

Cloud Security

A Comprehensive Guide to Secure Cloud Computing

云计算安全指南

Firewall

Switch

Web Server

LAN
Switch

[美] Ronald L. Krutz Russell Dean Vines 著
张立强 译



NLIC2970903780

- 洞悉云计算风险，掌控数据安全防护
- 创新解决方案，保证云计算成本效益
- 全面了解云计算关键特性，充分发挥其潜能



人民邮电出版社
POSTS & TELECOM PRESS

TURING

图灵程序设计丛书

Cloud Security

A Comprehensive Guide to Secure Cloud Computing

云计算安全指南

[美] Ronald L. Krutz Russell Dean Vines 著

张立强 译

Firewall

Switch

Web Server

LAN
Switch

Database
Server



NLIC2970903780

人民邮电出版社

北京

图书在版编目(CIP)数据

云计算安全指南 / (美) 克鲁兹 (Krutz, R. L.),
(美) 瓦因斯 (Vines, R. D.) 著; 张立强译. — 北京:
人民邮电出版社, 2013. 7

(图灵程序设计丛书)

书名原文: Cloud security: a comprehensive guide
to secure cloud computing

ISBN 978-7-115-32150-3

I. ①云… II. ①克… ②瓦… ③张… III. ①计算机
网络—安全技术—指南 IV. ①TP393.08-62

中国版本图书馆CIP数据核字(2013)第121938号

内 容 提 要

《云计算安全指南》全面分析了云计算的基础知识、架构、风险、安全原则, 致力于帮助大家发挥云计算的最大潜能, 在尽可能保证云中信息安全的情况下获得最大投资回报。作者依据其多年的专业知识与技能细致分析了数据所有权、隐私保护、数据机动性、服务质量与服务级别、带宽成本、数据防护、支持等主题, 给出了解决云计算安全难题的方法和方案。

本书适合各水平层次的云计算用户, 以及欲了解更多安全知识的专家、信息系统从业者和学生参考阅读。

-
- ◆ 著 [美] Ronald L. Krutz Russell Dean Vines
译 张立强
责任编辑 毛倩倩
执行编辑 朱 玲
责任印制 焦志伟
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京鑫正大印刷有限公司印刷
- ◆ 开本: 800×1000 1/16
印张: 16.25
字数: 394千字 2013年7月第1版
印数: 1—2 500册 2013年7月北京第1次印刷
- 著作权合同登记号 图字: 01-2010-6565号
-

定价: 69.00元

读者服务热线: (010)51095186转604 印装质量热线: (010)67129223

反盗版热线: (010)67171154

广告经营许可证: 京崇工商广字第 0021 号

版 权 声 明

All Rights Reserved. This translation published under license. Authorized translation from the English language edition, entitled *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, ISBN 978-0-470-58987-8, by Ronald L. Krutz, Russell Dean Vines, Published by John Wiley & Sons. No part of this book may be reproduced in any form without the written permission of the original copyrights holder.

Simplified Chinese translation edition published by POSTS & TELECOM PRESS Copyright © 2013.

本书简体中文版由John Wiley & Sons, Inc.授权人民邮电出版社独家出版。

本书封底贴有John Wiley & Sons, Inc.激光防伪标签，无标签者不得销售。

版权所有，侵权必究。

版权声明

我爱我的家人，他们是上帝给我的最好礼物。

——Ronald L. Krutz

献给 Elzy，从今时到永远。

——Russell Dean Vines

致 谢

我想感谢我的妻子 Hilda，感谢她在我写作期间的支持与鼓励。

——Ronald L. Krutz

首先，对 Gotham Technology Group 的全体成员表示由衷的感谢，并特别感谢 Ken Phelan、Joe Jessen 和 Nancy Rand 所提供的无私帮助。我还要感谢 Paul M. Pellicci 和 Lawrence Levin 医生给予我健康。最最感谢我的妻子 Elzy，感谢她持续而坚定地支持我。

——Russell Dean Vines

在此，我们要感谢 John Wiley & Sons 的 Carol Long 和 Ed Connor 就本书提供的所有支持与帮助。

序

遇到一些新生事物时，我们通常都会去尝试了解它们，而根据经验寻找一些类似情况是了解新生事物的很好方式。不过，这种方式有时比较有效，有时却帮不上忙。

计算机安全就长期受限于人们对实体安全的经验。人们总是想当然地认为，几千年来确保实物财产安全的经验同样适用于确保数字财产安全。

因此，计算机安全中的很多理念都与如何将重要的数据放在一个安全区域，然后对该安全区域的访问进行控制有关。我现在还能清晰地回忆起 PC 网络刚兴起时与一个安全专家的对话。我问他如何确保 PC 上的数据安全，他说：“很简单，把数据存储在 PC 中，把 PC 放在一个保险箱中，然后把保险箱置于大海深处。”

多年来，我们一直在寻找一个支持访问控制的安全场所。在风险无处不在的世界中，在我们的组织内部都存在安全风险，我们甚至难以断定“安全”的真正含义。

如今，这种实体安全的经验越来越不管用了。相信我们都曾经看过剧情围绕某份重要数据展开的电影或电视剧。例如，恐怖分子袭击的下一个目标存储在一个 U 盘中，U 盘被盗或损坏，剧情因此跌宕起伏。这根本就不是数据的本质。数据是像病毒一样可传播的。数据从哪里来？它压根就没有存储在硬盘上？没有人就这次袭击向别人发送电子邮件进行告知？是否有人可以用这一 U 盘中的数据制作一个 YouTube 视频来告诉所有人？

进入云计算时代，实体世界中残存的最后一点经验也被一举抛弃。我们需要采用新的方式来了解数据的存取和验证——也许是本来就应该采用的一种理解方式。我们需要将数据安全理解为一种新的东西，需要采用新的和有创意的解决方案。

也许，信息安全专家目前正经受这种挑战。尽管增加了安全方面的投入，但公司却普遍发现目前的安全情况还不如五年前。安全工具与安全技术的发展没有跟上风险和攻击的步伐。当虚拟化和灵活性等需求驱使数据资产迁移到云中时，安全社区如何应对这些日益增长的威胁？

有一件事情我们可以肯定：安全不会主导这种变革。云计算能够降低成本和提高灵活性，任何需要这些优势的业务需求最终都将会占据支配地位。一直以来，安全专家都在尝试减缓一些技术的创新发展以试图控制风险。我们立时便可想到电子邮件、即时通信和 Web 浏览先后遭遇的处境。然而，基于以往的经验，实施适当的控制通常都会比简单地阻止这些创新要好得多。

作为安全专业人员，在数据安全和完整性方面谋求创新是我们的职责。我们需要工具和流程来认识数据的短暂性本质，并意识到未来在物理区域控制数据是不可行的。经过努力，我们可以得到适用于云计算的、尽可能消除风险的安全模型。我们不需要放弃安全，只需放弃一些陈腐的旧观念。

本书就会告诉大家怎么做。作为安全专业人员，我们可能不希望拥抱云，但是我们必须学着与云共处。

——Ken Phelan

CTO, Gotham Technology Group

前 言

云计算让你能够按照可计量的方式来使用计算资源和存储资源，能够降低组织在计算基础设施方面的投入成本。在物理硬件上运行的虚拟机可以动态地增容和降容，并由虚拟机监控器（hypervisor）进行控制。这是一种成本效率高、灵活性好的计算范式。

另外，将经过处理的海量数据（如健康记录）进行集成和广泛利用，对于研究者和业内用户而言有很大好处。

然而，和任何技术一样，若不了解云计算的能力、脆弱性、优势和利弊权衡，便不可能充分发挥其潜力。本书对这些领域进行了深入分析，介绍了在尽可能降低风险的情况下最充分发挥云计算优势的方法。

本书及技术概述

虽然云计算具有很多优势，但是云的规模、结构以及地域分散性等特点引发了人们对于云中数据安全与隐私的担忧。人们的忧虑涉及如下几个方面：

- ❑ 运行在同一台服务器上不同虚拟机之间的数据被泄露和非授权访问；
- ❑ 云服务提供商不能对敏感信息提供正确的处理和防护；
- ❑ 未经征求客户意见或未经客户认可，云服务提供商就向政府部门或执法机构提供关键的、敏感的用户数据；
- ❑ 不能满足合规性需求；
- ❑ 系统发生故障或宕机，导致云服务在较长时间内不可用；
- ❑ 黑客攻击位于云中的用户应用程序，获取并分发敏感信息；
- ❑ 云服务提供商设置的安全防护的健壮性；
- ❑ 云支持互操作的程度（互操作用于使用户在不同云服务提供商之间迁移用户应用程序，避免被厂商锁定）。

云用户还需要关注一下自身数据在较长一段时间内的可用性，以及云服务提供商是否会不正当地为了一己私利利用其敏感数据。

加密是一种对云中数据进行防护的方法。加密之后，云服务提供商和黑客不能得知数据内容，但是这会增加数据的检索和计算难度。

本书对这些问题进行了阐述，并详述了如何避免云计算的负面影响，以便你在不损害信息安

全的情况下用云取得最大投资回报。

本书内容

本书介绍了云计算的关键特性，包括可扩展性、灵活性、虚拟化、自动化、计费服务和普适网络连接，同时也介绍了这些特性与安全云计算的关系。

本书的章节安排如下：首先介绍云范式的演变，然后介绍设计架构特性、安全基础、云计算风险与威胁，最后介绍实现安全云计算的有效步骤。

第 1 章“云计算基础”定义了云计算，介绍了各种云计算应用观点以及云计算对计算领域的影响。接下来，这一章介绍了云计算的基础特性，并从历史架构影响、技术影响和运行影响等侧面建立了人们目前对云计算的认知。

第 2 章“云计算架构”采用各种基于云的计算架构模型介绍云计算架构的主要组成部分。在这一章我们将会介绍云交付模型（SPI 架构的 SaaS、PaaS 和 IaaS）、云部署模型（私有云、社区云、公有云和混合云），并介绍其他一些云架构模型（如 Jericho 云立方）。

第 3 章“云计算软件安全基础”介绍了云计算软件安全的基础概念，包括云安全服务、云安全原则、安全软件需求和测试理念。接下来，这一章介绍云业务连续性规划、灾难恢复、备份以及安全远程访问。

第 4 章“云计算的安全风险”详细介绍了云计算的安全风险与威胁。我们将会介绍云计算在隐私确保和合规性方面的风险，相对于“传统”数据风险、身份风险和访问控制风险而言云如何带来特殊的风险，以及为何说这些风险和威胁对于云服务提供商而言是独特的。

第 5 章“云计算的安全挑战”介绍身份管理挑战与机遇。安全管理必须能够判断具备哪些检测性与防御性的控制来清晰描绘组织的安全态势，特别是那些与虚拟化边界相关的安全态势。我们将会介绍安全策略和计算机入侵检测与响应技术，并深入探讨虚拟化安全管理问题。

第 6 章“云计算安全架构”介绍重要的云计算安全架构问题，包括可信云计算、安全执行环境和微架构。接下来，这一章对身份管理与访问控制等关键云安全原则进行扩展介绍，探讨自治系统和自主防御机制。

第 7 章“云计算生命周期议题”介绍云生命周期问题、重要的标准、事件响应方法、加密等内容，并探讨了云中虚拟机与应用安全下线。

第 8 章“实用的后续步骤与方法”概括重要的云计算安全理念，并就应该将哪些服务迁移到云中、哪些不能迁移到云中给出指导性意见。接下来，这一章介绍了目标用户会向云服务提供商提出的问题，并列出了在云应用、标准和互操作性方面提供支持与信息交流的组织。最后，这一章给出了着手云计算的建议和 10 个重要的相关考虑因素。

目标读者

本书作为一个宝贵的信息源，既面向那些尝试使用云计算的入门用户，也面向已深入体验和

了解云计算的专业人士。本书介绍了云计算的发展背景，详述了确保云计算安全的关键方法，这些方法能够对那些最适合云计算的应用产生影响。

我们认为本书适用于以下人士：

- 信息技术领域或信息系统安全领域的专业人士；
- 信息安全审计专家；
- 信息系统 IT 从业人员；
- 计算机或信息系统管理人员；
- 想要了解云计算相关的各类安全元素的高级管理人员；
- 参加信息系统安全认证或学习计算机安全的学生。

小结

我们希望本书作为那些关注云计算风险和数据安全防护者的参考书，能够为其提供帮助和良好的阅读体验。

要想尽可能地降低风险、实现云计算的最大利益化，你必须攻克数据所有权、隐私保护、数据机动性、服务质量与服务级别、带宽成本、数据防护等一系列难题。

当你置身于云计算中，想从布满雷区的安全迷宫中找寻出路时，请一定阅读本书。

目 录

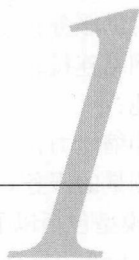
第 1 章 云计算基础.....1	第 2 章 云计算架构25
1.1 什么是云计算.....1	2.1 云计算的交付模型25
1.1.1 云计算不是什么.....5	2.1.1 SPI 框架25
1.1.2 其他观点.....6	2.1.2 软件即服务 (SaaS)28
1.2 基本特征.....7	2.1.3 平台即服务 (PaaS)29
1.2.1 按需自助服务.....7	2.1.4 基础设施即服务 (IaaS)31
1.2.2 宽带网络连接.....7	2.2 云计算的部署模型32
1.2.3 位置无关资源池.....7	2.2.1 公共云.....33
1.2.4 快速伸缩能力.....8	2.2.2 社区云.....34
1.2.5 可被测量的服务.....8	2.2.3 私有云.....35
1.3 架构的影响.....8	2.2.4 混合云.....36
1.3.1 高性能计算.....8	2.2.5 其他部署模型.....37
1.3.2 公用计算与企业网格计算.....10	2.3 预期的优势.....41
1.3.3 自治计算.....11	2.3.1 灵活性和可靠性.....42
1.3.4 服务整合.....11	2.3.2 降低成本.....42
1.3.5 水平扩展.....12	2.3.3 数据存储集中化.....43
1.3.6 Web 服务.....12	2.3.4 缩短部署周期.....43
1.3.7 高扩展性架构.....13	2.3.5 可扩展性.....43
1.4 技术的影响.....13	2.4 小结.....43
1.4.1 随时随地上网.....13	2.5 参考资料.....44
1.4.2 商品化.....14	
1.4.3 超额产能.....15	第 3 章 云计算软件安全基础.....45
1.4.4 开源软件.....15	3.1 云的信息安全目标46
1.4.5 虚拟化.....16	3.2 云安全服务.....47
1.5 运维的影响.....17	3.2.1 认证.....47
1.5.1 整合.....17	3.2.2 授权.....47
1.5.2 外包.....19	3.2.3 审计.....47
1.5.3 IT 服务管理.....22	3.2.4 可追究性.....48
1.5.4 自动化.....22	3.3 相关的云安全设计原则.....49
1.6 小结.....23	3.3.1 最小特权.....49
1.7 参考资料.....23	

3.3.2 权限分离	49	第5章 云计算的安全挑战	108
3.3.3 深度防御	50	5.1 实施安全策略	108
3.3.4 故障保护	50	5.1.1 策略类型	109
3.3.5 机制的经济性	50	5.1.2 计算机安全事件响应团队	110
3.3.6 完全仲裁	51	5.2 虚拟化安全管理	111
3.3.7 开放设计	51	5.2.1 虚拟化的安全威胁	112
3.3.8 最小公共机制	51	5.2.2 虚拟机的安全忠告	117
3.3.9 心理可接受性	51	5.2.3 虚拟机相关的安全技术	120
3.3.10 最弱链接	51	5.3 小结	123
3.3.11 利用现有组件	52	5.4 参考资料	124
3.4 安全云软件需求	52	第6章 云计算安全架构	125
3.4.1 安全开发实践	52	6.1 架构上的考虑	125
3.4.2 云软件需求工程方法	54	6.1.1 基本问题	125
3.4.3 云安全策略的实现和分解	58	6.1.2 可信云计算	132
3.4.4 NIST 33 安全原则	63	6.1.3 安全执行环境与安全通信	134
3.5 安全云软件测试	63	6.1.4 微体系结构	143
3.5.1 安全质量确保性测试	64	6.2 身份管理与访问控制	144
3.5.2 云渗透测试	71	6.2.1 身份管理	145
3.5.3 回归测试	80	6.2.2 访问控制	148
3.6 云计算与业务连续性规划/灾难恢复	81	6.3 自治安全	150
3.6.1 定义	81	6.3.1 自治系统	150
3.6.2 总体目标和实践	82	6.3.2 自治防护	151
3.6.3 使用云进行 BCP/DRP	85	6.3.3 自我修复	151
3.7 小结	86	6.4 小结	152
3.8 参考资料	87	6.5 参考资料	152
第4章 云计算的安全风险	89	第7章 云计算生命周期议题	153
4.1 CIA 三元组	89	7.1 标准	153
4.1.1 机密性	89	7.1.1 Jericho 论坛	153
4.1.2 完整性	89	7.1.2 分布式管理任务组	154
4.1.3 可用性	90	7.1.3 国际标准化组织	155
4.1.4 其他重要概念	90	7.1.4 欧洲电信标准研究院	159
4.2 隐私与一致性风险	90	7.1.5 结构化信息标准促进组织	159
4.3 基础设施、数据、访问控制的安全		7.1.6 网络存储工业协会	159
威胁	100	7.1.7 开放网格论坛	160
4.3.1 常见威胁与漏洞	100	7.1.8 开放 Web 应用安全项目	160
4.3.2 云访问控制问题	103	7.2 事故响应	163
4.4 云服务提供商威胁	104		
4.5 小结	106		
4.6 参考资料	107		

7.2.1	NIST SP 800-61	164	8.1.1	什么样的服务要迁移到云中	182
7.2.2	互联网工程任务组应急处理 指南	166	8.1.2	应该向云服务提供商咨询 哪些问题	183
7.2.3	分层安全与入侵检测系统	167	8.1.3	何时应该使用公有云、私 有云和混合云	184
7.2.4	计算机安全与应急响应团队	171	8.2	获取帮助	185
7.2.5	安全事件通知流程	172	8.2.1	云安全联盟	185
7.2.6	自动化通知与恢复机制	173	8.2.2	云计算谷歌用户组	186
7.3	加密与密钥管理	173	8.2.3	云计算互操作论坛	187
7.3.1	虚拟机架构	174	8.2.4	开放云联盟	187
7.3.2	密钥防护对策	174	8.3	准备开始	188
7.3.3	硬件防护	175	8.3.1	最重要的 10 个关键点	188
7.3.4	基于软件的防护	176	8.3.2	赠言	195
7.3.5	重复数据删除	176	8.4	参考资料	195
7.4	报废	177	附录 A	术语表和缩略词	196
7.5	小结	180	附录 B	参考文献	239
7.6	参考资料	181	索引		242
第 8 章	实用的后续步骤与方法	182			
8.1	获取答案	182			

第1章

云计算基础



极度的简洁脱胎于极度的复杂。

——温斯顿·丘吉尔

不同的人对云计算有着不同的理解。对有些人而言，云计算是指通过“云”所表示的因特网或某种网络来访问软件、存储数据和使用相关的服务。对另外一些人而言，云计算根本就不是什么新事物，它实际上就是20世纪60年代广泛采用的分时模型的现代版本。后来，随着计算平台的成本不断降低，计算模型逐渐演变为客户机/服务器模型，随后又演变为个人计算机，用户台式机具有了较强的计算能力，导致分时系统慢慢地淡出了人们的视线。

1961年，MIT的教授John McCarthy提出将计算资源作为像电力一样的基础设施^[1]。另外一名先驱是J.C.R. Licklider，他后来开发了ARPANET的基础，也就是因特网的前身。20世纪60年代，还在打孔卡片和批处理流行的时代，在美国国防部高级研究计划局和进行高科技研发的BBN公司任职的Licklider就提出了网络化计算机的观点。他指出：如果我初步设想中的网络可以投入运行的话，我们将会拥有至少4台大型计算机，也许6台或者8台小型计算机，以及大量的磁盘文件和磁带设备，更不用说许多远程控制台和电传打字站了，它们都能连在一起共同工作^[2]。

公用计算与普适互联网络概念的结合，为云计算未来的发展奠定了基础。

1.1 什么是云计算

2009年10月，美国国家标准和技术局（NIST）信息技术实验室的Peter Mell和Tim Grance在一篇题为“Effectively and Securely Using the Cloud Computing Paradigm”^[3]（安全有效地使用云范式）的演示文稿中对云计算做了如下定义：

云计算是一种模型，能支持便捷地按需通过网络访问一个可配置的共享计算资源池（包括网络、服务器、存储、应用程序、服务），共享池中的资源能够以最少的用户管理投入或最少的服务提供商互动实现快速供给和回收。

云模型有5个基本特征、3个服务模型和4个部署模型。其中, 5个基本特征包括:

- 按需自助服务;
- 普适网络连接;
- 资源池;
- 快速伸缩能力;
- 可被测量的服务。

3个服务模型包括以下几项。

- SaaS (Software as a Service, 软件即服务): 通过网络使用提供商的应用程序。
- PaaS (Platform as a Service, 平台即服务): 将用户创建的应用程序部署到云中。
- IaaS (Infrastructure as a Service, 基础设施即服务): 租赁处理能力、存储能力、网络带宽以及其他基础计算资源。

美国国家标准和技术局总结的部署模型(包括内部实现和外部实现的)包括以下几项。

- 私有云 (private cloud): 企业建立或租用的云。
- 社区云 (community cloud): 为某个特定社区所建立的共享基础设施。
- 公共云 (public cloud): 面向大众的超大规模基础设施。
- 混合云 (hybrid cloud): 两个以上云的组合。

这些基本特征和模型将会在第2章详细介绍。

2009年, 为了促进云计算服务供应的应用实践, IBM、英特尔和谷歌等公司发表了“开放云宣言”(www.opencloudmanifesto.org)。在该宣言中, 云计算被赋予的特征包括以下几项。

- 具备以较高成本效率动态地调整并提供计算资源的能力。
 - 能够让消费者(最终用户、组织或IT职员)最大限度地利用资源而无须应对底层复杂的技术。
 - 云架构自身可以是私有的(位于某组织的防火墙内部), 也可以是公用的(位于因特网上)。
- 该宣言中列出的价值主张包括如下几点。

- **按需扩展** 所有的企业都要应对各自环境的变化。云计算解决方案的一大优势在于规模的灵活性。如果企业在某些时期对计算资源的需求急剧增加或降低, 那么云计算技术(无论是私有云还是公共云)都可以应对这些变化。
- **精简数据中心** 无论企业的规模大小如何, 都需要对企业的数据中心进行大量的投资。这些投资包括购买与维护相关的软硬件、提供容纳这些硬件的基础设施, 以及雇用相关技术人员负责数据中心的运维。企业可以通过在内部建立私有云, 或者将数据中心外包给公共云的方式, 精简数据中心。
- **改善业务流程** 云为改善业务流程提供了基础设施。企业及其供应商、合作伙伴可以在云上共享数据和应用程序, 让参与其中的每个人把焦点都放到业务流程上, 而不是放到承载业务流程的基础设施上。
- **最大程度降低创业成本** 对于刚起步的公司、新兴市场上的各类组织, 甚至是大型机构的重点科研部门, 云计算都可以大幅降低初始建设成本。新企业可以在基础设施皆已到

位的状态下启动，从而将建设数据中心所要花费的时间与其他资源负担转移给云服务提供商，不管是公共云还是私有云。

Dave Malcolm Surgient在ZDNet上所发表的“云计算的5个界定特征”(http://news.zdnet.com/2100-9595_22-287001.html)一文中从不同的角度阐述了云计算的5个界定特征，具体如下。

- **动态计算基础设施** 云计算具有标准化的、可扩展的、动态的、虚拟化的、安全的物理基础设施，通过不同级别的冗余实现高可用性。
- **以IT服务为中心的方法** 与服务器为中心的模型不同，云计算能够给应用程序或服务提供一个易于访问的专有实例。
- **基于自助服务的使用模型** 云计算具有针对业务服务提供按需上传、构建、部署、调度、管理和报告的能力。
- **自主管理平台** 通过下列软件的自动化实现自主管理。
 - 供给引擎：实现服务的部署和撤销，对资源进行回收以实现较高层次的资源重用。
 - 调度与保留资源的机制。
 - 配置、管理和报告功能：确保针对多组用户的资源分配与再分配。
 - 资源访问控制机制：包括控制资源访问的工具和确保资源如何使用以及操作如何执行的策略。
- **按使用量计费** 用户根据他们所使用的资源量支付费用。

影响云计算发展的重要因素

云计算的出现是由很多相关因素推动的，包括软件互操作性标准、虚拟化技术、高带宽通信、企业应用程序的交付模型以及Web 2.0等。

Web 2.0是一个专用术语，指Web设计从传统的静态页面转换为交互式的动态传输机制，它被看做一个取代桌面计算机应用的软件运行平台。通常，人们认为O'Reilly Media公司创始人Tim O'Reilly是“Web 2.0”一词的发明者。Web 2.0的相关特征如下。

- 使用异步JavaScript和XML (Ajax);
- 一些不同来源的服务组合成一个新的服务 (mashup);
- 免费的Web服务;
- 简易信息聚合的应用 (RSS);
- 社交网络;
- 交互式词典和百科全书;
- 博客;
- 协同应用;
- 复杂游戏;
- 维基百科和其他维基站点;
- 优化的搜索引擎。