

采购云方案前的十大注意事项

Anthony Kelly

Erick Trombley

David DeBrandt

Carina Veksler

2015 年 1 月

目标:

云计算能够帮助公共部门以更低成本快速灵活地获取 IT 资源。各机构能够根据自身设计思路与 IT 部门运营方式配置与需求相符的计算资源类型与规模,从而摆脱沉重的前期投入压力。作为此项举措的重要组成部分,云计算还带来了新的机遇,允许我们对现有采购策略加以重新评估,旨在建立一套速度更快、更为灵活且能够充分发挥云规模效应与灵活性优势的采纳流程。云服务的采用与公共部门以往所熟知的传统技术采购有所区别,且我们必须着眼于其中的诸多关键元素,通过基础设施改进以及系统层面的创新性功能强化实现云成本降低与性能提升。

在以下十项云方案采购注意事项当中,我们将共同探讨公共部门云发展战略中需要考量的各项关键因素。这些注意事项源自 AWS 的多年实践经验,相信能够帮助大家更为有理有据且安全可靠地建立起自己的大规模全球化基础设施。

1. 在着手之前考虑如何发挥云技术的全部潜能

作为成功云战略中的一大关键性元素,我们应当尽早将各主要相关方引入实施流程(包括采购、法务、预算/财务、安全、IT 以及业务部门负责人)。这将确保组织始终对云采用给现有实践的影响保持清晰的认知。能够建立成功云采购策略的组织往往会在早期专注于构建服务快速实现机制,同时消除一切可能障碍充分发挥云技术优势的采购复杂性或者不相关进程。具体障碍将在以下几项论点中具体探讨。需要强调的是,大多数传统方案要求、方法及术语在云计算服务领域并无意义,因此组织应当在设计采购策略时考虑到云技术的特殊性。

2. 避免采取过度规范化的要求

成功的云采购策略专注于整体应用层面及基于性能的实际要求。其不应在此类要求当中引入过多特定方法、硬件及设备约束。大家应当意识到,云技术的采购工作应作为一类商用产品(将在后文中具体讨论),整个实施过程则须利用云服务供应商建立的商业最佳实践以支持数据中心运营。采购活动不应指定过于具体的设备或者规程(例如机架与服务器类型等)要求。换言之,通过引入云行业标准术语以及商业处理惯例,客户将能够借此获得最具创新性 & 成本效益的解决方案选项。

3. 指定商用项目条款

云计算的采购工作应该遵循商用产品思路。云服务供应商的特定产品与条款属于实现云计算收益的必要前提,这是因为实用型云服务往往需要立足于超大规模、持续创新及成本效益基础方可带来预期价值。不必要的限制或者变更可能会限制这方面优势,包括影响规模化能力以及创新型服务变更的实现频率。有鉴于此,大家应当对现有商用产品的采购规程进行审视,考虑各条款与条件是否与之冲突,而后清除不必要的要求以充分发挥云技术的可扩展性与按需交付能力。

4. 了解不同云服务模式

目前存在多种不同云服务模式可供选择，具体包括基础设施即服务（简称 IaaS）、平台即服务（简称 PaaS）以及软件即服务（简称 SaaS），另有多种不同方案用于实现采购、管理、计费以及安全保护。对于考虑采用云计算服务的客户，当务之急应该是掌握各类云模式及其创建方法。大家可以通过标准与技术研究院（简称 NIST）官方网站获取与云服务类型相关的信息与国际公认标准：

<http://www.nist.gov/itl/cloud/>.

5. 区分云基础设施（即非托管服务）与托管服务

成功的云采购策略需要将云基础设施的采购工作与云迁移及工作负载的相关规划、开发、执行及维护任务所涉及的服务与人力区分开来。这种准确区分能够确保大家获得最为理想的成本效率。

6. 纳入一套实用型计费模式

首先需要明确的是，云计算的一大主要优势在于其不像传统方案那样采用固定价格协议。相反，其提供的是一类按需使用、以实用性为先且不存在强迫性额外支出的采购模式。要享受到这种波动式成本计算机制，客户需要签订合同以约定仅需要为实际使用的服务资源付费。云服务供应商的计费政策应当：

- 通过按使用量计费机制提供实用模式，客户只需要在每月末根据具体资源使用情况支付费用。
- 允许根据市场行情灵活调整服务费率，保证客户能够充分享受到云服务的动态与竞争性计费收益。

允许云服务供应商提供多种不同计费模式，客户则结合自身实际需求对每种计费模式进行评估，而不再像过去那样面向计算或者存储单元进行粗放的售价比较。云服务供应商应当提供透明、公开且及时更新的定价政策，同时具备相关工具以帮助客户准确评估实际费用预期——例如 AWS 的 Simple Monthly Calculator: <http://aws.amazon.com/calculator>。另外，云服务供应商还应当向客户提供用于生成细化且可定制计费报告的工具选项，从而满足客户的业务与合规性需求。

7. 利用第三方认证资质强化安全性、隐私性与审计性

利用安全性、隐私性与审计性相关业界最佳实践作为保障手段，从而有效执行物理及逻辑型安全控制措施，防止出现过分繁琐的流程或者未被执行到位的风险控制及合规性遵循行为。目前可资参考的安全框架、最佳实践与审计标准多种多样，而可作为云标准化控制方案的选项包括：联邦风险与授权管理计划（简称 FedRAMP）、服务组织控制（简称 SOC）1、取证标准声明（简称 SSAE）16、国际标准取证标准（简称 ISAE）3401（原被称为第 70 号审计标准声明[简称 SAS]）、SOC 2、SOC 3、支付卡行业数据安全标准（简称 PCI DSS）、国际标准化组织（简称 ISO）27001、ISO 9001、国防部风险管理框架（简称 DoD RMF，云安全模型）、联邦信息安全管理法案（简称 FISMA）、国际武器贸易条例（简称 ITAR）以及联邦信息处理标准（简称 FIPS）140-2 等等。

8. 将安全工作视为须共同分担的职责

随着云计算客户立足于云基础设施构建各类系统，安全性与合规性遵循责任应当由服务供应商同云消费者共同分担。在 IaaS 模式下，客户能够控制基础设施架构并保护运行于其上的应用及数据，而云服务供应商则负责在高安全性且高度受控的平台之上交付服务，同时带来更多安全功能。云服务供应商与客户的各自职责取决于具体云部署模式（如第四点中所述），而客户方亦需要清楚自身在各类模式中的责任所在。

9. 设计并实现云数据治理

云客户应当保留对自有数据的完整控制权与所有权，并有能力自由选择数据存储所在的地理位置。而云服务供应商则利用身份与访问控制约束指向客户基础设施与数据的访问行为。云服务供应商应当为客户提供灵活的选项，允许其指定如何存储、管理及保护自己的数据，且无需签订长期或者排他性合同。相较于传统 IT 基础设施，云计算的一大主要优势在于确保客户能够避免供应商锁定问题。而云服务供应商则应当允许客户要求需要随时关闭现有平台并迁移业务数据。

10. 定义云评估标准

云评估标准应当注重系统性能要求，在云服务供应商的协助下建立资源池，从而发挥云技术的弹性、成本效益与快速扩展性等能力。这套方案能够确保客户结合实际需求选择最佳云服务，实现最佳服务价值并促进市场驱动型创新。NIST 给出的云效益定义可以成为制定云评估标准时的理想参考点：<http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf>。

在运用 **AWS** 服务时，大家可以采取一套高效的采购流程以快速实现服务启动。而在其中遵循以上十项重点，将切实帮助大家在节约成本的同时获得与预期相符的良好效果。