
云计算概要和建议

国家标准和技术研究所的建议

内部资料

翻译：高卓

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

计算机安全

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

2012 年 5 月



美国商务部
代部长：John Bryson

国家标准和技术研究所
商务部副部长兼所长：Patrick D. Gallagher

北京江南天安科技有限公司

目录

执行摘要

1 介绍

- 1.1 权限
- 1.2 目的和适用范围
- 1.3 适用对象
- 1.4 篇章结构

2 云计算定义

3 典型的商业服务条款

- 3.1 承诺
- 3.2 限制
- 3.3 义务
- 3.4 建议

4 云环境总论

- 4.1 究竟由谁控制云中资源
- 4.2 本地私有云场景
- 4.3 外包私有云场景
- 4.4 本地社区云场景
- 4.5 外包社区云场景
- 4.6 公共云场景
- 4.7 混合云场景

5. 软件即服务云环境

- 5.1 抽象交互动力学
- 5.2 软件栈和供应商/消费者的控制范围
- 5.3 好处
 - 5.3.1 软件工具的内存占用量极低
 - 5.3.2 有效使用软件许可证
 - 5.3.3 集中化管理数据
 - 5.3.4 供应商负责管理平台
 - 5.3.5 节约前期成本
- 5.4 问题和隐忧
 - 5.4.1 基于浏览器的风险和风险治理
 - 5.4.2 网络依赖
 - 5.4.3 SaaS 云之间缺乏可转移性
 - 5.4.4 隔离与效率（安全与成本权衡）
- 5.5 候选应用类别
- 5.6 软件即服务建议

6. 平台即服务云环境

- 6.1 抽象交互动力学
- 6.2 软件栈和供应商/消费者的控制范围
- 6.3 好处

- 6.3.1 简便的可伸缩应用开发和部署
- 6.4 问题和隐忧
 - 6.4.1 PaaS 云之间缺乏可转移性
 - 6.4.2 基于事件的处理程序时序安排
 - 6.4.3 PaaS 应用的安全工程
- 6.5 候选应用类别
- 6.6 平台即服务建议
- 7. 基础设施即服务云环境**
 - 7.1 抽象交互动力学
 - 7.2 软件栈和供应商/消费者的控制范围
 - 7.3 运行
 - 7.3.1 云管理器的运行
 - 7.3.2 集群管理器的运行
 - 7.3.3 计算机管理器的运行
 - 7.4 好处
 - 7.4.1 通过虚拟机管理访问权全面控制计算资源
 - 7.4.2 灵活高效的计算硬件租用
 - 7.4.3 与老旧应用的可转移性和互操作性
 - 7.5 问题和隐忧
 - 7.5.1 老旧安全漏洞
 - 7.5.2 虚拟机泛滥
 - 7.5.3 验证 IaaS 云供应商网站的真实性
 - 7.5.4 虚拟机层面隔离的力度
 - 7.5.5 提供隔离的动态网络配置性能
 - 7.5.6 数据抹除
 - 7.6 基础设施即服务建议
- 8. 有待解决的问题**
 - 8.1 计算性能
 - 8.1.1 延时
 - 8.1.2 脱机数据同步
 - 8.1.3 可伸缩的编程
 - 8.1.4 数据存储管理
 - 8.2 云的可靠性
 - 8.2.1 网络依赖
 - 8.2.2 云供应商停机
 - 8.2.3 安全关键系统
 - 8.3 经济目的
 - 8.3.1 业务连续性风险
 - 8.3.2 服务协议评估
 - 8.3.3 工作负荷的可转移性
 - 8.3.4 云供应商之间的互操作性
 - 8.3.5 灾害恢复
 - 8.4 合规

- 8.4.1 缺乏可见度
- 8.4.2 数据的物理位置
- 8.4.3 司法管辖权和法规
- 8.4.4 支持取证
- 8.5 信息安全
 - 8.5.1 意外数据泄露风险
 - 8.5.2 数据隐私
 - 8.5.3 系统完整性
 - 8.5.4 多租户
 - 8.5.5 浏览器
 - 8.5.6 信任的硬件支持
 - 8.5.7 密钥管理

9. 一般性建议

- 9.1 管理
- 9.2 数据治理
- 9.3 安全性和可靠性
- 9.4 虚拟机
- 9.5 软件和应用

附录 A 角色和责任

附录 B 缩略语

附录 C 术语表

附录 D 参考文献

附录 E 相关 NIST 出版物