



白皮书

# 使用负载均衡最佳 实践优化 Web 性能 和可靠性

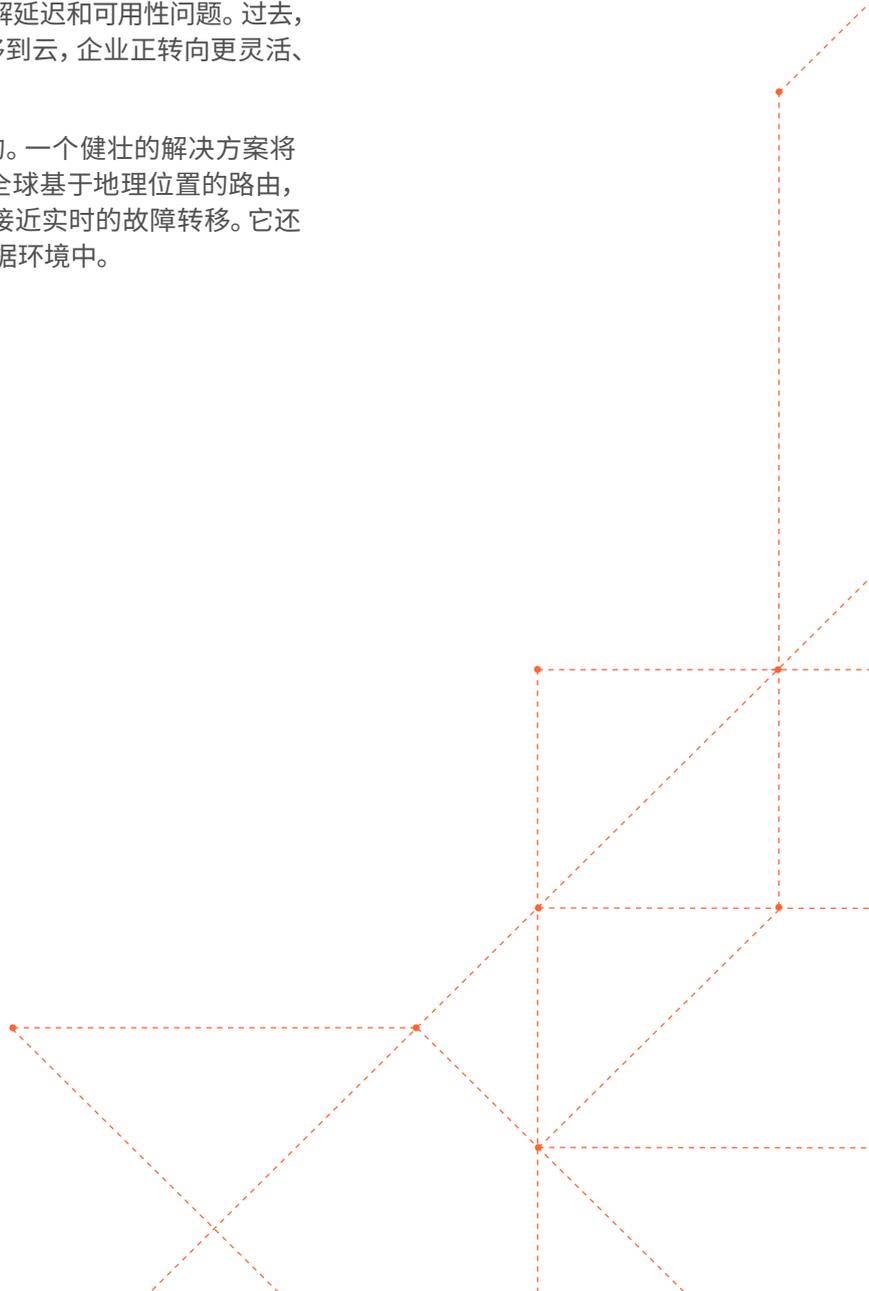
# 摘要

每年，企业因网站运行缓慢和停机而损失数百万美元，主要表现为收入减少。站点和应用运行缓慢或不可用也会对内部生产力产生不利影响，并导致搜索引擎排名下降。这些性能和可靠性问题可能由诸多因素引起，包括：

- 服务器过载或运行不正常
- 最终用户和服务器之间的距离
- DNS 解析缓慢
- 分布式拒绝服务 (DDoS) 攻击
- 访问者用于访问互联网的设备类型

负载均衡器将 Web 流量均匀地分散到服务器网络中，确保任一服务器不会超载，即使一台服务器出现故障，Web 资源仍然可用，从而缓解延迟和可用性问题。过去，企业在数据中心部署物理负载均衡器，但随着计算迁移到云，企业正转向更灵活、更低成本、更易使用、基于云的负载均衡解决方案。

然而，并非所有基于云的负载均衡解决方案都是相同的。一个健壮的方案将集成全球内容分发网络 (CDN) 并提供各种功能，例如全球基于地理位置的路由，DDoS 防御，第 3、4 层负载均衡功能，分析能力，以及接近实时的故障转移。它还将无缝集成到当今大多数企业拥有的多云和混合云数据环境中。



# 延迟和宕机的原因

**延迟和宕机对业务有显著的负面影响。企业遭遇延迟和宕机的原因很多**

## 服务器负载分布不均衡

利用率过高的服务器运行更加缓慢，请求争夺有限的资源。超负荷的服务器会降低网站和应用程序的性能，甚至使服务器完全不可用。

有效的负载平衡将工作负载均匀地分布在服务器网络上，从而显著提高性能。例如，一家 SaaS 公司的客户在全球不同地区遭遇延迟问题。然而，在部署 Cloudflare Load Balancing 后，他们立即体验到了延迟的改善，页面加载时间缩短了 2-3 秒。<sup>1</sup>

## 地理距离

全球互联网普及率呈爆炸式增长。**2023 年 1 月，世界人口的 64.4% 已经联网，而且在 2022 年有超过 1 亿人首次上网。**<sup>2</sup>

互联网的全球化对网络性能产生了多方面的影响。随着活跃用户数量的增加，每个用户的可用带宽会减少，从而导致延迟。

过去几年中，随着远程办公扩大，用户也变得更加分散。过去企业环境中的东西向流量如今在南北方向移动，穿越

互联网到达远程用户。这种转变给基础设施增加了额外的负荷，并延长了流量从用户到服务器的往返距离，增加了延迟。<sup>3</sup>

## 站点和应用复杂性

互联网经历了多个演变阶段，每次迭代都给网站和应用程序增加了更多的复杂性。现代网站比以往任何时候都更加笨重，自 2011 年以来，总页面大小持续增加。<sup>4</sup>

视频会议、在线游戏和类似的在线服务也增加了网站和应用程序的大小和复杂性。这些应用程序消耗大量带宽，并对延迟敏感，给企业的网络和基础设施带来额外的负荷和压力。



## 设备类型

超过60%的网站流量来自移动设备,<sup>5</sup>而大约一半的移动用户希望应用程序在两秒或更短的时间内响应。<sup>6</sup>因此,有必要针对移动设备设计和优化网站和应用程序。

5G 移动网络的出现并不能保证移动用户拥有高速、无限制的网络访问。客户转化率取决于在移动设备上快速交付内容的能力。

## DNS 解析缓慢

DNS 解析器将域名转换为 IP 地址,为计算机提供路由 Web 资源请求所需的信息。DNS 解析是访问在线资源的重要第一步,优化 DNS 解析对于最大化性能至关重要。

并非所有 DNS 提供商都为解析速度进行了优化。运行缓慢的 DNS 提供商解析每个 DNS 查询可能需要 20-120 ms。<sup>7</sup>最快的 DNS 提供商可在 20 ms 内解析查询;例如,Cloudflare DNS 平均解析时间为 8.92 ms。<sup>8</sup>

这些数字可能看起来无关紧要,但需要考虑到渲染单个页面可能需要多个 HTTP 和 DNS 请求。例如,平均每个网页在桌面电脑上涉及 71 个 HTTP 请求,在移动设备上涉及 66 个请求。<sup>9</sup>尽管其中一些请求可能是针对同一域名的,但每个唯一的 DNS 请求都会增加延迟。

## 服务器运行状况

服务器可能因为各种不同的原因而出现故障。一旦服务器崩溃,托管在其上的应用程序和网页就可能对用户不可用。

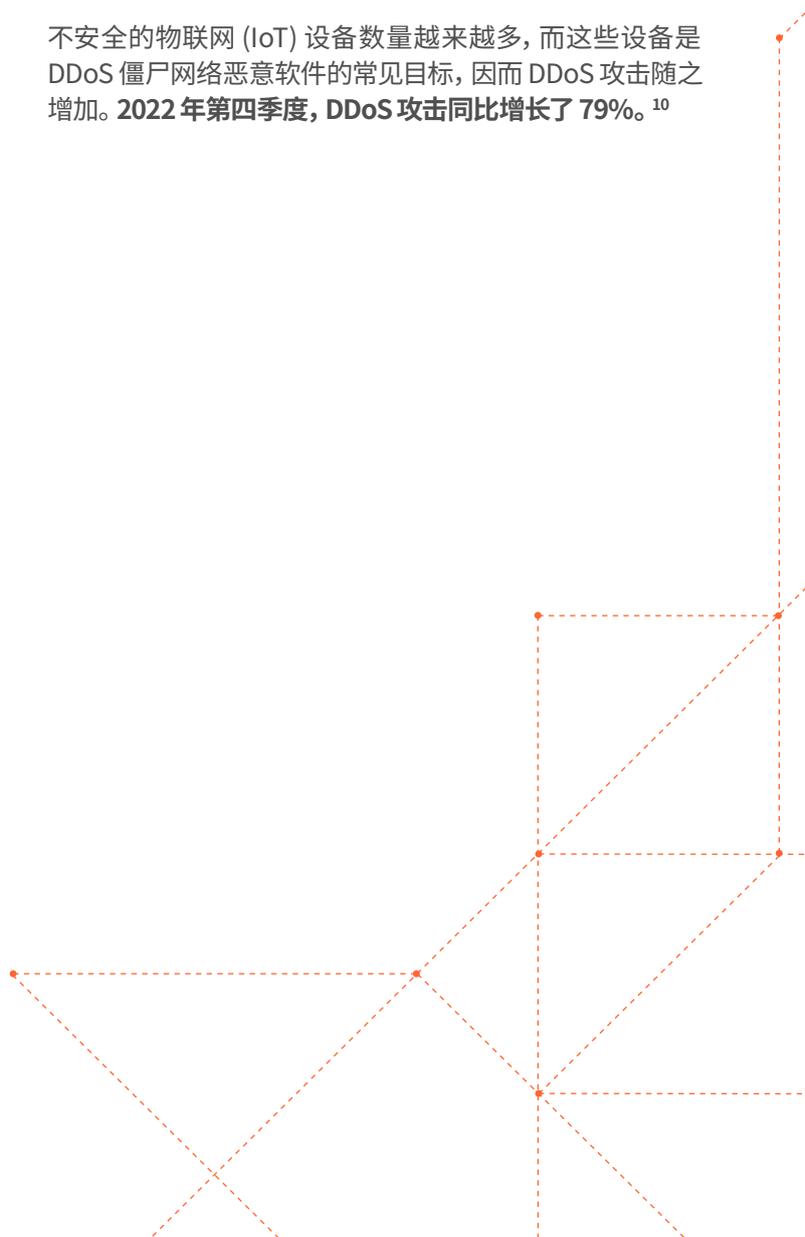
用户也在消费更多视频内容,而在当今世界上,如果某件事走红,大量流量可能会使你的服务失去响应。在 IT 基础设施中添加负载均衡解决方案和冗余变得至关重要,以防止合法流量像 DDoS 攻击一样导致应用程序崩溃。

负载均衡解决方案应该监视服务器运行状况,以维持应用程序的可用性。否则,流量可能会无意中被路由到存在问题的服务器,从而导致长时间的延迟或用户中断。

## 网络攻击

分布式拒绝服务 (DDoS) 攻击对在线服务的运行状况和可用性构成了严重的威胁。DDoS 攻击向网络服务器发送大量垃圾请求,淹没合法流量,并有可能充当掩盖其他攻击的烟雾弹。

不安全的物联网 (IoT) 设备数量越来越多,而这些设备是 DDoS 僵尸网络恶意软件的常见目标,因而 DDoS 攻击随之增加。2022 年第四季度,DDoS 攻击同比增长了 79%。<sup>10</sup>



# 延迟和宕机的代价

网络延迟和站点加载时间对客户体验和转化率有着重大影响。事实上，短至 100 ms 的延迟都会对消费者行为产生可衡量的影响。

网络延迟可对业务产生各种负面影响。延迟和宕机的常见代价包括：

- **收入损失：**公司越来越多地通过其网站与客户建立联系并提供服务。由于宕机和延迟，客户无法访问组织的网站，或由于页面加载时间缓慢而放弃购物车，从而导致销售机会的错失。
- **客户流失：**页面加载缓慢等同于失去销售机会。**加载时间为 1 秒的页面转化率三倍于加载时间为 5 秒的页面。**<sup>11</sup>
- **生产力损失：**内部应用程序的延迟和宕机也会影响员工的生产力。例如，**美国员工平均每使用一分钟应用程序就要花费约 1 秒钟的等待时间。**<sup>12</sup>这相当于每年失去超过 4 天的工作时间。
- **品牌可见度：**Google 将页面速度作为桌面和移动搜索的排名因素。<sup>13</sup>加载速度缓慢页面可能会损害品牌的可见度。
- **法律和监管合规性：**在线服务提供商可能会受到包括可用性和正常运行时间在内的服务级别协议 (SLA) 的约束。宕机和延迟可能会导致罚款和潜在的法律诉讼。

宕机对企业来说是非常昂贵的。宕机的平均成本约为每分钟 9000 美元，<sup>14</sup>但具体因行业和企业规模而异。例如，Facebook 在一次长达 14 小时的宕机中估计损失了 9000 万美元，相当于每分钟超过 10.7 万美元。<sup>15</sup>



# 了解负载均衡

延迟和宕机给组织带来巨大的成本。负载均衡器是一种服务，位于源服务器网络和互联网之间，通过将负载均匀分配到多个服务器上来帮助减轻这些成本。通过防止个别服务器因流量激增而不堪重负，确保应用程序的可靠性、效率和响应能力。

## 为什么需要负载均衡器

最终用户访问一个网页时，源服务器接受请求并进行响应。其中包括处理请求、收集所需的内容，并将其发送到用户的浏览器中进行渲染。

单个源服务器能够处理的请求数量取决于物理基础设施和代码复杂性。然而，一个网站接收到的请求数量可能会超过最好的硬件和最高性能的 Web 应用程序的处理能力。如果发生这种情况，那么请求可能需要在队列中等待——增加延迟——或者被完全丢弃。

负载均衡器可以防止单个服务器遇到这些问题。负载均衡器位于最终用户和一组源服务器之间，可以将负载均匀地分配到服务器池中。通过减轻每个服务器的负载，负载均衡器可以提高网站的性能和韧性。

## 传统负载均衡器

传统上，负载均衡器部署在本地数据中心中。通常，这些服务器是使用专用硬件实现的，但也提供虚拟化选项。

为了确保韧性，这些设备通常成对部署，以便在主系统发生故障时备份系统可以接管。

这些基于传统硬件的负载均衡器存在重大限制，它们带来的挑战包括如下：

- **前期成本：**负载均衡器设备必须在使用前购买和安装，这可能相当昂贵，而且所有成本是提前发生的。
- **可扩展性：**基于硬件的解决方案有设定的最大容量限制，如果组织经历异常的流量激增，负载均衡器可能会成为瓶颈。随着组织带宽需求的增长，现有的解决方案必须通过增加硬件或更换新硬件来进行扩展。
- **地理限制：**负载均衡器设备只能部署在公司可以安装物理硬件的数据中心，因此它们只能管理本地应用程序的流量，而不能管理云端应用程序的流量。
- **技能缺口：**公司内部的负载均衡器主要必须由内部人员进行配置和操作。公司可能难以吸引和留住具备必要技能的员工。
- **缺乏灵活性：**硬件负载均衡器连接到组织的物理网络基础设施，因此公司难以适应不断变化的需求。

## 下一代、基于云的负载均衡器

绝大多数公司正在迅速向云端迁移。87% 的组织使用多云基础设施，72% 的组织具有混合云环境，即同时使用公共云和私有云。<sup>16</sup> 越来越多的企业应用程序不能再依赖于硬件负载均衡器。

健壮、独立且基于云的负载均衡器可与混合环境中基于传统硬件的设备一同使用，也可与公有云原生的负载均衡器一同使用。独立的负载均衡器是一个中立、与云无关的层，处于企业基于硬件和公有云原生的负载均衡器之上。企业选择主要供应商来将所有流量引导到那里。当负载均衡器检测到故障时，它自动将流量路由到备份提供商或地区。如果企业在公有云或自有基础设施中体验到间歇性的网络连接中断，独立的云负载均衡器自动故障转移到运行正常的提供商或服务器。

可以在云中部署虚拟化负载均衡器，以管理到这些应用程序的流量。这些基于云的负载均衡器提供各种好处，包括以下：

- **近乎无限的可扩展性：**云负载均衡器具有云的灵活性和可扩展性优势。可以根据需要快速增加额外的容量，以管理企业 Web 应用程序的流量激增。
- **使用基于用量的计费方式可以节省成本：**云负载均衡器通常以基于服务的模式提供。公司只需为使用的容量付费，而不必购买过大的设备。
- **更大的地理覆盖范围：**理想情况下，云负载均衡器应该在覆盖全球的网络上运行，使其可以接近位于任何地方的应用程序。



- **易于配置和管理：**如果负载均衡器作为一项服务提供，服务提供商将执行大部分配置和管理工作。这减少了组织的开销和对专业人员的需求。
- **灵活性：**独立的云负载均衡器可轻松地重新配置或移动，以支持在新环境下运行的应用程序。这使得公司可以快速适应变化，避免供应商锁定。
- **韧性：**基于云的负载均衡器可以利用云内置的韧性和可用性保证。这降低了宕机使负载均衡器后面的应用程序离线风险。
- **功能整合：**使用基于云的解决方案，在启用负载均衡后，可以轻松地添加其他模块，如 Web 应用程序防火墙 (WAF)、机器人管理等，无需付出额外努力。对于硬件解决方案，升级通常需要更换整个硬件设备或添加物理模块或刀片。这些修改可能迫使公司安排维护停机，导致客户失去保护，并对企业产生负面影响。

# 评估基于云的负载均衡解决方案时 要注意什么

基于云的负载均衡解决方案可以帮助组织降低延迟和停机时间，并减少它们对业务的影响。在评估负载均衡器解决方案时，应考虑以下功能：

## 集成全球内容分发网络 (CDN)

负载均衡器和 CDN 都是旨在减少延迟和提高可用性的解决方案。CDN 在网络边缘缓存静态内容，减少请求和响应需要传输的距离。此外，通过从分布式 CDN 服务器提供内容，可以减轻源服务器的负载。

将负载均衡与内容分发网络 (CDN) 集成，以优化内容传递。负载均衡器将请求在 CDN 集群和源服务器之间进行分配，以优化性能和最小化带宽消耗。

## 基于地理位置的路由

服务器和最终用户之间的地理距离对请求和响应的延迟有巨大的影响。负载均衡器应该将流量路由到最近的可用基础设施，从而最大限度地减少所需的传输距离。例如，英国的流量应被引导到位于伦敦的数据中心，而非纽约的数据中心。

负载均衡器还应该提供优化的、快速的 DNS 查找。例如，应将 DNS 查询定向到最近的健康 DNS 服务器，以最大限度地减少 DNS 查找引起的延迟。



## 应用交付与安全的统一

负载均衡器和 CDN 网络必须设计成能够解决各种安全问题。例如，DDoS 攻击对服务器的运行状况和可用性构成严重威胁。因此，应当对 CDN 网络应该进行扩展和保护，以承受甚至最大规模的 DDoS 攻击。

负载均衡器和 CDN 面临的另一个主要问题是符合隐私和安全标准。例如，负载均衡器应该支持使用 TLS/SSL 来加密客户数据并验证 Web 流量。

## 第 3 & 4 层负载均衡功能

DDoS 攻击可以在 OSI 模型的多个层进行操作。容量耗尽型 DDoS 攻击是指将大量流量发送到 Web 服务器上实现各种业务的端口。例如，DDoS 攻击可以瞄准 SMTP 端口以破坏电子邮件，或用于实现自定义游戏协议和其他在线服务的自定义端口。负载均衡器应具有针对 3/4 层 DDoS 攻击的防护功能，并有足够的容量在这些攻击期间维持正常的服务。

## 接近实时的故障转移

基于云的负载均衡器常常依赖于公共 DNS，后者存在更改传播缓慢的问题，推迟了发生问题时的故障转移。负载均衡器应该使用具有较短 TTL 的 DNS 解析器，确保故障转移可以在几秒钟内发生。

## 多云和混合云支持

大多数公司拥有多云环境或混合云环境。为了避免供应商锁定，降低复杂性，并尽量减少多云和混合环境中的错误配置，请确保负载均衡解决方案是一个中性层，在本地和任何公共云中都能工作。

一个不与供应商无关的负载均衡器不会取代云供应商的原生负载均衡器或传统的硬件设备，而是与它们协同工作，使多云基础设施正常发挥功能。

## 自动化和 DevOps 支持

负载均衡器被设计成将请求分发到一组服务器上。随着敏捷的 DevOps 流程和云计算的出现，企业应用基础设施可能会不断变化，使其成为一个不断变动的目标。

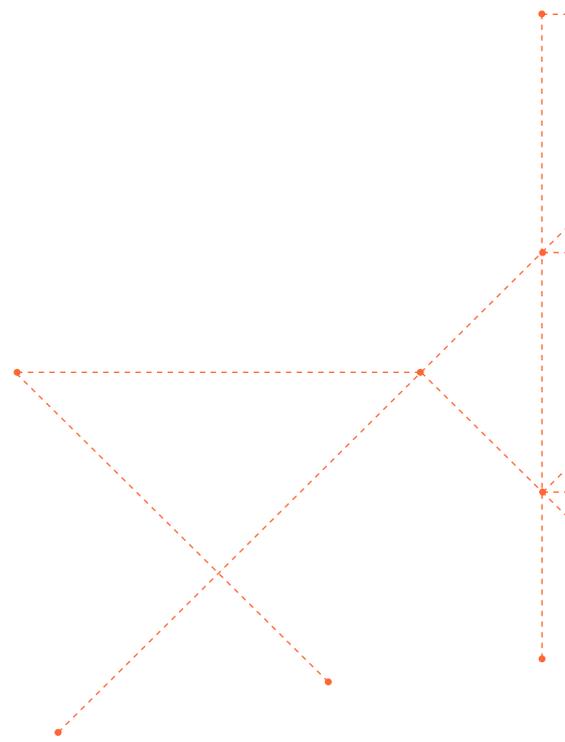
依赖人类操作者定义和实施配置更改会给可用性和性能构成重大风险。负载均衡器应该整合自动化和 DevOps 支持，以确保随着企业 IT 基础设施的发展，快速大规模地进行更改。

## 易用性

即使是对于技术熟练的人员，负载均衡解决方案的配置和管理都可能是一项耗时且资源密集型的任务。优秀的云负载均衡器配置和设置仅需数分钟，且管理非常简单。该解决方案应该支持图形用户界面和强大的 API，并且应该易于重新配置，以支持不断发展的业务需求。

## 详细分析

负载均衡器位于最终用户和应用程序之间，用于收集可据以行动的业务情报。负载均衡器可以看到客户行为、应用程序性能、安全状态和其他运营见解。负载均衡解决方案应该捕获这些分析数据并与您现有的分析提供商进行集成。

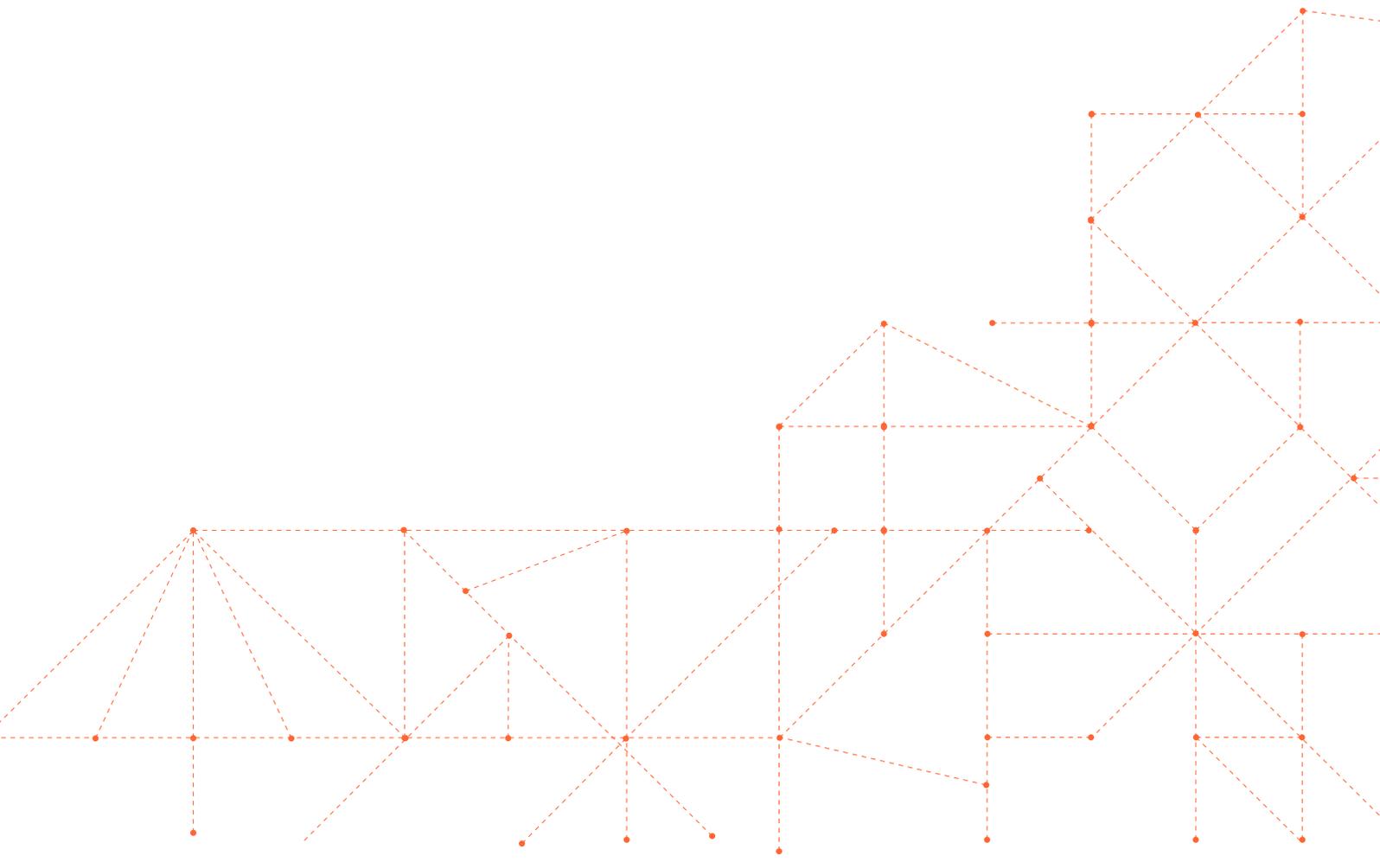


# 总结

现代网站和应用程序如果不使用负载均衡器，将无法正常运行或保持持续在线状态。功能强大、基于云的负载均衡器远胜于传统基于硬件的解决方案。

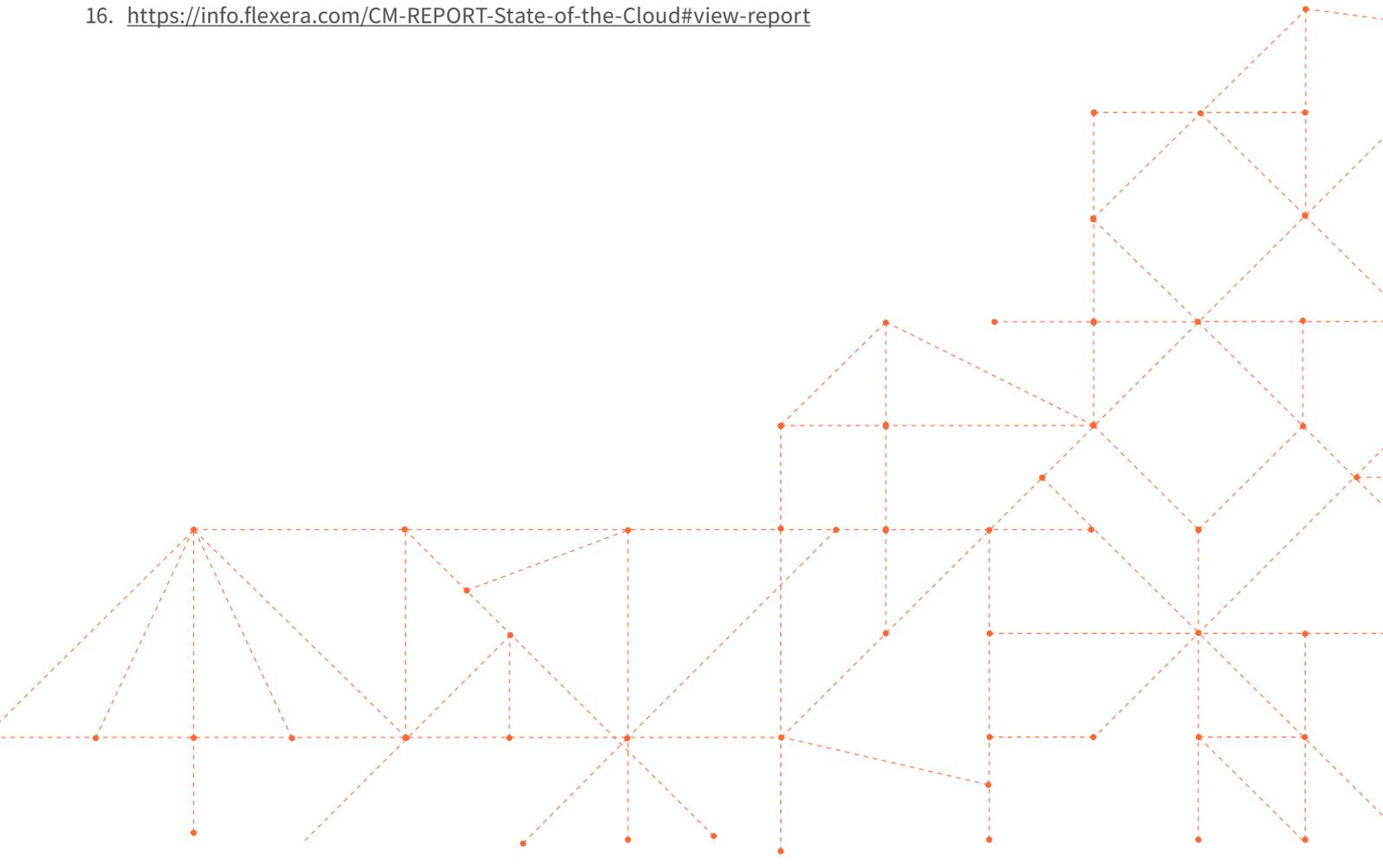
除了成本较低、易于使用和可扩展之外，基于云的独立负载均衡器还可以增强传统基于硬件的负载均衡器以及公共云供应商提供的专有解决方案，确保 Web 资产始终保持可用和高性能。

Cloudflare 的全球网络和高性能 CDN 帮助组织最大程度地提高可用性并减少延迟。进一步了解 [Cloudflare Load Balancing](#)。



## 参考资料

1. <https://www.cloudflare.com/case-studies/crisp/>
2. <https://datareportal.com/global-digital-overview>
3. <https://www.techwalla.com/articles/network-latency-milliseconds-per-mile>
4. <https://httparchive.org/reports/state-of-the-web#bytesTotal>
5. <https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/#yearly-2011-2022>
6. [https://techbeacon.com/sites/default/files/gated\\_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf](https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf)
7. <https://sematext.com/glossary/dns-lookup-time/>
8. <https://www.dnsperf.com/>
9. <https://httparchive.org/reports/state-of-the-web#reqTotal>
10. <https://blog.cloudflare.com/zh-cn/ddos-threat-report-2022-q4-zh-cn/>
11. <https://www.portent.com/blog/analytics/research-site-speed-hurting-everyones-revenue.htm>
12. <https://www.apmdigest.com/the-impact-of-app-performance-on-productivity>
13. <https://developers.google.com/search/blog/2018/01/using-page-speed-in-mobile-search>
14. [https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11\\_51190\\_1.pdf](https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf)
15. <https://www.ccn.com/facebooks-blackout-90-million-lost-revenue/>
16. <https://info.flexera.com/CM-REPORT-State-of-the-Cloud#view-report>





© 2023 Cloudflare Inc.保留所有权利。Cloudflare 徽标是 Cloudflare 的商标。所有其他公司和产品名称分别是与其关联的各自公司的商标。

010 8524 1783 | [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [www.cloudflare.com](http://www.cloudflare.com)

REV:BDES/4505.2023APR27