HZ BOOKS
华章IT

云计算与虚拟化技术丛书

WILEY

Virtualization Security
Protecting Virtualized Environments

虚拟化安全解决方案

［美］戴夫·沙克尔福（Dave Shackleford）著
张小云 等译

资深虚拟化安全专家撰写，系统且深入阐释虚拟化安全涉及的工具、方法、原则和最佳实践

深入剖析虚拟基础设施各个层面的问题，从虚拟网络到管理程序平台和虚拟机，重点阐释三大主流虚拟化技术解决方案，能为工程师与架构师设计、安装、维护和优化虚拟化安全解决方案提供有效指导

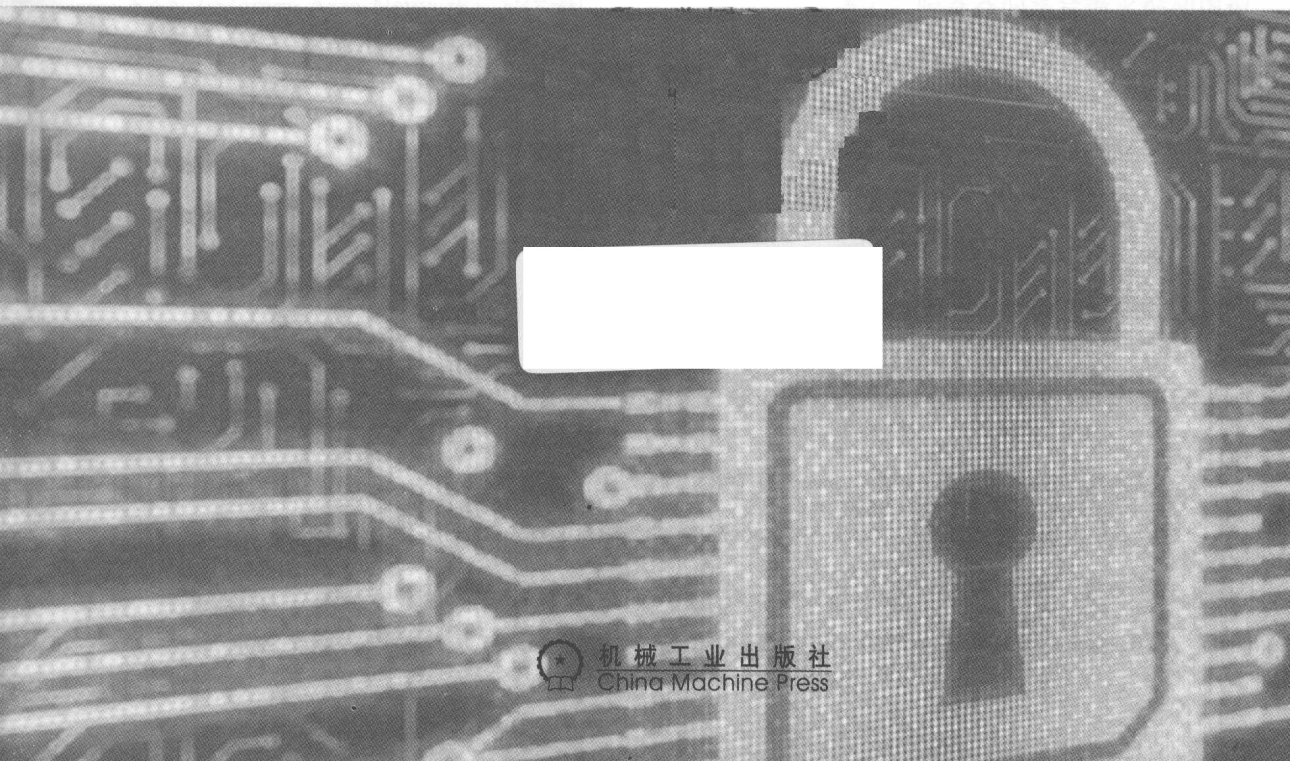
机械工业出版社
China Machine Press

云计算与虚拟化技术丛书

Virtualization Security
Protecting Virtualized Environments

虚拟化安全解决方案

[美] 戴夫·沙克尔福（Dave Shackleford）著
张小云 等译



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

虚拟化安全解决方案 /（美）沙克尔福（Shackleford, D.）著；张小云等译 . —北京：机械工业出版社，2016.1
（云计算与虚拟化技术丛书）
书名原文：Virtualization Security: Protecting Virtualized Environments

ISBN 978-7-111-52231-7

I. 虚… II. ①沙… ②张… III. 计算机网络－安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2015）第 280798 号

本书版权登记号：图字：01-2014-4758

虚拟化安全解决方案

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：秦　健　　责任校对：殷　虹
印　　刷：三河市宏图印务有限公司　　版　　次：2016 年 1 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：17.75
书　　号：ISBN 978-7-111-52231-7　　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）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

The Translator's Words 译 者 序

为什么翻译本书

云计算是随着多核处理器、虚拟化、分布式存储、宽带互联网和自动化管理技术发展而产生的一种新的计算模式。本质上，云计算是终端用户通过远程连接，获取存储、计算、数据库等计算资源。云计算产生于21世纪初期，随着Web 2.0技术的出现，互联网迎来了新的发展高峰。网站或业务系统处理的数据呈现爆发式增长，用户的数量也在快速增长。随着移动终端的智能化、移动宽带的普及，越来越多的移动设备接入互联网，现有Web服务器的技术已经越来越不能满足海量数据的服务请求。于是，以GFS（Google File System）SAN（Storage Area Network）为代表的高性能存储技术出现了。服务器的整合需求推动虚拟化安全的发展和进化、多核技术的广泛应用、SaaS的出现和普及等，所有这些最终导致云计算的产生。

计世资讯（CCW Research）《2014—2015年中国云计算市场现状与发展趋势研究报告》的数据表明：2014年中国云建设市场规模为383.6亿元，同比2013年增长达44.1%。云计算从2011年开始爆发式发展。无论是IT巨头还是新出现的“互联网+”概念，都以大数据的计算作为基础设施，云计算市场已经成为一个炙手可热的领域，未来云计算安全也必将会得到越来越多企业的重视。云计算的应用与作为云计算基础的虚拟化安全是密不可分的。而虚拟化安全正是本书讨论的重点，译者认为翻译本书在当下具有极强的指导意义，相信读者也能从本书中获益颇多。

读者对象

- 虚拟化服务器管理人员。虚拟化服务器管理人员可以通过本书了解：虚拟化安全的基本原理、当前主流虚拟化技术的安全管理方法和策略、虚拟化安全的威胁；如何

使用主流虚拟化技术实现虚拟化安全；如何保护虚拟化基础设施的安全；使用什么策略实施虚拟化安全；如何保护虚拟机，以及进行日志和审计，灾难恢复、变更和配置管理。

- 软件开发人员。开发人员阅读本书可以扩大知识面，了解和规避虚拟化技术中的安全漏洞，防范各种针对虚拟化技术的攻击。
- 软件行业的管理人员。管理人员可以从本书中获得虚拟化安全的基本理论，了解如何设计安全的虚拟化网络，如何提高虚拟化产品的安全，以保障客户服务，提高公司竞争力。

本书的主要内容

本书共分为 11 章。第 1 章主要介绍虚拟化安全的基础理论；第 2 章讲述如何保护管理程序；第 3 章讲述如何设计安全的虚拟网络；第 4 章讲述高级虚拟网络操作；第 5 章讲述虚拟化管理和客户安全；第 6 章讲述如何保护虚拟机；第 7 章讲述日志和审计方面的实践；第 8 章讲述虚拟化安全的变更和配置管理；第 9 章讲述如何应对虚拟化安全的不良后果以实现灾难恢复和业务连续性；第 10 章讲述脚本自动化的提示与技巧；第 11 章讲述虚拟化安全要考虑的其他因素。

致谢

感谢华章公司的编辑，他们对本书翻译的指导和建议使本书最终得以出版，同时还要感谢华章公司的同仁对本书出版所做的努力。

最后，译者向支持本书翻译工作的家人深表谢意，感谢他们的理解和支持。

Preface 序　言

什么是虚拟化安全？这里有许多不同的定义，但最简单的是：系统锁定和虚拟化基础设施所有组件与安全相关的技术及过程化控制的应用。为什么需要虚拟化安全？世界正在快速变化，现代数据中心的形态正快速发生变化，许多组织的网络边界比以往任何时候都显得更模糊。我们开始利用组织内部和外部的数据云，这往往涉及大量虚拟化技术。我们的整个网络好比在“一个盒子里”，所有组件都从它们的对应物——网络设备、存储器、应用程序组件、整个服务器和桌面中抽象出来。最后，也可能是最重要的，在计算机堆栈中，我们比以往任何时候拥有更多的层，而更多的层意味着更糟糕的安全，这是IT多年来得到的一个教训。

由于这些原因，我们需要正确理解如何适当锁定这一技术。就任何安全努力来说，你做什么和怎样做的效果和严格程度，取决于你的业务和风险承受能力。对于一些安全问题，我们应该更侧重于政策和流程而不是技术。例如，作为一个良好的虚拟化安全策略的一部分，变更控制和配置管理这两个方面确实需要关注，但它们不像其他策略一样解决实际技术问题。另外，在虚拟化领域有许多旋钮要调，按钮要按，知道它们是什么和什么时候扭或按下是更多运营和安全团队现在需要了解的一项关键技能。当你基于一种技术构建基础设施时，你最好知道如何恰当地保护它。

我真诚地希望这本书能为读者提供实用的指南，欢迎任何反馈或改进。

谁应该阅读本书

我认为本书对每个人都有益处，但“每个人”是一个相当宽泛的定义，我会将它的范围缩小一点。本书是一本专著，尤其是为IT运营团队即管理虚拟环境（包括虚拟网络和存储）任何方面的团队所写。本书理论方面非常简短，直奔主题，使你能够快速应用概念，完成工作。IT管理员、网络工程师、技术架构师和许多其他关注运营的人员也可以从本书获益。

这本书也是为信息安全团队写的。尽管他们可能不亲自执行许多虚拟化环境的配置，但他们却可能参与审计和设置策略，如果他们知道的技术知识更多，他们就能更好地完成工作。

最后，这里有许多材料，技术经理和审计员也会很感兴趣。尽管不是所有材料都会引起他们的兴趣，更有可能是这里有足够的背景资料使经理们能够快速掌握，并且有审计员能用来评估环境的状态的技术控制和命令。

你将学到什么

通过本书，你将学到保护虚拟基础设施的最佳实践和特定技术控制。笔者将讲述全部组件，包括从虚拟网络到管理程序平台和虚拟机。本书的教学重点之一是涵盖了三种主流管理程序平台供应商，即 VMware、Microsoft 和 Citrix。尽管有许多其他虚拟化技术（如 KVM），但这三个是最普遍的，笔者将讲述配置和管理它们的大多数方面。你将学到一些脚本撰写基础知识，设置灾难恢复工具及技术，各种配置选项，一些审计和评估技术，以及在大多数情况下如何从 GUI 和命令行角度保护这些技术。

本书是如何组织的

第 1 章：虚拟化安全基础 该章解释虚拟化如何改变 IT 运营界的功能，以及在日常活动中为什么确保运营团队实现安全是重要的。

第 2 章：安全虚拟机管理程序 最常用的管理程序平台，如 VMware ESXi、Microsoft Hyper-V 和 Citrix XenServer 等都有许多配置控制，它们由系统管理员实现和维护。该章将描述这些控制，就性能、维护的简单性和对虚拟化运行其他方面的影响而言，对运营团队来说，它们各有优缺点。该章介绍的特定内容包括配置 VMware vSphere 和 ESXi，在 Windows Server 2008 和 Windows Server 2012 上配置 Microsoft Hyper-V 和配置 Citrix XenServer。

第 3 章：设计安全的虚拟网络 当设计或更新虚拟网络时，实现网络策略和将虚拟网络集成到现有物理基础设施需要考虑许多安全因素。该章将概述网络和虚拟化运营团队的特定设计元素，以及 vSphere 和 Hyper-V 本地虚拟交换机的配置建议及其他类型交换机的一些讨论。该章介绍的特定内容包括虚拟网络和物理网络、虚拟网络安全考虑因素、配置虚拟交换机、虚拟网络与物理网络集成。

第 4 章：高级虚拟网络操作 该章建立在第 3 章的基础上，包括更详细的网络运营考虑因素，例如负载均衡、流量整形和网络监控。还包括与现有网络工具的集成，以及对管理员有益的新工具类型和技术（包括脚本）。该章介绍的特定内容包括网络运营挑战和解决方案，

虚拟环境中的负载均衡、流量整形和网络性能，创建合理的网络监控策略。

第 5 章：虚拟化管理和客户端安全 管理服务器和用于连接它们的客户端也可能是潜在的暴露点。该章描述的问题类型可能存在于各种供应商的组件中，并且概述配置选项和架构考虑因素，它们可被有效地用于创建更加安全的设施。而且，该章将概述 VMware、Microsoft 和 Citrix 用于某些特定企业用例的角色与权限。该章介绍的特定内容包括管理平台安全考虑，保护 VMware vCenter、Microsoft SCVMM 和 Citrix XenCenter，以及角色和权限用例。

第 6 章：保护虚拟机 在不影响生产环境的情况下，管理员能做什么以使他们的虚拟机更加安全？一些最大的安全缺陷来源于虚拟化产品自身的内部功能，因此，该章将深入一些细节，如在不为管理员创建其他运行开销的情况下，怎样更有效地保护 Microsoft、Citrix 和 VMware 虚拟机。该章介绍的特定内容包括安全考虑因素、威胁，虚拟机的缺陷以及锁定 VMware、Microsoft 和 Citrix 虚拟机。

第 7 章：日志和审计 虚拟化管理员需要确保虚拟机和虚拟基础设施组件都能产生日志。该章将概述一些最佳实践，虚拟化管理员可以按照这些最佳实践，确保他们能够获得故障诊断和安全、正确的日志信息，日志以尽可能有效的方式进行管理，在需要的时候日志可有效地用于审计和安全目的。该章介绍的特定内容包括为什么日志和审计很关键，虚拟日志和审计选项，与现有日志平台集成和有效的日志管理。

第 8 章：变更和配置管理 虚拟化可以极大地增强变更和配置管理实践，但这个通常需要改变现有过程和做事情的新方法。该章将描述一些不同的方法来将虚拟化集成到现有的工作流，创建新的（可能更有效的）策略、变更和配置管理过程的方法，以及有助于使这些关键操作过程更有效的虚拟化方法。该章介绍的特定内容包括变更和配置管理概述，虚拟机如何影响变更和配置管理，将虚拟化集成到变更管理，虚拟化配置管理的最佳实践，以及用虚拟化改进运营。

第 9 章：灾难恢复和业务连续性 虚拟化可以在灾难恢复（Disaster Recovery，DR）和业务连续性计划（Bussiness Continuity Planning，BCP）操作方面发挥巨大作用。该章将深入讨论一些优化 DR 和 BCP 过程的方法，创建更简单和更有效的 DR 和 BCP 工作流，同时减少成本。该章介绍的特定内容包括为 DR/BCP 使用虚拟化和私有云，以及改进 DR/BCP 的提示。

第 10 章：脚本使用提示和自动化技巧 总之，脚本可以通过多种方式使虚拟化管理员的管理变得简单。该章将概述脚本工具，它们可用于 VMware、Microsoft 和 Citrix 平台以完成特定运营和以安全为中心的任务。该章介绍的特定内容包括为什么脚本对于管理员是重要

的，虚拟化管理员的脚本类型，PowerShell 应用，在 VMware、Microsoft 和 Citrix 平台使用脚本，以及其他虚拟化脚本想法。

第 11 章：虚拟基础设施的其他安全考虑因素 该章将探索虚拟桌面基础设施（Virtual Desktop Infrastructure，VDI）、虚拟存储、应用程序虚拟化的若干关键安全考虑因素。该章介绍的特定内容包括 VDI 优点和缺点、VDI 架构及其安全利用、安全存储虚拟化，以及安全应用程序虚拟化。

硬件和软件要求

为了从本书中获得最大的益处，你应该有一个基于 VMware vSphere、Microsoft Hyper-V 或 Citrix XenServer 的虚拟基础设施。

本书中讨论的某些特性和功能可能依赖讨论的供应商的特定许可版本。在尝试配置你的基础设施之前，你应该检查当前有哪些许可功能！下面列出了 VMware、Microsoft 和 Citrix 的许可信息。

- VMware vSphere：www.vmware.com/products/datacenter-virtualization/vsphere/compare-editions.html
- Microsoft Hyper-V：www.microsoft.com/en-us/server-cloud/buy/pricing-licensing.aspx
- Citrix XenServer：www.citrix.com/English/ps2/products/subfeature.asp?contentID=2313292

如何使用本书

本书不需要从前到后顺序阅读，每个章节都包含你能立刻使用的特定信息。

如何联系作者

欢迎读者的反馈及对本书的改进意见。有任何反馈请通过 shackleford@voodoosec.com 联系笔者。

www.sybex.com/go/virtualizationsecurity 将提供其他内容和对本书的更新。

Acknowledgements 致　谢

我想感谢很多人，很多事，不仅仅是为这本书。对于许多技术人员或第一次出书的任何人，你真的希望列出所有帮助过你的人。对于我，那将是一份相当长的名单，因此我将仅列出一部分对我的生活和职业生涯有重要影响的人。

首先，感谢在我青年时期指导过我的老师们：Rose Bridgeman，她认为我可能是一位优秀的公众演讲者；Carol Lofgren（当我认识她的时候），她使在学校中学习拉丁语变成最酷的事情；Janet Weeks，她培养了我热爱学习和阅读美妙的文学，实际上当我需要一个朋友时，她帮我度过了一个艰难的时期。

感谢 Paul Janus，他给了我信念，帮助我完成从非技术性职业到技术职业的转型。他可能很久没有想起过我了，但他在早期对我影响很大。感谢 Herb Mattord，他雇佣了我，使我第一次接触企业的信息安全。感谢我的朋友 John Lampe，他是我认识和尊敬的第一个严肃的黑客，并且教会我做事情总是有不止一种方法。感谢我的朋友 Lara Dawson，很久以前，他让我走上了系统管理、审计、网络和安全的道路。感谢 Stephen Northcutt，他在早期指导了我很多知识，让我接触到了我最感兴趣的全球信息网络。还要感谢 SANS 所有的教师同事和整个团队。

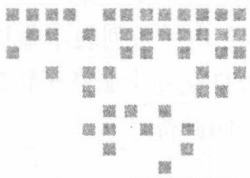
我的朋友 Chris Farrow 在我的职业生涯的关键点给我很多帮助——实际上，我接管了他的工作，事实证明这个过程是如此得跌宕起伏。Chris，如果你正在读这本书，你是我这些年来最好的朋友，非常感谢你为我所做的一切。

感谢 IANS 所有的朋友和同事，尤其是 Phil Gardner，他是一个非常棒的朋友。感谢我在 Voodoo 安全的非常好的客户——每次，你们总是使我能够尽全力做事。另一个需要感谢的人是 Robert Kiyosaki，他的书《富爸爸，穷爸爸》说服我在很久前开始购买房产，事实证明这是明智之举。

非常感谢 Sybex 的团队——Pete Gaughan、Mariann Barsolo、Rebecca Anderson、Connor O'Brien 和 Stef Jones，他们在编辑我的草稿时做了很多卓越的工作。感谢我的技术编辑 Steve Pate——你是一个很好的朋友和同事，这本书因为你的努力而变得更好。

最后我要感谢的当然是我的家庭。我的妻子 Karrie 和女儿 Mia，在过去的一年里遭受了我战士般的疯狂，让我所做的一切都值得。离开你们我不能做成任何事，我真心爱你们。

Contents 目　录



第 1 章 Chapter 1

虚拟化安全基础

虚拟化技术已经以多种形式存在许多年了，范围包括从主机上的逻辑分区到当今高度多样化的技术，如桌面、服务器和应用程序虚拟化。虚拟化的概念已深深地嵌入今天的数据中心，并将长期存在。然而，随着虚拟化技术的快速发展，出现了黑暗的一面，即安全风险。本章将探讨当今虚拟技术的基础，解释它代表的意思及各种活动部件如何一起工作。

然后，将探索虚拟化环境中的各种威胁，其中有一些迫在眉睫，有一些虽然偏理论化但仍值得一提。最后，我们将深入研究虚拟基础设施的安全环境变迁以及它怎样改变我们的做事方式。

本章是本书的其他部分的基础，并且是较理论化的内容。首先，为了明了我们为什么关心虚拟化安全，理解相关理论和概念是很有必要的。如果你是安全专家，这些概念对你来说都有点熟悉。如果你是一个管理员或工程师，则可能熟悉其中的一部分，但我猜想你更加关注的是把事情做好。在本章以后，本书重点将果断由“安全理论”转向实践。

在本章，你将学习到以下内容：

- ❑ 虚拟化架构。
- ❑ 虚拟化环境的威胁。
- ❑ 安全虚拟化环境的挑战。
- ❑ 虚拟化环境中脆弱性测试的挑战。

1.1 虚拟化架构

所有虚拟化的核心都是对物理硬件层计算资源的抽象。在服务器虚拟化领域中，主机是

底层服务器虚拟化平台，它将被用于向虚拟服务器提供虚拟硬件层。虚拟客户（通常也被称为虚拟机或 VM）由一系列表示虚拟服务器或系统的文件组成。这些文件在与主机软件和主机安装的底层硬件交互中服务于特定目的。虚拟机可直接安装在主机的本地存储设备上或一个及多个网络存储设备上。

一些术语定义

下面是本书中使用的术语：

主机 主机是运行系统管理软件的虚拟化平台。常见的主机平台包括 VMware ESXi、Microsoft Hyper-V、Citrix XenServer、Red Hat KVM 和其他。所有虚拟化系统都运行在这个主机管理程序平台之上。

虚拟客户、虚拟机、VM、客户系统 一个虚拟客户，通常称为虚拟机（Virtual Machine, VM），是任何运行在被抽象为一个虚拟模型环境的系统。VM 是一组文件，它代表一个基于硬件的计算平台，包括存储器、内存和配置组件。

虚拟服务器 许多虚拟化项目由虚拟化基于硬件的服务器开始。术语虚拟服务器常用于指代这些服务器。虚拟服务器真的只不过是一个特殊类型的虚拟机。

管理程序是服务器虚拟化平台的主要组件。通常被称为虚拟机监视器（Virtual Machine Monitor，VMM），管理程序是虚拟基础设施的中枢神经系统。它管理主机的底层硬件资源和处理所有由客户启动的操作系统（OS）和应用程序对 CPU、内存、I/O 和硬盘资源的请求。

目前有两种类型的管理程序：**类型 1 管理程序**根本上是独立的操作平台并直接安装在主机硬件上。由于这个原因，这些管理程序常被称为物理硬件管理程序。虚拟机运行在硬件“之上”的一层，允许通过系统管理软件完成更彻底的隔离。这种类型的管理程序的一个例子是 VMware 的 ESXi。这种类型的管理程序的例子如图 1.1 所示。

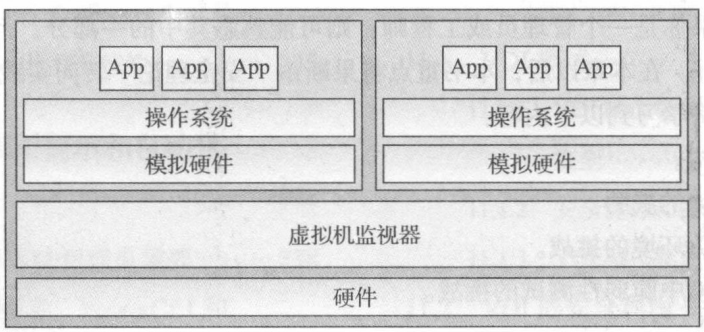


图 1.1 类型 I 管理程序

类型 2 管理程序是安装在现有操作系统平台上的应用程序，如图 1.2 所示。类型 2 管理程序的例子是 VMware 工作站。