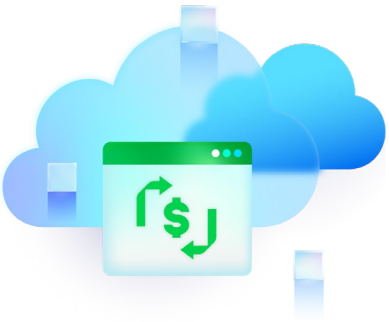
掌握混合云备份成本、安全和管理

混合云备份成功的关键洞察和最佳实践

内容

介绍

这本电子书旨在提供动态资源，提供全面概述和可行洞察，帮助您做出明智的战略决策，从而使您的组织拥有一个成本优化且安全的环境。无论您是 IT 专业人士、业务领导者还是公司云团队成员，本电子书都旨在加深您对管理云成本、安全性和备份的复杂性的理解，以便您自信从容地应对不断变化的混合和多云环境。



控制云成本

安全备份

统一管理

第 1 章：控制云成本

在混合云和多云环境中，成本控制至关重要，这或许可以解释为什么 82% 的组织将管理云支出视为其首要业务挑战。[1] 如果资源分布在内部基础架构和多个云服务中，则会加剧管理的复杂性，并可能产生高昂支出。如果没有成本控制措施，组织将面临因重复工作、资产利用不足和资源错位而产生不必要费用的风险。

简而言之，您必须计划、实施和优化才能实现有效且经济高效的云战略。[2] 通过全面理解和遵守以下指南，组织将能够最大限度地提高其云存储解决方案的财务效率。

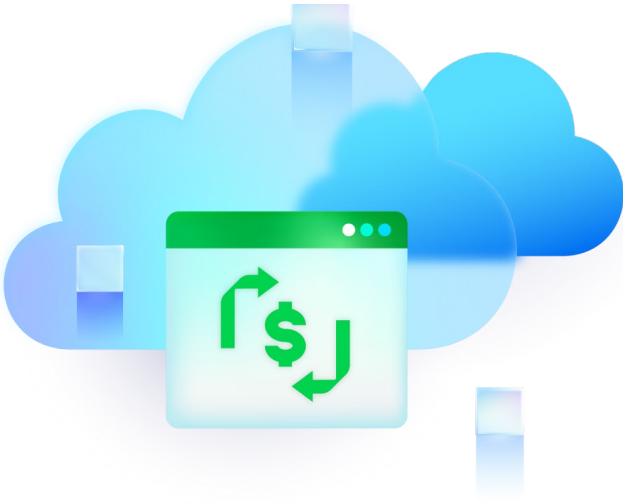
计划

快照与备份

首先，在负责管理混合云或多云环境时，了解快照和备份之间的区别至关重要。

快照是数据集的时间点副本，通常用于快速恢复目的。然而，与存储快照一样，云服务快照通常存储在它们应该保护的同一卷上。因此，它们无法防范所有数据丢失场景，如主数据存储意外删除、损坏、安全事件等。

另一方面，备份是存储在不同位置的数据集的单独副本。它们提供了额外的保护层和恢复点，因此在发生人为错误或安全事件时，您可以灵活地恢复数据。借助备份，组织可确保全面的网络弹性和恢复选项，使其成为确保数据弹性和业务连续性的首选。



[1-2] 削减云成本的考虑因素

成本计算器

利用云技术可能要付出高昂成本。如果没有适当的关注和研究，则可能会使组织面临意外的高昂支出和超支。因此，组织必须正确规划、监控和优化其使用情况，以打造成本优化的环境。超大规模云服务提供商和第三方供应商提供了许多工具，可帮助组织预测其支出。主动预测及持续监控和警报可通过大小调整实例、自动扩展、终止未使用的资源、数据生命周期管理等措施来帮助控制高昂支出。

成本计算器在数据保护方面尤其有用，因为企业需要创建并存储多个数据副本，而且存储时间通常很长。在不影响弹性的情况下平衡服务级别目标 (SLO)、保留和预算可能很棘手，但通过适当的计算和评估，这肯定会变得更容易。

实施

生命周期策略

高级数据生命周期策略对于在整个生命周期内以经济高效的方式管理数据至关重要，尤其是在云环境中。这些策略是一组规则和自动化，用于规定从创建数据到删除数据的处理方式。它们决定了数据应何时迁移到不同的存储层、应保留多长时间以及何时应归档或清除数据。通过根据数据的使用年限、访问模式和相关性自动将数据迁移到经济高效的存储层，组织可以大幅降低存储成本。

同样，保留策略可能会删除出于法律或业务原因不再需要的数据。采用这种细粒度控制有助于确保组织不会在不需要的高级存储上超支，并确保运营支出与实际数据使用量和价值保持一致。

压缩

在云存储设置中实施数据压缩具有多种优势。首先，文件大小的减小可直接转化为更低的存储成本。云存储提供商通常根据存储的数据量收费；通过压缩数据，您可以存储更少的字节并产生更少的成本。压缩还能够加快数据传输速度并减少网络带宽消耗，这在处理基于网络的大规模数据传输或备份时当然至关重要。

在考虑将数据压缩作为一项节省成本的措施时，组织应评估其数据的性质、访问频率以及与云存储提供商相关的特定功能和成本。

优化

自动化流程

采用自动化工具已成为弹性和可扩展数据管理策略的基石，充当定义的规则集，规定如何以及何时启动、维护和停用数据备份，而无需人工干预。

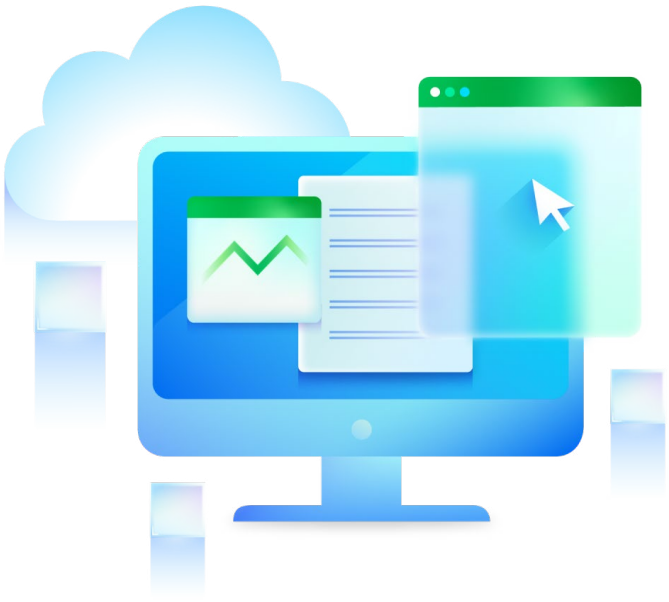
这些策略可能会考虑数据类型、重要性及数据变化频率等因素，以确定备份频率和方法。自动化工具通过处理有时容易出现人为错误的日常、耗时的任务来减轻 IT 团队的负担；它们可以在高峰时段扩大规模，然后在较安静时段缩小规模，以确保一致的性能、节约资源和减少费用。

监控备份

特别是对于云服务，所提供的灵活性和可扩展性可能会导致复杂性，尤其是在备份策略方面。随着组织规模的扩大，其数据保护需求也会增长。随着运营环境的变化，组织的初始备份配置变得不合适的情况并不少见。

审查备份策略不仅需要检查备份的频率和成功率，还需要检查数据管理，并识别暴露出弹性和合规性差距的未受保护资源。

Veeam 等组织提供的工具通过跨平台支持和增强型功能（如预测分析、集中管理的单一平台和高级成本管理功能）带来更高价值，提供更复杂的分析，这种分析在跨多个云提供商的大型或复杂环境中很有用。



第 2 章：构建安全云备份

数据保护对于各种规模的企业都是必不可少的。95% 的企业表示对他们的云安全态势感到中度到极度担忧[3]，这非常令人震惊，这一担忧源于一个简单而严酷的现实：网络威胁不断演变，破坏性事件的频率在不断提高。85% 的组织在去年遭遇过至少一次勒索软件攻击，事实证明，有必要实施全面的云备份策略。[4]

无论组织认为他们的安全和保护措施有多么彻底，完美的防御几乎无法实现。避免的每一次攻击都是一次胜利，但只要有一次疏忽，就会发生入侵 — 由于 93% 的网络攻击针对的是备份，因此，总有一天您的组织必须将重点从防止网络攻击转移到限制破坏并恢复正常运营。[5]

那么，你可以做些什么来准备呢？

[3] 2022 年 Fortinet 云安全报告
[4] 2024 年勒索软件趋势报告，Veeam
[5] 93% 的网络攻击以备份存储为目标，迫使受害者支付赎金
[6] 3-2-1 备份规则是什么？

遵循 3-2-1-0-0 规则

3-2-1-0-0 规则是一种适用于所有环境的数据备份策略，包括云。它建议使用三个数据副本，存储在两种不同类型的介质上，其中一个副本保存在异地。“0-0”方面强调需要物理隔离和不可变性，以及在备份和恢复测试和流程期间实现零错误。该规则可确保数据冗余、防止硬件故障以及防止因自然灾害、人为错误或网络威胁导致的数据丢失。遵守 3-2-1-0-0 原则可最大限度地降低永久数据丢失的风险，并确保云中关键数据的可用性和可恢复性。

将 3-2-1-1-0 规则纳入云备份策略 可提高数据防御计划的深度和广度。 6 这是一种行之有效的方法，将冗余和弹性融入到数据管理结构中，确保组织能够及时从数据丢失中恢复，从而最大限度降低运营停机时间并减轻数据相关灾难的后果 。

物理隔离

物理隔离一直是数据保护领域的主流，通常通过将备份存储在弹出磁带上来实现，从而将备份数据与网络物理分离。然而，在云中，我们无法控制物理基础架构，并且网络连接始终处于打开状态，因此必需进行**逻辑隔离**。

在三大云提供商 Amazon Web Services（AWS）、Microsoft Azure 和 Google 云中，将备份生产负载逻辑分离需要进行规划和实施的专用帐户、订阅和 / 或项目 — 甚至私有云或其他云 — 将保护数据与生产隔离开来。无论是在内部还是在云中生产，都是如此。逻辑隔离（以及下面讨论的所需精细访问控制）对于防止威胁行为者侵入您的环境并破坏备份数据至关重要。

零信任和最小权限访问

“最小权限原则”是**零信任网络安全**的基本原则，提倡给予工作所需的最低级别的用户权限。[7] 在云环境中，可以通过 Identity and Access Management (IAM) 规则、基于角色的访问控制 (RBAC) 和多重身份验证 (MFA) 的组合来实现最小特权。

IAM 系统是控制用户身份及其对云中各种资源的访问不可或缺的一部分。它们通过细粒度的细节管理权限，允许管理员准确指定用户可以对哪些资源执行哪些操作。启用 IAM 可以显著降低未经授权访问或意外数据暴露的风险。

RBAC 通过为角色而不是单个用户分配权限来更进一步。然后根据用户需要执行的特定任务为用户分配角色。此模型简化了用户权限的管理，使得随着工作职能的发展或组织内人员的变化而调整角色变得更加简单。通过为单个用户分配角色而不是特定权限，可以更轻松地确保在整个组织中实施一致的访问策略。

MFA 是一项重要的安全功能，可以增加一层保护。通过要求用户提供两个或更多个验证因素才能访问云资源，MFA 降低了凭据泄露导致安全漏洞的风险，从而大大增加了攻击者进行未经授权的访问的难度。

[7] **零信任网络安全**

访问权限的日常维护对于防止“权限蔓延”至关重要，权限蔓延是指用户随着时间的推移积累不再需要用于其工作职能的访问权限。组织需要定期审查和修改用户权限，确保撤销旧凭据、访问权限适合当前角色，并且在完成后删除为执行特殊任务而授予的任何临时权限。此外，定期轮换凭据（例如密码和访问密钥）可以避免潜在泄露。

不变性

数据不可变性是云环境中数据保护和完整性的关键方面。随着组织越来越依赖云存储来存储其关键数据，实施防止未经授权的修改或删除的措施变得至关重要。

云中的不可变性是通过 Amazon S3 对象锁、Azure Blob Storage 的不可变存储等功能有效实现的，可将备份数据置于一写多读 (WORM) 状态。通过这种方式，数据可以保持不可更改（例如加密、损坏或删除），保持数据完整性，并确保在灾难发生时干净、成功地还原数据。

加密

由于数据泄露现在已成为主要云安全问题之一，因此，加密可确保即使在未经授权的访问或盗窃的情况下，数据仍然无法读取，因此数据对攻击者来说价值不大。为了促进用户友好且强大的加密功能，云提供商将提供专门的服务。

AWS Key Management Service (KMS) 提供了一种可扩展且安全的方式来管理用于加密数据的加密密钥。[8] AWS KMS 与其他 AWS 服务集成，提供集中式架构，允许跨 AWS 工作负载加密数据。AWS KMS 可确保安全使用加密密钥，而且从来不向最终用户暴露加密密钥，并且它将维护一套严格的策略，规定如何以及何时使用、审核和轮换密钥。

Azure Key Vault 是 Microsoft Azure 提供的一项服务，用于管理应用程序和服务保持安全可能需要的加密密钥、机密和其他敏感信息。[9] 借助 Azure Key Vault，只要使用在这些安全保管库中存储和管理的密钥，就可以对备份数据进行加密。这不仅增强了数据的安全防护，而且还提供了对密钥生命周期管理的全面控制，包括密钥的创建、存储、授权和删除。

AWS KMS 和 Azure Key Vault 都提供了实现静态加密和传输过程中加密的方法。它们还提供广泛的日志记录功能，可以跟踪加密密钥的使用时间和位置。这种级别的审核对于检测和响应任何未经授权的访问尝试至关重要。此外，使用这些服务还有助于满足法规合规要求，即通过加密保护敏感 数据。

[8] AWS KMS 加密
[9] 第 4 步：启用数据加密

第 3 章：管理混合云 / 多云备份

在可扩展性、灵活性和成本效益的推动下，各种规模的组织都纷纷采用云技术。软件即服务 (SaaS)、平台即服务 (PaaS) 和基础架构即服务 (IaaS) 等云解决方案提供了不同级别的控制和抽象，可满足各种需求，使企业能够专注于创新，而不是管理硬件和数据中心。

日益复杂的现代数据环境清楚地表明，传统的数据管理实践已无法满足需求。组织必须通过采用高级云管理工具、采用自动化和编排的工作流程、确保云服务之间的通信以及全面、强大的安全措施来应对这种复杂性。

混合云与多云管理

混合云和多云管理是企业云采用的两种截然不同的策略，各自满足不同的业务需求和技术要求。

混合云模式将内部基础架构（即私有云）与公有云相结合，支持在它们之间共享数据和应用程序。[10] 这种方法为企业提供了更大的灵活性和更多的部署选项，这对于在私有数据中心进行大量投资的公司或处理因监管要求而可能不适合在公有云中使用的敏感数据的公司尤其有利。

多云模式涉及使用来自不同提供商的多种云服务。[11] 多云方案不是统一私有云和单个公有云，而是允许组织使用不同云提供商的一流服务来满足特定的应用程序要求。通过多云战略，公司可以避免厂商限制，根据性能、功能或成本效益为不同的任务选择不同的提供商。

如何在混合云和多云策略之间进行选择通常取决于企业的特定业务需求、技术要求和战略目标。[12] 然而，通过云提供商跨平台移动数据并不容易，通常会使组织受到厂商限制。

[10] 混合云
[11] 多云
[12] 多云与混合云

克服混合云和多云环境中的挑战

混合云和多云环境具有诸多优势，可满足企业对灵活性、弹性及服务优化的期望。尽管如此，这些福利也带来了一系列挑战，如果未解决，可能会阻碍组织充分发挥其潜力。

能见度：随着在不同平台上部署各种服务，对成本、性能指标和安全性进行全面监控成为一项复杂的任务。通过传统方法几乎无法获得全面视图，因此需要使用统一的仪表板作为集成控制面板，并且这些仪表板能将来自多个云服务的数据合并到单一、连贯的界面中。通过提供实时洞察和分析，IT 经理能够快速做出明智决策，掌握整个云生态系统的脉搏，包括识别潜在风险或低效问题。

成本管理：如果没有谨慎的治理，随着实例激增以及服务超出其初始范围（通常称为“云扩散”），成本很容易急剧上升。有效的成本管理策略通常涉及云管理软件，该软件提供复杂的工具来跟踪和优化资源使用情况。此外，遵循标准的云最佳实践（例如设置预算警报和使用云提供商提供的成本管理解决方案）有助于防止意外支出并保持财务控制。

合规：虽然云提供商通常会提供旨在满足严格合规标准（例如政府、医疗保健或金融）的专门服务，但这些服务可能会被孤立，或者因提供商而异。这一现实需要细致的规划和部署策略，以确保将工作负载放置在适当的云上。合规性不仅涉及数据的物理位置，还涉及访问、审核、交互和数据管理等流程 — 所有这些都需要精心协调，以避免不合规及随之而来的后果。

数据保护和备份：环境的多样性可能需要使用多种工具和管理方法来保护数据。这增加了层层的运营开销，并且需要负责管理这些系统的人员提供大量的专业知识。此外，数据的可移植性（移动备份或跨云边界执行灾难恢复操作）也是一个至关重要的考虑因素。组织需要确保不同云之间的互操作性和兼容性，以及灵活处理不同数据格式、服务模型和 API 的能力。

应对这些挑战需要一种深思熟虑的战略方法，利用工具、实践和专业知识的正确组合。从易于管理的统一仪表板到管理软件的主动成本控制，从严格的合规性要求到全面的数据保护机制，混合云和多云环境都需要注重细节和对卓越运营的坚定承诺。

总结

当面临将新云服务整合到您的技术堆栈中时，现有的传统工具和单点产品无法提供您所需的数据弹性和自由度。但事实并非如此...

Veeam 可在混合和多云环境中为您的团队提供全面、行业领先的数据弹性和恢复功能。原生保护、安全和恢复混合环境合并至一个无缝平台，可以消除多个单点产品和传统工具的麻烦和低效问题。更棒的是，Veeam 可随时为您提供无与伦比的数据自由，帮助您跨任何平台备份、恢复、迁移和现代化应用程序与数据并实现现代化。

无论您是支持安全协议、简化数据保护，还是转向现代云 基础架构和平台，都可以看看 Veeam。我们将消除在混合或多云环境中确保弹性的复杂性，以便您将资源集中在创新和增长上，同时确信您的数据受到保护且可恢复。

观看我们的云成本管理网络研讨会，看成本节约现场实践演示

了解有关 Veeam 混合云解决方案的更多信息

关于 Veeam Software

Veeam® 是数据弹性领域的 #1 全球市场领导者，其坚信每家企业在中断后都应该能够绝地反弹，并且能够在需要时随时随地自信地控制其所有数据。Veeam 称之为极致弹性，我们致力于通过创新方法来帮助我们的客户实现这一目标。Veeam 解决方案专门通过提供数据备份、数据恢复、数据自由、数据安全和数据智能功能增强数据弹性。借助 Veeam，IT 和安全领导者可以高枕无忧，因为他们知道其应用程序和数据受到了保护，并且始终在云、虚拟、物理、SaaS 和 Kubernetes 环境中可用。Veeam 总部位于西雅图，在 30 多个国家和地区设有办事处，保护着全球超过 550,000 家客户，包括 74% 的全球 2000 强公司，他们信赖 Veeam 保证其业务正常运行。极致弹性始于 Veeam。请访问 www.veeam.com.cn 了解更多信息或关注 Veeam 的 LinkedIn @veeam-software 和 X @veeam。