



The bridge to possible



2022 年全球混合云 趋势报告

基于云的技术如何影响企业基础设施、运营和战略。

目录

执行摘要	2
关于本报告	2
主要调查成果	3
混合云已经成为新常态	4
客户面临的主要挑战	6
构建云就绪环境: DevOps 和 CloudOps 的观点	9
智能化云运营需要采用新技术	12
加速采用云原生技术	13
结论	17
调查方法	18



执行摘要

我们的一项全球性调查显示，融合本地基础设施和基于云的资源混合云模式已经成为企业常态。参与调查的绝大多数组织（92%）正在使用多个公共云，这不仅是为了利用这些公共云的独特优势，同时也是为了提升运营敏捷性、安全性、应用性能和业务弹性。

参与调查的受访者能够敏锐地认识到混合云模式带来的各种挑战，他们也在用各种方式努力适应这些变化。很多受访者将

NetOps、CloudOps 和 DevOps 团队之间的合作视为应对技术和运营挑战的关键。基础设施现代化、重构应用以及增强与 AIOps 的合作以及部署自动化也被视为混合云取得成功的重要推动因素。

受访者意识到网络、云运营和 DevOps 团队之间合作的价值。向云原生和混合云转型促使 DevOps 团队采用针对混合模式进行了优化的基础设施，兼顾现有应用和新应用。

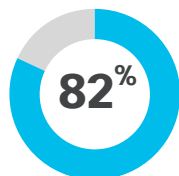
关于本报告

本报告介绍了混合云采用情况的最新趋势、对企业基础设施和运营的影响，以及为取得更佳的技术和业务成果所采取的策略。除非另有说明，本报告中的数据和洞察均来自思科委托 451 Research（隶属于 S&P Global Market Intelligence）对来自

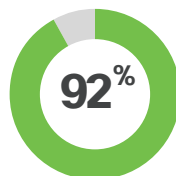
13 个国家/地区的 2500 名 IT 决策者进行的一项全球性调查。调查受访者包括云计算、DevOps 以及企业网络领域的专业人士，他们所在的组织都在广泛、深入地使用云技术。（请参阅[“调查方法”](#)章节了解更多详细信息。）

主要调查成果

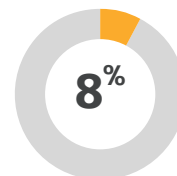
混合云和多云已经成为常态。



的受访者已采用混合云。



的组织使用不止两家公共云提供商。



的组织使用单一公共云提供商。



安全性和复杂性是组织面临的重大挑战。

- 37% 的受访者认为, 安全性是组织部署混合云时面临的重大挑战。
- 不断增加的运营复杂性和成本管理也被视为重要挑战 (33%), 其次是合规性和隐私性 (31%)。



协作是成功所必需的。

- 55% 的受访者表示其所在组织组建了由技术和业务代表组成的跨职能团队。
- 50% 的受访者表示其所在组织拥有集中的 CloudOps 和 NetOps 职能团队, 以确保组织的混合云策略满足业务目标。
- 受访者表示, 网络和云运营团队之间加强和深化协作有助于提升云安全 (45%) 和运营效率 (41%)。



开发人员正积极拥抱混合云和基础设施即代码 (IaC)。

- 53% 的组织每周在本地和云环境之间移动工作负载。
- 58% 的组织正在采用基础设施即代码 (IaC)。44% 的组织正在部署云原生技术以改善安全态势。



混合云正在推动组织采用新兴技术。

- 所在组织正在部署 AIOps (45%)、基础设施自动化 (41%) 和边缘计算 (41%) 的受访者占比很大。
- 79% 的受访者表示, 由于超过一半的工作负载将在不同环境中的不同硬件上运行, 他们迫切需要使用功能全面的工具集来管理这些工作负载。



组织正在加快采用云原生技术。

- 91% 的担任 CloudOps 和 DevOps 角色的受访者表示, 他们的组织已经或将要使用云原生技术来重构应用。
- 47% 的 CloudOps 和 DevOps 角色受访者表示, “云优先” 原则是组织改变开发流程和工具的转折点。

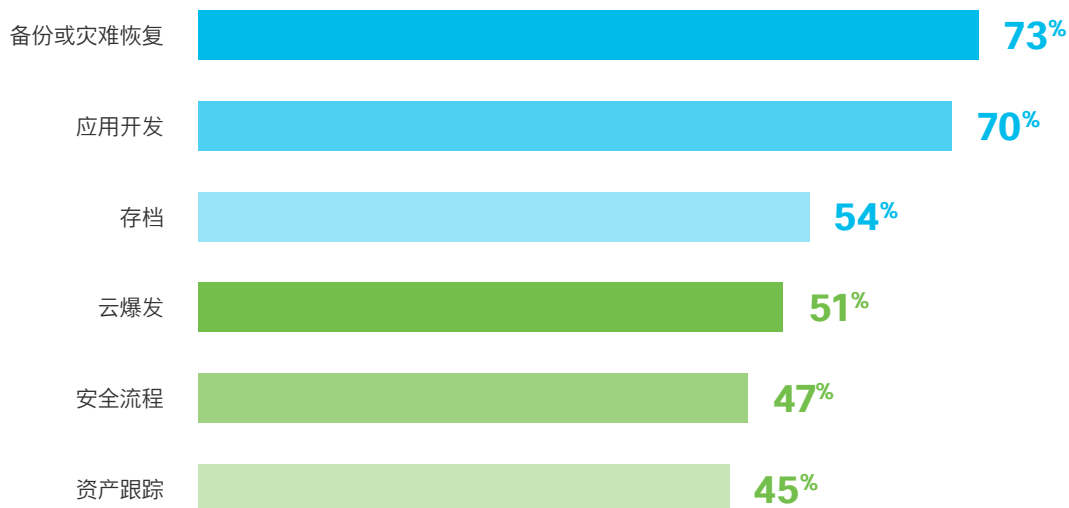


混合云已经成为新常态

全球大多数组织目前都在使用多云支持各种应用，不断改进业务敏捷性和可扩展性。在本次进行的全球性调查中，82% 的受访者表示，他们目前正在使用基于云的基础设施即服务 (IaaS) 来托管工作负载。这种混合方式使组织能够打造更敏捷、更可扩展的开发环境 (42%)，还能够

加速业务敏捷性和创新步伐 (40%)。另外，在组织考虑眼下和未来处理工作负载的最佳环境时，使用多云已经成为一种颇受青睐的方式。采用这种方式，组织可以综合考虑区域合规性、安全性和性能等因素为工作负载选择最佳环境。

图 1. 组织正在使用混合云模式支持各种工作负载



问题：您目前正在混合 IT 环境中运行以下哪些工作负载或流程？

调查对象：所有受访者 (人数：2577)

资料来源：思科《2022 年全球混合云趋势报告》

只有 8% 的受访组织使用单一公共 IaaS 云提供商。

大多数受访组织 (58%) 使用 2-3 家公共 IaaS 云提供商处理工作负载。31% 的受访组织使用 4-10 家公共云提供商。使用的是 AWS、Azure 和 Google Cloud 之外的云提供商, 其中可能包括专门提供公共云服务的提供商, 或其广泛的产品组合中包含云服务的提供商 (如电信公

司)。调查显示, 员工人数超过 5000 的组织 (8%) 比员工人数较少的组织 (5%) 更有可能使用不止 10 家公共云提供商, 因为大型组织有更多业务部门需求, 可以推动跨平台和 IT 之外的使用。

图 2. 组织为什么使用多云



问题: 您的组织为所有服务 (如基础设施即服务 (IaaS)、平台即服务 (PaaS) 以及 SaaS) 使用多云 (公共云和私有云) 的最重要驱动因素是什么?
调查对象: 所有受访者 (人数: 2577)
资料来源: 思科《2022 年全球混合云趋势报告》

结论: 融合本地和基于云的资源模式已经成为常态。绝大多数公司都在利用多云来管理安全性、增强应用开发能力和提升业务敏捷性, 并为每种工作负载选择最佳环境。

值得注意的是, 在参与本次调查的大部分地区, 各地理区域之间的差异很小。这说明运营混合云环境的人员拥有相同的经历。他们是一组特定的人群, 处理的问题在世界范围内都是相通的。

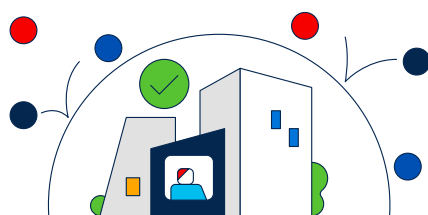
在 SaaS 方面, 组织使用的提供商更多。23% 的受访者表示其组织正在使用 20-100 家不同的 SaaS 提供商处理业务, 应用的范围也十分

广泛, 包括电子邮件、协作和视频通话、客户关系管理 (CRM) 以及人力资本管理 (HCM) 等各种类别。近一半的受访者 (45%) 使用 5-10 家 SaaS 提供商。由于许多 SaaS 应用只能满足特定业务或 IT 需求, 组织需要与多家供应商进行合作。



客户面临的主要挑战

使用混合云和多云的过程充满挑战。受访者表示，安全性是他们在使用多云时面临的^{最大}挑战。正如前面提到的，安全性也是受访者使用多云的首要原因（37%），因为他们希望在安全性与性能和扩展需求之间取得平衡（42%）。三分之一的受访者面临与这些环境中的运营复杂性（33%）和管理成本（33%）相关的挑战。受访者采取了各种策略应对这些挑战，并强烈渴望利用新技术解决当前难题。



挑战 1: 安全性

无论组织目前处于多云采用旅程的哪个阶段，安全性始终都是他们面临的一项严峻挑战，因为威胁在不断变化，技术和流程需要迅速做出调整。需要注意的是，安全性涵盖混合运营的许多方面。在不断扩展的环境中，运营安全性是普遍存在的问题。除允许组织进行分段（安全性最基本的控制之一）外，混合模式还允许组织进行隔离，使组织能够为不同用例使用不同的云。

云运营趋于成熟的一个因素是，组织能够在自由选择工作负载和数据存放位置的基础上进行风险管理。混合环境可以为安全团队提供多种选择，让他们能够平衡工作负载存放位置。例如，

将一些工作负载托管在公共云，并将其他工作负载保留在本地，或通过使用不同的区域来满足数据存放要求。这是混合环境的优势，但同时也伴随风险，因为在多个不同的环境中运营势必会增加运营复杂性。每个云环境都有自己特有的运营模式和管理环境。如果没有一个通用框架来管理这些环境，安全团队就只能在每一个新的云环境中构建独立框架，这需要投入大量时间和资源。

考虑到应用需要经常从一个环境移动到另一个环境，安全问题变得更加复杂。超过一半的受访者表示，他们每周都要在本地和外部环境之间移动应用。除了在本地和不同公共云之间对工作负载进行分段外，企业还积极尝试其他方法改善安全态势，包括使用云原生技术（44% 的受访者）和使用基础设施即代码（58%）。除了管理整个环境的安全状况外，如何确保 API 在多云中的安全性也是一个非常棘手的问题（32% 的受访者）。

各企业正积极采用各种方法来改善安全态势, 包括使用云原生技术...

在这个问题上, 自动化和抽象化最有助于实现混合云对安全性的承诺, 同时还能克服与复杂性相关的挑战。如果安全团队能够利用合适的工具, 通过一个通用框架对多云进行安全管理, 他们就能减少配置错误和运营错误带来的最大风

险, 同时确保在适当的环境部署适当的工作负载。混合环境的复杂性已经让安全团队变得不堪重负, 而能够提供抽象能力的强大管理平台定可以帮助他们显著提高工作效率。

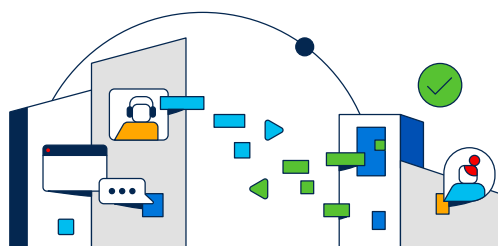
图 3. 组织在采用多云过程中面临的主要运营挑战



问题: 您的组织在使用多云时正在面临或将要面临的最大的挑战有哪些?

调查对象: 所有受访者 (人数: 2577)

资料来源: 思科《2022 年全球混合云趋势报告》



挑战 2: 运营复杂性

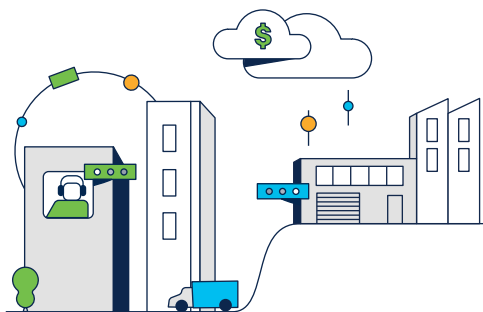
市场上用于简化云环境管理的工具层出不穷, 但仍有 33% 的受访组织表示, 运营复杂性是组织

在采用混合或多云模式时面临的一个突出问题。在混合环境中, 组织除了要管理不同的云环境之外, 还必须管理不同的硬件。许多受访者 (79%) 表示, 由于超过一半的工作负载要在不同环境中的不同硬件上运行, 他们迫切需要使用一套功能全面的工具来管理这些工作负载。例如, 大多数受访者使用作为服务交付的基于云的 IT 运营平台 (94%), 这可以帮助组织量化运营复杂性、提供完整生命周期管理, 以及提供对本地基础设施的主动支持。以上这些关键能力也成为受访者选择基于云的 ITOps 平台的首要标准。

大多数受访者 (94%) 使用作为服务交付的基于云的 IT 运营平台。

组织需要全面洞察更加复杂的基础设施, 能够跨多云环境提供管理支持的解决方案成为他们关注的重点。为确保满足业务目标, 基于 SaaS

的运营平台成为受访组织的首选解决方案 (60%)。



挑战 3: 管理成本

管理云成本充满挑战; 但是, 推动大多数组织使用多云的因素并不是期望用这种方法减少云服务成本 (66% 的受访者)。相反, 一半以上的受访者 (56%) 使用成本/效益法来验证和平衡云服务的采购。

成本优化是衡量多云是否成功的标准之一, 但使用云服务不一定会降低成本。管理多个不同的云会增加复杂性, 进而增加运营成本。而随着组织对云价值的理解趋于成熟, 他们的期望正从降低成本转向成本管理, 以实现最佳的敏捷性和可扩展性, 这也是推动组织采用多云的两个主要因素。

为取得最佳效果, 成本管理应在实现预期业务成果的基础上进行。各组织采用了各种方法来提高运营和成本效率。调查显示, 建立云卓越中心 (57%)、采用成本/效益法或 AIOps 模式 (53%), 以及集中的 CloudOps 和 NetOps 职能团队 (50%) 是最常使用的方法。

结论: 在混合云环境中使用多云增加了与安全性、运营复杂性和成本管理相关的挑战。大多数组织正在采用 SaaS 运营平台、基础设施即代码和 AIOps 运营模式来应对这些挑战。他们还建立了云卓越中心, 并拥有集中的 CloudOps 和 NetOps 职能团队。

图 4. 组织为确保取得预期业务成果所采取的策略



问题: 为确保云策略满足业务目标, 您采取了以下哪些策略?

调查对象: 所有受访者 (人数: 2577)

资料来源: 思科《2022 年全球混合云趋势报告》



构建云就绪环境： DevOps 和 CloudOps 的观点

开发人员在制定组织的云策略方面变得更有影响力，他们在选择支持应用开发和基础设施现代化的云平台和服务方面常常发挥关键作用。担任云运营和 DevOps 角色的受访者表示，在开发所有新应用时坚持“云优先”原则 (34%) 是组织改变开发流程和工具的转折点，成本优化 (19%) 和自动化 (18%) 则是推动因素。这也是组织对云环境的理解趋于成熟的一个表现，因为组织开始认识到，运营能力是多云旅程中不可或缺的一部分。

“云优先”原则可能更适合全新应用，因为大多数企业同时还在运行旧应用，而这些应用需要使用不同的方法来实现转型。绝大多数 (91%) 的 CloudOps 和 DevOps 受访者表示，他们的组织已经或将要使用云原生技术重构应用。对于任务关键型应用和旧应用，他们实现转型的方法是就地进行现代化改造 (38%) 或重构和迁移 (25%)，同时利用云原生技术支持这一转型。受访者对这种转型保持乐观，只有 8% 的受访者计划继续保留原有任务关键型工作负载。

云就绪型网络的重要性

无论组织决定在何处运行特定应用，网络始终是确保应用正常运行的关键。开发人员认为，他们在确定网络优先事项方面必须拥有话语权。大多数开发人员认同或强烈认同 (92%)，在确定组织网络策略和优先事项方面，拥有一定话语权非常重要。调查显示，在本地和外部环境之间移动工作负载的频率越高的受访者，对网络的重视度也越高。对于在这些环境之间移动工作负载和/或应用的频率，53% 的受访者每周移动一次，39% 的受访者每月移动一次。

在核心团队之外开展合作的问题上，受访组织普遍持开放和乐观的态度。他们认为这有助于确保混合云环境的安全性，同时还能提升效率和性能。受访者认识到，NetOps、CloudOps 和 DevOps 团队之间的合作能够创造价值。

91% 的 CloudOps 和 DevOps 受访者表示，他们的组织已经或将要使用云原生技术重构应用。

受访者认同, NetOps 和 CloudOps 团队之间加强协作会带来诸多裨益, 最大的收益是提升云安全性 (45%) ...

倡导协作文化

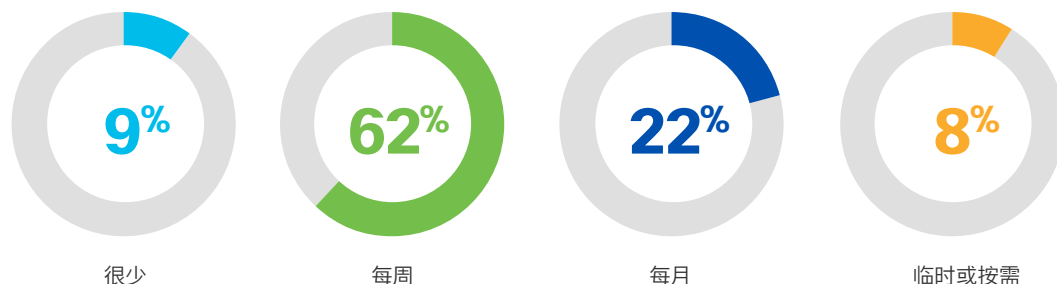
受访者认同, NetOps 和 CloudOps 团队之间加强协作会带来诸多裨益, 最大的收益是提升云安全性 (45%), 其次是提高整体运营效率 (41%) 和增强云应用性能 (39%)。

超过一半的受访者 (55%) 表示其组织组建了由技术和业务代表组成的跨职能团队, 有 50% 的受访者表示其组织拥有集中的 CloudOps 和 NetOps 职能团队, 以确保组织的混合云策略满足业务目标。相较于亚太地区的受访组织 (48%), 北美地区的受访组织 (58%) 更有可能构建这项功能。

同时, 网络专业人士也认为这种关系非常重要: 在担任网络角色的受访者中, 有 57% 强烈认同 DevOps 团队需要一同参与制定组织的网络策略。事实上, 大多数开发人员表示他们已经制定了与网络团队协作的流程, 84% 的 DevOps 受访者定期与网络团队举行会议, 有的是每周举行 (62%), 有的是每月举行 (22%)。

尽管大多数受访者认为 DevOps 和网络团队之间的协作程度已经足够高 (83%), 但实际上仍有一些阻碍深入合作的因素。团队之间有相互冲突的优先事项 (45%)、抗拒变革 (43%)、目标和激励措施不同 (41%), 这些都是阻碍 DevOps

图 5. NetOps 和 DevOps 团队之间的协作非常频繁



问题: 您与网络运营团队多长时间协作一次?

调查对象: 担任 DevOps 角色的受访者 (人数: 647)

资料来源: 思科《2022 年全球混合云趋势报告》

48% 的开发人员表示, 网络可靠性是他们面临的最紧迫的挑战之一。

和网络团队展开高效合作的因素。要想进一步加强团队协作, 各团队需要对网络如何加快开发速度和提升开发效率有相同的认识, 并确定相同的业务目标。团队之间已在进行一定程度的协作, 但在解决开发人员关注的网络问题方面, 仍有许多深度协作的空间。

团队希望更全面地洞察网络问题。有 41% 的开发人员表示, 进行根本原因分析是他们面临的一项重要挑战, 此外还包括缺乏通用的工具、平台和接口。高效协作有助于开发人员更好地了解网络优先事项, 同时确保应用需求和业务需求被视为整体网络策略的一部分。

在本次调查中, 48% 的开发人员表示, 网络可靠性是他们面临的最紧迫的挑战之一。DevOps



结论: NetOps、CloudOps 和 DevOps 职能团队之间的协作对于混合云取得成功至关重要。这使企业迫切需要利用集中化平台, 为不同团队、工具和环境提供可视性、协调性和自动化。





智能化云运营需要采用新技术

在本次调查中, 受访者对可从混合架构中获益的一系列前沿技术表现出浓厚兴趣, 包括部署基础设施自动化 (49%)、边缘计算 (41%) 以及组合型基础设施 (27%)。

41% 的受访者已经部署某种形式的边缘计算能力, 另有 53% 的受访者期望在未来两年内部署这项能力。边缘计算的应用范围十分广泛, 而边缘计算的混合方法可以确保在适当的位置部署适当的能力级别, 以优化应用性能和客户体验。使用 10 个或更多 IaaS 云平台的组织更有可能在边缘计算方面加大投资力度 (57% 的受访者已经部署了这项技术)。

基础设施自动化是实现云效率和可扩展性的关键, 部署自动化技术的受访组织数量略有增加 (49%)。组织以往在这个领域的投资往往不足。与云的整体采用情况相比, 基础设施自动化的采用情况差别很大。在只使用单一公共云的受访组织中, 有 39% 部署了自动化技术。而在使用 10 个以上云服务的受访组织中, 部署自动化技术的比例要高出很多, 达到 55%。这表明, 自动化正在成为组织管理日益复杂混合云的必备

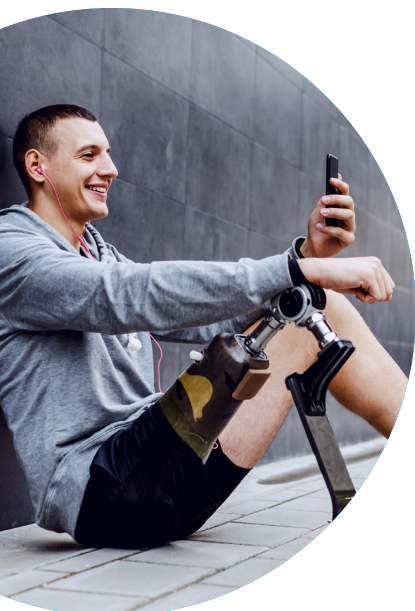
技术。利用自动化技术的工具 (例如作为基于云的服务交付并支持基础设施生命周期管理的 IT 运营平台) 可以帮助组织更有效地应对混合云的复杂性。

同时, 受访者也在积极寻找更高效的运营方式, 他们对使用遥测和 AIOps 技术的预测能力表现出浓厚兴趣。这也表明他们的运营思维趋于成熟, 因为他们从响应型模式转变为预测型模式, 开始化被动为主动。几乎有一半的受访组织 (45%) 目前正在使用某种形式的 AIOps 技术, 还有 49% 的组织计划在明年部署这项技术。

在关于互联能力和数据访问重要性的调查中, 释放的信号非常明显。数据交换矩阵可以确保数据在混合环境中的可用性, 88% 的受访者现已具备这种能力, 或计划在两年内具备这种能力。部署高性能基础设施以访问能够处理所有这些数据的应用也被视为关键能力, 91% 的受访者计划在未来两年内部署专用 5G 无线网络。混合环境依赖于高效的数据分发和访问能力。

结论: 混合云模式正在推动组织采用新兴技术, 包括 AIOps、基础设施自动化和边缘计算。既能支持这些功能, 又能提供有效的数据访问和分发的基础设施变得至关重要。

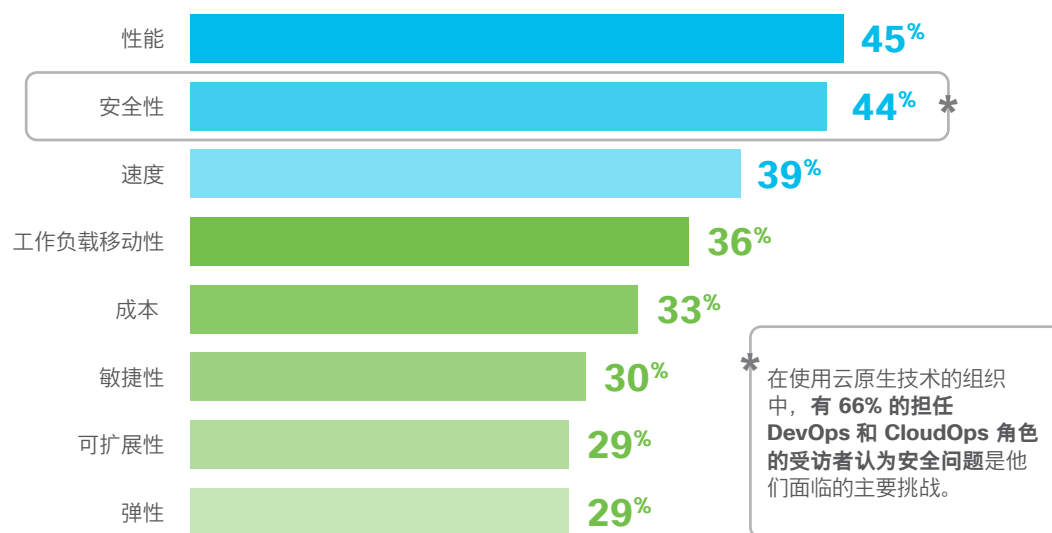




加速采用云原生技术

组织期望利用云原生技术提升应用性能和安全性，这加速了组织向云原生应用架构的转型。大多数受访者 (91%) 正在积极利用或计划利用云原生技术，迁移或重构生产工作负载和应用。对性能 (45%)、安全性 (44%) 和速度 (39%) 的需求是 DevOps 和 CloudOps 受访者考虑采用云原生技术的推动因素。

图 6. 性能和安全性是组织使用云原生技术的主要驱动因素



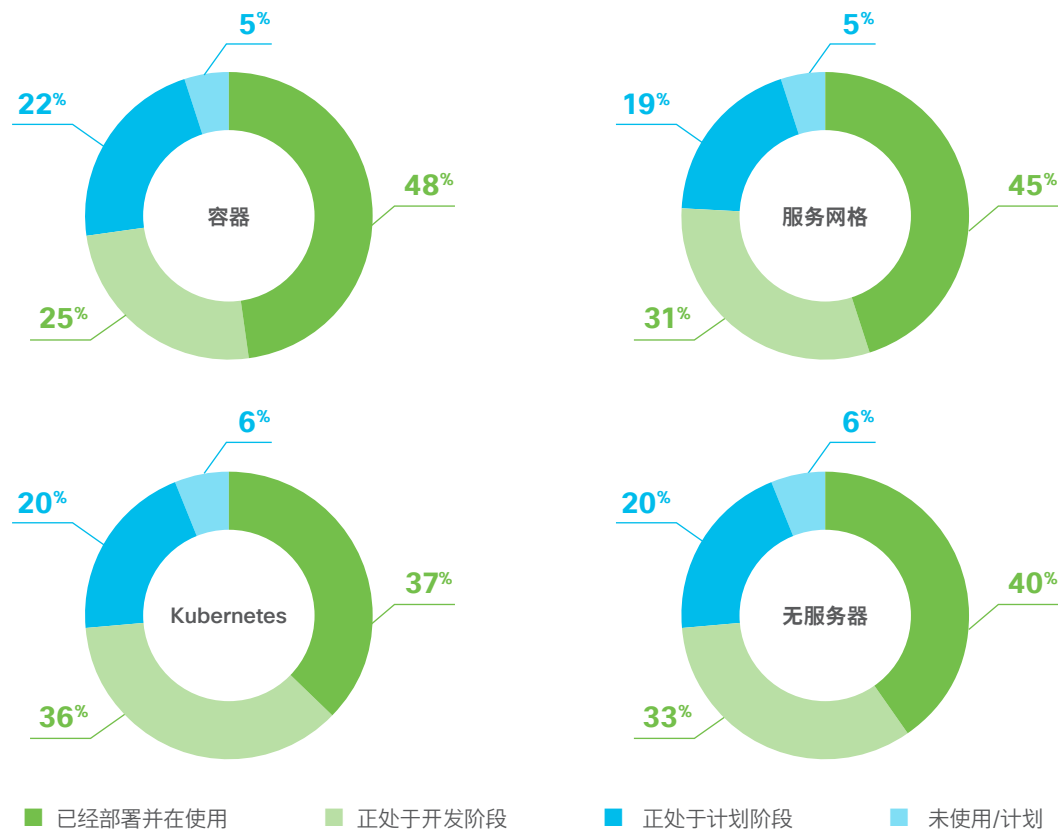
问题: 您之前提及，自己知道企业计划使用云原生技术。您认为推动这些计划的需求是什么？
问题: 您的组织在使用云原生技术时面临的主要挑战有哪些？
调查对象: 担任 DevOps 或 CloudOps 角色的受访者 (人数: 1286)
资料来源: 思科《2022 年全球混合云趋势报告》

担任 CloudOps 和 DevOps 角色的受访者认为, 云原生技术产生了积极影响...

在使用云原生技术的组织中, 近一半受访者表示, 他们的组织已经部署和使用了容器 (48%), 45% 的组织使用了服务网格, 40% 的组织使用了无服务器技术, 37% 的组织部署了

Kubernetes。不到 5% 的受访者目前尚未使用或不计划使用任何云原生技术, 许多组织目前还处于计划或开发阶段。

图 7. 几乎所有组织目前都在使用或计划使用云原生技术



问题: 您的组织正在考虑或已在使用以下哪些云原生技术?
 调查对象: 使用云原生技术的受访者 (人数: 1165)
 资料来源: 思科《2022 年全球混合云趋势报告》

安全性的提升是使用 IaC 的重要成果, 担任云运营角色的受访者尤其认同此观点...

虽然受访者对云原生技术所具备的潜力持乐观态度, 但他们也敏锐地意识到, 组织在有效实施这项技术时将面临严峻挑战。在担任 DevOps 和 CloudOps 角色的受访者中, 有三分之二 (66%) 表示, 安全问题是使用云原生技术时面临的主要难题, 其他难题还包括流程和工具集成 (57%), 以及预算限制 (52%)。

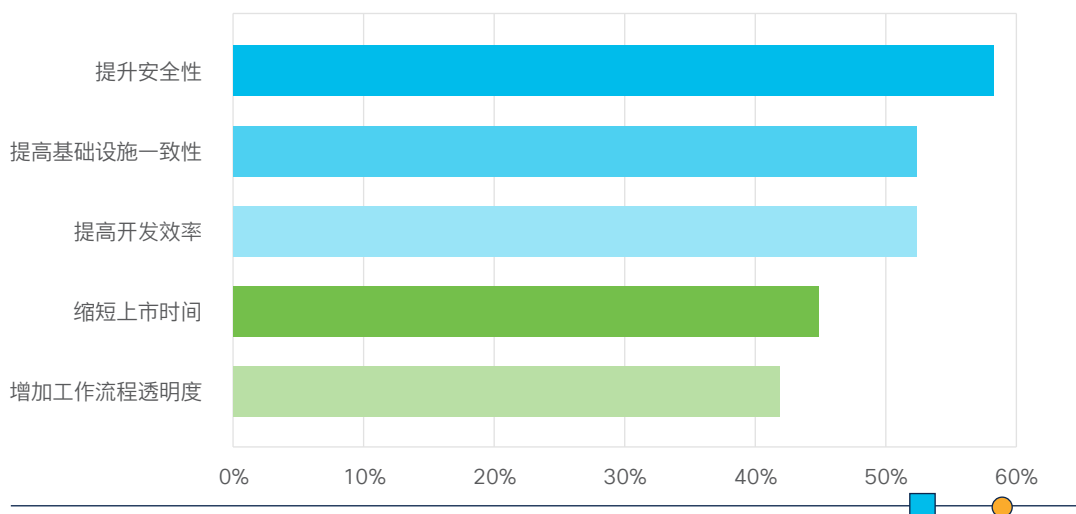
由于许多组织缺少技术和预算, 安全问题可能变得更加严重, 这会导致云原生环境中的数据和工作负载无法获得足够的保护, 进而影响开发效率。除了影响组织的安全策略外, 使用云原生应用架构还会影响网络策略。担任 CloudOps 和 DevOps 角色的受访者认为, 云原生技术产生了

积极影响, 它让网络的自动化程度更高 (24%), 让网络变得更加安全 (25%)。

使用基础设施即代码 (IaC)

利用云原生应用的开发人员和 CloudOps 专业人士可以使用基础设施即代码 (IaC), 通过代码而非手动流程对基础设施进行管理, 以进一步构建组织的自动化和安全能力。安全性的提升是使用 IaC 的重要成果, 担任云运营角色的受访者对此尤为认同, 他们中有 68% 认为提升安全性是采用 IaC 的一个关键推动因素, 持这一观点的 DevOps 受访者占 48%。69% 的

图 8. 采用基础设施即代码 (IaC) 的主要原因



问题: 使用基础设施即代码 (IaC) 的最重要驱动因素有哪些?

调查对象: 所有受访者 (人数: 1286)

资料来源: 思科《2022 年全球混合云趋势报告》

在如何构建现有 IaC 功能方面, DevOps 和 CloudOps 受访者的观点有所不同...

DevOps 和 CloudOps 受访者认为, 管理云安全也是 IaC 的主要用例之一。IaC 在管理复杂应用方面发挥了重要作用 (61%), 特别是对于使用 10 个以上公共云的组织 (72%)。

担任 DevOps 和 CloudOps 角色的受访者也看到了 IaC 在提升开发效率 (52%) 和改进基础设施一致性 (52%) 方面所具备的能力。从受访者的地理位置来看, 拉丁美洲超过一半的组织表示, 降低风险 (52%) 是他们使用 IaC 的主要驱动因素, 在北美地区, 持这一看法的组织占 34%。

在如何构建现有或未来 IaC 功能上, DevOps 和 CloudOps 受访者的观点有所不同, 有的认为应

扩展现有管理系统 (36%), 有的认为应使用基于 SaaS 的 IaC 服务 (34%) 或构建全新的开发环境 (30%)。在确保 IaC 安全性所需的步骤方面, DevOps 和 CloudOps 受访者最关注的是识别易受攻击的设置和扫描 IaC 配置以发现易受攻击的设置, 并将这两方面视为优先事项 (各占 55%)。这种偏好可能与组织关注更广泛的云安全问题有关。值得注意的是, 受访者对这些漏洞问题的关注度要高于身份和访问管理 (41% 的受访者) 以及嵌入式密码 (47%), 而这两个领域也是基于云的基础设施中最普遍存在的安全问题。显然, 这些都是受访者非常关注的安全问题。



结论: 几乎所有组织都在使用或计划使用云原生技术来移动或重构应用。基础设施即代码 (IaC) 有助于加快应用开发流程, 同时提升安全性。



结论

混合和多云模式已成为企业常态。如果采用得当，这些模式将有助于组织提升安全性、性能、业务敏捷性和运营弹性。这些模式有助于组织采用一系列前沿技术，以提升应用开发和运营效率。参与本次调查的组织依赖多云实现交付，他们都在广泛、深入地使用这项技术。他们的优势在于对云的使用和运营采用了更成熟的方法。他们希望充分发挥敏捷性、可扩展性和技术优势，同时期望利用 SaaS 运营平台、自动化和 AIOps 来管理成本和复杂性。

即使是最有效的混合云方法，也会增加与安全性和运营复杂性相关的挑战。混合云环境需要各利益相关者相互协作，以确定技术决策对业

务其他领域和整体混合云策略的影响。组织需要使用统一的云运营模式，以支持各种不同的用户和云框架。云运营、网络和 DevOps 团队展开主动一致的协作有助于确保安全性、效率和敏捷性。随着组织寻找新方法和加快创新速度，这些运营挑战将持续存在。

混合云和多云模式具有很多优势。但要想充分发挥这些优势，组织必须掌握相应技能，同时提升运营能力。他们必须认识到，混合云环境对基础设施有深远影响。如果不能切实有效地保护和管理工作，就有可能在市场中失去竞争优势。



如需了解详细信息，请访问 https://www.cisco.com/c/zh_cn/solutions/hybrid-cloud.html。



调查方法

本报告引用的调查数据由 451 Research (隶属于 S&P Global Market Intelligence) 收集自全球 2500 多名担任云计算、DevOps 和企业网络角色的 IT 决策者和专业人士的反馈, 构成独立网络调查的一部分。思科是本次调查的委托方。思科《2022 年全球混合云趋势报告》于 2022 年 4 月 11 日至 5 月 6 日完成。本次调查在北美、拉丁美洲、亚太地区和西欧的 13 个国家/地区进行, 包括美国、加拿大、巴西、墨西哥、澳大利亚、中国、印度尼西亚、韩国、日本、新加坡、英国、法国和德国。

本次调查旨在研究混合云趋势, 因为这些趋势与企业的整体基础设施和全球网络策略息息相关。本报告探寻了全球各组织通过采用新技术和新流程实现混合云承诺的进展情况, 并提出相关建议, 以帮助各组织将对混合云的期望与当前现状、互补和新兴技术相结合。

© 2022 思科和/或其附属公司。版权所有。Cisco 和 Cisco 徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表, 请访问以下网址: www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1110R) 08/22



The bridge to possible