快速跟踪您的
多云监控计划

splunk>
turn data into doing™

多云
的兴起

云迁移呈上升趋势，以至于Gartner 预测到 2025 年，80% 的企业将完全从内部基础设施迁移出去。云计算的最新发展是多云的兴起，这是一种组织在单一架构中使用至少两种云服务的策略。换句话说，不同的云堆栈用于不同的任务，例如，Google Cloud Platform 用于内部应用程序，而 Amazon Web Services (AWS) 则用于面向客户的应用程序。这种方法变得如此流行，以至于今天超过80% 的公司都在使用它。

有不同种类的云解决方案可以组成多云环境。公共云服务包括 AWS、Microsoft Azure、Google Cloud Platform 和第三方提供商提供的其他云计算服务。另一方面，私有云限制了对特定组织的访问。服务和基础设施在专用网络上维护，与公共云相比，提供了更高的安全性和控制能力。

不同的堆栈
用于不同的任务

为什么组织使用多个公共云

AWS 用于开发
微服务
容器
EC2、虚拟机、存储

GCP 用于内部服务
G Suite、Workday、
Salesforce

Azure
用于提升和移动
降低成本
灾难恢复

了解
多云环境

它还值得定义“混合云”和“多云”。混合云解决方案意味着，组织使用内部、公共云和私有云基础设施的组合，而多云指的是，组织使用多个云提供商进行多种相同类型的云部署的方式，例如，如果他们使用来自两个不同供应商的公共云。不同的团队有不同的需求，所以他们通常会选择最适合他们特定标准的云供应商。

有何差异?

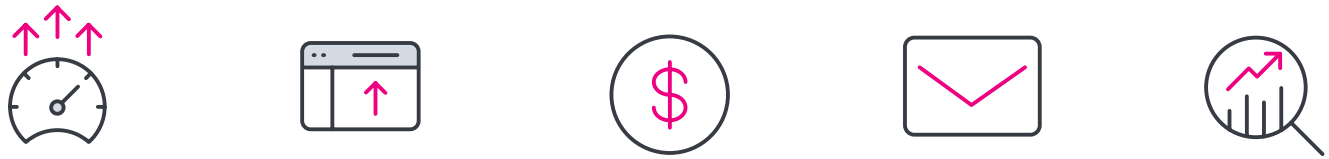
多云	混合云
来自不同供应商的相同（公共或私有）的多个云部署	服务组合（本地、私有、公共、第三方）以及它们之间的集成或编排
示例：两个公共云，AWS+Azure	**示例：**公共云和客户自行维护的内部数据中心基础设施

为什么公司采取多云方法?

优化性能：如果主云停机或出现性能问题，被动云可以作为后备解决方案。该策略最终会减少或完全消除停机时间，直到主云恢复在线。

节约成本：将改进的可靠性和优化的性能相结合意味着为企业节约成本。银行停机可能会导致收入损失，而医院停机可能会导致收入损失和生命危险。无论情况如何，保持网络正常运行对于每个组织的持续成功至关重要。

灵活性：多云方法有助于避免与供应商捆绑在一起，在这种情况下，组织依赖于特定云提供商的基础设施和服务，如果他们更换供应商，可能会面临巨大的成本和限制。使用供应商组合后，组织还可以选择满足其特定需求的服务组合，从而优化性能。特定的公司可能会选择将 Microsoft 工具用于一个用例，将 Google 或 AWS 用于其他用例（例如，基础设施和开发）。



多云环境中的**关键挑战**

虽然多云战略有很多好处，但挑战也并非微不足道。提供更高灵活性和可靠性的相同功能也带来了额外的安全风险和 IT 挑战。

IT 团队在云计算中面临的所有挑战在多云环境中被放大，使得团队更难识别、调查和解决云中的关键问题；更多的服务意味着更多的复杂性，孤立的系统使得整体监控更加困难。

在安全方面，最近的研究显示，所使用的云服务数量与以下可能性之间存在联系：Nominet 2019 年的一项研究发现，在过去一年中，52% 的多云环境遭到破坏，相比之下，混合云组织和单云用户的这一比例分别为 24% 和 24%。多云环境也更容易遭受多次入侵：69% 的此类组织报告了 11 到 30 起入侵事件，相比之下，单云组织和混合云用户的比例分别为 19% 和 13%。

多云环境带来的挑战以不同的方式影响着 IT 和安全团队：

多个系统会导致孤立：多云方法可以提高安全性和系统可靠性，因为服务分布在多个云解决方案中。但是，这也可能带来风险，因为这使得组织更难看到所有主机和服务。

使用不同的云解决方案，每个解决方案都有自己的本地监控和安全工具，这意味着 IT 团队无法有效地查看整个堆栈，以判断服务降级或停机是由特定服务引起的，还是系统按预期工作。

传统的网络安全基础不一定适用于多云环境。组织可以使用多种解决方案来监控其云服务，但是这种方法会减慢团队的速度，并且是有代价的，尤其是当对时间敏感的问题发生时。

增加平均解决时间 (MTTR)：对于 IT 和安全团队来说，关于多云系统中断或漏洞的争论可能是一个令人头痛的问题，并且会耗费组织的时间、金钱，导致客户满意度和信任度降低。

整个堆栈可见性的降低意味着，团队要花费更多的时间来找出中断发生的位置和原因，不得不在多个监控系统之间转换，以关联和分析事件数据，从而获得对问题的完整理解。在服务中断或恶意攻击中，每一分钟都很重要，多云系统的额外复杂性会对底线产生直接影响。

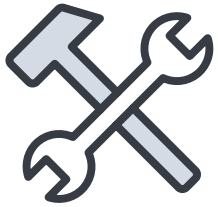
数据治理、法规遵从性和基础设施漏洞：此外，由于缺乏跨多个堆栈的可见性，导致更难满足法规遵从性要求和抵御黑客，黑客更容易发现和利用组织分布式基础设施中的漏洞。本质上，每个额外的云服务都会增加网络接入点的数量。

可见性问题还会产生数据治理和法规遵从性问题。多个云可以提供更大的灵活性，但也会带来监管挑战。例如，组织可能会在未经批准的环境中意外运行应用程序，并违反一般数据保护法规 (GDPR) 的规定。违反这些准则和其他准则可能会导致巨额罚款。

使用不同的本机云工具
进行监控可以导致:

- **孤立的视图**
- **孤立的团队**
- **孤立的数据**

团队很难识别、调查和解决云中的关键问题。

缺乏可见度  无法了解服务降级或停机是否由云服务引起	**复杂的工具集**  使用多个云服务使得很难有一个统一的监控策略
MTTR 差  花费太多时间来弄清楚中断发生的地点和原因	**难以扩展**  难以跨多地区、多客户和多云环境收集数据

如何应对
多云监控

那么组织如何克服这些挑战呢？随着云基础设施的范围和复杂性不断扩大，企业拥有应对这些安全和 IT 挑战的监控解决方案和策略变得更加重要。

好消息是，对于组织来说，在减轻伴随的风险的同时，完全有可能获得多云方法的好处。现代 IT 基础设施越来越复杂，在整个多云环境中采用集中式方法进行监控和故障排除至关重要。如果没有合适的工具，今天的企业将会发现，获得正确处理停机和事故所需的数据更具挑战性。投资现代 IT 工具的组织可以创造积极的客户体验，并最终最大限度地提高创新和收入。

减轻监控痛苦的途径

第一步是找到整合的 IT 基础设施监控解决方案，取代众多的监控和故障排除工具。使用一种工具进行监控和使用另一种工具进行故障排除，可能会导致不必要的复杂性，甚至在出现关键问题时，还会减慢团队的速度，但是简化工具集后，可以在同一个解决方案中实现这两种功能。接下来，需要无缝获取数据。在此，引导式数据加载至关重要 — 正确的解决方案需要能够轻松从多个云供应商收集数据，并将所有数据整合到一个视图中。这使组织能够更好地跟踪其所有不同云环境的运营、安全性和成本。

最后，一个跨基础设施、应用程序和服务统一监控并使用人工智能 (AI) 和机器学习功能的解决方案，可以帮助组织预测和防止云中断发生。特别是对于多云环境，组织需要一种解决方案来简化和托管来自多个云的数据收集，通过对不同的云服务进行分组来提供环境的聚合视图，并让团队跟踪所有环境中的总体云使用情况。

了解如何做到。

监控多云环境可能是一项挑战，但企业不需要大量工具来跟上其云基础设施中发生的变化。

请联系 sales@splunk.com简化您的工具集。

2020-IT-splunk-multicloud monitoring-EB-113

splunk> turn data into doing™