



白皮書

利用负载均衡最佳化 Web 效能和可靠性的 最佳做法

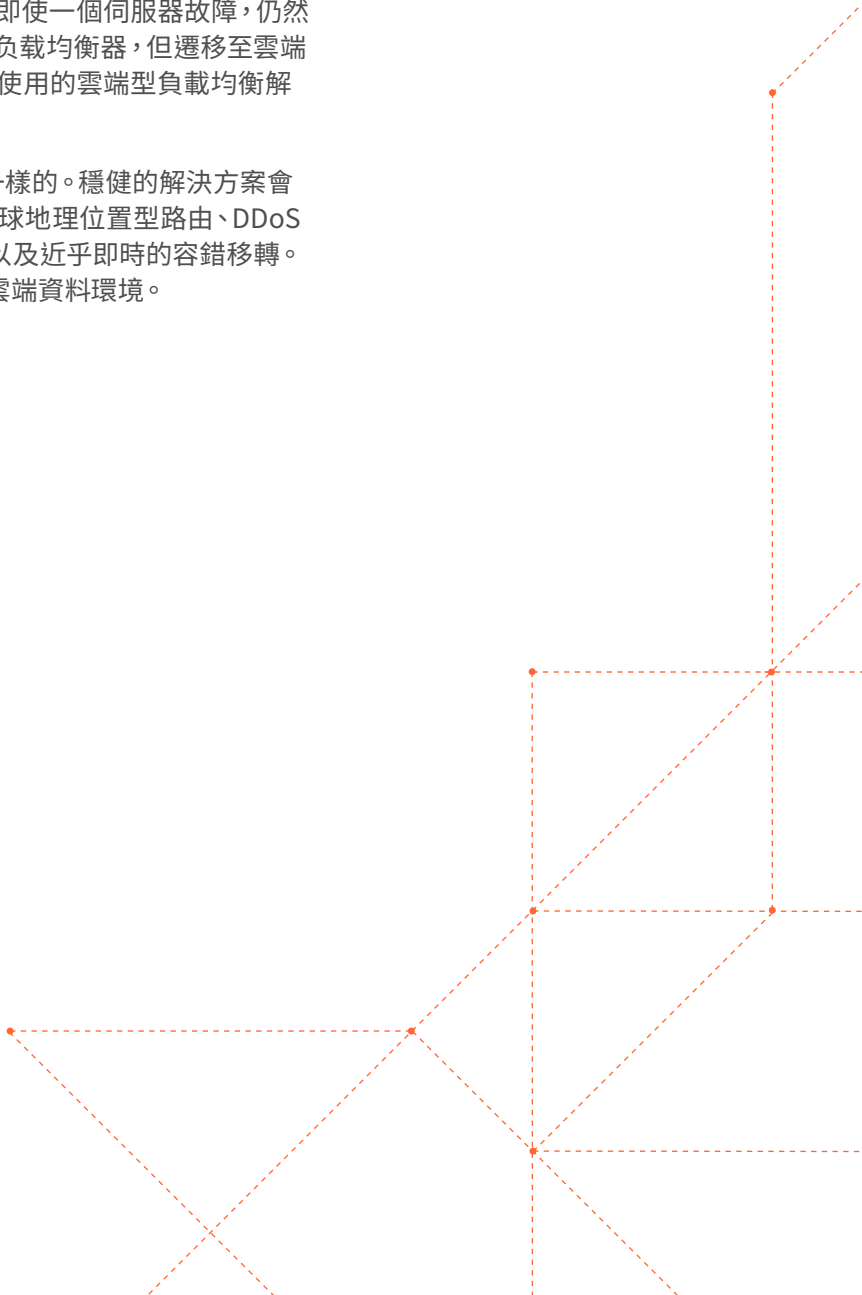
報告摘要

每年，企業都會因網站遲緩和停機損失數百萬美元，且大多表現為營收損失。緩慢或無法使用的網站和應用程式也會對內部生產力造成負面影響，並導致搜尋引擎排名下降。導致這些效能和可靠性問題的因素有很多，包括：

- 伺服器工作過量或運作異常
- 終端使用者與伺服器之間的地理距離
- DNS 解析速度較慢
- 分散式阻斷服務 (DDoS) 攻擊
- 訪客用於存取網際網路的裝置類型

負載均衡器透過將網路流量均勻地分散到各伺服器網路，藉此緩解延遲和可用性問題，同時確保沒有任何一個伺服器會不堪負荷，而且即使一個伺服器故障，仍然可以使用網路資產。以往，公司會在資料中心部署實體負載均衡器，但遷移至雲端運算後，企業即改為採用更為靈活、成本更低且更方便使用的雲端型負載均衡解決方案。

但是，並非所有雲端型負載均衡解決方案的建立都是一樣的。穩健的解決方案會與全球內容傳遞網路 (CDN) 整合，並提供以下功能：全球地理位置型路由、DDoS 復原能力、第 3 層和第 4 層負載均衡功能、分析能力，以及近乎即時的容錯移轉。還將無縫整合至多數企業目前都擁有的多雲端和混合雲端資料環境。



延遲和停機的原因

延遲和停機會對業務造成極大的負面影響。公司會遇到各種原因造成的延遲和停機

伺服器工作負載分佈不均

由於要求爭搶有限的資源，過度使用的伺服器執行速度較慢。負擔過重的伺服器可能會降低網站和應用程式效能或使其完全無法使用。

有效的負載均衡會在伺服器網路中均勻地分佈工作負載，可顯著提高效能。例如，一個 SaaS 公司的客戶在全球不同地區都存在延遲問題。然而，在部署 Cloudflare Load Balancing 之後，其延遲立即有所改進，網頁載入時間縮短了 2-3 秒。¹

地理距離

全球網際網路普及率呈爆炸式增長。2023 年 1 月，64.4% 的世界人口已連線，而連線人數在 2022 年首次超過了一億。²

網路網路全球化對網路效能產生了多方面的影響。隨著作用中使用者數量的增加，每個使用者的可用頻寬會減少，從而導致延遲。

在過去幾年中，隨著遠端工作的發展，使用者也變得越來越分散。以前被視為在企業環境內東西移動的流量現在開始南北移動，因為它會穿越網際網路，到達遠端使

用者。這種轉換會為基礎架構增加負載，並延長流量從使用者傳輸到伺服器然後再傳回的來回距離，從而增加延遲。³

網站和應用程式複雜性

網際網路的演進經歷了多個階段，每次迭代都會增加網站和應用程式的複雜性。現代網站比以往更為龐大，自 2011 年以來，總頁面大小一直在穩步攀升。⁴

視訊會議、線上遊戲和類似的線上服務也會增加網站和應用程式的大小和複雜性。這些應用程式會耗用大量頻寬且對延遲敏感，為企業網路和基礎架構上的傳遞帶來了額外的負載和壓力。



裝置類型

超過 60% 的網路流量來自行動裝置，⁵ 大約一半的行動使用者希望應用程式的回應時間不超過兩秒。⁶ 必須針對行動裝置設計和最佳化網站和應用程式。

5G 行動網路的出現並不能保證行動使用者的網路存取不受限制且速度很快。客戶轉換率取決於在行動裝置上快速傳遞內容的能力。

DNS 解析較慢

DNS 解析程式會將網域名稱轉譯為 IP 位址，從而為電腦提供所需的資訊來路由 Web 資產的要求。DNS 解析對存取線上資源而言是至關重要的第一步，而最佳化該解析對最大程度提升效能至關重要。

並非所有 DNS 解析程式都針對速度進行最佳化，很多 DNS 提供者解析每個 DNS 查詢會花費 20-120 毫秒。⁷ 最快速的 DNS 提供者解析查詢只需不到 20 毫秒；例如，Cloudflare DNS 解析查詢的平均時間為 8.92 毫秒。⁸

儘管這些數字可能看似微不足道，但一定要考慮到，轉譯單一頁面可能需要多個 HTTP 和 DNS 要求。例如，**平均每個網頁在桌上型電腦上包含 71 個 HTTP 要求，而在行動裝置上包含 66 個要求。**⁹ 儘管其中部分要求可能適用於相同的網域，但每個唯一的 DNS 要求都會增加延遲。

伺服器健康狀況

伺服器可能會因為形形色色的原因而無法運作。如果伺服器當機，則使用者可能無法使用其託管的應用程式和網頁。

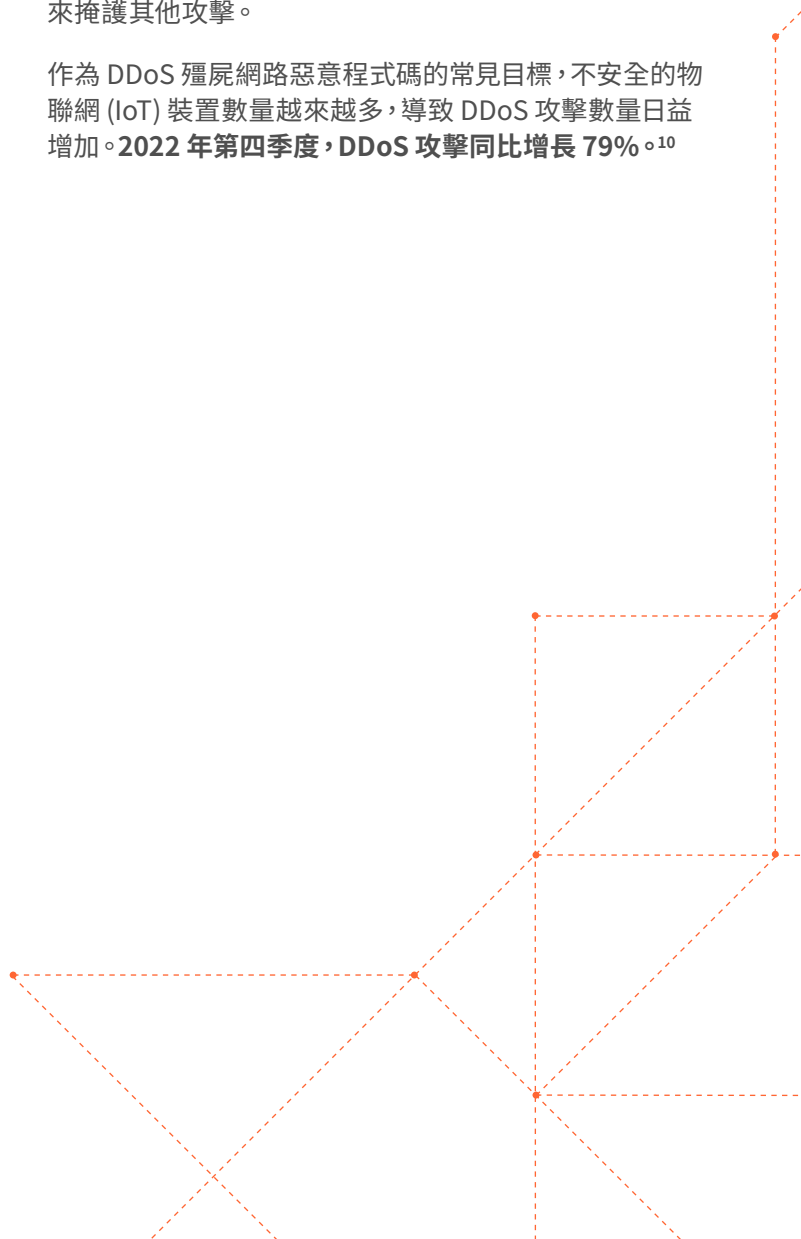
使用者也在耗用更多的視訊內容，而在當今世界，如果什麼東西像病毒一樣傳播，則大量的流量可能會導致您的服務無回應。在 IT 基礎架構中新增負載均衡解決方案和備援對於防範合法流量像 DDoS 攻擊一樣摧毀應用程式至關重要。

負載均衡解決方案應監控伺服器健康狀況，以維持應用程式可用性。否則，可能會無意中將流量路由至發生問題的伺服器，導致使用者長時間的延遲或服務中斷。

網路攻擊

分散式阻斷服務 (DDoS) 攻擊對線上服務的運作狀況和可用性構成重大威脅。DDoS 攻擊利用垃圾郵件要求淹沒了 Web 伺服器，不僅淹沒了合法流量，還可能充當煙幕來掩護其他攻擊。

作為 DDoS 殭屍網路惡意程式碼的常見目標，不安全的物聯網 (IoT) 裝置數量越來越多，導致 DDoS 攻擊數量日益增加。**2022 年第四季度，DDoS 攻擊同比增長 79%。**¹⁰



延遲和停機的成本

網路延遲和網站載入時間對客戶體驗和轉換率具有重大影響。實際上，即便延遲只有短暫的 100 毫秒，也會對客戶行為造成顯著的影響。

延遲會對業務造成各種各樣的負面影響。延遲和停機的成本通常包括：

- **營收損失**：越來越多的公司透過網站與客戶建立聯繫並提供服務。當客戶因為網頁載入時間較長而無法存取組織的網站或放棄購物車時，停機和延遲可能會導致錯過銷售機會。
- **客戶流失**：網頁載入時間較長等同於銷售損失。載入時間為 1 秒的網頁的轉換率是載入時間為 5 秒的網頁的 3 倍。¹¹
- **生產力損失**：內部應用程式的延遲和停機也會影響員工的生產力。例如，美國員工平均每使用應用程式一分鐘，等待時間約為 1 秒。¹² 這相當於每年損失超過 4 個工作日。
- **品牌知名度**：Google 使用網頁速度作為桌上型電腦和行動裝置搜尋的一個排名因素。¹³ 載入速度較慢的網頁會損害品牌知名度。
- **法律和監管合規性**：線上服務提供者很可能會受到服務等級協定 (SLA) 的約束，其中包括可用性和正常運作時間。停機和延遲可能會導致處罰和法律訴訟。

對業務而言，停機的代價十分高昂。停機的平均成本約為每分鐘 9000 美元，¹⁴ 但會根據產業及業務規模而變化。例如，Facebook 在 14 個小時的服務中斷中損失了約 9000 萬美元，每分鐘損失超過 10.7 萬美元。¹⁵



了解負載平衡

延遲和停機為組織帶來了高昂的成本。負載均衡器是一種位於原始伺服器網路和網際網路之間的服務，可透過在多台伺服器中平均分佈來協助降低這些成本。這可透過確保個別伺服器不會因流量暴增而不堪重負，從而確保應用程式的可靠性、效率和回應性。

為何需要負載均衡器？

當終端使用者造訪網頁時，原始伺服器會收到此要求並進行回應。這包括處理要求、收集所需內容並傳送它以在使用者瀏覽器中呈現。

單一原始伺服器可以處理的要求數取決於實體基礎架構和程式碼複雜性。然而，網站收到的要求數甚至會超過最佳硬體和效能最高的 Web 應用程式。如果發生這種情況，則要求可能需要在佇列中等待（這會增加延遲），也可能完全捨棄要求。

負載均衡器可防止個別伺服器成為這些問題的受害者。負載均衡器位於終端使用者和原始伺服器叢集之間，並在伺服器集區中均勻地均衡負載。透過減少每台伺服器上的負載，負載均衡器可提高網站效能和復原能力。

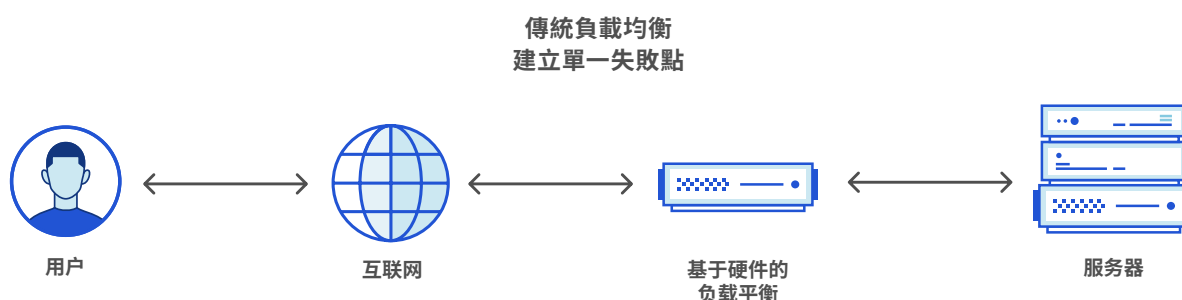
傳統負載均衡器

以往，負載均衡器部署在內部部署資料中心。通常使用專用硬體實作，但也可以使用虛擬選項。為了確保復原能力，

這些裝置通常成對部署，以便主要系統發生故障時，備份系統可以接管。

這些傳統硬體型負載均衡器具有很大的局限性。它們帶來了以下挑戰：

- **前期成本：**必須先購買並安裝負載均衡器設備，然後才能使用。不僅成本高昂，而且所有成本都是預先支付。
- **可擴展性：**硬體型解決方案已設定最大容量，如果組織遇到流量異常激增，則負載均衡器可能會變成瓶頸。隨著組織頻寬需求的增長，必須擴充現有解決方案或使用新硬體將其取代。
- **地理限制：**負載均衡器設備只能部署在公司可安裝實體硬體的資料中心。因此，它們只能管理內部部署應用程式而非雲端型應用程式的流量。
- **技能差距：**內部負載均衡器必須主要由內部人員設定和操作。公司可能很難吸引並留住具有必要技能組合的員工。
- **缺乏靈活性：**硬體負載均衡器設備會連線至組織的實體網路基礎架構。因此，公司很難適應不斷變化的需求。



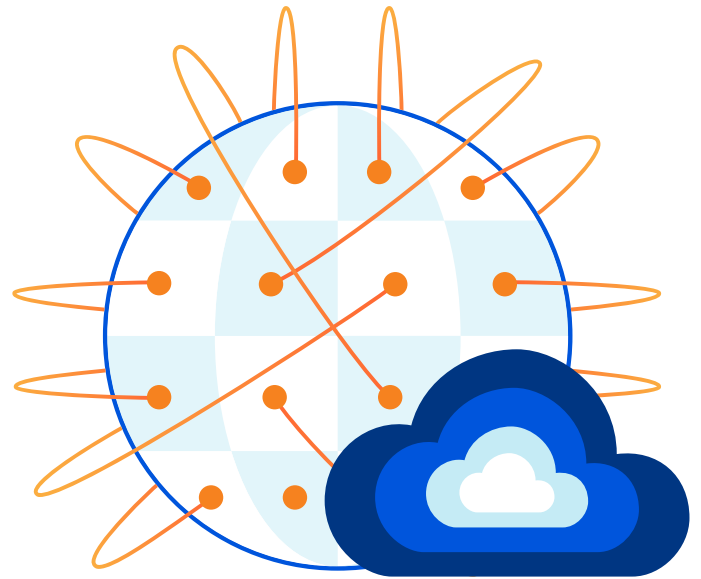
新一代雲端型負載均衡器

絕大多數公司都在快速向雲端遷移。87% 的組織具有多雲端基礎架構，72% 具有混合雲端環境，即同時包含公用雲端和私人雲端。¹⁶ 越來越多的企業應用程式不再依賴硬體負載均衡器。

穩健的獨立雲端型負載均衡器可與混合環境中的傳統硬體型裝置以及公用雲端原生負載均衡器組合使用。獨立負載均衡器屬於中立的雲端不受限層級，其位於企業硬體型和公用雲端原生負載均衡器之上。企業會選擇一個主要提供者來導向所有流量。當負載均衡器偵測到故障後，即會自動將流量路由傳送至備份提供者或區域。如果企業在公用雲端或自有基礎架構中遇到服務中斷或間歇性的網路連線問題，獨立雲端型負載均衡器將自動容錯移轉至運作正常的提供者或伺服器。

虛擬化負載均衡器可以部署在雲端，來管理這些應用程式的流量。這些雲端型負載均衡器具有各種各樣的優點，包括：

- **幾乎無限的可擴展性：**雲端負載均衡器具有雲端靈活性和可擴展性的優點。可根據需要快速增加更多容量，來管理企業 Web 應用程式的流量激增。
- **透過基於使用情況計費節省成本：**雲端負載均衡器通常在基於服務的模型下提供。公司只需為使用的容量付費，而不是購買超大的設備。
- **更大的地理區域：**理想情況下，雲端負載均衡器應在一個遍佈全球的網路上執行，以便靠近任何位置的應用程式。



- **易於設定和管理：**如果負載均衡器作為服務提供，則服務提供者會執行大部分設定和管理工作。這會減少組織的開支及其對專業人員的需求。
- **靈活性：**可以輕鬆重新設定或移動獨立雲端負載均衡器，以支援應用程式在新環境中運作。這讓公司能夠快速適應變化並避免廠商鎖定。
- **復原能力：**雲端型負載均衡器可以利用雲端的內建復原能力和可用性保證。這可降低服務中斷導致負載均衡器背後的應用程式離線的風險。
- **功能整合：**使用雲端型解決方案，在 Load Balancing 上線後，可以輕鬆地根據需要新增其他模組，例如 Web Application Firewall (WAF)、Bot Management 等，而無需任何額外工作。使用硬體解決方案，升級通常需要取代整個硬體裝置或新增實體模組或刀鋒。這些修改可能會迫使公司安排維護停機，讓客戶失去保護並對企業產生負面影響。

評估雲端型負載平衡解決方案時需要具備哪些能力

雲端型負載均衡解決方案可協助組織降低延遲和停機，並減少對業務的影響。評估負載均衡解決方案時，請嘗試尋找以下功能。

與全球內容傳遞網路 (CDN) 整合

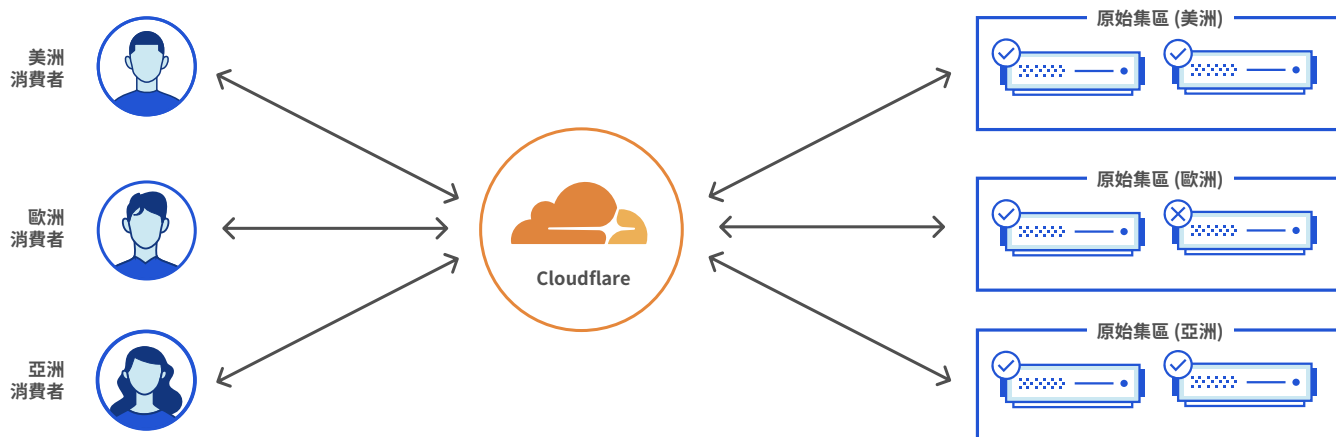
負載均衡器和 CDN 都是旨在減少延遲和提升可用性的解決方案。CDN 在網路邊緣快取靜態內容，縮短了要求和回應需要傳輸的距離。此外，透過從分散的 CDN 伺服器提供內容，減少了原始伺服器的負載。

將負載均衡與 CDN 整合可最佳化內容傳遞。負載均衡器在 CDN 叢集和原始伺服器中分佈要求，以最佳化效能，並最大程度減少頻寬消耗。

全球地理位置型路由

伺服器與終端使用者之間的地理距離對要求和回應的延遲具有極大的影響。負載均衡器應將流量路由至最近可用的基礎架構，從而最大程度縮短需要傳輸的距離。例如，英國流量應導向倫敦而不是紐約的資料中心。

負載均衡器還應提供最佳化的快速 DNS 查閱。例如，DNS 查詢應導向最近的運作正常的 DNS 伺服器，以最大程度減少 DNS 查閱所產生的延遲。



應用程式交付和網路安全的統一

負載均衡器和 CDN 網路必須旨在解決各種網路安全問題。例如，DDoS 攻擊對伺服器健康狀況和可用性構成重大威脅。因此，應擴展並保護 CDN 網路來抵禦規模最大的 DDoS 攻擊。

負載均衡器和 CDN 的另一個主要問題是遵循隱私權及安全性標準。例如，負載均衡器應支援使用 TLS/SSL 來加密客戶資料並驗證網路流量。

第 3 層和第 4 層負載均衡功能

DDoS 攻擊可能發生在 OSI 模型的多個層級。巨流量 DDoS 攻擊會使用傳送至實作各種服務之連接埠的大量流量淹沒 Web 伺服器。例如，DDoS 攻擊可以將 SMTP 連接埠作為目標來中斷電子郵件，也可以將用於實作自訂遊戲通訊協定以及其他線上服務的自訂連接埠作為目標。負載均衡器應能夠防範第 3/4 層 DDoS 攻擊，並具有足夠的容量，以在這些攻擊期間維持正常服務。

近乎即時的容錯移轉

雲端型負載均衡器頻繁依賴受到緩慢變更傳播困擾的公用 DNS，從而在發生問題時延遲容錯移轉。負載均衡器應使用具有短存留時間 (TTL) 的 DNS 解析程式，從而確保可在幾秒鐘內進行容錯移轉。

多雲端與混合雲端支援

大多數公司都具有多雲端環境或混合雲端環境。若要在多雲端和混合環境中避免廠商鎖定、減少複雜性並最大程度減少錯誤配置，請確保負載均衡解決方案為中立層級，並且可在內部部署和任何公用雲端中運作。

廠商獨立負載均衡器不會取代雲端廠商的原生負載均衡器或傳統硬體設備。但可與其協同工作，以便多雲端基礎架構順暢地運作。

自動化和 DevOps 支援

負載均衡器旨在於伺服器叢集中分佈要求。隨著敏捷性和 DevOps 處理程序以及雲端運算的出現，企業應用程式基礎架構可能會不斷變化，使其成為一個移動的目標。

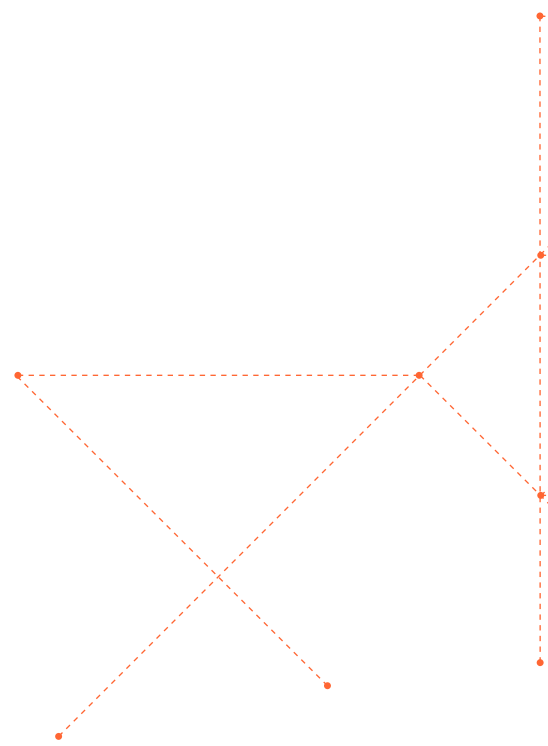
依賴人工操作員定義並實作設定變更會對可用性和效能構成重大風險。負載均衡器應整合自動化和 DevOps 支援，以確保隨著企業 IT 基礎架構的演進，可以快速進行大規模變更。

容易使用

對於技術人員而言，設定和管理負載均衡解決方案需要耗費大量的時間和資源。優秀的雲端型負載均衡器可在幾分鐘內設定完畢，而且不太需要管理。解決方案不僅應該支援圖形使用者介面和強大的 API，還應能夠輕鬆地重新設定，以支援不斷變化的業務需求。

詳盡分析

位於終端使用者和應用程式之間的負載均衡器用於收集可採取動作的商業情報。透過負載均衡器，可以瞭解客戶行為、應用程式效能、安全狀態及其他營運深入解析。負載均衡解決方案應擷取這些分析，並與現有的分析提供者整合。

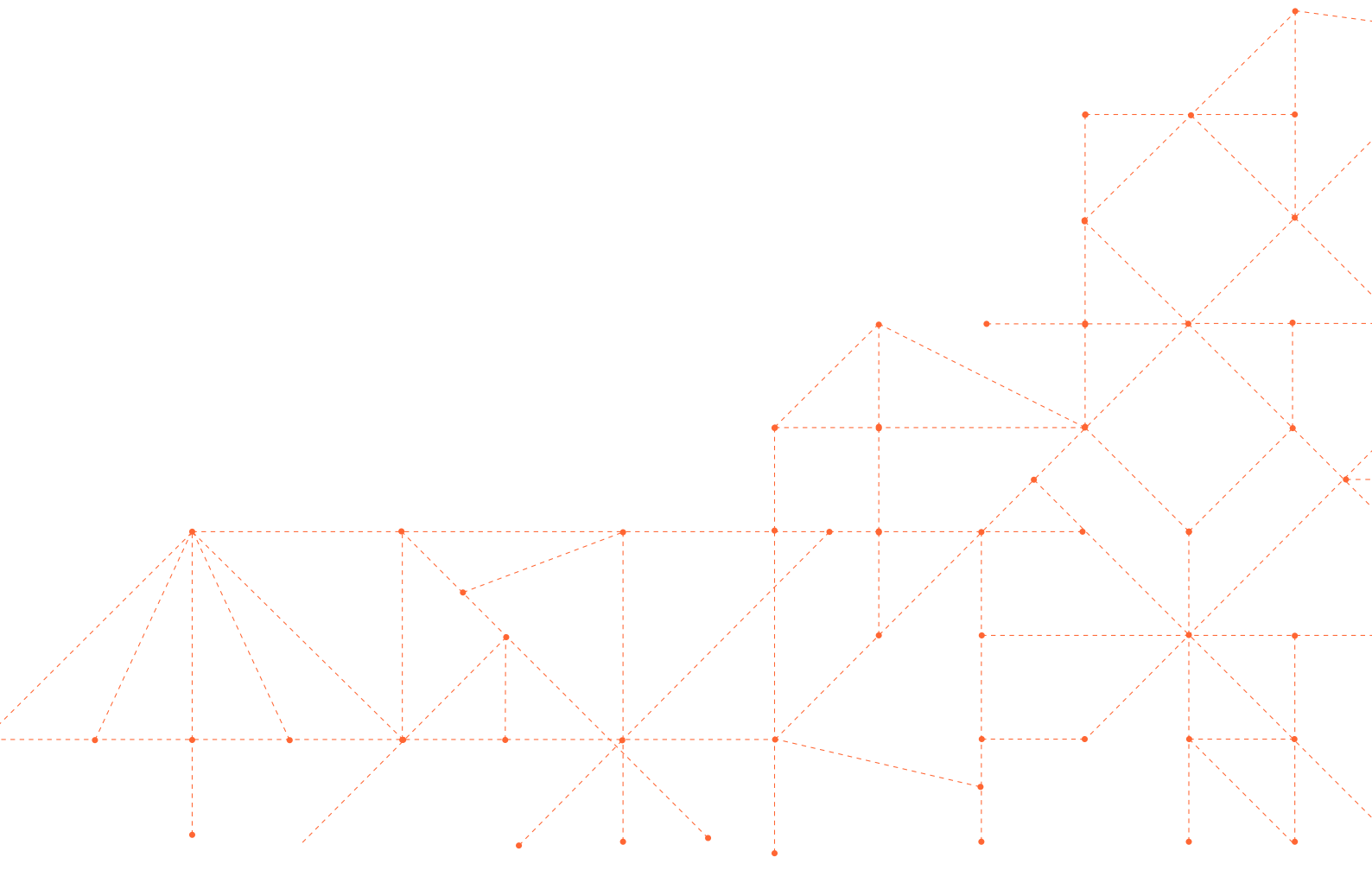


結論

如果不使用負載均衡器，現代網站和應用程式就無法正常執行或始終在線。比起傳統硬體型解決方案，穩健的雲端型負載均衡器是更好的選擇。

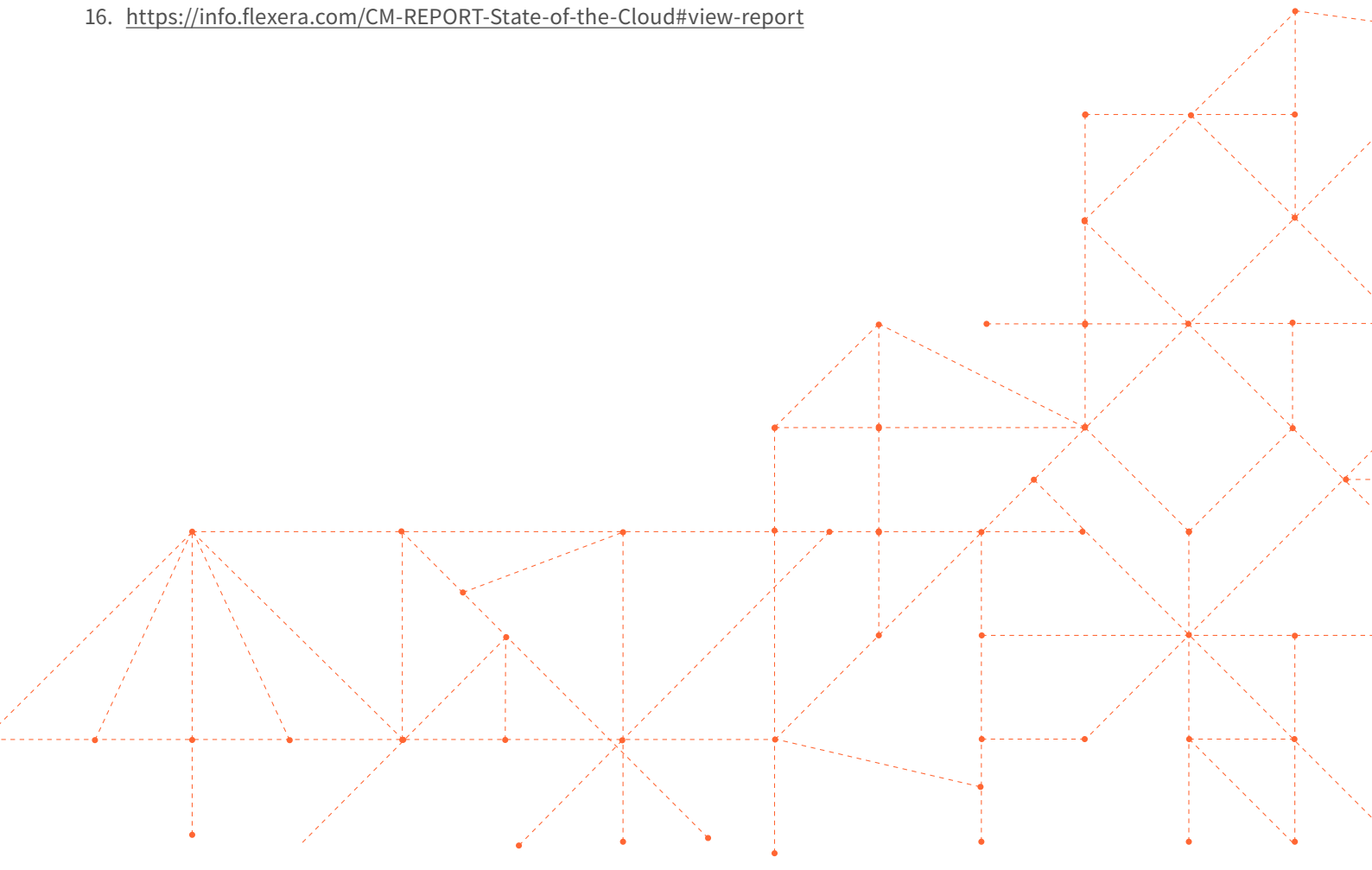
除了更為便宜、更方便使用及可擴展等特性外，獨立雲端型負載均衡器可擴充傳統硬體型負載均衡器以及由公用雲端提供者提供的專屬解決方案，從而確保 Web 資產永遠保持可用和高效能。

Cloudflare 的全球網路和高效能 CDN 可協助組織最大程度提升可用性和減少延遲。深入瞭解 [Cloudflare Load Balancing](#)。



參考文獻

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
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-tw/ddos-threat-report-2022-q4-zh-tw/>
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
15. <https://www.ccn.com/facebook-blackout-90-million-lost-revenue/>
16. <https://info.flexera.com/CM-REPORT-State-of-the-Cloud#view-report>





© 2023 Cloudflare Inc. 版權所有。Cloudflare 標誌是 Cloudflare 的商標。所有其他公司與產品名稱可能是各個相關公司的商標。

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

REV: BDES/4505.2023APR27