白皮書

# Cloudflare CDN 參考架構

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

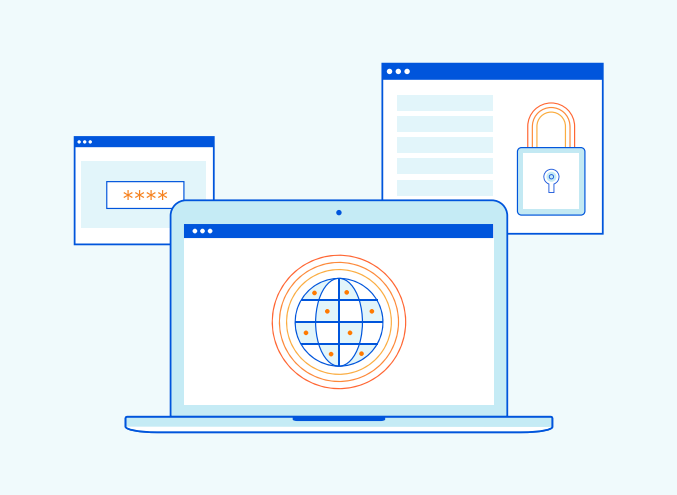
# 索引

按一下以跳到每個章節

# 概觀

每天，網際網路使用者都在享受內容傳遞網路 (CDN) 所提供的效能和可靠性帶來的好處。CDN 已成為對抗延遲的必需品，也是在網際網路上為使用者呈現內容的所有大型公司的必要條件。在為客戶提供效能和可靠性的同時，CDN 還讓公司能夠進一步保護其應用程式和削減成本。本文件討論客戶在使用 Web 應用程式時面臨的傳統挑戰、Cloudflare CDN 如何解決這些挑戰，以及 CDN 架構和設計。

# 部署 Web 應用程式的傳統挑戰




在過去幾年中，尤其是隨著 COVID-19 疫情的到來和向遠端工作的轉換，網際網路流量顯著增長，進一步增加了有效管理網路流量、減少延遲和提高效能的需求。

**在雲端或內部執行其應用程式的公司面臨以下挑戰：**

1. 實作解決方案以提高效能
2. 隨著需求的增長，擴展其架構以滿足可用性和備援需求
3. 保護其環境和應用程式，防禦不斷增長的網際網路威脅
4. 遏制與上述所有活動相關的成本

對於為全球客戶提供服務的公司而言，解決上述挑戰需要巨大的投入。傳統上，網站/應用程式集中部署並覆寫到另一個區域以供使用，或者網站/應用程式部署在少數伺服器上，有時跨多個資料中心以實現復原能力。

託管網站的伺服器稱為原始伺服器。當用戶端存取網站時，它們會從伺服器請求資源。導覽至一個網站可能從瀏覽器產生對 HTML、CSS、影像、影片等的數百個請求。對於 HTTP/2 之前的 HTTP 版本，每一個此類 HTTP 請求都需要一個新的 TCP 連線。

HTTP/2 中的增強功能允許透過單個 TCP 連線將多個請求多工處理傳送到同一伺服器，從而節省伺服器資源。然而，當伺服器回應這些請求時，仍會耗用計算和網路資源。隨著更多的用戶端存取網站，可能產生以下結果：

- 原始伺服器開始因請求過多而過載，影響可用性；公司開始考慮向外擴展以處理額外的負載
- 由於每個請求都必須到達原始伺服器，因此會因延遲而影響效能和使用者體驗
- 終端使用者面臨的延遲會與用戶端和原始伺服器之間的距離成正比，導致因用戶端位置的不同而產生不同的體驗
- 隨著原始伺服器回應不斷增加的請求，頻寬、輸出和計算成本也會急劇增加
- 即使客戶向外擴展以應對不斷增長的流量需求，他們仍然面臨基礎結構層級和應用程式層級的分散式阻斷服務 (DDoS) 攻擊

# 部署 Web 應用程式的傳統挑戰（續）

在下面的圖 1 中，沒有 CDN，只有一個位於美國的原始伺服器。隨著用戶端存取網站，第一步是 DNS 解析，通常由使用者的 ISP 完成。下一步是直接傳送至原始伺服器的 HTTP 請求。使用者體驗因其位置而異。例如，位於原始伺服器所在地的美國使用者所遭遇的延遲會低很多。而美國外的使用者所面臨的延遲則會增加，這樣會導致更高的往返時間 (RTT)。

隨著更多的用戶端對原始伺服器發起請求，網路和伺服器上的負載會增加，導致更高的延遲和更高的資源與頻寬使用成本。

從安全性角度來說，原始伺服器的基礎結構和應用程式層都容易遭受 DDoS 攻擊。DDoS 攻擊可能由殭屍網路發起，殭屍網路向原始伺服器傳送數百萬個請求，耗用資源並阻止其為合法用戶端提供服務。

此外，在復原能力方面，如果原始伺服器暫時離線，使用者將無法存取所有內容。

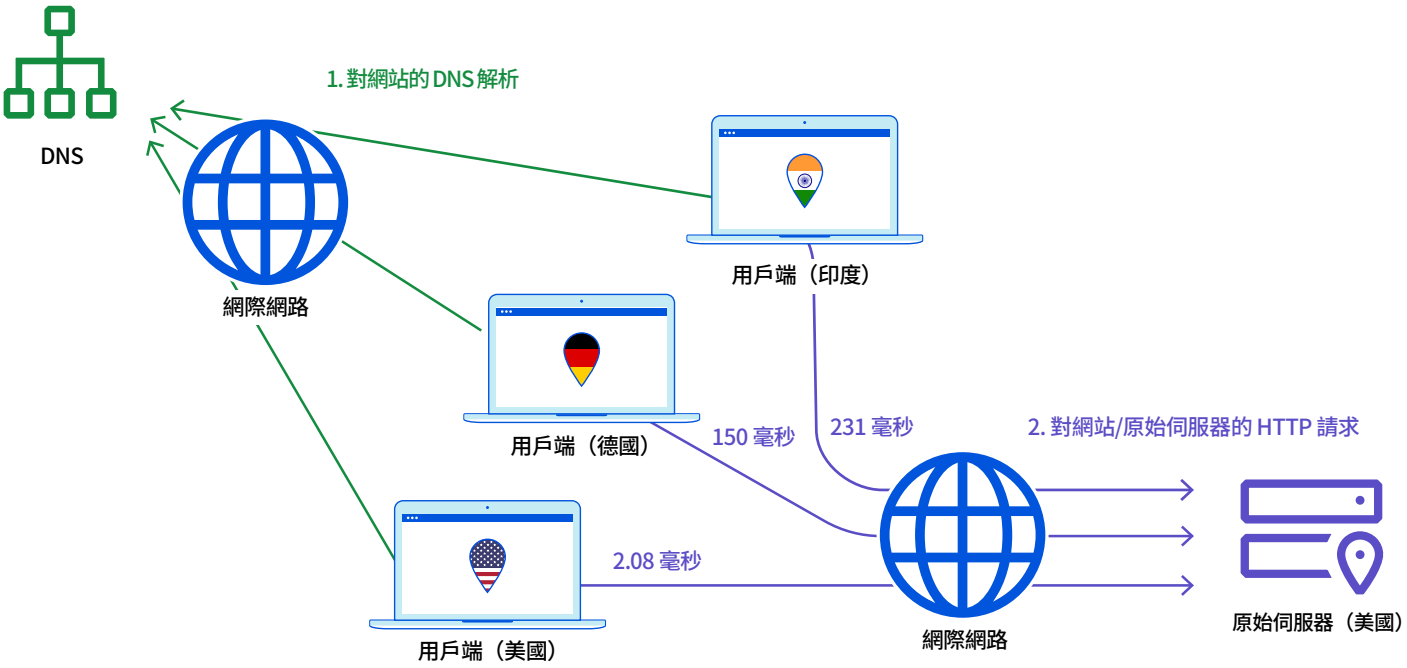



圖 1：沒有 CDN 的 HTTP 請求

# CDN 如何應對 Web 應用程式挑戰

CDN 可幫助解決客戶面臨的有關延遲、效能、可用性、備援、安全性和成本方面的挑戰。CDN 的核心目標是在盡可能靠近終端使用者或內容存取者的位置快取內容，以便為網站和應用程式減少延遲並提高效能。

CDN 在全球擁有許多資料中心位置來從源站快取內容，從而減少延遲並提高效能。目標是在盡可能靠近使用者的位置快取內容，以便在 CDN 提供者網路的邊緣快取內容。

**這樣做的影響包括：**

- **改善網站載入時間**
  以前每一個用戶端都向原始伺服器發起請求，而原始伺服器可能在相當遠的地方。使用 CDN 之後，請求被路由到本地伺服器，本地伺服器以快取的內容作出回應，從而減少延遲並提高整體效能。不管原始伺服器和用戶端位於何處，都可以為所有使用者提供更加一致的效能，因為 CDN 將盡可能提供本機快取的內容。
- **提高內容可用性和備援**
  由於每個用戶端請求不用再傳送到原始伺服器，CDN 不僅可提供效能方面的好處，還可提高可用性和備援。請求在具有快取內容的本地伺服器上進行負載平衡；這些伺服器回應本地請求，顯著降低了原始伺服器的整體負載。僅在需要時（當內容未快取或內容是動態不可快取內容時）聯絡原始伺服器。
- **加強網站安全性**
  CDN 充當反向代理，且位於原始伺服器前方。因此它可以提供增強的安全性，如 DDoS 緩解、安全憑證改進和其他最佳化。
- **減少頻寬成本**
  由於 CDN 使用快取的內容來回應請求，傳送至原始伺服器的請求數會減少，從而減少相關的頻寬成本。

部分 CDN 實作中的一個重要不同點是，它們將流量路由到各個本地 CDN 節點的方式。

**將請求路由到 CDN 節點可以透過兩種方法來完成：**

1. **DNS Unicast 路由**
   在這種方法中，遞迴 DNS 查詢將請求重新導向至 CDN 節點；用戶端的 DNS 解析程式將請求轉送至 CDN 的權威名稱伺服器。基於 DNS Unicast 路由的 CDN 並非理想之選，因為用戶端可能地理上遠離 DNS 解析程式。最接近 CDN 節點的決策基於用戶端的 DNS 伺服器，而不是用戶端的 IP 位址。

   而且，如果 DNS 回應需要進行任何變更，則會依賴於 DNS 存留時間 (TTL) 到期。

   此外，由於 DNS 路由使用 Unicast 位址，流量直接路由到具體節點，導致可能產生流量暴增的問題，就像在 DDoS 攻擊中發生的那樣。

   使用基於 DNS 的 CDN 的另一個挑戰是，在容錯移轉時不會很順暢。通常，必須為 DNS 解析程式啟動一個具有不同 IP 位址的新工作階段或應用程式來進行接管。
2. **Anycast 路由**
   CloudflareCDN（我們將在下一章節中進行更詳細的討論）使用 Anycast 路由。Anycast 允許網路上的節點擁有相同的 IP 位址。從不同位置的多個節點公告相同的 IP 位址，並透過網際網路的路由通訊協定 BGP 處理用戶端重新導向。

**使用基於 Anycast 的 CDN 有幾個優勢：**

- 傳入流量被路由到最近的資料中心，其有能力高效處理請求。
- 本身提供可用性和備援。由於多個節點擁有相同的 IP 位址，如果一個節點發生故障，請求會簡單地路由到另一個最靠近的節點。
- 由於 Anycast 跨多個資料中心分配流量，它會增加整體表面積，從而防止任何一個位置被過多請求所淹沒。出於此原因，Anycast 網路在遭到 DDoS 攻擊時擁有極強的復原能力。

# Cloudflare CDN 介紹

Cloudflare 為 CDN 提供軟體即服務 (SaaS) 模式。使用 Cloudflare 的 SaaS 模式，客戶可以從 Cloudflare CDN 中受益，而無需管理或維護任何基礎結構或軟體。

Cloudflare CDN 帶來的好處可歸因於以下兩點，本章節將對此進行更詳細的討論。

1. CDN 透過在靠近使用者的伺服器上快取內容來提高效能
2. 獨特的 Cloudflare 架構和整合式生態系統

圖 2 展示了 Cloudflare CDN 的精簡檢視。用戶端從 Cloudflare 全球 Anycast 邊緣網路上最靠近用戶端所在位置的伺服器接收它們的回應，從而大大減少了延遲和 RTT。該圖呈現了一致的終端使用者體驗，無論用戶端和源站的實體位置如何。

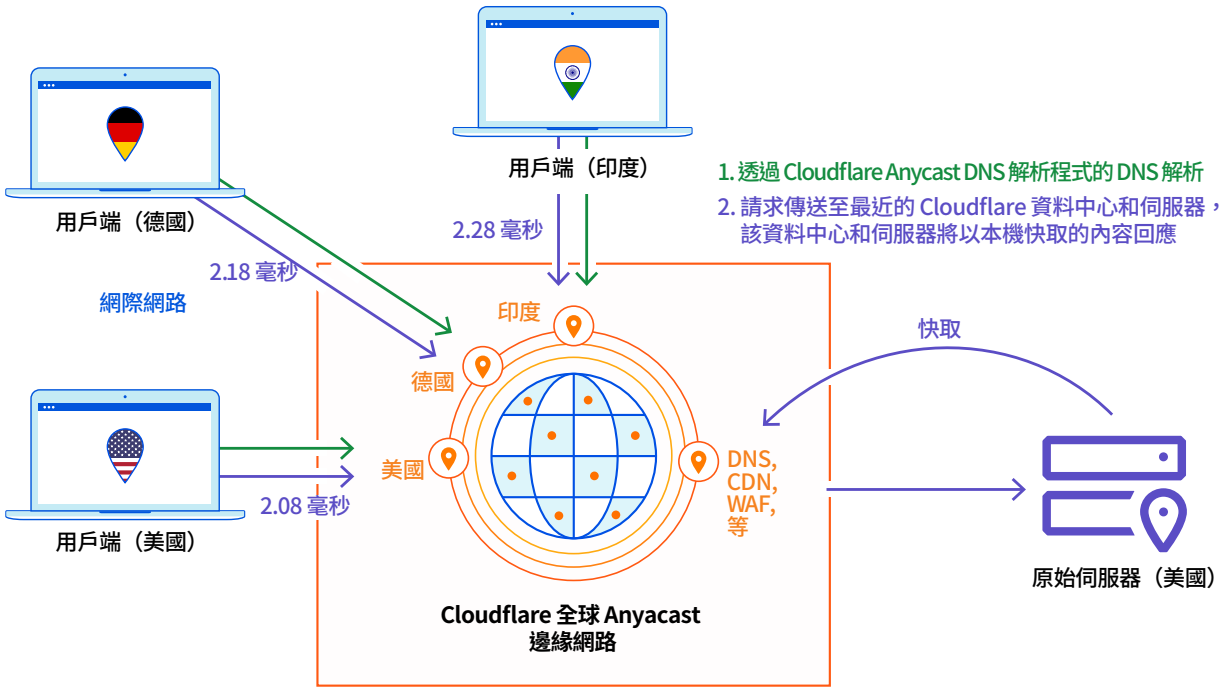



圖 2：到具有 Anycast 的 Cloudflare CDN 的 HTTP 請求

# Cloudflare CDN 架構和設計

圖 3 是全球 Anycast 邊緣網路上的 Cloudflare CDN 的檢視。除了使用 Anycast 來獲得網路效能和復原能力外，Cloudflare CDN 還利用 Argo Tiered Cache 來交付最佳化的結果，同時為客戶節省成本。客戶還可以啟用 Argo Smart Routing 以找到將請求路由到原始伺服器的最快網路路徑。這些功能將在本文件後文中進行詳細討論。

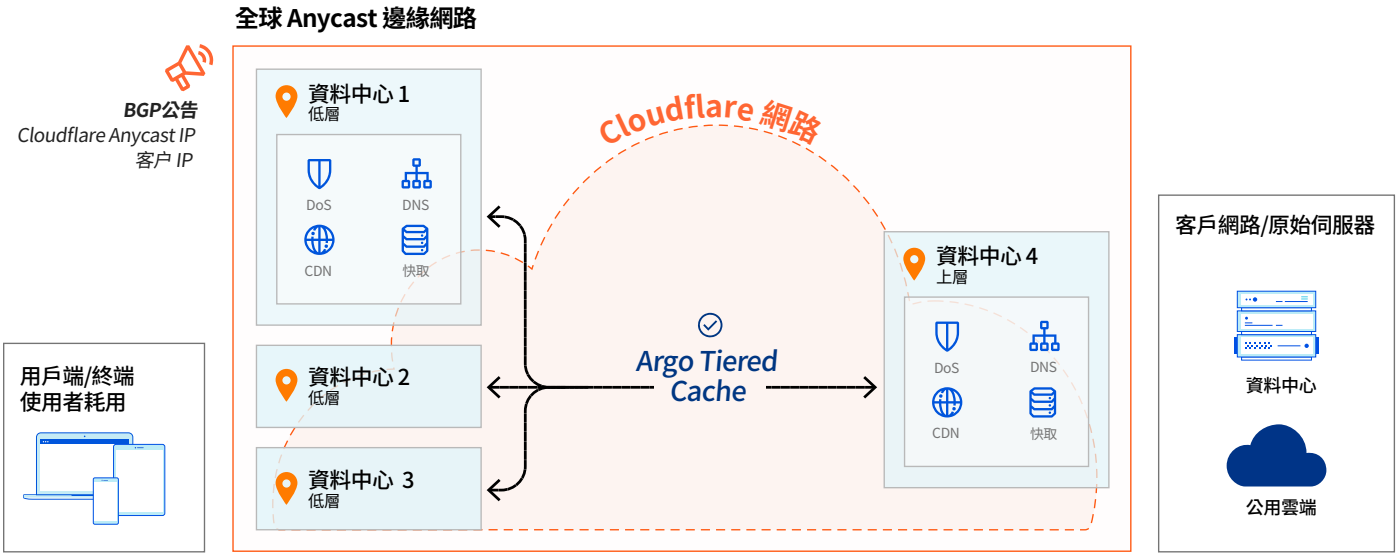



圖 3：全球 Anycast 邊緣網路上具有 Argo Tiered Cache 的 Cloudflare CDN

在上圖中，關於 Cloudflare CDN 及其所在的全球 Anycast 邊緣網路，有幾個重要的關鍵點需要瞭解：

- 一個重要的不同點是 Cloudflare 利用一個全球網路，並在每個 Cloudflare 資料中心的每台伺服器上執行每項服務，從而為終端使用者提供最接近 Cloudflare 的服務，並具有最高的規模、復原能力和效能。
- Cloudflare 是反向代理，意味著它接收來自用戶端的請求，並將請求代理回客戶的原始伺服器。

  因此，在到達客戶的網路之前，每一個請求都會通過 Cloudflare 的網路。

由於 Cloudflare 在邊緣（輸入）強化並保護其基礎結構，所有客戶也因此受到保護，免受基礎結構層級和大規模 DDoS 攻擊。請求和流量必須通過受保護的 Cloudflare 網路才能到達客戶的原始伺服器。

- Cloudflare CDN 利用 Cloudflare 全球 Anycast 邊緣網路。因此，傳入請求被路由至最靠近使用者（眼球）的節點並從該節點收到回應。
- Anycast 的固有好處是減少延遲、網路復原能力、更高的可用性，以及由於更大的表面積來吸收合法流量負載和 DDoS 攻擊而提高的安全性。

# Cloudflare CDN 架構和設計（續）

Cloudflare 的全球 Anycast 邊緣網路覆蓋 100 多個國家/地區的 250 多個城市，50 毫秒內即可聯繫全球 95% 的網際網路連線人口，同時提供 100 Tbps 的網路容量和 DDoS 防護功能。

- Cloudflare 網路內的邊緣節點從原始伺服器快取內容，且能夠透過快取的複本回應請求。Cloudflare 還使用同一邊緣架構提供 DNS、DDoS 防護 WAF 以及其他效能、復原能力和安全服務。
- Argo 在整個 Cloudflare 網路中使用最佳化的路由和快取技術，更快、更可靠、更安全地為使用者提供回應。Argo 包含 Smart Routing 和 Tiered Cache。Cloudflare 利用 Argo 提供增強的 CDN 解決方案。

## Argo Tiered Cache

當網站上線後，預設設定標準快取。使用標準快取，每個資料中心都充當原始伺服器的直接反向代理。任何資料中心中發生快取未命中都會導致請求從輸入資料中心傳送到原始伺服器。

儘管標準快取也能夠工作，但這並不是最優設計——其他 Cloudflare 資料中心中可能已經存在更靠近用戶端的快取內容，因此原始伺服器有時會不必要地過載。因此，最佳方法是啟用 Argo Tiered Cache，每一個 Cloudflare 方案中都已包含此功能。使用 Argo Tiered Cache，部分資料中心是其他資料中心到源站的反向代理，從而帶來更高的快取命中率和更快的回應時間。

Argo Tiered Cache 利用 Cloudflare 網路的規模，盡可能減少傳往客戶源站的請求。當請求進入一個 Cloudflare 資料中心時，如果請求的內容並未本地快取，則會檢查其他 Cloudflare 資料中心是否快取了該內容。

與資料中心和客戶原始伺服器之間的連線相比，Cloudflare 資料中心之間的距離更短，路徑更快，從而大大提高了快取命中率，最佳化對用戶端的回應。Cloudflare CDN 利用 Argo Smart Routing 資料來確定最佳上層資料中心，以用於 Argo Tiered Cache。還可以啟用 Argo Smart Routing 作為附加元件，以在出現快取未命中和其他類型的動態流量時，提供資料中心和原始伺服器之間的最快路徑。

Cloudflare CDN 允許客戶設定 Tiered Caching。請注意，基於 Cloudflare 方案，將為 Argo Tiered Cache 提供不同的拓撲。Tiered Caching 預設停用，可在主功能表的快取索引標籤下啟用。

## Argo Tiered Cache 拓撲

不同的快取拓撲讓客戶能夠控制 Cloudflare 與原始伺服器的交互方式，以幫助確保更高的快取命中率、更少的源站連線和更低的延遲。

| Argo Tiered Cache 拓撲 | | |
|---|---|---|
| **智慧型 Tiered Cache 拓撲**<br>（所有方案） | **通用全球分層拓撲**<br>（僅 Enterprise 方案） | **自訂 Tiered Cache 拓撲**<br>（僅 Enterprise 方案） |
| • 推薦用於大多數部署。這是啟用 Tiered Cache 時的預設設定。<br>• 非常適合想要利用 CDN 提高效能同時盡可能減少對原始伺服器的請求以及 Cloudflare 和原始伺服器之間頻寬使用率的客戶。<br>• Cloudflare 將使用 Argo 效能和路由資料動態地為源站找到單個最佳上層。 | • 推薦給在全球擁有較高流量且想要盡可能獲得最高快取使用和最佳效能的客戶。<br>• 通用全球分層拓撲會平衡快取效率與延遲。命令 Cloudflare 使用所有第 1 層資料中心作為上層。 | • 推薦給擁有更多使用者群體資料並擁有想要著重關注的特定地理區域的客戶。<br>• 自訂 Tiered Cache 拓撲讓客戶能夠設定符合其具體需求的自訂拓撲（範例：特定地理位置的上層服務更多客戶）。<br>• 與 Customer Success 經理 (CSM) 交流以建置自訂拓撲。 |

## 流量流程：Argo Tiered Cache、智慧型 Tiered Cache 拓撲

在圖 4 中，啟用了具 Smart Tiered Cache 拓撲的 Argo Tiered Caching。該圖呈現了兩個不同的流量流程，總結如下。第一個流量流程（綠色的用戶端 1）是來自一個用戶端的請求，進入資料中心 1。第二個流量流程（紫色的用戶端 2）是對同一資源的後續請求，進入另一個資料中心——資料中心 2。

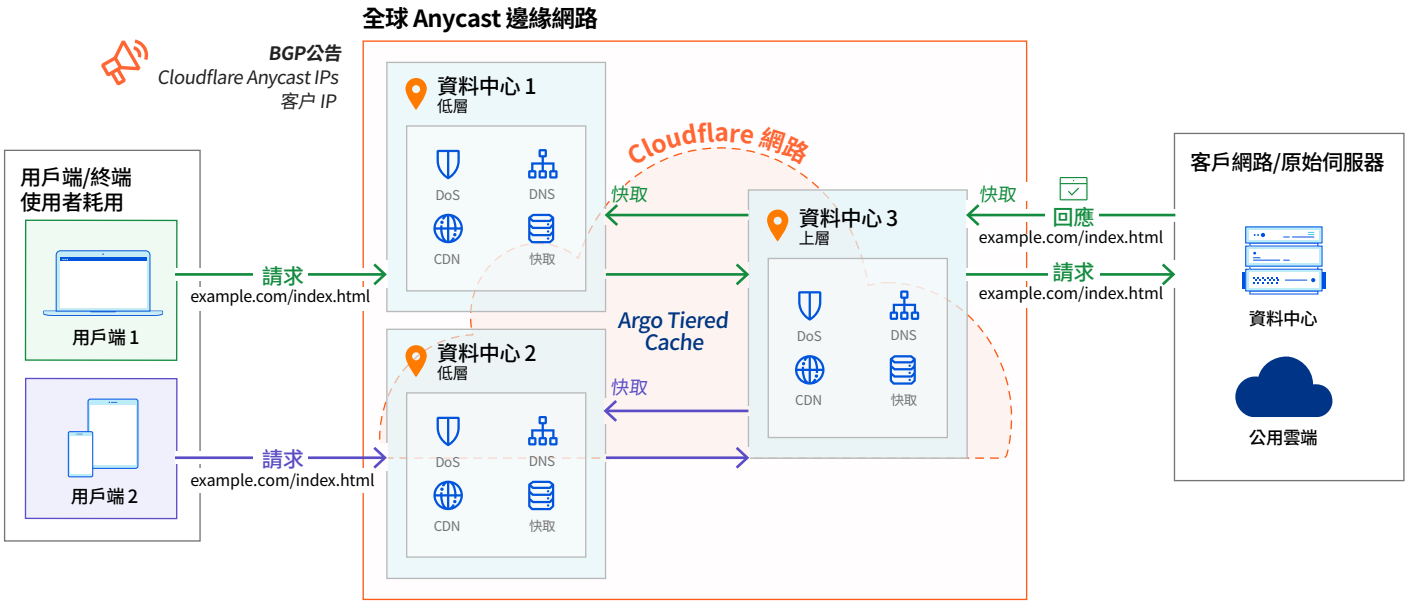



圖 4：通過 Cloudflare CDN 的 HTTP 請求和流量流程

### 用戶端 1

- 資料中心 1 中收到第一個請求，產生快取未命中，因為之前沒有任何用戶端發起過該請求。
- 沒有找到快取的內容，因此資料中心 1 檢查上層資料中心，以請求該內容的複本。
- 上層資料中心也沒有本機快取該內容，因此它向原始伺服器請求該內容。在收到內容後，上層資料中心本機快取該內容並將其轉送到請求內容的低層資料中心。低層資料中心快取該內容並回應用戶端。

### 用戶端 2

- 資料中心 2 中收到另一個用戶端發出的第二個請求，產生了快取未命中，因為資料中心 2 服務的所有用戶端都沒有發起過該請求。
- 沒有找到快取的內容，因此資料中心 2 檢查上層資料中心，以請求該內容的複本。
- 在上層資料中心中找到了快取的內容。資料中心 2 擷取並本機快取該內容，然後回應用戶端。

## 流量流程：Argo Tiered Cache、智慧型 Tiered Cache 拓撲（續）

在圖 4 中，用戶端 1 流量流程顯示了最靠近用戶端的資料中心（資料中心 1）接收用戶端請求時的流量流程。由於輸入資料中心上沒有本機快取內容且 Tiered Caching 已啟用，因此向上層資料中心傳送了請求，以請求要快取的內容的複本。

因為上層資料中心也沒有快取該內容，因此它向原始伺服器傳送請求，並在收到回應時快取收到的內容，然後使用快取的內容回應低層資料中心。低層資料中心快取該內容並回應用戶端。

請注意，當向另一資料中心（資料中心 2）發起針對相同內容的新請求時（用戶端 2 流量流程），該內容未本機快取；但是，從上層資料中心中擷取了該內容，因為在第一次請求該內容時已經快取。

由於上層資料中心為第二個請求返回了快取的內容，防止了前往原始伺服器的過程，從而提高了快取命中率、加速了回應時間、節省了 Cloudflare 網路和原始伺服器之間的頻寬成本，以及減少了原始伺服器回應請求的負載。

# Argo Smart Routing

Argo Smart Routing 是一項服務，可在整個 Cloudflare 網路中找到最佳化路線，以更快地向使用者提供回應。如之前所討論的，Cloudflare CDN 利用 Argo Smart Routing 來為 Argo Tiered Cache 確定最佳上層資料中心。

此外，可以啟用 Argo Smart Routing 以確保始終在上層資料中心和原始伺服器之間採用 Cloudflare 網路上的最快路徑。在沒有 Argo Smart Routing 的情況下，上層資料中心與原始伺服器之間的通訊仍然會智慧路由，以繞過網際網路上的問題，確保源站可存取性。

Argo Smart Routing 透過考慮來自每秒路由超過 2800 萬個 HTTP 請求的即時資料和網路智慧來加速流量；它確保通過 Cloudflare 網路上最快和最可靠的網路路徑到達原始伺服器。平均而言，Argo Smart Routing 將 Web 資產上的效能提高了 30%。

## 流量流程：Argo Tiered Cache、智慧型 Tiered Cache 拓撲與 Argo Smart Routing

圖 5 詳細描述了當未啟用 Argo Tiered Cache 和 Argo Smart Routing 時的流量流程。請求進入最近的資料中心，由於內容未本機快取且 Argo Tiered Cache 未啟用，請求直接被傳送原始伺服器以獲取內容。而且，由於 Argo Smart Routing 未啟用，在與原始伺服器通訊時採用了一條可靠但不一定最快的路徑。

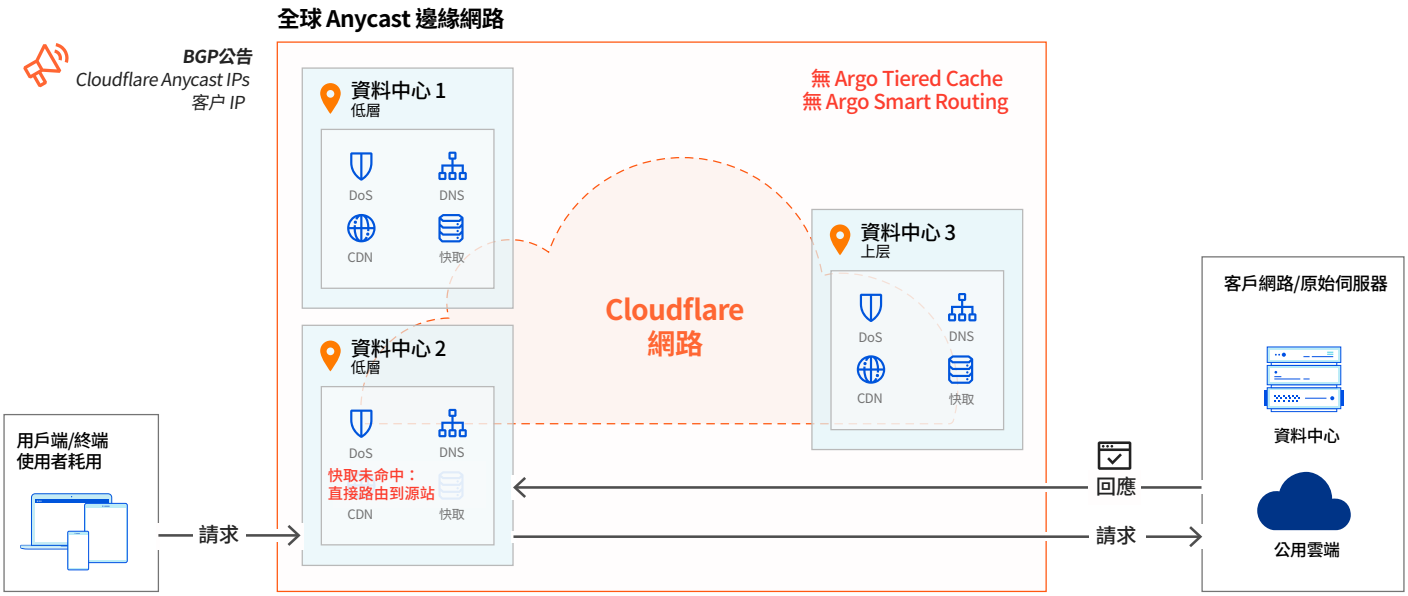



圖 5：沒有 Argo Tiered Cache 和 Argo Smart Routing 的 Cloudflare CDN

## 流量流程：Argo Tiered Cache、智慧型 Tiered Cache 拓撲與 Argo Smart Routing（續）

圖 6 清楚呈現了同時啟用 Argo Tiered Cache 和 Argo Smart Routing 時的流量流程。

在圖 6 中，當資料中心 1 收到請求且發生快取未命中時，檢查了上層資料中心（資料中心 3）的快取。如果在上層資料中心中未找到快取的內容，且 Argo Smart Routing 已啟用，則會採用最快的路徑將請求從上層資料中心傳送到源站。

最快路徑由 Argo 網路智慧功能確定，該功能會考慮擁塞、延遲和 RTT 等即時網路資料。

**使用 Cloudflare CDN，Argo Smart Routing 將在以下情況下使用：**

1. 發生快取未命中且需要將請求傳送至原始伺服器以擷取內容的情況；
2. 有對動態內容（範例：API）等不可快取內容的請求且該請求必須傳送到原始伺服器的情況。

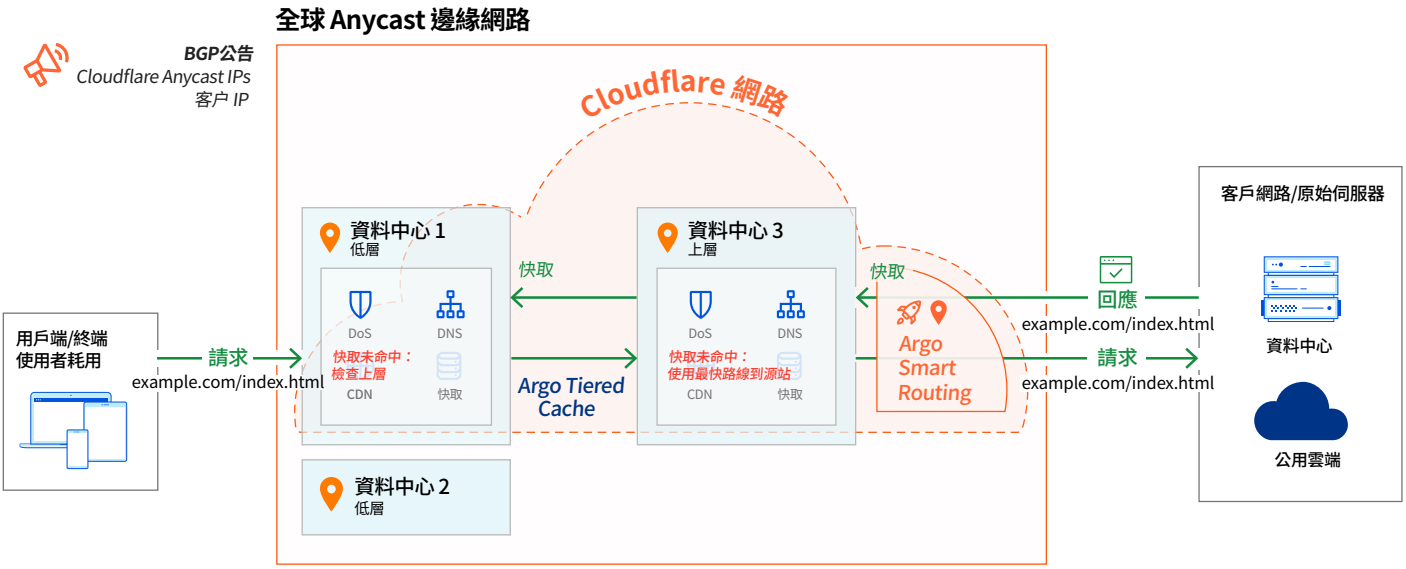



圖 6：啟用 Argo Tiered Cache 和 Argo Smart Routing 的 Cloudflare CDN

# 概述

總而言之，Cloudflare CDN 是一種 SaaS，可幫助解決客戶在延遲、效能、可用性、備援、安全性和成本方面面臨的挑戰。Cloudflare CDN 利用 Cloudflare 的全球 Anycast 邊緣網路和 Argo Tiered Cache 來提供最佳化的結果，同時為客戶節省成本。客戶還可以啟用 Argo Smart Routing 以確保使用最快網路路徑將請求路由到原始伺服器。