aws

VPC對等互連

Amazon Virtual Private Cloud

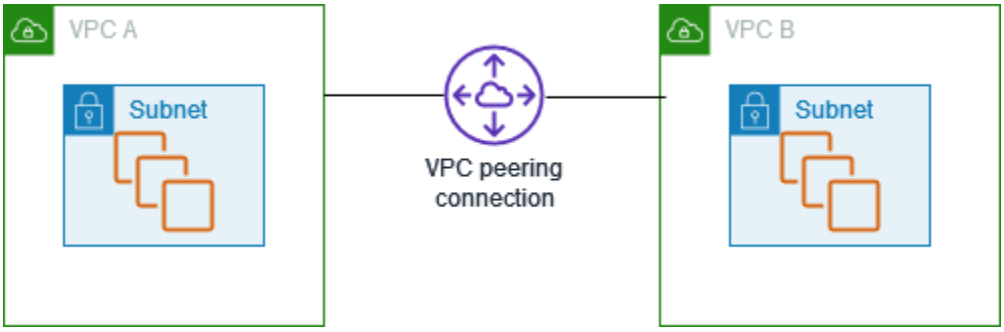
Amazon Virtual Private Cloud: VPC對等互連

Table of Contents

什麼是VPC對等互連？

虛擬私有雲 (VPC) 是專用於您的 AWS 帳戶. 它在邏輯上與 AWS 雲中的其他虛擬網絡隔離。您可以啟動 AWS 資源，例如 Amazon EC2 執行個體，到您的VPC.

VPC對等連線是兩者之間的網路連線，可VPCs讓您使用私人IPv4位址或IPv6位址在它們之間路由流量。其中一個執行個體都VPC可以彼此通訊，就像它們位於同一個網路中一樣。您可以在自己的帳戶之間建立VPC對等連線VPCs，或VPC在其他 AWS 帳戶中建立對等連線。VPCs可以位於不同的區域(也稱為區域間VPC對等連線)。



AWS 使用 a 的現有基礎結構VPC來建立VPC對等連接；它既不是閘道器也不是VPN連接，也不依賴於單獨的實體硬體。因此不會有通訊的單一故障點或頻寬瓶頸問題。

VPC對等連接可幫助您促進數據的傳輸。例如，如果您有一個以上的 AWS 帳戶，您可以VPCs在這些帳戶之間對等以建立檔案共用網路。您還可以使用VPC對等連接來允許其他VPCs人訪問您VPCs在其中一個.

當您在不同區域之間建立對等關係時，不VPCs同 AWS 區域中的資源 VPCs (例如，EC2執行個體和 Lambda 函數) 可以使用私有 IP 地址彼此通訊，而無需使用閘道、VPN連線或網路設備。 AWS 流量會保留在私人 IP 位址空間中。所有區域間流量都經過加密，沒有單一故障點或頻寬瓶頸問題。流量始終保持在全球 AWS 骨幹網上，並且永遠不會遍歷公共互聯網，從而減少了常見漏洞和攻擊等威脅。DDoS區域間VPC對等提供簡單且經濟實惠的方式，可在區域之間共用資源或複寫資料以提供地理備援。

對VPC等連線的定價

建立VPC對等連線無須付費。所有透過VPC對等連線保留在可用區域內的資料傳輸 (即使在不同帳戶之間) 都是免費的。透過跨可用區域和區域的VPC對等連線傳輸資料需支付費用。如需詳細資訊，請參閱 Amazon EC2 定價 。

VPC對等程序、生命週期和限制

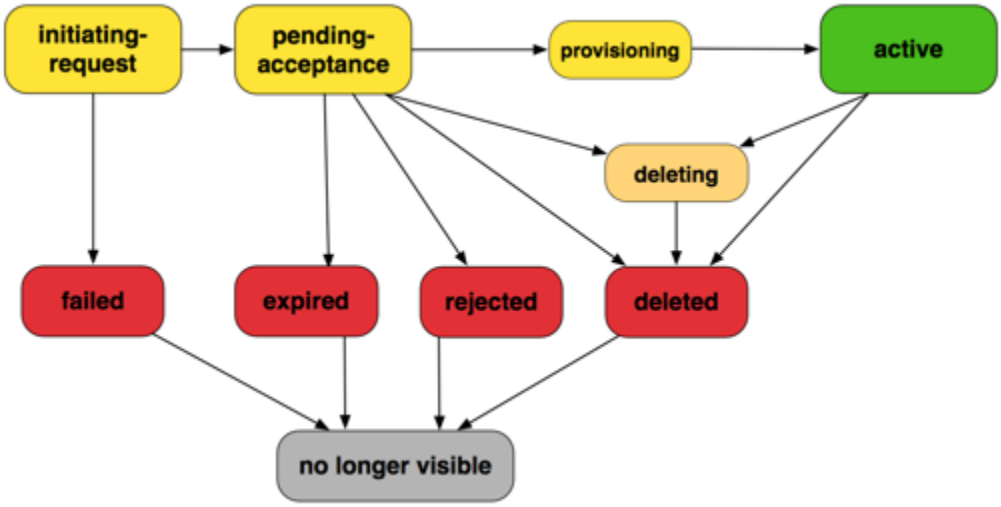
若要建立VPC對等連線，請執行下列動作：

1. 請求者的擁有者VPC會傳送請求給接受者的擁有者，VPC以建立對等連線。VPC接受者VPC可以由您或其他 AWS 帳戶擁有，且不能擁有與請求者CIDR區塊重疊的CIDR區塊。VPC
2. 接受者的擁有者VPC接受VPC對等連線要求，以啟動對等連線。VPC
3. 若要啟VPCs用使用私有 IP 位址之間的流量流量，對等連線VPC中每個位址的VPC擁有者必須手動新增路由至一或多個VPC路由表，該路由表指向另一個 VPC (對等端VPC) 的 IP 位址範圍。
4. 如有必要，請更新與EC2執行個體相關聯的安全群組規則，以確保進出對等的流量VPC不受限制。如果兩者VPCs都位於相同的區域中，您可以參考對等中的安全性群組，VPC作為安全性群組中輸入或輸出規則的來源或目的地。
5. 使用預設VPC對等連線選項時，如果對等連線兩端的EC2執行個VPC體使用公用DNS主機名稱互相連接，則主機名稱會解析為執行個體的公用 IP 位址。EC2若要變更此行為，請啟用VPC連線的DNS主機名稱解析。啟用DNS主機名稱解析後，如果對等連線任一端的EC2執行個體使用公用DNS主機名稱VPC彼此相互連接，則主機名稱會解析為EC2執行個體的私有 IP 位址。

如需詳細資訊，請參閱使用VPC對等連接。

VPC對等連線生命週期

VPC對等連線會經過各個階段，從要求起始時開始。在每個階段，您可以採取動作，而在其生命週期結束時，VPC對等連線會在 Amazon VPC 主控台和/API或命令列輸出中保持可見一段時間。



- 起始要求：已啟動對VPC等連線的要求。在此階段中，對等連線可能失敗或可能移至 pending-acceptance。
- 失敗：對VPC等連線的要求失敗。在此狀態期間，無法接受、拒絕或刪除該連線。失敗的VPC對等連線會在 2 小時內對要求者顯示。
- 暫VPC緩允收：對等連線請求正在等待接收者擁有者的允收。VPC在此狀態期間，請求者的擁有者VPC可以刪除要求，且接受者的擁有者VPC可以接受或拒絕要求。如果未對此請求採取任何動作，該請求會在 7 天後過期。
- 已過期：VPC對等連線要求已過期，任一VPC擁有者都無法對其採取任何動作。兩個VPC擁有者都可以看到過期的對VPC等連線 2 天。
- 已拒絕：接受者的擁VPC有者已拒絕pending-acceptanceVPC對等連線請求。在此狀態期間無法接受請求。拒絕的VPC對等連線會在請求者的擁有者看到 2 天內，且接受者的擁有者可以看見 2 小VPCVPC時。如果要求是在相同 AWS 帳戶中建立，則拒絕的要求會在 2 小時內保持可見。
- 佈建：VPC對等連線要求已接受，且即將進入狀active態。
- 作用中：VPC對等連線處於作用中狀態，流量可以在 VPCs (前提是您的安全性群組和路由表允許流量流動) 之間流動。處於此狀態時，任一VPC擁有者都可以刪除VPC對等連線，但無法拒絕它。

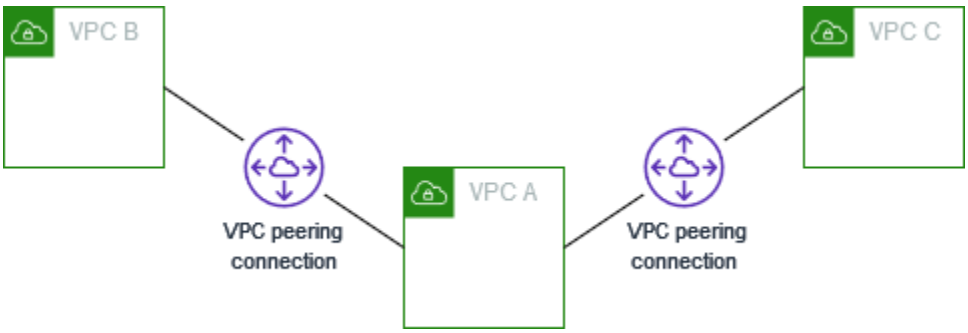
> **Note**
>
> 如果VPC所在區域中的某個事件阻止流量流動，VPC對等連線的狀態仍Active會保留。

- 刪除：套用至正在刪除的區域間VPC對等連線。的擁VPC有者已提交刪除activeVPC對等連線的請求，或者請求者的擁VPC有者已提交刪除pending-acceptanceVPC對等連線要求的請求。
- 已刪除：其中一個擁有者已刪除activeVPC對等連線，或VPC者要求者的擁有者已刪除pending-acceptanceVPC對等連線要求。VPC處於此狀態時，無VPC法接受或拒絕對等連線。刪除VPC對等連線的對等連線 2 小時後仍可看見，對方可見 2 天。如果VPC對等連線是在相同 AWS 帳戶中建立的，則刪除的要求會在 2 小時內保持可見。

多個VPC對等連接

VPC對等連接是兩VPCs個之間的一對一關係。您可以為每VPC個自己擁有的VPC連接建立多個對等連接，但不支援轉移對等關係。您沒有與您沒有直接對等VPCs的VPC任何對等關係。

下圖是一個對VPC等於兩個不同VPCs的示例。有兩種VPC對等連線：VPCA 是對等的，VPCB 與 C 和 VPC VPC C 都不是對等連線，而且不能使用 VPC A 做為 VPC B 與 C 之間對等互連的傳輸點。如果您想要啟用 VPC VPC B 和 VPC VPC C 之間的流量路由，則必須在它們之間建立唯一的VPC對等連線。



VPC對等限制

請考慮下列對VPC等連線的限制。在某些情況下，您可以使用傳輸閘道附件而非VPC對等連線。如需詳細資訊，請參閱 Amazon VPC 傳輸閘道中的範例。

連線

- 每VPC個使用中和擱置的對等VPC連線數目都有配額。如需詳細資訊，請參閱配額。
- 兩個連線之間不能同時有一個以VPCs上的VPC對等連線。
- 您為對VPC等連線建立的任何標記只會套用在您建立對等連線的帳戶或地區。
- 您無法在對等伺服器中連線或查詢 Amazon DNS 伺服器VPC。
- 如果對VPC等連線VPC中的IPv4CIDR區塊落在 RFC1918 所指定的私人IPv4位址範圍之外，則該對等連線的私人DNS主機名稱VPC無法解析為私有 IP 位址。若要將私人DNS主機名稱解析為私人 IP 位址，您可以啟用對VPC等連線的解DNS析度支援。如需詳細資訊，請參閱啟用對VPC等連線的DNS解析度。
- 您可以啟用VPC對等連線任一端的資源，以便透過IPv6通訊。您必須將IPv6CIDR區塊與每個區塊建立關聯VPC、啟用中的執行個體VPCs進行IPv6通訊，以及路由傳VPC送用於對等連線的VPC對等連線的IPv6流量。
- 不VPC支援對等連線中的單點傳送反向路徑轉送。如需詳細資訊，請參閱回應流量的路由。

重疊CIDR圖塊

- 您無法在具有相符或重疊IPv4或IPv6CIDR區塊VPCs之間建立對VPC等連線。
- 如果您有多個IPv4CIDR區塊，即使您打算只使用非重疊的CIDR區塊或僅IPv6CIDR使用區CIDR塊，也無法建立對VPC等連線。

轉移互連

- VPC對等不支援傳遞對等關係。例如，如果 A 和 VPC B 之間存在VPC對等連線，並且在 VPC VPC A 和 VPC C 之間存在對等連線，則無法透過 VPC A 將流量從 VPC B 路由傳送到 VPC C。若要在 VPC B 和 VPC C 之間路由流量，您必須在它們之間建立VPC對等連線。如需詳細資訊，請參閱三個 VPCs凝聚在一起。

透過閘道或私有連線的邊緣至邊緣路由

- 如果 VPC A 有一個互聯網網關，VPCB 中的資源不能使用 VPC A 中的互聯網網關訪問互聯網。
- 如果 VPC A 的NAT設備提供對 VPC A 中子網絡的 Internet 訪問，則 VPC B 中的資源無法使用 VPC A 中的NAT設備訪問互聯網。
- 如果 VPC A 與公司網路有VPN連線，VPCB 中的資源就無法使用VPN連線與公司網路通訊。
- 如果 VPC A AWS Direct Connect 連接到公司網絡，則 VPC B 中的資源無法使用該 AWS Direct Connect 連接與公司網絡進行通信。
- 如果 VPC A 的閘道端點提供連線到 VPC A 中私有子網路的 Amazon S3，則 VPC B 中的資源無法使用閘道端點存取 Amazon S3。

區域間VPC對等連接

- 跨區域VPC對等連線的最大傳輸單位 (MTU) 為 1500 位元組。區域間對VPC等連線不支援巨型框架 (MTUs最多 9001 位元組)。不過，相同區域中的對VPC等連線支援這些連線。如需有關巨型框架的詳細資訊，請參閱 Amazon EC2 使用者指南中的巨型框架 (9001MTU)。
- 您必須啟用對VPC等連線的解DNS析度支援，才能解析對等至私有 IP 位址的私人DNS主機名稱，即使用的VPC屬IPv4CIDR於 19 VPC 18 所指定的私人位IPv4址範圍也一樣。RFC

共用VPCs和子網路

- 只VPC有擁有者可以使用 (描述、建立、接受、拒絕、修改或刪除) 對等連線。參與者無法使用對等連線。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的VPC與其他帳戶共用。

使用VPC對等連接

VPC對等互連可讓您連接相同或不同 AWS 區域VPCs中的兩個。這可讓其中一個執行個VPC體與另一個執行個體進行通訊，就VPC像它們都是同一個網路的一部分一樣。

VPC對等互連會VPCs使用私人IPv4位址或IPv6位址，在兩者之間建立直接網路路由。連線之間傳送的流量VPCs不會遍歷網際網路、VPN連線或 AWS 直 Connect 連線連線。這讓VPC對等互連成為跨VPC界限共用資源 (例如資料庫或 Web 伺服器) 的安全方式。

若要建立VPC對等連線，您可以從一個對等連線要求建立對等連線要求，VPC並讓另一個連線的擁有者接受該要求。VPC建立連線之後，您可以更新路由表，以在VPCs. 這可讓其中一個執行個體存VPC取另一個執行個體中的資源VPC。

VPC對等互連是建置多重VPC架構和跨組織界限共用資源的重要工具。 AWS它提供了一種簡單、低延遲的連線方式，VPCs無需設定VPN或其他網路服務的複雜性。

請使用下列程序來建立和使用VPC對等連線。

任務

- 檢視您的VPC對等連線
- 建立或刪除對VPC等連線
- 接受或拒絕對VPC等連線
- 更新對VPC等連線的路由表
- 更新您的安全群組以參考對等安全群組
- 啟用對VPC等連線的DNS解析度
- 疑難排解VPC對等連線

檢視您的VPC對等連線

您可以在 Amazon VPC 主控台VPC中檢視所有對等連線。依預設，主控台會顯示處於不同狀態的所有VPC對等連線，包括最近刪除或拒絕的連線。如需對VPC等連線生命週期的詳細資訊，請參閱VPC對等連線生命週期。

若要檢視您的VPC對等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 系統會列出所有VPC對等連線。使用篩選條件搜尋列，以縮小搜尋結果。

使用指令列或描述VPC對等連線 API

- describe-vpc-peering-connections (AWS CLI)
- Get-EC2VpcPeeringConnections (AWS Tools for Windows PowerShell)
- DescribeVpcPeeringConnections（Amazon EC2 查詢API）

建立或刪除對VPC等連線

若要建立VPC對等連線，請先建立與另一個VPC對等連線的要求。您可以要求與您帳戶VPC中的其他人建立VPC對等連線，或使用不同 AWS 帳戶的VPC對等連線。對於位於不VPC同區域的區域間對VPCs等連線，請求必須從請求者的「區域」提出。VPC

要激活請求，接受者的所有者VPC必須接受請求。對於區域間VPC對等連線，請求必須在接受者的「區域」中接受。VPC如需詳細資訊，請參閱the section called “接受或拒絕”。如需 `Pending acceptance` 對等互連狀態的詳細資訊，請參閱 VPC對等連線生命週期。

任務

- 必要條件
- VPCs在同一帳戶和區域中創建
- VPCs在同一個帳戶和不同地區創建
- VPCs在不同的帳戶和相同的區域中創建
- VPCs在不同的帳戶和區域中創建
- 使用指令列建立VPC對等連線
- 刪除對VPC等連線

必要條件

- 檢閱對VPC等連線的限制和規則。
- 確保您VPCs沒有重疊的IPv4CIDR塊。如果它們重疊，對VPC等連接的狀態會立即變為`failed`。即使VPCs具有唯一的IPv6CIDR區塊，也會套用此限制。

VPCs在同一帳戶和區域中創建

在相同帳戶和區域VPCs中建立VPC對等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 關閉 Create peering connection (建立對等互連)。
4. 設定下列資訊，完成後選擇建立對等互連：
   - 名稱：您可以選擇性地命名VPC對等連線。
   - VPCID (請求者)：在您的帳戶VPC中選取您要用來建立VPC對等連線的帳戶。
   - 對於選擇另一個VPC對等方式，選擇我的帳戶，然後選擇另一個您的帳戶VPCs。
   - (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤金鑰和值。
5. 選擇動作 > 接受請求。
6. 出現確認提示時，請選擇接受請求。
7. 選擇 [立即修改我的路由表]，將路由新增至VPC路由表格，讓您可以透過對等連線傳送和接收流量。如需詳細資訊，請參閱更新對VPC等連線的路由表。

VPCs在同一個帳戶和不同地區創建

在相同帳戶和不同區域VPCs中建立VPC對等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 關閉 Create peering connection (建立對等互連)。
4. 設定下列資訊，完成後選擇建立對等互連：
   - 名稱：您可以選擇性地命名VPC對等連線。執行此作業會使用 `Name` 做為索引鍵，以及您指定的值來建立標籤。
   - VPCID (請求者)：在您的帳戶VPC中選取要求對等連線的要求者VPC。
   - 帳戶：選擇我的帳戶。
   - 區域：選擇其他區域，然後選取接受者VPC的「區域」。
   - VPCID (接受者)：選取接受VPC者。
5. 在「區域」選取器中，選取接受者VPC的「區域」。

6. 在導覽窗格中，選擇 Peering connections (對等互連)。選取您建立的VPC對等連線，然後選擇動作，接受請求。
7. 出現確認提示時，請選擇接受請求。
8. 選擇 [立即修改我的路由表]，將路由新增至VPC路由表格，讓您可以透過對等連線傳送和接收流量。如需詳細資訊，請參閱更新對VPC等連線的路由表。

VPCs在不同的帳戶和相同的區域中創建

要求與不VPC同帳戶和相同VPCs區域的對等連接

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 關閉 Create peering connection (建立對等互連)。
4. 設定如下資訊，完成後選擇建立對等互連：

   - 名稱：您可以選擇性地命名VPC對等連線。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。只有您可以看到此標籤；對等體的擁有者VPC可以為對等連線建立自己的VPC標籤。
   - VPCID (請求者)：VPC在您的帳戶中選取要用來建立對等連線的VPC對等連線。
   - Account (帳戶)：選擇 Another account (其他帳戶)。
   - 帳戶識別碼：輸入擁有接受者VPC的識別碼。 AWS 帳戶
   - VPCID (接受者)：輸入要VPC用來建立VPC對等連線的 ID。

VPCs在不同的帳戶和區域中創建

要求VPCs在不同帳戶和區域中建立VPC對等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 關閉 Create peering connection (建立對等互連)。
4. 設定如下資訊，完成後選擇建立對等互連：

   - 名稱：您可以選擇性地命名VPC對等連線。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。只有您可以看到此標籤；對等體的擁有者VPC可以為對等連線建立自己的VPC標籤。

- VPCID (請求者)：VPC在您的帳戶中選取要用來建立對等連線的VPC對等連線。
- Account (帳戶)：選擇 Another account (其他帳戶)。
- 帳戶識別碼：輸入擁有接受者VPC的識別碼。 AWS 帳戶
- 區域：選擇其他區域，然後選取接受者VPC所在的區域。
- VPCID (接受者)：輸入要VPC用來建立VPC對等連線的 ID。

使用指令列建立VPC對等連線

您可以使用下列指令建立VPC對等連線：

- create-vpc-peering-connection (AWS CLI)
- New-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)

刪除對VPC等連線

對等連線VPC中的任一擁有者都可以隨時刪除VPC對等連線。您也可以刪除您要求但仍處於`pending-acceptance`狀態的VPC對等連線。

當VPC對等連線處於狀態時，您無法刪除VPC對等連線。`rejected`我們會自動為您刪除連線。

在 Amazon VPC 主控台VPC中刪除屬於作用中對等連線的一部分，也會刪除VPC對VPC等連線。如果您要求與另一個帳戶中的VPC對等連線，而您VPC在另一方接受要求VPC之前刪除您的對等連線，則VPC對等連線也會一併刪除。您無法刪除您在其他帳戶VPC中有`pending-acceptance`要求的。VPC您必須先拒絕VPC對等連線要求。

當您刪除對等連線時，狀態會先設為 `Deleting`，然後設為 `Deleted`。刪除連線後，就無法接受、拒絕或編輯連線。如需對等互連可持續顯示多久時間的詳細資訊，請參閱VPC對等連線生命週期。

若要刪除對VPC等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 選取VPC對等連線。
4. 選擇 Actions (動作) 和 Delete peering connection (刪除對等互連)。
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

若要使用指令行或刪除VPC對等連線 API

- delete-vpc-peering-connection (AWS CLI)
- Remove-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- DeleteVpcPeeringConnection (Amazon EC2 查詢API)

接受或拒絕對VPC等連線

處於pending-acceptance狀態的VPC對等連線必須由接受者的擁有者接受VPC才能啟動。如需 Deleted 對等互連狀態的詳細資訊，請參閱 VPC對等連線生命週期。您無法接受已傳送至其他 AWS 帳戶的VPC對等連線要求。如果您要在同一 AWS 帳戶中建立VPC對等連線，則必須自行建立並接受請求。

如果VPCs在不同的區域，請求必須在接受者的區域被接受VPC。

> **Important**
>
> 不接受來自不明 AWS 帳號的VPC對等連線。惡意使用者可能已向您傳送VPC對等連線要求，以取得未經授權的VPC網路存取。這種手法稱為對等釣魚。您可以安全地拒絕不必要的VPC對等連線要求，而不會有請求者存取您 AWS 帳戶或您帳戶的任何資訊的風險。VPC如需詳細資訊，請參閱接受或拒絕對VPC等連線。您也可以忽略請求使其過期；根據預設，請求會在 7 天後過期。

接受VPC對等連線之後，您必須在路由表中新增項目，以啟用對等之間的流量。VPCs如需詳細資訊，請參閱更新對VPC等連線的路由表。

您可以拒絕您收到的任何處於此pending-acceptance狀態的VPC對等連線要求。您應該只接受您 AWS 帳戶 已知且信任的VPC對等連線；您可以拒絕任何不想要的要求。如需 Rejected 對等互連狀態的詳細資訊，請參閱 VPC對等連線生命週期。

接受或拒絕對VPC等連線

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 使用區域選擇器選擇接受者VPC的區域。
3. 在導覽窗格中，選擇 Peering connections (對等互連)。
4. 若要拒絕對等連線，請選取VPC對等連線，然後選擇動作，拒絕請求。出現確認提示時，請選擇拒絕請求。

5. 若要接受對等互連連線，請選取擱置的VPC對等連線 (狀態為pending-acceptance)，然後選擇動作，接受請求。如需對等互連生命週期狀態的詳細資訊，請參閱VPC對等連線生命週期。

   > **Tip**
   >
   > 如果您看不到擱置的VPC對等連線，請檢查 [地區]。在接受者的「區域」中，必須接受區域間對等請求。VPC

6. 出現確認提示時，請選擇接受請求。
7. 選擇 [立即修改我的路由表]，將路由新增至VPC路由表格，讓您可以透過對等連線傳送和接收流量。如需詳細資訊，請參閱更新對VPC等連線的路由表。

使用指令行或接受VPC對等連線的步驟 API

- accept-vpc-peering-connection (AWS CLI)
- Approve-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- AcceptVpcPeeringConnection (Amazon EC2 查詢API)

使用指令行或拒絕VPC對等連接的步驟 API

- reject-vpc-peering-connection (AWS CLI)
- Deny-EC2VpcPeeringConnection (AWS Tools for Windows PowerShell)
- RejectVpcPeeringConnection (Amazon EC2 查詢API)

更新對VPC等連線的路由表

若要啟用對等執行個體之間的私人IPv4流量VPCs，您必須將路由新增至與這兩個執行個體的子網路相關聯的路由表格。路由目的地是對等端的CIDR區塊 (或CIDR區塊的一部分)，VPC而目標則是VPC對等連線的識別碼。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的設定路由表。

以下是路由表的範例VPCs，可在兩個對等 (VPCA 和 B) 中的執行VPC個體之間進行通訊。每個表格都有一個區域路由，以及將對等VPCVPC連線傳送流量的路由。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域

路由表	目的地	目標
	VPC B CIDR	多氯化合物*11112222*
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	多氯化合物*11112222*

同樣地，如果VPC對等連線VPCs中的具有相關聯的IPv6CIDR區塊，您可以新增路由來啟用與對等端VPC的IPv6通訊。

如需有關對VPC等連線支援之路由表組態的詳細資訊，請參閱一般VPC對等連線組態。

考量事項

- 如果您有多個具有重疊或匹配IPv4CIDR塊VPCs的對等，請確保已配置路由表，以避免將響應流量從您的發送VPC到不正VPC確的。VPC AWS 目前不支援在檢查封包來源 IP 的VPC對等連線中的單點傳送反向路徑轉送，並將回覆封包路由傳回至來源。如需詳細資訊，請參閱回應流量的路由。
- 您的帳戶的每個路由表可新增的項目數具有配額。如果您的VPC對等連線數目VPC超過單一路由表的路由表項目配額，請考慮使用多個子網路，每個子網路都與自訂路由表相關聯。
- 您可以為`pending-acceptance`狀態中的VPC對等連線新增路由。但是，路由的狀態為`blackhole`，且在對VPC等連接處於狀`active`態之前沒有任何作用。

新增對VPC等連IPv4線的路由

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選取與您執行個體所在之子網相關聯的路由表旁邊的核取方塊。

   如果您沒有明確與該子網路相關聯的路由表，則的主路由表會隱含地與子網路產生關聯。VPC
4. 選擇 Actions (動作)、Edit routes (編輯路由)。
5. 選擇 Add route (新增路由)。
6. 針對目的IPv4地，輸入必須將對VPC等連線中網路流量導向的位址範圍。您可以指定對等的整個IPv4CIDR區塊VPC、特定範圍或個別位IPv4址，例如要與之通訊的執行個體 IP 位址。例如，如果對等CIDR區塊VPC是`10.0.0.0/16`，您可以指定部分`10.0.0.0/24`或特定 IP 位址`10.0.0.7/32`。

7. 針對「目標」，選取VPC對等連線。
8. 選擇 Save changes (儲存變更)。

對等的擁有者也VPC必須完成這些步驟，才能新增路由，以VPC透過對等連線將流量VPC引導回您的路由。

如果您在使用IPv6地址的不同 AWS 區域中有資源，則可以建立區域間對等連線。然後，您可以為資源之間的通信添加IPv6路由。

新增對VPC等連IPv6線的路由

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選取與您執行個體所在之子網相關聯的路由表旁邊的核取方塊。

> **Note**
>
> 如果您沒有與該子網路相關聯的路由表，請選取的主路由表VPC，因為子網路接著依預設會使用此路由表。

4. 選擇 Actions (動作)、Edit routes (編輯路由)。
5. 選擇 Add route (新增路由)。
6. 在目的地中，輸入對等的IPv6位址範圍VPC。您可以指定對等的整個IPv6CIDR區塊VPC、特定範圍或個別IPv6位址。例如，如果對等CIDR區塊VPC是`2001:db8:1234:1a00::/56`，您可以指定部分`2001:db8:1234:1a00::/64`或特定 IP 位址`2001:db8:1234:1a00::123/128`。
7. 針對「目標」，選取VPC對等連線。
8. 選擇 Save changes (儲存變更)。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的路由表。

使用指令行或加入或取代佈線的步驟 API

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- CreateRoute (Amazon EC2 查詢API)
- replace-route (AWS CLI)

- Set-EC2Route (AWS Tools for Windows PowerShell)
- ReplaceRoute（ Amazon EC2 查詢API ）

更新您的安全群組以參考對等安全群組

您可以更新VPC安全性群組的輸入或輸出規則，以參考要對等VPCs的安全性群組。這樣做可讓流量往返於與對等中參照安全性群組相關聯的執行個體。VPC

> **Note**
>
> 對等中的安全性群組VPC不會顯示在主控台中供您選取。

要求

- 若要參照對等中的安全性群組VPC，VPC對等連線必須處於狀`active`態。
- 對等VPC可以是您的帳戶VPC中，也可以是另一個 AWS 帳戶VPC中的對等。若要參照位於另一個 AWS 帳戶但相同區域中的安全性群組，請包含帳戶號碼與安全性群組的 ID。例如：`123456789012/sg-1a2b3c4d`。
- 您無法參考位於不同區域中的對等端點VPC的安全性群組。相反，使用對等體的CIDR塊VPC。
- 如果您將路由設定為透過中間設備來轉遞不同子網中兩個執行個體之間的流量，則您必須確保兩個執行個體的安全群組均允許流量在執行個體之間流動。每個執行個體的安全性群組都必須參照另一個執行個體的私有 IP 位址，或包含其他執行個體的子網路CIDR範圍做為來源。如果您參考另一個執行個體的安全群組作為來源，這不會允許流量在執行個體之間流動。

使用主控台更新您的安全群組規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [安全性群組]。
3. 選取安全性群組，然後執行下列其中一項作業：
   - 若要修改輸入規則，請選擇 [動作] > [編輯輸入規則]。
   - 若要修改輸出規則，請選擇動作 > 編輯輸出規則。
4. 若要新增規則，請選擇新增規則，然後指定類型、通訊協定和連接埠範圍。針對來源 (輸入規則) 或目的地 (輸出規則)，執行下列其中一項作業：
   - 對於相同帳戶和區域VPC中的對等，請輸入安全性群組的 ID。

- 對於不同帳戶但相同區域VPC中的對等，請輸入帳戶 ID 和安全性群組 ID，並以正斜線分隔 (例如，123456789012/sg-1a2b3c4d)。
- 對於不同區域VPC中的同儕，請輸入對等端點的區CIDR塊VPC。

5. 若要編輯現有規則，請變更其值 (例如來源或描述)。
6. 若要刪除規則，請選擇規則旁邊的刪除。
7. 選擇儲存規則。

使用命令列更新傳入規則

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

例如，若要更新您的安全性群組，sg-aaaa1111以允許對等端HTTP的sg-bbbb2222輸入存取VPC，請使用下列命令。如果對等位VPC於同一區域，但帳戶不同，請新增 `--group-owner` *aws-account-id*.

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --
port 80 --source-group sg-bbbb2222
```

使用命令列更新傳出規則

- authorize-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)
- revoke-security-group-egress (AWS CLI)

更新安全性群組規則之後，請使用describe-security-groups命令來檢視安全性群組規則中參照的安全性群組。

識別您的參考安全群組

若要判斷您的安全性群組是否在對等中的安全性群組的規則中參考VPC，請針對您帳戶中的一或多個安全性群組使用下列其中一個指令。

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)
- DescribeSecurityGroupReferences（Amazon EC2 查詢API）

在下列範例中，回應指出中的安全性群組sg-bbbb2222正在參考安全性群組 VPCvpc-aaaaaaaa：

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

如果VPC對等連線已刪除，或者對等體的擁有者VPC刪除參照的安全性群組，則安全性群組規則會過時。

使用過時的安全性群組規則檢視和刪除

過時的安全性群組規則是參照相同VPC或對等中已刪除安全性群組的規則VPC，或參考已刪除對等連線之VPC對等中安全性群組的規則。VPC過時的安全群組規則不會自動從您的安全群組移除，您必須手動將其移除。如果安全性群組規則因為VPC對等連線已刪除而過時，如果您使用相同連線建立新的對VPC等連線，則該規則將不再標示為過時。VPCs

您可以VPC使用 Amazon VPC 主控台檢視和刪除過時的安全群組規則。

檢視和刪除過時安全群組規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [安全性群組]。
3. 選擇 Actions (動作)、Manage stale rules (管理過時規則)。
4. 對於 VPC，選擇VPC與陳舊規則。
5. 選擇編輯。

6. 選擇要刪除之規則右側的 Delete (刪除) 按鈕。選擇 Preview changes (預覽變更) 及 Save rules (儲存規則)。

使用命令列或描述過時的安全性群組規則 API

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)
- DescribeStaleSecurityGroups（Amazon EC2 查詢API）

在下列範例中，VPCA(vpc-aaaaaaaa) 和 VPC B 已對等，而VPC對等連線已刪除。VPCB sg-aaaa1111 中 VPC A 中的安全性群組參考sg-bbbb2222時，當您執行您的describe-stale-security-groups命令時VPC，回應會指出安全性群組sg-aaaa1111具有參照sg-bbbb2222的過時SSH規則。

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
    "StaleSecurityGroupSet": [
        {
            "VpcId": "vpc-aaaaaaaa",
            "StaleIpPermissionsEgress": [],
            "GroupName": "Access1",
            "StaleIpPermissions": [
                {
                    "ToPort": 22,
                    "FromPort": 22,
                    "UserIdGroupPairs": [
                        {
                            "VpcId": "vpc-bbbbbbbb",
                            "PeeringStatus": "deleted",
                            "UserId": "123456789101",
                            "GroupName": "Prod1",
                            "VpcPeeringConnectionId": "pcx-b04deed9",
                            "GroupId": "sg-bbbb2222"
                        }
                    ],
                    "IpProtocol": "tcp"
                }
            ],
            "GroupId": "sg-aaaa1111",
```

```
            "Description": "Reference remote SG"
        }
    ]
}
```

識別過時的安全性群組規則後，您可以使用revoke-security-group-ingress或revoke-security-group-egress命令將其刪除。

啟用對VPC等連線的DNS解析度

若要啟用從對等中的執行個VPC體查詢時，將公用IPv4DNS主機名稱解析為私人IPv4位址VPC，您必須修改現有的對等連線。

VPCs必須針對DNS主機名稱和DNS解析啟用兩者。

當您建立新的對等連線時，您無法啟用DNS解析度支援。您可以為`active`狀態中的現有對等連線啟用DNS解析度支援。

啟用對等連線的DNS解析度

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇 Peering connections (對等互連)。
3. 選取VPC對等連線，然後選擇 [動作] > [編輯DNS設定]。
4. 若要確保從對等方VPC解析為本機中的私人 IP 位址的查詢VPC，請選擇啟用對等方查詢解DNS析的選項VPC。此選項為「請求者DNS解析」或「接受者DNS解析」，視請求者或接VPC受者而定。VPC
5. 如果對等端點處VPC於相同狀態 AWS 帳戶，您可以在對等連線VPCs中啟用兩者的DNS解析度。
6. 選擇 Save changes (儲存變更)。
7. 如果對等端點位VPC於不同的 AWS 帳戶或不同的區域中，則對等端的擁有者VPC必須登入VPC主控台，執行步驟 2 到 4，然後選擇 [儲存變更]。

使用指令行或啟用DNS解析度的步驟 API

- modify-vpc-peering-connection-選項（ ）AWS CLI
- Edit-EC2VpcPeeringConnectionOption (AWS Tools for Windows PowerShell)
- ModifyVpcPeeringConnectionOptions（Amazon EC2 查詢API）

如果您是VPC對等連線的請求者，則必須修改請求者對等連線選項；如果您是VPC對等連線的接受者，則必須修改接受者VPC對等連線選項。VPC您可以使用describe-vpc-peering-connections或Get-EC2VpcPeeringConnections指令來確認哪一VPC個VPC是對等連線的接受者與請求者。對於區域間對等連線，您必須使用請求者的「區域」VPC 來修改請求者對VPC等選項，並使用接受者的「區域」VPC 來修改接受者對等選項。VPC

在此範例中，您是對VPC等連線的請求者，因此請使用下列步驟修改對等連線選項： AWS CLI

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb
 --requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

疑難排解VPC對等連線

如果您無法從對等中的資源連接VPC到資源VPC，請執行以下操作：

- 對於每個資源中的每個資源VPC，請確認其子網路的路由表包含傳送目的地對等VPCVPC連線之流量的路由。這可確保網路流量可以在兩者之間正確流動VPCs。如需詳細資訊，請參閱更新路由表。
- 對於涉及的任何EC2執行個體，請確認這些執行個體的安全性群組是否允許來自對等的輸入和輸出流量VPC。安全群組規則會控制允許哪些流量存取您的EC2執行個體。如需詳細資訊，請參閱參考對等安全群組。
- 檢查包含資源ACLs之子網路的網路是否允許來自對等VPC的必要流量。網路ACLs是額外的安全性層級，可篩選子網路層級的流量。

如果您仍然遇到問題，可以利用 Reachability Analyzer。可 Reachability Analyzer 可以幫助識別導致兩者之間的連接問題的特定組件 ACL-無論是路由表，安全組還是網絡-。VPCs如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

徹底驗證您的VPC網路組態是疑難排解和解決您可能遇到的任何VPC對等連線問題的關鍵。

一般VPC對等連線組態

本節說明您可以實作的兩種常見VPC對等互連組態類型：

- VPC對等組態與整個路由VPC：在此組態中，您可以在每VPC個路由表格中建立路由，以傳送目的地為對等VPC連線的所有流量。VPC這允許任何一個資源與VPC對等中的任何資源進行通信VPC，從而簡化管理。不過，這也表示之間的所有流量都VPCs會經過對等連線，如果流量很高，這可能會成為瓶頸。
- VPC使用特定路由對等組態：或者，您可以在每個路由表中建立更精細VPC的路由，只將流量傳送至對等中的特定子網路或資源。VPC這可讓您將流經對等連線的流量限制為只有必要的流量，這樣可以更有效率。但是，它也需要更多的維護，因為每當您在需要通信的對等體中添加新資源時，您都需VPC要更新路由表。

最佳方法取決於各種因素，例如VPC架構的大小和複雜度、之間預期的流量VPCs，以及您組織對安全性和資源存取的需求。許多企業使用混合式方法，針對常見流量模式提供廣泛的路由，針對更敏感或頻寬密集的使用案例提供特定路由。

組態

- VPC對等組態與整個路線 VPC
- VPC具有特定路由的對等組態

VPC對等組態與整個路線 VPC

您可以配置VPC對等連接，以便您的路由表可以訪問對等VPC的整個CIDR塊。如需有關可能需要特定對VPC等連線組態之案例的詳細資訊，請參閱VPC對等連線網路案例。若要取VPC得有關建立和使用對等連接的更多資訊，請參閱〈〉使用VPC對等連接。

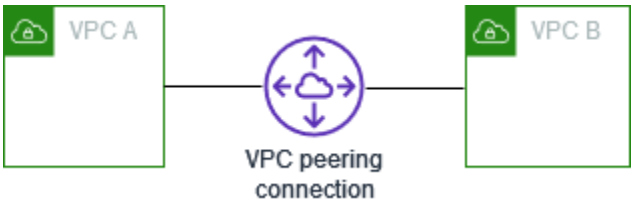
如需更新路由表的詳細資訊，請參閱更新對VPC等連線的路由表。

組態

- 兩個VPCs凝聚在一起
- 一個與VPC兩個 VPCs
- 三個VPCs凝聚在一起
- 多個VPCs對等在一起

兩個VPCs凝聚在一起

在此配置中，VPCA 和 B（pcx-11112222）之間存VPC在對等連接。這VPCs些是相同的 AWS 帳戶 ，它們的CIDR塊不重疊。



當您有兩個需要彼此資源存取權時VPCs，您可以使用此組態。例如，您為會計記錄設定 A，為財務記錄設定 VPC B，而這些記錄VPC必須能夠VPC不受限制地從另VPC一個記錄存取資源。

單 VPC CIDR

更新每個路由表，其中VPC包含傳送對等VPCVPC連線CIDR區塊的流量的路由。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	VPC B CIDR	pcx-11112222
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	pcx-11112222

多 IPv4 VPC CIDRs

如果 VPC A 和 VPC B 有多個關聯的IPv4CIDR塊，則可以VPC使用對等部分或所有塊的路由更新每個IPv4CIDR塊的路由表VPC。

路由表	目的地	目標
VPCA	*VPC A CIDR 1*	區域
	VPC A CIDR 2	區域
	VPC B CIDR 1	pcx-11112222

路由表	目的地	目標
	VPC B CIDR 2	pcx-11112222
VPCB	*VPC B CIDR 1*	區域
	VPC B CIDR 2	區域
	VPC A CIDR 1	pcx-11112222
	VPC A CIDR 2	pcx-11112222

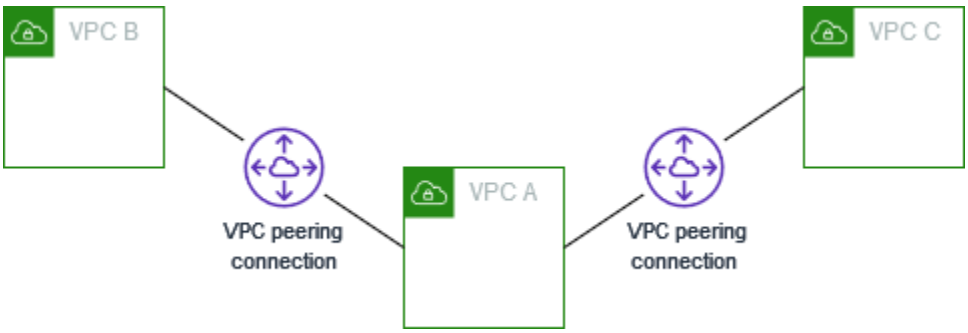
IPv4和 IPv6 VPC CIDRs

如果 VPC A 和 VPC B VPC 具有關聯的IPv6CIDR塊，則可以使用對等IPv4和IPv6CIDR塊的路由更新每個塊的路由表VPC。

路由表	目的地	目標
VPCA	*VPC A IPv4 CIDR*	區域
	VPC A IPv6 CIDR	區域
	VPC B IPv4 CIDR	pcx-11112222
	VPC B IPv6 CIDR	pcx-11112222
VPCB	*VPC B IPv4 CIDR*	區域
	VPC B IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-11112222
	VPC A IPv6 CIDR	pcx-11112222

一個與VPC兩個 VPCs

在此配置中，存在一個中央VPC（VPCA），VPCA 和 VPC B（ ）之間的對等連接以及 VPC A 和 VPC C（pcx-12121212pcx-23232323）之間的對等連接。所有這三個VPCs都是相同的 AWS 帳戶 ，它們的CIDR塊不重疊。



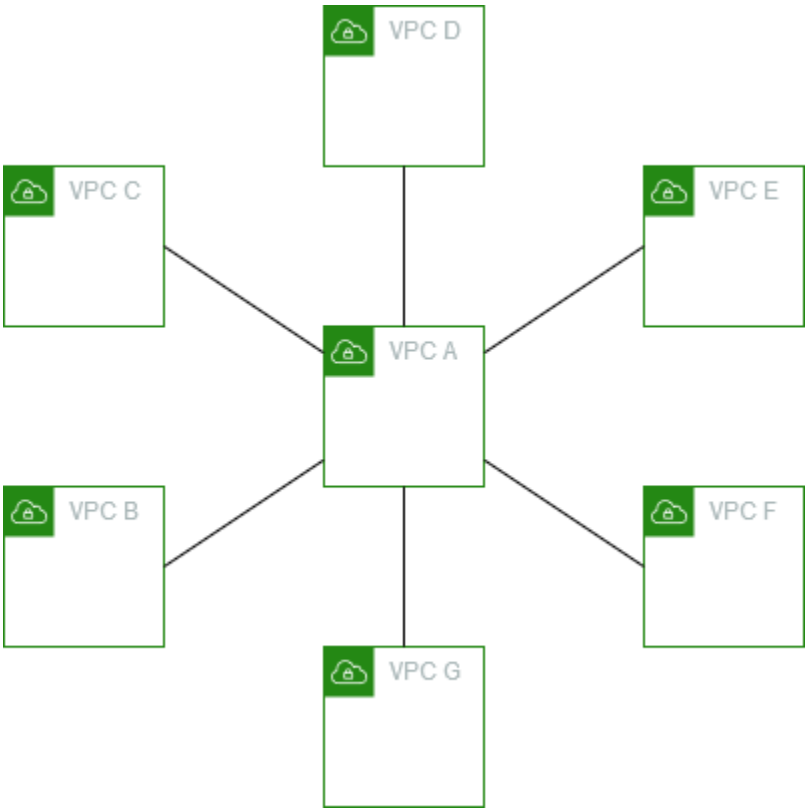
VPCB 和 VPC C 無法透過 A 直接傳送流量給VPC彼此，因為對等互連不支援傳遞對等關係。VPC您可以在 VPC B 和 VPC C 之間建立VPC對等連線，如中三個VPCs凝聚在一起所示。如需不支援互連藍本的詳細資訊，請參閱the section called “VPC對等限制”。

當您在中央上有資源 (例如服務的儲存庫)VPC，而其他人VPCs需要存取時，您可以使用此組態。另一方VPCs不需要存取彼此的資源；他們只需要存取中央的資源即可VPC。

更新每個路由表，VPC如下所示，以使用每個CIDR塊實現此配置VPC。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	VPC B CIDR	pcx-12121212
	VPC C CIDR	pcx-23232323
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	pcx-12121212
VPCC	*VPC C CIDR*	區域
	VPC A CIDR	pcx-23232323

您可以將此配置擴展到其他配置VPCs。例如，VPCA 使用和與 VPC B 到 VPC G 對IPv6CIDRs等IPv4，但另一個VPCs不相互對等。在此圖中，線代表VPC對等連接。



如下所示更新路由表。

路由表	目的地	目標
VPCA	*VPC A IPv4 CIDR*	區域
	VPC A IPv6 CIDR	區域
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd

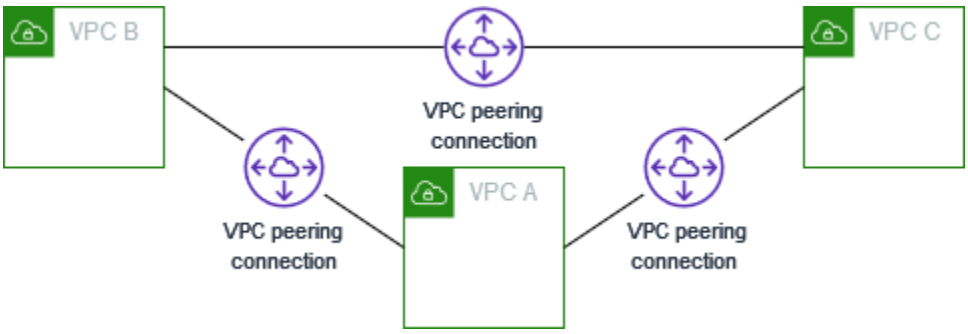
路由表	目的地	目標
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPCB	*VPC B IPv4 CIDR*	區域
	VPC B IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
VPCC	*VPC C IPv4 CIDR*	區域
	VPC C IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
VPCD	*VPC D IPv4 CIDR*	區域
	VPC D IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
VPCE	*VPC E IPv4 CIDR*	區域
	VPC E IPv6 CIDR	區域

路由表	目的地	目標
	VPC A IPv4 CIDR	pcx-aaaaeeee
	VPC A IPv6 CIDR	pcx-aaaaeeee
VPCF	*VPC F IPv4 CIDR*	區域
	VPC F IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
VPCG	*VPC G IPv4 CIDR*	區域
	VPC G IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg

三個VPCs凝聚在一起

在此配置中，有三VPCs個 AWS 帳戶 與不重疊的CIDR圖塊相同。在VPCs完整網格中對等，如下所示：

- VPCA 通過對等連接對VPC等到 VPC B `pcx-aaaabbbb`
- VPCA 通過對等連接對VPC等到 VPC C `pcx-aaaacccc`
- VPCB 通過對等連接對VPC等到 VPC C `pcx-bbbbcccc`



當您需要不受限制地彼此共享資源時，可以使用此配置。VPCs例如，作為檔案共享系統。

按照以下步驟更新每個VPC路由表以實現此配置。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-bbbbcccc
VPCC	*VPC C CIDR*	區域
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc

如果 VPC A 和 VPC B 同時具有IPv4和IPv6CIDR塊，但 VPC C 沒有IPv6CIDR塊，請按如下方式更新路由表。VPCA 和 VPC B 中的資源可以使用IPv6VPC對等連接進行通信。但是，VPCC 無法使用IPv6. VPC VPC

路由表	目的地	目標
VPCA	*VPC A IPv4 CIDR*	區域
	VPC A IPv6 CIDR	區域
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc

路由表	目的地	目標
VPCB	*VPC B IPv4 CIDR*	區域
	VPC B IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc
VPCC	*VPC C IPv4 CIDR*	區域
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc

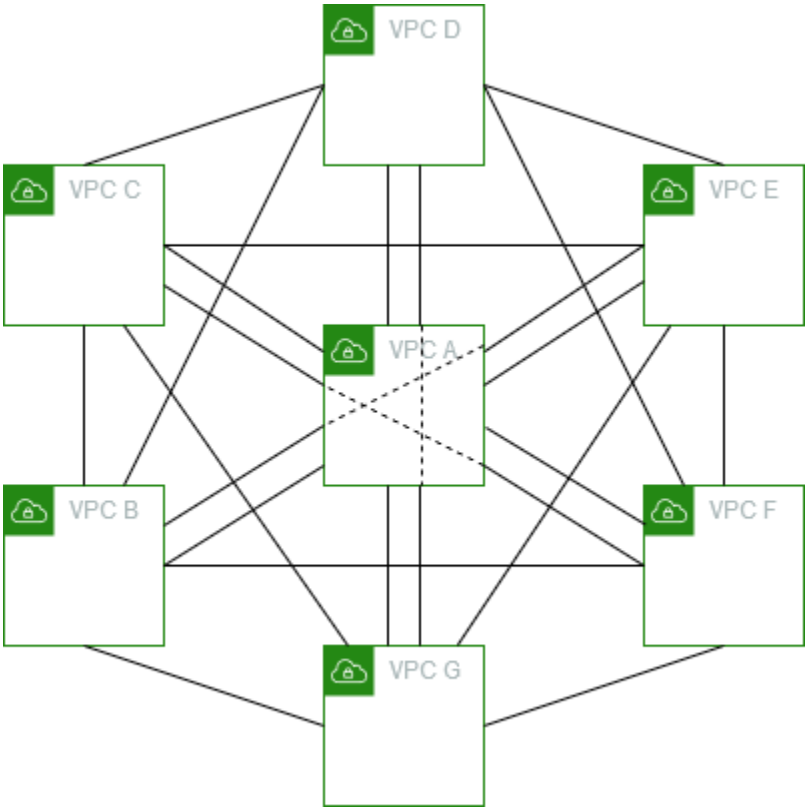
多個VPCs對等在一起

在此組態中，完整網格組VPCs態中有七個對等。這VPCs些是相同的 AWS 帳戶 ，它們的CIDR塊不重疊。

VPC	VPC	VPC對等連接
A	B	pcx-aaaabbbb
A	C	pcx-aaaacccc
A	D	pcx-aaaadddd
A	E	pcx-aaaaeeee
A	F	pcx-aaaaffff
A	G	pcx-aaaagggg
B	C	pcx-bbbbcccc
B	D	pcx-bbbbdddd

VPC	VPC	VPC對等連接
B	E	pcx-bbbbeeee
B	F	pcx-bbbbffff
B	G	pcx-bbbbgggg
C	D	pcx-ccccdddd
C	E	pcx-cccceeee
C	F	pcx-ccccffff
C	G	pcx-ccccgggg
D	E	pcx-ddddeeee
D	F	pcx-ddddffff
D	G	pcx-ddddgggg
E	F	pcx-eeeeffff
E	G	pcx-eeeegggg
F	G	pcx-ffffgggg

當您有多個VPCs必須能夠不受限制地存取彼此資源時，您可以使用此配置。例如，檔案共享網路時。在此圖中，線代表VPC對等連接。



按照以下步驟更新每個VPC路由表以實現此配置。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	VPC D CIDR	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	pcx-aaaabbbb

路由表	目的地	目標
	VPC C CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-bbbbdddd
	VPC E CIDR	pcx-bbbbeeee
	VPC F CIDR	pcx-bbbbffff
	VPC G CIDR	pcx-bbbbgggg
VPCC	*VPC C CIDR*	區域
	VPC A CIDR	pcx-aaaacccc
	VPC B CIDR	pcx-bbbbcccc
	VPC D CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-cccceeee
	VPC F CIDR	pcx-ccccffff
	VPC G CIDR	pcx-ccccgggg
VPCD	*VPC D CIDR*	區域
	VPC A CIDR	pcx-aaaadddd
	VPC B CIDR	pcx-bbbbdddd
	VPC C CIDR	pcx-ccccdddd
	VPC E CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-ddddffff
	VPC G CIDR	pcx-ddddgggg
VPCE	*VPC E CIDR*	區域

路由表	目的地	目標
	VPC A CIDR	pcx-aaaaeeee
	VPC B CIDR	pcx-bbbbeeee
	VPC C CIDR	pcx-cccceeee
	VPC D CIDR	pcx-ddddeeee
	VPC F CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-eeeegggg
VPCF	*VPC F CIDR*	區域
	VPC A CIDR	pcx-aaaaffff
	VPC B CIDR	pcx-bbbbffff
	VPC C CIDR	pcx-ccccffff
	VPC D CIDR	pcx-ddddffff
	VPC E CIDR	pcx-eeeeffff
	VPC G CIDR	pcx-ffffgggg
VPCG	*VPC G CIDR*	區域
	VPC A CIDR	pcx-aaaagggg
	VPC B CIDR	pcx-bbbbgggg
	VPC C CIDR	pcx-ccccgggg
	VPC D CIDR	pcx-ddddgggg
	VPC E CIDR	pcx-eeeegggg
	VPC F CIDR	pcx-ffffgggg

如果所有圖塊都VPCs有相關聯的IPv6CIDR區塊，請按如下方式更新路由表。

路由表	目的地	目標
VPCA	*VPC A IPv4 CIDR*	區域
	VPC A IPv6 CIDR	區域
	VPC B IPv4 CIDR	pcx-aaaabbbb
	VPC B IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-aaaacccc
	VPC C IPv6 CIDR	pcx-aaaacccc
	VPC D IPv4 CIDR	pcx-aaaadddd
	VPC D IPv6 CIDR	pcx-aaaadddd
	VPC E IPv4 CIDR	pcx-aaaaeeee
	VPC E IPv6 CIDR	pcx-aaaaeeee
	VPC F IPv4 CIDR	pcx-aaaaffff
	VPC F IPv6 CIDR	pcx-aaaaffff
	VPC G IPv4 CIDR	pcx-aaaagggg
	VPC G IPv6 CIDR	pcx-aaaagggg
VPCB	*VPC B IPv4 CIDR*	區域
	VPC B IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaabbbb
	VPC A IPv6 CIDR	pcx-aaaabbbb
	VPC C IPv4 CIDR	pcx-bbbbcccc

路由表	目的地	目標
	VPC C IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-bbbbdddd
	VPC D IPv6 CIDR	pcx-bbbbdddd
	VPC E IPv4 CIDR	pcx-bbbbeeee
	VPC E IPv6 CIDR	pcx-bbbbeeee
	VPC F IPv4 CIDR	pcx-bbbbffff
	VPC F IPv6 CIDR	pcx-bbbbffff
	VPC G IPv4 CIDR	pcx-bbbbgggg
	VPC G IPv6 CIDR	pcx-bbbbgggg
VPCC	*VPC C IPv4 CIDR*	區域
	VPC C IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaacccc
	VPC A IPv6 CIDR	pcx-aaaacccc
	VPC B IPv4 CIDR	pcx-bbbbcccc
	VPC B IPv6 CIDR	pcx-bbbbcccc
	VPC D IPv4 CIDR	pcx-ccccdddd
	VPC D IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-cccceeee
	VPC E IPv6 CIDR	pcx-cccceeee
	VPC F IPv4 CIDR	pcx-ccccffff

路由表	目的地	目標
	VPC F IPv4 CIDR	pcx-ccccffff
	VPC G IPv4 CIDR	pcx-ccccgggg
	VPC G IPv6 CIDR	pcx-ccccgggg
VPCD	*VPC D IPv4 CIDR*	區域
	VPC D IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaadddd
	VPC A IPv6 CIDR	pcx-aaaadddd
	VPC B IPv4 CIDR	pcx-bbbbdddd
	VPC B IPv6 CIDR	pcx-bbbbdddd
	VPC C IPv4 CIDR	pcx-ccccdddd
	VPC C IPv6 CIDR	pcx-ccccdddd
	VPC E IPv4 CIDR	pcx-ddddeeee
	VPC E IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-ddddffff
	VPC F IPv6 CIDR	pcx-ddddffff
	VPC G IPv4 CIDR	pcx-ddddgggg
	VPC G IPv6 CIDR	pcx-ddddgggg
VPCE	*VPC E IPv4 CIDR*	區域
	VPC E IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaaeeee

路由表	目的地	目標
	VPC A IPv6 CIDR	pcx-aaaaeeee
	VPC B IPv4 CIDR	pcx-bbbbeeee
	VPC B IPv6 CIDR	pcx-bbbbeeee
	VPC C IPv4 CIDR	pcx-cccceeee
	VPC C IPv6 CIDR	pcx-cccceeee
	VPC D IPv4 CIDR	pcx-ddddeeee
	VPC D IPv6 CIDR	pcx-ddddeeee
	VPC F IPv4 CIDR	pcx-eeeeffff
	VPC F IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-eeeegggg
	VPC G IPv6 CIDR	pcx-eeeegggg
VPCF	*VPC F IPv4 CIDR*	區域
	VPC F IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaaffff
	VPC A IPv6 CIDR	pcx-aaaaffff
	VPC B IPv4 CIDR	pcx-bbbbffff
	VPC B IPv6 CIDR	pcx-bbbbffff
	VPC C IPv4 CIDR	pcx-ccccffff
	VPC C IPv6 CIDR	pcx-ccccffff
	VPC D IPv4 CIDR	pcx-ddddffff

路由表	目的地	目標
	VPC D IPv6 CIDR	pcx-ddddffff
	VPC E IPv4 CIDR	pcx-eeeeffff
	VPC E IPv6 CIDR	pcx-eeeeffff
	VPC G IPv4 CIDR	pcx-ffffgggg
	VPC G IPv6 CIDR	pcx-ffffgggg
VPCG	*VPC G IPv4 CIDR*	區域
	VPC G IPv6 CIDR	區域
	VPC A IPv4 CIDR	pcx-aaaagggg
	VPC A IPv6 CIDR	pcx-aaaagggg
	VPC B IPv4 CIDR	pcx-bbbbgggg
	VPC B IPv6 CIDR	pcx-bbbbgggg
	VPC C IPv4 CIDR	pcx-ccccgggg
	VPC C IPv6 CIDR	pcx-ccccgggg
	VPC D IPv4 CIDR	pcx-ddddgggg
	VPC D IPv6 CIDR	pcx-ddddgggg
	VPC E IPv4 CIDR	pcx-eeeegggg
	VPC E IPv6 CIDR	pcx-eeeegggg
	VPC F IPv4 CIDR	pcx-ffffgggg
	VPC F IPv6 CIDR	pcx-ffffgggg

VPC具有特定路由的對等組態

您可以設定VPC對等連線的路由表，以限制對等網路區CIDR塊、特定區CIDR塊 (如果VPC有多個CIDR區塊) 或對等VPC中特定資源的存取。在這些範例中，一VPC個中心與至少兩個具有重疊CIDR圖塊VPCs的對等。

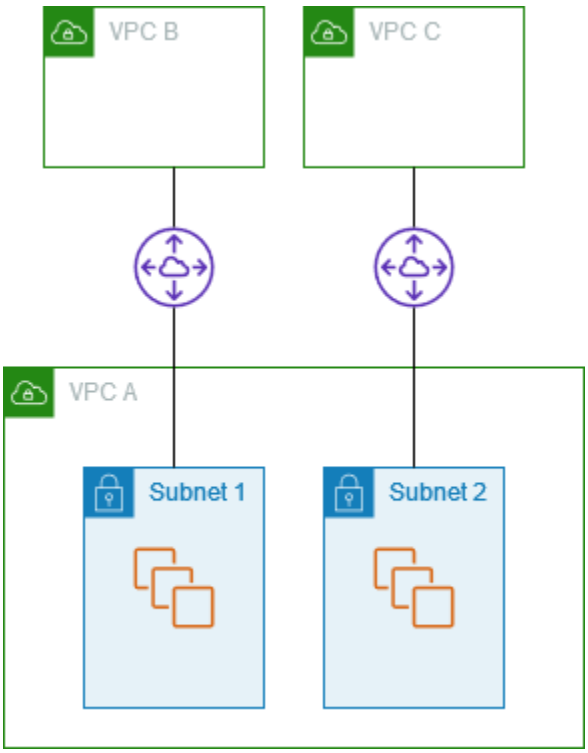
如需您可能需要特定對VPC等連線組態的案例範例，請參閱VPC對等連線網路案例。如需使用對VPC等連線的更多資訊，請參閱使用VPC對等連接。如需更新路由表的詳細資訊，請參閱更新對VPC等連線的路由表。

組態

- 兩個VPCs在一個訪問特定子網 VPC
- 兩個VPCs在一個訪問特定CIDR塊 VPC
- 一VPC個訪問兩個特定子網 VPCs
- 一個執行個體中VPC存取兩個特定執行個體 VPCs
- 一個VPCVPCs使用最長前綴匹配訪問兩個
- 多種VPC配置

兩個VPCs在一個訪問特定子網 VPC

在此配置中，有一個VPC具有兩個子網（VPCA）的中心，VPCA 和 VPC B（ ）之間的對等連接以及 VPC A 和 VPC C（pcx-aaaabbbb）之間的對等連接。pcx-aaaacccc每個都VPC需要存取 A 中的其中一個子網路中VPC的資源。



子網路 1 的路由表使用VPC對等連線pcx-aaaabbbb來存取 B 的整個CIDR區塊。VPC B 的路由表用pcx-aaaabbbb來存取 VPC A 中子網路 1 的CIDR區塊。子網路 2 的路由表使用VPC對等連線pcx-aaaacccc來存取 C 的整個CIDR區塊。VPC C 表的路由表用pcx-aaaacccc來存取 A 中子網路 2 的CIDR區塊。VPC VPC VPC

路由表	目的地	目標
子網路 1 (VPCA)	*VPC A CIDR*	區域
	VPC B CIDR	pcx-aaaabbbb
子網路 2 (VPCA)	*VPC A CIDR*	區域
	VPC C CIDR	pcx-aaaacccc
VPCB	*VPC B CIDR*	區域
	Subnet 1 CIDR	pcx-aaaabbbb
VPCC	*VPC C CIDR*	區域
	Subnet 2 CIDR	pcx-aaaacccc

您可以將此組態延伸至多個CIDR區塊。假設 VPC A 和 VPC B 同時具有IPv4和IPv6CIDR塊，並且子網 1 具有關聯的IPv6CIDR塊。您可以啟IPv6用 VPC B 透過使用VPC對等連線與 VPC A 中的子網路 1 進行通訊。為VPC此，請將路由添加到 A 的路由表，其中包含 VPC B IPv6 CIDR 塊的目的地，並添加到 VPC B 的路由表，其目的地為 VPC A 中子網 1 IPv6 CIDR 的路由。

路由表	目的地	目標	備註
VPCA 中的子網路 1	*VPC A IPv4 CIDR*	區域	
	VPC A IPv6 CIDR	區域	自動新增用IPv6於在 VPC.
	VPC B IPv4 CIDR	pcx-aaaabbbb	
	VPC B IPv6 CIDR	pcx-aaaabbbb	路由到 VPC B IPv6 CIDR 塊。
VPCA 中的子網路 2	*VPC A IPv4 CIDR*	區域	
	VPC A IPv6 CIDR	區域	自動新增用IPv6於在 VPC.
	VPC C IPv4 CIDR	pcx-aaaacccc	
VPCB	*VPC B IPv4 CIDR*	區域	
	VPC B IPv6 CIDR	區域	自動新增用IPv6於在 VPC.
	Subnet 1 IPv4 CIDR	pcx-aaaabbbb	
	Subnet 2 IPv4 CIDR	pcx-aaaabbbb	路由到 IPv6 CIDR VPC A 的塊
VPCC	*VPC C IPv4 CIDR*	區域	
	Subnet 2 IPv4 CIDR	pcx-aaaacccc	

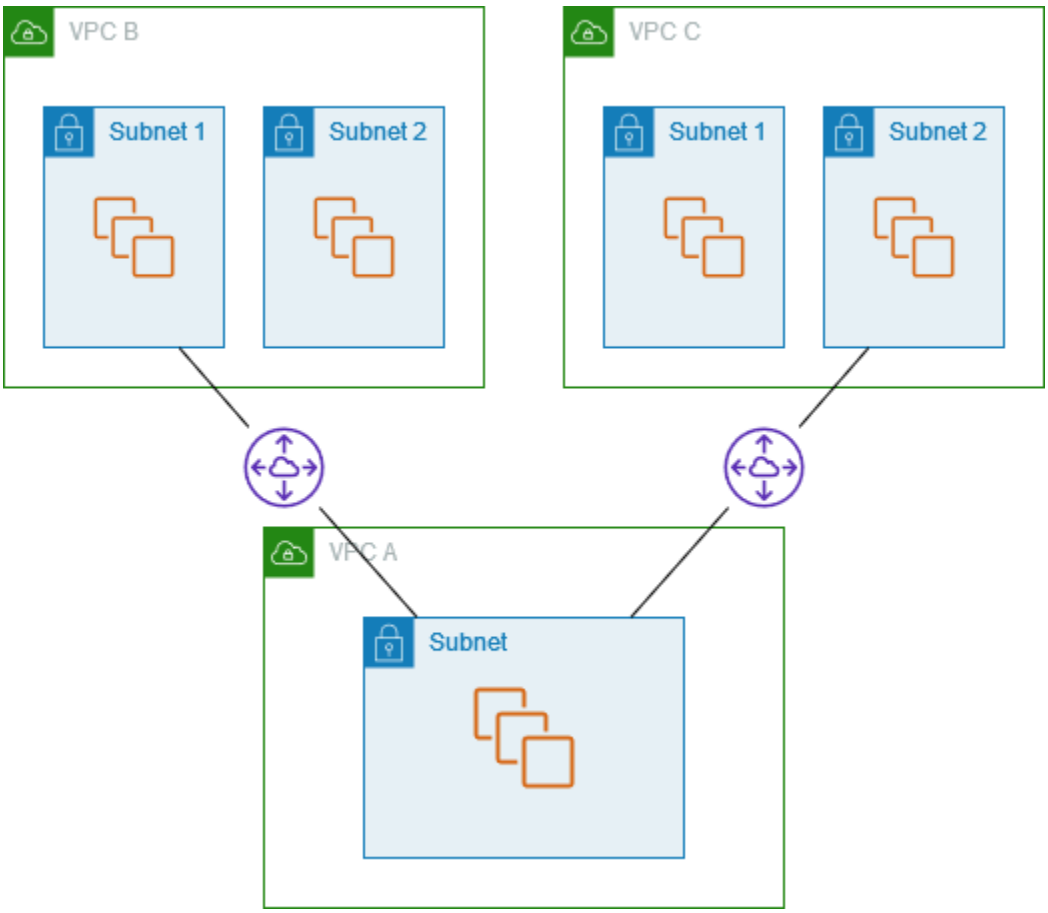
兩個VPCs在一個訪問特定CIDR塊 VPC

在此配置中，存在一個中央VPC（VPCA），VPCA 和 VPC B（ ）之間的對等連接以及 VPC A 和 VPC C（pcx-aaaabbbbpcx-aaaacccc）之間的對等連接。VPCA 對每個對等連線都有一個CIDR區塊。

路由表	目的地	目標
VPCA	*VPC A CIDR 1*	區域
	VPC A CIDR 2	區域
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
VPCB	*VPC B CIDR*	區域
	VPC A CIDR 1	pcx-aaaabbbb
VPCC	*VPC C CIDR*	區域
	VPC A CIDR 2	pcx-aaaacccc

一VPC個訪問兩個特定子網 VPCs

在這種配置中，有一個中央VPC（VPCA）與一個子網，VPCA 和 VPC B（pcx-aaaabbbb）之間的對等連接以及 VPC A 和 VPC C（pcx-aaaacccc）之間的對等連接。VPCB 和 VPC C 各有兩個子網路。VPCA 和 VPC B 之間的對等連接僅使用 B 中的一個子網路VPC。A 和 C 之間VPC的對等連接僅使用 VPC C 中的其中一個子網路。VPC



當您擁有具有其他人VPCs需要存取VPC的單一資源集 (例如 Active Directory 服務) 的中央時，請使用此組態。中央VPC不需要完全訪問它與之相似的。VPCs

VPCA 的路由表使用對等連接僅存取對等中的特定子網路。VPCs子網路 1 的路由表使用與 VPC A 的對等連線來存取 VPC A 中的子網路。子網路 2 的路由表使用與 A 的對等連線來存取 VPC A 中的子網路。VPC

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	Subnet 1 CIDR	pcx-aaaabbbb
	Subnet 2 CIDR	pcx-aaaacccc
子網路 1 (VPCB)	*VPC B CIDR*	區域
	Subnet in VPC A CIDR	pcx-aaaabbbb

路由表	目的地	目標
子網路 2 (VPCC)	*VPC C CIDR*	區域
	Subnet in VPC A CIDR	pcx-aaaacccc

回應流量的路由

如果您有多個具有重疊或匹配CIDR塊VPCs的對等，請確保已配置路由表，以避免將響應流量從您的發送VPC到不正VPC確的。VPC AWS 在檢查封包的來源 IP 並將回覆封包路由傳回至來源的VPC對等連線中，不支援單點傳送反向路徑轉送。

例如，VPCA 與 VPC B 和 C 對等，B 和 VPC VPC C VPC 具有匹配CIDR塊，並且它們的子網具有匹配CIDR的塊。VPCB 中子網路 2 的路由表指VPC向對等連接pcx-aaaabbbb以存取 VPC A 子網路。路由表格設定為傳送目的地至對等連線的VPCCIDR流量。VPC pcx-aaaaccccc

路由表	目的地	目標
子網路 2 (VPCB)	*VPC B CIDR*	區域
	Subnet in VPC A CIDR	pcx-aaaabbbb
VPCA	*VPC A CIDR*	區域
	VPC C CIDR	pcx-aaaacccc

假設 VPC B 中子網路 2 中的執行個體會使用VPC對等連線pcx-aaaabbbb將流量傳送到 VPC A 中的 Active Directory 伺服器。VPC會將回應流量傳送至作用中目錄伺服器。不過，路由表格設定為將VPCCIDR範圍內的所有流量傳送至VPC對等連pcx-aaaacccc線。VPC如果 VPC C 中的子網路 2 具有與子網中兩個子網路中的執行個體具有相同 IP 位址的VPC執行個體，則會從 VPC A 接收來自 A 的回應流量。VPC B 中子網路 2 中的執行個體不會收到對 VPC A 的要求的回應。

若要避免這種情況發生，您可以將特定路由新增至 VPC A 路由表格，而 VPC B 中CIDR的子網路 2 作為目的地和目標pcx-aaaabbbb。新路由較為明確，因此傳送至子網路 2 的流量會路CIDR由至VPC對等連線 pcx-aaaabbbb

或者，在下列範例中，VPCA 路由表具有每個對VPC等連線的每個子網路的路由。VPCA 可以與 B 中的子網路 VPC B 和 VPC C 中的子網路 A 通訊，如果您需要新增另一個與 VPC B 和 VPC C 位於相

同位址範圍內的子網路的對VPC等連線，這個案例很有用，您只需為該特定子網路新增另一個路由即可。

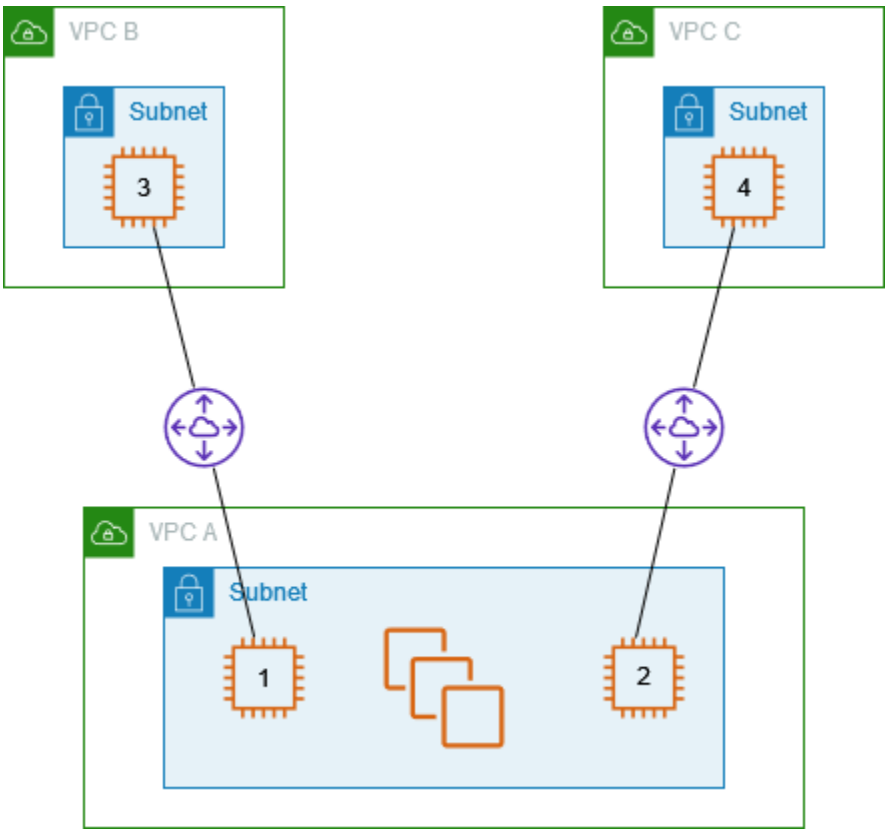
目的地	目標
VPC A CIDR	區域
Subnet 2 CIDR	pcx-aaaabbbb
Subnet 1 CIDR	pcx-aaaacccc

或者，根據您的使用案例，您可以在 VPC B 中建立通往特定 IP 位址的路由，以確保流量路由回正確的伺服器 (路由表使用最長的前綴相符來排列路由的優先順序)：

目的地	目標
VPC A CIDR	區域
Specific IP address in subnet 2	pcx-aaaabbbb
VPC B CIDR	pcx-aaaacccc

一個執行個體中VPC存取兩個特定執行個體 VPCs

在這種配置中，有一個中央VPC（VPCA）與一個子網，VPCA 和 VPC B（pcx-aaaabbbb）之間的對等連接以及 VPC A 和 VPC C（pcx-aaaacccc）之間的對等連接。VPCA 有一個子網路，每個對等連線都有一個執行個體。您可以使用此組態將對等互連流量限制為特定執行個體。

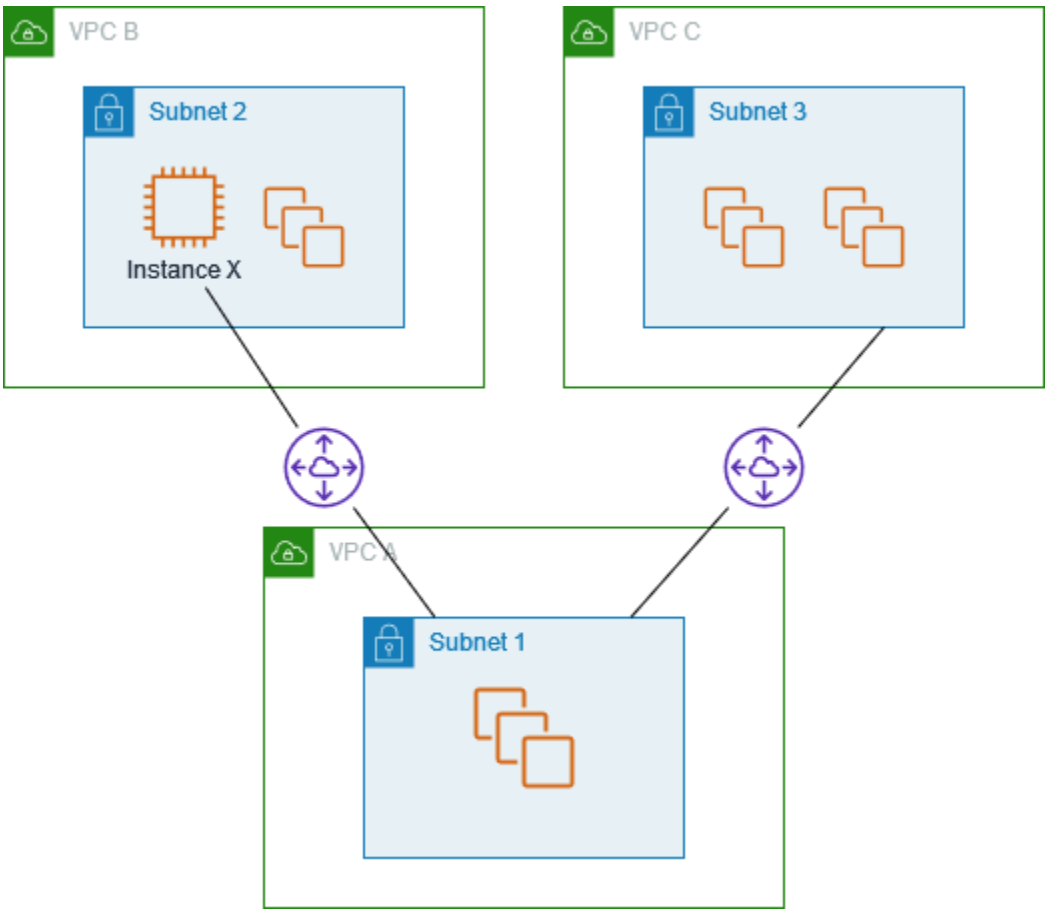


每個VPC路由表都指向相關的VPC對等連接，以訪問對等VPC中的單個 IP 地址（因此是特定的實例）。

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	Instance 3 IP address	pcx-aaaabbbb
	Instance 4 IP address	pcx-aaaacccc
VPCB	*VPC B CIDR*	區域
	Instance 1 IP address	pcx-aaaabbbb
VPCC	*VPC C CIDR*	區域
	Instance 2 IP address	pcx-aaaacccc

一個VPCVPCs使用最長前綴匹配訪問兩個

在這種配置中，有一個中央VPC（VPCA）與一個子網，VPCA 和 VPC B（pcx-aaaabbbb）之間的對等連接以及 VPC A 和 VPC C（pcx-aaaacccc）之間的對等連接。VPCB 和 VPC C 具有匹配CIDR塊。您可以使用VPC對等連pcx-aaaabbbb線，在 VPC A 和 VPC B 中的特定執行個體之間路由流量路由傳送至 VPC VPC B 和 VPC C 共用之CIDR位址範圍的所有其他流量。pcx-aaaacccc



VPC路由表使用最長的前綴匹配來選擇所需的對VPC等連接中最特定的路由。所有其他流量都會透過下一個相符路由 (在此情況下) 透過VPC對等連pcx-aaaacccc線進行路由。

路由表	目的地	目標
VPCA	*VPC A CIDR block*	區域
	Instance X IP address	pcx-aaaabbbb
	VPC C CIDR block	pcx-aaaacccc

路由表	目的地	目標
VPCB	*VPC B CIDR block*	區域
	VPC A CIDR block	pcx-aaaabbbb
VPCC	*VPC C CIDR block*	區域
	VPC A CIDR block	pcx-aaaacccc

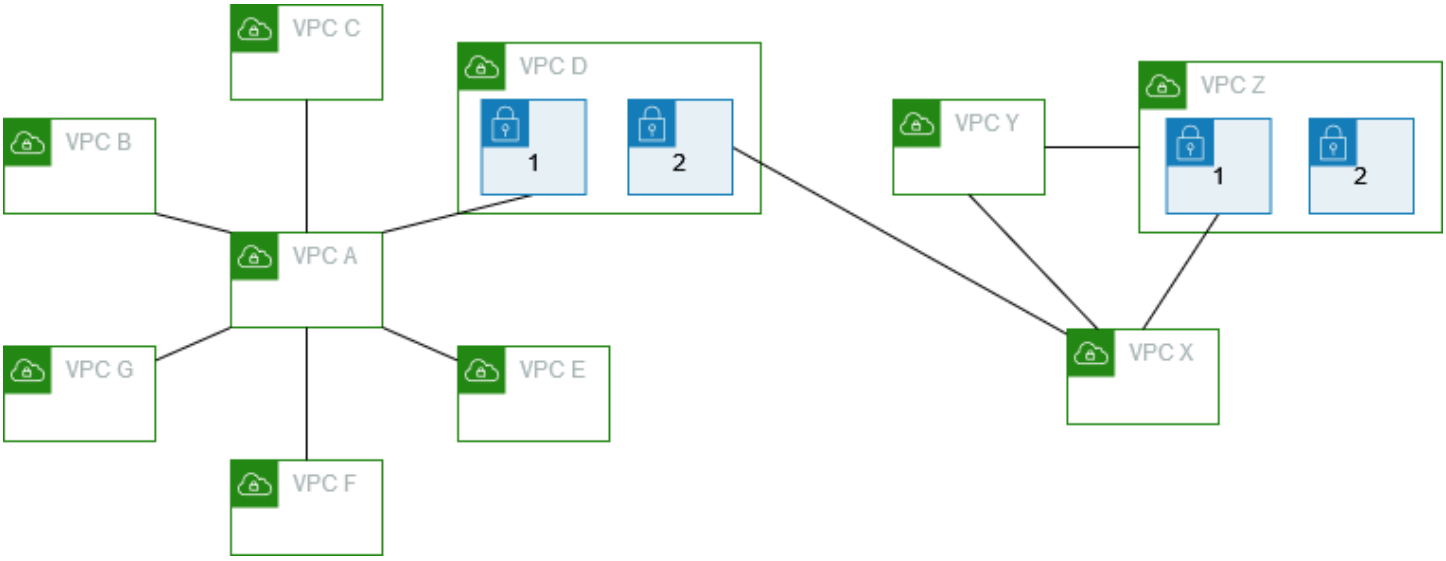
> **Important**
>
> 如果 VPC B 中執行個體 X 以外的執行個體將流量傳送到 VPC A，則回應流量可能會路由到 VPC C 而不是 VPC B。如需詳細資訊，請參閱回應流量的路由。

多種VPC配置

在此配置中，有一個中央VPC（VPCA）在支點配置VPCs中與多個對等。在完整網格組態中，您也有三個 VPCs (VPCsX、Y 和 Z) 對等。

VPCD 還與 VPC X（`pcx-ddddxxxx`）具有VPC對等連接。VPCA 和 VPC X 具有重疊的CIDR塊。這意味著 VPC A 和 VPC D 之間的對等流量僅限於 D 中的特定子網（子網路 1），這是為了確保如果 VPC D 接收來自 VPC A 或 VPC X 的請求，它會將響應流量發送到正VPC確的VPC。 AWS 在檢查封包的來源 IP 並將回覆封包路由傳回至來源的VPC對等連線中，不支援單點傳送反向路徑轉送。如需詳細資訊，請參閱回應流量的路由。

同樣，VPCD 和 VPC Z 具有重疊的CIDR塊。VPCD 和 VPC X 之間的對等流量限制為 VPC D 中的子網路 2，VPCX 和 VPC Z 之間的對等流量限制為 VPC Z 中的子網路 1。這是為了確保如果 VPC X 接收來自 VPC D 或 VPC Z 的對等流量，它會將回應流量傳送回正確的回應流量。VPC



VPCsB、C、E、F 和 G 的路由表指向相關的對等連接以存取 A 的完整CIDR區塊，而 VPC A 路由表則指向 VPCs B、C、E、F 和 G 的相關對等連接以存取其完整CIDR區塊。VPC對於對等連接pcx-aaaadddd，VPCA 路由表將流量路由到 VPC D 中的子網路 1，D 中的子網路 1 路由表指向 A 的完整CIDR區塊。VPC VPC

VPCY 路由表指向相關的對等連線以存取 VPC X 和 VPC Z 的完整CIDR區塊，VPCZ 路由表指向相關的對等連線以存取 Y 的完整區CIDR塊VPC。VPC Z 中的子網路 1 路由表指向相關對等連線，以存取 Y 的完整區CIDR塊VPC。VPC X 路由表指向存取 VPC D 中子網路 2 和 Z 中的子網路 2 的相關對等連線。VPC

路由表	目的地	目標
VPCA	*VPC A CIDR*	區域
	VPC B CIDR	pcx-aaaabbbb
	VPC C CIDR	pcx-aaaacccc
	Subnet 1 CIDR in VPC D	pcx-aaaadddd
	VPC E CIDR	pcx-aaaaeeee
	VPC F CIDR	pcx-aaaaffff
	VPC G CIDR	pcx-aaaagggg

路由表	目的地	目標
VPCB	*VPC B CIDR*	區域
	VPC A CIDR	pcx-aaaabbbb
VPCC	*VPC C CIDR*	區域
	VPC A CIDR	pcx-aaaacccc
VPCD 中的子網路 1	*VPC D CIDR*	區域
	VPC A CIDR	pcx-aaaadddd
VPCD 中的子網路 2	*VPC D CIDR*	區域
	VPC X CIDR	pcx-ddddxxxx
VPCE	*VPC E CIDR*	區域
	VPC A CIDR	pcx-aaaaeeee
VPCF	*VPC F CIDR*	區域
	VPC A CIDR	pcx-aaaaffff
VPCG	*VPC G CIDR*	區域
	VPC A CIDR	pcx-aaaagggg
VPCX	*VPC X CIDR*	區域
	Subnet 2 CIDR in VPC D	pcx-ddddxxxx
	VPC Y CIDR	pcx-xxxxyyyy
	Subnet 1 CIDR in VPC Z	pcx-xxxxzzzz
VPCY	*VPC Y CIDR*	區域
	VPC X CIDR	pcx-xxxxyyyy

路由表	目的地	目標
	VPC Z CIDR	pcx-yyyyzzzz
VPCZ	*VPC Z CIDR*	區域
	VPC Y CIDR	pcx-yyyyzzzz
	VPC X CIDR	pcx-xxxxzzzz

VPC對等連線網路案例

您VPCs可能需要VPC在您的或您擁有的帳戶和不同 AWS 帳戶之間設置VPC對等連接的原因有很多。VPC下列案例可協助您判斷哪種組態最符合您的聯網需求。

案例

- 對等兩個或兩個以上以VPCs提供資源的完整存取權
- 對等互連以存VPC取集中式資源

對等兩個或兩個以上以VPCs提供資源的完整存取權

在這個案例中，您有兩個或更多VPCs您想要對等，以啟用所有資源之間的完整共用VPCs。下列是一些範例：

- 您的公司有一VPC個財務部門，另一個VPC用於會計部門。財務部門需要存取所有位於會計部門的資源，會計部門也需要存取所有位於財務部門的資源。
- 您的公司有多個 IT 部門，每個部門都有自己的VPC。VPCs有些位於同一 AWS 帳戶內，而另一些則位於不同的 AWS 帳戶中。您想要將所有人對等，VPCs以便 IT 部門能夠完全存取彼此的資源。

如需如何針對此案例設定VPC對等連線組態和路由表的詳細資訊，請參閱下列文件：

- 兩個VPCs凝聚在一起
- 三個VPCs凝聚在一起
- 多個VPCs對等在一起

如需在 Amazon VPC 主控台中建立和使用VPC對等連線的詳細資訊，請參閱使用VPC對等連接。

對等互連以存VPC取集中式資源

在這個案例中，您有一個中央VPC，其中包含您想要與其他人共用的資源VPCs。您的中心VPC可能需要對對等端的完全或部分訪問權限VPCs，同樣地，對等VPCs可能需要對中央的完全或部分訪問權限VPC。下列是一些範例：

- 您公司的 IT 部門有一VPC個文件共享。您想要對等VPCs到該中心VPC，但是，您不希望對VPCs方互相發送流量。

- 您的公司有一VPC個您想要與客戶分享的內容。每個客戶都可以與您建立VPC對等連線VPC，但是，您的客戶無法將流量路由VPCs到與您對等的其他客戶，也無法察覺其他客戶的路由。
- 你有一個用VPC於活動目錄服務的中心。對等VPCs傳送要求中的特定執行個體至 Active Directory 伺服器，且需要對中央的完整存取權VPC。中央VPC不需要對等端的完整存取權VPCs，只需要將回應流量路由到特定的執行個體。

如需在 Amazon VPC 主控台中建立和使用VPC對等連線的詳細資訊，請參閱使用VPC對等連接。

對等互連的身分識別與存取VPC管理

依預設，使用者無法建立或修改VPC對等連線。若要授與VPC對等資源的存取權，請將IAM原則附加至IAM身分識別，例如角色。

範例

- 範例：建立對VPC等連線
- 範例：接受對VPC等連線
- 範例：刪除對VPC等連線
- 範例：在特定帳戶內運作
- 範例：使用主控台VPC管理對等連線

如需 Amazon 動VPC作的清單，以及每個動作的支援資源和條件金鑰，請參閱服務授權參考EC2中適用於 Amazon 的動作、資源和條件金鑰。

範例：建立對VPC等連線

下列原則會授與Purpose=Peering使VPCs用者使用標記為標記的VPC對等連線要求的權限。第一個陳述式會將條件 key (ec2:ResourceTag) 套用至資VPC源。請注意，CreateVpcPeeringConnection動作的VPC資源始終是請求者VPC。

第二個陳述式會授與使用者建立VPC對等連線資源的權限，因此會使用 * 萬用字元來取代特定資源ID。

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*"
    }
  ]
}
```

下列政策授予指定 AWS 帳戶中的使用者使用指定區域VPC中的任何建立對VPC等連線的權限，但前提是接受對等連線的是特定帳戶VPC中的特定連線時。VPC

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
        }
      }
    }
  ]
}
```

範例：接受對VPC等連線

下列原則授與使用者接受來自特定 AWS 帳戶VPC之對等連線要求的權限。這有助於防止使用者接受來自未知帳戶的VPC對等連線要求。該陳述式使用 ec2:RequesterVpc 條件金鑰強制執行此作業。

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

```
      "Effect":"Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id-2:vpc/*"
        }
      }
    }
  ]
}
```

如果VPC具有標籤Purpose=Peering，下列原則會授與使用者接受VPC對等連接要求的權限。

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "ec2:AcceptVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Peering"
        }
      }
    }
  ]
}
```

範例：刪除對VPC等連線

下列策略授與指定帳戶中的使用者刪除任何VPC對等連線的權限，但使用指定VPC連線 (位於相同帳戶的使用者除外)。原則會指定ec2:AccepterVpc和ec2:RequesterVpc條件索引鍵，因為VPC可能是原始對等連線要求VPC中的要求者VPC或VPC對等。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
```

```
      "Action": "ec2:DeleteVpcPeeringConnection",
      "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnNotEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id",
          "ec2:RequesterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    }
  ]
}
```

範例：在特定帳戶內運作

下列原則授與使用者在特定帳戶內使用VPC對等連線的權限。使用者可以檢視、建立、接受、拒絕和刪除VPC對等連線，前提是這些連線都在同一個 AWS 帳戶內。

第一個陳述式會授與使用者檢視所有VPC對等連線的權限。在這種情況下，Resource元素需要使用 * 萬用字元，因為此API動作 (DescribeVpcPeeringConnections) 目前不支援資源層級權限。

第二個陳述式會授予使用者建立VPC對等連線的權限，以及存取指定帳戶VPCs中所有連線的權限，以便這麼做。

第三個陳述式使用 * 萬用字元做為Action元素的一部分，以授與所有VPC對等連線動作的權限。條件鍵可確保只能在屬於帳戶一部分的VPC對等連VPCs線上執行動作。例如，如果接受者或請求者位於不VPC同的帳戶中，則使用者無法刪除VPC對等連線。使用者無法使用不同帳戶建立VPC對等連線。VPC

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeVpcPeeringConnections",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["ec2:CreateVpcPeeringConnection","ec2:AcceptVpcPeeringConnection"],
      "Resource": "arn:aws:ec2:*:account-id:vpc/*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcPeeringConnection",
      "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
      "Condition": {
        "ArnEquals": {
          "ec2:AccepterVpc": "arn:aws:ec2:*:account-id:vpc/*",
          "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
        }
      }
    }
  ]
}
```

範例：使用主控台VPC管理對等連線

若要在 Amazon VPC 主控台中檢視VPC對等連線，使用者必須擁有使用該ec2:DescribeVpcPeeringConnections動作的權限。若要使用 Create Peering Connection (建立對等連線) 頁面，使用者必須具備使用 ec2:DescribeVpcs 動作的許可。這會授予他們檢視和選取的權限VPC。您可以將資源層級許可套用至所有 ec2:*PeeringConnection 動作 (但 ec2:DescribeVpcPeeringConnections 除外)。

下列原則會授與使用者檢視VPC對等連線的權限，以及使用 [建立VPC對等連線] 對話方塊，僅使用特定要求者建立VPC對等連線。VPC如果使用者嘗試使用不同的要求者建立VPC對等連線VPC，則要求會失敗。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect":"Allow",
      "Action": "ec2:CreateVpcPeeringConnection",
      "Resource": [
        "arn:aws:ec2:*:*:vpc/vpc-id",
```

```
        "arn:aws:ec2:*:*:vpc-peering-connection/*"
      ]
    }
  ]
}
```

VPC帳戶的對等連線配額

VPC對等連接允許您連接兩個VPCs。這可讓其中一個VPC資源與另一個資源進行通訊，就VPC像它們位於同一個網路中一樣。VPC無論是位於相同地區還是不同 AWS 區域VPCs，對等互連都是非常有用的功能。本節說明使用VPC對等連線時應注意的配額。

下表列出 AWS 帳戶對VPC等連線的配額 (先前稱為限制)。除非另做說明，否則您可以請求提高這些配額。

如果您發現目前的VPC對等連線需求超出預設配額，我們建議您提交提高服務限制要求。我們將審查您的使用案例，並與您合作相應地調整配額，確保您的VPC環境能夠滿足您不斷增長的業務需求。

名稱	預設	可調整
作用中VPC對等連線 (每個) VPC	50	是 (最多 125 個)
未完成VPC的對等連線要求	25	是
未接受的對VPC等連線要求到期時間	1 星期 (168 小時)	否

如需使用對VPC等連線之規則的詳細資訊，請參閱VPC對等限制。如需 Amazon 配額的其他相關資訊 VPC，請參閱 Amazon VPC使用者指南中的 Amazon VPC 配額。

Amazon 對VPC等互連指南的文檔歷史記錄

下表說明 Amazon 對VPC等互連指南的文件版本。

變更	描述	日期
建立時的標籤	您可以在建立VPC對等連接和路由表格時新增標籤。	2020 年 7 月 20 日
區域間的對等互連	DNS亞太區域 (香港) 區域內的區域間VPC對等連線支援主機名稱解析。	2019 年 8 月 26 日
區域間的對等互連	您可以VPCs在不同 AWS 區域之間建立VPC對等連線。	2017 年 11 月 29 日
DNS對VPC等互連的解析度支援	您可以啟用本機，在從VPC對等中的執行個體查詢時，將公用DNS主機名稱解析為私有 IP 位址。VPC	2016 年 7 月 28 日
過時的安全群組規則	您可以識別您的安全性群組是否正在對等中的安全性群組的規則中參考，而VPC且您可以識別過時的安全性群組規則。	2016 年 5 月 12 日
透 ClassicLink 過VPC對等連線使用	您可以修改對等連線，讓本機連結 EC2-VPC Classic 執行個體與對等中的執行個體進行通訊VPC，反之亦然。	2016 年 4 月 26 日
VPC凝視	您可以在兩者VPC之間建立VPC對等連線VPCs，讓中的執行個體使用私有 IP 位址彼此通訊	2014 年 3 月 24 日

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。