開發人員指南

AWS Global Accelerator

AWS Global Accelerator: 開發人員指南

Table of Contents

什麼是 AWS Global Accelerator？

AWS Global Accelerator 是您在其中建立加速器，改善應用程式的效能，提升本機和全球使用者的使用體驗。根據您選擇的加速器類型，您可以獲得額外的好處。

- 藉由使用標準加速器，您可改善網際網路應用程式的可用性，供全球觀眾使用。使用標準加速器，全球加速器會透過 AWS 全球網路將流量導向最接近用戶端區域的終端節點。
- 透過使用自訂路由加速器，您可以將一個或多個使用者對應至多個目的地之間的特定目的地。

全球加速器是一項全球服務，支援多個 AWS 區域的終端節點，列於AWS 區域表格。

根據預設，全域加速器會提供您與加速器相關聯的兩個靜態 IP 位址。使用標準加速器，而不是使用全域加速器所提供的 IP 位址，您可以將這些進入點設定為來自您自己的 IP 位址範圍的 IPv4 位址，這些進入點可供全域加速器使用。靜態 IP 位址是從 AWS 邊緣網路進行任何廣播。

> **Important**
>
> 只要它存在，靜態 IP 位址就會保持指派給加速器，即使您停用加速器且不再接受或路由流量。但是，當您delete加速器時，您會遺失指派給它的靜態 IP 位址，因此您無法再使用它們來路由流量。您可以使用 IAM 政策 (例如標籤型權限) 搭配全域加速器來限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

對於標準加速器，全球加速器使用 AWS 全球網路，根據您設定的運作狀況、用戶端位置和政策，將流量路由到最佳區域端點，進而增加應用程式的可用性。標準加速器的終端節點可以是位於一個 AWS 區域或多個區域的網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。此服務會立即回應健全狀況或設定的變更，以確保來自用戶端的網際網路流量永遠會導向正常的端點。

自訂路由加速器僅支援虛擬私有雲 (VPC) 子網路端點類型，並將流量路由至該子網路中的私有 IP 地址。

如需目前支援全球加速器和其他服務的 AWS 區域清單，請參閱AWS 區域表格。

主題

- AWS Global Accelerator 元件
- AWS Global Accelerator 如何運作

- 加速器類型
- Global Accelerator 節點伺服器的位置和 IP 地址範圍
- AWS Global Accelerator 使用案例
- AWS Global Accelerator 速度比較工具
- 如何開始使用 AWS Global Accelerator
- AWS Global Accelerator 中的標籤
- AWS Global Accelerator 的定價

AWS Global Accelerator 元件

AWS Global Accelerator 包含下列元件：

靜態 IP 地址

全域加速器為您提供一組兩個靜態 IP 位址，這些位址是從 AWS 邊緣網路進行任何廣播。如果您將自己的 IP 地址範圍帶入 AWS (BYOIP)，供 Global Accelerator 使用，則可從自己的集區指派 IP 地址，供加速器使用。如需詳細資訊，請參閱 在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)。

IP 位址做為用戶端的單一固定入口點。如果您已經為應用程式設定了 Elastic Load Balancing 器、Amazon EC2 執行個體或彈性 IP 位址資源，您可以輕鬆將這些資源新增到全球加速器中的標準加速器。這可讓全域加速器使用靜態 IP 位址來存取資源。

只要它存在，靜態 IP 位址就會保持指派給加速器，即使您停用加速器且不再接受或路由流量。但是，當您delete加速器時，您會遺失指派給它的靜態 IP 位址，因此您無法再使用它們來路由流量。您可以使用 IAM 政策 (例如標籤型權限) 搭配全域加速器來限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

加速器

加速器會透過 AWS 全球網路將流量導向終端節點，以改善網際網路應用程式的效能。每個加速器都包含一或多個接聽程式。

加速器有兩種類型：

- A標準加速器會根據數個因素，將流量導向最佳 AWS 終端節點，包括使用者的位置、終端節點的健全狀況以及您設定的終端節點權重。如此可改善應用程式的可用性和效能。端點可以是網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。

- A自訂路由加速器可讓您確定地將多個使用者路由到加速器後面的特定 EC2 目的地，如某些使用案例所需。您可以將使用者導向至加速器上唯一的 IP 位址和連接埠 (全域加速器已對應至目的地) 來達成此目的地。

如需詳細資訊，請參閱 加速器類型。

DNS 名稱

全域加速器會為每個加速器指派預設的網域名稱系統 (DNS) 名稱，類似於a1234567890abcdef.awsglobalaccelerator.com，指向全域加速器指派給您的靜態 IP 位址，或您從自己的 IP 位址範圍中選擇的靜態 IP 位址。視使用案例而定，您可以使用加速器的靜態 IP 位址或 DNS 名稱，將流量路由至加速器，或設定 DNS 記錄，以使用您自己的自訂網域名稱來路由流量。

網路區域

網路區域服務來自唯一 IP 子網路的加速器的靜態 IP 位址。與 AWS 可用區域類似，網路區域是具有自己一組實體基礎設施的隔離單元。當您設定加速器時，依預設，全域加速器會為其配置兩個 IPv4 位址。如果由於某些用戶端網路的 IP 位址封鎖或網路中斷而導致網路區域中的某個 IP 位址無法使用，則用戶端應用程式可以從其他隔離網路區域重試健全的靜態 IP 位址。

接聽程式

監聽器會根據您設定的連接埠 (或連接埠範圍) 和通訊協定 (或通訊協定)，處理從屬端到「全域加速器」的輸入連線。您可以為 TCP、UDP 或 TCP 和 UDP 通訊協定設定接聽程式。每個接聽程式都有一或多個與其相關聯的端點群組，而流量會轉送到其中一個群組中的端點。您可以透過指定要分配流量的區域，將端點群組與接聽程式建立關聯。使用標準加速器，流量會分散到與接聽程式相關聯的端點群組內的最佳端點。

端點群組

每個端點群組都與特定 AWS 區域相關聯。端點群組包含區域中的一或多個端點。使用標準加速器，您可以增加或減少將導向至端點群組的流量百分比，方法是調整流量撥打。流量撥號可讓您輕鬆進行效能測試或藍色/綠色部署測試，例如，針對不同 AWS 區域的新版本。

端點

端點是「全域加速器」將流量導向的資源。

標準加速器的端點可以是網路負載平衡器、應用程式負載平衡器、EC2 執行個體或彈性 IP 位址。Application Load Balancer 端點可以是網際網路面向或內部。標準加速器的流量會根據端點的健全狀況以及您選擇的組態選項 (例如端點加權) 路由至端點。您可以針對每個端點設定權重，這些

權重是可用來指定路由傳送至每個端點的流量比例的數字。例如，這可能是有用的，在一個區域內進行性能測試。

自訂路由加速器的終端節點是虛擬私有雲 (VPC) 子網路，其中包含一個或多個 Amazon EC2 執行個體作為流量目的地。

AWS Global Accelerator 如何運作

AWS Global Accelerator 提供的靜態 IP 地址作為用戶端的單一固定入口點。當您使用全域加速器設定加速器時，會將靜態 IP 位址與一或多個 AWS 區域中的區域終端節點建立關聯。對於標準加速器，端點為網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。對於自訂路由加速器，端點是具有一或多個 EC2 執行個體的虛擬私有雲 (VPC) 子網路。靜態 IP 位址接受從最接近使用者的節點位置傳入 AWS 全球網路的傳入流量。

> **Note**
>
> 如果您將自己的 IP 地址範圍帶入 AWS (BYOIP)，供 Global Accelerator 使用，則可從自己的集區指派靜態 IP 地址，供加速器使用。如需詳細資訊，請參閱 在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)。

從節點位置，會根據您設定的加速器類型路由應用程式的流量。

- 對於標準加速器，流量會根據數個因素路由到最佳 AWS 終端節點，包括使用者的位置、終端節點的健全狀況以及您設定的終端節點權重。
- 對於自訂路由加速器，每個用戶端都會根據您提供的外部靜態 IP 位址和接聽程式連接埠，路由到 VPC 子網路中的特定 Amazon EC2 執行個體和連接埠。

流量會透過受到良好監控、無擁塞、冗餘的 AWS 全球網路傳輸到終端節點。全球加速器可將流量在 AWS 網路上的時間最大化，確保流量始終透過最佳網路路徑進行路由。

對於某些端點類型 (位於某些 AWS 區域)，您可以選擇保留和存取用戶端 IP 位址。兩種類型的端點可以將用戶端的來源 IP 位址保留在傳入封包中：應用程式負載平衡器和 Amazon EC2 執行個體。全域加速器不支援 Network Load Balancer 和彈性 IP 位址端點的用戶端 IP 位址保留。自訂路由加速器上的端點一律會保留用戶端 IP 位址。

全域加速器會終止來自 AWS 節點用戶端的 TCP 連線，並且幾乎同時建立與您的終端節點的新 TCP 連線。這可讓用戶端更快的回應時間 (更低的延遲) 並提高輸送量。

在標準加速器中，全域加速器會持續監控所有端點的健全狀況，並在判斷主動端點狀況不良時，立即開始將流量導向另一個可用端點。這可讓您為 AWS 上的應用程式建立高可用性架構。Health 檢查不會與自訂路由加速器搭配使用，而且也沒有容錯移轉，因為您指定路由流量的目的地。

當您新增加速器時，您已設定的安全群組和 AWS WAF 規則會繼續運作，如同新增加速器之前一樣。

如果您想要對全域流量進行細微控制，可以在標準加速器中為端點設定權重。您也可以增加 (調升) 或減少 (調降) 至特定端點群組的流量百分比，例如，供效能測試或堆疊升級使用。

當您使用 Global Accelerator 時，請注意下列事項：

- AWS Direct Connect 不會透過公用虛擬介面公告 AWS Global Accelerator 的 IP 位址首碼。我們建議您不要透過 AWS Direct Connect 公用虛擬介面宣傳用來與全球加速器通訊的 IP 位址。如果您透過 AWS Direct Connect 公用虛擬介面宣傳用來與全球加速器通訊的 IP 位址，則會產生不對稱的流量流量：您對全球加速器的流量會透過網際網路進入全球加速器，但會傳回現場部署的流量網路會透過您的 AWS Direct Connect 公用虛擬界面進行。
- 全域加速器不支援將屬於另一個 AWS 帳戶的資源新增為終端節點。

主題

AWS Global Accelerator 中的閒置逾時

AWS Global Accelerator 會設定適用於其連線的閒置逾時期間。若閒置逾時的時間過後都沒有傳送或接收的資料，則 Global Accelerator 會關閉連線。若要確保連線保持活動狀態，用戶端或端點必須在閒置逾時期間過後至少傳送 1 個位元組的資料。

網路連線的「全域加速器」閒置逾時取決於連線類型：

- TCP 連線的逾時時間為 340 秒。
- UDP 連線的逾時時間為 30 秒。

全域加速器會繼續將流量導向端點，直到達到閒置逾時為止，即使端點標示為狀況不良。全域加速器只有在新連線啟動或閒置逾時之後，才會視需要選取新的端點。

AWS Global Accelerator 中的靜態 IP 地址

您可以使用全球加速器指派給加速器的靜態 IP 位址 (或從自己的 IP 位址集區指定的標準加速器)，將網際網路流量路由到靠近使用者所在位置的 AWS 全球網路 (不論使用者所在位置為何)。對於標準加速器，您可以將地址與在單一 AWS 區域或多個區域中執行的網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址相關聯。對於自訂路由加速器，您可以將流量導向至一或多個區域中 VPC 子網路中的 EC2 目的地。透過 AWS 全球網路路由流量可改善可用性和效能，因為流量不需要透過公用網際網路進行多個躍點。使用靜態 IP 位址也可讓您將傳入的應用程式流量分配到多個 AWS 區域的多個端點資源。

此外，使用靜態 IP 位址可讓您更輕鬆地將應用程式新增至更多區域或移轉區域之間的應用程式。使用固定 IP 位址表示當您進行變更時，使用者會以一致的方式連線到您的應用程式。

如果您願意，您可以將自己的自訂網域名稱與加速器的靜態 IP 位址產生關聯。如需詳細資訊，請參閱將自訂網域流量路由至您的加速器。

除非您將自己的 IP 位址範圍帶到 AWS，然後從該集區指定靜態 IP 位址，否則全球加速器會為您提供來自 Amazon IP 位址集區的靜態 IP 位址。(如需詳細資訊，請參閱「在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)」)。若要在主控台上建立加速器，第一個步驟是提示全域加速器為您的加速器輸入名稱或選擇您自己的靜態 IP 位址來佈建靜態 IP 位址。若要查看建立加速器的步驟，請參閱AWS Global Accelerator。

只要它存在，靜態 IP 位址就會保持指派給加速器，即使您停用加速器且不再接受或路由流量。但是，當您delete加速器時，您會遺失指派給它的靜態 IP 位址，因此您無法再使用它們來路由流量。您可以使用 IAM 政策 (例如標籤型權限) 搭配全域加速器來限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

使用流量撥號和端點權數的流量管理

有兩種方式可以自訂 AWS Global Accelerator 使用標準加速器將流量傳送到終端節點的方式：

- 變更流量撥號以限制一或多個端點群組的流量
- 指定權數，以變更群組中端點的流量比例

流量撥號的運作方式

對於標準加速器中的每個端點群組，您可以設定流量撥號，以控制傳送至端點群組的流量百分比。此百分比只會套用至已導向至端點群組的流量，而非所有接聽程式流量。

流量撥號會限制端點群組接受的流量部分，以導向至該端點群組的流量百分比表示。例如，如果您在us-east-1設定為 50 (也就是 50%)，且加速器會將 100 個使用者要求導向該端點群組，則群組只會接受 50 個要求。加速器會將剩餘的 50 個要求導向其他區域中的端點群組。

如需詳細資訊，請參閱 使用流量撥號調整流量。

權重的運作方式

對於標準加速器中的每個端點，您可以指定加速器路由至每個端點之流量比例的數字。例如，這可能是有用的，在一個區域內進行性能測試。

權數是決定加速器導向至端點之流量比例的值。根據預設，端點的權重是 128，也就是權重最大值 255 的一半。

加速器會計算端點群組中端點的權重總和，然後根據每個端點的權重與總計的比率，將流量導向端點。如需加權的運作方式範例，請參閱 端點權重。

流量撥號和權重會影響標準加速器以不同方式服務流量的方式：

- 您可以設定流量撥號端點群組。流量撥號可讓您根據其他因素 (例如鄰近程度)，「撥號」加速器已指向該群組的流量 (或所有流量) 中斷某個百分比的流量 (或所有流量)。
- 另一方面，您可以使用權重來設置個別端點位於端點群組。權重提供分割端點群組內流量的方法。例如，您可以使用權重對區域中的特定端點執行效能測試。

> **Note**
>
> 如需流量撥打和加權如何影響容錯移轉的詳細資訊，請參閱狀況不良端點的容錯移轉。

AWS Global Accelerator 運作 Health 檢查

對於標準加速器，AWS Global Accelerator 會自動檢查與靜態 IP 位址相關聯的終端節點的運作狀況，然後僅將使用者流量導向正常的終端節點。

全域加速器包含自動執行的預設健全狀況檢查，但您可以設定檢查和其他選項的時間。如果您已設定自訂健全狀況檢查設定，則全域加速器會根據您的組態，以特定方式使用這些設定。您可以在 Amazon EC2 執行個體的全域加速器或彈性 IP 位址端點中設定這些設定，或是在網路負載平衡器或應用程式負載平衡器的 Elastic Load Balancing 主控台上設定這些設定。如需詳細資訊，請參閱 運作狀態檢查選項。

將端點新增至標準加速器時，必須先通過健全狀況檢查，才能將流量導向至該加速器。如果全域加速器沒有任何正常的端點，可將流量路由傳送至標準加速器中，則會將要求路由傳送至所有端點。

加速器類型

AWS 全域加速器可以使用兩種類型的加速器：標準加速器和自訂路由加速器。這兩種類型的加速器會透過 AWS 全球網路路由流量，以改善效能和穩定性，但每種加速器都是針對不同的應用程式需求而設計。

標準加速器

透過使用標準加速器，您可以改善在應用程式負載平衡器、網路負載平衡器或 Amazon EC2 執行個體上執行的應用程式的可用性和效能。透過標準加速器，全域加速器會根據地理位置接近和端點健全狀況，跨區域端點路由用戶端流量。它也允許客戶根據流量撥號和端點權數等控制項，在端點間轉移用戶端流量。這適用於各種使用案例，包括藍色/綠色部署、A/B 測試和多區域部署。若要查看更多使用案例，請參閱 AWS Global Accelerator 使用案例。

如需進一步了解，請參閱使用 AWS Global Accelerator 中的標準加速器。

自訂路由加速

自訂路由加速器適用於您想要使用自訂應用程式邏輯，將一或多位使用者導向特定目的地和連接埠，同時仍可取得全域加速器的效能優勢的案例。其中一個範例是指派多個來電者給特定媒體伺服器的 VoIP 應用程式，以啟動語音、視訊和訊息工作階段。另一個範例是線上即時遊戲應用程式，您可以根據地理位置、玩家技能和遊戲模式等因素，將多位玩家指派至遊戲伺服器上的單一工作階段。

如需進一步了解，請參閱使用 AWS Global Accelerator 中的自訂路由加速器。

根據您的特定需求，您可以建立其中一種加速器來加速客戶流量。

Global Accelerator 節點伺服器的位置和 IP 地址範圍

如需 Global Accelerator 節點伺服器位置清單，請參閱AWS Global Accelerator 今天在哪裡部署？一節AWS Global Accelerator 常見(憑證已建立！) 頁面上的名稱有些許差異。

AWS 會以 JSON 格式發佈目前的 IP 地址範圍。若要檢視目前範圍，請下載ip-範圍.json。如需詳細資訊，請參閱「」AWS IP 地址範圍中的Amazon Web Services 一般參考。

若要尋找與 AWS Global Accelerator 邊緣伺服器關聯的 IP 地址範圍，請在ip-ranges.json用於下列字串：

```
"service": "GLOBALACCELERATOR"
```

全域加速器項目，包含"region": "GLOBAL"是指配置給加速器的靜態 IP 位址。如果您想要透過來自某個區域的目前狀態點 (POP) 的加速器來篩選流量，請篩選包含特定地理區域的項目，例如us-*或eu-*。因此，例如，如果您過濾us-*，您只會看到通過美國 (美國) 持久性有機污染物的流量。

AWS Global Accelerator 使用案例

使用 AWS Global Accelerator 可協助您達成各種目標。本節列出了其中的一些，讓您了解如何使用全域加速器來滿足您的需求。

擴充以提高應用程式使用率

當應用程式使用量增加時，您需要管理的 IP 位址和端點數目也會增加。全域加速器可讓您擴充或縮小網路。它可讓您將區域資源 (例如負載平衡器和 Amazon EC2 執行個體) 關聯到兩個靜態 IP 地址。您只需在用戶端應用程式、防火牆和 DNS 記錄中包含一次允許清單中的這些位址。使用全域加速器，您可以在 AWS 區域中新增或移除終端節點、執行藍色/綠色部署以及進行 A/B 測試，而無需更新用戶端應用程式中的 IP 位址。這對於您無法經常更新用戶端應用程式的 IoT、零售、媒體、汽車和醫療保健使用案例特別有用。

延遲敏感應用程式的加速

許多應用程式 (尤其是在遊戲、媒體、行動應用程式和財務等領域) 都需要非常低的延遲才能獲得絕佳的使用者體驗。為了改善使用者體驗，全域加速器會將使用者流量導向最接近用戶端的應用程式端點，以減少網際網路延遲和抖動。全球加速器使用 Anycast 將流量路由到最近的節點，然後透過 AWS 全球網路將流量路由到最近的區域終端節點。全域加速器會快速回應網路效能的變更，以改善使用者的應用程式效能。

災難復原與多區域復原

您必須能夠依賴網路才能使用。您可能會跨多個 AWS 區域執行應用程式，以支援災難復原、更高的可用性、更低的延遲或合規。如果全域加速器偵測到您的應用程式終端節點在主要 AWS 區域發生故障，它會立即觸發流量重新路由到下一個可用、最接近的 AWS 區域中的應用程式終端節點。

保護您的應用程式

將您的 AWS 來源 (例如應用程式負載平衡器或 Amazon EC2 執行個體) 暴露給公用網際網路流量，為惡意攻擊提供機會。全域加速器會將您的來源遮罩在兩個靜態進入點後面，藉此降低攻擊的風

險。預設情況下，這些入口點會受到保護，避免使用 AWS Shield 的分散式阻斷服務 (DDoS) 攻擊。全球加速器使用私有 IP 地址與 Amazon Virtual Private Cloud 建立對等連線，從而在公有網際網路上保持與內部應用程式負載平衡器或私有 EC2 執行個體的連線。

改善 VoIP 或線上遊戲應用程式的效能

使用自訂路由加速器，您可以為 VoIP 或遊戲應用程式運用全域加速器的效能優勢。例如，您可以針對將多個玩家指派給單一遊戲工作階段的線上遊戲應用程式使用全域加速器。針對需要自訂邏輯將使用者對應至特定端點 (例如多人遊戲或 VoIP 通話) 的應用程式，使用全域加速器來減少全域延遲和抖動。您可以使用單一加速器將用戶端連接到在單一或多個 AWS 區域中執行的數千個 Amazon EC2 執行個體，同時完全控制哪個用戶端會導向哪個 EC2 執行個體和連接埠。

AWS Global Accelerator 速度比較工具

您可以使用 AWS Global Accelerator 速度比較工具查看全球加速器下載速度與 AWS 區域的直接網際網路下載速度相比。此工具可讓您使用瀏覽器查看使用全域加速器傳輸資料時的效能差異。您可以選擇要下載的檔案大小，工具會透過 HTTPS/TCP 從不同區域的應用程式負載平衡器下載檔案至您的瀏覽器。對於每個地區，您會看到下載速度的直接比較。

若要存取速度比較工具，請將下列 URL 複製到您的瀏覽器：

```
https://speedtest.globalaccelerator.aws
```

> **Important**
>
> 當您多次執行測試時，結果可能會有所不同。下載時間會根據全球加速器外部因素而有所不同，例如您使用的最後一哩網路中連線的品質、容量和距離。

如何開始使用 AWS Global Accelerator

您可以使用 API 或使用 AWS Global Accelerator 主控台開始設定 AWS Global Accelerator。由於全球加速器是全球服務，因此不會與特定 AWS 區域繫結。請注意，全球加速器是支援多個 AWS 區域的終端節點的全球服務，但您必須指定美國西部 (奧勒岡) 區域才能建立或更新加速器。

若要開始使用全域加速器，請遵循下列一般步驟：

1. 選擇您要建立的加速器類型：標準加速器或自訂路由加速器。

2. 設定「全域加速器」的初始設定： 提供加速器的名稱。然後，根據您指定的通訊協定和連接埠 (或連接埠範圍)，設定一或多個監聽器來處理從屬端的輸入連線。
3. 為加速器設定區域端點群組： 您可以選取一或多個區域端點群組，新增至接聽程式。接聽程式會將要求路由傳送至您新增至端點群組的端點。

   對於標準加速器，全域加速器會使用針對每個端點定義的健全狀況檢查設定，來監控群組內端點的健全狀況。對於標準加速器中的每個端點群組，您可以設定流量撥打百分比來控制端點群組將接受的流量百分比。此百分比只會套用至已導向至端點群組的流量，而非所有接聽程式流量。根據預設，所有地區端點群組的流量撥號設定為 100%。

   對於自訂路由加速器，流量會根據接收流量的接聽程式連接埠，決定性地路由至 VPC 子網路中的特定目的地。
4. 將端點新增至端點群組： 您新增的端點取決於加速器類型。
   - 對於標準加速器，您可以將一或多個區域資源 (例如負載平衡器或 EC2 執行個體端點) 新增至每個端點群組。接下來，您可以透過設定端點權數來決定要路由到每個端點的流量。
   - 對於自訂路由加速器，您可以新增一或多個具有多達數千個 Amazon EC2 執行個體目的地的虛擬私有雲 (VPC) 子網路。

如需如何使用 AWS Global Accelerator 加速器主控台建立標準加速器或自訂路由加速器的詳細步驟，請參閱AWS Global Accelerator。若要使用 API 作業，請參閱可搭配 AWS Global Accelerator 使用的常見動作與AWS Global Accelerator API 參考。

AWS Global Accelerator 中的標籤

標籤是您用於識別和組織 AWS 資源的文字或短句 (中繼資料)。可以新增多個標籤到每個資源，且每個標籤皆包含您所定義的金鑰和值。例如，金鑰可能是`environment`，並且值可能是`production`。可以根據新增的標籤來搜尋與篩選資源。在 AWS Global Accelerator 中，您可以為加速器加上標籤。

下列兩個範例指出在 Global Accelerator 中使用標籤會是非常實用的做法。

- 使用標籤來追蹤不同類別中的帳單資訊。若要這樣做，請將標籤套用至加速器或其他 AWS 資源 (例如網路負載平衡器、應用程式負載平衡器或 Amazon EC2 執行個體)，然後啟用標籤。AWS 會以逗號分隔值 (CSV 檔案) 格式產生一份成本分配報告，其中包含按啟用的標籤匯總的用量與成本。您可以套用代表業務類別 (例如成本中心、應用程式名稱或擁有者) 的標籤，來整理多個服務中的成本。如需詳細資訊，請參閱 AWS Billing 與成本管理中的使用成本分配標記。
- 使用標籤強制使用以標籤為基礎的加速器。若要執行此動作，請建立 IAM 政策，以指定標籤和標籤值以允許或不允許動作。如需詳細資訊，請參閱 標籤型政策。

如需使用慣例和其他標記相關資源的連結，請參閱AWS 資源標記中的AWS 一般參考資料。如需使用標籤的秘訣，請參閱標記最佳實務：AWS 資源標籤策略中的AWS 白皮書部落格。

如需在 Global Accelerator 新增至資源的標籤數量上限的詳細資訊，請參閱。AWS Global Accelerator 的配額。

您可以使用 AWS 主控台、AWS CLI 或 Global Accelerator API 新增和更新標籤。本章包含在主控台中使用標記的步驟。如需使用 AWS CLI 和全域加速器 API (包括 CLI 範例) 使用標籤的詳細資訊，請參閱AWS Global Accelerator API 參考：

- 建立加速器
- TagResource
- UntagResource
- ListTagsForResource

全域加速器中的標記支援

AWS Global Accelerator 支援加速器的標記。

Global Accelerator 支援 AWS Identity and Access Management (IAM) 的標籤型存取控制功能。如需詳細資訊，請參閱 標籤型政策。

新增、編輯和刪除在 Global Accelerator 中的標籤

下列程序說明如何新增、編輯和刪除在 Global Accelerator 主控台適用於加速器的標籤。

> **Note**
>
> 您可以使用主控台、AWS CLI 或 Global Accelerator API 作業新增或移除標籤。如需詳細資訊 (也含 CLI 範例)，請參閱TagResource中的AWS Global Accelerator API 參考。

若要新增標籤、編輯或刪除在 Global Accelerator 中的標籤

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 選擇您要新增或更新標籤的加速器。
3. 在 中Tags (標籤)區段中，您可以執行下列操作：

新增標籤

選擇新增標籤，然後輸入一個金鑰，並選擇性地輸入標籤的值。

編輯標籤

更新金鑰、值或兩者的文字。也可以清除標籤的值，但仍須金鑰。

刪除標籤

選擇Remove (移除)在值欄位右側。

4. 選擇 Save changes (儲存變更)。

AWS Global Accelerator 的定價

使用 AWS Global Accelerator，您只需按實際用量付費。每個加速器會依小時費率和資料傳輸費用（不管狀態為啓用或禁用），向您收取費用。如需詳細資訊，請參閱「AWS Global Accelerator 定價」。

AWS Global Accelerator

這些教學課程提供使用主控台開始使用 AWS Global Accelerator 的步驟。您也可以使用 AWS Global Accelerator API 作業來建立和自訂加速器。在本教學課程的每個步驟中，都有一個連結到對應的 API 作業，以程式設計方式完成工作。(當您設定自訂路由加速器時，必須針對特定設定步驟使用 API。) 如需 AWS Global Accelerator API 操作的詳細資訊，請參閱AWS Global Accelerator API 參考。

> **Tip**
>
> 若要探索如何使用全域加速器來改善 Web 應用程式的效能和可用性，請參閱下列自訂進度研討會：AWS Global Accelerator 講座。

全球加速器是一項全球服務，可支援多個 AWS 區域的終端節點，列於AWS 區域表格。

本章包含兩個教學課程：一個用於建立標準加速器，另一個用於建立自訂路由加速器。若要進一步了解這兩種加速器，請參閱使用 AWS Global Accelerator 中的標準加速器和使用 AWS Global Accelerator 中的自訂路由加速器。

主題

- 標準 Accelerator 入門
- 自訂路由加速器

標準 Accelerator 入門

本節提供建立標準加速器，以將流量路由至最佳端點。

工作

- 開始之前
- 步驟 1：建立加速器
- 步驟 2：新增接聽程式
- 步驟 3：新增端點群組
- 步驟 4：新增端點
- 步驟 5：測試您的加速器

- 步驟 6 (選擇性)：刪除加速器

開始之前

建立加速器之前，請至少建立一個資源，您可以將其新增為端點，以便將流量導向。例如，建立下列其中一項：

- 啟動至少一個要新增為終端節點的 Amazon EC2 執行個體。如需詳細資訊，請參閱「」建立 EC2 資源並啟動 EC2 執行個體中的Amazon EC2 Linux 執行個體使用者指南。
- 選擇性地建立一或多個包含 EC2 執行個體的網路負載平衡器或應用程式負載平衡器。如需詳細資訊，請參閱「」建立 Network Load Balancer Application Load Balancer中的網路負載平衡器使用者指南。

當您建立資源以新增至 Global Accelerator 時，請注意下列事項：

- 當您在全域加速器中新增內部 Application Load Balancer 或 EC2 執行個體端點時，您可以將網際網路流量鎖定在私有子網路中，以便直接進出虛擬私有雲 (VPC) 的端點。包含負載平衡器或 EC2 執行個體的 VPC 必須具有網際網路閘道連接到它，以表明 VPC 接受互聯網流量。如需詳細資訊，請參閱 AWS Global Accelerator 中的安全 VPC 連線。
- 全域加速器要求您的路由器和防火牆規則允許來自與 Route 53 健全狀況檢查程式相關聯之 IP 位址的輸入流量，以完成 EC2 執行個體或彈性 IP 位址端點的健全狀況檢查。如需有關與 Amazon Route 53 運作狀態檢查程式相關聯的 IP 位址範圍的資訊，請參閱目標群組運作狀態檢查中的Amazon Route 53 開發人員指南。

步驟 1：建立加速器

若要建立加速器，請輸入名稱。

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱建立加速器中的AWS Global Accelerator API 參考。

建立加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。

2. 選擇建立加速器。
3. 提供加速器的名稱。
4. 或者，新增一或多個標籤，以利識別 Global Accelerator 資源。
5. 選擇下一步。

步驟 2：新增接聽程式

建立接聽程式，以處理從使用者至 Global Accelerator 的入站連線。

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱CreateListener中的AWS Global Accelerator。

建立接聽程式

1. 在新增接聽程式頁面上，輸入要與接聽程式產生關聯的連接埠或連接埠範圍。接聽程式支援連接埠 1-65535。
2. 為您輸入的連接埠選擇通訊協定。
3. 選擇性地選擇啟用用戶端親和性。接聽程式的用戶端親和性表示「全域加速器」可確保來自特定來源 (用戶端) IP 位址的連線一律路由至相同的端點。若要啟用此行為，請在下拉式清單中選擇來源 IP。

   預設為 。無，表示未啟用用戶端親和性，而且「全域加速器」會在接聽程式的端點群組中的端點間平均分配流量。

   如需詳細資訊，請參閱 用戶端親和性。
4. 選擇性地選擇新增接聽程式以新增額外的偵聽程式。
5. 完成接聽程式，請選擇下一頁。

步驟 3：新增端點群組

新增一或多個端點群組，每個群組都與特定 AWS 區域相關聯。

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱建立端點群組中的AWS Global Accelerator。

新增端點群組

1. 在新增端點群組頁面上，在偵聽程式的區段中，選擇區域從下拉式清單。
2. (可選)流量撥打中，輸入介於 0 到 100 之間的數字，以設定此端點群組的流量百分比。此百分比只會套用至已導向至此端點群組的流量，而非所有接聽程式流量。根據預設，端點群組的流量撥號設定為 100 (也就是 100%)。
3. 或者，對於自訂健全狀況檢查值，請選擇設定運作狀態檢查。當您設定健全狀況檢查設定時，全域加速器會使用 EC2 執行個體和彈性 IP 位址端點的健全狀況檢查設定。針對 Network Load Balancer 和 Application Load Balancer 端點，全域加速器會使用您已為負載平衡器本身設定的健全狀況檢查設定。如需詳細資訊，請參閱 運作狀態檢查選項。
4. 選擇性地選擇新增端點群組，以針對此接聽程式或其他接聽程式新增其他端點群組。
5. 選擇下一步。

步驟 4：新增端點

新增一或多個與特定端點群組相關聯的端點。不需要此步驟，但除非端點包含在端點群組中，否則不會將流量導向區域中的端點。

> **Note**
>
> 如果您要以程式設計方式建立加速器，則會新增端點做為新增端點群組的一部分。如需詳細資訊，請參閱「」建立端點群組中的AWS Global Accelerator。

新增端點

1. 在建立端點頁面上，在端點的區段中，選擇端點。
2. (可選)Weight (粗細)中，輸入介於 0 到 255 之間的數字，以設定將流量路由傳送至此端點的權數。將權重新增至端點時，您可以設定 Global Accelerator，以根據指定的比例路由流量。依預設，所有端點的權重皆為 128。如需詳細資訊，請參閱 端點權重。

3. 或者，針對 Application Load Balancer 端點，在保留用戶端 IP 地址中，選取保留地址。如需詳細資訊，請參閱 在 AWS Global Accelerator 中保留用戶端 IP 地址。
4. 選擇性地選擇新增端點以新增更多端點。
5. 選擇下一步。

在您選擇下一頁，在 [全域加速器] 儀表板上，您會看到一則訊息，指出您的加速器正在進行中。程序完成時，儀表板中的加速器狀態為作用中。

步驟 5：測試您的加速器

採取步驟測試您的加速器，以確保流量被導向到您的端點。例如，執行捲曲命令 (如下所示)，取代加速器的其中一個靜態 IP 位址，以顯示處理請求的 AWS 區域。如果您為端點設定不同的權數，或調整端點群組上的流量撥號，這會特別有用。

運行如下所示的 curl 命令，替換加速器的靜態 IP 地址之一，調用 IP 地址 100 次，然後輸出每個請求的處理位置的計數。

```
for ((i=0;i<100;i++)); do  curl http://198.51.100.0/ >> output.txt; done; cat
 output.txt | sort | uniq -c ; rm output.txt;
```

如果您已調整任何端點群組上的流量撥號，此命令可協助您確認加速器是否將正確的流量百分比導向不同群組。如需詳細資訊，請參閱下列部落格文章AWS Global Accelerator。

步驟 6 (選擇性)：刪除加速器

如果您已建立加速器做為測試，或者您不再使用加速器，您可以將其刪除。請在主控台上停用加速器，然後您就可以將其刪除。您不需要從加速器移除接聽程式和端點群組。

若要使用 API 作業而非主控台來刪除加速器，您必須先移除與加速器相關聯的所有接聽程式和端點群組，並停用加速器。如需詳細資訊，請參閱 。刪除加速器中的操作AWS Global Accelerator。

移除端點或端點群組或刪除加速器時，請注意下列事項：

- 當您建立加速器時，全域加速器會提供一組兩個靜態 IP 位址。只要 IP 位址存在，即使您停用加速器且不再接受或路由流量，也會指派給您的加速器。但是，當您delete加速器時，您會遺失指派給加速器的靜態 IP 位址，因此您無法再使用它們來路由流量。最佳作法是確保您擁有適當的權限，以避免不小心刪除加速器。您可以將 IAM 政策搭配全域加速器 (例如標籤型權限) 使用，以限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

- 如果您在將 EC2 執行個體從全域加速器的端點群組中移除之前終止該 EC2 執行個體，然後使用相同的私人 IP 位址建立另一個執行個體，且運作狀況檢查已通過，則全域加速器會將流量路由傳送到新的端點。如果您不想發生這種情況，請在終止執行個體之前從端點群組移除 EC2 執行個體。

刪除加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 選擇想要刪除的加速器。
3. 選擇 Edit (編輯)。
4. 選擇停用加速，然後選擇Save (儲存)。
5. 選擇想要刪除的加速器。
6. 選擇刪除加速器。
7. 在確認對話方塊中，選擇 Delete (刪除)。

自訂路由加速器

本節提供建立自訂路由加速器的步驟，該加速器將流量確定路由傳送到虛擬私有雲 (VPC) 子網路端點中的 Amazon EC2 執行個體目的地。

工作

開始之前

建立自訂路由加速器之前，請先建立可新增做為端點的資源，以便將流量引導至。自訂路由加速器端點必須是 Virtual Private Cloud (VPC) 子網路，其中可以包含多個 Amazon EC2 執行個體。如需建立資源的指示，請參閱下列主題：

- 建立 VPC 子網路。如需詳細資訊，請參閱「」建立和設定您的 VPC中的AWS Directory Service 管理指南。
- 或者，在 VPC 中啟動一或多個 Amazon EC2 執行個體。如需詳細資訊，請參閱「」建立 EC2 資源並啟動 EC2 執行個體中的Amazon EC2 Linux 執行個體使用者指南。

當您建立資源以新增至 Global Accelerator 時，請注意下列事項：

- 當您在全域加速器中新增 EC2 執行個體端點時，可透過將網際網路流量鎖定在私有子網路中，讓網際網路流量直接進出 VPC 中的端點。包含 EC2 執行個體的 VPC 必須具有網際網路閘道連接到它，以表明 VPC 接受互聯網流量。如需詳細資訊，請參閱 AWS Global Accelerator 中的安全 VPC 連線。

步驟 1：建立自訂路由加速器

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱建立自訂路由加速器中的AWS Global Accelerator。

建立加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 提供加速器的名稱。
3. 適用於加速器類型中，選取自訂路由。
4. 或者，新增一或多個標籤，以利識別加速器資源。
5. 選擇下一頁以新增接聽程式、端點群組和 VPC 子網路端點。

步驟 2：新增接聽程式

建立接聽程式，以處理從使用者至 Global Accelerator 的入站連線。

您在建立接聽程式時指定的範圍會定義您可以搭配自訂路由加速器使用的接聽程式連接埠和目的地 IP 位址組合數目。若要獲得最大的彈性，建議您指定較大的連接埠範圍。您指定的每個接聽程式連接埠範圍至少必須包含 16 個連接埠。

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱建立自訂路由監聽程式中的AWS Global Accelerator。

建立接聽程式

1. 在新增接聽程式頁面上，輸入要與接聽程式產生關聯的連接埠或連接埠範圍。接聽程式支援連接埠 1-65535。
2. 為您輸入的連接埠選擇通訊協定。
3. 選擇性地選擇新增接聽程式以新增額外的偵聽程式。
4. 完成接聽程式，請選擇下一頁。

步驟 3：新增端點群組

新增一或多個端點群組，每個群組都與特定 AWS 區域相關聯。針對每個端點群組，指定一或多組連接埠範圍和通訊協定。全球加速器使用這些功能將流量導向區域子網路中的 Amazon EC2 執行個體。

對於您提供的每個連接埠範圍，您也可以指定要使用的通訊協定：UDP、TCP 或同時使用 UDP 和 TCP。

> **Note**
>
> 若要使用 API 操作而非主控台來完成此任務，請參閱建立自訂佈線端點群組中的AWS Global Accelerator。

新增端點群組

1. 在新增端點群組頁面上，在偵聽程式的區段中，選擇區域。
2. 適用於連接埠和協定集中，輸入 Amazon EC2 執行個體的連接埠範圍和通訊協定。
   - 輸入從連接埠和至連接埠指定一個範圍內的連接埠。
   - 針對每個連接埠範圍，指定該範圍的通訊協定。

連接埠範圍不一定是接聽程式連接埠範圍的子集，但是接聽程式連接埠範圍中必須有足夠的總連接埠，才能支援您指定的連接埠總數。

3. 選擇 Save (儲存)。
4. 選擇性地選擇新增端點群組，以針對此接聽程式或其他接聽程式新增其他端點群組。
5. 選擇下一步。

步驟 4：新增 VPC 子網路端點

針對此區域端點群組新增一或多個 Virtual Private Cloud (VPC) 子網路端點。自訂路由加速器的端點定義可透過自訂路由加速器接收流量的 VPC 子網路。每個子網路可以包含一個或多個 Amazon EC2 執行個體目的地。

當您新增 VPC 子網路端點時，全域加速器會產生新的連接埠對應，您可以使用此對應將流量路由傳送至子網路中的目的地 EC2 執行個體 IP 位址。然後，您可以使用全域加速器 API 取得子網路之所有連接埠對應的靜態清單，並使用對應決定性地將流量導向至特定 EC2 執行個體。

> **Note**
>
> 此處的步驟顯示如何在主控台中新增端點。如果您要以程式設計方式建立加速器，請新增具有端點群組的端點。如需詳細資訊，請參閱「」建立自訂佈線端點群組中的AWS Global Accelerator。

新增端點

1. 在新增端點頁面上，在想要新增端點的端點群組區段中，選擇端點。
2. 選擇性地執行下列其中一項作業，以啟用子網路中 EC2 執行個體目的地的流量：

   - 若要允許流量導向至子網路上的所有 EC2 端點和連接埠，請選取允許所有流量
   - 若要允許流量到子網路上的特定 EC2 端點和連接埠，請選取允許流量到特定目的地通訊端位址。然後指定要允許的 IP 位址以及連接埠或連接埠範圍。最後，請選擇允許這些目標。

   根據預設，不允許傳輸到子網路端點。如果您沒有選取允許流量的選項，子網路中所有目的地的流量都會遭到拒絕。

> **Note**
>
> 如果您想要啟用子網路中特定 EC2 執行個體和連接埠的流量，您可以透過程式設計方式執行此動作。如需詳細資訊，請參閱「」允許自訂路由流量中的AWS Global Accelerator。

3. 選擇下一步。

在您選擇下一頁，在全域加速器的儀表板上，您會看到一則訊息，指出您的加速器正在進行中。程序完成時，儀表板中的加速器狀態為作用中。

步驟 5 (選擇性)：刪除加速器

如果您已建立加速器做為測試，或者您不再使用加速器，您可以將其刪除。請在主控台上停用加速器，然後您就可以將其刪除。您不需要從加速器移除接聽程式和端點群組。

若要使用 API 作業而非主控台來刪除加速器，您必須先移除與加速器相關聯的所有接聽程式和端點群組，並停用加速器。如需詳細資訊，請參閱 。刪除自訂佈線加速器中的操作AWS Global Accelerator。

刪除加速器時請注意下列事項：

- 當您建立加速器時，全域加速器會提供一組兩個靜態 IP 位址。只要 IP 位址存在，即使您停用加速器且不再接受或路由流量，也會指派給您的加速器。但是，當您delete加速器時，您會遺失指派給加速器的靜態 IP 位址，因此您無法再使用它們來路由流量。最佳作法是確保您擁有適當的權限，以避免不小心刪除加速器。您可以使用 IAM 政策 (例如標籤型權限) 搭配全域加速器來限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

刪除加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 選擇想要刪除的加速器。
3. 選擇 Edit (編輯)。
4. 選擇停用加速，然後選擇Save (儲存)。
5. 選擇想要刪除的加速器。
6. 選擇刪除加速器。
7. 在確認對話方塊中，選擇 Delete (刪除)。

可搭配 AWS Global Accelerator 使用的常見動作

本節列出可搭配全域加速器資源使用的常見 AWS 全域加速器動作，以及相關文件的連結。

搭配標準資源使用的動作

下表列出可搭配「全域加速器」標準加速器使用的常見「全域加速器」動作，以及相關文件的連結。

Action	使用全域加速器主控台	使用全域加速器 API
建立標準加速器	請參閱 標準 Accelerator 入門	請參閱 CreateAccelerator
為建立接聽程式	請參閱 AWS Global Accelerator 中標準加速器的接聽程式	請參閱 CreateListener
建立標準加速器的端點群組	請參閱 AWS Global Accelerator 中標準加速器的端點群組	請參閱 CreateEndpointGroup
更新標準加速器	請參閱 AWS Global Accelerator 中的標準加速器	請參閱 UpdateAccelerator
列出您的加速器	請參閱 檢視您的加速器	請參閱 ListAccelerator
取得加速器的所有資訊	請參閱 檢視您的加速器	請參閱 DescribeAccelerator
刪除加速器	請參閱 建立或更新標準加速器	請參閱 DeleteAccelerator

與自訂路由資源搭配使用的動作

下表列出可與自訂路由加速器搭配使用的常見「全域加速器」動作，以及相關文件的連結。

Action	使用全域加速器主控台	使用全域加速器 API
建立自訂路由加速器	請參閱 自訂路由加速器	請參閱 CreateCustomRoutingAccelerator
為建立接聽程式	請參閱 AWS Global Accelerator 中自訂路由加速器的偵聽程式	請參閱 CreateCustomRoutingListener
為建立端點群組	請參閱 AWS Global Accelerator 中用於自訂路由加速器的端點群組	請參閱 CreateCustomRoutingEndpointGroup
更新自訂路由加速器	請參閱 AWS Global Accelerator 中的自訂路由加速器	請參閱 UpdateCustomRoutingAccelerator
列出您的自訂路由加速器	請參閱 檢視您的自訂路由加速器	請參閱 ListCustomRoutingAccelerator
取得自訂路由加速器的所有資訊	請參閱 檢視您的自訂路由加速器	請參閱 DescribeCustomRoutingAccelerator
刪除自訂路由加速器	請參閱 建立或更新自訂路由加速器	請參閱 DeleteCustomRoutingAccelerator
取得自訂路由加速器的靜態連接埠對應	無	請參閱 ListCustomRoutingPortMappings
允許自訂路由加速器中子網路的所有目的地流量	請參閱 新增、編輯或移除 VPC 子網路端點	請參閱 AllowCustomRoutingTraffic
拒絕自訂路由加速器中子網路的所有目的地流量	請參閱 新增、編輯或移除 VPC 子網路端點	請參閱 DenyCustomRoutingTraffic

Action	使用全域加速器主控台	使用全域加速器 API
在自訂路由加速器中允許流量到特定目的地	請參閱 新增、編輯或移除 VPC 子網路端點	請參閱 AllowCustomRoutingTraffic
在自訂路由加速器中拒絕特定目的地的流量	請參閱 新增、編輯或移除 VPC 子網路端點	請參閱 DenyCustomRoutingTraffic

使用 AWS Global Accelerator 中的標準加速器

本章包含在 AWS Global Accelerator 中建立標準加速器的程序和建議。使用標準加速器，全域加速器會為您的流量選擇最接近的正常端點。

如果您想要使用自訂應用程式邏輯，將一或多個使用者導向多個端點之間的特定端點，請建立自訂路由加速器。如需詳細資訊，請參閱 使用 AWS Global Accelerator 中的自訂路由加速器。

若要設定標準加速器，請執行下列步驟：

1. 建立加速器，然後選擇標準加速器選項。
2. 新增具有特定連接埠或連接埠範圍的監聽器，然後選擇要接受的協定：TCP、UDP 或兩者。
3. 新增一或多個端點群組，為您擁有端點資源的每個 AWS 區域新增一個端點群組。
4. 在端點群組中新增一或多個端點。這不是必需的，但如果您沒有任何端點，則不會路由流量。端點可以是網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。

下列各節逐步說明使用標準加速器、接聽程式、端點群組和端點。

主題

AWS Global Accelerator 中的標準加速器

A標準加速器會將流量導向 AWS Global Accelerator (透過 AWS Global Accelerator)，提升網際網路應用程式的可用性和效能，提升全球觀眾的使用體驗。每個加速器都包含一或多個接聽程式。監聽器會根據您設定的通訊協定 (或通訊協定) 和連接埠 (或通訊埠範圍)，處理從屬端到「全域加速器」的輸入連線。

當您建立加速器時，根據預設，全域加速器會提供一組兩個靜態 IP 位址。如果您將自己的 IP 地址範圍帶入 AWS (BYOIP)，則可以從自己的集區指派靜態 IP 地址，以利搭配加速器使用。如需詳細資訊，請參閱 在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)。

> **Important**
>
> 只要 IP 位址存在，就會指派給加速器，即使您停用加速器且不再接受或路由流量。但是，當您delete加速器時，您會遺失指派給加速器的全域加速器靜態 IP 位址，因此您無法再使用它們來路由流量。最佳作法是確保您擁有適當的權限，以避免意外刪除加速器。您可以將 IAM 政策搭配全域加速器 (例如標籤型權限) 使用，以限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

本節說明如何在全域加速器主控台上建立、編輯或刪除標準加速器。如果您想要使用 API 作業搭配 Global Accelerator，請參閱AWS Global Accelerator API 參考。

主題

建立或更新標準加速器

本節說明如何在主控台上建立或更新標準加速器。若要以程式設計方式使用全域加速器，請參閱AWS Global Accelerator API 參考。

建立標準加速器的步驟

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 選擇建立加速器。
3. 提供加速器的名稱。
4. 適用於加速器類型中，選取Standard (標準)。
5. 或者，如果您將自己的 IP 位址範圍帶到 AWS (BYOIP)，則可以為加速器指定靜態 IP 位址，每個位址集區中一個。針對加速器的兩個靜態 IP 位址，選擇此選項。
   - 針對每個靜態 IP 位址，選擇要使用的 IP 位址集區。

> **Note**
>
> 您必須為每個靜態 IP 位址選擇不同的 IP 位址集區。此限制是因為「全域加速器」會將每個位址範圍指派給不同的網路區域，以達到高可用性。

- 如果您選擇自己的 IP 地址集區，請從集區選擇特定的 IP 地址。如果您選擇預設的 Amazon IP 位址集區，則全域加速器會為您的加速器指派特定 IP 位址。

6. 或者，您可以新增一或多個標籤，以利識別加速器資源。
7. 選擇下一頁以新增接聽程式、端點群組和端點。

編輯標準加速器的步驟

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器清單中，選擇加速器，然後選擇Edit (編輯)。
3. 在編輯加速器頁面上，進行任何您喜歡的變更。例如，您可以停用加速器，讓加速器不再接受或路由流量，或讓您可以將其刪除。或者，如果加速器已停用，您可以加以啟用。
4. 選擇 Save changes (儲存變更)。

刪除加速器

如果您已建立加速器做為測試，或者您不再使用加速器，您可以將其刪除。請在主控台上停用加速器，然後您就可以將其刪除。您不需要從加速器移除接聽程式和端點群組。

若要使用 API 作業而非主控台來刪除加速器，您必須先移除與加速器相關聯的所有接聽程式和端點群組，然後將其停用。如需詳細資訊，請參閱 。刪除加速器中的操作AWS Global Accelerator API 參考。

停用加速器的步驟

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在清單中，選擇您要停用的加速器。
3. 選擇 Edit (編輯)。
4. 選擇停用加速器，然後選擇Save (儲存)。

刪除加速器的步驟

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在清單中，選擇您要刪除的加速器。
3. 選擇 Delete (刪除)。

> **Note**
>
> 如果您尚未停用加速器，請先刪除無法使用。

4. 在確認對話方塊中，選擇 Delete (刪除)。

> **Important**
>
> 刪除加速器時，您會遺失指派給加速器的靜態 IP 位址，因此您無法再使用它們來路由流量。

檢視您的加速器

您可以在主控台上檢視加速器的相關資訊。若要以程式設計方式查看加速器的說明，請參閱清單加速器和DescribeAccelerator中的AWS Global Accelerator API 參考。

檢視加速器的相關資訊

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 若要查看加速器的詳細資料，請在清單中選擇加速器，然後選擇檢視。

建立負載平衡器時新增加速器

在 AWS 管理主控台中建立 Application Load Balancer 時，您可以選擇性地使用同時新增加速器。Elastic Load Balancing 和全域加速器共同運作，為您透明地添加加速器。加速器會在您的帳戶中建立，並將負載平衡器做為端點。使用加速器可提供靜態 IP 地址，並改善應用程式的可用性和效能。

> **Important**
>
> 若要建立加速器，您必須擁有正確的權限。如需詳細資訊，請參閱 主控台存取、驗證管理和存取控制所需的權限。

設定及檢視您的加速器

您必須更新 DNS 組態，將流量導向至加速器的靜態 IP 位址或 DNS 名稱。在組態變更完成之前，流量不會通過加速器進入負載平衡器。

在 Amazon EC2 主控台上選擇全域加速器附加元件來建立負載平衡器後，請前往整合服務索引標籤，以查看加速器的靜態 IP 地址和網域名稱系統 (DNS) 名稱。您可以使用此資訊，透過 AWS 全球網路啟動將使用者流量路由至負載平衡器。如需更多關於指派給加速器的 DNS 名稱的資訊，請參閱AWS Global Accelerator 中的 DNS 定址和自訂網域。

您可以檢視和設定加速器瀏覽至 Global Accelerator(在 AWS 管理主控台中)。例如，您可以查看與您的帳戶相關聯的加速器，或將其他負載平衡器新增至加速器。如需更多詳細資訊，請參閱 檢視您的加速器 及 建立或更新標準加速器。

定價

使用 AWS Global Accelerator，您只需按實際用量付費。每個加速器會依小時費率和資料傳輸費用（不管狀態為啓用或禁用），向您收取費用。如需詳細資訊，請參閱「AWS Global Accelerator 定價」。

停止使用加速器

如果您想要停止透過全域加速器將流量路由傳送至負載平衡器，請執行下列動作：

1. 更新 DNS 組態，將流量直接指向負載平衡器。
2. 從加速器刪除負載平衡器。如需詳細資訊，請參閱「」移除端點中的新增、編輯或移除標準端點。
3. 刪除加速器。如需詳細資訊，請參閱 刪除加速器。

使用全域靜態 IP 位址而非區域靜態 IP 位址

如果您想要在 AWS 資源前使用靜態 IP 地址，例如 Amazon EC2 執行個體，則有多個選項。例如，您可以分配彈性 IP 地址，這是一個靜態 IPv4 地址，您可以與單一 AWS 區域中的 Amazon EC2 執行個體或網路界面建立關聯。

如果您擁有全球受眾，您可以使用全球加速器建立加速器，以取得從全球 AWS 節點宣佈的兩個全球靜態 IP 位址。如果您已經在一個或多個區域 (包括 Amazon EC2 執行個體、網路負載平衡器和應用程式負載平衡器) 中為應用程式設定 AWS 資源，則可以輕鬆地將這些資源新增到全球加速器，以便使用全球靜態 IP 地址。

選擇使用全域加速器佈建的全域靜態 IP 位址也可以改善應用程式的可用性和效能。使用全域加速器，靜態 IP 位址可接受從最接近使用者的節點位置傳入 AWS 全域網路的傳入流量。將流量在 AWS 網路上的時間最大化，可以提供更快、更好的客戶體驗。如需詳細資訊，請參閱 AWS Global Accelerator 如何運作 。

您可以從 AWS 管理主控台新增加速器，或透過 AWS CLI 或開發套件搭配使用 API 操作來新增加速器。如需詳細資訊，請參閱 建立或更新標準加速器。

新增加速器時請注意以下事項：

- 只要加速器存在，即使您停用加速器且不再接受或路由流量，全域加速器佈建的全域靜態 IP 位址仍然會指派給您。不過，如果您刪除加速器，就會遺失指派給它的靜態 IP 位址。如需詳細資訊，請參閱 刪除加速器。
- 使用 AWS Global Accelerator，您只需按實際用量付費。每個加速器會依小時費率和資料傳輸費用（不管狀態為啓用或禁用），向您收取費用。如需詳細資訊，請參閱「AWS Global Accelerator 定價」。

AWS Global Accelerator 中標準加速器的接聽程式

使用 AWS Global Accelerator，您可以新增監聽程式，以根據您指定的連接埠和通訊協定處理來自用戶端的輸入連線。接聽程式支援 TCP、UDP 或 TCP 和 UDP 通訊協定。

當您在立標準加速器時便定義標準接聽程式，然後可隨時新增接聽程式更多接聽程式。您可以將每個接聽程式與一或多個端點群組建立關聯，然後將每個端點群組與一個 AWS 區域建立關聯。

主題

- 新增、編輯或移除標準監聽器
- 用戶端親和性

新增、編輯或移除標準監聽器

本節說明如何使用 AWS Global Accelerator 主控台上的接聽程式。若要使用 API 作業而非主控台來完成這些工作，請參閱CreateListener、UpdateListener，以及DeleteListener中的AWS Global Accelerator API 參考。

加入接聽程式

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 選擇 Add listener (新增接聽程式)。
4. 在新增接聽程式頁面上，輸入要與接聽程式產生關聯的連接埠或連接埠範圍。接聽程式支援連接埠 1-65535。
5. 選擇您輸入的連接埠的通訊協定。
6. 選擇性地選擇啟用用戶端親和性。接聽程式的用戶端親和性表示「全域加速器」可確保來自特定來源 (用戶端) IP 位址的連線一律路由至相同的端點。若要啟用此行為，請在下拉式清單中選擇來源 IP。

   預設為 。無，表示未啟用用戶端親和性，而且「全域加速器」會在接聽程式的端點群組中的端點間平均分配流量。

   如需詳細資訊，請參閱 用戶端親和性。
7. 選擇 Add listener (新增接聽程式)。

編輯標準監聽器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 選擇接聽程式，然後選擇編輯接聽程式。
4. 在編輯接聽程式頁面上，變更您要與接聽程式產生關聯的連接埠、連接埠範圍或通訊協定。
5. 選擇性地選擇啟用用戶端親和性。接聽程式的用戶端親和性表示「全域加速器」可確保來自特定來源 (用戶端) IP 位址的連線一律路由至相同的端點。若要啟用此行為，請在下拉式清單中選擇來源 IP。

   預設為 。無，表示未啟用用戶端親和性，而且「全域加速器」會在接聽程式的端點群組中的端點間平均分配流量。

如需詳細資訊，請參閱 用戶端親和性。

6. 選擇 Save (儲存)。

移除接聽程式

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 選擇接聽程式，然後選擇Remove (移除)。
4. 在確認對話方塊中，選擇Remove (移除)。

用戶端親和性

如果您有與標準加速器搭配使用的可設定狀態應用程式，則可以選擇讓全域加速器將特定來源 (用戶端) IP 位址之使用者的所有要求導向至相同的端點資源，以維護用戶端親和性。

根據預設，標準接聽程式的用戶端親和性設定為無和全域加速器會在接聽程式的端點群組中的端點間平均分配流量。

Global Accelerator 會使用一致流程雜湊演算法來選擇使用者連線的最佳端點。如果您將全域加速器資源的用戶端親和性設定為無時，全域加速器會使用 5 元組屬性 (來源 IP、來源連接埠、來源連接埠、目的地 IP、目的地連接埠和通訊協定) 來選取雜湊值。接下來，它會選擇提供最佳效能的端點。如果指定的用戶端使用不同的連接埠連線到 Global Accelerator，並且您已指定此設定，則 Global Accelerator 無法確保來自用戶端的連線永遠路由到相同的端點。

如果您想要透過將特定使用者 (由其來源 IP 位址識別) 路由傳送至每次連線時的相同端點來維護用戶端親和性，請將用戶端親和性設定為來源 IP。當您指定此選項時，Global Accelerator 會使用 2 元組屬性 (來源 IP 和目的地 IP) 來選取雜湊值，並在連線時將使用者路由到相同的端點。全域加速器會在您選取的端點群組之後接受用戶端親和性。

AWS Global Accelerator 中標準加速器的端點群組

端點群組會將請求路由至 AWS Global Accelerator 中的一個或多個註冊端點。當您在標準加速器中新增接聽程式時，您可以為全域加速器指定要將流量導向的端點群組。端點群組及其中的所有端點必須位於一個 AWS 區域。您可以為不同的用途新增不同的端點群組，例如，用於藍色/綠色部署測試。

全域加速器會根據用戶端位置和端點群組的健全狀況，將流量導向標準加速器中的端點群組。您也可以視需要設定傳送至端點群組的流量百分比。您可以使用流量撥打來增加 (向上撥打) 或減少 (向下撥打)

至群組的流量。此百分比只會套用至全域加速器已導向至端點群組的流量，而非所有傳入接聽程式的流量。

您可以為每個端點群組定義全域加速器的健全狀況檢查設定。透過更新運作狀態檢查設定，您可以變更輪詢和驗證 Amazon EC2 執行個體和彈性 IP 位址端點的運作狀態需求。對於 Network Load Balancer 和 Application Load Balancer 端點，請在 Elastic Load Balancing 主控台上設定健全狀況檢查設定。

全域加速器會持續監控標準端點群組中所包含之所有端點的健全狀況，並僅將要求路由傳送至狀況良好的作用中端點。如果沒有任何正常的端點可路由流量到達，則全域加速器會將要求路由傳送至所有端點。

本節說明如何在 AWS Global Accelerator 主控台上使用標準加速器的端點群組。如果您想要使用 AWS Global Accelerator，請參閱AWS Global Accelerator API 參考。

主題

新增、編輯或移除標準端點群組

您可以在 AWS Global Accelerator 主控台上或使用 API 作業來使用端點群組。您可以隨時從端點群組新增端點或移除端點。

本節說明如何在 AWS Global Accelerator 主控台上使用標準端點群組。如果您想要使用 API 作業搭配 Global Accelerator，請參閱AWS Global Accelerator API 參考。

新增標準端點群組

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇您要為其新增端點群組的接聽程式 ID。
4. 選擇新增端點群組。
5. 在監聽器的段落中，從下拉式清單中選擇一個「區域」，指定端點群組的「區域」。
6. (選用)流量撥打中，輸入介於 0 到 100 之間的數字，以設定此端點群組的流量百分比。此百分比只會套用至已導向至此端點群組的流量，而非所有接聽程式流量。根據預設，流量撥號設定為 100。

7. 或者，若要覆寫用於將流量路由傳送至端點的接聽程式連接埠，並將流量重新路由傳送至端點上的特定連接埠，請選擇設定連接埠覆寫。如需詳細資訊，請參閱 連接埠覆寫。
8. 或者，若要指定要套用至 EC2 執行個體和彈性 IP 位址端點的自訂健全狀況檢查值，請選擇設定運作狀態檢查。如需詳細資訊，請參閱 運作狀態檢查選項。
9. 選擇性地選擇新增端點群組，為此接聽程式或其他接聽程式新增其他端點群組。
10. 選擇新增端點群組。

編輯端點群組

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇與端點群組相關聯的接聽程式 ID。
4. 選擇編輯端點群組。
5. 在編輯端點群組頁面上，變更區域、調整流量撥號百分比，或選擇設定運作狀態檢查來修改運作狀態檢查設定。
6. 選擇 Save (儲存)。

移除標準端點群組

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式區段中，選擇接聽程式，然後選擇Remove (移除)。
4. 在 中端點群組區段中，選擇端點群組，然後選擇Remove (移除)。
5. 在確認對話方塊上，選擇Remove (移除)。

使用流量撥號調整流量

針對每個標準端點群組，您可以設定流量撥號，以控制導向至群組的流量百分比。此百分比只會套用至已導向至端點群組的流量，而非所有接聽程式流量。

根據預設，加速器中所有區域端點群組的流量撥號設定為 100 (也就是 100%)。例如，流量撥號可讓您輕鬆地針對不同 AWS 區域的新版本進行效能測試或藍/綠部署測試。

以下是幾個範例，說明如何使用流量撥號將流量變更至端點群組。

按地區升級您的應用程式

如果您想要升級區域中的應用程式或進行維護，請先將流量撥號設定為 0，以切斷區域的流量。當您完成工作並準備好將區域恢復服務時，請將流量撥號調整為 100 以撥回流量。

混合兩個區域之間的流量

此範例顯示當您同時變更兩個地區端點群組的流量撥號時，流量流量的運作方式。假設您有兩個用於加速器的端點群組，一個用於us-west-2區域，另一個用於us-east-1區域，而且您已將每個端點群組的流量撥號設定為 50%。

現在，假設你有 100 個要求來到你的加速器，50 個來自美國東海岸，50 個來自西海岸。加速器會指示流量，如下所示：

- 每個海岸上的前 25 個要求 (總共 50 個要求) 會從其附近的端點群組提供服務。也就是說，25 個要求會導向至us-west-2中的端點群組，而 25 則會導向至us-east-1。
- 接下來的 50 個要求會導向至相反的區域。也就是說，接下來的 25 個要求從東海岸服務us-west-2，接下來的 25 個來自西海岸的請求將由us-east-1。

此案例的結果是兩個端點群組的服務流量相同。不過，每一個都會收到來自兩個區域的流量混合。

連接埠覆寫

依預設，加速器會使用您在建立接聽程式時指定的通訊協定和連接埠範圍，將使用者流量路由到 AWS 區域中的終端節點。例如，如果您定義接聽程式接受連接埠 80 和 443 上的 TCP 流量，則加速器會將流量路由傳送至端點上的那些連接埠。

但是，當您新增或更新端點群組時，您可以覆寫用來將流量轉傳到端點的接聽程式連接埠。例如，您可以建立連接埠覆寫，接聽程式會在其中的連接埠 80 和 443 上接收使用者流量，但加速器會將該流量分別路由至端點上的連接埠 1080 和 1443。

連接埠覆寫可協助您避免接聽受限制連接埠的問題。在端點上執行不需要超級使用者 (root) 權限的應用程式會比較安全。不過，在 Linux 和其他類 Unix 系統中，您必須具有超級使用者權限，才能在受限的連接埠 (TCP 或 UDP 連接埠低於 1024) 上接聽。藉由將接聽程式上的受限連接埠對應至端點上的非受限連接埠，連接埠覆寫可讓您避免此問題。您可以在全域加速器後方的端點上執行沒有 root 存取權的應用程式時，接受受限制連接埠上的流量 例如，您可以將接聽程式連接埠 443 覆寫至端點連接埠 8443。

針對每個連接埠覆寫，您可以指定接受來自使用者流量的接聽程式連接埠，以及全域加速器將路由傳送該流量的目標端點連接埠。如需詳細資訊，請參閱 新增、編輯或移除標準端點群組。

當您建立連接埠覆寫時，請謹記下列事項：

- 端點連接埠不能重疊接聽程式連接埠範圍。 您在連接埠覆寫中指定的端點連接埠不能包含在您為加速器設定的任何接聽程式連接埠範圍中。例如，假設您有兩個加速器的接聽程式，而且您已將這些接聽程式的連接埠範圍分別定義為 100-199 和 200-299。當您建立連接埠覆寫時，您無法定義從接聽程式連接埠 100 到端點連接埠 210 的連接埠，例如，因為端點連接埠 (210) 包含在您定義 (200-299) 的接聽程式連接埠範圍中。
- 沒有重複的端點連接埠。 如果加速器中的一個連接埠覆寫指定了端點連接埠，則您無法使用來自不同接聽程式連接埠覆寫的連接埠來指定相同的端點連接埠。例如，您無法指定從接聽程式連接埠 80 到端點連接埠 90 的連接埠覆寫，以及從接聽程式連接埠 81 到端點連接埠 90 的覆寫。
- Health 檢查會繼續使用原始連接埠。 如果您為設定為健全狀況檢查連接埠的連接埠指定連接埠覆寫，則健全狀況檢查仍會使用原始連接埠，而不是覆寫連接埠。例如，假設您在接聽程式連接埠 80 上指定健全狀況檢查，也指定從接聽程式連接埠 80 到端點連接埠 480 的連接埠覆寫。Health 檢查會繼續使用端點連接埠 80。不過，透過連接埠 80 進入的使用者流量會移至端點上的連接埠 480。

  此行為可維持 Network Load Balancer、Application Load Balancer、EC2 執行個體和彈性 IP 位址端點之間的一致性。由於在全域加速器中指定連接埠覆寫時，網路負載平衡器和應用程式負載平衡器不會將運作狀況檢查連接埠對應至不同的端點連接埠，因此全域加速器將運作狀況檢查連接埠對應至 EC2 執行個體和彈性 IP 的不同端點連接埠位址端點。
- 安全性群組設定必須允許連接埠存取。 確定您的安全群組允許流量到達您在連接埠覆寫中指定的端點連接埠。例如，如果您將接聽程式連接埠 443 覆寫到端點連接埠 1433，請確定在安全群組中為該 Application Load Balancer 或 Amazon EC2 端點設定的任何連接埠限制允許連接埠 1433 上的輸入流量。

運作狀態檢查選項

AWS Global Accelerator 會定期將請求傳送到標準端點來測試其狀態。這些健全狀況檢查會自動執行。決定每個端點健全狀況以及健全狀況檢查的時間的指引取決於端點資源的類型。

> **Important**
>
> 全域加速器要求您的路由器和防火牆規則允許來自與 Route 53 健全狀況檢查程式相關聯之 IP 位址的輸入流量，以完成 EC2 執行個體或彈性 IP 位址端點的健全狀況檢查。如需有關與 Amazon Route 53 運作狀態檢查程式相關聯的 IP 位址範圍的資訊，請參閱目標群組運作狀態檢查中的Amazon Route 53 開發人員指南。

您可以為端點群組設定下列健全狀況檢查選項。如果您指定健全狀況檢查選項，則全域加速器會使用 EC2 執行個體或彈性 IP 位址健全狀況檢查的設定，但不會使用網路負載平衡器或應用程式負載平衡器。

- 對於 Application Load Balancer 或 Network Load Balancer 端點，您可以使用 Elastic Load Balancing 組態選項來設定資源的健全狀況檢查。如需詳細資訊，請參閱「」目標群組運作狀態檢查。您在全域加速器中選擇的健全狀況檢查選項不會影響您新增為端點的應用程式負載平衡器或網路負載平衡器。

  > **Note**
  >
  > 當您擁有包含多個目標群組的 Application Load Balancer 或 Network Load Balancer 時，全域加速器會將負載平衡器端點視為狀況良好，只有在每個目標群組至少有一個狀況良好的目標。如果負載平衡器的任何單一目標群組只有狀況不良的目標，則全域加速器會將該端點視為狀況不良。

- 對於新增至使用 TCP 設定之接聽程式的 EC2 執行個體或彈性 IP 位址端點，您可以指定用於運作狀況檢查的連接埠。根據預設，如果您未指定健全狀況檢查的連接埠，則全域加速器會使用您為加速器指定的接聽程式連接埠。
- 對於具有 UDP 接聽程式的 EC2 執行個體或彈性 IP 位址端點，全域加速器會使用接聽程式連接埠和 TCP 通訊協定進行健全狀況檢查，因此您的端點上必須有 TCP 伺服器。

  > **Note**
  >
  > 請務必檢查您在每個端點上為 TCP 伺服器設定的連接埠是否與您在全域加速器中為健全狀況檢查指定的連接埠相同。如果連接埠號碼不相同，或者您尚未為端點設定 TCP 伺服器，則無論端點的健全狀況為何，全域加速器都會將端點標示為狀況不良。

運作 Health 檢查埠

Global Accelerator 在屬於此端點群組的端點上，執行運作狀態檢查時，使用的連接埠。

> **Note**
>
> 您無法設定健全狀況檢查連接埠的連接埠覆寫。

運作狀態檢查通訊協定

Global Accelerator 在屬於此端點群組的端點上，執行運作狀態檢查時，使用的通訊協定。

運作 Health 檢查間隔

端點每次運作狀態檢查間的間隔秒數。

閾值計數

將運作狀態不佳的目標視為運作狀態良好或運作狀態不佳之前，需連續運作狀態檢查的次數。

每個接聽程式只會將要求路由傳送至狀況良好 新增端點後，必須通過運作狀態檢查，才會被視為運作狀態良好。每次運作狀態檢查完成後，接聽程式即會關閉其為執行運作狀態檢查而建立的連線。

AWS Global Accelerator 中的標準加速器終端節點

AWS Global Accelerator 中標準加速器的終端節點可以是網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。使用標準的加速器，靜態 IP 地址可做為用戶端單一連絡窗口，然後全域加速器會將傳入流量分配到運作狀態良好的端點。全域加速器會使用您為端點之端點群組所屬接聽程式指定的連接埠 (或連接埠範圍)，將流量導向端點。

每個端點群組可有多個端點。您可以將每個端點新增至多個端點群組，但端點群組必須與不同的接聽程式相關聯。當您將資源新增為端點時，資源必須是有效且作用中的。

全域加速器會持續監控標準端點群組中所包含之所有端點的健全狀況。它只會將流量路由傳送至狀況良好的作用中端點。如果全域加速器沒有任何正常的端點可路由流量到達，則會將流量路由傳送到所有端點。

請注意下列特定類型的全域加速器標準端點：

負載平衡器端點

- Application Load Balancer 端點可以是網際網路面向或內部。Network Load Balancer 端點必須面向網際網路。

Amazon EC2 執行個體端點

- EC2 執行個體端點 (針對標準和自訂路由加速器) 不能是下列類型之一：
  C1、C1、C2、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、C1、
- EC2 執行個體僅支援部分 AWS 區域中的端點。如需支援的區域的清單，請參閱 用戶端 IP 位址保留的支援 AWS 區域。

- 建議您在終止執行個體之前，先從全域加速器端點群組移除 EC2 執行個體。如果您在將 EC2 執行個體從全域加速器的端點群組中移除之前終止該 EC2 執行個體，然後在具有相同私人 IP 位址的同一 VPC 中建立另一個執行個體，且運作狀況檢查已通過，則全域加速器會將流量路由傳送到新端點。

主題

新增、編輯或移除標準端點

您可以將端點新增至端點群組，以便將流量導向至您的資源。您可以編輯標準端點以變更端點的權重。或者，您也可以從端點群組移除加速器中移除端點。移除端點不會影響端點本身，但全域加速器無法再將流量導向該資源。

全域加速器中的端點可以是網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。您必須先建立其中一個資源，然後再將其新增為全域加速器中的端點。當您將資源新增為端點時，資源必須是有效且作用中的。

您可以根據使用情況，從端點群組新增端點或移除端點。例如，如果對應用程式的需求增加，您可以建立更多資源，然後將更多端點新增至一或多個端點群組，以處理增加的流量。全域加速器會在您新增端點之後立即啟動將請求路由到端點，並且端點通過初始的運作狀態檢查。您可以透過調整端點上的權重來管理端點的流量，按比例傳送或多或少的流量到端點。

如果您要新增具有用戶端 IP 位址保留的端點，請先檢閱用戶端 IP 位址保留的支援 AWS 區域和在 AWS Global Accelerator 中保留用戶端 IP 地址。

例如，如果您需要為端點提供服務，您可以從端點群組中移除端點。移除端點會將端點移出端點群組，但不會影響端點。一旦您從端點群組移除，全域加速器就會停止將流量導向端點。端點會進入等待所有目前要求完成的狀態，因此進行中的用戶端流量不會中斷。當您準備讓端點繼續接收請求時，可以將端點新增回端點群組。

本節說明如何使用 AWS Global Accelerator 主控台上的端點。如果您想要搭配 AWS Global Accelerator 使用 API 作業，請參閱AWS Global Accelerator API 參考。

新增標準端點

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式一節, 用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組一節, 用於端點群組 ID下，選擇您要為其新增端點的端點群組 ID。
5. 在 中端點區段中，選擇新增端點。
6. 在新增端點頁面上，從下拉式清單中選擇資源。

   如果您沒有任何 AWS 資源，則清單中沒有任何項目。若要繼續，請建立 AWS 資源，例如負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。然後回到這裡的步驟，並從列表中選擇一個資源。
7. (選用項目)Weight (粗細)中，輸入介於 0 到 255 之間的數字，以設定將流量路由傳送至此端點的權數。將權重新增至端點時，您可以設定全域加速器，以根據指定的比例路由流量。根據預設，所有端點的權重都是 128。如需詳細資訊，請參閱 端點權重。
8. (可選) 為面對網際網路的 Application Load Balancer 端點啟用用用用戶端 IP 地址保留。之下保留用戶端 IP 地址，選取保留地址。

   一律為內部 Application Load Balancer 和 EC2 執行個體端點選取此選項，並且從未為 Network Load Balancer 和彈性 IP 位址端點選取此選項。如需詳細資訊，請參閱 在 AWS Global Accelerator 中保留用戶端 IP 地址。

   > **Note**
   >
   > 在新增並開始將流量路由傳送至保留用戶端 IP 位址的端點之前，請確定已更新所有必要的安全性設定 (例如安全性群組)，以便在允許清單中包含使用者用戶端 IP 位址。
9. 選擇 Add endpoint (新增端點)。

編輯標準端點的步驟

您可以編輯端點組態來變更權重。如需詳細資訊，請參閱 端點權重。

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式一節, 用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組一節, 用於端點群組 ID下，選擇端點群組的 ID。

5. 選擇編輯端點。
6. 在編輯端點頁面、進行更新，然後選擇Save (儲存)。

移除端點

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式一節, 用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組一節, 用於端點群組 ID下，選擇端點群組的 ID。
5. 選擇移除端點。
6. 在確認對話方塊中，選擇Remove (移除)。

端點權重

權數是決定全域加速器導向至標準加速器中端點的流量比例的值。端點可以是網路負載平衡器、應用程式負載平衡器、Amazon EC2 執行個體或彈性 IP 地址。全域加速器會計算端點群組中端點的權重總和，然後根據每個端點的權重與總計的比率，將流量導向端點。

加權路由可讓您選擇將多少流量路由傳送至端點群組中的資源。這可用於數種方式，包括負載平衡和測試新版本的應用程式。

端點權重的運作方式

若要使用權重，請為端點群組中的每個端點指派相對權重，該值對應於您要傳送到端點群組的流量規模。根據預設，端點的權重是 128，也就是權重最大值 255 的一半。Global Accelerator 會根據指派給端點的權重 (佔該群組中所有端點總權重的比例) 將流量傳送到端點：

$$\frac{\text{Weight for a specified endpoint}}{\text{Sum of the weights for all endpoints}}$$

例如，如果您想要將一小部分的流量傳送到一個端點，並將其餘流量傳送到另一個端點，則可以指定權重 1 和 255。權重 1 的端點會取得 1/256 (1/1+255) 的流量，另一個端點會取得 255/256 (255/1+255) 的流量。您可以透過變更權重逐步變更負載平衡。如果您想要全域加速器停止傳送流量到端點，可以將該資源的權重變更為 0。

狀況不良端點的容錯移轉

如果端點群組中沒有正常的端點，權重大於零，則全域加速器會嘗試容錯移轉至另一個端點群組中權重大於零的狀況良好的端點。對於此容錯移轉，全域加速器會忽略流量撥號設定。因此，例如，如果端點群組的流量撥號設為零，則全域加速器仍會在容錯移轉嘗試中包含該端點群組。

如果全域加速器在嘗試其他三個終端群組 (也就是三個 AWS 區域) 後找不到權重大於零的狀況良好的終端節點，則會將流量路由到最接近用戶端的終端節點群組中的隨機終端節點。也就是說，它開啟失敗。

請注意以下內容：

- 選擇用於容錯移轉的端點群組可能是流量撥號設定為零的端點群組。
- 最近的端點群組可能不是原始端點群組。這是因為全域加速器選擇原始端點群組時，會考量帳戶流量撥號設定。

例如，假設您的組態有兩個端點，一個狀況良好，一個狀況不良，而且您已將每個端點的權重設定為大於零。在此情況下，全域加速器會將流量路由傳送至狀況良好的端點。但是，現在假設您將唯一健康端點的權重設置為零。然後全域加速器會嘗試其他三個端點群組，以尋找權重大於零的狀況良好的端點。如果找不到，則全域加速器會將流量路由傳送至最接近用戶端的端點群組中的隨機端點。

新增具有用戶端 IP 位址保留的端點

在某些區域中，您可以與某些端點類型搭配使用的功能是用戶端 IP 地址保留。透過此功能，您可以針對抵達端點的封包，保留原始用戶端的來源 IP 位址。您可以將此功能與 Application Load Balancer 和 Amazon EC2 執行個體終端節點搭配使用。自訂路由加速器上的端點一律會保留用戶端 IP 位址。如需詳細資訊，請參閱 在 AWS Global Accelerator 中保留用戶端 IP 地址。

如果您打算使用用戶端 IP 位址保留功能，請在將端點新增至全域加速器時注意下列事項：

彈性網路界面

為了支援用戶端 IP 位址保留，全球加速器會在您的 AWS 帳戶中建立彈性網路介面，每個有端點的子網路都有一個。如需全域加速器如何搭配彈性網路介面運作的詳細資訊，請參閱用戶端 IP 位址保留的最佳作法。

私有子網路中的端點

您可以使用 AWS Global Accelerator 將 Application Load Balancer 或 EC2 執行個體設定為私有子網路中的目標，但您必須擁有網際網路閘道附加到包含端點的 VPC 上。如需詳細資訊，請參閱 AWS Global Accelerator 中的安全 VPC 連線。

新增用戶端 IP 地址至允許清單

在新增並開始將流量路由傳送至保留用戶端 IP 位址的端點之前，請確定已更新所有必要的安全性設定 (例如安全性群組)，以便在允許清單中包含使用者用戶端 IP 位址。網路存取控制清單 (ACL) 僅套用到傳出 (傳出) 流量。如果您需要篩選入口 (輸入) 流量，則必須使用安全性群組。

設定網路存取控制清單 (ACL)

當加速器上啟用用戶端 IP 位址保留時，與 VPC 子網路關聯的網路 ACL 會套用至輸出 (輸出) 流量。不過，若要讓流量透過全域加速器結束，您必須將 ACL 設定為輸入和輸出規則。

例如，若要允許使用暫時來源連接埠的 TCP 和 UDP 用戶端透過全域加速器連線到您的端點，請將端點的子網路與網路 ACL 建立關聯，以允許傳送到暫時 TCP 或 UDP 連接埠 (連接埠範圍 1024-65535，目的地 0.0.0/0) 的輸出流量。此外，請建立相符的傳入規則 (連接埠範圍 1024-65535，來源不限)。

> **Note**
>
> 安全群組和 AWS WAF 規則是一組額外的功能，您可以套用這些功能來保護您的資源。例如，與 Amazon EC2 執行個體和應用程式負載平衡器相關聯的入埠安全群組規則可讓您控制用戶端透過全域加速器可連接的目標連接埠，例如 HTTP 的連接埠 80 或 HTTPS 的連接埠 443。請注意，Amazon EC2 執行個體安全群組適用於到達執行個體的任何流量，包括來自全球加速器的流量以及指派給執行個體的任何公用或彈性 IP 地址。最佳作法是，如果您想確保流量只能由全域加速器傳遞，請使用私人子網路。此外，請確定已適當地設定輸入安全性群組規則，以正確允許或拒絕應用程式的流量。

轉換端點以使用用戶端 IP 位址保留

請遵循本節中的指引，將加速器中的一或多個端點轉換至保留使用者用戶端 IP 位址的端點。您可以選擇將 Application Load Balancer 端點或彈性 IP 位址端點轉換至具有用戶端 IP 位址保留的對應端點 (Application Load Balancer 或 EC2 執行個體)。如需詳細資訊，請參閱 在 AWS Global Accelerator 中保留用戶端 IP 地址。

建議您轉換至使用用用戶端 IP 地址保留的速度緩慢。首先，新增您啟用的 Application Load Balancer 或 EC2 執行個體端點，以保留用戶端 IP 位址。然後在端點上設定權重，慢慢將流量從現有端點移至新端點。

> **Important**
>
> 開始將流量路由傳送至保留用戶端 IP 位址的端點之前，請確定已更新允許清單上包含全域加速器用戶端 IP 位址的所有組態，以改為包含使用者用戶端 IP 位址。

用戶端 IP 地址保留僅在特定 AWS 區域中提供。如需詳細資訊，請參閱 用戶端 IP 位址保留的支援 AWS 區域。

本節說明如何在 AWS Global Accelerator 主控台上使用端點群組。如果您想要使用 API 作業搭配使用，請參閱AWS Global Accelerator API 參考。

將少量流量移至具有用戶端 IP 位址保留的新端點之後，請測試以確定您的組態正常運作。然後透過調整對應端點上的權重，逐漸增加到新端點的流量比例。

若要轉換至保留用戶端 IP 位址的端點，請按照此處的步驟新增新端點，並針對面向網際網路的 Application Load Balancer 端點啟用用戶端 IP 位址保留。(一律為內部應用程式負載平衡器和 EC2 執行個體選取用戶端 IP 位址保留選項)。

新增具有用戶端 IP 位址保留的端點

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式區段中，選擇偵聽程式。
4. 在 中端點群組一節中，選擇端點群組。
5. 在 中端點區段中，選擇新增端點。
6. 在新增端點頁面的端點下拉式清單中，選擇 Application Load Balancer 端點或 EC2 執行個體端點。
7. 在 中Weight (粗細)欄位中，選擇與為現有端點設定的權重相比較低的數字。例如，如果對應 Application Load Balancer 的權重為 255，您可以為新的 Application Load Balancer 輸入 5 的權重，以開始。如需詳細資訊，請參閱 端點權重。
8. 對於面向外部的新 Application Load Balancer 端點，請在保留用戶端 IP 地址，選取保留地址。(一律針對內部應用程式負載平衡器和 EC2 執行個體選取此選項)。
9. 選擇 Save changes (儲存變更)。

接下來，請依照此處的步驟編輯對應的現有端點 (您要以用戶端 IP 位址保留取代新端點)，以減少現有端點的權重，以減少傳送到端點的流量。

減少現有端點的流量

1. 在端點群組頁面上，選擇沒有用戶端 IP 位址保留的現有端點。
2. 選擇 Edit (編輯)。
3. 在編輯端點頁面的Weight (粗細)欄位中，輸入比目前數字小的數字。例如，如果現有端點的權重為 255，則您可以為新端點輸入 220 的權重 (使用用戶端 IP 位址保留)。
4. 選擇 Save changes (儲存變更)。

將新端點的權重設定為較低的數字，以測試原始流量的一小部分之後，您可以繼續調整原始和新端點的權重，以慢慢轉換所有流量。

例如，假設您從權重設為 200 的現有 Application Load Balancer 開始，然後新增一個新的 Application Load Balancer 端點，並啟用用戶端 IP 位址保留，權重設為 5。透過增加新 Application Load Balancer 的權重，並減少原始 Application Load Balancer 的權重，逐漸將流量從原始 Application Load Balancer 移至新的 Application Load Balancer。例如：

- 原始重量 190/新重量 10
- 原始重量 180 /新重量 20
- 原始重量 170/ 新重量 30，等等。

當您將原始端點的權重降低為 0 時，所有流量 (在此範例案例中) 都會移至新的 Application Load Balancer 端點，其中包括用戶端 IP 位址保留。

如果您有其他要轉換為使用用戶端 IP 位址保留的端點 (應用程式負載平衡器或 EC2 執行個體)，請重複本節中的步驟來轉換它們。

如果您需要恢復端點的配置，以便端點的流量不會保留客戶端 IP 地址，則可以隨時執行此操作：增加非將用戶端 IP 位址保留為原始值，並降低端點的權重取代為用戶端 IP 位址保留設定為 0。

使用 AWS Global Accelerator 中的自訂路由加速器

本章包含在 AWS Global Accelerator 中建立自訂路由加速器的程序和建議。自訂路由加速器可讓您使用應用程式邏輯，將一個或多個使用者直接對應到許多目的地之間的特定 Amazon EC2 執行個體，同時獲得透過全球加速器路由流量的效能提升。當您有一個應用程式需要使用者群組在特定 EC2 執行個體和連接埠上執行的相同工作階段 (例如遊戲應用程式或 Voice over IP (VoIP) 工作階段) 上彼此互動時，此功能非常有用。

自訂路由加速器的端點必須是虛擬私有雲 (VPC) 子網路，而自訂路由加速器只能將流量路由到這些子網路中的 Amazon EC2 執行個體。建立自訂路由加速器時，您可以包含在單一或多個 VPC 子網路中執行的數千個 Amazon EC2 執行個體。如需進一步了解，請參閱自訂路由加速器如何在 AWS Global Accelerator 中運作。

如果您要「全域加速器」自動選擇最接近用戶端的狀況良好端點，請建立標準加速器。如需詳細資訊，請參閱 使用 AWS Global Accelerator 中的標準加速器。

要設定自訂路由加速器，請執行以下項目：

1. 檢閱建立自訂路由加速器的準則和需求。請參閱「自訂路由加速器的指導方針和限制」。
2. 建立 VPC 子網路。將子網路新增至全域加速器後，您可以隨時將 EC2 執行個體新增至子網路。
3. 建立加速器，然後選取自訂路由加速器的選項。
4. 新增接聽程式，並指定「全域加速器」要監聽的連接埠範圍。請確定您包含大範圍，且具有足夠的連接埠供全域加速器對應至您預期擁有的所有目的地。這些連接埠與您在下一個步驟中指定的目的地連接埠不同。如需接聽程式連接埠需求的詳細資訊，請參閱自訂路由加速器的指導方針和限制。
5. 為您擁有 VPC 子網路的 AWS 區域新增一或多個端點群組。您可以為每個端點群組指定下列項目：
   - 端點連接埠範圍，代表目的地 EC2 執行個體上能夠接收流量的連接埠。
   - 每個目的地連接埠範圍的通訊協定：UDP、TCP 或同時使用 UDP 和 TCP。
6. 針對端點子網路，選取子網路識別碼。您可以在每個端點群組中新增多個子網路，而子網路可以是不同的大小 (最多 /17)。

下列各節將逐步解說使用自訂路由加速器、接聽程式、端點群組和端點。

主題

- AWS Global Accelerator 中的自訂路由加速器
- AWS Global Accelerator 中自訂路由加速器的偵聽程式
- AWS Global Accelerator 中用於自訂路由加速器的端點群組
- 適用於 AWS Global Accelerator 中自訂路由加速器的 VPC 子網路終端節點

自訂路由加速器如何在 AWS Global Accelerator 中運作

透過在 AWS Global Accelerator 中使用自訂路由加速器，您可以使用應用程式邏輯，將一個或多個使用者直接對應到多個目的地之間的特定目的地，同時還能獲得全球加速器的效能優勢。自訂路由加速器會將接聽程式連接埠範圍對應至虛擬私有雲 (VPC) 子網路中的 EC2 執行個體目的地。這可讓全球加速器確定性地將流量路由到子網路中的特定 Amazon EC2 私有 IP 位址和連接埠目的地。

例如，您可以將自訂路由加速器搭配線上即時遊戲應用程式使用，您可以根據您選擇的因素 (例如地理位置、玩家技能和遊戲模式)，將多位玩家指派給 Amazon EC2 遊戲伺服器上的單一工作階段。或者，您可能會使用 VoIP 或社交媒體應用程式，將多位使用者指派給特定媒體伺服器，以進行語音、視訊和訊息工作階段。

您的應用程式可以呼叫全域加速器 API，並接收全域加速器連接埠及其相關聯的目的地 IP 位址和連接埠的完整靜態對應。您可以保存該靜態映射，然後您的配對服務使用它將用戶路由到特定的目的地 EC2 執行個體。您不用對用戶端軟體進行任何修改，即可開始使用 Global Accelerator。

若要設定自訂路由加速器，請選取 VPC 子網路端點。然後，您可以定義要對應傳入連線的目的地連接埠範圍，以便您的軟體可以在所有執行個體上偵聽相同的連接埠集。全域加速器會建立靜態對應，讓配對服務能夠將工作階段的目的地 IP 位址和連接埠號碼轉譯為您提供給使用者的外部 IP 位址和連接埠。

應用程式的網路堆疊可能會透過單一傳輸通訊協定來運作，或者您可能會使用 UDP 來快速傳遞，而 TCP 可靠傳遞。您可以為每個目的地連接埠範圍設定 UDP、TCP 或 UDP 和 TCP，以提供最大的彈性，而不必為每個通訊協定複製設定。

> **Note**
>
> 根據預設，自訂路由加速器中的所有 VPC 子網路目的地不允許接收流量。默認情況下，這是安全的，並且還可以讓您精細控制子網中允許哪些私有 EC2 實例目的地接收流量。您可以允許或拒絕傳輸到子網路，或特定 IP 位址和連接埠組合 (目的地通訊端)。如需詳細資訊，請參閱新增、編輯或移除 VPC 子網路端點。您也可以使用全域加速器 API 來指定目的地。如需詳細資訊，請參閱「」允許自訂路由流量和拒絕自訂路由流量。

自訂路由如何在全域加速器中運作的範例

舉例來說，假設您想要支援 10,000 個工作階段，讓使用者群組在全球加速器後方 1,000 個 Amazon EC2 執行個體之間互動，例如遊戲工作階段或 VoIP 通話工作階段。在此範例中，我們將指定 10001—20040 的接聽程式連接埠範圍，以及 81—90 的目的地連接埠範圍。我們會說，我們在東 1 中有四個 VPC 子網：子網-1，子網-2，子網 3 和子網 4。

在我們的範例配置中，每個 VPC 子網路的區塊大小為 /24，因此可以支援 251 個 Amazon EC2 執行個體。五個位址會保留且無法從每個子網路中使用，而且這些位址不會對應)。在每個 EC2 執行個體上執行的每個伺服器都提供以下 10 個連接埠，我們針對端點群組中的目的地連接埠指定：81-90 這意味著我們有 2510 個與每個子網相關聯的端口（ 10 x 251 ）。每個連接埠都可以與工作階段相關聯。

因為我們已在子網路中的每個 EC2 執行個體上指定了 10 個目的地連接埠，所以全域加速器會在內部將它們與 10 個接聽程式連接埠相關聯，您可以用來存取 EC2 執行個體。為了簡單地說明這一點，我們將說有一個接聽程式連接埠區塊，其開頭是第一組 10 的端點子網路的第一個 IP 位址，然後移至下一組 10 個接聽程式連接埠的下一個 IP 位址。

> **Note**
>
> 映射實際上是不可預測的，但我們在這裡使用順序映射來幫助顯示端口映射的工作原理。若要判斷接聽程式連接埠範圍的實際對應，請使用下列 API 作業：列出自訂路由連接埠對應和依目的地列出自訂路由連接埠對應。

在我們的範例中，第一個接聽程式連接埠是 10001。該連接埠與第一個子網路 IP 位址 192.0.2.4 和第一個 EC2 連接埠 81 相關聯。下一個接聽程式連接埠 10002 與第一個子網路 IP 位址 192.0.2.4 和第二個 EC2 連接埠 82 相關聯。下表說明此範例對應如何繼續執行第一個 VPC 子網路的最後一個 IP 位址，然後繼續執行至第二個 VPC 子網路的第一個 IP 位址。

Global Accelerator	VPC 子網路	EC2 執行個體連接埠
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84

Global Accelerator	VPC 子網路	EC2 執行個體連接埠
10005	192.0.2.4	85
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83

Global Accelerator	VPC 子網路	EC2 執行個體連接埠
12504	192.0.2.244	84
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89
12520	192.0.3.4	90

自訂路由加速器的指導方針和限制

在 AWS Global Accelerator 中建立和使用自訂路由加速器時，請牢記下列準則和限制。

Amazon EC2 執行個體目標

自訂路由加速器中的虛擬公用雲端 (VPC) 子網路端點只能包含 EC2 執行個體。自訂路由加速器不支援其他資源，例如負載平衡器。

全域加速器支援的 EC2 執行個體類型列於AWS Global Accelerator 中的標準加速器終端節點。

連接埠映射

新增 VPC 子網路時，全域加速器會建立靜態連接埠對應，將接聽程式連接埠範圍與子網路支援的連接埠範圍。特定子網路的連接埠對應永遠不會變更。

您可以透過程式設計方式檢視自訂路由加速器的連接埠映射清單。如需詳細資訊，請參閱 `ListCustomRoutingPortMappings`。

VPC 子網路大小

您新增至自訂路由加速器的 VPC 子網路必須至少為 /28，且最多為 /17。

監聽連接埠範圍

您必須透過指定接聽程式連接埠範圍來指定足夠的接聽程式連接埠，以容納您計劃新增至自訂路由加速器之子網路中包含的目的地數目。建立接聽程式時所指定的範圍會決定您可以搭配自訂路由加速器使用的接聽程式連接埠和目的地 IP 位址組合數目。為了獲得最大的彈性，以及減少發生錯誤的可用接聽程式連接埠不足的可能性，我們建議您指定較大的連接埠範圍。

當您將子網路新增至自訂路由加速器時，全域加速器會在區塊中配置連接埠範圍。我們建議您以線性方式配置接聽程式連接埠範圍，並讓範圍足以支援您想要擁有的目的地連接埠數目。也就是說，您應配置的連接埠數目至少應該是子網路大小乘以子網路中將擁有的目的地連接埠和通訊協定 (目的地組態) 數目。

> **Note**
>
> 全域加速器用來配置連接埠對應的演算法，可能需要您新增更多接聽程式連接埠 (超過此總數)。

建立接聽程式之後，您可以編輯接聽程式以新增其他連接埠範圍和相關聯的通訊協定，但無法減少現有的連接埠範圍。例如，如果您的接聽程式連接埠範圍為 5,000—10,000，則無法將連接埠範圍變更為 5900—10,000，而且無法將連接埠範圍變更為 5,000—9,900。

每個接聽程式連接埠範圍必須至少包含 16 個連接埠。接聽程式支援連接埠 1-65535。

目標連接埠範圍

您可以為自訂路由加速器指定連接埠範圍的兩個位置：新增接聽程式時指定的連接埠範圍，以及為端點群組指定的目的地連接埠範圍和通訊協定。

- 接聽連接埠範圍：用戶端連線之全域加速器靜態 IP 位址上的接聽程式連接埠。全域加速器會將每個連接埠對應至加速器後方 VPC 子網路上唯一的目的地 IP 位址和連接埠。
- 目標連接埠範圍：您為端點群組 (也稱為目的地組態) 指定的目的地連接埠範圍集合是接收流量的 EC2 執行個體連接埠。若要接收目的地連接埠上的流量，與 EC2 執行個體相關聯的安全群組必須允許其上的流量。

運作 Health 檢查

全域加速器不會針對自訂路由加速器執行健全狀況檢查，也不會容錯移轉至狀況良好的端點。無論目的地資源的健全狀況為何，自訂路由加速器的流量都會決定性地路由。

預設會拒絕所有流量

根據預設，透過自訂路由加速器導向的流量會拒絕到子網路中的所有目的地。若要讓目的地執行個體接收流量，您必須特別允許子網路的所有流量，或者允許子網路中的特定執行個體 IP 位址和連接埠的流量。

更新子網路或特定目的地以允許或拒絕流量需要時間才能在網際網路上傳播。若要判斷變更是否已傳播，您可以呼叫`DescribeCustomRoutingAccelerator`API 動作來檢查加速器狀態。如需詳細資訊，請參閱「」描述樣本路由加速器。

不支援 AWS CloudFormation

自訂路由加速器不支援 AWS CloudFormation。

AWS Global Accelerator 中的自訂路由加速器

A自訂路由加速器可讓您使用自訂應用程式邏輯，將一個或多個使用者導向多個目的地之間的特定目的地，同時使用 AWS 全球網路來改善應用程式的可用性和效能。

自訂路由加速器只會將流量路由到在虛擬私有雲 (VPC) 子網路中執行的 Amazon EC2 執行個體上的連接埠。使用自訂路由加速器，全域加速器不會根據端點的地理位置或健全狀況來路由流量。如需進一步了解，請參閱自訂路由加速器如何在 AWS Global Accelerator 中運作。

當您建立加速器時，根據預設，全域加速器會提供一組兩個靜態 IP 位址。如果您將自己的 IP 地址範圍帶入 AWS (BYOIP)，則可以從自己的集區指派靜態 IP 地址，以搭配加速器使用。如需詳細資訊，請參閱 在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)。

> **Important**
>
> 只要 IP 位址存在，就會指派給加速器，即使您停用加速器且不再接受或路由流量。但是，當您delete加速器時，您會遺失指派給加速器的全域加速器靜態 IP 位址，因此您無法再使用它們來路由流量。最佳作法是確保您擁有適當的權限，以避免不小心刪除加速器。您可以使用 IAM 政策 (例如以標籤為基礎的權限搭配全域加速器) 來限制具有刪除加速器權限的使用者。如需詳細資訊，請參閱 標籤型政策。

本節說明如何在全域加速器主控台上建立、編輯或刪除自訂路由加速器。若要了解如何使用 API 作業搭配全域加速器，請參閱AWS Global Accelerator API 參考。

主題

建立或更新自訂路由加速器

建立自訂路由加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 選擇建立加速。
3. 提供加速器的名稱。
4. 適用於加速器類型中，選取自訂路由。
5. 或者，如果您已將自己的 IP 位址範圍帶入 AWS (BYOIP)，則可以從該位址集區指定加速器的靜態 IP 位址。針對加速器的兩個靜態 IP 位址中的每個位址進行此選項。
   - 針對每個靜態 IP 位址，選擇要使用的 IP 位址集區。
   - 若您選擇自己的 IP 地址集區，請從集區選擇特定的 IP 地址。如果您選擇預設的 Amazon IP 位址集區，則全域加速器會指派特定 IP 位址給您的加速器。
6. 或者，新增一或多個標籤，以利識別加速器資源。
7. 選擇下一頁移至精靈中的下一頁，以新增接聽程式、端點群組和 VPC 子網路端點。

編輯自訂路由加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在自訂路由加速器清單中，選擇其中一個，然後選擇Edit (編輯)。
3. 在編輯加速頁面上，進行任何您喜歡的變更。例如，您可以停用加速器，以便刪除加速器。
4. 選擇 Save (儲存)。

檢視您的自訂路由加速器

您可以在主控台上檢視自訂路由加速器的相關資訊。若要以程式設計方式查看自訂路由加速器的說明，請參閱列出自訂路由加速器和描述樣本路由加速器中的 AWS Global Accelerator API 參考。

若要檢視自訂路由加速器的資訊

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 若要查看加速器的詳細資訊，請選擇加速器，然後選擇檢視。

刪除自訂路由加速器

如果您已建立自訂路由加速器做為測試，或者您不再使用加速器，您可以將其刪除。請在主控台上停用加速器，然後您就可以將其刪除。您不需要從加速器移除接聽程式和端點群組。

若要使用 API 作業而非主控台來刪除自訂路由加速器，您必須先移除與加速器相關聯的所有接聽程式和端點群組，然後將其停用。如需詳細資訊，請參閱 。刪除加速器中的AWS Global Accelerator API 參考。

停用自訂路由加速

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在清單中，選擇您要停用的加速器。
3. 選擇 Edit (編輯)。
4. 選擇停用加速，然後選擇Save (儲存)。

刪除自訂路由加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在清單中，選擇您要刪除的加速器。

3. 選擇 Delete (刪除)。

> **Note**
>
> 若您尚未停用加速器，刪除無法使用。若要停用加速器，請參閱上一個程序。

4. 在確認對話方塊中，選擇 Delete (刪除)。

> **Important**
>
> 刪除加速器時，您會遺失指派給加速器的靜態 IP 位址，因此您無法再使用它們來路由流量。

AWS Global Accelerator 中自訂路由加速器的偵聽程式

對於 AWS Global Accelerator 中的自訂路由加速器，您可以設定接聽程式，指定一系列接聽程式連接埠，其中包含全球加速器映射到 VPC 子網路終端節點中的特定目標 Amazon EC2 執行個體的相關協定。新增 VPC 子網路端點時，全域加速器會在您為接聽程式定義的連接埠範圍與子網路中的目的地 IP 位址和連接埠之間建立靜態連接埠對應。然後，您可以使用連接埠對應來指定加速器靜態 IP 位址以及接聽程式連接埠和通訊協定，將使用者流量導向至 VPC 子網路中的特定目標 Amazon EC2 執行個體 IP 位址和連接埠。

當您在立自訂路由加速器時便定義接聽程式，然後可隨時新增更多接聽程式。每個接聽程式可以有一個或多個端點群組，每個具有 VPC 子網路端點的 AWS 區域都有一個。自訂路由加速器中的接聽程式支援 TCP 和 UDP 通訊協定。您可以為定義的每個目的地連接埠範圍指定通訊協定：UDP、TCP 或同時使用 UDP 和 TCP。

如需詳細資訊，請參閱 自訂路由加速器如何在 AWS Global Accelerator 中運作。

新增、編輯或移除自訂路由接聽程式

本節說明如何在 AWS Global Accelerator 主控台上使用自訂路由接聽程式。若要了解如何搭配 AWS Global Accelerator 使用 API 操作，請參閱AWS Global Accelerator API 參考。

新增自訂路由加速器的接聽程式

您在建立接聽程式時指定的範圍會定義您可以搭配自訂路由加速器使用的接聽程式連接埠和目的地 IP 位址組合數目。若要獲得最大的彈性，建議您指定較大的連接埠範圍。您指定的每個接聽程式連接埠範圍至少必須包含 16 個連接埠。

> **Note**
>
> 建立接聽程式之後，您可以編輯接聽程式以新增其他連接埠範圍和相關聯的通訊協定，但無法減少現有的連接埠範圍。

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 選擇 Add listener (新增接聽程式)。
4. 在新增接聽程式頁面上，輸入您要與加速器產生關聯的接聽程式連接埠範圍。

   接聽程式支援連接埠 1-65535。若要使用自訂路由加速器獲得最大的彈性，建議您指定大型連接埠範圍。
5. 選擇 Add listener (新增接聽程式)。

編輯自訂路由加速器的接聽程式

當您編輯自訂路由加速器的接聽程式時，請注意您可以新增其他連接埠範圍和相關聯的通訊協定、增加現有的連接埠範圍或變更通訊協定，但無法減少現有的連接埠範圍。

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 選擇接聽程式，然後選擇編輯接聽程式。
4. 在編輯接聽程式頁面上，對現有連接埠範圍或通訊協定進行變更，或新增連接埠範圍。

   請注意，您無法減少現有連接埠範圍的範圍。
5. 選擇 Save (儲存)。

移除接聽程式

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 選擇接聽程式，然後選擇Remove (移除)。
4. 在確認對話方塊中，選擇Remove (移除)。

AWS Global Accelerator 中用於自訂路由加速器的端點群組

使用 AWS Global Accelerator 中的自訂路由加速器，端點群組可定義虛擬私有雲 (VPC) 子網路中 Amazon EC2 執行個體目標接受流量的連接埠和協定。

您可以為 VPC 子網路和 EC2 執行個體所在的每個 AWS 區域建立自訂路由加速器的終端節點群組。自訂路由加速器中的每個端點群組都可以有多個 VPC 子網路端點。同樣地，您可以將每個 VPC 新增至多個端點群組，但端點群組必須與不同的接聽程式相關聯。

針對每個端點群組，您可以指定一組一或多個連接埠範圍，其中包含您要在區域中 EC2 執行個體上將流量導向的連接埠。針對每個端點群組連接埠範圍，您可以指定要使用的通訊協定：UDP、TCP 或同時使用 UDP 和 TCP。這可為您提供最大的彈性，而不必為每個通訊協定複製連接埠範圍集。例如，您可能有一個遊戲伺服器的遊戲流量透過 UDP 在連接埠 8080-8090 上執行，而您也有一個伺服器在連接埠 80 上透過 TCP 接聽聊天訊息。

如需進一步了解，請參閱自訂路由加速器如何在 AWS Global Accelerator 中運作。

新增、編輯或移除自訂路由加速器的端點群組

您可以在 AWS 全域加速器主控台上使用自訂路由加速器的端點群組，或使用 API 作業。您可以隨時從端點群組新增或移除 VPC 子網路端點。

本節說明如何在 AWS 全域加速器主控台上使用自訂路由加速器的端點群組。若要了解如何使用 API 作業搭配全域加速器，請參閱AWS Global Accelerator API 參考。

新增端點群組以供自訂路由加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式區段, 用於接聽程式 ID下，選擇您要為其新增端點群組的接聽程式 ID。
4. 選擇新增端點群組。
5. 在監聽器的段落中，指定端點群組的「區域」。
6. 適用於連接埠和協定集中，輸入 Amazon EC2 執行個體的連接埠範圍和通訊協定。
   - 輸入從連接埠和移植指定一個範圍內的連接埠。
   - 針對每個連接埠範圍，指定該範圍的通訊協定。

連接埠範圍不一定是接聽程式連接埠範圍的子集，但接聽程式連接埠範圍中必須有足夠的連接埠總數，才能支援您為自訂路由加速器中的端點群組指定的連接埠總數。

7. 選擇 Save (儲存)。
8. 選擇性地選擇新增端點群組為此接聽程式新增其他端點群組。您也可以選擇其他接聽程式並新增端點群組。
9. 選擇新增端點群組。

編輯自訂路由加速器的端點群組

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式區段, 用於接聽程式 ID下，選擇與端點群組關聯之接聽程式 ID。
4. 選擇編輯端點群組。
5. 在編輯端點群組頁面上，變更區域、連接埠範圍或某個連接埠範圍的通訊協定。
6. 選擇 Save (儲存)。

移除自訂路由加速器

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇加速器。
3. 在 中接聽程式區段中，選擇接聽程式，然後選擇Remove (移除)。
4. 在 中端點群組區段中，選擇端點群組，然後選擇Remove (移除)。
5. 在確認對話方塊上，選擇Remove (移除)。

適用於 AWS Global Accelerator 中自訂路由加速器的 VPC 子網路終端節點

自訂路由加速器的端點是虛擬私有雲 (VPC) 子網路，可透過加速器接收流量。每個子網路可以包含一個或多個 Amazon EC2 執行個體目標。當您新增子網路端點時，全域加速器會產生新的連接埠對應。然後，您可以使用全域加速器 API 取得子網路之所有連接埠對應的靜態清單，您可以使用此清單將流量路由傳送至子網路中的目的地 EC2 執行個體 IP 位址。如需詳細資訊，請參閱「」列出自訂路由連接埠對應。

您只能將流量導向子網中的 EC2 執行個體，而不能將負載平衡器等其他資源導向 (與標準加速器相反)。支援的 EC2 執行個體類型列於AWS Global Accelerator 中的標準加速器終端節點。

如需進一步了解，請參閱自訂路由加速器如何在 AWS Global Accelerator 中運作。

當您為自訂路由加速器新增 VPC 子網路時，請注意下列事項：

- 根據預設，透過自訂路由加速器導向的流量無法抵達子網路中的任何目的地。若要讓目的地執行個體接收流量，您必須選擇允許子網路的所有流量，或者啟用子網路中特定執行個體 IP 位址和連接埠 (目的地通訊端) 的流量。

  > **Important**
  >
  > 更新子網路或特定目的地以允許或拒絕流量需要時間才能在網際網路上傳播。若要判斷變更是否已傳播，您可以呼叫`DescribeCustomRoutingAccelerator`API 動作來檢查加速器狀態。如需詳細資訊，請參閱「」描述樣本路由加速器。

- 由於 VPC 子網路會保留用戶端 IP 位址，因此當您將子網路新增為自訂路由加速器的端點時，應該檢閱相關的安全性和組態資訊。如需詳細資訊，請參閱 新增具有用戶端 IP 位址保留的端點。

新增、編輯或移除 VPC 子網路端點

您可以將虛擬私有雲 (VPC) 子網路終端節點新增到自訂路由加速器中的端點群組，以便將使用者流量導向子網路中的目的地 Amazon EC2 執行個體。

當您從子網路新增和移除 EC2 執行個體，或啟用或停用 EC2 目的地的流量時，您會變更這些目的地是否可以接收流量。不過，全域加速器連接埠對應不會變更。

若要允許傳輸到子網路中某些目的地，但不是全部，請為您要允許的每個 EC2 執行個體輸入 IP 位址，以及您要接收流量的執行個體上的連接埠。您指定的 IP 位址必須適用於子網路中的 EC2 執行個體。您可以從針對子網路對應的連接埠指定連接埠或連接埠範圍。

您可以從加速器移除 VPC 子網路，方法是從端點群組中移除該子網路。移除子網路不會影響子網路本身，但全域加速器無法再將流量導向到子網路或其中的 Amazon EC2 執行個體。此外，全域加速器會回收 VPC 子網路的連接埠對應，以便將它們用於您新增的新子網路。

本節中的步驟說明如何在 AWS 全域加速器主控台上新增、編輯或移除 VPC 子網路終端節點。若要了解如何搭配 AWS Global Accelerator 使用 API 操作，請參閱AWS Global Accelerator API 參考。

新增 VPC 子網路端點

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組部分，用於端點 ID下，選擇您要新增 VPC 子網路終端節點的終端節點群組 (AWS 區域) 識別碼。
5. 在 中端點區段中，選擇新增端點。
6. 在新增端點頁面上的端點下，選擇 VPC 子網路。

   如果您沒有任何 VPC，清單中沒有任何項目。若要繼續，請至少新增一個 VPC，然後回到此處的步驟，並從清單中選擇一個 VPC。
7. 對於您新增的 VPC 子網路端點，您可以選擇允許或拒絕子網路中所有目的地的流量，或者只允許特定 EC2 執行個體和連接埠的流量。預設為拒絕子網路中所有目的地的流量。
8. 選擇 Add endpoint (新增端點)。

允許或拒絕特定目的地的流量

您可以編輯端點的 VPC 子網路連接埠對應，以允許或拒絕子網路中特定 EC2 執行個體和連接埠 (目的地通訊端) 的流量。

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組部分，用於端點 ID下，選擇要編輯之 VPC 子網路端點的端點群組 (AWS 區域) 的識別碼。
5. 選擇端點子網路，然後選擇View details (檢視詳細資訊)。
6. 在端點頁面，在連接埠映射、選擇 IP 位址，然後選擇Edit (編輯)。
7. 輸入您想要啟用流量的連接埠，然後選擇允許這些目標。

允許或拒絕子網路的所有流量

您可以更新端點，以允許或拒絕 VPC 子網路中所有目的地的流量。

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。

2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組部分，用於端點 ID下，選擇要更新之 VPC 子網路端點的端點群組 (AWS 區域) 的識別碼。
5. 選擇允許/拒絕所有流量。
6. 選擇一個選項，允許所有流量或拒絕所有流量，然後選擇Save (儲存)。

移除端點

1. 開啟全域加速器主控台，網址為https://console.aws.amazon.com/globalaccelerator/home。
2. 在加速器頁面上，選擇自訂路由加速器。
3. 在 中接聽程式部分，用於接聽程式 ID下，選擇接聽程式的識別碼。
4. 在 中端點群組部分，用於端點 ID中，選擇要移除之 VPC 子網路端點的端點群組 (AWS 區域) 識別碼。
5. 選擇移除端點。
6. 在確認對話方塊中，選擇Remove (移除)。

AWS Global Accelerator 中的 DNS 定址和自訂網域

本章說明 AWS Global Accelerator 如何進行 DNS 路由，並包括使用具有全域加速器的自訂網域的相關資訊。

主題

Support 全域加速器中的 DNS 定址

當您建立自訂路由或標準加速器時，全域加速器會為您佈建兩個靜態 IP 位址。別名稱系統 (DNS) 名稱也會指派預設的加速器，類似`a1234567890abcdef.awsglobalaccelerator.com`，指向靜態 IP 位址。靜態 IP 位址會使用從 AWS 邊緣網路到終端節點的任何廣播進行全球廣告。您可以使用加速器的靜態 IP 位址或 DNS 名稱，將流量路由傳送至加速器。DNS 伺服器和 DNS 解析器使用循環配置資源來解析加速器的 DNS 名稱，因此該名稱會解析為加速器的靜態 IP 位址 (由 Amazon Route 53 以隨機順序傳回)。用戶端通常會使用傳回的第一個 IP 位址。

> **Note**
>
> 全域加速器會建立兩個指標 (PTR) 記錄，將加速器的靜態 IP 位址對應至全域加速器所產生的對應 DNS 名稱，以支援反向 DNS 查閱。這就是所謂的反向託管區域。請注意，全域加速器為您產生的 DNS 名稱無法設定，而且您無法建立指向自訂網域名稱的 PTR 記錄。全域加速器也不會為您帶到 AWS (BYOIP) 的 IP 位址範圍內的靜態 IP 位址建立 PTR 記錄。

將自訂網域流量路由至您的加速器

在大多數情況下，您可以將 DNS 設定為使用自訂網域名稱 (例如`www.example.com`)，而不是使用指派的靜態 IP 位址或預設 DNS 名稱。首先，使用 Amazon Route 53 或其他 DNS 供應商建立網域名稱，然後使用您的全域加速器 IP 位址新增或更新 DNS 記錄。或者，您可以將自訂網域名稱與加速器的 DNS 名稱建立關聯。完成 DNS 設定，並等待變更透過網際網路傳播。現在當用戶端使用您的自訂網域名稱發出請求時，DNS 伺服器為您的加速器解析 DNS 名稱。

當您使用 Route 53 做為 DNS 服務時，若要將自訂網域名稱與全域加速器搭配使用，您可以建立別名記錄，將自訂網域名稱指向指派給加速器的 DNS 名稱。別名記錄是 DNS 的 Route 53 延伸。別名記錄與 CNAME 記錄類似，但您可以同時為根網域 (如`example.com`，以及子網域 (例如`www.example.com`。如需詳細資訊，請參閱「」選擇別名或非別名記錄Amazon Route 53 開發人員指南中。

若要使用加速器的別名記錄來設定 Route 53，請遵循下列主題中包含的指導：別名目標Amazon Route 53 開發人員指南中。若要查看全域加速器的資訊，請向下捲動別名目標(憑證已建立！) 頁面上的名稱有些許差異。

在 AWS Global Accelerator 中使用自有 IP 地址 (BYOIP)

AWS Global Accelerator 使用靜態 IP 地址作為加速器的進入點。這些 IP 地址是來自 AWS 節點的任何廣播。根據預設，全域加速器會提供來自亞馬遜 IP 地址池。您可以將這些進入點設定為來自您自己位址範圍的 IPv4 位址，而不是使用全域加速器所提供的 IP 位址。此主題說明如何使用您自己的 IP 位址範圍與全域加速器使用。

您可以將現場部署網路的一部分或全部公有 IPv4 地址範圍用於您的 AWS 帳戶，以便搭配全球加速器使用。您仍擁有自己的位址範圍，但 AWS 會在網際網路上公告。

您無法將帶到 AWS 的 IP 位址用於一個 AWS 服務與另一個服務搭配使用。此章節中的步驟說明如何使用您自己的 IP 位址範圍僅供在 AWS Global Accelerator 中使用。如需將您自己的 IP 地址範圍用於 Amazon EC2 中的步驟，請參閱使用自有 IP 地址 (BYOIP)《Amazon EC2 使用者指南》中的 Requests。

> **Important**
>
> 您必須停止從其他位置公告您的 IP 地址範圍，之後再透過 AWS 進行公告。如果 IP 位址範圍是多重主目錄 (也就是說，該範圍是由多個服務供應商同時通告)，我們無法保證該位址範圍的流量會進入我們的網路，或者您的 BYOIP 廣告工作流程會順利完成。

在您將地址範圍用於 AWS 之後，該地址範圍就會顯示為您帳戶的地址集區。當您建立加速器時，您可以從範圍指派一個 IP 位址給它。全球加速器會從 Amazon IP 位址範圍中指派第二個靜態 IP 位址。如果您將兩個 IP 位址範圍帶入 AWS，則可以將每個範圍的一個 IP 位址指派給加速器。此限制是因為「全域加速器」會將每個位址範圍指派給不同的網路區域，以達到高可用性。

若要使用您自己的 IP 位址範圍搭配全域加速器，請檢閱需求，然後遵循本主題中提供的步驟。

主題

Requirements

每個 AWS 帳戶最多可以將兩個合格的 IP 地址範圍帶到 AWS Global Accelerator。

若要符合資格，您的 IP 地址範圍必須符合下列要求：

- IP 地址範圍必須向下列區域網際網路註冊管理機構 (RIR) 註冊：美洲網際網路號碼註冊管理機構 (ARIN) 或歐洲 IP 網路資源協調中心 (RIPE) 或亞太區域資訊中心 (APNIC)。地址範圍必須以商業或機構實體註冊。它無法以個人身分註冊。
- 您可以使用的最明確地址範圍是 /24。IP 位址的前 24 位元會指定網路號碼。例如，198.51.100 是 IP 地址 198.51.100.0 的網路號碼。
- IP 地址範圍中的 IP 地址都必須有良好的歷史記錄。也就是說，他們不能有不良的聲譽或與惡意行為相關聯。如果我們調查 IP 位址範圍的評價，並發現 IP 位址範圍包含的 IP 位址沒有完全記錄的 IP 位址記錄，我們保留拒絕該範圍的權利。

此外，根據您註冊 IP 位址範圍的位置，我們還需要下列分配和指派網路類型或狀態：

- 阿林：`Direct Allocation`和`Direct Assignment`網路類型
- 成熟：`ALLOCATED PA`、`LEGACY`，以及`ASSIGNED PI`配置狀態
- 自用：`ALLOCATED PORTABLE`和`ASSIGNED PORTABLE`配置狀態

準備將 IP 地址範圍用於 AWS 帳戶：授權

為了確保只有您可以將您的 IP 地址空間帶到 Amazon，我們需要兩個授權：

- 您必須授權亞馬遜宣傳 IP 地址範圍。

- 您必須提供您擁有 IP 位址範圍的證明，因此有權將 IP 位址帶到 AWS。

> **Note**
>
> 當您使用 BYOIP 將 IP 位址範圍帶入 AWS 時，在我們進行廣告時，您無法將該位址範圍的擁有權轉移到其他帳戶或公司。您也無法將 IP 位址範圍從一個 AWS 帳戶直接傳輸到另一個帳戶。若要在 AWS 帳戶之間轉移擁有權或轉移，您必須取消佈建位址範圍，然後新擁有者必須遵循步驟將位址範圍新增至其 AWS 帳戶。

要授權亞馬遜宣傳 IP 地址範圍，您可以向亞馬遜提供一個簽名的授權消息。使用路由來源授權 (ROA) 來提供此授權。ROA 是關於您透過區域網際網路註冊管理機構 (RIR) 建立的路由公告的密碼編譯陳述式。ROA 包含 IP 地址範圍、允許公告 IP 地址範圍的自發系統號碼 (ASN) 和過期日期。ROA 授權 Amazon 公告特定自發系統（AS）下的 IP 地址範圍。

ROA 不會授權您的 AWS 帳戶將 IP 地址範圍用於 AWS。若要提供此授權，您必須發佈自簽 X.509 憑證中的 IP 位址範圍的註冊資料存取通訊協定 (RDAP) 備註中。該憑證包含公有金鑰，可讓 AWS 用來驗證您提供的授權內容簽章。保護私有金鑰的安全，並使用它來簽署授權內容的訊息。

以下各節提供完成這些授權任務的詳細步驟。Linux 支援這些步驟中的命令。如果您使用 Windows，則可以存取適用於 Linux 的 Windows 子系統來執行 Linux 命令。

提供授權的步驟

- 步驟 1：建立 ROA 物件
- 步驟 2：建立自簽 X.509 憑證
- 步驟 3：建立已簽署的授權訊息

步驟 1：建立 ROA 物件

建立 ROA 物件來授權 Amazon ASN 16509 宣傳您的 IP 地址範圍，以及目前獲授權宣傳 IP 地址範圍的 ASN。ROA 必須包含您要 AWS 用的 /24 IP 位址，且您必須設定最大長度上限為 /24。

如需有關建立 ROA 要求的詳細資訊，請參閱下列章節，視您註冊 IP 位址範圍的位置而定：

- 阿林：ROA Requests
- 成熟：管理 ROA
- 自用：路由管理

步驟 2：建立自簽 X.509 憑證

建立 key pair 和自我簽署的 X.509 憑證，並將憑證加入到您 RIR 的 RDAP 記錄中。下列步驟說明如何執行這些任務。

> **Note**
>
> 所以此`openssl`命令需要 OpenSSL 1.0.2 版或更新版本。

建立和新增 X.509 憑證

1. 使用下列命令產生 RSA 2048 位元 key pair。

   ```
   openssl genrsa -out private.key 2048
   ```

2. 使用下列命令，從 key pair 中建立公開 X.509 憑證。

   ```
   openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
   ```

   在此範例中，憑證會在 365 天後過期；在這段時間之後，就無法再信任此憑證。當您執行命令時，請確定您將`-days`選項設定為所需的值，以便正確的到期日。當提示您輸入其他資訊時，您可以接受預設值。

3. 使用下列步驟，視您的 RIR 使用下列步驟，視您的 RIR 更新 RDAP 記錄。

   1. 使用下列命令來檢視憑證。

      ```
      cat publickey.cer
      ```

   2. 執行下列動作來新增憑證：

      > **Important**
      >
      > 請務必包含`-----BEGIN CERTIFICATE-----`和`-----END CERTIFICATE-----`從憑證。

      - 若是 ARING INTO，請將憑證新增至`Public Comments`區段以瞭解 IP 地址範圍。
      - 若是 RIPE，請將憑證新增為新的`descr`欄位中的 IP 地址範圍。

- 對於 APNIC，請將公鑰電子郵件發送到helpdesk@apnic.net(IP 位址的 APNIC 授權聯絡人)，以要求他們手動將該 IP 位址的remarks欄位。

步驟 3：建立已簽署的授權訊息

創建簽名的授權消息，以允許亞馬遜宣傳您的 IP 地址範圍。

訊息的格式如下所示，其中YYYYMMDD日期是郵件的到期日。

```
1|aws|aws-account|address-range|YYYYMMDD|SHA256|RSAPSS
```

若要建立已簽署的授權訊息

1. 建立純文字的授權訊息，並將其儲存到名為的變數text_message，如下列範例所示。將範例中的帳戶號碼、IP 位址範圍和到期日用您自己的值取代。

   ```
   text_message="1|aws|123456789012|203.0.113.0/24|20191201|SHA256|RSAPSS"
   ```

2. 簽署授權訊息text_message使用您在先前一節建立的 key pair。
3. 將訊息儲存到名為的變數signed_message，如下列範例所示。

   ```
   signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt
         rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform
    PEM | openssl base64 |
         tr -- '+=/' '-_~' | tr -d "\n")
   ```

佈建地址範圍以用於 AWS Global Accelerator

當您佈建地址範圍以用於 AWS 時，即已確認您擁有該地址範圍並授權 Amazon 公告該地址範圍。我們會驗證您是否擁有自己的位址範圍。

您必須使用 CLI 或全域加速器 API 作業佈建位址範圍。此功能不適用於 AWS 主控台。

若要佈建地址範圍，請使用下列ProvisionByoipCidr指的是命令。所以此--cidr-authorization-context參數會使用您在上一節建立的變數，而非 ROA 訊息。

```
aws globalaccelerator provision-byoip-cidr --cidr address-range --cidr-authorization-
context Message="$text_message",Signature="$signed_message"
```

以下是佈建位址範圍的範例。

```
aws globalaccelerator provision-byoip-cidr
    --cidr 203.0.113.25/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

佈建地址範圍是一種非同步操作，系統會立即傳回呼叫。但是，位址範圍尚未準備好使用，直到其狀態從PENDING_PROVISIONING至READY。完成佈建程序最長需要 3 週。若要監控已佈建之地址範圍的狀態，請使用下列清單條件命令

```
aws globalaccelerator list-byoip-cidrs
```

若要查看 IP 位址範圍的狀態清單，請參閱BYOIPCDR。

佈建 IP 位址範圍時，State返回的list-byoip-cidrs是READY。例如：

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "READY"
        }
    ]
}
```

透過 AWS 公告地址範圍

佈建好地址範圍之後，即可將其公告。佈建好地址範圍之後，您必須公布。對於已經佈建好的地址範圍，您不能必須只公布一部分。此外，您必須先停止從其他位置公告您的 IP 地址範圍，之後再透過 AWS 進行公告。

您必須使用 CLI 或全域加速器 API 作業宣傳 (或停止廣告) 您的位址範圍。此功能不適用於 AWS 主控台。

> **Important**
>
> 使用來自集區的 IP 位址與全域加速器的 IP 位址之前，請確定 AWS 已通告您的 IP 位址範圍。

若要公告地址範圍，請使用下列廣告公告指的是命令。

```
aws globalaccelerator advertise-byoip-cidr --cidr address-range
```

以下是要求全域加速器通告位址範圍的範例。

```
aws globalaccelerator advertise-byoip-cidr --cidr 203.0.113.0/24
```

若要監控已公告之地址範圍的狀態，請使用下列清單條件指的是命令。

```
aws globalaccelerator list-byoip-cidrs
```

當您的 IP 位址範圍通告時，State返回的list-byoip-cidrs是ADVERTISING。例如：

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "ADVERTISING"
        }
    ]
}
```

若要停止公告地址範圍，請使用下列withdraw-byoip-cidr指的是命令。

> **Important**
>
> 若要停止廣告您的位址範圍，您必須先移除具有從位址集區配置的靜態 IP 位址的任何加速器。若要使用主控台或使用 API 作業刪除加速器，請參閱 刪除加速器。

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

以下是要求全域加速器撤銷位址範圍的範例。

```
aws globalaccelerator withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

解除佈建地址範圍

若要停止對 AWS 使用您的位址範圍，請先從位址集區移除任何具有靜態 IP 位址的加速器，並停止公告您的位址範圍。完成這些步驟之後，您可以取消佈建位址範圍。

您必須使用 CLI 或全域加速器 API 作業停止廣告並取消佈建位址範圍。此功能不適用於 AWS 主控台。

步驟 1：刪除任何關聯的加速器。若要使用主控台或使用 API 作業刪除加速器，請參閱 刪除加速器。

步驟 2. 停止公告地址範圍。若要停止公告該範圍，請使用下列提款智能手機指的是命令。

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

步驟 3. 解除佈建地址範圍。若要取消佈建範圍，請使用下列取消規定的條件指的是命令。

```
aws globalaccelerator deprovision-byoip-cidr --cidr address-range
```

使用您的 IP 位址建立加速器

現在，您可以使用您的 IP 位址建立加速器。如果您將一個位址範圍帶入 AWS，則可以為加速器指派一個 IP 位址。如果您有兩個位址範圍，您可以從每個位址範圍指派一個 IP 位址給加速器。

您可以使用自己的 IP 位址來建立加速器的靜態 IP 位址：

- 使用全域加速器主控台建立加速器。 如需更多詳細資訊，請參閱 建立或更新標準加速器 及 建立或更新自訂路由加速器。
- 使用全域加速器 API 建立加速器。 如需詳細資訊，包括使用 CLI 的範例，請參閱建立加速器和建立自訂路由加速器《AWS Global Accelerator API 參考》中的 Requests。

在 AWS Global Accelerator 中保留用戶端 IP 地址

保留和存取 AWS Global Accelerator 用戶端 IP 位址的選項取決於您使用加速器設定的終端節點。有兩種類型的端點可以在傳入封包中保留用戶端的來源 IP 位址：應用程式負載平衡器和 Amazon EC2 執行個體。

- 當您使用面向網際網路的 Application Load Balancer 做為具有全域加速器的端點時，新加速器預設會啟用用戶端 IP 位址保留功能。這表示到達負載平衡器的封包會保留原始用戶端的來源 IP 位址。您可以選擇在建立加速器或稍後編輯加速器時停用此選項。
- 當您使用內部 Application Load Balancer 或搭配全域加速器的 EC2 執行個體時，端點一律會啟用用戶端 IP 位址保留。

> **Note**
>
> 全域加速器不支援 Network Load Balancer 和彈性 IP 位址端點的用戶端 IP 位址保留。

當您計劃新增用戶端 IP 地址保留時，請注意下列事項：

- 在新增並開始將流量路由傳送至保留用戶端 IP 位址的端點之前，請確定已更新所有必要的安全性設定 (例如安全性群組)，以便在允許清單中包含使用者用戶端 IP 位址。
- 僅在特定 AWS 區域支援用戶端 IP 位址保留。如需詳細資訊，請參閱 用戶端 IP 位址保留的支援 AWS 區域。

主題

如何啟用用戶端 IP 位址保留

當您建立新的加速器時，依預設會針對支援的端點啟用用戶端 IP 位址保留。

請注意以下事項：

- 內部應用程式負載平衡器和 EC2 執行個體一律啟用用戶端 IP 位址保留。您無法停用這些端點的選項。
- 當您使用 AWS 主控台建立新的加速器時，Application Load Balancer 端點預設會啟用用戶端 IP 位址保留選項。如果您不想保留面向網際網路的 Application Load Balancer 端點的用戶端 IP 位址，您可以隨時停用此選項。
- 當您使用 AWS CLI 或 API 動作建立新的加速器，但未指定用戶端 IP 位址保留選項時，面向網際網路的 Application Load Balancer 端點預設會啟用用戶端 IP 位址保留。
- 全域加速器不支援 Network Load Balancer 和彈性 IP 位址端點的用戶端 IP 位址保留。

對於現有的加速器，您可以將不保留用戶端 IP 位址的端點轉換至保留用戶端 IP 位址的端點。現有的 Application Load Balancer 端點可以轉換至新的 Application Load Balancer 端點，而現有的彈性 IP 位址端點可以轉換至 EC2 執行個體端點。Network Load Balancer 端點不支援用戶端 IP 位址保留。) 若要轉換至新端點，建議您執行下列動作，將流量從現有端點緩慢移至具有用戶端 IP 位址保留的新端點：

- 對於現有的 Application Load Balancer 端點，請先將重複的 Application Load Balancer 端點新增至全域加速器，並且如果它是面向網際網路的 Application Load Balancer，則為其啟用用戶端 IP 位址保留。然後調整端點上的權重，以慢慢地從負載平衡器移動流量非已啟用負載平衡器的用戶端 IP 位址保留取代為用戶端 IP 地址保留。
- 對於現有的彈性 IP 位址端點，您可以將流量移至具有用戶端 IP 位址保留的 EC2 執行個體端點。首先將 EC2 執行個體端點新增至全域加速器，然後調整端點上的權重，以慢慢將流量從彈性 IP 位址端點移至 EC2 執行個體端點。

如需逐步轉換指引，請參閱 轉換端點以使用用戶端 IP 位址保留。

用戶端 IP 地址保留的好處

對於未啟用用戶端 IP 位址保留的端點，邊緣網路上的全域加速器服務所使用的 IP 位址會取代要求使用者的 IP 位址，做為抵達封包中的來源位址。當流量傳送到加速器後方的系統時，不會保留原始用戶端的連線資訊 (例如用戶端的 IP 位址和用戶端的連接埠)。這適用於許多應用程序，特別是那些可供所有用戶使用的應用程序，如公共網站。

不過，對於其他應用程式，您可能想要使用具有用戶端 IP 位址保留的端點來存取原始用戶端 IP 位址。例如，當您擁有用戶端 IP 位址時，您可以根據用戶端 IP 位址收集統計資料。您也可以使用 IP 位址型

篩選器，例如應用程式負載平衡器上的安全性群組來篩選流量。您可以在 Application Load Balancer 端點後面的 Web 層伺服器上執行的應用程式中，套用特定於使用者 IP 位址的邏輯，方法是使用負載平衡器的X-Forwarded-For標頭，其中包含原始的用戶端 IP 位址資訊。您也可以在與 Application Load Balancer 相關聯的安全性群組中的安全性群組規則中使用用戶端 IP 位址保留。如需詳細資訊，請參閱 如何在 AWS Global Accelerator 中保留用戶端 IP 位址。對於 EC2 執行個體端點，會保留原始用戶端 IP 位址。

對於沒有用戶端 IP 位址保留的端點，您可以篩選全域加速器在從 Edge 轉送流量時所使用的來源 IP 位址。您可以檢閱全域加速器流程記錄檔，以查看傳入封包的來源 IP 位址 (也就是啟用用戶端 IP 位址保留時的用戶端 IP 位址) 相關資訊。如需更多詳細資訊，請參閱 Global Accelerator 節點伺服器的位置和 IP 地址範圍 及 AWS Global Accelerator 中的流程日誌。

如何在 AWS Global Accelerator 中保留用戶端 IP 位址

對於 Amazon EC2 執行個體和應用程式負載平衡器，AWS Global Accelerator 會以不同方式保留用戶端的來源 IP 地址：

- 對於 EC2 執行個體端點，會針對所有流量保留用戶端的 IP 位址。
- 對於具有用戶端 IP 位址保留的 Application Load Balancer 端點，全域加速器會與 Application Load Balancer 搭配使用，以提供X-Forwarded標頭，X-Forwarded-For，其中包括原始用戶端的 IP 位址，以便您的 Web 層可以存取它。

HTTP 請求和 HTTP 回應使用標頭欄位來傳送有關 HTTP 訊息的資訊。標頭欄位是以冒號分隔的名稱值組，以歸位字元 (CR) 和換行 (LF) 分隔。一組以 RFC 2616 定義的標準 HTTP 標頭欄位，訊息標頭。也有應用程式廣泛採用的非標準 HTTP 標頭可用。有些非標準 HTTP 標頭具有X-Forwardedprefix.

由於 Application Load Balancer 會終止傳入的 TCP 連線，並建立到後端目標的新連線，因此不會將用戶端 IP 位址一直保留到目標程式碼 (例如執行個體、容器或 Lambda 程式碼)。您的目標在 TCP 封包中看到的來源 IP 位址是 Application Load Balancer 的 IP 位址。不過，Application Load Balancer 會保留原始用戶端 IP 位址，方法是將其從原始封包的回覆位址中移除，並將其插入 HTTP 標頭，然後再透過新的 TCP 連線將要求傳送到後端。

所以此X-Forwarded-For請求標頭的格式如下所示：

```
X-Forwarded-For: client-ip-address
```

以下範例顯示X-Forwarded-For要求標頭，具有 203.0.113.7 IP 地址的用戶端。

```
X-Forwarded-For: 203.0.113.7
```

用戶端 IP 位址保留的最佳作法

當您在 AWS Global Accelerator 中使用用戶端 IP 位址保留時，請記住本節中針對彈性網路介面和安全群組的資訊和最佳實務。

為了支援用戶端 IP 位址保留，全球加速器會在您的 AWS 帳戶中建立彈性網路介面，每個有端點的子網路都有一個。彈性網路界面是代表虛擬網路卡之 VPC 中的邏輯網路元件。全域加速器會使用這些彈性網路介面，將流量路由傳送至加速器後方設定的端點。用於以這種方式路由流量的支援端點為應用程式負載平衡器 (內部和網際網路面向) 和 Amazon EC2 執行個體。

> **Note**
>
> 當您在全域加速器中新增內部 Application Load Balancer 或 EC2 執行個體端點時，可以透過將網際網路流量鎖定在私有子網路中，讓網際網路流量直接進出虛擬私有雲 (VPC) 中的端點。如需詳細資訊，請參閱 AWS Global Accelerator 中的安全 VPC 連線。

全域加速器如何使用彈性網路介面

當您啟用用戶端 IP 位址保留的 Application Load Balancer 時，負載平衡器所在的子網路數目會決定全域加速器在您的帳戶中建立的彈性網路介面數目。全域加速器為每個子網路建立一個 elastic network interface，該子網路中至少有一個 Application Load Balancer elastic network interface，該介面由您帳戶中的加速器開始。

下列範例說明其如何運作：

- 範例 1：如果 Application Load Balancer 在子網路 A 和子網路 B 中具有彈性網路介面，然後將負載平衡器新增為加速器端點，則全域加速器會在每個子網路中建立兩個彈性網路介面。
- 範例 2：例如，如果您將子網路 A 和子網路 B 中具有彈性網路介面的 ALB1 新增至加速器 1，然後在子網路 A 中新增含彈性網路介面的 ALB2，子網路 B 新增至加速器 2，則全域加速器只會建立兩個彈性網路介面：一個位於子網路介面，一個位於子網路介面，一個位於子網路介面，一個位於子網路 A，一個位於子網路 A，一個位於子網路中，另一個位於
- 範例 3：如果您將子網路和子網路中具有彈性網路介面的 ALB1 新增至加速器 1，然後在子網路 A 中新增含彈性網路介面的 ALB2，將子網路介面新增至加速器 2，全域加速器會建立三個彈性網路介面：一個在子網路介面，一個在子網路介面，一個在子網路中，一個在子網路中，一個在子

網路，一個在子網路中，一個在子網路中，一個在子網路中，一個在子網路 子 NetA 中的 elastic network interface 可同時提供加速器 1 和加速器 2 的流量。

如範例 3 所示，如果相同子網路中的端點位於多個加速器後方，則彈性網路介面會在加速器間重複使用。

全域加速器建立的邏輯彈性網路介面不代表單一主機、輸送量瓶頸或單一失敗點。就像在可用區域或子網路中顯示為單一 elastic network interface 的其他 AWS 服務一樣 — 像是網路位址轉譯 (NAT) 閘道或網路負載平衡器等服務 — 全球加速器實作為水平擴展、高可用性的服務。

評估加速器中端點所使用的子網路數目，以判斷全域加速器將建立的彈性網路介面數目。建立加速器之前，請確定您有足夠的 IP 位址空間容量可用於所需的彈性網路介面，每個相關子網路至少有一個可用的 IP 位址。如果您沒有足夠的可用 IP 位址空間，則必須建立或使用具有足夠可用 IP 位址空間供應 Application Load Balancer 和相關聯的全域加速器彈性網路介面使用的子網路。

當全域加速器判斷您帳戶中加速器中的任何端點未使用 elastic network interface 時，全域加速器會刪除該介面。

全域加速器建立的安全性群組

使用全域加速器和安全性群組時，請檢閱下列資訊和最佳作法。

- 全域加速器會建立與其彈性網路界面相關聯的安全性群組。雖然系統不會阻止您這麼做，但您不應該編輯這些群組的任何安全性群組設定。
- 全域加速器不會刪除它所建立的安全性群組。不過，如果您帳戶中加速器中的任何端點未使用 elastic network interface，則全域加速器會刪除該介面。
- 您可以使用全域加速器建立的安全性群組作為您維護的其他安全性群組中的來源群組，但全域加速器只會將流量轉送至您在 VPC 中指定的目標。
- 如果您修改全域加速器所建立的安全群組規則，端點可能會變得狀況不良。如果發生此情況，請聯絡AWS Support尋求協助。
- 全域加速器會為每個 VPC 建立特定的安全性群組。針對特定 VPC 內端點建立的 elastic network interface，無論彈性網路介面與哪個子網路相關聯，都會使用相同的安全群組。

用戶端 IP 位址保留的支援 AWS 區域

您可以在下列 AWS 區域中為 AWS Global Accelerator 啟用用戶端 IP 位址保留功能。

區域名稱	區域
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1 (except AZ usw1-az2)
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1 (except AZ apne1-az3)
Asia Pacific (Seoul)	ap-northeast-2
Canada (Central)	ca-central-1 (except AZ cac1-az3)
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1

區域名稱	區域
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1

中的記錄和監控

您可以使用流量日誌和 AWS CloudTrail 來監控 AWS Global Accelerator 中的加速器、分析流量模式並對與接聽器和端點相關的問題進行故障診斷。

主題

AWS Global Accelerator 中的流程日誌

流程日誌可讓您在 AWS Global Accelerator 中，擷取傳入及傳出網路界面的 IP 地址流量相關資訊。流程日誌資料會發佈至 Amazon S3，您可以在建立流程日誌後擷取和檢視您的資料。

流程日誌可協助您處理幾項任務。例如，您可以針對特定流量沒有觸達端點的原因進行故障診斷，進而協助診斷限制性過高的安全群組規則。您也可以使用流程日誌做為安全工具，監控觸達端點的流量。

流程日誌記錄代表您流程日誌中的網路流。每個記錄都會為特定擷取視窗，擷取特定 5 元組的網路流，5 元組為五個不同值的組合，指定 IP 流程的來源、目標和通訊協定。擷取期間是一段時間，在此期間流程日誌服務會在發佈流程日誌記錄前彙整資料。擷取期間大約是 10 秒，但最多可能需要 1 分鐘。

使用流程日誌時，CloudWatch 日誌需支付費用，即使日誌直接發佈至 Amazon S3 也是如此。如需詳細資訊，請參閱「」將記錄傳送至 S3atAmazon CloudWatch 定價。

主題

將流程日誌發佈到 Amazon S3

AWS Global Accelerator 的流程日誌會發佈至 Amazon S3 到您指定的現有 S3 儲存貯體。流程日誌記錄會發佈至儲存貯體中的一系列日誌檔案物件。

若要建立搭配流程日誌使用的 Amazon S3 儲存貯體，請參閱建立儲存貯體中的Amazon Simple Storage Service 入門指南。

流程日誌檔案

流程日誌會收集流程日誌記錄，將這些記錄整合為日誌檔，然後每隔 5 分鐘將日誌檔發佈至 Amazon S3 儲存貯體。每個日誌檔皆包含過去五分鐘所記錄之 IP 地址流量的流程日誌記錄。

日誌檔的大小上限為 75 MB。如果日誌檔案在五分鐘期間內達到檔案大小上限，流程日誌會停止將流程日誌記錄新增至日誌檔案，然後將它發佈至 Amazon S3 儲存貯體，然後建立新的日誌檔案。

日誌檔案將儲存至指定的 Amazon S3 儲存貯體，並使用由流程日誌的 ID、區域及其建立之日期而決定的資料夾結構。儲存貯體資料夾結構使用以下格式：

```
s3-bucket_name/s3-bucket-prefix/AWSLogs/aws_account_id/globalaccelerator/region/yyyy/mm/dd/
```

同樣的，日誌檔案名稱也是由流程日誌的 ID、區域，以及建立日誌檔案的日期和時間決定。檔案名稱使用下列格式：

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

請注意下列有關記錄檔的資料夾和檔案名稱結構：

- 時間戳記使用 YYYYMMDDTHHmmZ 格式。
- 如果您為 S3 儲存貯體前置詞指定斜線 (/)，則記錄檔儲存貯體資料夾結構將包含雙斜線 (//)，如下所示：

  ```
  s3-bucket_name//AWSLogs/aws_account_id
  ```

以下範例顯示由 AWS 帳戶建立之流程日誌日誌檔案的資料夾結構與檔案名稱123456789012的加速器，識別碼為1234abcd-abcd-1234-abcd-1234abcdefgh，於二零一八年十一月二十三日上午零時零五分：

```
my-s3-bucket/prefix1/AWSLogs/123456789012/globalaccelerator/us-west-2/2018/11/23/123456789012_globalaccelerator_1234abcd-abcd-1234-abcd-1234abcdefgh_20181123T0005Z_1fb1234.log.gz
```

單一流程記錄檔包含具有多個 5 元組記錄的交錯項目；也就是說client_ip、client_port、accelerator_ip、accelerator_port、protocol。若要查看加速器的所有流程記錄檔，請尋找accelerator_id和您的account_id。

用於將流程日誌發佈至 Amazon S3 的 IAM 角色

IAM 主體 (例如 IAM 使用者) 必須有足夠的許可才能將流程日誌發佈至 Amazon S3 儲存貯體。IAM 政策必須包含下列許可：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeliverLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGlobalAcceleratorService",
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "s3Perms",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

流程日誌的 Amazon S3 儲存貯體許可

根據預設，Amazon S3 儲存貯體及其所包含的物件皆為私有。只有儲存貯體擁有者可存取儲存貯體及存放於其中的物件。但是，儲存貯體擁有者可藉由編寫存取政策，將存取授予其他資源和使用者。

如果建立流程日誌的使用者擁有儲存貯體，則服務會自動將下列政策連接至儲存貯體，為流程日誌提供許可，以便將日誌發佈至儲存貯體：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/
*",
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}
```

如果建立流程日誌的使用者並未擁有儲存貯體，或者沒有儲存貯體的 `GetBucketPolicy` 與 `PutBucketPolicy` 許可，流程日誌的建立將會失敗。在此情況下，儲存貯體擁有者必須手動將上述政策手動新增至儲存貯體，然後指定流程日誌建立者的 AWS 帳戶 ID。如需詳細資訊，請參閱「」如何新增 S3 儲存貯體政策？中的Amazon Simple Storage Service 入門指南。如果儲存貯體從多個帳戶接收流程日誌，請將 `Resource` 元素項目新增至每個帳戶的 `AWSLogDeliveryWrite` 政策陳述式。

例如，以下儲存貯體政策允許 AWS 帳戶 123123123123123123 和 456456456456456456 將流程日誌發佈至名為`flow-logs`在名為的儲存貯體中`log-bucket`：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> 建議您將AWSLogDeliveryAclCheck和AWSLogDeliveryWrite許可新增至日誌交付服務主體，而非個別 AWS 帳戶 ARN。

使用 SSE-KMS 儲存貯體必要的 CMK 金鑰政策

若您透過客戶託管的客戶主金鑰 (CMK) 來使用受 AWS KMS 受管金鑰 (SSE-KMS) 啟用 Amazon S3 儲存貯體伺服器端加密，您必須新增下列內容到 CMK 的金鑰原則，讓流程日誌可將日誌檔案寫入儲存貯體：

```
{
    "Sid": "Allow AWS Global Accelerator Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
```

```
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Amazon S3 日誌檔案許可

除了必要的儲存貯體原則之外，Amazon S3 使用存取控制清單 (ACL) 來管理流程日誌所建立之日誌檔案的存取。根據預設，儲存貯體擁有者擁有各個日誌檔案的 FULL_CONTROL 許可。日誌交付擁有者與儲存貯體擁有者不同時，就沒有任何許可。日誌交付帳戶擁有 READ 與 WRITE 許可。如需詳細資訊，請參閱「」存取控制清單 (ACL) 概觀中的Amazon Simple Storage Service 入門指南。

啟用將流程日誌發佈至 Amazon S3

若要在 AWS Global Accelerator 中啟用流程日誌，請遵循此程序中的步驟。

在 AWS Global Accelerator 中啟用流量日誌

1. 為您的 AWS 帳戶中的流程日誌建立 Amazon S3 儲存貯體。
2. 為啟用流程日誌的 AWS 使用者新增所需的 IAM 政策。如需詳細資訊，請參閱 用於將流程日誌發佈至 Amazon S3 的 IAM 角色。
3. 使用您要用於日誌檔的 Amazon S3 儲存貯體名稱和前綴執行下列 AWS CLI 命令：

```
aws globalaccelerator update-accelerator-attributes
       --accelerator-arn
 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh
       --region us-west-2
       --flow-logs-enabled
       --flow-logs-s3-bucket s3-bucket-name
       --flow-logs-s3-prefix s3-bucket-prefix
```

Amazon S3 中的處理流程日誌記錄

日誌檔案已壓縮。如果您使用 Amazon S3 主控台開啟日誌檔案，這些檔案將會解壓縮，並顯示流程日誌記錄。如果您下載這些檔案，則必須解壓縮才能檢視流程日誌記錄。

交付日誌檔案的時間

AWS Global Accelerator 為您設定的加速器交付日誌檔案一小時多達數次。一般而言，日誌檔案包含有關請求的資訊，加速器在特定期間內收到此請求。通常，全球加速器會將該時段的日誌檔案，在出現於日誌中事件的一小時內交付到 Amazon S3 儲存貯體。一個時段的部分或全部日誌檔案項目有時會延遲高達 24 小時。當日誌項目延遲時，Global Accelerator 將它們儲存在日誌檔案中，其中檔案名稱包含發生請求的日期和時段，而不是交付檔案時的日期和時間。

建立日誌檔案時，Global Accelerator 為加速器從所有節點整合資訊，此節點在日誌檔案涵蓋的時段間收到請求。

您啟用記錄後，Global Accelerator 會開始可靠地交付日誌檔案大約四個小時。此時段之前，您可能會收到幾個日誌檔案。

> **Note**
>
> 如果在時段內沒有使用者連接至您的加速器，您便不會收到該時段的任何日誌檔案。

流程日誌記錄語法

流程日誌記錄是以空格分隔的字串，並具有以下格式：

```
<version> <aws_account_id> <accelerator_id> <client_ip>
<client_port> <accelerator_ip> <accelerator_port> <endpoint_ip>
<endpoint_port> <protocol> <ip_address_type> <packets>
<bytes> <start_time> <end_time> <action> <log-status>
<globalaccelerator_source_ip> <globalaccelerator_source_port>
<endpoint_region> <globalaccelerator_region> <direction> <vpc_id>
```

1.0 版格式不包含 VPC 識別碼vpc_id。2.0 版格式，其中包含vpc_id) 會在全域加速器將流量傳送至具有用戶端 IP 位址保留的端點時產生。

下表說明流程日誌記錄的欄位。

欄位	描述
`version`	流程會記錄版本。

欄位	描述
aws_account_id	流程日誌的 AWS 帳戶 ID。
accelerator_id	要記錄流量的加速器 ID。
client_ip	來源 IPv4 地址。
client_port	來源連接埠。
accelerator_ip	加速器的 IP 地址。
accelerator_port	加速器的港口
endpoint_ip	流量的目標 IP 地址。
endpoint_port	流量的目標連接埠。
protocol	流量的 IANA 通訊協定號碼。如需詳細資訊，請參閱指派的網際網路通訊協定號碼。
ip_address_type	IPv4。
packets	在擷取期間傳輸的封包數。
bytes	在擷取期間傳輸的位元組數。
start_time	擷取期間的開始時間 (單位為 Unix 秒)。
end_time	擷取期間的結束時間 (單位為 Unix 秒)。

欄位	描述
action	與流量關聯的動作： • ACCEPT：記錄的流量已獲得安全群組或網路 ACL 的許可。該值目前總是接受。
log-status	流程日誌的記錄狀態： • OK：資料正常記錄至選擇的目的地。 • NODATA：在擷取期間沒有任何流入或流出網路界面的網路流量。 • SKIPDATA：在擷取期間已跳過一部分流程日誌記錄。這可能是因為內部容量的條件約束，或是內部錯誤。
globalaccelerator_source_ip	全域加速器網路介面所使用的 IP 位址。
globalaccelerator_source_port	全域加速器網路介面所使用的連接埠。
endpoint_region	端點所在的 AWS 區域。
globalaccelerator_region	提供請求的節點 (存在點)。每個節點都有一個三字母的代碼，以及一個任意指派的號碼，例如 DFW3。三字母代碼通常對應於節點附近機場的國際航空運輸協會機場代碼。(未來這些縮寫可能會改變。)
direction	流量的方向。表示進入全域加速器網路的流量 (INGRESS) 或返回客戶端 (EGRESS。
vpc_id	VPC 識別符。當全域加速器將流量傳送至具有用戶端 IP 位址保留的端點時，隨附於 2.0 版流量記錄中。

如果欄位不適用於特定記錄，則記錄會針對該項目顯示一個 '-' 符號。

搭配 AWS Global Accelerator 使用 Amazon CloudWatch

AWS Global Accelerator 會為您的加速器發佈資料點到 Amazon CloudWatch。CloudWatch 可讓使用一組時間序列資料的形式來擷取這些資料點的相關統計資料，也就是指標。您可以將指標視為要監控的變數，且資料點是該變數在不同時間點的值。例如，您可以透過加速器監控指定期間內的流量。每個資料點都有關聯的時間戳記和可選的測量單位。

您可以使用指標來確認系統的運作符合預期。例如，若指標超過您認為能夠接受的範圍，您可以建立 CloudWatch 警示來監控指定的指標並執行動作 (例如傳送通知到電子郵件地址)。

只會在請求穿越加速器時回報指標到 CloudWatch。如果請求穿越加速器，Global Accelerator 會以 60 秒為間隔來測量並傳送其指標。如果沒有請求進出加速器，或者指標沒有資料，則不會回報該指標。

如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

內容

Global Accelator 指標

`AWS/GlobalAccelerator` 命名空間包含下列指標。

指標	描述
`NewFlowCount`	在期間內，從用戶端到端點建立的新 TCP 和 UDP 流程 (或連線) 總數。 報告條件：有非零值。 統計資料：唯一有用的統計數據是`Sum`。 Dimensions • `Accelerator`

指標	描述
	• Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress
ProcessedBytesIn	由加速器處理的傳入位元組總數，包含 TCP/IP 標頭。此計數包括通往端點的所有流量。 報告條件：有非零值。 統計資料：唯一有用的統計數據是Sum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

指標	描述
ProcessedBytesOut	由加速器處理的傳出位元組總數，包含 TCP/IP 標頭。此計數包含來自端點的流量，減去運作狀態檢查流量。 報告條件：有非零值。 統計資料：唯一有用的統計數據是Sum。 Dimensions • Accelerator • Accelerator, Listener • Accelerator, Listener, EndpointGroup • Accelerator, SourceRegion • Accelerator, DestinationEdge • Accelerator, TransportProtocol • Accelerator, AcceleratorIPAddress

加速器的指標維度

若要篩選加速器的指標，請使用下列維度。

維度	描述
Accelerator	依加速器篩選指標資料。透過加速器 ID (加速器 ARN 的最後部分) 指定加速器。例如，如果 ARN 是arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh ，您指定下列項目：**1234abcd-abcd-1234-abcd-1234abcdefgh** 。
Listener	依監聽器篩選指標資料。透過偵聽程式識別碼 (偵聽程式 ARN 的最後一部分) 來指定偵聽程式。例如，如果 ARN 是arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz ，您指定下列項目：**0123wxyz**。

維度	描述
EndpointGroup	依端點群組篩選指標資料。依 AWS 區域指定端點群組，例如**us-east-1**（全部小寫）。
SourceRegion	依來源區域篩選指標資料，這是執行應用程式終端節點的 AWS 區域的地理區域。來源區域為下列其中一個項目： • NA — 美國和加拿大 • EU — 歐洲 • AP — 亞太區 * • KR — 南韓 • IN — 印度 • AU — 澳洲 • ME — 中東 • SA — 南美洲 * 韓國及印度除外
DestinationEdge	依目標邊緣篩選指標資料，這是為用戶端流量提供服務的 AWS 節點地理區域。目標邊緣為下列其中一項： • NA — 美國和加拿大 • EU — 歐洲 • AP — 亞太區 * • KR — 南韓 • IN — 印度 • AU — 澳洲 • ME — 中東 • SA — 南美洲 • ZA — 南非 * 韓國及印度除外

維度	描述
`Transport Protocol`	依傳輸通訊協定篩選指標資料：UDP 或 TCP。
`AcceleratorIPAddress`	依加速器的 IP 位址篩選指標資料：也就是指派給加速器的其中一個靜態 IP 位址。

Global Accelerator 指標統計資

CloudWatch 根據由 Global Accelerator 發佈的指標資料點提供統計資料。統計資料是在一段指定期間內的指標資料彙總。當您請求統計資料時，傳回的資料流是藉由指標名稱和維度做識別。維度是用來單獨辨識指標的名稱/值組。例如，您可以為加速器請求處理的位元組，其中位元組是從歐洲的 AWS 節點提供服務 (目的地邊緣為「EU」)。

以下是您可能會覺得有用的度量/標註組合範例：

- 依據您的兩個加速器 IP 位址，檢視服務的流量 (例如處理字元輸出)，以驗證您的 DNS 設定是否正確。
- 檢視使用者流量的地理位置分佈，並監視其中有多少是本地 (例如，北美至北美) 或全球 (例如，澳洲或印度至北美洲)。若要判斷這個問題，請檢視「目的地邊緣」和「SourceRegion」維度設定為特定值的處理位元組在或處理位元組輸出的度量。

檢視適用於您加速器的 CloudWatch 指標

您可以使用 CloudWatch 主控台或 AWS CLI 來檢視加速器的 CloudWatch 指標。在主控台中，指標會以監控圖表的形式顯示。只會在加速器處於作用中狀態並接收請求時顯示資料點。

您必須在主控台或使用 AWS CLI 時檢視美國西部 (奧勒岡) 區域的 CloudWatch 指標。使用 AWS CLI 時，請包含下列參數來指定命令的美國西部 (俄勒岡州) 區域：`--region us-west-2`。

使用 CloudWatch 主控台檢視指標

1. 於開啟 CloudWatch 主控台https://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2。
2. 在導覽窗格中，選擇指標。
3. 選取GlobalAccelerator命名空間。

4. (選用) 若要檢視所有維度的指標，請在搜尋欄位中鍵入其名稱。

使用 AWS CLI; 檢視指標

使用下列 list-metrics 命令來列出可用指標：

```
aws cloudwatch list-metrics --namespace AWS/GlobalAccelerator --region us-west-2
```

使用 AWS CLI 取得指標的統計資料

使用下列項目取得指標-統計資料命令取得指定指標和維度的統計資料。請注意，CloudWatch 將把維度的各獨特組合視為個別指標。您無法使用未具體發佈的維度組合來擷取統計資料。您必須指定建立指標時所使用的相同維度。

下列範例列出從北美 (NA) 目的地邊緣服務的加速器處理位元組總數 (以每分鐘為單位)。

```
aws cloudwatch get-metric-statistics --namespace AWS/GlobalAccelerator \
--metric-name ProcessedBytesIn \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=Accelerator,Value=1234abcd-abcd-1234-abcd-1234abcdefgh
 Name=DestinationEdge,Value=NA \
--start-time 2019-12-18T20:00:00Z --end-time 2019-12-18T21:00:00Z
```

以下為此命令的範例輸出：

```
{
    "Label": "ProcessedBytesIn",
    "Datapoints": [
        {
            "Timestamp": "2019-12-18T20:45:00Z",
            "Sum": 2410870.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:47:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:46:00Z",
```

```
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:42:00Z",
            "Sum": 1560.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:48:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:43:00Z",
            "Sum": 1343.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:49:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:44:00Z",
            "Sum": 35791560.0,
            "Unit": "Bytes"
        }
    ]
}
```

使用 AWS CloudTrail 記錄 AWS Global Accelerator API 呼叫

AWS Global Accelerator 整合了 AWS CloudTrail，後者是一項服務，可提供由使用者、角色或 AWS 服務在 Global Accelerator 中所採取之動作的記錄。CloudTrail 會將針對的所有 API 呼叫擷取為事件，包括自全域加速器主控台以及自程式碼呼叫對全域加速器 API 的呼叫。如果您建立線索，就可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括全球加速器的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。

若要進一步了解 CloudTrail，請參閱 AWS CloudTrail User Guide。

CloudTrail 中的全球加速器資訊

CloudTrailAWS當您建立帳戶時，系統會在您的帳戶中啟用 。此外，Global Accelerator 發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他 AWS 服務事件記錄到事件歷史記錄。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

若要持續記錄 AWS 帳戶中的事件 (包括 Global Accelerator 事件)，請建立線索。追蹤記錄可讓 CloudTrail 將日誌檔案交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有區域。線索會記錄來自 AWS 分割區中所有區域的事件，然後將所有日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列主題：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Global Accelerator 動作，並記錄在AWS Global Accelerator API 參考。例如，呼叫至`CreateAccelerator`、`ListAccelerators`和`UpdateAccelerator`操作會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或記錄項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 IAM 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

了解全域加速器日誌檔案項目

線索是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。每個 JSON 格式的 CloudTrail 日誌檔案可包含一或多個日誌項目。每個日誌項目代表任何來源提出的單一請求，並且包括了請求的動作、包括任何參數、動作的日期和時間等相關資訊。日誌項目不保證以任何特定順序存在；它們不是 API 呼叫的有序堆疊追蹤。

以下範例顯示的是包含這些全域加速器動作的 CloudTrail 日誌項目：

- 列出帳戶的加速器：eventName是ListAccelerators。
- 建立接聽程式：eventName是CreateListener。
- 更新接聽程式：eventName是UpdateListener。
- 描述接聽程式：eventName是DescribeListener。
- 列出帳戶的監聽程式：eventName是ListListeners。
- 刪除接聽程式：eventName是DeleteListener。


```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:14Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListAccelerators",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "083cae81-28ab-4a66-862f-096e1example",
```

```
      "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:04:49Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
```

```
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
```

```
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
```

```
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
            "fromPort": 81,
            "toPort": 81
          }
        ]
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            },
            {
```

```
            "fromPort": 81,
            "toPort": 81
          }
        ],
        "protocol": "TCP",
        "clientAffinity": "NONE"
      }
    },
    "requestID": "008ef93c-b3a3-44b4-afb3-768example",
    "eventID": "85958f0d-63ff-4a2c-99e3-6ffbexample",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "A1B2C3D4E5F6G7EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/smithj",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
        "attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2018-11-17T21:02:36Z"
        },
        "sessionIssuer": {
          "type": "Role",
          "principalId": "A1B2C3D4E5F6G7EXAMPLE",
          "arn": "arn:aws:iam::111122223333:user/smithj",
          "accountId": "111122223333",
          "userName": "smithj"
        }
      }
    },
    "eventTime": "2018-11-17T21:06:05Z",
    "eventSource": "globalaccelerator.amazonaws.com",
    "eventName": "DescribeListener",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
    "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
    "requestParameters": {
```

```
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListListeners",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample"
      },
      "responseElements": null,
```

```
      "requestID": "08e4b0f7-689b-4c84-af2d-47619example",
      "eventID": "f4fb8e41-ed21-404d-af9d-037c4example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:24Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DeleteListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
```

```
    ]
}
```

AWS Global Accelerator 安全

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足對安全最為敏感的組織需求。

安全是 AWS 與您共同肩負的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端 內部 的安全：

- 雲端安全性 – AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎設施。AWS 也會提供您可以安全使用的服務。在我們的 AWS 合規計劃中，第三方稽核人員會定期檢測及驗證我們的安全有效。若要進一步了解適用於全域加速器的合規計劃，請參閱合規計劃的 AWS 服務範圍。
- 雲端內部安全 – 您的責任取決於您所使用的 AWS 服務。您也必須對資料敏感度、組織要求，以及適用法律和法規等其他因素負責。

本文件會協助您了解使用全球加速器時共同責任模型的適用情形。下列主題將說明如何設定全域加速器以達到您的安全目標。

主題

AWS Global Accelerator 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取，包括 AWS Global Accelerator 資源。管理員使用 IAM 控制誰是身分驗證(已登入) 和已授權(具有權限) 來使用全域加速器資源。IAM 是 AWS 帳戶內含的一項功能，無須額外付費。

> **Important**
>
> 如果您不熟悉 IAM，請檢閱此頁面的入門資訊，然後參閱入門 IAM。或者，您可以進一步了解身份驗證和存取控制，方法是檢視什麼是身分驗證？、什麼是存取控制？，以及什麼是政策？。

主題

概念與術語

身分驗證— 若要登入 AWS，您必須使用以下登入資料：根使用者登入資料 (不建議)、IAM 使用者登入資料，或使用 IAM 角色的臨時登入資料。若要進一步了解這些實體，請參閱什麼是身分驗證？。

存取控制— AWS 管理員使用政策來控制對 AWS 資源的存取，例如全球加速器中的加速器。如需進一步了解，請參閱什麼是存取控制？和什麼是政策？。

> **Important**
>
> 帳戶內的所有資源由帳戶擁有，無論這些資源的建立者是誰。您必須取得存取權以建立資源。然而，即使是您建立的資源也不表示您會自動擁有存取該資源的完整存取權。管理員必須對您要執行的每個動作明確授與許可。該管理員也可以隨時撤銷您的許可。

為了協助您了解 IAM 運作方式的基本知識，請檢閱以下詞彙：

資源

AWS 服務 (例如全域加速器和 IAM) 通常包含稱為資源的物件。在大多數情況下，您可以從服務中建立、管理和刪除這些資源。IAM 資源包括使用者、群組、角色和政策：

使用者

IAM 使用者代表使用登入資料與 AWS 互動的人員或應用程式。使用者由名稱、用於登入 AWS 管理主控台的密碼，以及最多兩個可與 AWS CLI 和 AWS API 一起使用的存取金鑰組成。

群組

IAM 群組是 IAM 使用者的集合。管理員可以使用群組來指定成員使用者的許可。這可讓管理員輕鬆管理多名使用者的許可。

角色

IAM 角色沒有任何與之關聯的長期登入資料 (密碼或存取金鑰)。任何需要角色且擁有許可的人員皆可擔任該角色。IAM 使用者可擔任一個角色，為了特定任務來臨時採用不同許可。聯合身分使用者可以使用對應到角色的外部身分供應商來擔任該角色。某些 AWS 服務可以假設服務角色以代您存取 AWS 資源。

政策

政策為 JSON 文件，可定義所連接的物件的許可。AWS Support身分類型政策您可以連接到身分 (使用者、群組或角色)。某些 AWS 服務允許您將資源型政策資源來控制委託人 (人員或應用程式) 可對該資源執行的操作。全域加速器不支援資源類型政策。

身分

身分是 IAM 資源，您可以為其定義許可。包括使用者、群組和角色。

實體

實體是您用於身份驗證的 IAM 資源。包括使用者和角色。

Principals (委託人)

在 AWS 中，委託人是使用實體登入並向 AWS 提出請求的人員或應用程式。身為委託人，您可以使用 AWS 管理主控台、AWS CLI 或 AWS API 來執行操作 (例如刪除加速器)。這會對該操作建立請求。您的請求指定動作、資源、委託人、委託人帳戶以及關於請求的任何其他資訊。所有這些資訊都為 AWS 提供context以取得您的請求。AWS 會檢查所有適用於請求內容的政策。只有在政策允許請求的每個部分時，AWS 才會授權該請求。

若要檢視驗證和存取控制程序的圖表，請參閱了解 IAM 的運作方式中的IAM 使用者指南。如需 AWS 如何決定是否允許請求的詳細資訊，請參閱Policy Evaluation Logic中的IAM 使用者指南。

主控台存取、驗證管理和存取控制所需的權限

若要使用全球加速器或管理授權和為自己或他人存取控制，您必須擁有正確的許可。

建立全域加速器所需的權限

若要建立 AWS Global Accelerator 速器，使用者必須具有建立與全域加速器相關聯的服務連結角色的權限。

若要確保使用者具有在全域加速器中建立加速器的正確權限，請將原則附加至使用者，如下所示。

> **Note**
>
> 如果您建立更嚴格的身分型許可政策，則具有該政策的使用者將無法建立加速器。

```
{
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "globalaccelerator.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*"
    }
```

使用全域加速器主控台所需的許可

若要存取 AWS Global Accelerator 主控台，您必須擁有一組最基本的許可，讓您可以列出和檢視 AWS 帳戶中全球加速器資源的詳細資訊。如果您建立比最低必要許可更嚴格的身分類型許可政策，則對於具有該政策的實體而言，主控台將無法如預期運作。

為確保那些實體仍可使用全球加速器主控台或 API 動作，請也將以下 AWS 受管政策連接至使用者，如在 JSON 標籤上建立政策：

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

附加第一個原則，GlobalAcceleratorReadOnlyAccess，如果使用者只需要在主控台中檢視資訊，或呼叫使用List*或Describe*操作。

附加第二個原則，GlobalAcceleratorFullAccess，提供給需要建立或更新加速器的使用者。此完整存取政策包括FULL權限，以及describe權限和 Elastic Load Balancing。

> **Note**
>
> 如果您建立的身分授權政策不包含 Amazon EC2 和 Elastic Load Balancing 所需的權限，則具有該政策的使用者將無法將 Amazon EC2 和 Elastic Load Balancing 資源新增到加速器。

以下是完整存取原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

驗證管理所需的權限

若要管理自己的登入資料，例如密碼、存取金鑰和多重驗證 (MFA) 裝置，您的管理員必須授與您必要的許可。若要查看包含這些許可的政策，請參閱允許使用者自行管理其認證。

身為 AWS 管理員，您需要完整存取 IAM 的權限，您才能在 IAM 中建立和管理使用者、群組、角色和政策。您應該使用AdministratorAccessAWS 受管政策，其中包含對所有 AWS 的完整存取權。此政策不提供對 AWS Billing and Cost Management 主控台的存取權，也不允許需要 AWS 帳戶根使用者登入資料的任務。如需詳細資訊，請參閱「」需要 AWS 帳戶根使用者登入資料的 AWS 任務中的AWS 一般參考資料。

> **Warning**
>
> 只有管理員使用者應擁有 AWS 的完整存取權。使用此政策的任何人都有許可完全管理身分驗證和存取控制，以及修改 AWS 中的每個資源。若要了解如何建立此使用者，請參閱建立 IAM 管理員使用者。

存取控制所需的權限

如果管理員提供您 IAM 使用者登入資料，則管理員已將政策連接到 IAM 使用者來控制您可以存取哪些資源。若要在 AWS 管理主控台中檢視連接到使用者身分的政策，您必須擁有以下許可：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "ListUsersViewGroupsAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

如果您需要額外許可，請要求管理員更新您的政策，以允許您存取所需的動作。

瞭解全球加速器如何搭配 IAM 使用

服務可與 IAM 搭配運作，以多種方式：

動作

全域加速器支援在政策中使用動作。這可讓管理員控制實體是否可以在全域加速器中完成操作。例如，若要允許實體呼叫GetPolicyAWS API 操作來檢視政策，管理員必須附加允許iam:GetPolicy動作。

下列範例政策允許使用者執行CreateAccelerator操作以編程方式為您的 AWS 帳戶創建加速器：

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "globalaccelerator:CreateAccelerator"
         ],
         "Resource":"*"
      }
   ]
}
```

資源層級許可

全域加速器支援資源層級的許可。資源層級許可讓您可以使用 ARN 在政策中指定個別的資源。

以資源為基礎的政策

全域加速器不支援資源類型政策。使用以資源為基礎的政策，您可以將政策連接到服務內的資源。以資源為基礎的政策包括Principal元素來指定哪些 IAM 身分可以存取該資源。

根據標籤的授權

全域加速器支援授權型標籤。此功能可讓您在政策的條件中使用資源標籤。

暫時性登入資料

全域加速器支援臨時登入資料。使用暫時登入資料，您可以搭配聯合登入、擔任 IAM 角色，或是擔任跨帳戶角色。您取得暫時安全登入資料的方式是呼叫 AWS STS API 操作 (例如，AssumeRole或GetFederationToken。

服務連結角色

Global Accelerator 支援服務連結角色。此功能可讓服務代表您擔任服務連結角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

服務角色

全域加速器不支援服務角色。此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這可能會破壞此服務的功能。

驗證與存取控制疑難排解

請使用以下資訊來協助您診斷和修復使用 IAM 時發生的常見問題。

主題

- 我未獲授權，不得在全域加速器中執行動作
- 我是管理員，想要允許其他人存取全域加速器
- 我想要了解 IAM 而無需成為專家

我未獲授權，不得在全域加速器中執行動作

若 AWS 管理主控台告知您並未獲得執行動作的授權，您必須聯絡提供您使用者名稱和密碼的管理員。

下列範例會在名為my-user-name會嘗試使用主控台執行globalaccelerator:CreateAccelerator動作，但沒有權限：

```
User: arn:aws:iam::123456789012:user/my-user-name is not authorized to perform: aws-globalaccelerator:CreateAccelerator on resource: my-example-accelerator
```

在這種情況下，要求管理員更新您的政策，以允許您存取`my-example-accelerator`資源使用`aws-globalaccelerator:CreateAccelerator`動作。

我是管理員，想要允許其他人存取全域加速器

若要允許其他人存取全球加速器，您必須針對需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的登入資料來存取 AWS。您接著必須將原則連線到實體，在全域加速器中授與正確的許可。

若要立即開始，請參閱入門 IAM。

我想要了解 IAM 而無需成為專家

若要進一步了解 IAM 詞彙、概念和程序，請參閱下列主題：

- 什麼是身分驗證？
- 什麼是存取控制？
- 什麼是政策？

標籤型政策

設計 IAM 政策時，您可能會透過授予對特定資源的存取來設定精密許可。隨著您管理的資源數量增加，此任務變得越來越困難。標記加速器並在政策陳述式條件中使用標籤，可讓此任務更輕鬆。您可以對具有特定標籤的任何加速器大量授予存取。然後，您會在建立加速器或稍後更新加速器時，對相關的加速器重複套用此標籤。

> **Note**
>
> 在條件中使用標記是控制資源和請求的存取權限的方式之一。如需 Clobal Accelerator 標記功能的詳細資訊，請參閱AWS Global Accelerator 中的標籤。

可以將標記連接到資源或在請求中將標記傳遞至支援標記的服務。在全域加速器中，只有加速器可以包含標籤。在建立 IAM 政策時，可使用標記條件鍵來控制以下項目：

- 可在加速器上執行動作的使用者 (根據資料已具有的標記)。
- 可在動作請求中傳遞的標記。
- 是否可在請求中使用特定的標籤索引鍵。

關於標籤條件索引鍵的完整語法和語義，請參閱使用 IAM 標籤控制存取中的IAM 使用者指南。

例如，全域加速器GlobalAcceleratorFullAccess受管使用者政策可提供使用者在任何資源上執行任何全域加速器動作的許可。以下政策會限制此能力，拒絕未授權的使用者許可，禁止在任何生產加速器。除了受管使用者政策之外，客戶的管理員必須將此 IAM 政策連接到未授權的 IAM 使用者。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:RequestTag/stage":"prod"
            }
         }
      },
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:ResourceTag/stage":"prod"
            }
         }
      }
   ]
}
```

的服務連結角色

AWS Global Accelerator 使用 AWS Identity and Access Management (IAM)服務連結角色。服務連結角色是直接連結至服務的一種特殊 IAM 角色類型。服務連結角色由服務預先定義，並包含該服務在代表您呼叫其他 AWS 服務時，需要用到的所有權限。

全域加速器使用以下 IAM 服務連結角色：

- 全球加速器的 AWS 服務— 全域加速器使用此角色來允許全域加速器建立及管理用戶端 IP 位址保留所需的資源。

當第一次需要此角色才能支援全域加速器 API 作業時，全域加速器會自動建立名為 AWsServices 為全域加速器的角色。「AWsServices 全域加速器」角色可讓「全域加速器」建立和管理用戶端 IP 位址保留所需的資源。在全域加速器中使用加速器時，需要此角色。AWSServiceRoleFor全球加速工具角色的 ARN 看起來類似如下：

```
arn:aws:iam::123456789012:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator
```

服務連結角色可讓設定及使用全球加速器變得更輕鬆，因為您不必手動新增必要的許可。全球加速器會定義其服務連結角色的許可，且唯有全球加速器可以擔任此角色。已定義的許可包括信任政策和許可政策。許可原則無法附加到其他任何 IAM 實體。

您必須移除任何關聯的全域加速器資源，才能刪除服務連結角色。這有助於保護您的全域加速器資源，確保您不會移除在存取作用中資源時仍有需要的服務連結角色。

如需支援服務連結角色之其他服務的資訊，請參閱與 IAM 搭配使用的 AWS 服務並尋找有是中的服務連結角色資料行。

的服務連結角色許可

全域加速器使用名為的服務連結角色全球加速器的 AWS 服務。下列小節說明角色的許可。

服務連結角色許可

此服務連結的角色可讓全域加速器管理 EC2 彈性網路介面和安全性群組，並協助診斷錯誤。

針對
AWSServiceRoleForCloForCloForCollControlForCloForCollControlForCollControlForCloForCloForClo

- `globalaccelerator.amazonaws.com`

此角色許可政策允許全球加速器對指定資源完成下列動作，如政策所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

您必須設定許可，讓 IAM 實體 (如使用者、群組或角色) 刪除全球加速器服務連結角色。如需詳細資訊，請參閱「」服務連結角色許可中的IAM 使用者指南。

為建立全域加速器建立服務連結角色

您不需要手動建立全域加速工具的服務連結角色。服務會在您第一次建立加速器時，自動為您建立角色。若您移除全域加速器資源並刪除服務連結角色，則當您建立新的加速器時，服務將會自動重新建立角色。

編輯全域加速器服務連結角色

全域加速器不允許您編輯 AWSServiceRoleFor全域加速器服務連結角色。在此服務建立服務連結角色之後，您將無法變更該角色的名稱，因為各種實體皆可能會參考該角色。然而，您可使用 IAM 編輯角色的描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除全域加速器服務連結角色

如果您不再需要使用全域加速器，建議您刪除服務連結角色。如此一來，您就沒有非主動監控或維護的未使用實體。然而，您必須先清除您帳戶中的全球加速器資源，然後才能手動刪除這些角色。

停用並刪除您的加速程式後，您可以刪除服務連結角色。如需有關刪除加速器的詳細資訊，請參閱 建立或更新標準加速器。

> **Note**
>
> 如果您已停用並刪除加速器，但是全球加速器未完成更新，則刪除服務連結角色的動作可能會失敗。如果發生此情況，請等候數分鐘，然後再次嘗試服務連結角色刪除步驟。

手動刪除 AWSServiceRoleFor全球加速工具服務連結角色

1. 登入 AWS 管理主控台，然後前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在 IAM 主控台的導覽窗格中，選擇 Roles (角色)。然後，選擇您要刪除的角色名稱旁的核取方塊，而非名稱或資料列本身。
3. 在頁面頂端的 Role (角色) 動作中選擇 Delete (刪除) 角色。
4. 在確認對話方塊中，檢閱服務上次存取資料，以顯示每個所選取角色上次存取 AWS 服務的時間。這可協助您確認角色目前是否作用中。如果您想要繼續進行，請選擇 Yes, Delete (是，刪除) 來提交服務連結角色以進行刪除。

5. 查看 IAM 主控台通知，監視服務連結角色刪除的進度。因為 IAM 服務連結角色刪除不同步，所以在您提交角色進行刪除之後，刪除任務可能會成功或失敗。如需詳細資訊，請參閱「」刪除服務連結角色中的IAM 使用者指南。

全球加速器服務連結角色 (AWS 受管政策) 的更新

檢視自此服務開始追蹤這些變更後，服務連結角色更新的詳細資料。如需有關此頁面變更的自動警示，請在 AWS Global Accelerator 上訂閱 RSS 摘要文件歷史記錄(憑證已建立！) 頁面上的名稱有些許差異。

變更	描述	日期
全球加速器的 AWS 服務— 已更新政策	全域加速器新增了新的權限，以協助全域加速器診斷錯誤。 Global Acceleratorec2:DescribeRegions 以判斷客戶所在的 AWS 區域，這可協助全球加速器疑難排解錯誤。	2021 年 5 月 18 日
全球加速器開始追蹤變更	全球加速器開始追蹤其 AWS 受管政策的變更。	2021 年 5 月 18 日

全域加速器服務連結角色的支援區域

全球加速器支援在支援全球加速器的 AWS 區域中，使用服務連結角色。

如需目前支援全球加速器和其他服務的 AWS 區域清單，請參閱AWS 區域表格。

存取和驗證概觀

如果您是 IAM 的新手，請閱讀下列主題來開始在 AWS 中授權和存取。

主題

- 什麼是身分驗證？
- 什麼是存取控制？
- 什麼是政策？

- 入門 IAM

什麼是身分驗證？

身份驗證是使用登入資料登入 AWS 的方式。

> **Note**
>
> 若要快速開始使用，您可以忽略此部分。首先，檢閱上的入門資訊AWS Global Accelerator 的 Identity and Access Management，然後參閱入門 IAM。

作為委託人，您必須身分驗證(登入至 AWS)，使用實體 (根使用者、IAM 使用者或 IAM 角色) 將請求傳送至 AWS。IAM 使用者可有長期登入資料 (例如，使用者名稱和密碼或一組存取金鑰)。擔任 IAM 角色時，您會取得臨時安全登入資料。

若要從 AWS 管理主控台以使用者身分進行驗證，您必須使用您的使用者名稱和密碼登入。若要從 AWS CLI 或 AWS API 取得身分驗證，您必須提供存取金鑰和私密金鑰或臨時登入資料。AWS 提供開發套件和 CLI 工具，以密碼編譯方式使用登入資料簽署您的請求。如果您未使用 AWS 工具，則必須自行簽署請求。無論您使用何種身份驗證方法，您可能還需要提供額外的安全性資訊。例如，AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。

身為委託人，您可以使用以下實體 (使用者或角色) 登入 AWS：

AWS 帳戶根使用者

當您首次建立 AWS 帳戶，您會先有單一的登入身分，可以完整存取帳戶中所有 AWS 服務與資源。此身分稱為 AWS 帳戶「根使用者」，是藉由您用來建立帳戶的電子郵件地址和密碼以登入並存取。強烈建議您不要以根使用者處理日常作業，即使是管理作業。反之，請遵循僅以根使用者建立您第一個 &IAM; 使用者的最佳實務。接著請妥善鎖定根使用者登入資料，只用來執行少數的帳戶與服務管理作業。

IAM 使用者

AIAM 使用者是 AWS 帳戶內具備特定許可的實體。支援 Global Acceler簽章版本 4，這是用來驗證傳入 API 請求的協定。如需有關驗證請求的詳細資訊，請參閱簽章版本 4 簽章程序中的AWS 一般參考資料。

IAM 角色

AIAM 角色是您可以在帳戶中建立的 IAM 身分，具有特定許可。IAM 角色類似於 IAM 使用者，因為同樣是 AWS 身分，也有許可政策可決定該身分在 AWS 中可執行和不可執行的操作。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性登入資料。使用臨時登入資料的 IAM 角色在下列情況中非常有用：

聯合身分使用者存取

非建立 IAM 使用者，而是使用來自 AWS Directory Service、您的企業使用者目錄或 Web 身分供應商的現有身分。這些稱為「聯合身分使用者」。透過身份供應商請求存取時，AWS 會將角色指派給聯合身份使用者。如需聯合身分使用者的詳細資訊，請參閱聯合身分使用者和角色中的IAM 使用者指南。

暫時使用者權限

IAM 使用者可擔任一個角色，為了特定任務來採用不同許可。

跨帳戶存取

您可以使用 IAM 角色，允許不同帳戶中信任的委託人存取您帳戶的資源。角色是授予跨帳戶存取的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色做為代理)。全域加速工具不支援這些資源類型政策。有關選擇使用角色或資源型政策，以允許跨帳戶存取的詳細資訊，請參閱控制對不同帳戶中委託人的存取。

AWS 服務存取

服務角色是IAM 角色服務會擔任代表您執行動作。服務角色提供的存取權僅限在您的帳戶內，不能用來授予存取其他帳戶中的服務。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱「」建立角色以將許可委派給 AWS 服務中的IAM 使用者指南。

在 Amazon EC2 上執行的應用程式

針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時登入資料。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體描述檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時登入資料。如需詳細資訊，請參閱「」使用 IAM 角色為在 Amazon EC2 執行個體上執行的應用程式授予許可中的IAM 使用者指南。

什麼是存取控制？

在您登入 (通過驗證) AWS 後，您對 AWS 資源和操作的存取會受政策管制。存取控制也稱為授權。

> **Note**
>
> 若要快速開始使用，您可以忽略此頁面。首先，檢閱上的入門資訊AWS Global Accelerator 的 Identity and Access Management，然後參閱入門 IAM。

在授權期間，AWS 會使用來自請求內容以檢查套用的政策。接著使用政策以決定是否允許或拒絕請求。大多數的政策儲存在 AWS 中做為 JSON 文件，並指定允許或拒絕委託人的許可。如需 JSON 政策文件的結構和內容的詳細資訊，請參閱什麼是政策？。

政策可讓管理員指定哪些使用者有權存取 AWS 資源，以及他們可以對這些資源執行哪些操作。每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。換言之，在預設狀態下，使用者無法執行任何動作，甚至不能查看自己的存取金鑰。若要授予使用者執行動作的許可，管理員必須將許可政策連接到使用者。或者，可以將使用者加入到具有預期的許可的群組中。管理員將許可給予群組時，群組內的全部使用者都會獲得那些許可。

您可以透過有效登入資料來驗證您的請求，但還須管理員授與許可才能建立或存取 AWS Global Accelerator 資源。例如，您必須具有明確許可才能建立 AWS Global Accelerator。

做為管理員，您可以編寫政策以控制存取下列項目：

- Principals (委託人)— 控制發出請求的人員或應用程式 (委託人) 被允許這樣做。
- IAM 身分識別— 控制哪些 IAM 身分 (群組、使用者與角色) 可被存取以及存取的方法。
- IAM 政策-控制哪些使用者可以建立、編輯和刪除客戶受管政策，以及哪些使用者可以連接和分離所有受管政策。
- AWS 資源— 控制哪些使用者有權使用以身分為基礎的政策或以資源為基礎的政策來存取資源。
- AWS 帳戶— 控制是否僅允許特定帳戶的成員發出請求。

控制 委託人的存取權限

許可政策會控制身為委託人的您可允許執行的動作。管理員必須將身分型許可政策連接到可提供許可的身分 (使用者、群組或角色)。許可政策允許或存取 AWS。管理員也可以設定 IAM 實體 (使用者或角色) 的許可界限，以定義實體可擁有的最大許可。許可界限是進階 IAM 功能。如需有關許可界限的詳細資訊，請參閱IAM 身份的許可界限中的IAM 使用者指南。

如需詳細資訊和如何控制主參與者 AWS 存取的範例，請參閱控制主參與者的存取中的IAM 使用者指南。

控制身份的存取

管理員可以建立政策限制對身分可執行的動作或是可存取的人員，藉以控制您可以對 IAM 身分 (使用者、群組或角色) 執行的動作。然後，他們會將該政策連接到提供您許可的身分。

例如，管理員可能允許您為三個特定的使用者重設密碼。為此，他們會將政策連接到 IAM 使用者，您可以選擇僅為自己和具有三個指定使用者 ARN 的使用者重設密碼。這可讓您重設團隊成員的密碼，但非其他 IAM 使用者。

如需使用政策控制 AWS 身分存取的詳細資訊和範例，請參閱控制身份的存取中的IAM 使用者指南。

控制原則的存取

管理員可控制哪些使用者可以建立、編輯和刪除客戶受管政策，以及哪些使用者可以連接和分離所有受管政策。當您檢閱政策時，您可以檢視政策摘要，其中包括該政策內每項服務的存取層級摘要。AWS 將每個服務動作分類為四個動作之一存取層級基於每個動作的作用：`List`、`Read`、`Write`, 或`Permissions management`。您可以使用這些存取層級，來判斷哪些動作要包含到您的政策中。如需詳細資訊，請參閱「」了解政策摘要中的存取層級摘要中的IAM 使用者指南。

> **Warning**
>
> 您應該限制`Permissions Management`的存取層級許可。否則，您的帳戶成員可以為自己建立政策，擁有比應有更多的許可。或者，他們可以建立能夠完全存取 AWS 的個別使用者。

如需詳細資訊和如何控制 AWS 對政策的存取權限的範例，請參閱控制原則的存取中的IAM 使用者指南。

控制 資源的存取權限

管理員可以控制哪些使用者有權使用以身分為基礎的政策或以資源為基礎的政策來存取資源。在以身分為基礎的政策中，您將政策附加到一個身分並指定該身分可以存取哪些資源。在以資源為基礎的政策中，您將政策附加到要控制的資源。在該政策中，您指定哪些委託人可以存取該資源。

如需詳細資訊，請參閱「」控制資源的存取中的IAM 使用者指南。

資源建立者沒有自動具有權限

帳戶內的所有資源由帳戶擁有，無論這些資源的建立者是誰。AWS 帳戶根使用者是帳戶擁有者，因此具有可在帳號中任何資源上執行任何動作的許可。

> **Important**
>
> 強烈建議您不要以根使用者處理日常作業，即使是管理作業。反之，請遵循僅使用根使用者建立您第一個 IAM 使用者的最佳實務。接著請妥善鎖定根使用者登入資料，只用來執行少數的帳戶與服務管理作業。若要檢視需要您以根使用者身分登入的工作，請參閱需要根使用者的 AWS 任務。

必須授與 AWS 帳戶中的實體 (使用者或角色) 存取權以建立資源。不過，即使他們建立資源也不表示他們會自動擁有存取該資源的完整權限。管理員必須明確為每個動作授予許可。此外，管理員隨時可以撤銷這些許可，只要管理使用者和角色許可。

控制對不同帳戶中委託人的存取

管理員可以使用 AWS 資源型政策、IAM 跨帳戶角色或 AWS Organizations 服務，讓其他帳戶中的主管人員可以存取您帳戶中的資源。

對於某些 AWS 服務，管理員可以授與跨帳戶存取資源的許可。為此，管理員會將政策直接將政策連接到他們要分享的資源，而不是以代理方式使用角色。如果服務支援此政策類型，則管理員共用的資源也必須支援資源型政策。不像以使用者為基礎的政策，以資源為基礎的政策會指定誰可以存取該資源 (以 AWS 帳戶 ID 號碼清單形式)。全域加速器不支援資源類型政策。

以資源為基礎的政策的跨帳戶存取比角色更具有優勢。若使用透過資源型政策存取的資源，委託人 (人員或應用程式) 仍可在信任的帳戶中運作，不需放棄其使用者許可，而代之以角色許可。換言之，委託人可同時在受信任的帳戶和信任的帳戶中存取資源。這對於某些任務很實用，例如從一個帳戶複製資訊到另一個帳戶。如需有關使用跨帳戶角色的詳細資訊，請參閱在您擁有的另一個 AWS 帳戶中提供 IAM 使用者存取權限中的IAM 使用者指南。

AWS Organizations 為您擁有的多個 AWS 帳戶提供以政策為基礎的管理。使用 Organizations，您可以建立帳戶群組、自動化帳戶的建立、套用和管理這些群組的政策。Organizations 可讓您集中管理多個帳戶的政策，而不需要自訂指令碼和手動程序。使用 AWS Organizations，您可以建立服務控制政策 (SCP) 來集中控制 AWS 服務的 AWS 服務使用。如需詳細資訊，請參閱「」什麼是 AWS Organizations？中的AWS Organizations 使用者指南。

什麼是政策？

您可以透過建立政策並將其連接到 IAM 身分或 AWS 資源，在 AWS 中控制存取。

> **Note**
>
> 若要快速開始使用，您可以忽略此頁面。首先，檢閱上的入門資訊AWS Global Accelerator 的 Identity and Access Management，然後參閱入門 IAM。

政策為 AWS 中的一個物件，當與實體或資源相關聯時，會定義它們的許可。當像使用者這類的委託人提出請求時，AWS 會評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式存放在 AWS 中。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，如果原則允許GetUser動作，則具有該政策的使用者可以從 AWS 管理主控台、AWS CLI 或 AWS API 取得使用者資訊。當您建立 IAM 使用者時，您可以設定使用者以允許主控台存取或程式化存取。IAM 使用者可以利用使用者名稱和密碼登入主控台。或者，使用存取金鑰以使用 CLI 或 API。

以下政策類型 (按頻率列出) 會影響請求是否能獲授權。如需詳細資訊，請參閱「」。政策類型中的IAM 使用者指南。

以身分為基礎的政策

您可以將受管和內嵌政策連接到 IAM 身分 (使用者與使用者所屬的群組和角色)。

以資源為基礎的政策

您可以在某些 AWS 服務中將內嵌政策連接到資源。以資源為基礎的政策的最常見範例是 Amazon S3 儲存貯體政策和 IAM 角色信任政策。全域加速器不支援資源類型政策。

Organizations SCP

您可以使用 AWS Organizations 服務控制政策 (SCP) 將許可界限套用到 AWS Organizations 或組織單位 (OU)。這些許可會套用到成員帳戶中的所有實體。

存取控制清單 (ACL)

您可以使用 ACL 控制哪些委託人可以存取資源。ACL 類似以資源為基礎的政策，雖然是不使用 JSON 政策文件結構的唯一政策類型。全域加速器支援 OR 不支援 ACL。

這些政策類型可歸類為許可政策或許可界限。

許可政策

您可以將許可政策連接到 AWS 中的資源來定義該物件的許可。在單一帳戶內，AWS 將所有許可政策一起做評估。許可政策是最常見的政策。您可以使用以下政策類型做為許可政策：

以身分為基礎的政策

當您將受管或內嵌政策連接到 IAM 使用者、群組或角色，該政策會定義實體的許可。

以資源為基礎的政策

當您將 JSON 政策文件連接到資源，您會定義該資源的許可。該服務必須支援以資源為基礎的政策。

存取控制清單 (ACL)

當您將 ACL 連接到資源，您會定義具有存取該資源許可的委託人清單。資源必須支援 ACL。

許可界限

您可以使用政策來定義實體 (使用者或角色) 的許可界限。許可界限控制實體可以擁有的許可上限。許可界限是進階 AWS 功能。當在請求中套用多個許可界限，AWS 會個別評估每個許可界限。您可以在下列情況套用許可界限：

組織

您可以使用 AWS Organizations 服務控制政策 (SCP) 將許可界限套用到 AWS Organizations 或組織單位 (OU)。

IAM 使用者或角色

您可以針對使用者使用受管政策或角色的許可界限。如需詳細資訊，請參閱「」IAM 實體的許可界限中的IAM 使用者指南。

主題

以身分為基礎的政策

您可以將政策連接到 IAM 身分。例如，您可以執行下列操作：

將許可政策連接到您帳戶中的使用者或群組

若要將建立 AWS Global Access 資源 (例如加速器) 的許可授予使用者，您可以將許可政策連接至使用者或使用者所屬的群組。

將許可政策連接至角色 (授予跨帳戶許可)

您可以將以身分為基礎的許可政策連接到 IAM 角色，以授與跨帳戶許可。例如，帳戶 A 管理員可以建立角色，來授予橫跨另一個 AWS 帳戶 (如帳戶 B) 或 AWS 服務的跨帳戶許可，如下所示：

1. 帳戶 A 管理員建立 IAM 角色，並將許可政策連接到可授予帳戶 A 中資源許可的角色。
2. 帳戶 A 管理員會將信任政策連接至將帳戶 B 識別為可擔任角色之委託人的角色。
3. 帳戶 B 管理員接著可將擔任該角色的許可委派給帳戶 B 的任何使用者，如此可讓帳戶 B 的使用者建立或存取帳戶 A 的資源。如果您想要將擔任該角色的許可授予 AWS 服務，則信任政策的委託人也可以是 AWS 服務委託人。

如需使用 IAM 來委派許可的詳細資訊，請參閱存取管理中的IAM 使用者指南。

如需使用者、群組、角色和許可的詳細資訊，請參閱身分 (使用者、群組和角色)中的IAM 使用者指南。

以下是可搭配全域加速器使用的兩個政策範例第一個範例政策授與使用者以程式設計方式存取 AWS 帳戶中加速器的所有「清單」和「說明」動作：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

下列範例會授與程式設計存取`ListAccelerators`操作：

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:ListAccelerators",
            ],
            "Resource": "*"
        }
    ]
}
```

以資源為基礎的政策

以資源為基礎的政策是連接到資源的 JSON 政策文件。以資源為基礎政策則可控制指定委託人在何種條件下對哪些資源執行哪些動作。最常見的資源型政策是 Amazon S3 儲存貯體。資源型政策是只存在於資源上的內嵌政策。不存在受管的以資源為基礎的政策。

使用資源型政策對其他 AWS 帳戶的成員授與權限對於 IAM 角色有一些優勢。如需詳細資訊，請參閱「」IAM 角色與資源類型政策有何差異中的IAM 使用者指南。

原則存取層級分類

在 IAM 主控台，會使用以下存取層級分類來將動作分組：

列出

提供許可來列出服務內資源，以判斷物件是否存在。具有此層級存取權的動作，可以列出物件，但無法查看資源的內容。具有 List (清單) 存取層級的多數動作無法在特定資源上執行。當您使用這些動作建立政策陳述式，您必須指定 All resources (所有資源) ("*")。

閱讀

提供許可來讀取但無法編輯服務內資源的內容和屬性。例如，Amazon S3 操作`GetObject`和`GetBucketLocation`擁有閱讀存取層級。

寫入

提供許可來建立、刪除或修改服務內的資源。例如，Amazon S3 操作`CreateBucket`、`DeleteBucket`，以及`PutObject`擁有寫入存取層級。

許可管理

提供許可來授予或修改服務內的資源許可。例如，大多數 IAM 和 AWS Organizations 政策動作具有許可管理存取層級。

> **Tip**
>
> 為了改善 AWS 帳戶的安全性，請限制或定期監控包含許可管理存取層級分類。

標記

提供許可來建立、刪除或修改附加到服務內資源的標籤。例如，Amazon EC2`CreateTags`和`DeleteTags`操作具有標記存取層級。

入門 IAM

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可讓您安全地管理服務和資源的存取權。IAM 是 AWS 帳戶可享的一項功能，無須額外付費。

> **Note**
>
> 在您開始使用 IAM 之前，請檢閱上的AWS Global Accelerator 的 Identity and Access Management。

當您首次建立 AWS 帳戶，您會先有單一的登入身分，可以完整存取帳戶中所有 AWS 服務與資源。此身分稱為 AWS 帳戶「根使用者」，是藉由您用來建立帳戶的電子郵件地址和密碼以登入並存取。強烈建議您不要以根使用者處理日常作業，即使是管理作業。反之，請遵循僅以根使用者建立您第一個 &IAM; 使用者的最佳實務。接著請妥善鎖定根使用者登入資料，只用來執行少數的帳戶與服務管理作業。

建立 IAM 管理員使用者

為您自己建立一個管理員使用者，並將使用者新增至管理員群組 (主控台)

1. 登入。IAM 主控台作為帳戶擁有者，請選擇根使用者並輸入您的 AWS 帳戶電子郵件地址。在下一頁中，輸入您的密碼。

   > **Note**
   >
   > 強烈建議您遵循使用**`Administrator`**IAM 使用者會遵循並妥善鎖定根使用者登入資料。只在需要執行少數帳戶和服務管理任務時，才以根使用者身分登入。

2. 在導覽窗格中，選擇 Users (使用者)，然後選擇 Add user (新增使用者)。
3. 在 User name (使用者名稱) 中輸入 **`Administrator`**。
4. 選取 AWS Management Console access (AWS 管理主控台存取) 旁的核取方塊。然後選取 Custom password (自訂密碼)，接著在文字方塊中輸入您的新密碼。
5. (選用) 根據預設，AWS 會要求新使用者在第一次登入時建立新密碼。您可以清除 User must create a new password at next sign-in (使用者下次登入必須建立新的密碼) 旁的核取方塊，讓新使用者登入時可以重設密碼。
6. 選擇下一頁: 許可。
7. 在 Set permissions (設定許可) 下，選擇 Add user to group (將使用者新增至群組)。
8. 選擇 Create group (建立群組)。
9. 在 Create group (建立群組) 對話方塊中，請於 Group name (群組名稱) 輸入 **`Administrators`**。
10. 選擇篩選政策，然後選取AWS 託管-工作功能來篩選表格內容。
11. 在政策清單中，選取 AdministratorAccess 的核取方塊。接著選擇 Create group (建立群組)。

> **Note**
>
> 您必須先啟用 IAM 使用者和角色對帳單的存取權，才能使用 `AdministratorAccess` 許可存取 AWS 帳單和成本管理主控台。若要這樣做，請遵循委派對帳單主控台的存取權相關教學課程的步驟 1 中的指示。

12. 回到群組清單，選取新群組的核取方塊。必要時，選擇 Refresh (重新整理) 以顯示清單中的群組。
13. 選擇下一頁: Tags (標籤)。
14. (選用) 藉由附加標籤做為索引鍵/值組，將中繼資料新增至使用者。如需有關在 IAM 中使用標籤的詳細資訊，請參閱標記 IAM 實體中的IAM 使用者指南。
15. 選擇下一頁: 檢閱以查看要新增至新使用者的群組成員資格清單。準備好繼續時，請選擇 Create user (建立使用者)。

您可以使用這個相同的程序建立更多群組和使用者，以及讓使用者能夠存取您的 AWS 帳戶資源。如需了解以政策限制使用者對特定 AWS 資源的許可，請參閱存取管理和政策範例。

為 Global Accelerator 建立委派使用者

若要支援 AWS 帳戶中的多個使用者，您必須委派許可，讓其他人員能夠執行您允許的動作。若要這樣做，請使用者需要的許可建立 IAM 群組，然後在您建立 IAM 使用者時，將 IAM 使用者新增到必要的群

組。您可以使用此程序來設定您整個 AWS 帳戶的群組、使用者和許可。中小型組織最適合使用此解決方案，其中 AWS 管理員可以手動管理使用者和群組。對於大型組織，您可以使用自訂 IAM 角色、聯合, 或單一登入。

在下列程序中，您會建立名為的三個使用者**arnav**、**carlos**，以及**martha**，並附加授與權限的政策，以建立名為**my-example-accelerator**，但僅在接下來的 30 天內。您可以使用這裡提供的步驟，透過不同許可新增使用者。

為另一人建立委派使用者 (主控台)

1. 登入 AWS 管理主控台，然後前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 使用者，然後選擇 新增使用者。
3. 在 User name (使用者名稱) 中輸入 **arnav**。
4. 選擇 Add another user (新增其他使用者) 並為第二個使用者輸入 **carlos**。然後選擇 Add another user (新增其他使用者) 並為第三個使用者輸入 **martha**。
5. 選取AWS 管理主控台存取，然後選取自動產生密碼。
6. 清除 User must create a new password at next sign-in (使用者下次登入必須建立新的密碼) 旁的核取方塊，讓新使用者登入時可以重設密碼。
7. 選擇下一頁: 許可。
8. 選擇 Attach existing policies directly (直接連接現有政策)。您將為使用者建立新的受管政策。
9. 選擇 Create policy (建立政策)。

   Create policy (建立政策) 精靈會在新索引標籤或瀏覽器視窗中開啟。
10. 在 Visual editor (視覺化編輯器) 標籤上，選擇 Choose a service (選擇一項服務)。然後選擇 Global Accelerator。您可用上方的搜尋框來限制服務清單中的結果。

    所以此Service (服務)區段會關閉，並且動作區段會自動開啟。
11. 選擇您要允許的全域加速器動作。例如，若要授予建立加速器的許可，請輸入**globalaccelerator:CreateAccelerator**中的篩選動作文字方塊。當全域加速器動作清單已篩選，請選取**globalaccelerator:CreateAccelerator**。

    全域加速器動作依存取層級分類分組，讓您能夠輕鬆快速地判斷每個動作提供的存取層級。如需詳細資訊，請參閱 原則存取層級分類。
12. 如果在前面步驟中選擇的動作不支援選擇特定資源，則所有資源已為您選取。在該情況下，您不能編輯此區塊。

如果選擇一個或多個支援資源等級許可的動作，視覺化編輯器將在 Resources (資源) 區段列出這些資源類型。選擇您選擇了需要加速器資源類型，選擇是否要為政策輸入特定加速器。

13. 如果您想要針對所有資源允許 `globalaccelerator:CreateAccelerator` 動作，請選擇 All resources (所有資源)。

    如果您想要指定資源，請選擇 Add ARN (新增 ARN)。指定區域和帳戶 ID (或帳戶 ID) (或選擇任何)，然後輸入**`my-example-accelerator`**資源。接著選擇 Add (新增)。

14. 選擇 Specify request conditions (optional) (指定請求條件 (選用))。

15. 選擇加入條件，授與建立加速器的許可在未來 7 天內。假設今天日期為 2019 年 1 月 1 日。

16. 對於 Condition Key (條件金鑰)，請選擇 aws:CurrentTime。這個條件金鑰會檢查使用者提出請求的日期和時間。它會傳回 true，因此只有日期和時間在指定範圍內，才允許 **`globalaccelerator:CreateAccelerator`** 動作。

17. 適用於限定詞，請保留預設值。

18. 若要指定何時開始允許的日期和時間範圍，對於 Operator (運算子)，請選擇 DateGreaterThan。對於 Value (價值)，輸入 **`2019-01-01T00:00:00Z`**。

19. 選擇 Add (新增) 以儲存條件。

20. 選擇 Add another condition (新增其他條件) 來指定結束日期。

21. 按照類似的步驟，指定何時結束允許的日期和時間範圍。對於 Condition Key (條件金鑰)，請選擇 aws:CurrentTime。對於 Operator (運算子)，選擇 DateLessThan。對於 Value (值)，輸入 **`2019-01-06T23:59:59Z`** (第一個日期後 7 天)。然後選擇 Add (新增) 以儲存條件。

22. (選用) 若要查看您正在建立的政策之 JSON 政策文件，請選擇JSON索引標籤。您可以隨時切換 Visual editor (視覺化編輯器) 與 JSON 標籤。但是，如果您進行變更或選擇檢閱政策中的Visual editor (視覺化編輯器)索引標籤上，IAM 可能會調整您的政策結構以針對視覺編輯工具進行最佳化。如需詳細資訊，請參閱「」調整政策結構中的IAM 使用者指南。

23. 完成時，選擇 Review policy (檢閱政策)。

24. 在檢閱政策(用於) 頁面上的名稱，輸入**`globalaccelerator:CreateAcceleratorPolicy`**。對於 Description (說明)，輸入 **`Policy to grants permission to create an accelerator`**。檢閱政策摘要以確認您已授予所需的許可，然後選擇 Create policy (建立政策) 來儲存您的新政策。

25. 返回原始索引標籤或視窗，並重新整理您的政策清單。

26. 在搜尋方塊中，輸入 **`globalaccelerator:CreateAcceleratorPolicy`**。選取新政策旁邊的核取方塊。然後選擇 Next Step (下一步)。

27. 選擇下一頁: 檢閱預覽您的新使用者。準備好繼續時，請選擇 Create user (建立使用者)。
28. 下載或複製新使用者的密碼，並安全地將其傳送給使用者。另外，為使用者提供連結至您的 IAM 使用者主控台頁面和您剛建立的使用者名稱。

允許使用者自行管理其認證

您必須擁有實體存取託管使用者的虛擬 MFA 裝置的硬體，才能設定 MFA。例如，您可以為使用者設定 MFA，該使用者將使用在智慧型手機上執行的虛擬 MFA 裝置。在這種情況下，您必須有可用的智慧型手機，才能完成精靈。因此，您可能想要讓使用者設定和管理自己的虛擬 MFA 裝置。在這種情況下，您必須授與使用者執行必要 IAM 動作的許可。

建立政策以允許登入資料自我管理 (主控台)

1. 登入 AWS 管理主控台，然後前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 Policies (政策)，然後選擇 Create policy (建立政策)。
3. 選擇 JSON 標籤並從下列 JSON 政策文件複製文字。將此文字貼上至 JSON 文字方框中。

> **Important**
>
> 本範例政策不允許使用者在登入時重設密碼。新使用者和密碼過期的使用者可以執行此操作。您可以透過將 `iam:ChangePassword` 和 `iam:CreateLoginProfile` 新增至 `BlockMostAccessUnlessSignedInWithMFA` 陳述式，來允許這項作業。但是，IAM 不建議執行此作業。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid":
"AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:DeleteAccessKey",
                "iam:DeleteLoginProfile",
                "iam:GetLoginProfile",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey",
                "iam:UpdateLoginProfile",
                "iam:ListSigningCertificates",
                "iam:DeleteSigningCertificate",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate",
                "iam:ListSSHPublicKeys",
                "iam:GetSSHPublicKey",
                "iam:DeleteSSHPublicKey",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowIndividualUserToViewAndManageTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
```

```
            "Sid":
 "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        },
        {
            "Sid": "BlockMostAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:ListVirtualMFADevices",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice",
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListSSHPublicKeys",
                "iam:ListAccessKeys",
                "iam:ListServiceSpecificCredentials",
                "iam:ListMFADevices",
                "iam:GetAccountSummary",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

此政策的功能為何？

- 所以此AllowAllUsersToListAccounts陳述式可讓使用者在 IAM 主控台中查看帳戶及其使用者的基本資訊。這些許可必須位於自己的陳述式中，因為它們不支援或不需要指定特定的資源 ARN，而需要指定 "Resource" : "*"。
- 所以此AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation陳述式可讓使用者在 IAM 主控台中管理自己的使用者、密碼、存取金鑰、簽章憑證、SSH 公有金鑰和 MFA 資訊。還允許使用者首次登錄，管理員要求使用者設置首次密碼。資源 ARN 僅限在使用者自己的 IAM 使用者實體中使用這些許可。
- 第 AllowIndividualUserToViewAndManageTheirOwnMFA 個陳述式讓使用者預先檢視或管理其 MFA 裝置。請注意，此陳述式中的資源 ARN 僅允許存取 MFA 裝置，或者與目前登入使用者完全同名的使用者。使用者不能建立或更改除自己裝置外的任何 MFA 裝置。
- 使用者可以透過第 AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA 個陳述式單獨停用自己的 MFA 裝置 (僅在使用者使用 MFA 登入時)。這可防止僅具有存取金鑰 (沒有 MFA 裝置) 的其他使用者停用 MFA 裝置，並存取其帳戶。
- 所以此BlockMostAccessUnlessSignedInWithMFA陳述式會使用"Deny"和"NotAction"拒絕存取 IAM 和其他 AWS 服務中的一些動作以外的所有動作如使用者未使用 MFA 登入。如需更多此陳述式邏輯的資訊，請參閱帶拒絕的 NotAction中的IAM 使用者指南。如果使用者使用 MFA 登入，則 "Condition" 測試失敗，最後一個「拒絕」陳述式失效；使用者的政策或陳述式可能會判斷使用者的許可。此陳述式可確保當使用者日後不使用 MFA 登入時，他們只能執行所列的動作，而且只有在另一個陳述式或政策允許存取這些動作時才行。

  ...IfExists 運算子的 Bool 版本會確認，如果 aws:MultiFactorAuthPresent 金鑰遺失，條件將返回 true。這就表示，拒絕使用長期登入資料 (如存取金鑰) 存取 API 的使用者存取為非 IAM API 操作。

4. 完成時，選擇 Review policy (檢閱政策)。
5. 在 Review (檢閱) 頁面上，針對政策名稱輸入 **Force_MFA**。如需政策描述，請輸入**This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.**檢閱政策摘要以查看您的政策授予的許可，然後選擇建立政策儲存您的工作。

   新的政策會出現在受管政策清單中，並且已準備好連接。

將政策連接至使用者 (主控台)

1. 在導覽窗格中，選擇 Users (使用者)。
2. 選擇您要編輯的使用者的名稱 (而非核取方塊)。
3. 在 Permissions (許可) 標籤上，選擇 Add permissions (新增許可)。
4. 選擇 Attach existing policies directly (直接連接現有政策)。
5. 在搜尋方塊中，輸入 **`Force`**，然後在清單中選擇 Force_MFA 旁的核取方塊。然後選擇 Next (下一步)：檢閱。
6. 檢閱您的變更，然後選擇 Add permissions (新增許可)。

為 IAM 使用者啟用 MFA

為了提高安全性，我們建議所有 IAM 使用者設定多重驗證 (MFA) 以協助保護您的全球加速器資源。MFA 可增加額外的安全，因為它會要求使用者在標準登入資料外，從支援 AWS 的 MFA 裝置提供唯一的身份驗證。最安全的 AWS MFA 裝置是 U2F 安全金鑰。如果您的公司已有 U2F 裝置，則我們建議您為 AWS 啟用這些裝置。否則，您必須為每個使用者購買裝置，並等待硬體送達。如需詳細資訊，請參閱「」啟用 U2F 安全金鑰中的IAM 使用者指南。

如果您還沒有 U2F 裝置，您可以啟用虛擬 MFA 裝置，以低成本的方式快速開始。這需要您在現有的手機或其他行動裝置上安裝軟體應用程式。裝置會根據時間同步的一次性密碼演算法產生六位數字代碼。當使用者登入 AWS，會收到提示輸入裝置的代碼。每個指派給使用者的虛擬 MFA 裝置都必須是唯一的。使用者無法輸入另一個使用者虛擬 MFA 裝置的代碼來進行身份驗證。如需可以用來做為虛擬 MFA 裝置的支援應用程式清單，請參閱 Multi-Factor Authentication。

> **Note**
>
> 您必須擁有實體存取託管使用者虛擬 MFA 裝置的行動裝置的行動裝置，才能為 IAM 使用者設定 MFA。

針對 IAM 使用者啟用虛擬 MFA 裝置 (主控台)

1. 登入 AWS 管理主控台，然後前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 Users (使用者)。
3. 在 User Name (使用者名稱) 清單中，選擇適用的 MFA 使用者名稱。
4. 選擇 Security credentials (安全登入資料) 標籤。在 Assigned MFA device (指派的 MFA 裝置) 旁，選擇 Manage (管理)。

5. 在 Manage MFA Device (管理 MFA 裝置) 精靈中，選擇 Virtual MFA device (虛擬 MFA 裝置)，然後選擇 Continue (繼續)。

   IAM 會產生並顯示虛擬 MFA 裝置的配置資訊，包括 QR 代碼圖形。此圖形代表「私密組態金鑰」，可用來在不支援 QR 碼的裝置上手動輸入。

6. 開啟您的虛擬 MFA 應用程式。

   如需可以用於託管虛擬 MFA 裝置的應用程式清單，請參閱 Multi-Factor Authentication。如果虛擬 MFA 應用程式支援多個帳戶 (多個虛擬 MFA 裝置)，請選擇對應的選項以建立新帳戶 (新的虛擬 MFA 裝置)。

7. 判定 MFA 應用程式是否支援 QR 碼，然後執行以下操作之一：

   - 從精靈中，選擇 Show QR code (顯示 QR 碼)，然後使用應用程式掃描 QR 碼。例如，您可選擇相機圖示或選擇與 Scan code (掃描代碼) 類似的選項，然後使用裝置的相機掃描此代碼。
   - 在 Manage MFA Device (管理 MFA 裝置) 精靈中，選擇 Show secret key (顯示私密金鑰)，然後在您的 MFA 應用程式中輸入私密金鑰。

   完成操作後，虛擬 MFA 裝置會開始產生一次性密碼。

8. 在 Manage MFA Device (管理 MFA 裝置) 精靈中的 MFA code 1 (MFA 代碼 1) 方塊內，輸入虛擬 MFA 裝置上目前顯示的一次性密碼。請等待 30 秒，裝置將產生新的一次性密碼。然後將第二個一次性密碼輸入 MFA code 2 (MFA 代碼 2) 方塊中。選擇 Assign MFA (指派 MFA)。

   > **Important**
   >
   > 產生代碼之後立即提交您的請求。如果在產生代碼後等待很長時間才提交請求，MFA 裝置會成功地與使用者建立關聯，但 MFA 裝置不同步。會發生這種情況是因為定時式的一次性密碼(TOTP) 在過了一段短期時間候到期。這種情況下，您可以重新同步裝置。如需詳細資訊，請參閱「」重新同步虛擬及硬體 MFA 裝置中的IAM 使用者指南。

   虛擬 MFA 裝置現已準備好與 AWS 一起使用。

AWS Global Accelerator 中的安全 VPC 連線

當您在 AWS Global Accelerator 中新增內部 Application Load Balancer 或 Amazon EC2 執行個體終端節點時，您可以將網際網路流量定位在私有子網路中，以便直接進出虛擬私有雲 (VPC) 的終端節點。

包含負載平衡器或 EC2 執行個體的 VPC 必須具備網際網路閘道連接到它，以表明 VPC 接受互聯網流量。但是，您不需要負載平衡器或 EC2 執行個體上的公用 IP 位址。您也不需要子網路相關聯的網際網路閘道路由。

這與典型的網際網路閘道使用案例不同，在這種情況下，網際網路流量需要公用 IP 位址和網際網路閘道路由，才能流向 VPC 中的執行個體或負載平衡器。即使目標的彈性網路介面存在於公用子網路 (也就是具有網際網路閘道路由的子網路)，當您針對網際網路流量使用全域加速器時，全域加速器會覆寫一般的網際網路路由，以及透過全域加速器也會透過全域加速器傳回，而非透過網際網路閘道傳回。

> **Note**
>
> 對 Amazon EC2 執行個體使用公有 IP 地址和使用公有子網路並不典型，但可以使用這些執行個體設定您的組態。安全群組適用於到達執行個體的任何流量，包括來自全域加速器的流量，以及指派給執行個體 ENI 的任何公用或彈性 IP 位址。使用私人子網路，確保流量僅由全域加速器傳遞。

考慮網路周邊問題並設定與網際網路存取管理相關的 IAM 權限時，請記住此資訊。如需控制 VPC 的網際網路存取的詳細資訊，請參閱此服務控制政策範例。

AWS Global Accelerator 中的記錄和監控

監控功能是維護全球加速器和您 AWS 解決方案之可靠性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便更輕鬆地除錯出現的多點故障。AWS 提供多種工具來監控全球加速器資源和活動，以及回應潛在事件：

AWS Global Accelerator 流量日誌

伺服器流程記錄提供有關流經加速器至端點之流量的詳細記錄。伺服器流程日誌對許多應用程式來說，都是個 例如，流程記錄資訊在安全與存取稽核中相當實用。如需詳細資訊，請參閱 AWS Global Accelerator 中的流程日誌。

Amazon CloudWatch 指標和警示

您可以使用 CloudWatch 來即時監控您的 AWS 資源以及在 AWS 上執行的應用程式。CloudWatch 會收集並追蹤指標，這些指標是您隨著時間而測量的變數。您可以建立警示來監控特定指標，然後在指標超過特定閾值時，傳送通知或自動變更您所監控的資源。如需詳細資訊，請參閱 搭配 AWS Global Accelerator 使用 Amazon CloudWatch。

AWS CloudTrail 日誌

CloudTrail 會提供由使用者、角色或 AWS 服務在全球加速器中採取動作的記錄。CloudTrail 會將針對全球加速器的所有 API 呼叫擷取為事件，包括自全球加速器主控台以及自程式碼呼叫對全球加速器 API 的呼叫。如需詳細資訊，請參閱 使用 AWS CloudTrail 記錄 AWS Global Accelerator API 呼叫。

AWS Global Accelerator 的合規驗證

在多個 AWS 合規計畫中，第三方稽核人員會評估 AWS Global Accelerator 的安全與合規。這些包括 SOC、PCI、HIPAA、GDPR、ISO 等。

如需特定合規計劃的 AWS 服務範圍清單，包括全球加速器，請參閱合規計劃的 AWS 服務範圍。如需一般資訊，請參閱 AWS 合規計劃。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱「」下載 AWS Artifact 中的報告。

您使用全球加速器的合規責任，取決於資料的機密性、您公司的合規目標及適用法律和法規。AWS 提供下列資源，以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心基準環境的架構考量和步驟。
- HIPAA 安全與合規架構白皮書 – 本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- AWS 合規資源 – 這組手冊和指南可能適用於您的產業和位置。
- 使用規則評估資源中的AWS Config 開發人員指南-AWS Config 服務評定資源組態符合內部實務、業界準則和法規的程度。
- AWS 安全中樞 – 此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。

AWS Global Accelerator 的彈性

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域與可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了支援 AWS 全球基礎設施外，全球加速器還提供下列支援資料復原的功能：

- 網路區域服務來自唯一 IP 子網路的加速器的靜態 IP 位址。與 AWS 可用區域類似，網路區域是具有自己一組實體基礎設施的隔離單元。當您設定加速器時，全域加速器會為其配置兩個 IPv4 位址。如果某個網路區域的某個 IP 位址因為某些用戶端網路的 IP 位址封鎖或網路中斷而變得無法使用，則用戶端應用程式可以從其他隔離網路區域重試健全的靜態 IP 位址。
- 全域加速工具會持續監控所有端點的運作狀態。當它判斷主動端點狀況不良時，全域加速器會立即開始將流量導向另一個可用端點。這可讓您為 AWS 上的應用程式建立高可用性架構。

AWS Global Accelerator 的基礎設施安全

AWS Global Accelerator 是受管服務，受到 AWS 全球網路安全程序的保護，如Amazon Web Services：安全程序概觀白皮書。

您可使用 AWS 發佈的 API 呼叫，透過網路存取全球加速器。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。此外，請求必須使用存取金鑰 ID 和與 IAM 委託人相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全登入資料來簽署請求。

AWS Global Accelerator 的配額

您的 AWS 帳戶具有與 AWS Global Accelerator 相關的特定配額 (也稱為限制)。

Service Quotas 主控台提供了有關「全域加速器」配額的資訊。除了檢視預設配額之外，您還可以使用 Service Quotas 主控台來要求配額增加以取得可調整的配額。請注意，當您要求全域加速器的配額增加時，您必須位於美國東部 (維吉尼亞北部)。

主題

一般配額

以下是全域加速器的整體配額。

實體	Quota
每個 AWS 帳戶的加速器	20 您可以請求提高配額。
每個加速器的監聽程式	10 您可以請求提高配額。
每個監聽器的連接埠範	10
每個端點群組的連接埠覆寫	10 您可以請求提高配額。

每個端點群組的端點配額

以下是適用於端點群組中端點數目的全域加速器配額。

實體	描述	Quota
具有多個端點類型的端點群組	端點群組中包含多個端點類型的端點數目。	10
僅使用應用程式負載平衡器的端點群組	僅包含 Application Load Balancer 端點的端點群組中的應用程式負載平衡器數目。	10
僅使用網路負載平衡器的端點群組	僅包含 Network Load Balancer 端點的端點群組中的網路負載平衡器數目。	10
僅含 Amazon EC2 執行個體的端點群組	端點群組中僅包含 EC2 執行個體端點的 EC2 執行個體數。	10 您可以請求提高配額。
僅具有彈性 IP 位址的端點群組	僅包含彈性 IP 位址端點的端點群組中彈性 IP 位址數目。	10 您可以請求提高配額。
僅具有 Amazon Virtual Private Cloud 子網路的端點群組	僅包含子網路端點的端點群組中的 Amazon VPC 子網路數目。	10 您可以請求提高配額。

相關配額

除了 Global Accelerator 中的配額之外，還有一些配額可套用至您用作加速器端點的資源。如需詳細資訊，請參閱下列內容：

- 彈性 IP 地址配額中的Amazon EC2 使用者指南。
- Amazon EC2 服務配額中的Amazon EC2 使用者指南。
- 網路負載平衡器的配額中的網路負載平衡器使用者指南。
- Application Load Balancer 的配額中的Application Load Balancer 使用者指南。
- Amazon VPC 配額中的Amazon VPC 使用者指南。

AWS Global Accelerator 相關資訊

此處所列的資訊與資源可協助您進一步了解 Global Accelerator。

主題

- AWS Global Accelerator 加速器
- 取得支援
- Amazon Web Services 部落格的秘訣

AWS Global Accelerator 加速器

以下相關資源可協助您使用此服務。

- AWS Global Accelerator API 參考— 提供 API 動作、參數和資料類型的完整說明，以及服務會傳回的錯誤清單。
- AWS Global Accelerator 產品資訊— 提供 Global Accelerator 相關資訊的主要網頁，包括其功能與定價資訊。
- 使用條款— 我們的著作權與商標；您的帳戶、授權與網站存取；以及其他主題的詳細資訊。

取得支援

Support 全域加速器有數種形式。

- 開發論壇— 由社群參與的論壇，可讓開發人員討論 Global Accelerator 的相關技術問題。
- AWS 支援中心 – 此網站匯集了關於您近期支援案例的資訊，和 AWS Trusted Advisor 與運作狀態檢查的結果，並提供連結，可連到開發論壇、技術常見問答集、服務運作狀態儀表板，以及 AWS 支援方案的相關資訊。
- AWS Premium Support 資訊 – 提供 AWS Premium Support 相關資訊的主要網頁，AWS Premium Support 是一對一的快速回應支援服務管道，可幫助您在 AWS Infrastructure Services 上建置和執行應用程式。
- 聯絡我們 – 用來查詢帳單或帳戶相關問題的連結。對於技術問題，請使用上述開發論壇或支援連結。

Amazon Web Services 部落格的秘訣

AWS 部落格有許多文章，以協助您使用 AWS 服務。例如，請參閱以下有關 Global Accelerator 部落格文章：

- 適用於可用性和效能的 AWS Global Accelerator
- AWS Global Accelerator 加速器
- 使用亞馬遜雅典和亞馬遜 QuickSight 分析 AWS Global Accelerator 流程日誌並視覺化

如需 AWS Global Accelerator 部落格的完整清單，請參閱AWS Global Accelerator在 AWS 部落格文章的 [聯網和內容交付] 類別中。

文件歷史記錄

以下項目說明 AWS Global Accelerator 文件中的重要變更。

- API 版本：最新
- 文件最新更新時間：2020 年 12 月 9 日

變更	描述	日期
全域加速器現有服務連結角色的更新	全域加速器新增了新的權限`ec2:DescribeRegions` ，以允許全域加速器取得 AWS 區域資訊以協助診斷錯誤。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html。	2021 年 5 月 7 日
新增自訂路由加速器	全域加速器推出了新類型的加速器自訂路由加速器。自訂路由加速器適用於您想要使用自訂應用程式邏輯，將一或多位使用者導向特定目的地和連接埠，同時仍可取得全域加速器的效能優勢的案例。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html。	2020 年 12 月 9 日
新增連接埠覆寫支援	全域加速器現在支援覆寫用於將流量路由傳送至端點的接聽程式連接埠，以便您可以將流量重新路由傳送至端點	2020 年 10 月 21 日

變更	描述	日期
	上的特定連接埠。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html。	
新增兩種區域	Global Accelerator 現已支援非洲 (開普敦) 和歐洲 (米蘭)。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html。	2020 年 5 月 20 日
標籤與 BYOIP	此版本新增支援將標籤新增至加速器，以及將您自己的 IP 位址帶入 AWS Global Accelerator (BYOIP)。如需更多詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html 及 https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html。	2020 年 2 月 27 日
已更新安全性章節	新增符合性、恢復能力和基礎結構安全性的內容。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html。	2019 年 12 月 20 日

變更	描述	日期
Support EC2 執行個體和預設 DNS 名稱	AWS Global Accelerator 現在支援在支援的 AWS 區域中新增 EC2 執行個體。此外，全域加速器會建立預設 DNS 名稱，該名稱對應至加速器的靜態 IP 位址。如需更多詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html 及 https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing。	2019 年 10 月 29 日
保留應用程式負載平衡器的用戶端 IP 位址	您現在可以選擇讓 AWS Global Accelerator 在支援的 AWS 區域中保留應用程式負載平衡器的用戶端 IP 位址。如需詳細資訊，請參閱 https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html。	2019 年 8 月 28 日
AWS Global Accelerator 服務發行	AWS Global Accelerator 開發人員指南提供有關設定和使用加速器 (網路層流量管理員) 的資訊，以改善具有全球使用者的網際網路應用程式的可用性和效能。	2018 年 11 月 26 日

AWS 詞彙表

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。