

<<云计算安全指南>>

图书基本信息

书名：<<云计算安全指南>>

13位ISBN编号：9787115321503

10位ISBN编号：7115321507

出版时间：2013-6

出版时间：人民邮电出版社

作者：[美] Ronald L. Krutz,[美] Russell Dean Vines

译者：张立强

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<云计算安全指南>>

内容概要

把计算机当做接入口，一切都交给互联网吧！

最大程度地降低成本，最大程度地享受服务，云计算就是要将各种IT资源以服务的方式通过互联网交付给用户，这包括但不限于计算资源、存储资源、软件开发、系统测试、系统维护和各种丰富的应用服务，它们都将像水和电一样方便使用，并可按量计费。

然而，处身云中，我们如何确保数据安全与隐私保护呢？

《云计算安全指南》全面探讨云的基础知识、架构、风险、安全原则，让我们不仅了解其灵活性、高效性、经济实用性，而且充分认识其脆弱性并学会补救方法。

两位知名的安全专家Ronald L. Krutz和Russell Dean Vines将带你攻克数据所有权、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、支持等难题，帮助你保证信息安全并通过云计算获得最大的投资回报。

如果你身处云中，本书将引领你走出布满雷区的安全迷宫！

<<云计算安全指南>>

作者简介

作者简介：

Ronald L. Krutz

高级信息系统安全顾问，电子与计算机工程学博士，有30余年信息安全保障方法、信息安全培训、分布式计算系统、计算机体系结构、实时系统方面的从业经验，独立或与他人合著图书十余部。

另外，他还是Wiley信息安全认证系列图书的编辑顾问、纽黑文大学杰出的客座讲师、美国米德威学院兼职教授、宾夕法尼亚州注册工程师。

Russell Dean Vines

CISSP（国际注册信息系统安全专家）、CEH（认证道德黑客）、CISM（注册信息安全经理）、支付卡行业QSA（合格安全性评估人），通过了CompTIA Security+认证。

他置身信息系统行业20余年，参与著作十余本，是亚马逊名列前茅的畅销书作者，在面向各种人群传播复杂的安全知识方面具备独有的天赋，常在Comdex和Networld+Interop等行业活动中发表演讲。

译者简介：

张立强

博士，武汉大学计算机学院、软件工程国家重点实验室讲师，从事信息安全与软件工程方面的科研与教学工作，研究方向为可信云计算、软件安全工程等。

<<云计算安全指南>>

书籍目录

目 录

第1章 云计算基础	1	
1.1 什么是云计算	1	
1.1.1 云计算不是什么	5	
1.1.2 其他观点	6	
1.2 基本特征	7	
1.2.1 按需自助服务	7	
1.2.2 宽带网络连接	7	
1.2.3 位置无关资源池	7	
1.2.4 快速伸缩能力	8	
1.2.5 可被测量的服务	8	
1.3 架构的影响	8	
1.3.1 高性能计算	8	
1.3.2 公用计算与企业网格计算	10	
1.3.3 自治计算	11	
1.3.4 服务整合	11	
1.3.5 水平扩展	12	
1.3.6 Web服务	12	
1.3.7 高扩展性架构	13	
1.4 技术的影响	13	
1.4.1 随时随地上网	13	
1.4.2 商品化	14	
1.4.3 超额产能	15	
1.4.4 开源软件	15	
1.4.5 虚拟化	16	
1.5 运维的影响	17	
1.5.1 整合	17	
1.5.2 外包	19	
1.5.3 IT服务管理	22	
1.5.4 自动化	22	
1.6 小结	23	
1.7 参考资料	23	
第2章 云计算架构	25	
2.1 云计算的交付模型	25	
2.1.1 SPI框架	25	
2.1.2 软件即服务 (SaaS)	28	
2.1.3 平台即服务 (PaaS)	29	
2.1.4 基础设施即服务 (IaaS)	31	
2.2 云计算的部署模型	32	
2.2.1 公共云	33	
2.2.2 社区云	34	
2.2.3 私有云	35	
2.2.4 混合云	36	
2.2.5 其他部署模型	37	
2.3 预期的优势	41	

<<云计算安全指南>>

2.3.1	灵活性和可靠性	42
2.3.2	降低成本	42
2.3.3	数据存储集中化	43
2.3.4	缩短部署周期	43
2.3.5	可扩展性	43
2.4	小结	43
2.5	参考资料	44
第3章	云计算软件安全基础	45
3.1	云的信息安全目标	46
3.2	云安全服务	47
3.2.1	认证	47
3.2.2	授权	47
3.2.3	审计	47
3.2.4	可追究性	48
3.3	相关的云安全设计原则	49
3.3.1	最小特权	49
3.3.2	权限分离	49
3.3.3	深度防御	50
3.3.4	故障保护	50
3.3.5	机制的经济性	50
3.3.6	完全仲裁	51
3.3.7	开放设计	51
3.3.8	最小公共机制	51
3.3.9	心理可接受性	51
3.3.10	最弱链接	51
3.3.11	利用现有组件	52
3.4	安全云软件需求	52
3.4.1	安全开发实践	52
3.4.2	云软件需求工程方法	54
3.4.3	云安全策略的实现和分解	58
3.4.4	NIST 33安全原则	63
3.5	安全云软件测试	63
3.5.1	安全质量确保性测试	64
3.5.2	云渗透测试	71
3.5.3	回归测试	80
3.6	云计算与业务连续性规划/灾难恢复	81
3.6.1	定义	81
3.6.2	总体目标和实践	82
3.6.3	使用云进行BCP/DRP	85
3.7	小结	86
3.8	参考资料	87
第4章	云计算的安全风险	89
4.1	CIA三元组	89
4.1.1	机密性	89
4.1.2	完整性	89
4.1.3	可用性	90
4.1.4	其他重要概念	90

<<云计算安全指南>>

4.2	隐私与一致性风险	90	
4.3	基础设施、数据、访问控制的安全威胁	100	
4.3.1	常见威胁与漏洞	100	
4.3.2	云访问控制问题	103	
4.4	云服务提供商威胁	104	
4.5	小结	106	
4.6	参考资料	107	
第5章	云计算的安全挑战	108	
5.1	实施安全策略	108	
5.1.1	策略类型	109	
5.1.2	计算机安全事件响应团队	110	
5.2	虚拟化安全管理	111	
5.2.1	虚拟化的安全威胁	112	
5.2.2	虚拟机的安全忠告	117	
5.2.3	虚拟机相关的安全技术	120	
5.3	小结	123	
5.4	参考资料	124	
第6章	云计算安全架构	125	
6.1	架构上的考虑	125	
6.1.1	基本问题	125	
6.1.2	可信云计算	132	
6.1.3	安全执行环境与安全通信	134	
6.1.4	微体系结构	143	
6.2	身份管理与访问控制	144	
6.2.1	身份管理	145	
6.2.2	访问控制	148	
6.3	自治安全	150	
6.3.1	自治系统	150	
6.3.2	自治防护	151	
6.3.3	自我修复	151	
6.4	小结	152	
6.5	参考资料	152	
第7章	云计算生命周期议题	153	
7.1	标准	153	
7.1.1	Jericho论坛	153	
7.1.2	分布式管理任务组	154	
7.1.3	国际标准化组织	155	
7.1.4	欧洲电信标准研究院	159	
7.1.5	结构化信息标准促进组织	159	
7.1.6	网络存储工业协会	159	
7.1.7	开放网格论坛	160	
7.1.8	开放Web应用安全项目	160	
7.2	事故响应	163	
7.2.1	NIST SP 800-61	164	
7.2.2	互联网工程任务组应急处理指南	166	
7.2.3	分层安全与入侵检测系统	167	
7.2.4	计算机安全与应急响应团队	171	

<<云计算安全指南>>

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

<<云计算安全指南>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>