

简译版

多重云的成熟度如何

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Where do we stand when it comes to multi-cloud maturity?		
原文作者	米尔科·佐兹 (Mirko Zorz)	原文发布日期	2021 年 8 月 17 日
作者简介	米尔科·佐兹是 Help Net Security 的主编。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/08/17/multi-cloud-maturity/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	随着联邦政府继续强调云迁移和部署，各机构的技术领导者希望更好地理解多重云的概念，及其对机构来说意味着什么。大多数 IT 领导者都认同，他们未来的 IT 环境将是多重云环境。目前，我们尚无法确定未来的多重云环境是什么样的、如何实现多重云环境，以及如何衡量多重云环境是否是成功的。也就是说，我们尚未实现多重云成熟。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

多重云的成熟度如何

米尔科·佐兹

2021 年 8 月 17 日

在接受 Help Net Security 的采访时，Booz Allen Hamilton 公司的高级副总裁梅丽莎·萨瑟兰（Melissa Sutherland）谈到了多重云成熟度、云迁移策略以及云未来的演变问题。

长期以来，企业一直在使用云。我们是否已实现多重云成熟？

大多数联邦机构已经开始实施企业云战略，尽管其成熟度各不相同。那些处于转型初期的机构正在评估其现有的应用程序、保护初始基础架构环境并规划云迁移。那些更进一步的机构已经开始实施或利用企业级安全云环境，来托管关键任务应用程序和敏感数据。

大多数机构通过选择并专注于自己的数据中心（私有云）或单个云服务提供商（CSP），来开始这一旅程。然而，随着时间的推移，这些机构发现他们拥有了由多个云环境支持的应用程序、服务、数据和功能。

随着联邦政府继续强调云迁移和部署，各机构的技术领导者希望更好地理解多重云的概念，及其对机构来说意味着什么。大多数 IT 领导者都认同，他们未来的 IT 环境将是多重云环境。目前，我们尚无法确定未来的多重云环境是什么样的、如何实现多重云环境，以及如何衡量多重云环境是否是成功的。也就是说，我们尚未实现多重云成熟。

对于需要为政府机构制定云迁移策略的云架构师，有什么建议？此类策略有何独特之处？

政府机构的云迁移策略，其独特之处是需要满足一系列严格的安全标准——“联邦风险和授权管理计划”（FedRAMP）。美国政府要求其所有 CSP 都要获得 FedRAMP 授权，以确保联邦数据的安全性。

这方面的建议是关注基础技术。首先，CSP 要获得 FedRAMP 授权。除此之外，机构应确保关键基础能力的到位和成熟，以便有效地设计多重云架构。这些基础技术和能力包括容器编排平台（包括容器化应用程序）、企业 DevSecOps、“基础设施即代码”、企业应用程序编程接口网关和解决方案，以及数据管理平台、软件定义网络和网络自动化。在这些支持功能中，大多数都符合“一切皆代码”的原则。

企业如何在云迁移期间进行成本优化，以最大程度地节省成本？

多年前，新兴的云讨论包括“通过将应用程序迁移到云中来节省成本”。后来，许多领导者发现，将应用程序迁移到云中通常无法降低企业的整体 IT 成本。但是，云的灵活性、弹性和安全性确实能够为企业提供更好的成本价值。

举例来说，国防部（DoD）正在通过其 Advana 数据分析平台解决这个问题。国防部拥有世界上最大的运营预算来支持其敏感的全球任务。鉴于其运营的复杂性，几十年来一直面临着对数千个会计和业务系统进行准确和全面财务审计的挑战。

Advana 集成了整个国防部的数百个业务系统，包括财务、医疗、人事和供应链，通过通用数据模型、自然语言处理和自助服务分析，制定明智的决策。这一方法有助于数据的发现、理解和使用，能够帮助国防机构提高成本效率、改进决策，应对关键任务和业务挑战。

空军还使用云来提高其 Platform One 软件开发平台的效率，该平台允许用户部署 DevSecOps 软件工厂，在软件出现问题时可以从 90%（而非从头）开始进行解决。

大多数机构在从 CSP 处采购更大的应用程序和服务组合时，成本节约最为显著，并且具有最佳的谈判能力。将这些产品组合拆分成更小的部分并跨 CSP 迁移应用程序，会降低他们在当前云经济状态下的优势。

另一个与成本相关的误解是，将应用程序部署到多个云环境，能够将工作负载转移到最具成本效益的基础架构上。云管理机构可以跟踪各个 CSP 不断变化的成本结构和激励措施，从而选择最佳定价。

不幸的是，这种方法目前不太可能在应用程序级别节省任何成本，因为这会产生与 CSP 无关的额外成本。此外，将应用程序从一个云环境迁移到另一个云环境时也会产生迁移成本。

随着市场不断成熟，多重云架构越来越容易实施、管理和迁移，上述情况可能会发生改变。但在可预见的不久的将来，成本节约不会是在应用程序层面实施多重云架构的驱动因素。

在将应用程序迁移到云中时，企业通常会忽略哪些问题？

一些企业急于进行云迁移，却发现他们的 CSP 无法满足其所有需求。因此，企业应确保云原生应用程序是模块化和开放的，这有助于在未来无缝集成新服务。

各机构还应了解自己的资源和人才是如何支持多重云的。通过嵌入标准的开发实践和平

台，企业可以加速部署、更好地利用他们的人才并减少人为错误。在机构内推出一致的蓝图和共享服务，有助于部署标准和“基础设施即代码”实践，使团队能够将宝贵的时间用在增值的自定义应用程序上。

另外，机构也不应夸大云安全的重要性。迁移到云中的应用程序，必须能够填补商业 CSP 提供的安全控制与策略要求的安全控制之间的差距。

预计未来五年多重云将如何发展？

目前，大多数应用程序和工作负载都位于数据中心。在接下来的五年里，经过认证的云服务提供商会大量增加，这会促进更广泛的云采用。

CSP 正在进行一场军备竞赛，以确保获得最高机密级别的认证，使他们能够为国防部和情报界提供服务。对于国防和情报界来说，提高云采用水平对未来几年的任务至关重要。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司（AVL TEAM）更多信息请访问：<http://www.avlsec.com>