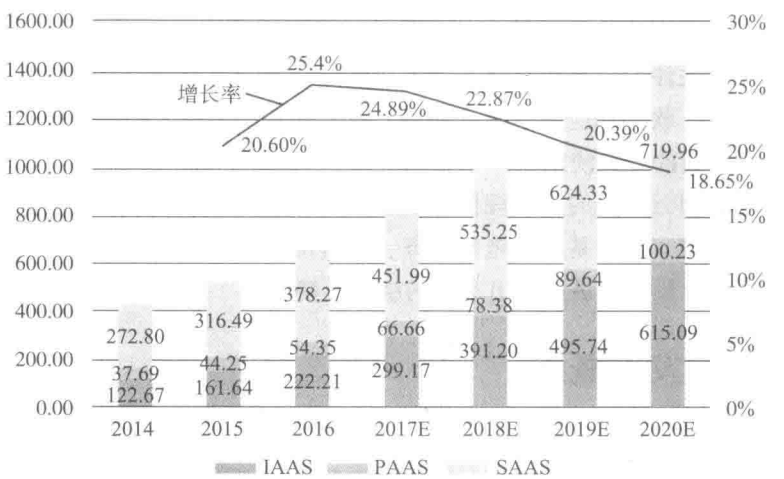

图 1-1　全球云计算市场规模

然而，云计算在提高 IT 资源使用效率的同时，其动态虚拟化管理方式、强大的计算与存储能力也会引发新的安全问题，并给现有的安全管理体系带来巨大冲击。自 2013 年“棱镜”事件被曝光之后，世界各国纷纷开始关注信息安全，云安全是其中必不可少的一部分。近年来，云安全事件频出：2014 年 8 月，苹果 iCloud 服务遭遇攻击，导致大量租户的隐私数据泄露以及服务中断；2015 年 6 月，美国联邦人事管理局发生泄密事件，该事件影响到 2210 万人。云安全问题使得许多企业和机构对云计算望而却步。RSA 首席技术官 Hartman 也指出，在企业将当前应用向第三方云环境迁移的过程中，首先需要考虑的就是对云服务的信任问题。租户把安全敏感数据、关键应用部署在云计算平台中会感到数据不可控，无法完全信任云平台供应商，担心租户隐私受到供应商的危害。在 IDC 全球调查中，对云计算安全、性能、可靠性等抱有怀疑态度的用户占 70% 以上。即使云服务提供商本身并无恶意，但目前的云平台依旧无法让租户放心，各大平台都存在着安全漏洞，服务随时可能宕机。2015 年爆出的 KVM/Xen 虚拟机的“毒液（VENOM）”

漏洞可导致攻击者越过虚拟化技术的限制，实现“虚拟机逃逸”，侵入甚至控制其他租户的虚拟机，给 IaaS 服务商的虚拟主机服务带来极大的安全隐患，影响了全球数以百万计的平台主机。2015 年 3 月，Xen 漏洞修补事件造成亚马逊 AWS、IBM SoftLayer、Linode 及 Rackspace 等多家云服务商的主机大面积重启，仅亚马逊 AWS 就有近 10% 的云主机租户业务暂停。而在主流云资源管理平台——OpenStack 中在 2015 年 4 月已经发现 173 个安全漏洞。

总之，虽然政府通过政策引导并投入大量资金进行云计算基础设施的建设，但安全问题在一段时间内都会是限制云计算普及和推广的重要原因。

1.2　云服务体系结构

在过去几年里，云计算技术有了长足发展，许多 IT 企业已经推出了各自的云服务，从服务层次上来看，可以分为基础设施即服务、平台即服务和软件即服务，图 1-2 给出了云服务体系结构。

1. 基础设施即服务

基础设施即服务（Infrastructure as a Service，IaaS）根据租户需求提供计算资源实例，将处理、存储、网络以及其他基础性的计算资源作为一种服务提供给云租户。租户可以自主请求资源实例，并在其上部署或运行其所需的软件，包括操作系统或应用。在这种模式下，“云”提供了弹性的服务资源，所有需求都可以通过增加可用资源来实现，当租户不再需要时资源即被释放，避免了传统虚拟环境下无法动态要求服务质量和能力的弊端，租户能够根据需求随时动态请求资源服务。这种架构的典型应用有 Amazon 的弹性云（EC2）。

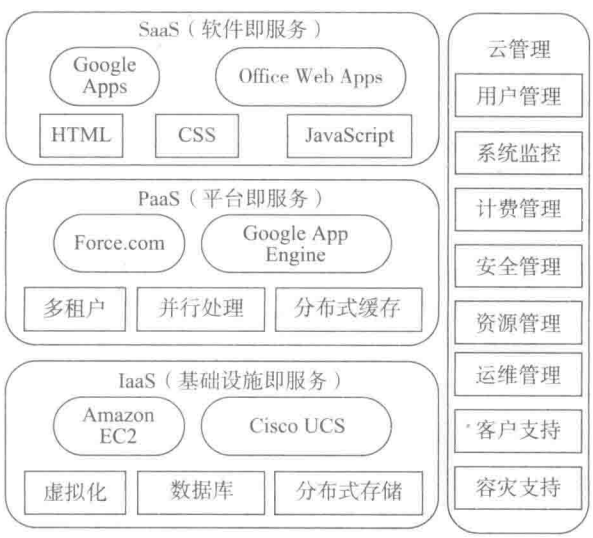

图 1-2　云服务体系结构

对于租户而言，IaaS 具有良好的自主性，租户可以像使用本地系统那样使用云提供的资源，且云平台的构建相对简单，管理也较为容易。通常，使用 IaaS 可以帮助租户降低技术设施的成本，但同时租户必须自己处理大规模计算任务中的作业调度、协同通信、数据可靠性、扩展性等问题，有较高的应用开发要求。

2. 平台即服务

平台即服务（Platform as a Service，PaaS）是指租户通过编程语言和工具，对 IaaS 中的应用进行开发。在 PaaS 云服务中，服务提供方根据需求为租户提供直接的程序执行环境和存储服务，提供资源的动态扩展、容错管理以及协同通信，租户不需要对基础设施云、网络、服务器、操作系统或存储进行管理和控制，仅需要遵循服务商提供的接口和模式对应用程序进行部署，“云”会自动将作业和数据在网络中的计算节点和存储节点进行调度和处理。使用 PaaS 的租户会看到一个封装式服务，该服务通过 API 提供给租户。客户通过 API 与该平台互动，而且该平台执行一切必要的操作来管理和扩展其本身，以提供规定的服务水平。典型的 PaaS 是 Google 的 App Engine。

PaaS 架构具有良好的租户体验，能够帮助租户省略大量的业务无关逻辑。但 PaaS 也要求租户必须遵循其编程模型，一些原有的应用系统要想使用 PaaS 就需要重新进行编译，这也会带来应用移植的问题。同时，PaaS 也对云平台的管理员和构建者提出了较高的要求。

3. 软件即服务

软件即服务（Software as a Service，SaaS）是指租户通过各种终端设备上的 Web 浏览器访问云服务商提供的各类应用。SaaS 既不像 PaaS 那样提供计算或存储资源类型的服务，也不像 IaaS 那样提供运行租户自定义应用程序的环境，它只提供专门用途的服务应用调用。租户不需要管理或控制底层的云基础设施、网络、服务器、操作系统、存储和应用等，可以直接按需租用应用，同时可以对这些应用进行一系列自定义配置等操作。早期的 SaaS 方法 ASP（Application Service Provider，应用服务提供商）就是这种形式，ASP 交付软件并根据软件的使用情况收费，使用者只需随需租用软件，而无须购买。典型的应用有 Salesforce Online CRM（Customer Relationship Management，客户关系管理）服务、Google Docs 等。通过 CRM 可以在网上随时随地查阅与分析客户的营销状况，不仅提高了工作效率，而且软件的支付费用也大为下降。同样，只要能连上网络，租户就可以随时随地使用 Google Docs 来处理日常的文档工作，既不需要安装、维护软件，也不占用个人计算机资源。

值得一提的是，随着云计算的不断发展，不同云计算解决方案之间相互渗透融合，同一种产品往往会横跨两种以上类型。例如，Amazon Web Service 是以 IaaS 发展的，但提供的弹性 MapReduce 服务、SimpleDB（简单数据库）服务却是 PaaS 的范畴。三个不同层次的服务模型存在依赖性，SaaS 建立在 PaaS 和 IaaS 之上，PaaS 建立在 IaaS 之上；同样，

安全问题也随着层次的递进而有所继承与改变，使用者所承担的安全和管理的责任随着所在服务层次的上升而减少。

另一方面，云计算服务的部署模式分为公有云、私有云和混合云三类。

1）**公有云**：由某个组织拥有，其云基础设施可用于公共场所，理论上，任何人都可以通过授权接入该平台。它是私有云的扩展和公共服务化，公有云在充分发挥云计算系统的规模经济效益的同时也增加了安全风险。

2）**私有云**：云基础设施仅为某个组织运作，由该组织或某个第三方负责管理，可以是场内服务（on-premises），也可以是场外服务（off-premises）。私有云系统存在于企业防火墙之内，只针对企业内部服务。私有云比公有云的安全性好，但成本高，而且基础设施的利用率也低于公有云。

3）**混合云**：云基础设施由两个或多个云（私有的、公共的）组成，它既可以保持单一云形式的整体性，也可以通过接口和技术手段使不同云形式中的数据应用进行交互，这些技术促成数据和应用的可移植性（例如用于云之间负载分担的 cloud bursting 技术）。混合云可以同时提供私有的和公共的云服务，它是介于公有云和私有云之间的一种折中方案。

1.3 云服务安全面临的重要挑战

当前，云计算的发展和普及受到许多关键因素的制约，其中安全问题首当其冲[5]，并且伴随云计算的发展和普及，安全问题的重要性也日益凸显。根据 CSA（Cloud Security Alliance，云安全联盟）发布的调查结果显示，大约 73% 的受访企业认为安全问题是阻碍云计算发展的首要挑战。对于云服务目前面临的安全问题，CSA 在 2016 年公布的云安全威胁报告中列出了十二项重要的安全威胁[6]，包括数据丢失和泄露、系统漏洞利用、账户劫持和拒绝服务攻击等。

传统的 IT 系统是封闭的，运行于企业内部，对外提供的只是网页、邮件等服务接口，因此，在网络边界采取设置防火墙、访问控制等安全措施，便可以解决大部分的安全问题[7]。在云计算环境中，云计算服务将资源的所有权、管理权及使用权进行了分离，租户因此失去了对物理基础设施的直接控制。相对于传统的计算模式将信息保存在自己可控制的环境中，云计算模式中租户的应用和数据都保存在“云”中，因此，如何保证租户应用和数据的安全，以及如何证明计算和存储环境的可靠性，已成为制约云计算发展的关键要素之一。

云计算面临的安全问题主要有以下两个方面[8]。

1. 虚拟化安全

虚拟化技术是支撑云计算的核心技术[9-10]，将系统资源虚拟化能够解决目前硬件和系统软件的异构性问题，屏蔽下层硬件及指令集的差异，从而充分满足应用软件对系统资源多样性的需求。尽管与基于物理机上的计算相比，基于虚拟化计算机系统上的计算有许多优势[11]，但是也给云计算带来了许多新的安全威胁。

作为虚拟化的核心，Hypervisor运行在操作系统与物理设备之间，其自身的安全非常重要。目前，在国际上最权威的漏洞数据库CVE中，虚拟化软件的漏洞已累计超过700条。攻击者可能利用虚拟化软件中存在的安全漏洞，攻破Hypervisor从而造成“虚拟机逃逸”，影响其上所有虚拟机的安全性。

虚拟机资源容易被合法租用却发起非法的攻击，特别是如果利用数万台云服务器资源对国家重要行业的网络设备、安全设备等发起攻击或进行密码破解，则会给整个社会带来不可估量的损失。

同时，虚拟机是承接底层硬件和上层服务应用的关键层次，建立安全可信的虚拟化环境是对上层管理应用安全的基本支持。需要对虚拟机可信、隔离、迁移等技术进行更深入的研究，以解决虚拟化给云计算带来的新风险。

2. 服务可用性

服务可用性问题是云计算的一个核心安全问题，云环境下管理的数据和服务来源于数量庞大的用户群，如果云平台发生服务不可用问题，那么造成的影响将大大超过传统信息系统。

造成服务中断的威胁可能来源于云系统内部，也可能来源于外部。内部的威胁主要是云平台自身的可靠性问题，如发生服务器宕机和数据大规模丢失等都会造成云服务不可用。服务可用性的外部威胁主要是拒绝服务攻击威胁。

因此，虚拟化安全面临着以下几个方面的重要挑战。

第一，在云服务可信构建方面，运行在云环境中的应用和数据面临严重的安全威胁。

首先，通用操作系统内核的代码量庞大，结构复杂，存在大量攻击窗口，而且越来越多的漏洞报告和攻击案例表明内核的安全问题十分严峻。然而，安全敏感的应用程序不可避免地将内核作为可信基，用来管理底层硬件和提供系统服务。当内核被攻陷后，敏感应用程序通常很难抵御来自底层的不可信内核的攻击。近年来，在不可信内核中保护敏感应用程序已成为云服务安全领域的热点问题之一。目前，应用程序保护的主流方法是为应用程序构建安全可信的执行环境，而当前可信执行环境构建技术无法直接应用于云环境。云环境的多租户、多层次的服务模式特征使得现有可信计算技术很难满足动态复杂的租户执行环境的需要。本书将关注当前复杂云环境的可验证的动态环境构建机制，研究如何在可信执行环境下构建安全云服务。

第二，在云服务安全监控方面，缺乏适用于云环境的全面、实时、有效的安全监控机制。

虚拟机系统是云租户应用程序和数据的直接执行环境，其安全性十分重要，然而它往往也成为最直接的攻击目标。针对虚拟机的安全监控技术分为虚拟机内部监控和虚拟机外部监控。

因为虚拟机内部监控与监视保护对象处于同一计算环境，所以可以对监控对象提供本地的、语义丰富的监控视角，以便于对象的安全分析。但同时，该方法通常对计算环境依

赖性较强，不便移植，且其安全部件也暴露在监控环境的恶意软件面前，当系统环境遭到破坏时，安全部件往往也不能免于攻击。

虚拟机外部监控可以在一定程度上隔离安全部件与监控环境中的恶意软件，有效保护安全部件免受攻击。同时，这一方式对监控环境的影响较小，便于透明实现，在系统兼容性上也有优势。但这种方式存在“语义断层”（semantic gap）问题，即在虚拟机外监控的信息将会丢失很多虚拟机内的语义信息，给安全分析带来困难。

本书将对如何在云环境下实现全面、实时、有效的安全监控进行研究，这是云服务安全运行的重要保障手段。

第三，在虚拟域的安全保障方面，面临虚拟化技术引发的安全威胁。

虚拟化技术的高动态性（虚拟机回滚、迁移等操作）导致云服务安全敏感状态不一致。云环境虚拟域的状态回滚增加了时间状态的动态性，跨节点多虚拟机加入或退出虚拟域以及虚拟机迁移增加了空间状态的动态性，这给云环境虚拟域的安全状态一致性带来了巨大挑战。而安全状态的不一致可能会被攻击者利用，从而对云服务发起攻击。本书将提出云虚拟域安全状态一致性保障机制。

第四，在云服务高可靠性方面，缺乏适用于云环境的服务高可靠性保障机制。

云环境的服务超大规模性、软件高度复杂性和数据海量交互性为可靠性保障机制带来了新的挑战。云服务的可靠性极易受到服务基础设施故障、服务遭受恶意攻击或服务交互数据出错的影响，使得云环境下的服务质量难以得到保障，成为阻碍云服务发展的一大瓶颈。本书将介绍适用于云环境的服务高可靠性保障机制，这对于构建高可靠云服务中心具有重大意义。

1.4 本书的组织结构

本书主要针对云服务安全机制进行研究，全书的组织结构如下。

第 1 章为引言。首先介绍云计算的发展状况、云服务的体系结构，接着介绍 IaaS、SaaS、PaaS 等概念，然后分析现阶段云服务面临的安全挑战，最后给出全书的组织结构。

第 2 章为相关技术背景，将对本书涉及的虚拟化技术、可信计算技术、安全监控技术和容错技术分别进行详细介绍。

第 3 章为云服务可信构建。首先将分析云服务安全当前的研究背景，然后针对现有研究的不足提出云平台动态可信度量机制、云平台透明信任链机制和可信云服务构建机制，并分别对这些机制解决的问题和解决思路进行详细说明。

第 4 章为云服务安全监控。首先将分析云环境下安全监控的研究现状以及相关技术，然后根据监控对象和监控手段的不同提出基于行为的云平台通用监控机制、基于数据流分析的主动监控机制和云平台可信监控框架，并对这些机制的设计思路进行介绍。

第5章为虚拟域安全保障。首先将分析当前云平台虚拟域安全的研究现状，针对其不足提出了几个安全保障机制，即虚拟域安全控制、可信虚拟域和虚拟域可信回滚。

第6章为云服务高可靠机制。首先将分析当前云服务可靠性机制的研究现状，针对现有研究的不足提出云服务分层故障检测机制、基于日志分析的故障诊断机制、云环境软件故障容忍机制、面向云计算的动态软件升级机制和虚拟机镜像离线更新机制，并详细介绍上述机制的设计架构以及关键技术。

第7章将总结全书并展望云服务安全的发展方向，最后给出未来的研究热点。

第2章

相关技术背景

本章将详细介绍本书涉及的技术背景，包括虚拟化技术、可信计算技术、安全监控技术和容错技术，为读者理解本书的后续章节奠定基础。

2.1 虚拟化技术

2.1.1 概述

虚拟化技术（Virtualization Technology）起源于20世纪60年代，IBM将该技术应用于大型机，允许租户在一台主机上运行多个操作系统以充分利用昂贵的资源。随后，大型机上的虚拟化技术开始向小型机或UNIX服务器上移植，HP、Sun也跟随IBM在自己的RISC（Reduced Instruction Set Computer，精简指令集计算机）服务器上提供了虚拟化技术，但由于真正使用大型机和小型机的租户还是少数，加上各家产品和技术之间并不兼容，因此虚拟化技术仍旧没有得到公众关注。

近年来，随着计算系统的资源规模不断扩展、处理能力快速增强、资源种类日益丰富、应用需求灵活多样，特别是随着x86处理器性能的提升和应用普及，以及多核技术的发展，虚拟化技术已成为商业和学术界关注的热点。

虚拟化计算系统能够动态组织多种计算资源，隔离具体的硬件体系结构和软件系统之间的紧密依赖关系，实现透明化的可伸缩计算系统架构，从而灵活构建满足多种应用需求的计算环境，提高计算资源的使用效率，发挥计算资源的聚合效能，并为租户提供个性化和普适化的计算资源使用环境。虚拟化计算系统可以更加合理地利用计算资源，满足日益多样的计算需求，使人们能够透明、高效、可定制地使用计算资源，从而真正实现灵活构建、按需计算的理念。

从是否需要修改客户机操作系统内核的角度来看，虚拟化技术可以分为半虚拟化（Para-virtualization）技术和全虚拟化（Full-virtualization）技术。在起初的全虚拟化技术中，二进制转换带来的开销使得其虚拟化性能大打折扣，为了解决这个问题，在Denali项目和Xen

项目中引入了新的半虚拟化模式[12]。半虚拟化的实施不需要进行二进制转换，而需要对客户机操作系统进行代码级的修改。半虚拟化技术绕开了传统 x86 体系结构的虚拟化漏洞，并以良好的性能赢得了在开源软件操作系统（如 Linux）上的广泛关注，但却无法支持像 Windows 这样的“私有”操作系统。为了更好地支持全虚拟化，Intel VT[13] 和 AMD SVM（Secure Virtual Machine，安全虚拟机）[14] 实现了“硬件虚拟化”，它们在芯片硬件层面上弥补了 x86 体系结构的虚拟化漏洞，使得虚拟机管理器对未经修改的操作系统的支持成为可能[15]。

为了满足不同的功能需求，目前已出现了许多不同种类的虚拟化解决方案，由于其采用不同的实现方式和抽象层次，使得这些虚拟化系统呈现出不同的特性。《计算系统虚拟化——原理与应用》[9] 一书从虚拟机实现所采用的抽象层次的角度对虚拟化系统进行了如下分类。

- 指令集虚拟化。指令集虚拟化即通过将虚拟机中执行的指令翻译成主机指令，然后在真实的硬件上执行，因此也被称为模拟器（Emulator）。虚拟机和真实的硬件平台之间没有严格的绑定，因此这种虚拟化方法具有很强的可移植性。具有代表性的系统是 Bochs[16]、QEMU[17]、BIRD[18] 等。
- 硬件抽象层虚拟化。HAL（Hardware Abstraction Layer，硬件抽象层）虚拟化与指令集虚拟化非常相似，其不同之处在于，这种类型的虚拟化所考虑的是一种特殊情况，即客户执行环境和主机具有相同的指令集合。它通过虚拟机管理器在物理机上创建多个虚拟机，并且给每个虚拟机提供底层真实硬件的视图，让虚拟机中的操作系统或者应用程序认为其运行在真实的硬件之上，从而大大提高执行速度。具有代表性的系统是 VMware ESX Server[19]、Virtual PC[20]、Xen[21] 等。
- 操作系统级虚拟化。它通过共享真实的物理硬件和操作系统来为多个租户提供独立的、隔离的操作环境，可以快速地“克隆”当前主机的操作环境来进行沙盒（Sandbox）测试，从而免除了大量不必要的安装和配置开销。具有代表性的系统是 Linux-VServer[22]、Jails[23] 等。
- 编程语言级虚拟化。与传统的 ISA（Instruction Set Architecture，指令集架构）不同，它是在应用层提供一套自定义的、与处理器无关的指令集。利用该指令集进行开发的软件能够屏蔽硬件的异构性，其主要应用于与硬件平台无关的软件开发。具有代表性的系统是 Java[24]、Microsoft .NET CLI[25] 等。
- 程序库级虚拟化。它通过在应用层模拟一套租户级的应用编程接口（Application Programming Interface，API），从而隐藏与操作系统相关的细节。它可以在某种操作系统上运行其他操作系统的应用程序，如在 Linux 上运行 Windows 程序。具有代表性的系统是 WINE[26]、Cygwin[27] 等。

在这些不同层次的虚拟化技术中，硬件层次的虚拟化技术具有以下几个特性：可以将虚拟资源映射到物理资源、在虚拟机计算中使用本地硬件、高度的隔离性、支持不同的操作系统和应用程序而不需要重启机器、低风险和易于维护等。硬件层次的虚拟化技术有众