aws

使用者指南

Amazon Virtual Private Cloud



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

「什麼是 Amazon VPC？」 1
功能 1
Amazon VPC 入門 2
使用 Amazon VPC 2
Amazon VPC 的定價 3
Amazon VPC 如何工作 5
VPC 和子網 6
預設和非預設 VPC 6
路由表 6
存取網際網路 7
存取公司或家用網路 8
連接 VPC 和網路 8
AWS 私有全球網路 8
規劃您的 VPC 10
註冊 AWS 帳戶 10
註冊 AWS 帳戶 10
驗證許可 10
確定您的 IP 地址範圍 10
選取您的可用區域 11
規劃您的網際網路連線 11
建立您的 VPC 12
部署您的應用程式 12
IP 定址 13
私有 IPv4 地址 14
公有 IPv4 地址 14
IPv6 地址 15
公有 IPv6 地址 16
私有 IPv6 地址 16
使用您自己的 IP 地址 18
使用 Amazon VPC IP 地址管理員 18
VPC CIDR 區塊 18
IPv4 VPC CIDR 區塊 19
管理 VPC 的 IPv4 CIDR 區塊 20
IPv4 CIDR 區塊關聯限制 22

IPv6 VPC CIDR 區塊 24
子網路 CIDR 區塊 24
IPv4 的子網路規模調整 25
IPv6 的子網規模 26
比較 IPv4 和 IPv6 26
受管理的字首清單 28
字首清單的概念和規則 28
字首清單的 Identity and Access Management 29
由客戶管理之前綴清單 30
AWS管理的字首清單 39
使用字首清單最佳化 AWS 基礎設施管理 41
AWS IP 地址範圍 43
下載 44
輸出控制 45
地理位置提要 45
尋找位址範圍 45
語法 51
訂閱 通知 56
VPC 的 IPv6 支援 58
新增 VPC 的 IPv6 支援 58
雙堆疊 VPC 範例 62
上的 IPv6 支援 AWS 64
支援 IPv6 的服務 64
其他 IPv6 支援 77
進一步了解 77
Virtual Private Cloud (VPC) 78
VPC 基本概念 79
VPC IP 地址範圍 79
VPC 圖表 79
VPC 資源 80
VPC 組態選項 81
預設 VPC 82
預設 VPC 元件 83
預設子網路 85
使用預設 VPC 和預設子網路 85
建立 VPC 89

建立 VPC 以及其他 VPC 資源 89
僅建立 VPC 91
使用 AWS CLI 建立 VPC 93
視覺化 VPC 中的資源 97
新增或移除 CIDR 區塊 98
DHCP 選項集 100
什麼是 DHCP？ 101
DHCP 選項集概念 101
使用 DHCP 選項集 104
DNS 屬性 108
認識 Amazon DNS 109
檢視 EC2 執行個體的 DNS 主機名稱 113
檢視和更新 VPC 的 DNS 屬性 114
網路地址使用 115
超過 NAU 配額 116
NAU 的計算方式 116
NAU 範例 117
共用 VPC 子網路 119
共用子網路先決條件 119
使用共用子網路 120
適用於擁有者及參與者的計費和計量 122
擁有者和參與者的責任與許可 123
AWS 資源和共用 VPC 子網路 125
將 VPC 擴展至另一個區域 127
AWS 本機區域中的子網路 127
中的子網路 AWS Wavelength 132
中的子網路 AWS Outposts 134
刪除您的 VPC 135
使用主控台進行刪除 136
使用 CLI 進行刪除 137
從主控台操作產生基礎設施即程式碼 138
子網 139
子網基本概念 139
子網路 IP 地址範圍 139
子網類型 140
子網圖表 140

子網路由 141
子網設定 141
子網安全 142
建立子網 142
從您的子網路中新增或移除 IPv6 CIDR 區塊 144
修改子網路的公有 IP 位址屬性 145
子網路 CIDR 保留 146
透過主控台使用子網路 CIDR 保留 146
透過 AWS CLI 使用子網路 CIDR 保留 147
路由表 148
路由表概念 149
子網路由表 150
閘道路由表 156
路由優先順序 159
路由選項範例 161
建立路由表與路由 174
管理子網路路由表 176
取代主路由表 179
將路由表與閘道建立關聯 180
取代或還原本機路由的目標 181
進階路由 182
對連線能力問題進行疑難排解 225
中間設備路由精靈 226
中間設備路由精靈的先決條件 226
將 VPC 流量重新導向至安全設備 227
中間設備路由精靈的考量事項 229
中間設備案例 229
刪除子網路 238
連線 VPC 239
網際網路閘道 240
網際網路閘道基礎知識 241
建立網際網路閘道 243
刪除網際網路閘道 245
輸出限定網際網路閘道 246
輸出限定網際網路閘道基本概念 247
將僅輸出網際網路存取新增至子網路 248

NAT 裝置 250
NAT 閘道 252
NAT 執行個體 296
比較 NAT 裝置 307
彈性 IP 位址 309
彈性 IP 位址概念和規則 309
開始使用彈性 IP 位址 311
AWS 傳輸閘道 319
AWS Virtual Private Network 320
VPC 對等連線 321
監控 322
VPC 流程日誌 323
流量日誌基礎知識 324
流量日誌記錄 327
流量日誌記錄範例 341
流量日誌限制 350
定價 354
使用流量日誌工作 355
發佈至 CloudWatch Logs 358
發佈到 Amazon S3 365
發布至 Amazon Data Firehose 373
使用 Athena 查詢 381
VPC 流程日誌中的身分和存取管理 385
疑難排解 392
CloudWatch 指標 396
NAU 指標與維度 396
啟用或停用 NAU 監控 399
NAU CloudWatch 警示範例 399
帳單和用量報告 400
IP 位址管理 401
VPC 端點 401
傳輸閘道 402
網路分析 403
流量鏡射 403
VPC Lattice 403
跨帳戶/區域資源數量 404

描述 VPC 網路 404
地理位置 405
子網路 406
網路連線 407
安全控制項 412
流量管理 413
相關資源 416
安全 417
資料保護 417
網際網路流量隱私權 418
強制執行傳輸中的 VPC 加密 419
加密控制模式 419
監控流量流程的加密狀態 420
VPC 加密控制排除 421
實作工作流程 421
VPC 加密控制狀態 422
AWS 服務支援和相容性 422
定價 3
AWS CLI 命令參考 427
其他資源 427
Identity and Access Management 428
目標對象 428
使用身分進行驗證 429
使用政策管理存取權 430
Amazon VPC 如何與 IAM 搭配運作 431
政策範例 435
疑難排解 447
AWS 受管政策 448
使用服務連結角色 451
基礎設施安全 455
網路隔離 456
控制網路流量 456
比較安全群組和網路 ACL 457
Security groups (安全群組) 458
安全群組基礎知識 459
安全群組範例 461

安全群組規則 462
預設安全群組 466
建立安全群組 467
設定安全群組規則 469
刪除安全群組 471
將安全群組與多個 VPC 建立關聯 471
與 AWS Organizations 共用安全群組 474
網路 ACL 479
網路 ACL 基本概念 480
網路 ACL 規則 482
預設網路 ACL 483
自訂網路 ACL 484
路徑 MTU 探索 488
建立網路 ACL 489
管理網路 ACL 關聯 492
刪除網路 ACL 495
範例：控制對子網路中執行個體的存取 496
恢復能力 499
法規遵循驗證 499
封鎖對 VPC 和子網路的公開存取 500
VPC BPA 基礎知識 500
評估 VPC BPA 的影響並監控 VPC BPA 506
進階範例 510
最佳實務 562
搭配使用 與其他 服務 563
AWS PrivateLink 563
AWS Network Firewall 565
Route 53 Resolver DNS Firewall 566
Reachability Analyzer 567
範例 568
測試環境 569
概要 569
1. 建立 VPC 571
2. 部署您的應用程式 572
3. 測試組態 572
4. 清除 572

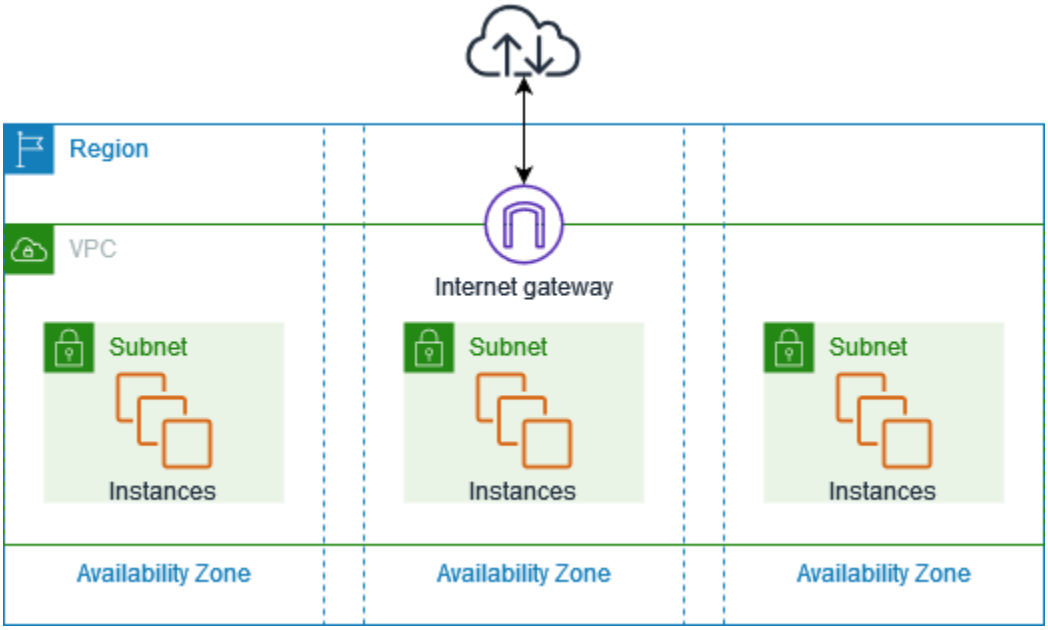
網頁和資料庫伺服器 573
概要 573
1. 建立 VPC 577
2. 部署您的應用程式 578
3. 測試組態 578
4. 清除 579
私有伺服器 579
概要 579
1. 建立 VPC 581
2. 部署您的應用程式 582
3. 測試組態 583
4. 清除 583
教學課程 584
使用 開始使用 Amazon VPC AWS CLI 584
先決條件 584
建立 VPC 585
建立子網路 586
設定網際網路連線 587
建立 NAT 閘道 589
設定子網路 590
建立安全群組 590
驗證 VPC 組態 591
部署 EC2 執行個體 592
疑難排解 195
清除資源 595
生產環境部署須知 597
後續步驟 597
透過 AWS CLI 建立包含私有子網路與 NAT 閘道的 VPC 597
必要條件 584
建立 VPC 與子網路 599
建立與設定網際網路連線 601
建立 NAT 閘道 602
建立 Amazon S3 的 VPC 端點 604
設定安全群組 604
建立 EC2 執行個體的啟動範本 605
建立負載平衡器與目標群組 607

建立 Auto Scaling 群組 608
測試組態 608
清除資源 595
後續步驟 597
配額 612
VPC 和子網路 612
DNS 612
彈性 IP 位址 613
閘道 613
由客戶管理之前綴清單 614
網路 ACL 614
網路介面 615
路由表 615
路由伺服器 616
Security groups (安全群組) 617
VPC 子網路共用 618
網路地址使用 619
Amazon EC2 API 調節 619
額外配額資源 619
文件歷史記錄 620
..... dcxxviii

「什麼是 Amazon VPC？」

使用 Amazon Virtual Private Cloud (Amazon VPC)，您可以在您定義的邏輯隔離虛擬網路中啟動 AWS 資源。這個虛擬網路與您在資料中心中操作的傳統網路非常相似，且具備使用 AWS可擴展基礎設施的優勢。

下圖顯示了範例 VPC。此 VPC 在區域的每個可用區域中具有一個子網路、在每個子網路中具有多個 EC2 執行個體，還有一個網際網路閘道，可允許您 VPC 和網際網路中資源之間的通訊。



如需詳細資訊，請參閱「Amazon Virtual Private Cloud (Amazon VPC)」。

功能

下列功能可協助您設定 VPC，以提供應用程式所需的連線：

虛擬私有雲端 (VPC)

VPC 是虛擬網路，非常近似於您在自有資料中心內運作的傳統網路。建立 VPC 後，您可以新增子網。

子網路

子網是您的 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。新增子網路後，您可以在 VPC 中部署 AWS 資源。

IP 定址

您可以將 IP 地址 (包括 IPv4 和 IPv6) 指派給 VPC 和子網路。您也可以將公有 IPv4 地址和 IPv6 GUA 地址帶到 AWS ，並將其配置給 VPC 中的資源，例如 EC2 執行個體、NAT 閘道和 Network Load Balancer。

路由

使用路由表決定子網或閘道中的網路流量導向何處。

閘道和端點

閘道會將 VPC 連線至另一個網路。例如，您可使用網際網路閘道將 VPC 連線至網際網路。使用 VPC 端點私 AWS 服務 下連接到 ，而無需使用網際網路閘道或 NAT 裝置。

對等互連

使用 VPC 對等互連可在兩個 VPC 中的資源之間路由流量。

流量鏡射

從網路介面複製網路流量，然後將其傳送至安全和監控設備進行深入封包檢查。

傳輸閘道

使用做為中央中樞的傳輸閘道，在 VPCs、VPN 連線和 Direct Connect 連線之間路由流量。

VPC 流量日誌

流量日誌會擷取傳入和傳出 VPC 網路介面之 IP 流量的資訊。

VPN 連線

使用 AWS Virtual Private Network (Site-to-Site VPN) 將 VPC 連線至內部部署網路。

Amazon VPC 入門

您的 在每個 中 AWS 帳戶 包含預設 VPC AWS 區域。預設 VPC 經過設定，因此您可立即開始啟動並連線至 EC2 執行個體。如需詳細資訊，請參閱規劃您的 VPC。

您可以選擇使用所需的子網、IP 地址、閘道和路由來建立其他 VPC。如需詳細資訊，請參閱the section called “建立 VPC”。

使用 Amazon VPC

您可以使用下列任一介面來建立和管理 VPC：

- AWS 管理主控台：提供 Web 介面，您可使用此介面來存取 VPC。
- AWS Command Line Interface (AWS CLI) — 為廣泛的 AWS 服務提供命令，包括 Amazon VPC，並在 Windows、Mac 和 Linux 上支援 。如需詳細資訊，請參閱AWS Command Line Interface。
- AWS SDKs — 提供語言特定的 APIs，並負責許多連線詳細資訊，例如計算簽章、處理請求重試和錯誤處理。如需詳細資訊，請參閱 AWS 開發套件。
- Query API — 提供您可以使用 HTTPS 請求呼叫的低層級 API 動作。使用查詢 API 是存取 Amazon VPC 最直接的方式，但這需要您的應用程式能處理低階詳細資訊，例如產生雜湊以簽署請求以及錯誤處理。如需詳細資訊，請參閱 Amazon EC2 API 參考中的 Amazon IPAM 動作。

Amazon VPC 的定價

使用 VPC; 無需負擔額外費用。然而，某些 VPC 元件需付費，例如 NAT 閘道、IP 位址管理員、流量鏡像、Reachability Analyzer 和網路存取分析器。如需詳細資訊，請參閱 Amazon VPC 定價。

您在虛擬私有雲端 (VPC) 中啟動的幾乎所有資源都提供用於連線的 IP 位址。VPC 中的絕大多數資源都使用私有 IPv4 地址。然而，需要透過 IPv4 直接存取網際網路的資源會使用公有 IPv4 地址。

Amazon VPC 可讓您啟動受管服務，例如 Elastic Load Balancing、Amazon RDS 和 Amazon EMR，而無需事先設定 VPC。如果您擁有預設 VPC，它會使用您帳戶中的預設 VPC 來執行此操作。由受管服務佈建到您帳戶的任何公有 IPv4 地址都會產生費用。這些費用將與 中的 Amazon VPC 服務相關聯 AWS Cost and Usage Report。

公有 IPv4 地址的定價

公有 IPv4 地址是可從網際網路路由的 IPv4 地址。若要透過 IPv4 從網際網路直接存取資源，必須使用公有 IPv4 地址。

如果您是現有或新的 AWS 免費方案客戶，您可免費使用 EC2 服務並取得 750 小時的公有 IPv4 地址使用量。如果您未在 AWS 免費方案中使用 EC2 服務，則會收取公有 IPv4 地址的費用。如需具體的定價資訊，請參閱《Amazon VPC 定價》中的 Public IPv4 address (公有 IPv4 地址) 索引標籤。

私有 IPv4 地址 (RFC 1918) 不收取費用。如需如何針對共用 VPC 收取公有 IPv4 地址費用的詳細資訊，請參閱擁有者和參與者的計費和計量。

公有 IPv4 地址具有下列類型：

- 彈性 IP 地址 EIPs)：Amazon 提供的靜態公有 IPv4 地址，您可以與 EC2 執行個體、彈性網路介面或 AWS 資源建立關聯。

- EC2 公有 IPv4 地址：Amazon 指派給 EC2 執行個體的公有 IPv4 地址 (如果 EC2 執行個體啟動到預設子網路，或者如果執行個體啟動到已設定為自動指派公有 IPv4 地址的子網路)。
- BYOIPv4 地址：在您 AWS 使用自有 IPv4 地址 (BYOIP) 帶至 的 IPv4 地址範圍內的公有 IPv4 地址。 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-byoip.html
- 服務受管 IPv4 地址：公有 IPv4 地址會自動佈建在 AWS 資源上，並由 AWS 服務管理。例如，Amazon ECS、Amazon RDS 或 Amazon WorkSpaces 上的公有 IPv4 地址。

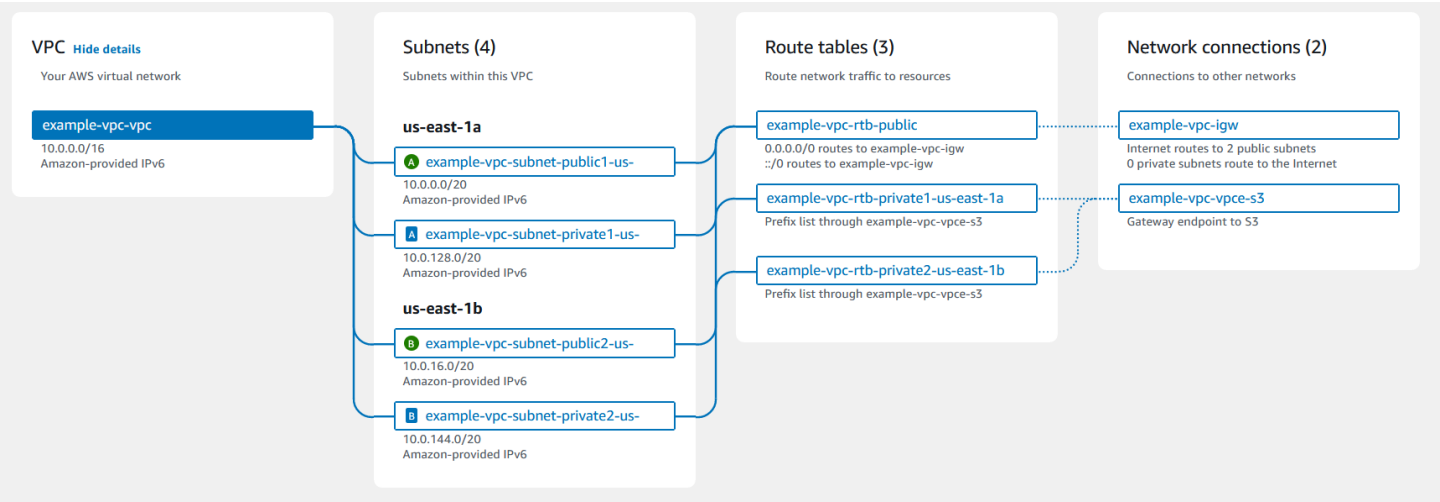
下列清單顯示可使用公有 IPv4 地址的最常見 AWS 服務。

- Amazon WorkSpaces 應用程式
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift Servers
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming for Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon Redshift
- AWS Site-to-Site VPN
- Amazon VPC NAT 閘道
- Amazon WorkSpaces
- Elastic Load Balancing

Amazon VPC 如何工作

使用 Amazon Virtual Private Cloud (Amazon VPC)，您可以在已定義的邏輯隔離虛擬網路中啟動 AWS 資源。這個虛擬網路與您在資料中心中操作的傳統網路非常相似，且具備使用 AWS可擴展基礎設施的優勢。

以下視覺效果呈現出使用 AWS 管理主控台建立 VPC 時所顯示的預覽窗格中的 VPC 及其資源。對於現有的 VPC，您可以在資源地圖索引標籤上存取此視覺化效果。此範例顯示當您選擇建立 VPC 和其他網路資源時，一開始在建立 VPC 頁面上選取的資源。此 VPC 的設定包含IPv4 CIDR 和 Amazon 提供的 IPv6 CIDR、兩個可用區域中的子網路、三個路由表、一個網際網路閘道，以及一個閘道端點。由於我們已選取網際網路閘道，因此視覺效果顯示來自公有子網路的流量會路由至網際網路，因為對應的路由表會將流量傳送至網際網路閘道。



概念

- VPC 和子網
- 預設和非預設 VPC
- 路由表
- 存取網際網路
- 存取公司或家用網路
- 連接 VPC 和網路
- AWS 私有全球網路

VPC 和子網

Virtual Private Cloud (VPC) 是您的 AWS 帳戶所專用的虛擬網路。它在邏輯上與 AWS 雲端中的其他虛擬網路隔離。您可以為 VPC 指定 IP 地址範圍、新增子網、新增閘道，以及與安全群組建立關聯。

子網是您的 VPC 中的 IP 地址範圍。您可以啟動 AWS 資源到子網，如 Amazon EC2 執行個體。您可以將子網連線至網際網路、其他 VPC 和您自己的資料中心，並使用路由表在子網往返路由流量。

進一步了解

- IP 定址
- Virtual Private Cloud (VPC)
- 子網

預設和非預設 VPC

若您是在 2013 年 12 月 4 日之後建立的帳戶，則帳戶在每個區域皆會有預設 VPC。預設 VPC 是已設定好可供您使用的 VPC。例如，VPC 在該區域的每個可用區域都有一個 預設子網路、一個連線的網際網路閘道、主路由表中將所有流量傳送到網際網路閘道的路由，以及 DNS 設定（可自動將公共 DNS 主機名稱分配給具有公共 IP 地址的執行個體，並透過 Amazon 提供的DNS伺服器啟用 DNS 解析的 DNS 設置 (參見 VPC 的 DNS 屬性) 因此，在預設子網中啟動的 EC2 執行個體會自動存取網際網路。若您在某個區域中具有預設 VPC，且在該區域啟動 EC2 執行個體時未指定子網，則我們會選擇其中一個預設子網，然後在該子網中啟動執行個體。

您也可以建立自己的 VPC，並根據需要進行設定。這稱為非預設 VPC。您在非預設 VPC 中建立的子網，以及您在預設 VPC 中建立的額外子網，稱為非預設子網。

進一步了解

- the section called “預設 VPC”
- the section called “建立 VPC”

路由表

路由表包含一組名為路由的規則，用來判斷來自 VPC 之網路流量的方向。您可以明確地將子網與特定路由表建立關聯。否則，子網會隱含地與主路由表相關聯。

路由表中的每個路由都會指定您想要傳送流量的 IP 地址範圍 (目的地)，以及傳送流量 (目標) 的閘道、網路介面或連線。

進一步了解

- 設定路由表

存取網際網路

您可以控制在 VPC 外部之 VPC 存取資源中啟動執行個體的方式。

預設 VPC 包含網際網路閘道，且每個預設子網皆為公有子網。您在預設子網中啟動的每個執行個體都具有私有 IPv4 地址和公有 IPv4 地址。這些執行個體可以透過網際網路閘道與網際網路通訊。網際網路閘道可讓您的執行個體透過 Amazon EC2 網路邊緣連線至網際網路。

根據預設，您在非預設子網中啟動的每個執行個體都具有私有 IPv4 地址，但不具有公有 IPv4 地址，除非您在啟動時特別為其指派公有 IPv4 地址，或修改子網的公有 IP 地址屬性。這些執行個體可以互相通訊，但無法存取網際網路。

您可以透過將網際網路閘道連接至其 VPC (如果其 VPC 不是預設 VPC)，並將彈性 IP 地址與該執行個體建立關聯，來為在非預設子網上啟動的執行個體啟用網路存取。

或者，您也可以使用網路地址轉譯 (NAT) 裝置，以允許 VPC 中的執行個體初始化網際網路傳出連線，但防止來自網際網路未經要求的傳入連線。NAT 會將多個私有 IPv4 地址映射至單一公有 IPv4 地址。您可以將 NAT 裝置設定為具有彈性 IP 地址，並透過網際網路閘道連線至網際網路。這樣一來，即可透過 NAT 裝置將私有子網中的執行個體連線至網際網路，NAT 裝置會將來自執行個體的流量路由至網際網路閘道，並將所有回應路由至該執行個體。

如果您將 IPv6 CIDR 區塊與 VPC 產生關聯，並將 IPv6 地址指派給執行個體，則執行個體可以透過網際網路閘道經由 IPv6 連線到網際網路。或者，執行個體也可以使用輸出限定網際網路閘道，經由 IPv6 初始化傳出到網際網路的連線。IPv6 流量與 IPv4 流量分開；您的路由表必須包含單獨的 IPv6 流量路由。

進一步了解

- 使用網際網路閘道啟用 VPC 的網際網路存取
- 使用輸出限定 (egress-only) 網際網路閘道來啟用傳出 IPv6 流量
- 使用 NAT 裝置連線至網際網路或其他網路

存取公司或家用網路

您可以選擇使用 IPsec 連線將 VPC 連接到自己的公司資料中心 AWS Site-to-Site VPN ，讓 AWS 雲端成為資料中心的延伸。

Site-to-Site VPN 連接包含 AWS 位於 端虛擬私有閘道或傳輸閘道之間的兩個 VPN 通道，以及位於您資料中心的客戶閘道裝置。客戶閘道裝置是在您這端的 Site-to-Site VPN 連線上配置的實體裝置或軟體裝置。

進一步了解

- AWS Site-to-Site VPN 使用者指南
- Amazon VPC 傳輸閘道

連接 VPC 和網路

您可以在兩個 VPC 之間建立 VPC 對等連線，透過此機制，您可以私下在兩者間路由流量。這兩個 VPC 中的執行個體能彼此通訊，有如位於相同網路中一樣。

您也可以建立傳輸閘道，並使用它來互連 VPC 和內部部署網路。傳輸閘道充當區域虛擬路由器，用於在其附件之間流動的流量，其中包括 VPCs、VPN 連接、 Direct Connect 閘道和傳輸閘道對等互連。

進一步了解

- Amazon VPC Peering Guide
- Amazon VPC 傳輸閘道

AWS 私有全球網路

AWS 提供高效能和低延遲的私有全球網路，可提供安全的雲端運算環境，以支援您的聯網需求。AWS 區域連接到多個網際網路服務提供者 (ISP) 以及私有全球網路骨幹，可為客戶傳送的跨區域流量提供增強的網路效能。

來自 AWS 網路上具有目的地 AWS 的網路的封包會保留在全球 AWS 網路上，但往返 AWS 中國區域和 AWS 歐洲主權雲端區域的流量除外。無論目的地是私有 IP 位址或公有 IP 位址，皆是如此。例如，兩個 VPC 中的 EC2 執行個體透過公有 IP 位址通訊，流量會保留在私有全域網路中。目的地可以位於相同的可用區域、相同區域中的不同可用區域，或不同的區域。

網路封包遺失有數個原因，包括網路流程碰撞、低層級 (Layer 2) 錯誤及其他網路故障。我們的網路設計和運作會盡可能減少封包遺失。我們跨連接 AWS 區域的 全球骨幹測量封包遺失率 (PLR)。我們骨幹網路的運作目標是每小時 PLR 的 p99，也就是少於 0.0001%。

規劃您的 VPC

完成下列任務，以準備建立和連接您的 VPC。完成後，您將能開始在 AWS上部署應用程式。

任務

- 註冊 AWS 帳戶
- 驗證許可
- 確定您的 IP 地址範圍
- 選取您的可用區域
- 規劃您的網際網路連線
- 建立您的 VPC
- 部署您的應用程式

註冊 AWS 帳戶

註冊 AWS 帳戶

若要開始使用 AWS，您需要 AWS 帳戶。如需建立 的相關資訊 AWS 帳戶，請參閱《 AWS 帳戶管理參考指南》中的 入門 AWS 帳戶。

驗證許可

您必須具有所需的許可，才能使用 Amazon VPC。如需詳細資訊，請參閱Amazon VPC 的身分和存取管理及Amazon VPC 原則範例。

確定您的 IP 地址範圍

您 VPC 中的資源能彼此相互通訊，也能使用 IP 地址來與網際網路上的資源進行通訊。建立 VPC 和子網路時，您可以選取其 IP 地址範圍。在子網路中部署 EC2 執行個體等資源時，它們會從子網路的 IP 地址範圍收到 IP 地址。如需詳細資訊，請參閱IP 定址。

選擇 VPC 的大小時，請考慮您的 AWS 帳戶 和 VPC 中需要多少個 IP 地址。確保您 VPC 的 IP 地址範圍不會與您自己網路的 IP 地址範圍重疊。如果您需要多個 VPC 之間的連線，則必須確保它們沒有重疊的 IP 地址。

IP 地址管理員 (IPAM) 可讓您更輕鬆地規劃、追蹤和監控您應用程式的 IP 地址。如需詳細資訊，請參閱《IP 地址管理員指南》。

選取您的可用區域

AWS 區域是我們叢集資料中心的實體位置，稱為可用區域。每個可用區域都具備獨立的電源、冷卻和實體安全措施，包含備援電源、聯網和連線能力。區域中的可用區域會以有意義的距離進行實體分隔，並透過高頻寬、低延遲聯網進行互連。您可以將應用程式設計為可在多個可用區域中執行，以達到更高的容錯能力。

生產環境

對於生產環境，我們建議您至少選取兩個可用區域，並在每個作用中的可用區域中平均部署 AWS 資源。

開發或測試環境

對於開發或測試環境，您可以選擇僅在一個可用區域中部署資源，以節省成本。

規劃您的網際網路連線

根據您的連線需求，透過規劃將每個 VPC 分成多個子網路。例如：

- 如果您有會接收來自網際網路上用戶端之流量的 Web 伺服器，請在每個可用區域中為這些伺服器建立子網路。
- 如果您也有只會接收來自 VPC 中其他伺服器之流量的伺服器，請在每個可用區域中為這些伺服器建立個別的子網路。
- 如果您有只會透過與您網路的 VPN 連線接收流量的伺服器，請在每個可用區域中為這些伺服器建立個別的子網路。

如果您的應用程式將接收來自網際網路的流量，則 VPC 必須有網際網路閘道。將網際網路閘道連接至不會自動讓執行個體可透過網際網路存取的 VPC。除了連接網際網路閘道之外，您必須以網際網路閘道的路由來更新子網路路由表。您也必須確保執行個體擁有公有 IP 地址與相關聯的安全群組，可允許透過應用程式要求的特定連接埠和通訊協定傳輸來自網際網路的流量。

或者，您也可以使用面向網際網路的負載平衡器註冊您的執行個體。負載平衡器會接收來自用戶端的流量，並將其分配到一或多個可用區域中已註冊的執行個體。如需詳細資訊，請參閱 Elastic Load Balancing。若要允許私有子網路中的執行個體存取網際網路 (例如，下載更新)，而不允許來自網際網

路的未經要求傳入連線，請在每個作用中可用區域中新增公有 NAT 閘道，並更新路由表以將網際網路流量傳送至 NAT 閘道。如需詳細資訊，請參閱the section called “從私有子網存取網際網路”。

建立您的 VPC

確定所需的 VPC 和子網路數目、要指派給 VPC 和子網路的 CIDR 區塊，以及如何將 VPC 連線至網際網路之後，您就可以開始建立 VPC 了。如果您使用 建立 VPC， AWS 管理主控台 並在組態中包含公有子網路，我們會為子網路建立路由表，並新增直接存取網際網路所需的路由。如需詳細資訊，請參閱the section called “建立 VPC”。

部署您的應用程式

建立 VPC 後，您就可以部署您的應用程式。

生產環境

針對生產環境，您可以使用下列其中一項服務，以在多個可用區域中部署伺服器、設定擴展，以維持應用程式所需的最少伺服器數目，以及使用負載平衡器註冊伺服器，以便在伺服器之間平均分配流量。

- Amazon EC2 Auto Scaling
- EC2 Fleet
- Amazon Elastic Container Service (Amazon ECS)

開發或測試環境

對於開發或測試環境，您可以選擇啟動單一 EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 入門。

您 VPC 和子網路的 IP 定址

IP 地址可讓您 VPC 中的資源彼此互相通訊，也能和網際網路上的資源通訊。

無類別域間路由 (CIDR) 標記法用於表示 IP 地址及其網路遮罩。這些地址的格式如下：

- 一個 IPv4 位址為 32 位元，由 4 組構成，每組最多 3 個十進位數字，範圍為 0-255。例如，10.0.1.0。
- 一個 IPv4 CIDR 區塊由一個 IPv4 位址後接斜線和一個 0 至 32 之間的數字構成。例如，10.0.0.0/16 代表從 10.0.0.0 至 10.0.255.255 的 65,536 個 IPv4 位址。
- 一個 IPv6 位址為 128 位元，由 8 個區段構成，每個區段包含 4 個十六進位數字。例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334。每個區段中無需包含前導零。您也可以在位址中，以雙冒號 (::) 一次性取代連續的全零區段。因此，範例位址可壓縮為 2001:db8:85a3::8a2e:370:7334。
- IPv6 CIDR 區塊包含以全零區段結尾的 IPv6 位址，其中全零區段已取代為雙冒號，後接斜線與 0 至 128 之間的數字。例如，2001:db8:1234:1a00::/56 代表 2^72 個 IPv6 位址，範圍從 2001:db8:1234:1a00:0000:0000:0000:0000 至 2001:db8:1234:1aff:ffff:ffff:ffff:ffff。

如需詳細資訊，請參閱什麼是 CIDR？

目錄

- 私有 IPv4 地址
- 公有 IPv4 地址
- IPv6 地址
- 使用您自己的 IP 地址
- 使用 Amazon VPC IP 地址管理員
- VPC CIDR 區塊
- 子網路 CIDR 區塊
- 比較 IPv4 和 IPv6
- 使用受管字首清單來整合和管理網路 CIDR 區塊
- AWS IP 地址範圍
- VPC 的 IPv6 支援
- AWS 支援 IPv6 的 服務

私有 IPv4 地址

私有 IPv4 地址 (本主題中又稱為私有 IP 地址) 無法透過網際網路存取，僅能用於您 VPC 中執行個體間的通訊。當您在 VPC 中啟動執行個體時，便會從子網路的 IPv4 位址範圍指派一個主要私有 IP 位址給執行個體的主要網路介面 (例如 eth0)。每個執行個體也會獲得一個私有 (內部) DNS 主機名稱，可解析為執行個體的私有 IP 地址。主機名稱可以是兩種類型：資源型或 IP 型。如需詳細資訊，請參閱《EC2 執行個體命名》。若您沒有指定主要私有 IP 地址，我們會為您在子網範圍中選取可用的 IP 地址。如需有關網路介面的詳細資訊，請參閱《Amazon EC2 使用者指南》中的彈性網路介面。

您可以為在 VPC 中執行的執行個體指派額外的私有 IP 地址 (又稱為輔助私有 IP 地址)。與主要私有 IP 地址不同，您可以將網路介面中的輔助私有 IP 地址重新指派給另一個網路介面。私有 IP 地址在執行個體停止和重新啟動時仍會維持與網路介面的關聯，而會在執行個體終止時予以釋出。如需主要和次要 IP 位址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的多個 IP 位址。

我們會用私有 IP 地址稱呼位於 VPC IPv4 CIDR 範圍中的 IP 地址。大多數的 VPC IP 地址範圍都位於私有 (無法公開路由) IP 地址範圍內 (以 RFC 1918 形式指定)；但是，您可以針對您的 VPC 使用可公開路由的 CIDR 區塊。無論您 VPC 的 IP 地址範圍為何，我們不支援從您 VPC 的 CIDR 區塊直接存取網際網路 (包含可公開路由的 CIDR 區塊)。您必須透過閘道設定網際網路存取，例如網際網路閘道、虛擬私有閘道、 AWS Site-to-Site VPN 連線或 Direct Connect。

我們絕不會將子網路的 IPv4 地址範圍公告至網際網路。

公有 IPv4 地址

所有子網都具有可判斷在子網中建立的網路介面是否能自動接收公有 IPv4 地址 (本主題中又稱為公有 IP 地址) 的屬性。因此，當您在啟用此屬性的子網路中啟動執行個體時，便會為針對執行個體建立的主要網路介面指派公有 IP 位址。公有 IP 地址會透過網路地址轉譯 (NAT) 映射至主要私有 IP 地址。

> **Note**
>
> AWS 收取所有公有 IPv4 地址的費用，包括與執行中執行個體相關聯的公有 IPv4 地址和彈性 IP 地址。如需詳細資訊，請參閱 Amazon VPC 定價頁面中的公有 IPv4 地址。

您可以執行下列作業，來控制您的執行個體是否接收公有 IP 地址：

- 修改子網的公有 IP 定址屬性。如需更多詳細資訊，請參閱 修改子網路的公有 IP 位址屬性。
- 在執行個體啟動期間啟用或停用公有 IP 定址功能，其可覆寫子網的公有 IP 定址屬性。

- 您可以在啟動後透過管理與網路介面相關聯的 IP 位址，從執行個體取消指派公有 IP 位址。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的管理 IP 位址。

公有 IP 地址會從 Amazon 的公有 IP 地址集區指派，且並未建立與您帳戶的關聯。取消公有 IP 地址與您執行個體的關聯時，會將其釋出回集區，且您將無法重複使用它。在特定情況下，我們會從您的執行個體釋出公有 IP 位址，或將新的公有 IP 位址指派給執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的公有 IP 位址。

若您需要配置給您的帳戶，可在您需要時指派給執行個體或從執行個體移除的持久性公有 IP 地址，請改為使用彈性 IP 地址。如需更多詳細資訊，請參閱 將彈性 IP 地址與 VPC 中的資源建立關聯。

若您的 VPC 已啟用支援 DNS 主機名稱，每個接收到公有 IP 地址或彈性 IP 地址的執行個體也會取得一個公有 DNS 主機名稱。我們會在執行個體網路外將公有 DNS 主機名稱解析為執行個體的公有 IP 地址，並會在執行個體網路內解析為執行個體的私有 IP 地址。如需詳細資訊，請參閱VPC 的 DNS 屬性。

如果您使用 Amazon VPC IP Address Manager (IPAM)，您可以從 取得連續的公有 IPv4 地址區塊，AWS 並使用它將循序彈性 IP 地址配置給 AWS 資源。使用連續 IPv4 地址區塊可大幅降低安全存取控制清單的管理開銷，並簡化企業在 上擴展的 IP 位址配置和追蹤 AWS。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的從 IPAM 集區配置循序彈性 IP 位址。

IPv6 地址

隨著網際網路不斷增長，IP 地址的需求也持續增加。IP 地址最常見的格式為 IPv4。IP 地址的新格式是 IPv6，其提供比 IPv4 更大的地址空間。IPv6 解決 IPv4 地址耗盡問題，並可讓您將更多裝置連接到網際網路。轉換是漸進式的，但隨著 IPv6 採用率的增加，您可以簡化網路並利用 IPv6 進階功能來提高連線能力、效能和安全性。

許多 AWS 服務，例如 Amazon EC2、Amazon S3 和 Amazon CloudFront，提供雙堆疊 (IPv4 和 IPv6) 或IPv6-only的支援，允許指派 IPv6 地址和透過 IPv6 通訊協定存取資源。這可簡化採用 IPv6 的客戶的網路組態和管理。

其他服務提供有限或部分雙堆疊和僅 IPv6 的支援。

如需支援 IPv6 服務的詳細資訊，請參閱 AWS 支援 IPv6 的 服務。

請注意，某些 IPv6 地址是由網際網路工程任務小組保留。如需預留 IPv6 地址範圍的詳細資訊，請參閱 IANA IPv6 Special-Purpose Address Registry 和 RFC4291。

> **Note**
>
> 公有和私有 IPv6 地址都可以在 中使用 AWS。 會 AWS 定義公有 IP 地址，如同在網際網路上公告的地址 AWS，而私有 IP 地址則不是也無法在網際網路上公告 AWS。

目錄

- 公有 IPv6 地址
- 私有 IPv6 地址

公有 IPv6 地址

Amazon 提供的 IPv6 位址一律會向網際網路公告。這些位址具備全域唯一性，因此可透過網際網路存取。您可以藉由控制子網路的路由，或是使用安全群組與網路 ACL，來控制 EC2 執行個體等資源是否能透過其 IPv6 位址被存取。

以下是您可以準備為工作負載使用公有 IPv6 地址的一些方法：

- 使用 Amazon VPC IP Address Manager 建立 IPAM，並將 Amazon 擁有的公有 IPv6 地址範圍佈建至 IPAM 地址集區。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的建立 IPv6 池。
- 如果您有 IPAM 且擁有公有 IPv6 地址範圍，請將部分或全部公有 IPv6 地址範圍帶至 IPAM，並將公有 IPv6 地址範圍佈建至 IPAM 地址集區。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的教學課程：將 IP 位址代入 IPAM。
- 如果您沒有 IPAM，但擁有公有 IPv6 地址範圍，請將部分或全部公有 IPv6 地址範圍帶入其中 AWS。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將自有 IP 位址 (BYOIP) 用於 Amazon EC2。

準備好使用公有 IPv6 位址後，您可以將公有 IPv6 位址指派給執行個體 (請參閱《Amazon EC2 使用者指南》中的 IPv6 位址)，也可以為 VPC 配置公有 IPv6 CIDR 區塊 (請參閱從您的 VPC 中新增或移除 CIDR 區塊)，並將 IPv6 CIDR 區塊與子網路建立關聯 (請參閱修改子網路的公有 IP 位址屬性)。

私有 IPv6 地址

私有 IPv6 地址是未公告且無法在網際網路上公告的 IPv6 地址 AWS。

如果您希望私有網路支援 IPv6，而且您無意將流量從這些地址路由到網際網路，則可以使用私有 IPv6 地址。如果想要從使用私有 IPv6 地址的資源連線至網際網路，您雖然可以連線，但必須透過另一個子網路中的資源路由流量，並使用公有 IPv6 地址來完成。

私有 IPv6 地址有兩種類型：

- IPv6 ULA 範圍：RFC4193 中定義的 IPv6 地址。這些地址範圍一律以「fc」或「fd」開頭，這使得它們易於識別。有效的 IPv6 ULA 空間為 fd00::/8 下不與 Amazon 保留範圍 fd00::/16 重疊的任何空間。
- IPv6 GUA 範圍：RFC3587 中定義的 IPv6 地址。使用 IPv6 GUA 範圍做為私有 IPv6 地址的選項預設為停用，必須先啟用才能使用。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的啟用佈建私有 IPv6 GUA CIDR。

注意下列事項：

- 私有 IPv6 地址只能透過 Amazon VPC IP Address Manager (IPAM) 使用。IPAM 會發現使用 IPv6 ULA 和 GUA 地址的資源，並監控集區是否有重疊的 IPv6 ULA 和 GUA 地址空間。
- 當您使用私有 IPv6 GUA 範圍時，您需要使用自己擁有的 IPv6 GUA 範圍。
- 私有 IPv6 地址不是且無法在網際網路上公告 AWS。 AWS 不允許從私有 IPv6 範圍直接輸出至公有網際網路，即使 VPC 中有網際網路閘道或僅輸出網際網路閘道。私有 IPv6 地址會自動在網際網路閘道邊緣捨棄，確保不會公開路由。
- AWS 會保留前 4 個子網路私有 IPv6 地址和最後一個地址。
- 私有 IPv6 ULA 的有效範圍為 /9 到 /60，開頭為 fd80::/9。
- 如果您的私有 IPv6 GUA 範圍已配置給 VPC，則無法使用與相同 VPC 中的私有 IPv6 GUA 空間重疊的公有 IPv6 GUA 空間。
- 支援使用私有 IPv6 ULA 和 GUA 地址範圍的資源之間的通訊 (例如跨 Direct Connect、VPC 互連、轉換閘道或 VPN 連接)。
- 您可以使用私有 IPv6 地址搭配僅 IPv6 和雙堆疊 VPC 子網路、彈性負載平衡器和 AWS Global Accelerator 端點。
- 私有 IPv6 地址不產生任何費用。

以下是您可以準備為工作負載使用私有 IPv6 地址的一些方法：

- 使用 Amazon VPC IP Address Manager 建立 IPAM，並將私有 IPv6 ULA 範圍佈建至 IPAM 地址集區。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的建立 IPv6 池。

- 使用 Amazon VPC IP Address Manager 建立 IPAM，並將私有 IPv6 GUA 範圍佈建至 IPAM 地址集區。使用 IPv6 GUA 範圍做為私有 IPv6 地址的選項預設為停用，必須先在 IPAM 上啟用才能使用。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的啟用佈建私有 IPv6 GUA CIDR。

準備好使用私有 IPv6 位址後，您可以從 IPAM 集區為 VPC 配置私有 IPv6 CIDR 區塊 (請參閱從您的 VPC 中新增或移除 CIDR 區塊)，並將 IPv6 CIDR 區塊與子網路建立關聯 (請參閱修改子網路的公有 IP 位址屬性)。

使用您自己的 IP 地址

您可以將部分或全部的公有 IPv4 地址範圍或 IPv6 地址範圍帶入 AWS 您的帳戶。依預設您仍擁有自己的地址範圍，但 AWS 會在網際網路上公告。將地址範圍帶至 之後 AWS，其會在您的帳戶中顯示為地址集區。您可以從 IPv4 地址集區建立彈性 IP 地址，也可以將 IPv6 地址集區中的 IPv6 CIDR 區塊與 VPC 建立關聯。

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的自有 IP 位址 (BYOIP)。

使用 Amazon VPC IP 地址管理員

Amazon VPC IP Address Manager (IPAM) 是一種 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控 AWS 工作負載的 IP 地址。您可以使用 IPAM，按照特定商業規則將 IP 地址 CIDR 配置給 VPC。

如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的什麼是 IPAM？。

VPC CIDR 區塊

您的虛擬私有雲端 (VPC) 的 IP 地址使用無類別域間路由 (CIDR) 表示法來表示。VPC 必須具有關聯的 IPv4 CIDR 區塊。您可以選擇將額外的 IPv4 CIDR 區塊與一個或多個 IPv6 CIDR 區塊建立關聯。如需詳細資訊，請參閱您 VPC 和子網路的 IP 定址。

目錄

- IPv4 VPC CIDR 區塊
- 管理 VPC 的 IPv4 CIDR 區塊
- IPv4 CIDR 區塊關聯限制
- IPv6 VPC CIDR 區塊

IPv4 VPC CIDR 區塊

在您建立 VPC 時，您必須指定 VPC 的 IPv4 CIDR 區塊。允許的區塊大小介於 /16 網路遮罩 (65,536 個 IP 地址) 和 /28 網路遮罩 (16 個 IP 地址) 之間。在您建立 VPC 之後，您可以將其他 IPv4 CIDR 區塊與 VPC 建立關聯。如需詳細資訊，請參閱從您的 VPC 中新增或移除 CIDR 區塊。

當您建立 VPC 時，我們建議您指定來自 RFC 1918 中指定之私有 IPv4 地址範圍的 CIDR 區塊。

RFC 1918 範圍	CIDR 區塊範例
10.0.0.0 – 10.255.255.255 (10/8 字首)	10.0.0.0/16
172.16.0.0 – 172.31.255.255 (172.16/12 字首)	172.31.0.0/16
192.168.0.0 – 192.168.255.255 (192.168/16 字首)	192.168.0.0/20

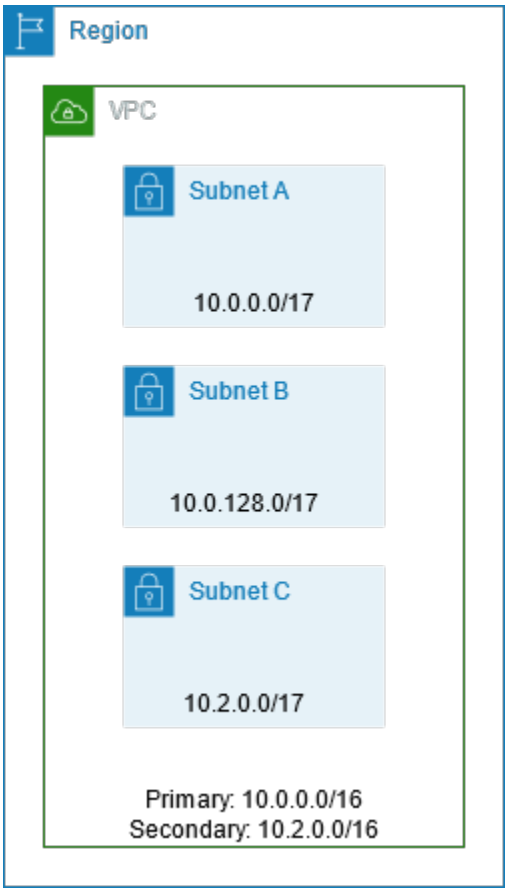
考量事項

- 您無法為 VPC 指定下列 CIDR 區塊：
  - 0.0.0.0/8
  - 127.0.0.0/8 (內部主機回送位址範圍)
  - 169.254.0.0/16 (連結本機位址範圍)
  - 224.0.0.0/4 (多播位址範圍)
- 當您建立 VPC 以搭配 AWS 服務使用時，請檢查服務文件，以確認其組態是否有特定需求。
- 有些 AWS 服務使用 `172.17.0.0/16` CIDR 範圍。如果該 IP 位址範圍已在網路中使用，服務可能會遇到 IP 位址衝突。例如， AWS Cloud9 Amazon SageMaker AI 使用 `172.17.0.0/16`。為避免發生衝突，請勿在建立 VPC 時使用此範圍。如需詳細資訊，請參閱《AWS Cloud9 使用者指南》中的無法連接到 EC2 環境，因為 VPC 的 IP 地址已由 Docker 使用。
- 您可以建立具有可公開路由 CIDR 區塊的 VPC，而此 CIDR 區塊不在 RFC 1918 所指定的私有 IPv4 地址範圍內。不過，基於本文件的用途，我們會將私有 IP 地址參照為您 VPC 之 CIDR 範圍內的 IPv4 地址。
- 如果您使用命令列工具或 Amazon EC2 API 建立 VPC，CIDR 區塊會自動修改為其正式形式。例如，如果您為 CIDR 區塊指定 100.68.0.18/18，我們會建立一個範圍為 100.68.0.0/18 CIDR 區塊。

管理 VPC 的 IPv4 CIDR 區塊

您可以將輔助 IPv4 CIDR 區塊與您的 VPC 建立關聯。當您將 CIDR 區塊與您的 VPC 建立關聯時，會自動將路由新增至您的 VPC 路由表，以啟用 VPC 內的路由 (目標為 CIDR 區塊，方向則是 `local`)。

在下列範例中，VPC 具有主要 CIDR 區塊及次要 CIDR 區塊。子網 A 和子網 B 的 CIDR 區塊來自主要 VPC CIDR 區塊。子網 C 的 CIDR 區塊來自次要 VPC CIDR 區塊。



下方的路由表顯示了 VPC 的本機路由。

目標	目標
10.0.0.0/16	區域
10.2.0.0/16	區域

若要將 CIDR 區塊新增到您的 VPC，將套用下列規則：

- 允許的區塊大小介於 /28 網路遮罩和 /16 網路遮罩之間。

- CIDR 區塊不可和任何現有與 VPC 相關聯的 CIDR 區塊重疊。
- 您可以使用的 IPv4 地址範圍有所限制。如需詳細資訊，請參閱 IPv4 CIDR 區塊關聯限制。
- 您無法增加或減少現有 CIDR 區塊的大小。
- 您可以與 VPC 建立關聯的 CIDR 區塊數，以及您可以新增到路由表的路由數皆具有配額。如果會導致您超過配額，便無法與 CIDR 區塊建立關聯。如需詳細資訊，請參閱 Amazon VPC 配額。
- CIDR 區塊不可和任何 VPC 路由表中路由的目的地 CIDR 範圍相同，或大於該範圍。例如，在主要 CIDR 區塊所在的 VPC 中 `10.2.0.0/16`，路由表中有一個現有的路由，其目的地 `10.0.0.0/24` 為虛擬私有閘道。您想要關聯 `10.0.0.0/16` 範圍中的次要 CIDR 區塊。由於現有的路由，您無法關聯 `10.0.0.0/24` 或更大的 CIDR 區塊。但是，您可以與 `10.0.0.0/25` 或更小的 CIDR 區塊建立關聯。
- 下列規則會在您將 IPv4 CIDR 區塊新增到做為 VPC 對等互連連線一部分的 VPC 時套用：
  - 若 VPC 對等互連連線為 `active`，只要它們不會和對等 VPC 的 CIDR 區塊重疊，您便可以將 CIDR 區塊新增到 VPC。
  - 若 VPC 對等互連連線為 `pending-acceptance`，則申請者 VPC 的擁有者便無法將任何 CIDR 區塊新增到 VPC，無論其是否與接受者 VPC 的 CIDR 區塊重疊。接受者 VPC 的擁有者必須接受對等互連連線，否則申請者 VPC 的擁有者必須刪除 VPC 對等互連連線請求、新增 CIDR 區塊，然後請求新的 VPC 對等互連連線。
  - 若 VPC 對等互連連線為 `pending-acceptance`，則接受者 VPC 的擁有者可將 CIDR 區塊新增到 VPC。若輔助 CIDR 區塊與申請者 VPC 的 CIDR 區塊重疊，則 VPC 對等互連連線會失敗，無法獲得接受。
- 如果您使用 透過 Direct Connect 閘道 Direct Connect 連線至多個 VPCs，則與 Direct Connect 閘道相關聯的 VPCs 不得有重疊的 CIDR 區塊。若您將 CIDR 區塊新增到其中一個與 Direct Connect 閘道建立關聯的 VPC，請確認新的 CIDR 區塊不會和任何其他相關聯 VPC 的現有 CIDR 區塊重疊。如需詳細資訊，請參閱《Direct Connect 使用者指南》中的 Direct Connect 閘道。
- 當您新增或移除 CIDR 區塊時，它可能會經過多種狀態：`associating` |`associated` |`disassociating` |`disassociated` |`failing` |`failed` 。當其處於 `associated` 狀態時，表示 CIDR 區塊已準備好可供您使用。

您可以取消關聯您已和 VPC 建立關聯的 CIDR 區塊；但是，您無法取消關聯您一開始用來建立 VPC (主要 CIDR 區塊) 的 CIDR 區塊。若要在 Amazon VPC 主控台中檢視 VPC 的主要 CIDR，請選擇 Your VPCs (您的 VPC)，接著選取 VPC 的核取方塊，然後選擇 CIDRs 標籤頁。若要使用 檢視主要 CIDR AWS CLI，請使用 describe-vpcs 命令，如下所示。主要 CIDR 會在頂層 `CidrBlock` `element` 中傳回。

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

以下為範例輸出。

```
10.0.0.0/16
```

IPv4 CIDR 區塊關聯限制

下表概述了現有 VPC CIDR 區塊允許與限制的關聯規則。限制的原因在於某些 AWS 服務會使用跨 VPC 和跨帳戶功能，這些功能需要在 AWS 服務端上無衝突的 CIDR 區塊。

現有的 IPv4 位址範圍	受限制的關聯	許可的關聯
10.0.0.0/8	來自其他 RFC 1918* 範圍 (172.16.0.0/12 及 192.168.0.0/16) 的 CIDR 區塊。 如果與 VPC 關聯的任何 CIDR 區塊位於 10.0.0.0/15 範圍 (10.0.0.0 至 10.1.255.255) 內，您便無法新增來自 10.0.0.0/16 範圍 (10.0.0.0 至 10.0.255.255) 的 CIDR 區塊。 來自 198.19.0.0/16 範圍的 CIDR 區塊。	介於 /16 網路遮罩和 /28 網路遮罩之間 10.0.0.0/8 範圍的任何其他 CIDR 區塊，不受限制。 /16 網路遮罩和 /28 網路遮罩之間的任何可公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或 /16 網路遮罩和 /28 網路遮罩之間 100.64.0.0/10 範圍的 CIDR 區塊。
169.254.0.0/16	如 RFC 5735 中所述，會保留來自「本機連結」區塊的 CIDR 區塊，且無法指派給 VPC。	
172.16.0.0/12	來自其他 RFC 1918* 範圍 (10.0.0.0/8 及 192.168.0.0/16) 的 CIDR 區塊。 來自 172.31.0.0/16 範圍的 CIDR 區塊。	介於 /16 網路遮罩和 /28 網路遮罩之間 172.16.0.0/12 範圍的任何其他 CIDR 區塊，不受限制。 /16 網路遮罩和 /28 網路遮罩之間的任何可公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或 /16 網路遮罩和 /28

現有的 IPv4 位址範圍	受限制的關聯	許可的關聯
	來自 198.19.0.0/16 範圍的 CIDR 區塊。	網路遮罩之間 100.64.0.0/10 範圍的 CIDR 區塊。
192.168.0.0/16	來自其他 RFC 1918* 範圍 (10.0.0.0/8 及 172.16.0.0/12) 的 CIDR 區塊。 來自 198.19.0.0/16 範圍的 CIDR 區塊。	/16 網路遮罩和 /28 網路遮罩之間 192.168.0.0/16 範圍的任何其他 CIDR 區塊。 /16 網路遮罩和 /28 網路遮罩之間的任何可公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或 /16 網路遮罩和 /28 網路遮罩之間 100.64.0.0/10 範圍的 CIDR 區塊。
198.19.0.0/16	來自 RFC 1918* 範圍的 CIDR 區塊。	/16 網路遮罩和 /28 網路遮罩之間的任何可公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或 /16 網路遮罩和 /28 網路遮罩之間 100.64.0.0/10 範圍的 CIDR 區塊。
可公開路由的 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊	來自 RFC 1918* 範圍的 CIDR 區塊。 來自 198.19.0.0/16 範圍的 CIDR 區塊。	/16 網路遮罩和 /28 網路遮罩之間的任何其他可公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或 /16 網路遮罩和 /28 網路遮罩之間 100.64.0.0/10 範圍的 CIDR 區塊。 您也可以關聯 RFC 1918 範圍內的一個 CIDR，但若要執行此操作，您必須在建立 VPC 時先新增該 CIDR，再新增非 RFC 1918 範圍內的 CIDR。

* RFC 1918 範圍是 RFC 1918 中指定的私有 IPv4 地址範圍。

IPv6 VPC CIDR 區塊

您可以在建立新 VPC 時關聯單一 IPv6 CIDR 區塊，或者從 /44 至 /60 (增量為 /4) 關聯最多五個 IPv6 CIDR 區塊。您可以從 Amazon 的 IPv6 地址集區中申請 IPv6 CIDR 區塊。如需詳細資訊，請參閱從您的 VPC 中新增或移除 CIDR 區塊。

若您已將 IPv6 CIDR 區塊與您的 VPC 建立關聯，您可以將 IPv6 CIDR 區塊與您 VPC 中的現有子網，或是在您建立新的子網時建立關聯。如需詳細資訊，請參閱the section called “IPv6 的子網規模”。

例如，您建立 VPC，並指定您希望將 Amazon 提供的 IPv6 CIDR 區塊與 VPC 建立關聯。Amazon 會指派下列 IPv6 CIDR 區塊給您的 VPC：2001:db8:1234:1a00::/56。您不能自行選擇 IP 地址的範圍。您可以建立子網，並關聯來自此範圍的 IPv6 CIDR 區塊；例如：2001:db8:1234:1a00::/64。

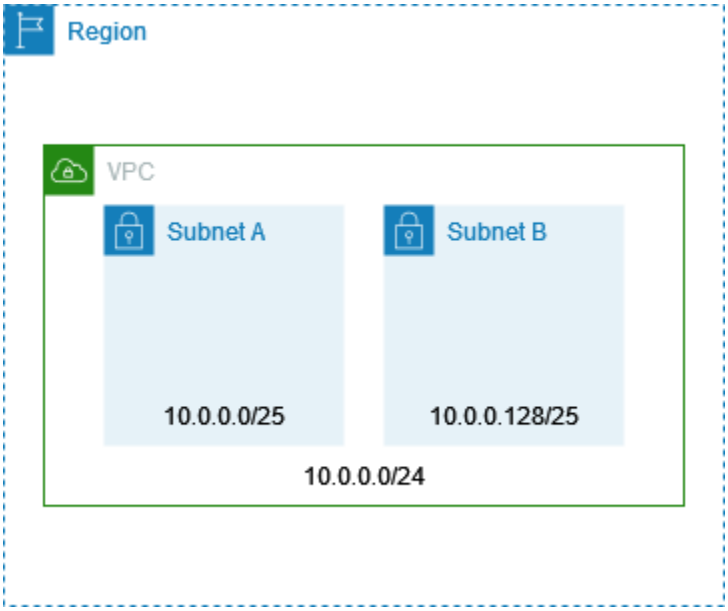
您可以取消 IPv6 CIDR 區塊與 VPC 的關聯 在您將 IPv6 CIDR 區塊與 VPC 取消關聯後，若您在稍後重新將 IPv6 CIDR 區塊與 VPC 建立關聯，您無法預期取得相同的 CIDR。

子網路 CIDR 區塊

您的子網路的 IP 地址使用無類別域間路由 (CIDR) 表示法來表示。子網路的 CIDR 區塊可以與 VPC 的 CIDR 區塊相同 (在 VPC 中建立單一子網路)，或是與 VPC 的 CIDR 區塊子集相同 (在 VPC 中建立多個子網路)。

若您在 VPC 中建立超過一個子網，子網的 CIDR 區塊不可重疊。

例如，若您使用 CIDR 區塊 10.0.0.0/24 建立 VPC，它便支援 256 個 IP 地址。您可以將此 CIDR 區塊拆成兩個子網，每個子網都支援 128 個 IP 地址。其中一個子網使用 CIDR 區塊 10.0.0.0/25 (針對 10.0.0.0 到 10.0.0.127 的地址)，另一個則使用 CIDR 區塊 10.0.0.128/25 (針對 10.0.0.128 到 10.0.0.255 的地址)。



網際網路中提供可協助計算和建立 IPv4 和 IPv6 子網路 CIDR 區塊的工具。您可以搜尋符合需求的工具，例如「子網計算器」或「CIDR 計算器」。網路工程群組亦可協助判斷要為子網路指定的 IPv4 和 IPv6 CIDR 區塊。

IPv4 的子網路規模調整

子網路的允許 IPv4 CIDR 區塊大小介於 /28 網路遮罩和 /16 網路遮罩之間。您無法使用每個子網 CIDR 區塊中的前四個 IP 地址和最後一個 IP 地址，並且無法將這些 IP 地址指派給資源，如 EC2 執行個體。例如，在使用 CIDR 區塊 10.0.0.0/24 的子網中，會預留下列五個 IP 地址：

- 10.0.0.0：網路地址。
- 10.0.0.1：由 AWS 為 VPC 路由器預留。
- 10.0.0.2：預留者 AWS。DNS 伺服器的 IP 地址是 VPC 網路範圍的基礎加 2。針對使用多個 CIDR 區塊的 VPC，DNS 伺服器的 IP 地址會位於主要 CIDR。我們也會為 VPC 中的所有 CIDR 區塊保留每個子網範圍的基礎加 2。如需詳細資訊，請參閱Amazon DNS 伺服器。
- 10.0.0.3：由 保留 AWS 以供日後使用。
- 10.0.0.255：網路廣播地址。我們不支援在 VPC 中廣播，因此我們會預留此地址。

如果您使用命令列工具或 Amazon EC2 API 建立子網，CIDR 區塊會自動修改為其正式形式。例如，如果您為 CIDR 區塊指定 100.68.0.18/18，我們會建立一個範圍為 100.68.0.0/18 CIDR 區塊。

如果您 AWS 使用 BYOIP 將 IPv4 地址範圍帶入 ，則可以使用範圍內的所有 IP 地址，包括第一個地址（網路地址）和最後一個地址 （廣播地址）。

IPv6 的子網規模

若您已將 IPv6 CIDR 區塊與您的 VPC 建立關聯，您可以將 IPv6 CIDR 區塊與您 VPC 中的現有子網，或是在您建立新的子網時建立關聯。可能的 IPv6 網路遮罩長度介於 /44 和 /64 之間，增量為 /4。

網際網路中具有可用的工具，可以協助您計算和建立 IPv6 子網路 CIDR 區塊。您可以透過搜尋「IPv6 子網路計算器」或「IPv6 CIDR 計算器」等用語，尋找符合需要的工具。此外，您的網路工程群組可協助您判斷要為您的子網指定的 IPv6 CIDR 區塊。

您無法使用每個子網 CIDR 區塊中的前四個 IPv6 地址和最後一個 IPv6 地址，也無法指派給 EC2 執行個體。例如，在使用 CIDR 區塊 2001:db8:1234:1a00/64 的子網中，會預留下列五個 IP 地址：

- 2001:db8:1234:1a00::
- 2001:db8:1234:1a00::1：由 AWS 為 VPC 路由器預留。
- 2001:db8:1234:1a00::2
- 2001:db8:1234:1a00::3
- 2001:db8:1234:1a00:ffff:ffff:ffff:ffff

除了上述範例中 AWS 為 VPC 路由器預留的 IP 地址之外，下列 IPv6 地址也會保留給預設 VPC 路由器：

- 使用 EUI-64 產生的 FE80::/10 範圍內的連結本機 IPv6 地址。如需有關連結本機地址的詳細資訊，請參閱連結本機地址。
- 連結本機 IPv6 地址FE80:ec2::1。

如果您需要透過 IPv6 與 VPC 路由器通訊，您可以將應用程式設定為與最符合您需求的地址進行通訊。

比較 IPv4 和 IPv6

下表摘要 Amazon EC2 和 Amazon VPC 中 IPv4 和 IPv6 的差異。

如需支援雙堆疊組態 (IPv4 和 IPv6) 和僅限 IPv6 組態的 AWS 伺服器清單，請參閱 支援 IPv6 的服務。

特性	IPv4	IPv6
VPC 大小	從 /16 至 /28 最多 5 個 CIDR。此配額是可調整的。	從 /44 至 /60 (增量為 /4) 最多 5 個 CIDR。此配額是可調整的。
子網大小	從 /16 到 /28。	從 /44 至 /64 (增量為 /4)。
地址選擇	您可以為您的 VPC 選擇 IPv4 CIDR 區塊，也可從 Amazon VPC IP 地址管理員 (IPAM) 分配 CIDR 區塊。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的什麼是 IPAM？。	您可以在 AWS 針對 VPC 使用自有 IPv6 CIDR 區塊、選擇 Amazon 提供的 IPv6 CIDR 區塊，或者從 Amazon VPC IP 地址管理員 (IPAM) 分配 CIDR 區塊。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的什麼是 IPAM？。
網際網路存取	需要網際網路閘道。	需要網際網路閘道。支援使用輸出限定網際網路閘道進行僅限傳出的通訊。
彈性 IP 位址	支援。為 EC2 執行個體提供永久、靜態的公有 IPv4 地址。	不支援。EIP 會在執行個體重新啟動時，使執行個體的公用 IPv4 地址維持靜態。IPv6 地址預設為靜態。
NAT 閘道	支援。私有子網路中的執行個體可以使用公有 NAT 閘道連線至網際網路，或使用私有 NAT 閘道連線至其他 VPC 中的資源。	支援。您可以搭配 NAT64 使用 NAT 閘道，來啟用僅限 IPv6 子網路中的執行個體，以在 VPC 內、VPC 間、內部部署網路中或透過網際網路，與僅限 IPv4 資源通訊。
DNS 名稱	執行個體會收到 Amazon 提供的 IPBN 或 RBN 型 DNS 名稱。DNS 名稱會解析為執行個體選取的 DNS 記錄。	執行個體會收到 Amazon 提供的 IPBN 或 RBN 型 DNS 名稱。DNS 名稱會解析為執行個體選取的 DNS 記錄。

使用受管字首清單來整合和管理網路 CIDR 區塊

受管前綴清單是一或多個 CIDR 區塊的集合。您可以使用字首清單，以便更輕鬆地設定和維護安全群組和路由表。您可以從經常使用的 IP 地址建立字首清單，並在安全群組規則和路由中以集合形式參考，而非個別參考。例如，您可以將具有不同 CIDR 區塊但連接埠和通訊協定相同的安全群組規則合併成使用字首清單的單一規則。如果您擴展網路且需要允許來自另一個 CIDR 區塊的流量，則可以更新相關的字首清單，以更新使用字首清單的所有安全群組。您也可以搭配其他使用 Resource Access Manager (RAM) AWS 的帳戶使用受管字首清單。

字首清單有兩個類型：

- 由客戶管理之前綴清單 — 您定義並管理的 IP 地址範圍集合。您可以與其他 AWS 帳戶共用您的字首清單，讓這些帳戶在其自己的資源中參考字首清單。
- AWS受管字首清單 — AWS 服務的 IP 地址範圍集。您無法建立、修改、共用或刪除 AWS管理的字首清單。

內容

- 字首清單的概念和規則
- 字首清單的 Identity and Access Management
- 由客戶管理之前綴清單
- AWS管理的字首清單
- 使用字首清單最佳化 AWS 基礎設施管理

字首清單的概念和規則

字首清單由項目組成。每個項目都包含一個 CIDR 區塊，以及 CIDR 區塊的選擇性描述。

由客戶管理之前綴清單

下列規則適用於由客戶管理之前綴清單：

- 字首清單僅支援單一類型的 IP 地址 (IPv4 或 IPv6)。您無法在單一字首清單中合併 IPv4 和 IPv6 CIDR 區塊。
- 字首清單僅適用於您建立該清單的「區域」。
- 當您建立字首清單時，必須指定字首清單可支援的最大項目數。

- 當您在資源中參考字首清單時，字首清單的項目數上限會計入資源項目數的配額。例如，如果您建立最多包含 20 個項目的字首清單，而您在安全群組規則中參考該字首清單，這就會計為該安全群組的 20 個規則。
- 當您在路由表中參考字首清單時，會套用路由優先順序規則。如需詳細資訊，請參閱字首清單的路由優先順序。
- 您可以修改字首清單。當您新增或移除項目時，我們都會建立新的字首清單版本。參考字首的資源永遠使用目前 (最新) 版本。您可以從舊版字首清單還原項目，其也會建立新版本。
- 字首清單有相關的配額。如需詳細資訊，請參閱由客戶管理之前綴清單。
- 所有商業 AWS 區域 (包括 GovCloud (美國) 及中國區域) 都提供客戶管理的字首列表。

AWS管理的字首清單

下列規則適用於 AWS受管字首清單：

- 您無法建立、修改、共用或刪除受 AWS管字首清單。
- 不同的 AWS受管字首清單在您使用時具有不同的權重。如需詳細資訊，請參閱AWS管理的字首清單權重。
- 您無法檢視 AWS受管字首清單的版本編號。

字首清單的 Identity and Access Management

根據預設， 使用者沒有建立、檢視、修改或刪除字首清單的許可。您可以建立允許使用者使用前綴清單的 IAM 政策，並將其連接至一個角色。

若要檢視 Amazon VPC 動作清單以及可在 IAM 政策中使用的資源與條件索引鍵，請參閱《服務授權參考》中的 Amazon EC2 的動作、資源和條件索引鍵。

下列範例政策只允許使用者檢視和使用字首清單 pl-123456abcde123456。使用者無法建立或刪除字首清單。

JSON

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

```
            "Action": [
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "ec2:RestoreManagedPrefixListVersion"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:prefix-
list/pl-123456abcde123456"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeManagedPrefixLists",
            "Resource": "*"
        }
    ]
}
```

如需在 Amazon VPC 中使用 IAM 的詳細資訊，請參閱 Amazon VPC 的身分和存取管理。

由客戶管理之前綴清單

客戶受管字首清單可讓您在 AWS中定義和維護自己的一組 IP 位址範圍，稱為字首。您可以建立集中式字首清單，並視需要參考，而不是將這些 IP 位址硬式編碼到各種資源中。這不僅簡化了 IP 地址的管理，還提升了整個 AWS 環境的一致性和可重複使用性。

客戶受管字首清單的突出功能之一是能夠與其他 AWS 帳戶共用。透過授予對字首清單的存取權，您可以讓其他團隊或組織在自己的資源中使用定義的 IP 地址範圍。這種協作方法可促進更具凝聚力和效率的雲端體驗，可在其中共用和同步 IP 位址管理。

在下列各節中，我們將深入探討使用客戶受管字首清單的實際層面，包括建立、管理和共用 IP 位址範圍的逐步指引。

> **Note**
>
> 您可以使用 Amazon VPC IPAM 實現字首清單管理自動化，根據自己定義的規則自動同步 CIDR。此功能可消除基礎架構發生變更時的手動更新需求。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的透過 IPAM 自動進行字首列表更新。

任務

- 使用由客戶管理之前綴清單

使用由客戶管理之前綴清單

本節說明如何使用客戶受管字首清單。

目錄

- 建立字首清單
- 檢視字首清單
- 檢視字首清單的項目
- 檢視字首清單的關聯 (參考)
- 修改字首清單
- 調整字首清單大小
- 還原舊版的字首清單
- 刪除字首清單
- 共用客戶受管字首清單

建立字首清單

當您建立字首清單時，必須指定字首清單可支援的最大項目數。

限制

如果規則數目加上字首清單項目上限超過帳戶每一安全群組的規則配額，則無法將字首清單新增至安全群組規則。

使用主控台建立字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選擇 Create prefix list (建立字首清單)。
4. 在 Prefix list name (字首清單名稱) 中，輸入字首清單的名稱。
5. 對於 Max entries (最大項目數)，請輸入字首清單的最大項目數。
6. 在 Address family (地址系列) 中，選擇字首清單支援 IPv4 或 IPv6 項目。

7. 在 Prefix list entries (字首清單項目) 中，選擇 Add new entry (新增項目)，然後輸入項目的 CIDR 區塊和描述。針對每個項目重複此步驟。
8. (選用) 對於 Tags (標籤)，對字首清單新增標籤，可於稍後協助識別。
9. 選擇 Create prefix list (建立字首清單)。

使用 建立字首清單 AWS CLI

使用 create-managed-prefix-list 命令。

檢視字首清單

您可以檢視字首清單、與您共用的字首清單，以及 AWS管理的字首清單。

使用主控台檢視字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 擁有者 ID 欄會顯示字首清單擁有者 AWS 的帳戶 ID。對於 AWS受管字首清單，擁有者 ID 為 AWS。

使用 檢視字首清單 AWS CLI

使用 describe-managed-prefix-lists 命令。

檢視字首清單的項目

您可以檢視字首清單的項目、與您共用的字首清單，以及 AWS受管字首清單。

使用主控台檢視字首清單的項目

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單的核取方塊。
4. 在下方窗格中，選擇 Entries (項目) 以檢視字首清單的項目。

使用 檢視字首清單的項目 AWS CLI

使用 get-managed-prefix-list-entries 命令。

檢視字首清單的關聯 (參考)

您可以檢視與字首清單相關聯之資源的 ID 和擁有者。關聯的資源是在其項目或規則中參考您的字首清單的資源。

限制

您無法檢視 AWS受管字首清單的相關資源。

使用主控台檢視字首清單關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單的核取方塊。
4. 在下方窗格中，選擇 Associations (關聯) 以檢視參考字首清單的資源。

使用 檢視字首清單關聯 AWS CLI

使用 get-managed-prefix-list-associations 命令。

修改字首清單

您可以修改字首清單的名稱，也可以新增或移除項目。如要修改最大項目數，請參閱調整字首清單大小。

更新字首清單的項目會建立新的字首清單版本。更新字首清單項目的名稱或數目上限並不會建立新的字首清單版本。

考量事項

- 您無法修改受 AWS管字首清單。
- 當您增加字首清單中的項目數目上限時，增加的大小上限會套用至參考字首清單之資源的項目配額。如果上述任何資源不支援增加的大小上限，則修改操作會失敗，並會還原先前的大小上限。

使用主控台修改字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單的核取方塊，然後選擇 Actions (動作)、Modify prefix list (修改字首清單)。

4. 在 Prefix list name (字首清單名稱) 中，輸入字首清單的新名稱。
5. 如果受管字首清單已設定為 IPAM 字首清單解析程式目標，即可看到 IPAM 字首清單解析程式同步選項。

   選擇啟用或停用 IPAM 字首清單解析程式同步功能。啟用後，字首清單 CIDR 會根據相關聯的解析程式 CIDR 選取規則自動更新。停用後，字首清單 CIDR 不會自動更新。如需此功能的詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的透過 IPAM 自動進行字首列表更新。
6. 在 Prefix list entries (字首清單項目) 中，選擇 Remove (移除) 以移除現有的項目。若要新增項目，請選擇 Add new entry (新增項目)，然後輸入項目的 CIDR 區塊和描述。
7. 選擇 Save prefix list (儲存字首清單)。

使用 修改字首清單 AWS CLI

使用 modify-managed-prefix-list 命令。

調整字首清單大小

您可以調整字首清單大小，並將字首清單的最大項目數修改至最多 1000。如需客戶受管字首清單配額的詳細資訊，請參閱 由客戶管理之前綴清單。

使用主控台調整字首清單大小

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單的核取方塊，然後選擇 Actions (動作)、Resize prefix list (調整字首清單大小)。
4. 若為 New max entries (新的最大項目數)，請輸入值。
5. 選擇 Resize (調整大小)。

使用 調整字首清單的大小 AWS CLI

使用 modify-managed-prefix-list 命令。

還原舊版的字首清單

您可以從舊版字首清單還原項目。這會建立新的字首清單版本。

如果您減少字首清單的大小，則必須確保字首清單的大小足以包含舊版的項目。

使用主控台還原舊版的字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單的核取方塊，然後選擇 Actions (動作)、Restore prefix list (還原字首清單)。
4. 對於 Select prefix list version (選取字首清單版本)，選取舊版。所選版本的項目會顯示在 Prefix list entries (字首清單項目) 中。
5. 選擇 Restore prefix list (還原字首清單)。

使用 還原先前版本的字首清單 AWS CLI

使用 restore-managed-prefix-list-version 命令。

刪除字首清單

若要刪除字首清單，您必須先移除資源中 (例如在路由表中) 對其進行的任何參考。如果您已使用 AWS RAM共用字首清單，則必須先移除消費者擁有資源中的任何參考項目。

限制

您無法刪除受 AWS管字首清單。

使用主控台刪除字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單，然後選擇 Actions (動作)、Delete prefix list (刪除字首清單)。
4. 在確認對話方塊中輸入 `delete`，然後選擇 Delete (刪除)。

使用 刪除字首清單 AWS CLI

使用 delete-managed-prefix-list 命令。

共用客戶受管字首清單

使用 AWS Resource Access Manager (AWS RAM)，客戶受管字首清單的擁有者可以與下列項目共用字首清單：

- 中組織內部或外部的特定 AWS 帳戶 AWS Organizations

- 中的組織單位 AWS Organizations
- 中的整個組織 AWS Organizations

已與其共用字首清單的消費者可以檢視字首清單及其項目，並且可以在其 AWS 資源中參考字首清單。

如需 的詳細資訊 AWS RAM，請參閱AWS RAM 《 使用者指南》 。如需詳細資訊配額，請參閱 AWS RAM 《 使用者指南》中的服務配額。

> **Important**
>
> 共用字首清單無須額外收費。

目錄

- 共用字首清單許可
- 使用共用字首清單

共用字首清單許可

擁有者的許可

擁有者負責管理共用字首清單及其項目。擁有者可以檢視參考字首清單 AWS 的資源 IDs。不過，他們無法新增或移除消費者所擁有 AWS 資源中字首清單的參考。

如果在消費者擁有的資源中參考了字首清單，則擁有者無法刪除該字首清單。

消費者的許可

消費者可以檢視共用字首清單中的項目，也可以在其 AWS 資源中參考共用字首清單。不過，消費者無法修改、還原或刪除共用的字首清單。

使用共用字首清單

AWS 字首清單提供方便的方式來管理和參考各種 AWS 服務所使用的 IP 地址範圍。除了 AWS受管字首清單之外，您也可以建立自己的客戶受管字首清單，並與其他 AWS 帳戶共用。

對於具有複雜聯網需求或需要跨多個 AWS 工作負載協調 IP 地址使用量的組織而言，共用字首清單特別有用。透過共用字首清單，您可以確保一致的 IP 位址管理，並簡化協作者的聯網組態。

本節說明如何共用字首清單，以及如何識別和使用已與您帳戶共用的字首清單。

目錄

- 共用字首清單
- 取消共享已共用的字首清單
- 識別共用的字首清單
- 識別共用字首清單的參考

共用字首清單

若要共用字首清單，您必須將它新增至資源共享。如果您沒有資源共享，則必須先使用 AWS RAM 主控台建立共用。

如果您是 組織的一部分 AWS Organizations，且已啟用組織內的共用，則組織中的取用者會自動獲得共用字首清單的存取權。否則，消費者會收到加入資源共享的邀請，並且在接受邀請後便能存取共用的字首清單。

您可以使用 AWS RAM 主控台或 AWS CLI建立資源共享，以及共用您擁有的字首清單。

> **Important**
>
> - 若要共用字首清單，您必須擁有字首清單。您無法將已分享給您的字首清單再分享出去。您無法共用受 AWS管字首清單。
> - 若要與組織或 AWS Organizations內的組織單位共用字首清單，您必須透過 AWS Organizations啟用共用。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的透過 AWS Organizations啟用共用。

使用 AWS RAM 主控台建立資源共用和共用字首清單

依照《AWS RAM 使用者指南》中建立資源共享的步驟進行。在 Select resource type (選取資源類型) 中，選擇 Prefix Lists (字首清單)，然後選取字首清單的核取方塊。

使用 AWS RAM 主控台將字首清單新增至現有資源共享

若要將您擁有的受管理字首新增至現有的資源共享，請依照《AWS RAM 使用者指南》中的更新資源共享步驟進行。在 Select resource type (選取資源類型) 中，選擇 Prefix Lists (字首清單)，然後選取字首清單的核取方塊。

使用 共享您擁有的字首清單 AWS CLI

使用下列命令來建立和更新資源共享：

- create-resource-share
- associate-resource-share
- update-resource-share

取消共享已共用的字首清單

取消共用字首清單時，消費者將無法在其帳戶中檢視字首清單或其項目，也無法在其資源中參考字首清單。如果消費者資源中已經參考字首清單，那些參考項目會繼續正常運作，而且您可以繼續檢視這些參考項目。如果您將字首清單更新為新版本，則參考會使用最新版本。

若要取消共用您擁有的共用字首清單，您必須使用 將其從資源共用中移除 AWS RAM。

使用 AWS RAM 主控台取消共用您擁有的共用字首清單

請參閱《AWS RAM 使用者指南》中的更新資源共享。

使用 取消共用您擁有的共用字首清單 AWS CLI

使用 disassociate-resource-share 命令。

識別共用的字首清單

擁有者和消費者可以使用 Amazon VPC 主控台和 AWS CLI來識別共用的字首清單。

使用 Amazon VPC 主控台識別共享的前綴清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 此頁面會顯示您擁有的字首清單，以及與您共用的字首清單。Owner ID (擁有者 ID) 欄會顯示字首清單擁有者的 AWS 帳戶 ID。
4. 若要檢視字首清單的資源共享資訊，請選取字首清單，然後選擇下方窗格中的 Sharing (共用)。

使用 識別共用字首清單 AWS CLI

使用 describe-managed-prefix-lists 命令。命令會傳回您擁有的字首清單和與您共用的字首清單。`OwnerId`會顯示字首清單擁有者 AWS 的帳戶 ID。

識別共用字首清單的參考

擁有者可以識別參考共用字首清單的消費者擁有資源。

使用 Amazon VPC 主控台識別共享前綴清單的參考

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。
3. 選取字首清單，然後在下方窗格中選擇 Associations (關聯)。
4. 參考字首清單的資源 ID 會列在 Resource ID (資源 ID) 欄中。資源的擁有者會列在 Resource Owner (資源擁有者) 欄中。

使用 識別共用字首清單的參考 AWS CLI

使用 get-managed-prefix-list-associations 命令。

AWS管理的字首清單

AWS受管字首清單是 AWS 服務的一組 IP 地址範圍。這些字首清單由 Amazon Web Services 維護，並提供參考各種 AWS 方案所用 IP 地址的方法。這在設定 VPC 內的安全群組或其他網路層級控制項時特別有用。

字首清單涵蓋各種 AWS 服務，包括 S3 和 DynamoDB 等。透過使用 受管字首清單，您可以確保您的網路組態是up-to-date，並正確考慮您所依賴 AWS 的服務所使用的 IP 地址。這有助於簡化聯網任務，並減少手動維護 IP 位址清單的管理開銷。

除了實際優點之外，使用受管字首清單也符合 AWS 安全最佳實務。透過依賴 提供的授權 IP 地址資訊 AWS，您可以將設定錯誤或非預期連線問題的風險降至最低。對於具有嚴格合規要求的任務關鍵應用程式或工作負載而言，這尤其重要。

目錄

- 可用的 AWS受管字首清單
- AWS管理的字首清單權重
- 使用 AWS受管字首清單

可用的 AWS受管字首清單

下列 服務提供 AWS受管字首清單。

AWS 服務	字首清單名稱	Weight (粗細)
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing (IPv4) com.amazonaws.global.ipv6.cloudfront.origin-facing (IPv6)	55
Amazon DynamoDB	com.amazonaws.*region*.dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws.*region*.ec2-instance-connect	2
	com.amazonaws.*region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.*region*.ipv6.route53-healthchecks	25
	com.amazonaws.*region*.route53-healthchecks	25
Amazon S3	com.amazonaws.*region*.s3	1
Amazon S3 Express One Zone	com.amazonaws.*region*.s3express	6
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager-managed-external-secrets	20
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice	10
	com.amazonaws.*region*.ipv6.vpc-lattice	10

使用主控台檢視 AWS受管字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Managed Prefix Lists (受管理的字首清單)。

3. 在搜尋欄位中，新增擁有者 ID： AWS 篩選條件。

使用 檢視 AWS受管字首清單 AWS CLI

如下所示使用 describe-managed-prefix-lists 命令。

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

AWS管理的字首清單權重

受 AWS管字首清單的權重是指它在資源中佔用的項目數。

例如，Amazon CloudFront 管理之前綴清單的權重為 55。以下說明這對您的 Amazon VPC 配額有何影響：

- 安全群組 – 預設配額為 60 條規則，因此在安全群組中只留下 5 條額外規則的空間。對於此配額，您可請求提高配額。
- 路由表 – 預設配額為 50 條路由，因此您必須請求提高配額，然後才能將前綴清單新增至路由表。

使用 AWS受管字首清單

AWS受管字首清單由 建立和維護， AWS 並且可供擁有 AWS 帳戶的任何人使用。您無法建立、修改、共用或刪除受 AWS管字首清單。

如同客戶受管字首清單，您可以使用 AWS受管字首清單搭配安全群組和路由表等 AWS 資源。如需詳細資訊，請參閱使用字首清單最佳化 AWS 基礎設施管理。

使用字首清單最佳化 AWS 基礎設施管理

您可以在下列 AWS 資源中參考字首清單。

Resources

- VPC security groups (VPC 安全群組)
- 子網路由表
- Transit Gateway 路由表
- AWS Network Firewall 規則群組
- Amazon Managed Grafana 網路存取控制

- AWS Outposts 機架本機閘道

VPC security groups (VPC 安全群組)

您可以指定字首清單作為傳入規則的來源，或作為傳出規則的目的地。如需詳細資訊，請參閱Security groups (安全群組)。

> **Important**
>
> 您無法修改現有的規則以使用字首清單。您必須建立新的規則才能使用字首清單。

使用主控台在安全群組規則中參考字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選取要更新的安全群組。
4. 選擇 Actions (動作)、Edit inbound rules (編輯傳入規則) 或 Actions (動作)、Edit outbound rules (編輯傳出規則)。
5. 選擇 Add rule (新增規則)。對於 Type (類型)，選取流量類型。對於來源 (輸入規則) 或目的地 (輸出規則)，選擇自訂。然後，在下一個欄位的字首清單下，選擇字首清單的 ID。
6. 選擇儲存規則。

使用 在安全群組規則中參考字首清單 AWS CLI

使用 authorize-security-group-ingress 和 authorize-security-group-egress 命令。對於 `--ip-permissions` 參數，請使用 `PrefixListIds` 指定字首清單的 ID。

子網路由表

您可以指定字首清單作為路由表項目的目的地。您無法在閘道路由表中參考字首清單。如需路由表的詳細資訊，請參閱設定路由表。

使用主控台在路由表中參考字首清單

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。

3. 選擇 Actions (動作)、Edit routes (編輯路由)。
4. 若要新增路由，請選擇 Add route (新增路由)。
5. 對於 Destination (目的地)，請輸入字首清單的 ID。
6. 針對 Target (目標)，選擇一個目標。
7. 選擇儲存變更。

使用 參考路由表中的字首清單 AWS CLI

使用 create-route (AWS CLI) 命令。使用 `--destination-prefix-list-id` 參數來指定字首清單的 ID。

Transit Gateway 路由表

您可以指定字首清單作為路由的目的地。如需詳細資訊，請參閱 Amazon VPC 傳輸閘道中的前綴清單參考資料。

AWS Network Firewall 規則群組

AWS Network Firewall 規則群組是一組可重複使用的條件，用於檢查和處理網路流量。如果您在 中建立 Suricata 相容具狀態規則群組 AWS Network Firewall，您可以從規則群組參考字首清單。如需詳細資訊，請參閱《AWS Network Firewall 開發人員指南》中的參考 Amazon VPC 字首清單和建立具狀態的規則群組。

Amazon Managed Grafana 網路存取控制

您可以指定一個或多個字首清單作為 Amazon Managed Grafana 工作區請求的傳入規則。如需有關 Grafana 工作區網路存取控制的詳細資訊，包括如何參考字首清單，請參閱《Amazon Managed Grafana 使用者指南》中的管理網路存取。

AWS Outposts 機架本機閘道

每個 AWS Outposts 機架都提供本機閘道，可讓您將 Outpost 資源連線至內部部署網路。您可以對字首清單中經常使用的 CIDR 進行分組，並在本機閘道路由表中將此清單參考為路由目標。如需詳細資訊，請參閱《機架AWS Outposts 使用者指南》中的管理本機閘道路由表。

AWS IP 地址範圍

AWS 會以 JSON 格式發佈其目前的 IP 地址範圍。透過此資訊，您可以識別來自 的流量 AWS。您也可以使用此資訊允許或拒絕往來部分 AWS 服務的流量。

考量事項

- 我們會發布客戶通常用來執行輸出篩選的服務的 IP 位址範圍。我們不會發布所有服務的 IP 位址範圍。
- 服務會利用其 IP 位址範圍與其他服務或客戶網路進行通訊。
- 您 AWS 透過使用自有 IP 地址 (BYOIP) 帶到 的 IP 地址範圍不包含在 `.json` 檔案中。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的透過 AWS公告地址範圍。

有些服務會使用 AWS受管字首清單來發佈其地址範圍。如需詳細資訊，請參閱the section called “可用的 AWS受管字首清單”。

目錄

- 下載 JSON 檔案
- 輸出控制
- 地理位置提要
- 尋找 的 IP 地址範圍 AWS 服務
- AWS IP 地址範圍 JSON 的語法
- AWS IP 地址範圍通知

下載 JSON 檔案

若要檢視目前的位址範圍，請下載 ip-ranges.json。若要保持歷史記錄，請在自己的電腦上儲存連續版本的 JSON 檔案。若要判斷自上次儲存檔案之後是否有所變更，請查看目前檔案中的發佈時間，然後比較最後所儲存檔案的發佈時間。

以下是將 JSON 檔案儲存至目前目錄的範例 curl 命令。

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```

如果您以程式設計方式存取此檔案，您必須負責確保只有當伺服器提出的 TLS 憑證驗證成功之後，才讓應用程式下載檔案。

若要接收 JSON 檔案更新通知，請參閱 AWS IP 地址範圍通知。

輸出控制

若要允許您使用一個 AWS 服務建立的資源只存取其他 AWS 服務，您可以使用 ip-ranges.json 檔案中的 IP 地址範圍資訊來執行輸出篩選。確保安全群組規則允許將輸出流量傳送至 AMAZON 清單中的 CIDR 區塊。有安全群組的配額。視每個區域中的 IP 地址範圍數目而定，每個區域可能需要多個安全群組。

> **Note**
>
> 有些 AWS 服務是以 EC2 為基礎，並使用 EC2 IP 地址空間。如果您封鎖傳送至 EC2 IP 地址空間的流量，也會封鎖這些非 EC2 服務的流量。

地理位置提要

中的 IP 地址範圍`ip-ranges.json`是依據 AWS 區域。然而，Local Zone 與其父區域不在相同的實體位置。在 Local Zones 的 geo-ip-feed.csv 帳戶中發布的地理位置資料。資料遵循 RFC 8805。

尋找 的 IP 地址範圍 AWS 服務

提供的 AWS IP 地址範圍 JSON 檔案 AWS 可以是尋找各種 AWS 服務的 IP 地址並使用該資訊來增強網路安全和存取控制的寶貴資源。透過剖析此 JSON 檔案中包含的詳細資訊，您可以精確識別與特定 AWS 服務 和區域相關聯的 IP 位址範圍。

例如，您可以使用 IP 地址範圍來設定強大的網路安全政策，設定精細防火牆規則以允許或拒絕存取特定 AWS 資源。此資訊也適用於各種 AWS Network Firewall 任務。此控制層級對於保護您的應用程式和資料至關重要，可確保只有授權流量能達到必要的 AWS 服務。此外，擁有此 IP 情報可協助您確保應用程式已正確設定為與正確的 AWS 端點通訊，從而改善整體可靠性和效能。

除了防火牆規則之外，`ip-ranges.json` 檔案也可以用來在您的網路基礎設施上設定複雜的輸出篩選。透過了解不同 的目的地 IP 地址範圍 AWS 服務，您可以設定路由政策或使用進階網路安全解決方案，例如根據其預期目的地選擇性地允許或封鎖傳出流量。此輸出控制對於降低資料外洩和未經授權存取的風險至關重要。

請務必注意，`ip-ranges.json` 檔案會定期更新，因此維護最新的本機複本對於確保您擁有最準確且最新的資訊至關重要。透過持續使用此檔案的內容，您可以有效率地管理以應用程式 AWS為基礎的網路存取和安全性，以強化您的整體雲端安全狀態。

下列範例可協助您將 AWS IP 地址範圍篩選為您正在尋找的內容。在 Linux 上，您可以下載並使用 jq 工具來剖析 JSON 檔案的本機複本。AWS Tools for Windows PowerShell 包含一個 cmdlet，Get-

AWSPublicIpAddressRange，您可以用來剖析此 JSON 檔案。如需詳細資訊，請參閱以下部落格：查詢 AWS的公有 IP 位址範圍。

若要取得 JSON 檔案，請參閱the section called “下載”。如需 JSON 檔案語法的詳細資訊，請參閱 the section called “語法”。

範例

- 取得檔案建立日期
- 取得特定區域的 IP 位址
- 取得所有 IPv4 地址
- 取得適用於特定服務的所有 IPv4 地址
- 取得特定區域中適用於特定服務的所有 IPv4 地址
- 取得所有 IPv6 地址
- 取得適用於特定服務的所有 IPv6 地址
- 取得特定邊界群組的所有 IP 位址

取得檔案建立日期

下列範例取得 `ip-ranges.json` 的建立日期。

jq

```
$ jq .createDate < ip-ranges.json

"2024-08-01-17-22-15"
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate

Thursday, August 1, 2024 9:22:35 PM
```

取得特定區域的 IP 位址

下列範例會篩選指定區域的 IP 位址的 JSON 檔案。

jq

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

取得所有 IPv4 地址

下列範例會篩選 IPv4 地址的 JSON 檔案。

jq

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json
```

```
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

取得適用於特定服務的所有 IPv4 地址

下列範例會篩選指定服務的 IPv4 地址的 JSON 檔案。

jq

```
$ jq -r '.prefixes[] | select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-
ranges.json

13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
```

```
15.197.36.0/22
...
```

取得特定區域中適用於特定服務的所有 IPv4 地址

下列範例會篩選指定區域中指定服務的 IPv4 地址的 JSON 檔案。

jq

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") |
 select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-ranges.json

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
99.82.166.0/24
99.82.171.0/24
...
```

取得所有 IPv6 地址

下列範例會篩選 IPv6 地址的 JSON 檔案。

jq

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
```

```
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

取得適用於特定服務的所有 IPv6 地址

下列範例會篩選指定服務的 IPv6 地址的 JSON 檔案。

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv6"} | select IpPrefix

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

取得特定邊界群組的所有 IP 位址

下列範例會篩選指定邊界群組的所有 IP 位址的 JSON 檔案。

jq

```
$ jq -r '.prefixes[] | select(.network_border_group=="us-west-2-lax-1")
 | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

AWS IP 地址範圍 JSON 的語法

AWS 會以 JSON 格式發佈其目前的 IP 地址範圍。若要取得 JSON 檔案，請參閱the section called “下載”。JSON 檔案的語法如下所示。

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
```

```
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

以 Unix epoch 時間格式表示的發佈時間。

類型：字串

範例：`"syncToken": "1416435608"`

createDate

出版日期和時間，以 UTC YY-MM-DD-hh-mm-ss 格式表示。

類型：字串

範例：`"createDate": "2014-11-19-23-29-02"`

字首

IPv4 地址範圍的 IP 字首。

類型：陣列

ipv6_prefixes

IPv6 地址範圍的 IP 字首。

類型：陣列

ip_prefix

使用 CIDR 表示法的公有 IPv4 地址範圍。請注意， AWS 可能會公告更特定範圍內的字首。例如，檔案中的字首 96.127.0.0/17 可能會宣告為 96.127.0.0/21、96.127.8.0/21、96.127.32.0/19 及 96.127.64.0/18。

類型：字串

範例：`"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

使用 CIDR 表示法的公有 IPv6 地址範圍。請注意， AWS 可能會公告更特定範圍內的字首。

類型：字串

範例：`"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

網路邊界群組的名稱，這是一組唯一的可用區域或本機區域，可從中 AWS 公告 IP 地址 或 GLOBAL。GLOBAL 服務的流量可以吸引到多個 （最多所有） 可用區域或從中 AWS 公告 IP 地址的本機區域。

類型：字串

範例：`"network_border_group": "us-west-2-lax-1"`

region

AWS 區域或 GLOBAL。GLOBAL 服務的流量可以吸引到多個 （最多所有） AWS 區域，或源自多個區域。

類型：字串

有效值：`af-south-1 | ap-east-1 | ap-east-2 | ap-northeast-1 | ap-northeast-2 | ap-northeast-3 | ap-south-1 | ap-south-2 | ap-southeast-1 | ap-southeast-2 | ap-southeast-3 | ap-southeast-4 | ap-southeast-5 | ap-southeast-6 | ap-southeast-7 | ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | mx-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-gov-east-1 | us-gov-west-1 | us-west-1 | us-west-2 | GLOBAL`

範例：`"region": "us-east-1"`

服務

IP 地址範圍的子集。列出的 API_GATEWAY 位址僅為輸出。指定 AMAZON 取得所有 IP 位址範圍 (表示每個子集也位於 AMAZON 子網路中)。不過，某些 IP 位址範圍只在 AMAZON 子集中 (表示它們在另一個子集中也不可用)。

類型：字串

有效值： AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL CHIME_MEETINGS | CHIME_VOICECONNECTOR | | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD DYNAMODB | EBS EC2 | EC2_INSTANCE_CONNECT | | GLOBALACCELERATOR | IVS_LOW_LATENCY | IVS_REALTIME | | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | | ROUTE53 ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER S3 WORKSPACES_GATEWAYS

範例：`"service": "AMAZON"`

範圍重疊

任何服務代碼所傳回的 IP 地址範圍也會由 AMAZON 服務代碼傳回。例如，S3 服務代碼所傳回的所有 IP 地址範圍也會由 AMAZON 服務代碼傳回。

當服務 A 使用服務 B 的資源時，會有服務 A 和服務 B 的服務代碼傳回的 IP 地址範圍。不過，這些 IP 地址範圍僅供服務 A 使用，而服務 B 無法使用。例如，Amazon S3 使用 Amazon EC2 的資源，因此有 S3 和 EC2 服務代碼傳回的 IP 地址範圍。不過，這些 IP 地址範圍僅供 Amazon S3 使用。因此，S3 服務代碼會傳回 Amazon S3 專門使用的所有 IP 地址範圍。若要識別 Amazon EC2 專門使用的 IP 地址範圍，請尋找 EC2 服務代碼 (但不是 S3 服務代碼) 傳回的 IP 地址範圍。

進一步了解

本節提供不同服務代碼的額外資訊連結。

- AMAZON_APPFLOW – IP 地址範圍
- AMAZON_CONNECT – 設定您的網路
- CHIME_MEETINGS — 為媒體和訊號設定
- CLOUDFRONT – CloudFront 邊緣伺服器的位置和 IP 地址範圍
- DYNAMODB – IP 地址範圍
- EC2 – 公有 IPV4 地址
- EC2_INSTANCE_CONNECT — EC2 Instance Connect 先決條件
- GLOBALACCELERATOR – Global Accelerator 邊緣伺服器的位置和 IP 地址範圍
- ROUTE53 – Amazon Route 53 伺服器的 IP 地址範圍
- ROUTE53_HEALTHCHECKS – Amazon Route 53 伺服器的 IP 地址範圍

- ROUTE53_HEALTHCHECKS_PUBLISHING – Amazon Route 53 伺服器的 IP 地址範圍
- WORKSPACES_GATEWAYS – PCoIP 閘道伺服器

版本備註

下表說明 ip-ranges.json 的語法更新。我們也會在每個地區啟用時新增區域代碼。

說明	發行日期
新增 IVS_LOW_LATENCY 服務代碼。	2025 年 7 月 29 日
新增 AURORA_DSQL 服務代碼。	2025 年 5 月 21 日
新增 IVS_REALTIME 服務代碼。	2024 年 6 月 11 日
新增 MEDIA_PACKAGE_V2 服務代碼。	2023 年 5 月 9 日
新增 CLOUDFRONT_ORIGIN_FACING 服務代碼。	2021 年 10 月 12 日
新增 ROUTE53_RESOLVER 服務代碼。	2021 年 6 月 24 日
新增 EBS 服務代碼。	2021 年 5 月 12 日
新增 KINESIS_VIDEO_STREAMS 服務代碼。	2020 年 11 月 19 日
新增 CHIME_MEETINGS 和 CHIME_VOICECONNECTOR 服務代碼。	2020 年 6 月 19 日
新增 AMAZON_APPFLOW 服務代碼。	2020 年 6 月 9 日
新增網路邊界群組的支援。	2020 年 4 月 7 日
新增 WORKSPACES_GATEWAYS 服務代碼。	2020 年 3 月 30 日
新增 ROUTE53_HEALTHCHECK_PUBLISHING 服務代碼。	2020 年 1 月 30 日
新增 API_GATEWAY 服務代碼。	2019 年 9 月 26 日

說明	發行日期
新增 EC2_INSTANCE_CONNECT 服務代碼。	2019 年 6 月 26 日
新增 DYNAMODB 服務代碼。	2019 年 4 月 25 日
新增 GLOBALACCELERATOR 服務代碼。	2018 年 12 月 20 日
新增 AMAZON_CONNECT 服務代碼。	2018 年 6 月 20 日
新增 CLOUD9 服務代碼。	2018 年 6 月 20 日
新增 CODEBUILD 服務代碼。	2018 年 4 月 19 日
新增 S3 服務代碼。	2017 年 2 月 28 日
新增 IPv6 地址範圍的支援。	2016 年 8 月 22 日
初始版本	2014 年 11 月 19 日

AWS IP 地址範圍通知

AWS 會以 JSON 格式發佈其目前的 IP 地址範圍。每當 AWS IP 地址範圍發生變更時，我們會傳送通知給名為 的 Amazon SNS 主題訂閱者AmazonIpSpaceChanged。如需 JSON 檔案語法的詳細資訊，請參閱 the section called “語法”。

通知承載內容包含以下格式的資訊。

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

建立日期和時間。

通知可能不會按順序傳送。因此，建議您查看時間戳記，確保順序正確。

synctoken

以 Unix epoch 時間格式表示的發佈時間。

md5

`ip-ranges.json` 檔案的密碼編譯雜湊值。您可以使用此值來檢查下載檔因是否損毀。

url

`ip-ranges.json` 檔案的位置。如需詳細資訊，請參閱the section called “下載”。

您可以訂閱以接收通知，如下所示。

訂閱 AWS IP 地址範圍通知

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 如有必要，請在導覽列中將「區域」變更為美國東部 (維吉尼亞北部)。您必須選取此區域，因為您要訂閱的 SNS 通知已在本區域中建立完成。
3. 在導覽窗格中，選擇 Subscriptions (訂閱)。
4. 選擇 Create subscription (建立訂閱)。
5. 在 Create subscription (建立訂閱) 對話方塊中，執行下列動作：
   a. 對於 Topic ARN (主題 ARN)，請複製下列 Amazon Resource Name (ARN)：

      ```
      arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
      ```

   b. 對於Protocol (通訊協定)，請選擇要使用的通訊協定 (例如，`Email`)。
   c. 對於Endpoint (端點)，請鍵入端點以接收通知 (例如，您的電子郵件地址)。
   d. 選擇建立訂閱。
6. 我們將會聯絡您有關所指定的端點，並要求您確認訂閱。例如，如果您指定了電子郵件地址，將會收到一封電子郵件訊息，主旨行為 `AWS Notification - Subscription Confirmation`。請依照指示來確認訂閱。

通知受制於端點的可用性。因此，您可能想要定期檢查 JSON 檔案，以確保取得最新的範圍。如需 Amazon SNS 可靠性的詳細資訊，請參閱https://aws.amazon.com/sns/faqs/#Reliability。

如果您不想再接收這些通知，請使用下列程序來取消訂閱。

取消訂閱 AWS IP 地址範圍通知

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇訂閱。
3. 勾選訂閱的核取方塊。
4. 對於 Actions (動作)，請選擇 Delete subscriptions (刪除訂閱)。
5. 出現確認提示時，請選擇刪除。

如需有關 Amazon SNS 的詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》。

VPC 的 IPv6 支援

如果您的現有 VPC 僅支援 IPv4，而且子網路中的資源設定成僅使用 IPv4，則可以新增 VPC 和資源的 IPv6 支援。您的 VPC 可在雙堆疊模式中運作：您的資源可透過 IPv4、IPv6 或兩者進行通訊。IPv4 和 IPv6 通訊彼此獨立。

您無法停用 VPC 和子網的 IPv4 支援；這是 Amazon VPC 和 Amazon EC2 的預設 IP 定址系統。

考量事項

- 沒有從僅限 IPv4 的子網路到僅限 IPv6 的子網路之遷移路徑。
- 本範例假設您的現有 VPC 包含公有和私有子網路。如需建立新 VPC 來搭配 IPv6 使用的相關資訊，請參閱the section called “建立 VPC”。
- 開始使用 IPv6 之前，請確定您已閱讀 Amazon VPC 的 IPv6 定址功能：比較 IPv4 和 IPv6。

目錄

- 新增 VPC 的 IPv6 支援
- 雙堆疊 VPC 組態範例

新增 VPC 的 IPv6 支援

下表概述了為您的 VPC 啟用 IPv6 的流程。

目錄

- 步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網的關聯
- 步驟 2：更新路由表

- 步驟 3：更新安全群組規則
- 步驟 4：將 IPv6 地址指派給執行個體

步驟	備註
步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網的關聯	將 Amazon 提供的或 BYOIP IPv6 CIDR 區塊與 VPC 和子網建立關聯。
步驟 2：更新路由表	更新路由表以遞送 IPv6 流量。針對公有子網，建立路由，以將所有 IPv6 流量從子網遞送至網際網路閘道。針對私有子網，建立路由，以將所有網際網路綁定型 IPv6 流量從子網遞送至輸出限定網際網路閘道。
步驟 3：更新安全群組規則	更新安全群組規則，以包含 IPv6 地址的規則。這可讓 IPv6 流量進出執行個體。如果您已建立自訂網路 ACL 規則來控制進出子網的流量流程，則必須包含 IPv6 流量的規則。
步驟 4：將 IPv6 地址指派給執行個體	將 IPv6 地址從子網的 IPv6 地址範圍指派給執行個體。

步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網的關聯

您可以建立 IPv6 CIDR 區塊與 VPC 的關聯，然後建立該範圍中的 /64 CIDR 區塊與每個子網的關聯。

建立 IPv6 CIDR 區塊與 VPC 的關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取您的 VPC。
4. 選擇動作、編輯 CIDR，然後選擇新增 IPv6 CIDR。
5. 選取下列其中一個選項，然後選擇選取 CIDR：
   - Amazon 提供的 IPv6 CIDR 區塊 – 使用 Amazon 的 IPv6 地址集區中的 IPv6 CIDR 區塊。針對網路邊界群組，選擇從中 AWS 公告 IP 地址的群組。

- IPAM 配置的 IPv6 CIDR 區塊 – 使用 IPAM 集區中的 IPv6 CIDR 區塊。選擇 IPAM 集區和 IPv6 CIDR 區塊。
- 我擁有的 IPv6 CIDR – 使用 IPv6 地址集區 (BYOIP) 中的 IPv6 CIDR 區塊。選擇 IPv6 地址集區和 IPv6 CIDR 區塊。

6. 選擇關閉。

建立 IPv6 CIDR 區塊與子網的關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選取子網路。
4. 選擇動作、編輯 IPv6 CIDR，然後選擇新增 IPv6 CIDRs。
5. 視需要編輯 CIDR 區塊 (例如，取代 `00`)。
6. 選擇儲存。
7. 為 VPC 中的任何其他子網路重複此程序。

如需詳細資訊，請參閱IPv6 VPC CIDR 區塊。

步驟 2：更新路由表

當您將 IPv6 CIDR 區塊與您的 VPC 建立關聯時，會自動將區域路由新增至 VPC 的每個路由表，以允許 VPC 中的 IPv6 流量。

您必須更新公有子網路的路由表，讓執行個體 (例如 Web 伺服器) 將網際網路閘道用於 IPv6 流量。您還必須更新私有子網路的路由表，讓執行個體 (例如資料庫執行個體) 將輸出限定網際網路閘道用於 IPv6 流量，因為 NAT 閘道不支援 IPv6。

更新公有子網路的路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。選取公有子網路。在路由表索引標籤上，選擇路由表 ID 以開啟路由表的詳細資訊頁面。
3. 選取 路由表。在 Routes (路由) 標籤中，選擇 Edit routes (編輯路由)。
4. 選擇 Add route (新增路由)。對於目的地，請選擇 `::/0`。選擇目標的網際網路閘道的 ID。
5. 選擇儲存變更。

更新私有子網路的路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇輸出限定網際網路閘道。選擇建立輸出限定網際網路閘道。從 VPC 中選擇您的 VPC，然後選擇建立輸出限定網際網路閘道。

   如需詳細資訊，請參閱使用輸出限定 (egress-only) 網際網路閘道來啟用傳出 IPv6 流量。
3. 在導覽窗格中，選擇 Subnets (子網)。選取私有子網路。在路由表索引標籤上，選擇路由表 ID 以開啟路由表的詳細資訊頁面。
4. 選取 路由表。在 Routes (路由) 標籤中，選擇 Edit routes (編輯路由)。
5. 選擇 Add route (新增路由)。對於目的地，請選擇 `::/0`。選擇目標的輸出限定網際網路閘道的 ID。
6. 選擇儲存變更。

> **Note**
>
> 路由表不能同時存在指向網際網路閘道與僅限輸出網際網路閘道的相同目的地 (::/0)。如果您在設定僅限輸出網際網路閘道時收到 "There are existing ipv6 routes with next hop as internet Gateway" 錯誤訊息，必須先刪除指向網際網路閘道的現有 IPv6 路由，才能新增指向僅限輸出網際網路閘道的路由。

如需詳細資訊，請參閱路由選項範例。

步驟 3：更新安全群組規則

若要讓執行個體透過 IPv6 傳送和接收流量，您必須更新安全群組規則以包含 IPv6 地址的規則。例如，在上述範例中，您可以更新 Web 伺服器安全群組 (`sg-11aa22bb11aa22bb1`) 以新增規則，允許透過 IPv6 地址的傳入 HTTP、HTTPS 和 SSH 存取。您不需要變更資料庫安全群組的傳入規則；允許來自 `sg-11aa22bb11aa22bb1` 之所有通訊的規則包含 IPv6 通訊。

更新傳入安全群組規則

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組，然後選取 Web 伺服器安全群組。
3. 在傳入規則索引標籤中，選擇編輯傳入規則。

4. 對於允許 IPv4 流量的每個規則，請選擇新增規則，然後將規則設定為允許對應的 IPv6 流量。例如，若要新增規則以允許透過 IPv6 的所有 HTTP 流量，請針對類型選擇 HTTP，然後針對來源選擇 `::/0`。
5. 當您完成新增規則的作業時，請選擇儲存規則。

更新傳出安全群組規則

當您將 IPv6 CIDR 區塊與 VPC 建立關聯時，我們會自動為允許所有 IPv6 流量的 VPC 的安全群組新增傳出規則。不過，如果您已修改安全群組的原始傳出規則，則不會自動新增此規則，而且您必須新增 IPv6 流量的對等傳出規則。

更新網路 ACL 規則

當您將 IPv6 CIDR 區塊與 VPC 建立關聯時，會自動將規則新增至預設網路 ACL 以允許 IPv6 流量。不過，如果您修改預設網路 ACL，或已建立自訂網路 ACL，則必須手動新增 IPv6 流量的規則。如需詳細資訊，請參閱新增與刪除規則。

步驟 4：將 IPv6 地址指派給執行個體

所有目前世代的執行個體類型都支援 IPv6。如果您的執行個體類型不支援 IPv6，您必須將執行個體的大小調整為支援的執行個體類型，然後才能指派 IPv6 地址。您將使用的程序取決於所選擇的新執行個體類型是否與目前的執行個體類型相容。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的變更執行個體類型。如果您必須從新的 AMI 啟動執行個體以支援 IPv6，則可以在啟動期間將 IPv6 地址指派給執行個體。

確認執行個體類型支援 IPv6 之後，即可使用 Amazon EC2 主控台將 IPv6 地址指派給執行個體。IPv6 位址會指派給執行個體的主要網路介面 (例如 eth0)。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將 IPv6 地址指派給執行個體。

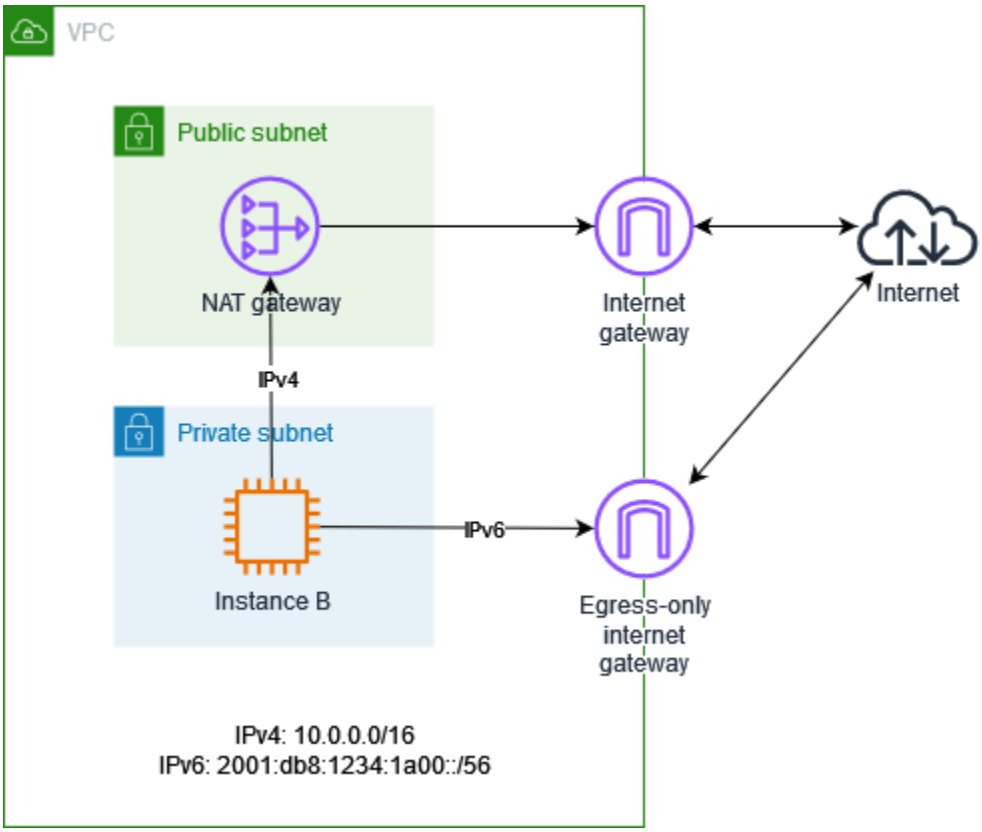
您可以使用執行個體的 IPv6 地址連線到執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的透過 SSH 用戶端連線至 Linux 執行個體。

如果您使用適用於目前版本作業系統的 AMI 啟動執行個體，則您的執行個體將設定為使用 IPv6。如果您無法從執行個體 ping IPv6 地址，請參閱適用於您作業系統的說明文件來設定 IPv6。

雙堆疊 VPC 組態範例

透過雙堆疊組態，您可以使用 IPv4 和 IPv6 地址，在 VPC 中的資源與透過網際網路的資源之間進行通訊。

下圖呈現 VPC 的架構。您的 VPC 具有公有子網路和私有子網路。VPC 和子網路必須具有 IPv4 CIDR 區塊和 IPv6 CIDR 區塊。私有子網路中有一個同時具有 IPv4 地址和 IPv6 地址的 EC2 執行個體。執行個體可以使用 NAT 閘道將傳出 IPv4 流量傳送到網際網路，並使用僅輸出網際網路閘道將傳出 IPv6 流量傳送到網際網路。



公有子網路路由表

以下是公有子網路的路由表。前兩個項目是本機路由。第三個項目會將所有 IPv4 流量傳送到網際網路閘道。請注意，僅當您計劃在公有子網路中啟動採用 IPv6 位址的 EC2 執行個體時，才必須用到第四個項目。

目標	Target
VPC A IPv4 CIDR	本機
VPC A IPv6 CIDR	區域
0.0.0.0/0	*internet-gateway-id*
::/0	*internet-gateway-id*

私有子網路路由表

以下是私有子網路的路由表。前兩個項目是本機路由。第三個項目會將所有 IPv4 流量傳送到 NAT 閘道。最後一個項目會將所有 IPv6 流量傳送到僅輸出網際網路閘道。

目標	Target
VPC A IPv4 CIDR	本機
VPC A IPv6 CIDR	區域
0.0.0.0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

AWS 支援 IPv6 的 服務

電腦和智慧型裝置會使用 IP 地址以在網際網路和其他網路上彼此進行通訊。隨著網際網路不斷增長，IP 地址的需求也持續增加。IP 地址最常見的格式為 IPv4。IP 地址的新格式是 IPv6，其提供比 IPv4 更大的地址空間。

AWS 服務 IPv6 的支援包括對雙堆疊組態 (IPv4 和 IPv6) 或僅限 IPv6 組態的支援。例如，虛擬私有雲端 (VPC) 是 的邏輯隔離區段，您可以在 AWS 雲端 其中啟動 AWS 資源。在 VPC 中，您可以建立僅限 IPv4、雙堆疊或僅限 IPv6 的子網路。

AWS 服務 支援透過公有端點存取。有些 AWS 服務 也支援使用 支援的私有端點進行存取 AWS PrivateLink。 AWS 服務 可以透過其私有端點支援 IPv6，即使它們不支援透過其公有端點存取 IPv6。支援 IPv6 的端點可以使用 AAAA 記錄回應 DNS 查詢。

支援 IPv6 的服務

下表列出 AWS 服務 提供雙堆疊支援的 、僅限 IPv6 的支援，以及支援 IPv6 的端點。我們會在推出其他 IPv6 支援時更新此表格。如需有關服務如何支援 IPv6 的詳細資訊，請參閱服務的說明文件。

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
AWS Amplify	是	否	是	

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon API Gateway	是	否	是	是
AWS App Mesh	是	是	是	否
AWS App Runner	是	否	是	是
AWS AppConfig	是	否	是	是
Application Auto Scaling	否	否	是	是
AWS Application Discovery Service	是	否	是	是
應用程式復原控制器 (ARC)	是	否	是	
Amazon WorkSpaces 應用程式	是	否	否	否
AWS AppSync[2]	部分	否	部分	是
Amazon Athena	是	否	是	是
AWS Audit Manager	否	否	是	是
Amazon Aurora	是	否	是	否
Amazon Aurora DSQL	否	否	是	是
AWS Auto Scaling	否	否	是	是
AWS B2B 資料交換	是	否	是	是
AWS Backup	是	否	是	是
AWS Batch	是	否	是	是
Amazon Bedrock	否	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
AWS 帳單與成本管理 資料匯出	是	否	是	是
AWS 帳單與成本管理 定價計算器	是	否	是	是
AWS Billing Conductor	是	否	是	是
AWS Budgets	是	否	是	
Amazon Braket	是	是	是	是
AWS Certificate Manager	是	否	是	否
Amazon Chime SDK	是	否	是	
Amazon Comprehend	是	是	是	是
AWS Clean Rooms	是	是	是	是
AWS Clean Rooms ML	是	是	是	是
AWS Cloud9	是	否	是	
AWS 雲端控制 API	是	否	是	是
CloudFormation	否	否	是	是
Amazon CloudFront	是	是	是	
AWS CloudHSM	是	否	是	是
AWS CloudTrail	是	否	是	是
Amazon CloudWatch	是	是	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon CloudWatch Application Insights	否	否	是	是
Amazon CloudWatch 網路監視器	否	否	是	是
Amazon CloudWatch Logs	是	是	是	是
Amazon CloudWatch Observability Access Manager	是	是	是	
Amazon CloudWatch Synthetics	是	否	是	是
AWS Cloud Map	是	是	是	是
AWS 雲端 WAN	是	否	是	否
AWS CodeArtifact	是	否	是	是
連接客戶設定檔	是	否	是	是
AWS CodeBuild	否	否	是	是
AWS CodeCommit	否	否	是	是
AWS CodeDeploy	否	否	是	是
AWS Compute Optimizer	否	否	是	是
Amazon Comprehend Medical	否	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon CodeGuru Profiler	是	否	是	是
Amazon Cognito	是	否	是	
AWS Config	否	否	是	是
AWS Control Tower	否	否	是	是
AWS Cost Explorer	是	否	是	是
AWS 成本最佳化中心	是	否	是	是
AWS Data Exchange	否	否	是	是
Amazon Data Firehose	否	否	是	是
Amazon Data Lifecycle Manager	是	否	是	是
AWS Database Migration Service	是	否	否	是
AWS DataSync	是	是	是	是
Amazon DataZone	否	否	是	是
AWS Deadline Cloud	是	否	是	是
Amazon Detective	是	是	是	
Direct Connect	是	是	否	是
Directory Service	否	否	是	是
Amazon EBS direct API	是	否	是	是
Amazon EC2	是	是	是	否

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
EC2 Image Builder	是	是	是	是
Amazon ECR	是	否	是	否
Amazon ECS	是	是	是	是
Amazon EFS	是	是	是	是
Amazon EKS	部分	部分	是	是
Amazon EMR	否	否	是	是
AWS Elastic Beanstalk	是	否	是	是
AWS 彈性災難復原	否	否	是	是
Elastic Load Balancing	部分	部分	是	否
Amazon ElastiCache	是	是	否	是
AWS Elemental MediaConvert	否	否	是	是
AWS Elemental MediaConnect	是	是	是	部分
AWS 最終使用者傳訊社交	是	否	是	否
AWS Entity Resolution	是	否	是	是
Amazon EventBridge	否	否	是	是
AWS Fargate	是	否	是	是
Amazon FSx	否	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon GameLift Streams	是	否	是	是
AWS Global Accelerator	是	否	是	
AWS Glue	是	否	否	是
AWS Glue DataBrew	否	否	是	是
Amazon Managed Grafana [3]	是	否	是	是
AWS Ground Station [4]	是	否	是	是
Amazon GuardDuty	否	否	是	是
AWS HealthImaging	否	否	是	是
AWS HealthLake	否	否	是	是
AWS HealthOmics	否	否	是	是
AWS Identity and Access Management (IAM)	是	是	是	否
AWS IAM Access Analyzer	是	否	是	是
AWS IAM Identity Center	是	否	是	
AWS IAM Roles Anywhere	否	否	是	是
Amazon Inspector	是	是	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon Interactive Video Service (IVS) [5]	是	否	是	是
AWS IoT Core	是	否	是	是
AWS IoT Device Defender	是	否	是	否
AWS IoT Device Management	是	否	是	否
AWS IoT FleetWise	是	否	是	是
AWS IoT Greengrass	是	否	是	否
AWS IoT SiteWise	是	否	是	是
AWS IoT TwinMaker	是	否	是	是
AWS IoT Wireless	是	否	是	是
Amazon Kendra	否	否	是	否
AWS Key Management Service	是	部分	是	是
Amazon Keyspaces	是	是	是	是
Amazon Keyspaces CDC streams	是	是	是	是
Amazon Kinesis Data Streams	是	否	是	是
AWS Lake Formation	否	否	否	是
AWS Lambda	是	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
AWS Launch Wizard	否	否	是	是
AWS License Manager	否	否	是	是
Amazon Lightsail	是	是	是	是
Amazon Location Service	否	否	是	是
Amazon MQ	否	否	是	是
Amazon MWAA	否	否	是	是
Amazon Macie	是	否	是	是
AWS Mainframe Modernization	是	否	是	是
Amazon Managed Grafana	否	否	是	是
Amazon Managed Service for Prometheus	是	否	是	是
AWS Migration Hub Orchestrator	否	否	是	是
AWS Network Firewall	是	是	否	是
AWS Network Manager	是	否	是	否
Amazon OpenSearch Service	是	否	是	
AWS Organizations	是	否	是	是
AWS Outposts	否	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon Personalize	是	否	是	是
Amazon Pinpoint	是	否	是	是
Amazon Polly	是	否	是	是
AWS 價格表	否	否	是	否
AWS 私有憑證授權單位	是	否	是	是
AWS 私有 CA 適用於 Active Directory 的連接器	是	否	是	是
AWS 私有 CA 適用於 SCEP 的連接器	是	否	是	是
AWS PrivateLink	是	是	是	
Amazon Q Business	否	否	是	否
Amazon RDS	是	否	是	否
Amazon RDS Data API	否	否	是	是
Amazon RDS Performance Insights	否	否	是	是
Amazon Redshift	是	否	是	
Amazon Rekognition	否	否	是	是
資源回收筒	是	否	是	是
AWS re:Post Private	是	否	是	是
AWS Resource Access Manager	是	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
AWS 資源總管	是	否	是	否
AWS Resource Groups	是	是	是	是
AWS Resource Groups Tagging API	是	是	是	是
Amazon Route 53	是	是	是	是
Amazon S3	是	否	是	否
Amazon S3 on Outposts	否	否	是	否
Amazon SageMaker	否	否	是	是
AWS Secrets Manager	是	否	是	是
AWS Security Hub	否	否	是	是
Amazon Security Lake	是	否	是	是
AWS Security Token Service	是	否	是	是
AWS Service Catalog	否	否	是	是
AWS Shield	是	是	否	是
Amazon Simple Email Service	是	否	是	是
Amazon Simple Notification Service	是	否	是	是
Amazon Simple Queue Service	是	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
Amazon Simple Workflow Service	是	否	是	是
AWS Site-to-Site VPN	是	否	是	否
AWS Snow Family	否	否	是	
AWS Step Functions	是	否	是	是
AWS Storage Gateway	是	是	是	是
AWS Systems Manager	否	否	是	是
AWS Systems Manager Incident Manager	否	否	是	是
AWS Systems Manager 適用於 SAP 的	否	否	是	是
Amazon Textract	否	否	是	是
Amazon Timestream	否	否	是	是
Amazon Transcribe	是	是	是	是
AWS Transfer Family [6]	是	否	是	是
AWS Transit Gateway	是	否	是	否
Amazon Translate	是	是	是	是
AWS Trusted Advisor	否	否	是	是
AWS 使用者通知	否	否	是	是
Amazon Verified Permissions	是	否	是	是

服務名稱	雙堆疊支援	僅限 IPv6 支援	公有端點支援 IPv6	私有端點支援 IPv6[1]
VMware Cloud on AWS	否	否	是	是
Amazon VPC	是	是	是	否
Amazon VPC Lattice	否	否	是	是
AWS WAF	是	是	否	
AWS WAFV2	否	否	是	是
AWS Well-Architected Tool	否	否	是	是
Amazon WorkMail	否	否	是	是
Amazon WorkSpaces	是	否	是	是
AWS X-Ray	是	否	是	是

[1] 空白儲存格表示服務沒有與 AWS PrivateLink整合。

[2] 此項目代表透過 AWS AppSync SDK API 對 AWS AppSync GraphlQL 與 Event API 組態操作的 IPv6 支援。IPv6 不支援用戶端連線至客戶受管 AWS AppSync GraphQL 和事件 APIs。

[3] 此項目代表對 Grafana 工作區管理操作 (例如更新工作區與工作區許可) 的 IPv6 支援。一般 Grafana 工作區操作 (例如建立與編輯儀表板、查詢資料來源) 皆不支援 IPv6。

[4] 此項目代表對 AWS Ground Station 控制平面操作 (例如呼叫 AWS Ground Station API) 的 IPv6 支援。 AWS Ground Station 資料平面不支援 IPv6，因此請確定您要交付資料的資源 （ 例如 Amazon EC2 執行個體 ） 可透過 IPv4 存取。

[5] 此項目代表對 Amazon IVS 控制平面操作 (例如呼叫 IVS 端點) 的 IPv6 支援。

[6] 如需 中 IPv6 支援的詳細資訊 AWS Transfer Family，請參閱 IPv6 限制。

其他 IPv6 支援

運算

- Amazon EC2 支援根據 Nitro System 將執行個體啟動至僅限 IPv6 子網路中。
- Amazon EC2 可為 Instance Metadata Service (IMDS) 和 Amazon Time Sync Service 提供 IPv6 端點。

遊戲開發

- Amazon GameLift Streams 支援在 Microsoft Windows Server 2022 Base 執行時期上透過 IPv6 進行串流傳輸。

聯網與內容交付

- Amazon VPC 支援建立僅限 IPv6 子網路。
- Amazon VPC 透過支援子網路上的 DNS64IPv6 AWS IPv4 和 NAT 閘道上的 NAT64，協助 IPvNAT64 資源通訊。

安全性、身分與合規

- Amazon Detective 在自身網路相關調查結果與實體設定檔中皆支援 IPv6 位址。
- AWS Identity and Access Management (IAM) 支援 IAM 身分型政策中的 IPv6 地址。
- Amazon Macie 可在個人身分識別資訊 (PII) 中支援 IPv6 地址。
- Amazon Security Lake 在日誌來源與訂閱用戶的所有操作中皆支援 IPv6 位址。

管理與管控

- AWS CloudTrail 記錄包括來源 IPv6 資訊。
- AWS CLI v2 支援透過僅限 IPv6 用戶端的 IPv6 連線進行下載。 IPv6-only

進一步了解

- AWS上的 IPv6
- 雙堆疊和僅限 IPv6 Amazon VPC 參考架構 (PDF)

設定虛擬私有雲

Amazon Virtual Private Cloud (VPC) 是基本的建置區塊，可讓您在 AWS 雲端中佈建邏輯上隔離的虛擬網路。透過建立您自己的 VPC，您可以完全控制聯網環境，包括定義 IP 位址範圍、子網路、路由表和連線選項的能力。

AWS 您的帳戶包含每個 AWS 區域的預設 VPC。此預設 VPC 預先設定了設定，使其成為快速啟動資源的便利選項。然而，預設 VPC 不一定符合您的長期聯網需求。在這裡，建立其他 VPC 可能會帶來優勢。

建立其他 VPCs 與依賴每個新 AWS 帳戶佈建的預設 VPC 有幾個優勢。使用自我管理的 VPC，您可以根據您的具體需求，精確地設計網路拓撲，無論是實現多層應用程式、連接至內部部署資源，還是根據部門或業務單位隔離工作負載。

此外，建立多個 VPC 可以在不同應用程式或業務單位之間實現更高的安全性和隔離性。每個 VPC 充當獨立的虛擬網路，讓您可以針對每個環境應用不同的安全政策、存取控制和路由配置。

最終，是否使用預設 VPC 或建立一個 (或多個) 自訂 VPC 應基於您的應用需求、安全需求以及長期可擴展性目標。投入時間仔細設計 VPC 基礎設施，將能以一個強大、安全且適應性高的雲端網路基礎作為回報。

目錄

- VPC 基本概念
- VPC 組態選項
- 預設 VPC
- 建立 VPC
- 視覺化 VPC 中的資源
- 從您的 VPC 中新增或移除 CIDR 區塊
- Amazon VPC 中的 DHCP 選項集
- VPC 的 DNS 屬性
- VPC 的網路地址使用
- 與其他帳戶共享 VPC 子網路
- 將 VPC 擴展至本機區域、Wavelength 區域或 Outpost
- 刪除您的 VPC
- 使用 Console-to-Code，從 VPC 主控台操作產生基礎設施即程式碼

VPC 基本概念

VPC 遍及整個區域內的所有可用區域。建立 VPC 之後，您可以在各個可用區域新增一個或多個子網。如需詳細資訊，請參閱子網。

目錄

- VPC IP 地址範圍
- VPC 圖表
- VPC 資源

VPC IP 地址範圍

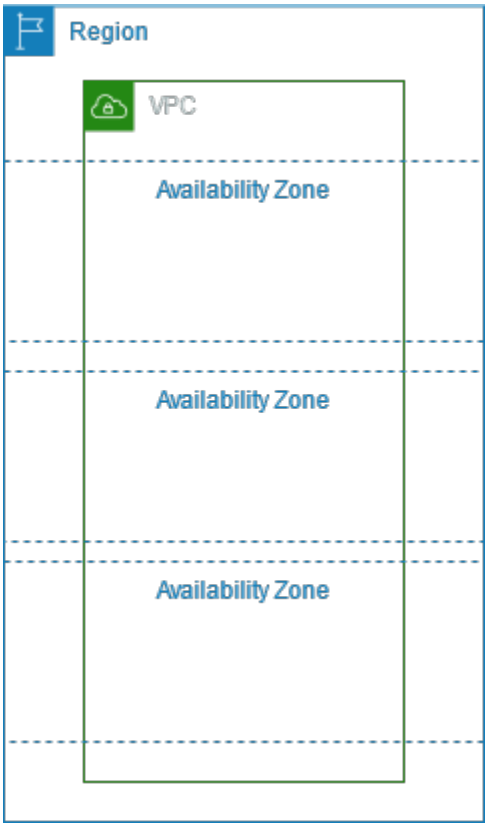
當您建立 VPC 時，您可按照下列方式指定其 IP 地址：

- 僅 IPv4 – VPC 具有 IPv4 CIDR 區塊，但沒有 IPv6 CIDR 區塊。
- 雙堆疊 – VPC 具有 IPv4 CIDR 區塊和 IPv6 CIDR 區塊。

如需詳細資訊，請參閱您 VPC 和子網路的 IP 定址。

VPC 圖表

下圖顯示沒有任何其他 VPC 資源的 VPC。如需範例 VPC 組態，請參閱範例。



VPC 資源

每個 VPC 都會自動提供下列資源：

- 預設 DHCP 選項集
- 預設網路 ACL
- 預設安全群組
- 主路由表

您可以為您的 VPC 建立下列資源：

- 網路 ACL
- 自訂路由表
- 安全群組
- 網際網路閘道
- NAT 閘道

VPC 組態選項

您可以在建立 VPC 時指定下列組態選項。

可用區域

在 AWS 區域中具有備援電源、聯網和連線能力的獨立資料中心。您可以使用多個 AZ 來操作生產應用程式和資料庫，相較於單一資料中心，其可用性、容錯能力和可擴展性更高。如果跨可用區域對執行於子網路中的應用程式進行分區，可以更完善地隔離和保護其免受停電、雷擊、龍捲風和地震等問題的影響。

CIDR 區塊

您必須指定 VPC 和子網路的 IP 地址範圍。如需詳細資訊，請參閱您 VPC 和子網路的 IP 定址。

DNS 選項

如果您需要公有 IPv4 DNS 主機名稱以將 EC2 執行個體啟動到子網路中，則必須啟用這兩個 DNS 選項。如需詳細資訊，請參閱VPC 的 DNS 屬性。

- 啟用 DNS 主機名稱：在 VPC 中啟動的 EC2 執行個體會接收與其公有 IPv4 地址相對應的公有 DNS 主機名稱。
- 啟用 DNS 解析：私有 DNS 主機名稱的 DNS 解析是由 Amazon DNS 伺服器 (稱為 Route 53 Resolver) 提供給 VPC 的 DNS 解析。

網際網路閘道

將您的 VPC 連線至網際網路。公有子網路中的執行個體可以存取網際網路，因為子網路路由表包含一個路由，能將目標為網際網路的流量傳送至網際網路閘道。如果伺服器不需要直接從網際網路連線，則不應將其部署到公有子網路中。如需詳細資訊，請參閱網際網路閘道。

名稱

系統會使用您為 VPC 和其他 VPC 資源指定的名稱來建立「名稱」標籤。如果您使用主控台中的名稱標籤自動產生功能，則標籤值會具有「*##-##*」的格式。

NAT 閘道

讓私有子網路中的執行個體能夠將傳出流量傳送至網際網路，但阻止網際網路上的資源連線至執行個體。在生產環境中，建議您在每個作用中 AZ 中部署 NAT 閘道。如需更多詳細資訊，請參閱 NAT 閘道。

路由表

包含一組名為路由的規則，可判斷來自子網或閘道之網路流量的方向。如需詳細資訊，請參閱路由表。

子網路

您 VPC 中的 IP 地址範圍。您可以在子網路中啟動 AWS 資源，例如 EC2 執行個體。每個子網路都完全位於一個可用區域內。藉由在至少兩個可用區域中啟動執行個體，您可以保護應用程式免於發生單一可用區域故障。

公有子網路會直接路由到網際網路閘道。公有子網路中的資源可以存取公有網際網路。私有子網路不會直接路由至網際網路閘道。私有子網路中的資源需要另一個元件 (例如 NAT 裝置)，才能存取公有網際網路。

如需詳細資訊，請參閱子網路。

租用

此選項會定義啟動至 VPC 的 EC2 執行個體，是否會在與其他 AWS 帳戶 共用的硬體上執行，或是在僅供您使用的硬體上執行。如果您選擇 VPC 的租用為 `Default`，則啟動至此 VPC 的 EC2 執行個體，將使用啟動執行個體時指定的租用屬性。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用定義的參數啟動執行個體。如果您選擇 VPC 的租用為 `Dedicated`，則執行個體將會一律以硬體上之專用預留執行個體 (專供您使用) 的形式執行。如果您使用的是 AWS Outpost，您的 Outpost 需要私有連線；您必須使用`Default`租用。

預設 VPC

當您開始使用 Amazon VPC 時，每個 AWS 區域都有一個預設 VPC。預設 VPC 在每個可用區域附帶一個公有子網路、一個網際網路閘道，以及啟用 DNS 解析的設定。因此，您可以在預設 VPC 中立即開始啟動 Amazon EC2 執行個體。您也可以在預設 VPC 中使用 Elastic Load Balancing、Amazon RDS 和 Amazon EMR 等服務。

預設 VPC 適合快速入門，也適合啟動公有執行個體，例如部落格或簡易的網站。您可視需要修改您預設 VPC 的元件。

您可以將子網路新增至預設 VPC。如需詳細資訊，請參閱the section called “建立子網”。

目錄

- 預設 VPC 元件

- 預設子網路
- 使用預設 VPC 和預設子網路

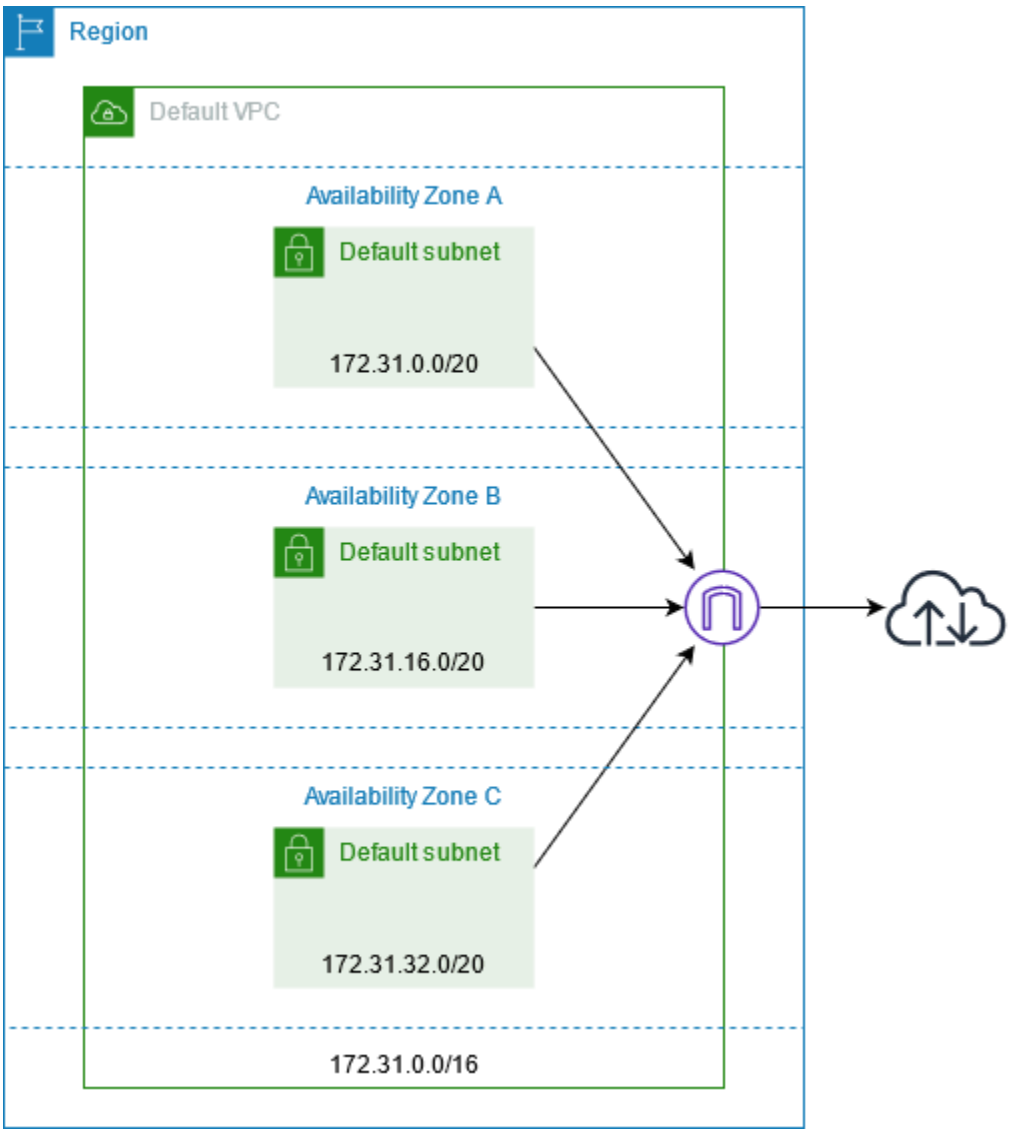
預設 VPC 元件

當我們建立預設的 VPC 時，我們會為您執行下列作業來設定它：

- 建立大小為 /16 IPv4 CIDR 區塊 (172.31.0.0/16) 的 VPC。這最多可提供 65,536 個私有 IPv4 地址。
- 在每個可用區域中建立大小為 /20 的預設子網路。每個子網路最多可提供 4,096 個地址，其中一些預留供我們使用。
- 建立網際網路閘道，並將它連線到您的預設 VPC。
- 將路由新增至主路由表，將所有流量 (0.0.0.0/0) 指向網際網路閘道。
- 建立預設的安全群組，並與您預設的 VPC 建立關聯。
- 建立預設的網路存取控制清單 (ACL)，並與您預設的 VPC 建立關聯。
- 將 AWS 為您的帳戶設定的預設 DHCP 選項與預設 VPC 建立關聯。

> **Note**
>
> - Amazon 代表您建立上述資源。IAM 政策不適用於這些動作，因為您不執行這些動作。例如，如果您的 IAM 政策拒絕呼叫 CreateInternetGateway 的能力，然後您呼叫了 CreateDefaultVpc，則仍會在預設的 VPC 中建立網際網路閘道。若要防止 Amazon 建立網際網路閘道，您必須拒絕 CreateDefaultVpc 和 CreateInternetGateway。
> - 若要封鎖您帳戶中網際網路閘道的所有往返流量，請參閱 封鎖對 VPC 和子網路的公開存取。

下圖顯示我們為預設 VPC 設定的主要元件。



下表顯示預設 VPC 主路由表中的路由。

目標	目標
172.31.0.0/16	區域
0.0.0.0/0	*internet_gateway_id*

使用預設 VPC 的方法和使用任何其他 VPC 一樣：

- 新增其他非預設的子網路。
- 修改主路由表。

- 新增其他路由表。
- 建立其他安全群組的關聯。
- 更新預設安全群組的規則。
- 新增 AWS Site-to-Site VPN 連線。
- 新增更多 IPv4 CIDR 區塊。
- 使用 Direct Connect 閘道存取遠端區域中的 VPC。如需 Direct Connect 閘道選項的資訊，請參閱《AWS Direct Connect 使用者指南》中的 Direct Connect 閘道。

您可如同使用任何其他子網路來使用預設的子網路；新增自訂路由表以及設定網路 ACL。您也可以在啟動 EC2 執行個體時，指定特定的預設子網路。

您可以選擇性建立 IPv6 CIDR 區塊與您預設 VPC 的關聯。

預設子網路

根據預設，預設子網路是公有子網路，因為主路由表會將以網際網路為目標的子網路流量傳送至網際網路閘道。您可將路由從目標 0.0.0.0/0 移至網際網路閘道，將預設子網路變成私有子網路。但若如此做，在該子網路中執行的任何 EC2 執行個體都無法存取網際網路。

您在預設子網路中啟動的執行個體會收到公有和私有 IPv4 地址及公有和私有 DNS 主機名稱。您在預設 VPC 之非預設子網路中啟動的執行個體不會收到公有 IPv4 地址或 DNS 主機名稱。您可以變更您子網路的預設公有 IP 定址行為。如需詳細資訊，請參閱修改子網路的公有 IP 位址屬性。

有時， AWS 可能會將新的可用區域新增至區域。在多數的情況下，我們會在幾天內自動於您預設 VPC 的這個可用區域中，建立新的預設子網路。但您若修改了預設的 VPC，我們就不會新增新的預設子網路。如果您希望新的可用區域中有預設的子網路，您可自行建立。如需詳細資訊，請參閱建立預設子網路。

使用預設 VPC 和預設子網路

本節說明如何使用預設 VPC 和預設子網路。

目錄

- 檢視您的預設 VPC 和預設子網路
- 建立預設 VPC
- 建立預設子網路
- 刪除您的預設子網路和預設 VPC

檢視您的預設 VPC 和預設子網路

您可以使用 Amazon VPC 主控台或命令列來檢視您的預設 VPC 和子網路。

使用 主控台檢視您的預設 VPC 和子網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 在 Default VPC (預設 VPC) 欄中，尋找 Yes (是) 的值。記下預設 VPC 的 ID。
4. 在導覽窗格中，選擇 Subnets (子網路)。
5. 在搜尋列中，輸入預設 VPC 的 ID。傳回的子網路是您預設 VPC 中的子網路。
6. 若要驗證哪些子網路是預設子網路，請在 Default Subnet (預設子網路) 欄中尋找 Yes (是) 的值。

使用命令列說明您的預設 VPC

- 使用 describe-vpcs (AWS CLI)
- 使用 Get-EC2Vpc (AWS Tools for Windows PowerShell)

使用具有 `isDefault` 篩選條件的命令，並將篩選條件值設為 `true`。

使用命令列說明您的預設子網路

- 使用 describe-subnets (AWS CLI)
- 使用 Get-EC2Subnet (AWS Tools for Windows PowerShell)

使用具有 `vpc-id` 篩選條件的命令，並將篩選條件值設為預設 VPC 的 ID。在輸出中，預設子網路的 `DefaultForAz` 欄位設為 `true`。

建立預設 VPC

如果您刪除預設的 VPC，您可以再建立一個新的。您無法還原已刪除的上一個預設 VPC，而且您無法將現有的非預設 VPC 標記為預設 VPC。

當您建立預設的 VPC 時，它是使用預設 VPC 的標準元件建立，包括每個可用區域中的預設子網路。您無法指定自己的元件。您新預設 VPC 的子網路 CIDR 區塊，可能不會映射到和上一個預設 VPC 相同的可用區域。例如，如果具有 CIDR 區塊 `172.31.0.0/20` 的子網路是建立在您上一個預設 VPC 的 `us-east-2a` 中，它就可以建立在您新預設 VPC 的 `us-east-2b`。

如果您在區域中已有預設的 VPC，即無法再建立另一個。

使用 主控台建立預設 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選擇 Actions (動作)、Create Default VPC (建立預設 VPC)。
4. 選擇 Create (建立)。關閉確認畫面。

使用命令列建立預設 VPC

您可以使用 create-default-vpc AWS CLI 命令。這個命令沒有任何輸入參數。

```
aws ec2 create-default-vpc
```

下列為範例輸出。

```
{
    "Vpc": {
        "VpcId": "vpc-3f139646",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

或者，您也可以使用 New-EC2DefaultVpc Tools for Windows PowerShell 命令或 CreateDefaultVpc Amazon EC2 API 動作。

建立預設子網路

> **Note**
>
> 您無法使用 AWS 管理主控台建立預設子網路。

您可以在沒有預設子網的可用區域中建立預設子網。例如，如果您已刪除預設子網路，或 AWS 已新增新的可用區域，但未在預設 VPC 中自動為該區域建立預設子網路，則建議您建立預設子網路。

當您建立預設的子網路時，它是在您預設 VPC 的下一個可用連續空間中，使用大小 /20 的 IPv4 CIDR 區塊建立。適用的規定如下：

- 您不能自行指定 CIDR 區塊。
- 您無法還原您刪除的上一個預設子網路。
- 每個可用區域只能有一個預設子網路。
- 您不能在非預設 VPC 中建立預設子網路。

如果您的預設 VPC 中地址空間不足而無法建立大小 /20 的 CIDR 區塊，請求即失敗。如果您需要更多的地址空間，您可在您的 VPC 中新增 IPv4 CIDR 區塊。

如果您已建立 IPv6 CIDR 區塊與您預設 VPC 的關聯，新的預設子網路就不會自動收到 IPv6 CIDR 區塊。但您可以在建立它之後，建立 IPv6 CIDR 區塊與預設子網路的關聯。如需詳細資訊，請參閱從您的子網路中新增或移除 IPv6 CIDR 區塊。

使用 建立預設子網路 AWS CLI

使用 create-default-subnet AWS CLI 命令，並指定要在其中建立子網路的可用區域。

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

以下為範例輸出。

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
```

```
    }
}
```

如需設定 的詳細資訊 AWS CLI，請參閱 AWS Command Line Interface 使用者指南。

或者，您可以使用 New-EC2DefaultSubnet Tools for Windows PowerShell 命令或 CreateDefaultSubnet Amazon EC2 API 動作。

刪除您的預設子網路和預設 VPC

您可以如同刪除任何其他子網路或 VPC 來刪除預設的子網路或預設的 VPC。不過，如果您刪除預設子網路或預設 VPC，您就必須在啟動執行個體時在其中一個 VPC 中明確指定子網路。如果您沒有其他 VPC，您就至少必須在一個可用區域中建立具有子網路的 VPC。如需詳細資訊，請參閱建立 VPC。

如果您刪除預設的 VPC，您可以再建立一個新的。如需更多詳細資訊，請參閱 建立預設 VPC。

如果您刪除預設的子網路，您可以再建立一個新的。如需詳細資訊，請參閱建立預設子網路。為確保您的新預設子網路能如預期運作，請修改子網路屬性以將公有 IP 地址指派給在該子網路中啟動的執行個體。如需更多詳細資訊，請參閱 修改子網路的公有 IP 位址屬性。每個可用區域只能有一個預設子網路。您不能在非預設 VPC 中建立預設子網路。

建立 VPC

使用下列程序建立虛擬私有雲端 (VPC)。VPC 必須具有其他資源 (例如子網路、路由表和閘道)，才能在 VPC 中建立 AWS 資源。

目錄

- 建立 VPC 以及其他 VPC 資源
- 僅建立 VPC
- 使用 AWS CLI 建立 VPC

如需有關修改 VPC 的資訊，請參閱the section called “新增或移除 CIDR 區塊”。

建立 VPC 以及其他 VPC 資源

使用下列程序建立 VPC 以及執行應用程式所需的其他 VPC 資源，例如子網路、路由表、網際網路閘道和 NAT 閘道。如需範例 VPC 組態，請參閱範例。

如何使用主控台建立 VPC、子網路和其他 VPC 資源

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 保持選取 自動產生名稱標籤 以建立 VPC 資源的「名稱」標籤，或將其清除以提供您自己的 VPC 資源「名稱」標籤。
5. 在IPv4 CIDR 區塊，輸入 VPC 的 IPv4 地址範圍。VPC 必須具有 IPv4 地址範圍。
6. (選用) 若要支援 IPv6 流量，請選擇 IPv6 CIDR 區塊 > Amazon 提供的 IPv6 CIDR 區塊。
7. 選擇租用選項。此選項會定義啟動至 VPC 的 EC2 執行個體，是否會在與其他 AWS 帳戶 共用的硬體上執行，或是在僅供您使用的硬體上執行。如果您選擇 VPC 的租用為 `Default`，則在此 VPC 中啟動的 EC2 執行個體將使用啟動執行個體時指定的租用屬性。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用定義參數啟動執行個體。如果您選擇 VPC 的租用為 `Dedicated`，則執行個體將會一律以硬體上之專用預留執行個體 (專供您使用) 的形式執行。如果您使用 AWS Outposts，則您的 Outpost 需要私人連線；您必須使用 `Default` 租用。
8. 對於可用區域 (AZ) 的數目，建議您至少在生產環境的兩個可用區域中佈建子網路。若要選擇子網路的 AZ，請展開自訂 AZ。否則，請讓 AWS 為您選擇設定。
9. 若要設定您的子網路，請選擇公有子網路數目和私有子網路數目的值。若要選擇子網路的 IP 地址範圍，請展開自訂子網路 CIDR 區塊。否則，請讓 AWS 為您選擇設定。
10. (選用) 如果私有子網路中的資源需要透過 IPv4 存取公有網際網路，請在 NAT 閘道選擇要在其中建立 NAT 閘道的 AZ 數目。在生產環境中，建議您在每個 AZ 中部署一個 NAT 閘道，並包含需要存取公有網際網路的資源。請注意，存在與 NAT 閘道關聯的成本。如需更多詳細資訊，請參閱 NAT 閘道的定價。
11. (選用) 如果私有子網路中的資源需要透過 IPv6 存取公用網際網路，請在僅限輸出的網際網路閘道選擇是。
12. (選用) 如果您需要直接從 VPC 存取 Amazon S3，請選擇 VPC 端點 > S3 閘道。這會為 Amazon S3 建立閘道 VPC 端點。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的閘道端點。
13. (選用) 在 DNS 選項，網域名稱解析的兩個選項都會依預設啟用。如果預設值不符合需求，您可以停用這些選項。
14. (選用) 若要將標籤新增至 VPC，請展開其他標籤，選擇新增標籤，然後輸入標籤金鑰和標籤值。
15. 在預覽窗格中，您可以透過視覺化方式掌握您已設定的 VPC 資源之間的關係。實線代表資源之間的關係。虛線代表 NAT 閘道、網際網路閘道和閘道端點的網路流量。建立 VPC 後，可以隨時使用資源映射索引標籤以此格式將 VPC 中的資源視覺化。如需更多詳細資訊，請參閱 視覺化 VPC 中的資源。

16. 當您完成設定 VPC 後，請選擇建立 VPC。

僅建立 VPC

使用下列程序透過 Amazon VPC 主控台建立不含任何其他 VPC 資源的 VPC。

如何使用主控台建立不含任何其他 VPC 資源的 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 在建立資源，選擇僅 VPC。
4. (選用) 在名稱標籤中，輸入您 VPC 的名稱。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。
5. 對於 IPv4 CIDR 區塊，執行下列其中一個動作：
   - 選擇 IPv4 CIDR 手動輸入，然後輸入 VPC 的 IPv4 地址範圍。
   - 選擇 IPAM 配置的 IPv4 CIDR 區塊，然後選取您的 Amazon IPAM VPC IP 地址管理員 (IPAM) IPv4 地址集區和網路遮罩。CIDR 區塊的大小會受 IPAM 集區上的分配規則所限制。IPAM 是一項 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控您 AWS 工作負載的 IP 地址。如需詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》。

     如果您是使用 IPAM 來管理 IP 地址，建議您選擇此選項。否則，您為 VPC 指定的 CIDR 區塊可能會與 IPAM CIDR 配置重疊。
6. (選用) 若要建立雙堆疊 VPC，請為您的 VPC 指定 IPv6 地址範圍。對於 IPv6 CIDR 區塊，執行下列其中一個動作：

   - 如果您使用 Amazon VPC IP Address Manager，並且想從 IPAM 集區佈建 IPv6 CIDR，選擇 IPAM-allocated IPv6 CIDR block (IPAM 配置的 IPv6 CIDR 區塊)。如果使用 IPAM 配置的 IPv6 CIDR 區塊將 IPv6 CIDR 佈建至 VPC，您能取得連續在 VPC 中建立 IPv6 CIDR 帶來的優勢。連續配置的 CIDR 即為依序配置的 CIDR。這些 CIDR 讓您能夠簡化安全與網路規則；IPv6 CIDR 可以彙總在網路與安全建構模組 (例如存取控制清單、路由表、安全群組與防火牆) 之間的單一項目中。

     CIDR block (CIDR 區塊) 下提供兩個用於將 IP 地址範圍佈建至 VPC 的選項：

     - Netmask length (網路遮罩長度)：選擇此選項可為 CIDR 選取網路遮罩長度。執行以下任意一項：

- 如果已為 IPAM 集區選取預設網路遮罩長度，您可以選擇 Default to IPAM netmask length (預設為 IPAM 網路遮罩長度)，以使用 IPAM 管理員為 IPAM 集區設定的預設網路遮罩長度。如需有關可選預設網路遮罩長度配置規則的詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的建立區域 IPv6 集區。
- 如果沒有為 IPAM 集區選取預設網路遮罩長度，則選擇比 IPAM 集區 CIDR 網路遮罩長度更為具體的網路遮罩長度。例如，如果 IPAM 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。

- Select a CIDR (選取 CIDR)：選擇此選項可手動輸入 IPv6 地址。只能選擇比 IPAM 集區 CIDR 的網路遮罩長度更具體的網路遮罩長度。例如，如果 IPAM 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。

- 選擇 Amazon 提供的 IPv6 CIDR 區塊，向 Amazon 的 IPv6 地址集區請求 IPv6 CIDR 區塊。在 Network Border Group (網路邊界群組) 欄位中，請選取 AWS 在其中公告 IP 地址的群組。Amazon 所提供 IPv6 CIDR 區塊的固定大小為 /56。
- 選擇 IPv6 CIDR owned by me (我擁有的 IPv6 CIDR)，佈建已帶入 AWS 的 IPv6 CIDR。如需自備 IP 位址範圍至 AWS 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 中的自備 IP 位址 (BYOIP)。您可以使用 CIDR 區塊 的下列選項來佈建 VPC 的 IP 位址範圍：
  - No preference (無偏好設定)：選擇此選項可使用網路遮罩長度 /56。
  - Select a CIDR (選取 CIDR)：選擇此選項可手動輸入 IPv6 地址，並選擇比 BYOIP CIDR 規模更具體的網路遮罩長度。例如，如果 BYOIP 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。

7. (選用) 選擇租用選項。此選項會定義啟動至 VPC 的 EC2 執行個體，是否會在與其他 AWS 帳戶共用的硬體上執行，或是在僅供您使用的硬體上執行。如果您選擇 VPC 的租用為 `Default`，則啟動至此 VPC 的 EC2 執行個體，將使用啟動執行個體時指定的租用屬性。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用定義的參數啟動執行個體。如果您選擇 VPC 的租用為 `Dedicated`，則執行個體將會一律以硬體上之專用預留執行個體 (專供您使用) 的形式執行。如果您使用 AWS Outposts，則您的 Outpost 需要私人連線；您必須使用 `Default` 租用。
8. (選用) 若要將標籤新增至 VPC，請選擇新增標籤，然後輸入標籤金鑰和標籤值。
9. 選擇建立 VPC。
10. 建立 VPC 後，您可以新增子網。如需更多詳細資訊，請參閱 建立子網。

使用 AWS CLI 建立 VPC

下列程序包含建立 VPC 的範例 AWS CLI 命令，以及執行應用程式所需的其他 VPC 資源。如果您執行此程序中的所有命令，您將會建立 VPC、公有子網路、私有子網路、每個子網路的路由表、網際網路閘道、僅限輸出的網際網路閘道，以及公有 NAT 閘道。如果您不需要所有這些資源，可以只使用您所需的範例命令。

必要條件

開始之前，請先安裝並設定 AWS CLI。設定 AWS CLI 時，系統會提示您輸入 AWS 登入資料。本程序中的範例假設您也設定了預設「區域」。否則，請將 `--region` 選項新增至每個命令。如需詳細資訊，請參閱安裝或更新 AWS CLI 和設定 AWS CLI。

標記

您可以在使用 create-tags 命令建立資源後，將標籤新增至資源。或者，您也可以如下所示將 `--tag-specification` 選項新增至資源的建立命令。

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

使用 AWS CLI 建立 VPC 與 VPC 資源

1. 使用下列 create-vpc 命令，以建立具有指定 IPv4 CIDR 區塊的 VPC。

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   或者，若要建立雙堆疊 VPC，請新增 `--amazon-provided-ipv6-cidr-block` 選項以新增 Amazon 提供的 IPv6 CIDR 區塊，如下列範例所示。

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

   這些命令會傳回新 VPC 的 ID。以下是範例。

   ```
   vpc-1a2b3c4d5e6f1a2b3
   ```

2. [雙堆疊 VPC] 使用下列 describe-vpcs 命令，取得已與您 VPC 建立關聯的 IPv6 CIDR 區塊。

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
```

下列為範例輸出。

```
2600:1f13:cfe:3600::/56
```

3. 視您的使用案例而定，可建立一或多個子網路。在生產環境中，建議您至少在兩個可用區域中啟動資源。使用下列其中一個命令來建立各個子網路。

   - 僅限 IPv4 子網路 – 若要建立具有特定 IPv4 CIDR 區塊的子網路，請使用下列 create-subnet 命令。

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
      --availability-zone us-east-2a --query Subnet.SubnetId --output text
     ```

   - 雙堆疊子網路 – 如果您建立了雙堆疊 VPC，您可以使用 `--ipv6-cidr-block` 選項來建立雙堆疊子網路，如下列命令所示。

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
      --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
     query Subnet.SubnetId --output text
     ```

   - 僅限 IPv6 子網路 – 如果您建立了雙堆疊 VPC，您可以使用 `--ipv6-native` 選項來建立僅限 IPv6子網路，如下列命令所示。

     ```
     aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
     cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
      Subnet.SubnetId --output text
     ```

   這些命令會傳回新子網路的 ID。以下是範例。

   ```
   subnet-1a2b3c4d5e6f1a2b3
   ```

4. 如果您的 Web 伺服器或 NAT 閘道需要公有子網路，請執行下列動作：

   a. 使用下列 create-internet-gateway 命令，建立網際網路閘道。該命令會傳回新網際網路閘道的 ID。

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
output text
```

b. 使用下列 attach-internet-gateway 命令，將網際網路閘道連接至您的 VPC。使用上一個步驟傳回的網際網路閘道 ID。

```
aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
gateway-id igw-id
```

c. 使用下列 create-route-table 命令，建立公有子網路的自訂路由表。該命令會傳回新路由表的 ID。

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. 使用下列 create-route 命令，在將所有 IPv4 流量傳送至網際網路閘道的路由表中建立路由。使用公有子網路的路由表 ID。

```
aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-id
```

e. 使用下列 associate-route-table 命令，將路由表與公有子網路建立關聯。使用公有子網路的路由表 ID 以及公有子網路的 ID。

```
aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
id subnet-id-public-subnet
```

5. [IPv6] 您可以新增輸出限定網際網路閘道，讓私有子網路中的執行個體可以透過 IPv6 存取網際網路 (例如用於取得軟體更新)，但網際網路上的主機無法存取您的執行個體。

a. 使用下列 create-egress-only-internet-gateway 命令，建立輸出限定網際網路閘道。該命令會傳回新網際網路閘道的 ID。

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
```

b. 使用下列 create-route-table 命令，建立私有子網路的自訂路由表。該命令會傳回新路由表的 ID。

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

c. 使用下列 create-route 命令，在將所有 IPv6 流量傳送至輸出限定網際網路閘道的私有子網路的路由表中建立路由。使用上一個步驟傳回的路由表 ID。

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block ::/0 --egress-only-internet-gateway eigw-id
```

d. 使用下列 associate-route-table 命令，將路由表與私有子網路建立關聯。

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

6. 如果私有子網路中的資源需要 NAT 閘道，請執行下列動作：

a. 使用下列 allocate-address 命令，建立 NAT 閘道的彈性 IP 地址。

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text
```

b. 使用下列 create-nat-gateway 命令，在公開子網路中建立 NAT 閘道。使用上一個步驟傳回的配置 ID。

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (選用) 如果您已在步驟 5 中建立私有子網路的路由表，請略過此步驟。否則，請使用下列 create-route-table 命令，建立私有子網路的路由表 該命令會傳回新路由表的 ID。

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. 使用下列 create-route 命令，在將所有 IPv4 流量傳送至 NAT 閘道之私有子網路的路由表中建立路由。使用您在此步驟或步驟 5 中建立的私有子網路的路由表 ID。

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (選用) 如果您已在步驟 5 中將路由表與私有子網路建立關聯，請略過此步驟。否則，請使用下列 associate-route-table 命令，將路由表與私有子網路建立關聯。使用您在此步驟或步驟 5 中建立的私有子網路的路由表 ID。

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

視覺化 VPC 中的資源

本節說明如何使用資源 地圖 索引標籤查看您 VPC 中資源的視覺化呈現。下列資源會顯示在資源映射中：

- VPC
- 子網路
  - 可用區域以字母表示。
  - 公有子網路顯示為綠色。
  - 私有子網路顯示為藍色。
- 路由表
- 網際網路閘道
- 輸出限定網際網路閘道
- NAT 閘道
- 閘道端點 (Amazon S3 和 Amazon DynamoDB)

資源映射顯示 VPC 內部資源之間的關係，以及流量如何從子網路流向 NAT 閘道、網際網路閘道和閘道端點。

可以使用資源映射來了解 VPC 的架構、查看其中有多少個子網路、哪些子網路與哪些路由表相關聯，以及哪些路由表具有通往 NAT 閘道、網際網路閘道和閘道端點的路由。

也可以使用資源映射來發現不需要或不正確的組態，例如從 NAT 閘道中斷連接的私有子網路，或直接路由到網際網路閘道的私有子網路。可以選擇資源映射中的資源，例如路由表，然後編輯這些資源的組態。

視覺化 VPC 中的資源

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 VPCs (VPC)。
3. 選取 VPC。
4. 選擇資源映射標籤以顯示資源的視覺效果。
5. 選擇顯示詳細資訊，以檢視除了預設顯示的資源 ID 和區域以外的其他詳細資訊。
   - VPC：指派給 VPC 的 IPv4 和 IPv6 CIDR 範圍。
   - 子網路：指派給每個子網路的 IPv4 和 IPv6 CIDR 範圍。
   - 路由表：子網路關聯和路由表中的路由數目。
   - 網路連線：與每種連線類型相關的詳細資訊：
     - 如果 VPC 中有公有子網路，則會有網際網路閘道資源，其中包含使用該網際網路閘道之流量的路由數目以及來源和目的地子網路。
     - 如果有輸出限定網際網路閘道，則會有輸出限定網際網路閘道資源，其中包含使用該輸出限定網際網路閘道之流量的路由數目以及來源和目標子網路。
     - 如果有 NAT 閘道，則會有 NAT 閘道資源，其中包含 NAT 閘道的網路介面數目和彈性 IP 地址。
     - 如果有閘道端點，則會有閘道端點資源，其中包含您使用該端點相連之 AWS 服務的名稱 (Amazon S3 或 Amazon DynamoDB)。
6. 將滑鼠游標暫留在資源上可查看資源之間的關係。實線代表資源之間的關係。虛線代表網路連接的網路流量。

從您的 VPC 中新增或移除 CIDR 區塊

本節說明如何從 VPC 新增或移除 IPv4 和 IPv6 CIDR 區塊。

Important

- 依預設，您的 VPC 最多可以有五個 IPv4 和五個 IPv6 CIDR 區塊，但此限制可調整。如需更多詳細資訊，請參閱 Amazon VPC 配額。如需 VPC 的 CIDR 區塊限制的相關資訊，請參閱VPC CIDR 區塊。

- 若您的 VPC 有超過一個相關聯的 IPv4 CIDR 區塊，您可以從 VPC 中移除 IPv4 CIDR 區塊。您無法移除主要 IPv4 CIDR 區塊。您只能移除整個 CIDR 區塊；您無法移除某個 CIDR 區塊子集或合併的 CIDR 區塊範圍。您必須先刪除 CIDR 區塊中的所有子網。
- 若您不再希望您的 VPC 支援 IPv6，但您想要繼續使用您的 VPC 建立 IPv4 資源並與之通訊，您可以移除 IPv6 CIDR 區塊。
- 若要移除 IPv6 CIDR 區塊，您必須先取消指派任何已指派給您子網路中任何執行個體的 IPv6 地址。
- 移除 IPv6 CIDR 區塊不會自動刪除任何安全群組規則、網路 ACL 規則，或是您已為 IPv6 聯網設定的路由表路由。您必須手動修改或刪除這些規則或路由。

使用主控台在 VPC 中新增或移除 CIDR 區塊

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 若要移除 CIDR，請選擇 CIDR 旁邊的 移除。
5. 若要新增 CIDR，請選擇 新增 IPv4 CIDR 或 新增 IPv6 CIDR。
6. 若要新增 CIDR，對於 IPv4 CIDR 區塊，請執行下列其中一個動作：
   - 選擇 IPv4 CIDR manual input (IPv4 CIDR 手動輸入)，然後輸入 IPv4 CIDR 區塊。
   - 選擇 IPAM-allocated IPv4 CIDR (IPAM 指派的 IPv4 CIDR)，然後從 IPv4 IPAM 集區中選取一個 CIDR。
   - 選擇儲存。
7. 若要新增 CIDR，對於 IPv6 CIDR 區塊，請執行下列動作：
   - 如果您使用 Amazon VPC IP Address Manager，並且想從 IPAM 集區佈建 IPv6 CIDR，選擇 IPAM-allocated IPv6 CIDR block (IPAM 配置的 IPv6 CIDR 區塊)。CIDR block (CIDR 區塊) 下提供兩個用於將 IP 地址範圍佈建至 VPC 的選項：
     - Netmask length (網路遮罩長度)：選擇此選項可為 CIDR 選取網路遮罩長度。執行以下任意一項：
       - 如果已為 IPAM 集區選取預設網路遮罩長度，您可以選擇 Default to IPAM netmask length (預設為 IPAM 網路遮罩長度)，以使用 IPAM 管理員為 IPAM 集區設定的預設網路遮罩長度。如需有關可選預設網路遮罩長度配置規則的詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的建立區域 IPv6 集區。

- 如果沒有為 IPAM 集區選取預設網路遮罩長度，則選擇比 IPAM 集區 CIDR 網路遮罩長度更為具體的網路遮罩長度。例如，如果 IPAM 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。
- Select a CIDR (選取 CIDR)：選擇此選項可手動輸入 IPv6 地址。只能選擇比 IPAM 集區 CIDR 的網路遮罩長度更具體的網路遮罩長度。例如，如果 IPAM 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。

- 選擇 Amazon 提供的 IPv6 CIDR 區塊，向 Amazon 的 IPv6 地址集區請求 IPv6 CIDR 區塊。在 Network Border Group (網路邊界群組) 欄位中，請選取 AWS 在其中公告 IP 地址的群組。Amazon 所提供 IPv6 CIDR 區塊的固定大小為 /56。
- 選擇 IPv6 CIDR owned by me (我擁有的 IPv6 CIDR)，佈建已帶入 AWS 的 IPv6 CIDR。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的將自有 IP 位址 (BYOIP) 用於 Amazon EC2。CIDR block (CIDR 區塊) 下提供兩個用於將 IP 地址範圍佈建至 VPC 的選項：
  - No preference (無偏好設定)：選擇此選項可使用網路遮罩長度 /56。
  - Select a CIDR (選取 CIDR)：選擇此選項可手動輸入 IPv6 地址，並選擇比 BYOIP CIDR 規模更具體的網路遮罩長度。例如，如果 BYOIP 集區 CIDR 是 /50，您可以為 VPC 選擇介於 /52 至 /60 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /60 之間 (增量為 /4)。
  - 完成後，請選擇 選取 CIDR。

8. 選擇關閉。
9. 如果將 CIDR 區塊新增至 VPC 後，您可以建立使用全新 CIDR 區塊的子網路。如需更多詳細資訊，請參閱 建立子網。

如何使用 AWS CLI 建立或取消 IPv4 CIDR 區塊與 VPC 的關聯

使用 associate-vpc-cidr-block 和 disassociate-vpc-cidr-block 命令。

Amazon VPC 中的 DHCP 選項集

VPC 中的網路裝置使用動態主機組態協定 (DHCP)。您可以使用 DHCP 選項集來控制虛擬網路中網路組態的以下部分：

- VPC 中裝置所使用的 DNS 伺服器、網域名稱或網路時間通訊協定 (NTP) 伺服器。
- VPC 中是否已啟用 DNS 解析。

目錄

- 什麼是 DHCP？
- DHCP 選項集概念
- 使用 DHCP 選項集

什麼是 DHCP？

TCP/IP 網路上的每個裝置均需要 IP 地址，才能透過網路進行通訊。過去，IP 地址必須手動指派給網路中的每個裝置。如今，使用動態主機組態協定 (DHCP) 的 DHCP 伺服器會動態指派 IP 地址。

EC2 執行個體上執行的應用程式可以根據需要與 Amazon DHCP 伺服器進行通訊，以擷取其 IP 地址租用或其他網路組態資訊 (例如 Amazon DNS 伺服器的 IP 地址或 VPC 中路由器的 IP 地址)。

您可以使用 DHCP 選項集指定由 Amazon DHCP 伺服器提供的網路組態。

如果您的 VPC 組態要求您的應用程式直接向 Amazon IPv6 DHCP 伺服器提出請求，則請注意以下事項：

- 雙堆疊子網路中的 EC2 執行個體只能從 IPv6 DHCP 伺服器中擷取其 IPv6 地址。無法從 IPv6 DHCP 伺服器中擷取任何其他網路組態，例如 DNS 伺服器名稱或網域名稱。
- 位於僅限 IPv6 之子網路中的 EC2 執行個體，可從 IPv6 DHCP 伺服器擷取其 IPv6 地址，還可以擷取其他聯網組態資訊，如 DNS 伺服器名稱和網域名稱。
- 對於僅 IPv6 子網路中的 EC2 執行個體，如果 DHCP 選項集中明確提及「AmazonProvidedDNS」，則 IPv4 DHCP 伺服器將傳回 169.254.169.253 做為名稱伺服器。如果選項集缺少「AmazonProvidedDNS」，無論選項集是否提及其他 IPv4 名稱伺服器，IPv4 DHCP 伺服器都不會傳回地址。

Amazon DHCP 伺服器還可以使用前綴委派向 VPC 中的網路介面提供完整的 IPv4 或 IPv6 前綴 (請參閱《Amazon EC2 使用者指南》中的為 Amazon EC2 網路介面指派字首)。DHCP 回應中不提供 IPv4 前綴委派。可以使用 IMDS 擷取指派給介面的 IPv4 前綴 (請參閱《Amazon EC2 使用者指南》中的執行個體中繼資料類別)。

DHCP 選項集概念

DHCP 選項集是 VPC 中的資源 (例如 EC2 執行個體) 用於透過虛擬網路進行通訊的一組網路設定。

每個區域都有預設 DHCP 選項集。每個 VPC 都會使用其區域的預設 DHCP 選項集，除非您建立自訂 DHCP 選項集並將其與 VPC 建立關聯，或設定沒有 DHCP 選項集的 VPC。

如果您的 VPC 未設定 DHCP 選項集：

- 對於建置在 Nitro System 上的 EC2 執行個體，會將 AWS 設定為169.254.169.253預設網域名稱伺服器。
- 對於建置在 Xen 上的 EC2 執行個體，並未設定網域名稱伺服器；而且由於 VPC 中的執行個體無法存取 DNS 伺服器，因此也無法存取網際網路。

您可以將一個 DHCP 選項集與多個 VPC 關聯，但每個 VPC 只能有一個關聯的 DHCP 選項集。

如果您刪除 VPC，則與該 VPC 相關聯的 DHCP 選項集會與 VPC 取消關聯。

目錄

- 預設 DHCP 選項集
- 自訂 DHCP 選項集

預設 DHCP 選項集

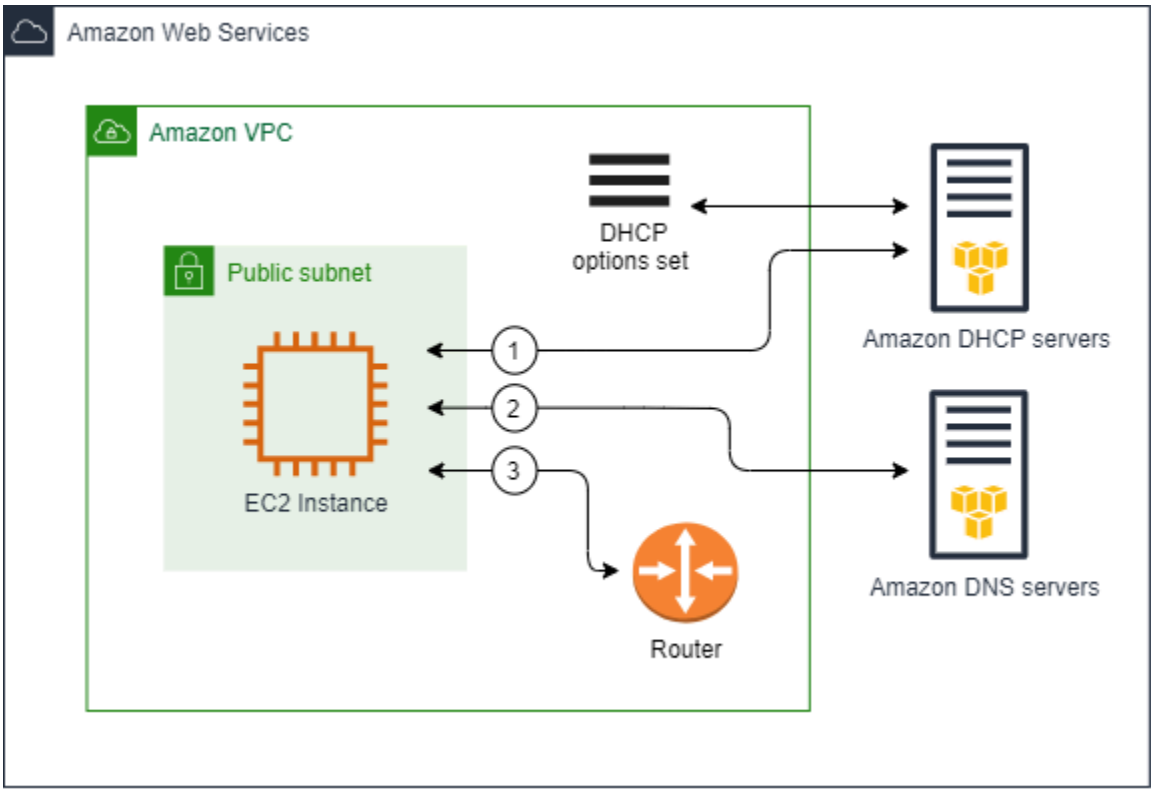
預設 DHCP 選項集包含以下設定：

- 網域名稱伺服器：您的網路介面將用於網域名稱解析的 DNS 名稱伺服器。對於預設 DHCP 選項集，這一律是 AmazonProvidedDNS。如需詳細資訊，請參閱Amazon DNS 伺服器。
- 網域名稱：用戶端在使用網域名稱系統 (DNS) 解析主機名稱時應使用的網域名稱。如需用於 EC2 執行個體使用之網域名稱的詳細資訊，請參閱 Amazon EC2 執行個體主機名稱。
- IPv6 偏好的租用時間：指派 IPv6 的執行中執行個體經過 DHCPv6 租賃續約的頻率。預設租賃時間為 140 秒。租賃續約通常發生在租賃時間已過一半時。

當您使用預設 DHCP 選項集時，將不會使用下列設定，但 EC2 執行個體有預設值：

- NTP 伺服器：EC2 執行個體預設會使用 Amazon Time Sync Service 來擷取時間。
- NetBIOS 名稱伺服器：對於執行 Windows 的 EC2 執行個體，NetBIOS 電腦名稱為指派給執行個體的易記名稱，用於在網路上識別該執行個體。對於使用 NetBIOS 作為其命名服務的網路，NetBIOS 名稱伺服器會維護 NetBIOS 電腦名稱和網路地址之間的映射清單。
- NetBIOS 節點類型：對於執行 Windows 的 EC2 執行個體，這是執行個體用於將 NetBIOS 名稱解析為 IP 地址的方法。

當您使用預設選項集時，Amazon DHCP 伺服器會使用預設選項集中的網路設定。當您在VPC 中啟動執行個體時，執行個體會執行以下操作，如圖所示：(1) 與 DHCP 伺服器互動，(2) 與 Amazon DNS 伺服器互動，以及 (3) 透過 VPC 的路由器連線至網路中的其他裝置。這些執行個體可以隨時與 Amazon DHCP 伺服器互動，以取得其 IP 地址租用及其他網路設定。



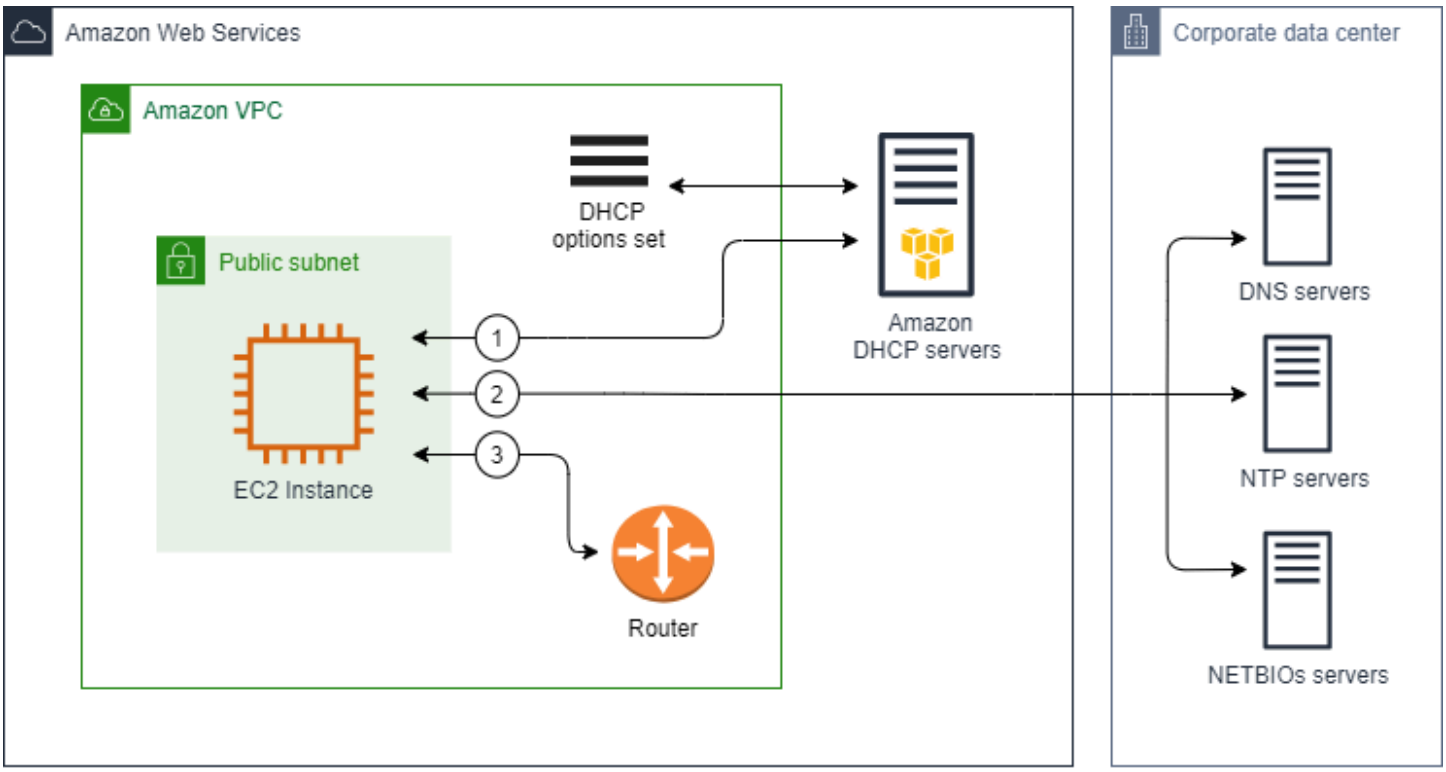
自訂 DHCP 選項集

您可以使用下列設定建立自訂 DHCP 選項集，然後將其與 VPC 建立關聯：

- 網域名稱伺服器：您的網路介面將用於網域名稱解析的 DNS 名稱伺服器。
- 網域名稱：用戶端在透過網域名稱系統 (DNS) 解析主機名稱時使用的網域名稱。
- NTP 伺服器：向執行個體提供時間的 NTP 伺服器。
- NetBIOS 名稱伺服器：對於執行 Windows 的 EC2 執行個體，NetBIOS 電腦名稱為指派給執行個體的易記名稱，用於在網路上識別該執行個體。對於使用 NetBIOS 作為其命名服務的網路，NetBIOS 名稱伺服器會維護 NetBIOS 電腦名稱和網路地址之間的映射清單。
- NetBIOS 節點類型：對於執行 Windows 的 EC2 執行個體，執行個體用於將 NetBIOS 名稱解析為 IP 地址的方法。
- IPv6 偏好的租賃時間 (選用)：指派 IPv6 的執行中執行個體經過 DHCPv6 租賃續約的頻率值 (以秒、分鐘、小時或年為單位)。可接受的值介於 140 和 4294967295 秒之間 (約 138 年)。如果未輸入任何

值，預設租賃時間會是 140 秒。如果您針對 EC2 執行個體使用長期定址，您可以增加租賃時間並避免頻繁的租賃續約請求。租賃續約通常發生在租賃時間已過一半時。

當您使用自訂選項集時，啟動至 VPC 中的執行個體將執行下列操作，如圖所示：(1) 使用自訂 DHCP 選項集中的網路設定，(2) 與自訂 DHCP 選項集中指定的 DNS、NTP 和 NetBIOS 伺服器互動，以及 (3) 透過 VPC 的路由器連線至網路中的其他裝置。



相關作業

- 建立 DHCP 選項集
- 變更與 VPC 關聯的選項集

使用 DHCP 選項集

使用下列程序來檢視並使用 DHCP 選項集。如需 DHCP 選項集如何運作的詳細資訊，請參閱 the section called “DHCP 選項集概念”。

任務

- 建立 DHCP 選項集
- 變更與 VPC 關聯的選項集

- 刪除 DHCP 選項集

建立 DHCP 選項集

自訂 DHCP 選項集可讓您使用自己的 DNS 伺服器、網域名稱等來自訂 VPC。您可以任意建立額外的 DHCP 選項集。但是，您一次只能將一個 DHCP 選項集與 VPC 建立關聯。

> **Note**
>
> 建立 DHCP 選項集之後，便無法再進行修改。若要更新 VPC 的 DHCP 選項，您必須建立新的 DHCP 選項集，然後將其與您的 VPC 建立關聯。

使用控制台建立 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP option sets (DHCP 選項集)。
3. 選擇 Create DHCP options set (建立 DHCP 選項集)。
4. 在 Tag settings (標籤設定) 中，可選擇是否輸入 DHCP 選項集的名稱。如果輸入值，則會自動建立 DHCP 選項集的名稱標籤。
5. 在選項中，請提供您需要的組態設定。

   - 網域名稱 (選用)：輸入用戶端在透過 DNS 解析主機名稱時應使用的網域名稱。如果您未使用 AmazonProvidedDNS，自訂網域名稱伺服器就必須視需要解析主機名稱。如果您使用 Amazon Route 53 私有託管區域，則可以使用 AmazonProvidedDNS。如需更多詳細資訊，請參閱 VPC 的 DNS 屬性。

     > **Note**
     >
     > 僅使用您完全掌控的網域名稱。

     部分 Linux 作業系統接受多個網域名稱，以空格分隔。但是，Windows 和其他 Linux 作業系統將值視為單一網域，將導致意外行為發生。如果您 的DHCP 選項集與 VPC 相關聯，該 VPC 的執行個體運做的作業系統將該值視為單個網域，請僅指定一個網域名稱。
   - Domain name servers (網域名稱伺服器) (選用)：輸入會用於透過主機名稱解析主機 IP 地址的 DNS 伺服器。

您可以輸入 **AmazonProvidedDNS** 或自訂網域名稱伺服器。兩者同時使用可能會導致非預期的行為。您可以輸入最多四個 IPv4 網域名稱伺服器的 IP 地址 (或最多三個 IPv4 網域名稱伺服器和 **AmazonProvidedDNS**) 以及四個以逗號分隔的 IPv6 網域名稱伺服器。您雖然可以指定最多八個網域名稱伺服器，但某些作業系統可能會限制較低的數量。如需有關 AmazonProvidedDNS 和 Amazon DNS 伺服器的詳細資訊，請參閱 Amazon DNS 伺服器。

> **Important**
>
> 如果您的 VPC 具有網際網路閘道，請務必指定您自己的 DNS 伺服器或 Amazon DNS 伺服器 (AmazonProvidedDNS) 用於網域名稱伺服器值。否則，VPC 中的執行個體將無法存取 DNS，進而會停用網際網路存取。

- NTP servers (NTP 伺服器) (選用)：輸入最多八個網路時間通訊協定 (NTP) 伺服器的 IP 地址 (四個 IPv4 地址和四個 IPv6 地址)。

  NTP 伺服器向網路提供時間。您可以在 IPv4 地址 `169.254.169.123` 或 IPv6 地址 `fd00:ec2::123` 指定 Amazon Time Sync Service。執行個體預設會與 Amazon Time Sync Service 進行通訊。請注意，IPv6 地址只能在建置於 Nitro 系統的 EC2 執行個體上進行存取。

  如需有關 NTP 伺服器選項的詳細資訊，請參閱 RFC 2132。如需有關 Amazon Time Sync Service 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的設定執行個體的時間。

- NetBIOS name servers (NetBIOS 名稱伺服器) (選用)：輸入最多四個 NetBIOS 名稱伺服器的 IP 地址。

  對於執行 Windows OS 的 EC2 執行個體，NetBIOS 電腦名稱為指派給執行個體的易記名稱，用於在網路上識別該執行個體。對於使用 NetBIOS 作為其命名服務的網路，NetBIOS 名稱伺服器會維護 NetBIOS 電腦名稱和網路地址之間的映射清單。

- NetBIOS node type (NetBIOS 節點類型) (選用)：輸入 **1**、**2**、**4** 或 **8**。建議您指定 **2** (點對點或 P 節點)。目前不支援廣播和多點傳播。如需這些節點類型的詳細資訊，請參閱 RFC 2132 的第 8.7 節，以及 RFC1001 的第 10 節。

  對於執行 Windows OS 的 EC2 執行個體，這是執行個體用於將 NetBIOS 名稱解析為 IP 地址的方法。在預設選項集中，NetBIOS 節點類型沒有任何值。

- IPv6 偏好的租賃時間 (選用)：指派 IPv6 的執行中執行個體經過 DHCPv6 租賃續約的頻率值 (以秒、分鐘、小時或年為單位)。可接受的值介於 140 和 2147483647 秒之間 (約 68 年)。如果未輸入任何值，預設租賃時間會是 140 秒。如果您針對 EC2 執行個體使用長期定址，您可以增加租賃時間並避免頻繁的租賃續約請求。租賃續約通常發生在租賃時間已過一半時。

6. 新增 Tags (標籤)。
7. 選擇 Create DHCP options set (建立 DHCP 選項集)。請記下新 DHCP 選項集的名稱或 ID。
8. 若要將您的 VPC 設定為使用新選項集，請參閱 變更與 VPC 關聯的選項集。

使用命令列為您的 VPC 建立 DHCP 選項集

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

變更與 VPC 關聯的選項集

建立 DHCP 選項集後，您可以將其與一個或多個 VPC 建立關聯。您一次只能將一個 DHCP 選項集與 VPC 建立關聯。如果您未將 DHCP 選項集與 VPC 建立關聯，則會停用 VPC 中的網域名稱解析。

在您將新的 DHCP 選項集與 VPC 建立關聯時，任何現有執行個體以及您在 VPC 內啟動的所有新執行個體都會使用這些新選項。您不必重新開始或重新啟動執行個體。執行個體會自動在幾個小時內進行變更，這取決於執行個體更新其 DHCP 租約的頻率。如果您想要，可以使用執行個體上的作業系統明確更新租約。

使用主控台變更與 VPC 相關的 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC 的核取方塊，然後選擇 Actions (動作) 和 Edit VPC settings (編輯 VPC 設定)。
4. 在 DHCP options set (DHCP 選項集) 中，選擇新的 DHCP 選項集。或者，選擇無 DHCP 選項集以停用 VPC 的網域名稱解析。
5. 選擇儲存。

使用命令列變更與 VPC 相關的 DHCP 選項集

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

刪除 DHCP 選項集

如果您不再需要 DHCP 選項集，請使用下列程序將其刪除。如果 DHCP 選項集正在使用中，則無法刪除該選項集。對於與要刪除的 DHCP 選項集相關聯的每個 VPC，您必須將不同的 DHCP 選項集與該 VPC 建立關聯，或將 VPC 設定為不使用 DHCP 選項集。如需更多詳細資訊，請參閱 the section called “變更與 VPC 關聯的選項集”。

使用主控台刪除 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP option sets (DHCP 選項集)。
3. 選取 DHCP 選項集的選項按鈕，然後選擇動作、刪除 DHCP 選項集。
4. 出現確認提示時，請輸入 **`delete`**，然後選擇刪除 DHCP 選項集。

使用命令列刪除 DHCP 選項集

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

VPC 的 DNS 屬性

網域名稱系統 (DNS) 是一種在網際網路上用於解析為對應 IP 地址的標準名稱。DNS 主機名稱是電腦的唯一絕對名稱；由主機名稱和網域名稱組成。DNS 伺服器會將 DNS 主機名稱解析為對應的 IP 地址。

公有 IPv4 地址可啟用透過網際網路的通訊，而私有 IPv4 地址可啟用執行個體網路內的通訊。如需詳細資訊，請參閱您 VPC 和子網路的 IP 定址。

Amazon 為您的 VPC 提供 DNS 伺服器 (Amazon Route 53 Resolver)。若要改用您自己的 DNS 伺服器，請為 VPC 建立一組新的 DHCP 選項。如需詳細資訊，請參閱Amazon VPC 中的 DHCP 選項集。

目錄

- 認識 Amazon DNS
- 檢視 EC2 執行個體的 DNS 主機名稱
- 檢視和更新 VPC 的 DNS 屬性

認識 Amazon DNS

身為 AWS 架構師或管理員，您會遇到的其中一個基礎聯網元件是 Amazon DNS 伺服器，也稱為 Route 53 Resolver。此 DNS 解析程式服務原生整合至您 AWS 區域內的每個可用區域，為 Virtual Private Cloud (VPC) 中的網域名稱解析提供可靠且可擴展的解決方案。在本節中，您將了解 Amazon DNS 伺服器的 IP 位址、可以解析的私有 DNS 主機名稱，以及管理其用量的規則。

目錄

- Amazon DNS 伺服器
- 規則和考量
- EC2 執行個體的 DNS 主機名稱
- VPC 的 DNS 屬性
- DNS 配額
- 私有託管區域

Amazon DNS 伺服器

Route 53 Resolver （也稱為「Amazon DNS 伺服器」或「AmazonProvidedDNS」）是一種 DNS Resolver 服務，內建於 AWS 區域中的每個可用區域。Route 53 Resolver 位於 `169.254.169.253` (IPv4)、`fd00:ec2::253` (IPv6) 以及佈建至 VPC+2 的主要私有 IPV4 CIDR 範圍。例如，如果您的 VPC 具有 `10.0.0.0/16` IPv4 CIDR 和 `2001:db8::/32` IPv6 CIDR，則您可以連線位於 `169.254.169.253` (IPv4)、`fd00:ec2::253` (IPv6) 或 `10.0.0.2` (IPv4) 的 Route 53 Resolver。VPC 內的資源會使用 DNS 查詢的連結本機地址。這些查詢會私下傳輸到 Route 53 Resolver，且不會顯示在網路上。在僅 IPv6 子網路中，只要「AmazonProvidedDNS」是 DHCP 選項集中的名稱伺服器，IPv4 連結本機地址 (169.254.169.253) 仍然可以連線。

當您在 VPC 中啟動執行個體時，我們會為該執行個體提供私有 DNS 主機名稱。如果該執行個體設定了公有 IPv4 地址，且 VPC DNS 屬性已啟用，我們也會提供公有 DNS 主機名稱。

私有 DNS 主機名稱的格式取決於您在啟動 EC2 執行個體時設定的方式。如需有關私有 DNS 主機名稱類型的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體主機名稱類型。

在您 VPC 中的 Amazon DNS 伺服器，會用於解析您在 Route 53 中私有託管區域中指定的 DNS 網域名稱。如需私有託管區域的詳細資訊，請參閱 Amazon Route 53 開發人員指南中的使用私有託管區域。

規則和考量

使用 Amazon DNS 伺服器時，須遵循以下規則和考量。

- 您無法使用網路 ACL 或安全群組來篩選與 Amazon DNS 伺服器往來的流量。
- 使用 Hadoop 框架的服務 (如 Amazon EMR)，會請求執行個體解析其完全合格的網域名稱 (FQDN)。在此情況下，如果 `domain-name-servers` 選項設定為自訂值，則 DNS 解析可能會失敗。若要確保正確解析 DNS，請考慮在您的 DNS 伺服器上新增條件式轉寄站，將針對 *region-name*`.compute.internal` 網域的查詢轉送至 Amazon DNS 伺服器。如需詳細資訊，請參閱 Amazon EMR 管理指南中的設定 VPC 以託管叢集。
- Amazon Route 53 Resolver 只支援遞迴 DNS 查詢。

EC2 執行個體的 DNS 主機名稱

當您啟動執行個體時，它始終會接收私有 IPv4 地址和對應至其私有 IPv4 地址的私有 DNS 主機名稱。如果您的執行個體具有公有 IPv4 地址，其 VPC 的 DNS 屬性會決定它是否接收對應於該公有 IPv4 地址的公有 DNS 主機名稱。如需詳細資訊，請參閱VPC 的 DNS 屬性。

啟用 Amazon 提供的 DNS 伺服器後，DNS 主機名稱解析如下。

私有 IPv4 DNS 名稱

執行個體的私有 IPv4 DNS 主機名稱將解析為其私有 IPv4 位址。您可以使用私有 IPv4 DNS 主機名稱，在同一個 VPC 中或多個已連線 VPC 中的執行個體之間進行通訊。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的私有 IPv4 位址。

公有 IPv4 DNS 名稱

執行個體的公有 IPv4 DNS 主機名稱將解析為其公有 IPv4 位址 (執行個體網路外部)，或其私有 IPv4 位址 (執行個體網路內部)。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的公有 IPv4 位址。

若要透過 VPC 對等互連將公有 IPv4 DNS 名稱解析為私有 IPv4 位址，您必須為對等互連啟用 DNS 解析功能。如需詳細資訊，請參閱啟用 VPC 對等互連的 DNS 解析。

私有資源 DNS 名稱

RBN 型 DNS 名稱，可解析為此執行個體選取的 A 和 AAAA DNS 記錄。此 DNS 主機名稱會顯示在雙堆疊和僅限 IPv6 子網中執行個體的執行個體詳細資訊中。如需有關 RBN 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 EC2 執行個體主機名類型。

VPC 的 DNS 屬性

下列 VPC 屬性會決定為您的 VPC 提供的 DNS 支援。如果啟用兩個屬性，則在 VPC 中啟動的執行個體會收到公有 DNS 主機名稱 (如果在建立時被指派公有 IPv4 地址或彈性 IP 地址)。如果您對 VPC 啟用兩個屬性 (原本並未啟用)，則已在 VPC 中啟動的執行個體會收到公有 DNS 主機名稱 (如果其具備公有 IPv4 地址或彈性 IP 地址)。

若要確認您的 VPC 是否啟用這些屬性，請參閱 檢視和更新 VPC 的 DNS 屬性。

屬性	說明
`enableDnsHostnames`	判斷 VPC 是否支援將公有 DNS 主機名稱指派給具有公有 IP 地址的執行個體。 此屬性的預設值為 `false`，除非 VPC 為預設 VPC。請注意以下此屬性的規則和考量事項。
`enableDnsSupport`	確定 VPC 是否支援透過 Amazon 提供的 DNS 伺服器進行 DNS 解析。 如果此屬性為 `true`，對 Amazon 提供的 DNS 伺服器的查詢成功。如需詳細資訊，請參閱Amazon DNS 伺服器。 此屬性的預設值為 `true`。請注意以下此屬性的規則和考量事項。

規則和考量

- 如果這兩個屬性都設定為 `true`，會發生下列情況：
  - 具有公有 IP 地址的執行個體會收到對應的公有 DNS 主機名稱。
  - Route 53 Resolver 伺服器可解析 Amazon 提供的私有 DNS 主機名稱。
- 如果至少一個屬性設定為 `false`，將發生以下情況：
  - 具有公有 IP 地址的執行個體不會收到對應的公有 DNS 主機名稱。
  - Route 53 Resolver 無法解析 Amazon 提供的私有 DNS 主機名稱。
  - 如果 DHCP 選項集中有自訂網域名稱，則執行個體會收到自訂私有 DNS 主機名稱。如果未使用 Route 53 Resolver 伺服器，您的自訂網域名稱伺服器就必須視需要解析主機名稱。

- 如果您使用 Amazon Route 53 中私有託管區域中定義的自訂 DNS 網域名稱，或使用具有介面 VPC 端點的私有 DNS (AWS PrivateLink)，則必須將 `enableDnsHostnames` 和 `enableDnsSupport` 屬性皆設為 `true`。
- Route 53 Resolver 可針對所有位址空間將私有 DNS 主機名稱解析為私有 IPv4 位址，包括當 VPC 的 IPv4 位址範圍不在 RFC 1918 指定之私有 IPv4 位址範圍內的情況。但是，如果您的 VPC 是在 2016 年 10 月之前建立，當 VPC 的 IPv4 位址範圍超出這些範圍時，Route 53 Resolver 就無法解析私有 DNS 主機名稱。若要啟用這項支援，請聯絡 支援。

DNS 配額

使用連結本機地址的服務有每秒 1024 個封包 (PPS) 限制。此限制包括 Route 53 Resolver DNS 查詢、執行個體中繼資料服務 (IMDS) 請求、Amazon Time Service Network Time Protocol (NTP) 請求和 Windows Licensing Service (適用於 Microsoft Windows 型執行個體) 請求的彙總。此配額無法增加。

依據查詢類型、回應大小以及使用的通訊協定而異，Route 53 Resolver 支援的每秒 DNS 查詢數目也不同。如需詳細資訊和可擴展的 DNS 架構建議，請參閱《AWS 混合 DNS 與 Active Directory 技術指南》。

如果您達到配額限制，Route 53 Resolver 會拒絕流量。達到配額限制的一些原因可能是 DNS 調節問題，或使用 Route 53 Resolver 網路介面的執行個體中繼資料查詢。如需關於如何解決 VPC DNS 節流問題的資訊，請參閱如何判斷我向 Amazon 提供之 DNS 伺服器的 DNS 查詢是否會因 VPC DNS 節流而失敗。如需有關執行個體中繼資料擷取的資訊，請參閱《Amazon EC2 使用者指南》中的擷取執行個體中繼資料。

私有託管區域

若要使用自訂 DNS 網域名稱存取 VPC 中的資源，例如 `example.com`，而不是使用私有 IPv4 地址或 AWS提供的私有 DNS 主機名稱，您可以在 Route 53 中建立私有託管區域。私有託管區域是一種容器，其中包含的資訊說明您可以如何在一或多個 VPC 中路由某個網域及其子網域的流量，而不用將資源公開至網際網路。接著，您可以建立 Route 53 資源紀錄集，以決定 Route 53 如何回應網域和子網域的查詢。舉例來說，如果您想將 example.com 的瀏覽器請求路由至 VPC 中的 Web 伺服器，您可以在私有託管區域中建立 A 記錄，然後指定該 Web 伺服器的 IP 地址。如需如何建立私有託管區域的詳細資訊，請參閱 Amazon Route 53 開發人員指南中的使用私有託管區域。

若要使用自訂 DNS 網域名稱來存取資源，您必須連線至 VPC 內的執行個體。您可以在執行個體中使用 `ping` 命令 (例如 `ping mywebserver.example.com`)，來測試私有託管區域中的資源是否可透

過其自訂 DNS 名稱來存取。(您必須確認執行個體的安全群組允許傳入 ICMP 流量，ping 命令才能運作。)

私有託管區域將無法支援 VPC 之外的轉移關係；這樣一來，您就無法使用資源的自訂私有 DNS 名稱從 VPN 連線另一端存取資源。

> **Important**
>
> 如果您使用在 Amazon Route 53 私有託管區域中定義的自訂 DNS 網域名稱，則必須將 `enableDnsHostnames` 和 `enableDnsSupport` 屬性設定為 `true`。

檢視 EC2 執行個體的 DNS 主機名稱

您可以使用 Amazon EC2 主控台或命令列，檢視運作中執行個體或網路介面的 DNS 主機名稱。了解這些主機名稱對於連線到您的資源非常重要。

與執行個體相關聯的 VPC 啟用 DNS 選項時，就可以使用 Public DNS (IPv4) (公有 DNS (IPv4)) 和 Private DNS (私有 DNS) 欄位。如需詳細資訊，請參閱the section called “VPC 的 DNS 屬性”。

執行個體

使用主控台檢視執行個體的 DNS 主機名稱

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 從清單選取執行個體。
4. 在詳細資訊窗格中，Public DNS (IPv4) (公有 DNS (IPv4)) 和 Private DNS (私有 DNS) 欄位會顯示 DNS 主機名稱 (如適用)。

使用命令列檢視執行個體的 DNS 主機名稱

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

網路介面

使用主控台檢視網路介面的私有 DNS 主機名稱

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Network Interfaces (網路介面)。
3. 從清單選取網路介面。
4. 在詳細資訊窗格中，Private DNS (IPv4) (私有 DNS (IPv4)) 欄位會顯示私有 DNS 主機名稱。

使用命令列檢視網路介面的 DNS 主機名稱

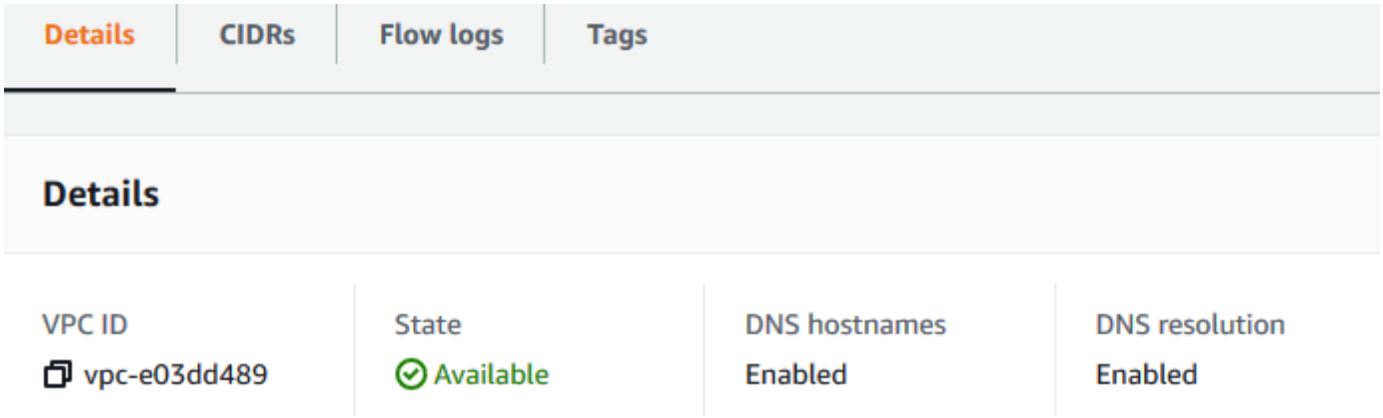
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

檢視和更新 VPC 的 DNS 屬性

您可以使用 Amazon VPC 主控台檢視和更新 VPC 的 DNS 支援屬性。這些設定控制您的執行個體是否取得公有 DNS 主機名稱，以及 Amazon DNS 伺服器是否可以解析您的私有 DNS 名稱。正確設定這些屬性對於確保 VPC 內的無縫通訊至關重要。

使用主控台來說明和更新 VPC 的 DNS 支援屬性

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC 的核取方塊。
4. 檢閱詳細資訊中的資訊。在此範例中，DNS 主機名稱及 DNS 解析均已啟用。



5. 若要更新這些設定，請選擇 Actions (動作)，然後選擇 Edit VPC settings (編輯 VPC 設定)。在適當的 DNS 屬性上選取或清除 Enable (啟用)，然後選擇 Save changes (儲存變更)。

使用命令列說明 VPC 的 DNS 支援

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

使用命令列更新 VPC 的 DNS 支援

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

VPC 的網路地址使用

網路地址使用 (NAU) 是套用至虛擬網路中資源的指標，可協助您規劃和監控 VPC 大小。每個 NAU 單位都會計入代表 VPC 大小的總計。

請務必了解組成 VPC NAU 的單位總數，因為下列 VPC 配額會限制 VPC 的大小：

- 網路地址使用 – 單一 VPC 可擁有的 NAU 單位數量上限。依預設，每個 VPC 最多可有 6.4 萬個 NAU 單位。您可以請求將配額增加至最多 25.6 萬個。
- 對等網路地址使用 – VPC 及其所有對等 VPC 的 NAU 單位數量上限。如果 VPC 與相同區域中的其他 VPC 對等互連，則依預設，所有的 VPC 加總最多可以有 12.8 萬個 NAU 單位。您可以請求將配額增加至最多 51.2 萬個。此配額適用於相同區域中 VPCs 之間的對等互連，包括不同 AWS 帳戶中 VPCs之間的對等互連。對等至不同區域的 VPCs 不會導致此配額。

您可用下列方式使用 NAU：

- 在建立虛擬網路之前，請先計算 NAU 單位，以協助您決定是否應將工作負載分散至多個 VPC。
- 建立 VPC 之後，請使用 Amazon CloudWatch 監控 VPC 的 NAU 用量，使其不會超出 NAU 配額。建議您建立 Amazon CloudWatch 警示來監控 NAU 配額。如需詳細資訊，請參閱the section called “CloudWatch 指標”。

超過 NAU 配額

如果您超過 VPC 的 NAU 配額，下列 API 呼叫會失敗並出現用戶端例外狀況：

- `RunInstances`
- `AttachNetworkInterface`
- `AssignPrivateIpAddresses`
- `AssignIpv6Addresses`
- `AcceptVpcPeeringConnection`

特定例外狀況取決於您超過的配額：

- `NetworkAddressUsageLimitExceeded` – VPC 超過其 NAU 配額。
- `NetworkAddressUsagePeeredLimitExceeded` – VPC 超過其對等 VPC NAU 配額。

這些失敗會影響您啟動執行個體、連接網路介面、指派新地址、接受 VPC 互連連線，以及擴展或管理受影響 VPCs 中工作負載的能力。為避免中斷，請使用 Amazon CloudWatch 監控 NAU 用量，並在達到配額之前請求增加。

NAU 的計算方式

如果您了解 NAU 的計算方式，它可以協助您規劃 VPC 的擴展。

下表說明 VPC 中構成 NAU 計數的資源，以及每個資源使用的 NAU 單位數量。有些 AWS 資源表示為單一 NAU 單位，有些資源表示為多個 NAU 單位。您可以使用此表來了解 NAU 的計算方式。

資源	NAU 單位
指派給 VPC 中 EC2 執行個體網路界面的每個私有或公有 IPv4 地址和每個 IPv6 地址	1
連接至 EC2 執行個體的其他網路介面	1
指派給網路介面的字首	1
每個 AZ 的 Network Load Balancer	6

資源	NAU 單位
每個 AZ 的 Gateway Load Balancer	6
每個 AZ 的VPC端點	6
傳輸閘道連接	6
Lambda 函式	6
NAT 閘道	6
EFS 掛載目標	6
EFA 介面 (EFA 搭配 ENA 裝置) 或僅 EFA 界面	1
Amazon EKS Pod	1

NAU 範例

下列範例顯示如何計算 NAU。

範例 1 – 使用 VPC 對等互連連接的兩個 VPC

同一區域中的對等 VPC 會佔用合併 NAU 配額。

- VPC 1
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位
  - 100 個 Lambda 函數 – 600 個 NAU 單位
- VPC 2
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位
  - 100 個 Lambda 函數 – 600 個 NAU 單位
- 對等互連 NAU 總計數：42,400 個單位

- 預設對等互連 NAU 配額：12.8 萬個單位

範例 2 – 使用傳輸閘道連接的兩個 VPC

使用傳輸閘道連接的 VPC 不會像對等 VPC 那樣佔用合併的 NAU 配額。

- VPC 1
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位
  - 100 個 Lambda 函數 – 600 個 NAU 單位
- VPC 2
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位
  - 100 個 Lambda 函數 – 600 個 NAU 單位
- 每個 VPC 的 NAU 總計數：21,200 個單位
- 每個 VPC 的預設 NAU 配額：6.4 萬個單位

範例 3 - 使用跨區域 VPCs 對等互連連接的兩個 VPC

對等跨不同區域的 VPCs 不會導致合併的 NAU 配額。 會根據自己的每個 VPC NAU 配額 AWS 來評估每個 VPC，而跨區域對等互連的資源不會計入任一 VPC 的對等 NAU。此範例假設每個 VPC 的唯一對等互連是顯示的跨區域對等互連 （沒有額外的區域間對等互連）。

- VPC 1 （區域 A)
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位
  - 100 個 Lambda 函數 – 600 個 NAU 單位
- VPC 2 （區域 B)
  - 個別可用區域的 2 個子網路中的 50 個網路負載平衡器 - 600 個 NAU 單位
  - 一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址)，另一個子網路中有 5,000 個執行個體 (每個執行個體都有 IPv4 地址和 IPv6 地址) - 20,000 個單位

  - 100 個 Lambda 函數 – 600 個 NAU 單位
- 每個 VPC 的 NAU 總計數：21,200 個單位
- 每個 VPC 的預設 NAU 配額：6.4 萬個單位
- 每個 VPC 的對等 NAU 計數：21，200 個單位（僅限 VPC 自己的資源計數；跨區域對等提供 0)
- 每個 VPC 的預設對等 NAU 配額：128，000 個單位（跨區域對等不會計入此配額）

與其他帳戶共享 VPC 子網路

VPC 子網路共用可讓多個 AWS 帳戶 建立其應用程式資源，例如 Amazon EC2 執行個體、Amazon Relational Database Service (RDS) 資料庫、Amazon Redshift 叢集和 AWS Lambda 函數，以共用、集中管理的虛擬私有雲端 (VPCs)。在此模型中，擁有 VPC 的帳戶（擁有者）會與其他屬於相同組織的帳戶（參與者）共用一或多個子網路 AWS Organizations。共用子網路後，參與者可以檢視、建立、修改及刪除與其共用之子網路中的應用程式資源。參與者無法檢視、修改或刪除屬於其他參與者或 VPC 擁有者的資源。

您可以共用 VPC 子網路，將 VPC 內的隱含路由用於需要高度互連性且位於相同信任界限內的應用程式。這樣會減少建立和管理的 VPC 數量，同時使用個別的帳戶進行帳單和存取控制。您可以使用連線功能，例如傳輸閘道和 VPC 對等互連共用 Amazon VPC 子網路 AWS PrivateLink，以簡化網路拓撲。如需 VPC 子網路共享利益的詳細資訊，請參閱 VPC 共享：多重帳戶和 VPC 管理的新途徑。

VPC 子網路共享有相關的配額。如需詳細資訊，請參閱VPC 子網路共用。

目錄

- 共用子網路先決條件
- 使用共用子網路
- 適用於擁有者及參與者的計費和計量
- 擁有者和參與者的責任與許可
- AWS 資源和共用 VPC 子網路

共用子網路先決條件

本節包含使用共用子網路的先決條件：

- VPC 擁有者和參與者的帳戶必須由 管理 AWS Organizations。

- 您必須從組織的管理帳戶在 AWS RAM 主控台中啟用資源共用。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的透過 AWS Organizations啟用共用。
- 您必須建立資源共享。您可以在建立資源共享時指定要共用的子網路，或稍後使用下一節中的程序將子網路新增至資源共享。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的建立資源共用。

使用共用子網路

本節說明如何在 AWS 主控台和 中使用共用子網路 AWS CLI。

目錄

- 共用子網路
- 取消共用的子網路
- 識別共用子網路的擁有者

共用子網路

您可以與組織中的其他帳戶共用非預設的資料夾，具體操作如下。此外，您可以跨 AWS Organizations 共用安全群組。如需詳細資訊，請參閱與 AWS Organizations 共用安全群組。

使用主控台共用子網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網路)。
3. 選取您的子網路，然後選擇操作、Share subnet (共用子網路。
4. 選取您的資源共享，然後選擇 Share subnet (共用子網路)。

使用 共用子網路 AWS CLI

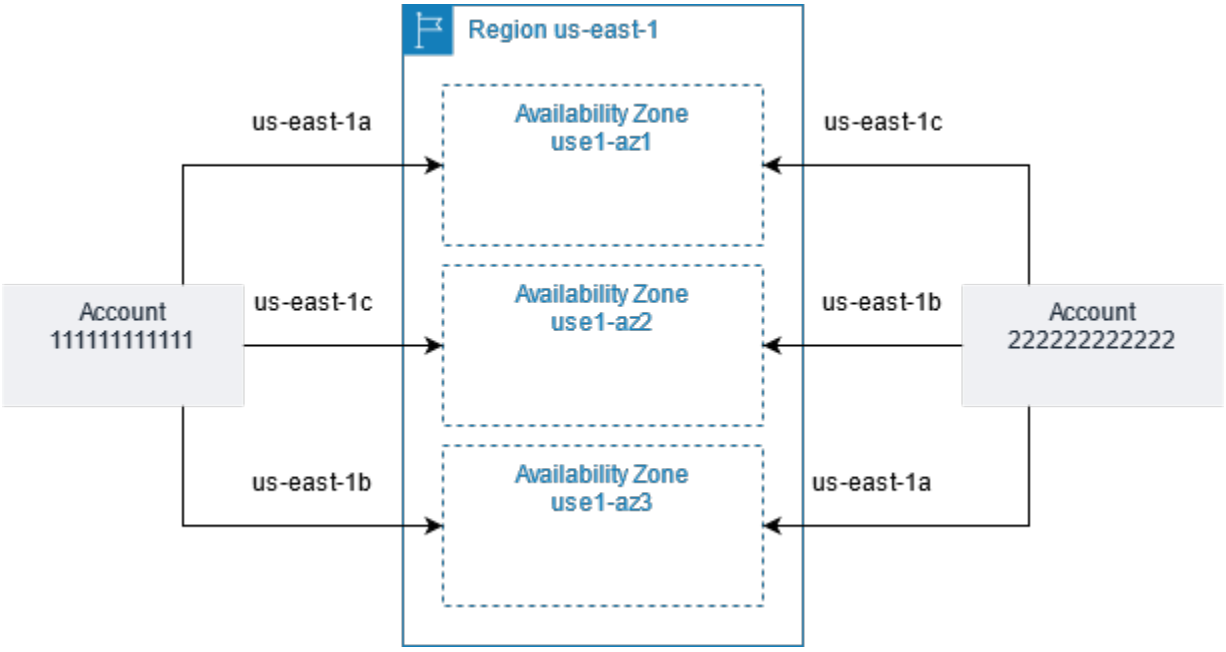
使用 create-resource-share 和 associate-resource-share 命令。

跨可用區域對應子網路

為確保資源分配至區域中的所有可用區域，可用區域會獨立映射至各個 帳戶的名稱。例如，`us-east-1a`您 AWS 帳戶的可用區域可能沒有與`us-east-1a`另一個 AWS 帳戶相同的位置。

若要跨帳戶協調可用區域以實現 VPC 共用，您必須使用 AZ ID，這是可用區域唯一且一致的識別符。例如，`use1-az1` 是 `us-east-1` 區域其中一個可用區域的 AZ ID。利用 AZ ID 來判斷某個帳戶資源在另一個帳戶中的相對位置。您可以在 Amazon VPC 主控台中檢視各子網路的 AZ ID。

以下圖表說明具有不同可用區域代碼映射至 AZ ID 的兩個帳戶。



取消共用的子網路

其擁有者隨時都可以取消共享和其他參與者共用的子網路。當擁者取消共享子網路後，便會套用以下規則：

- 現有參與者資源在具有自動化/受管工作流程（例如自動擴展或節點替換）的未共用 subnet. AWS managed 服務（例如 Elastic Load Balancing) 中繼續執行，可能需要持續存取部分資源的共用子網路。
- 參與者再也不能在已取消共用的子網路中建立新資源。
- 參與者可以修改、描述及刪除其在子網路中的資源。
- 如果參與者在已取消共用的子網路中仍擁有資源，該擁有者便無法刪除共用的子網路或共用的子網路 VPC。在參與者刪除已取消共用的子網路中的所有資源後，參與者只能刪除共用的子網路或共用的子網路 VPC。

使用主控台取消共用子網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇 Subnets (子網路)。
3. 選取您的子網路，然後選擇操作、Share subnet (共用子網路。
4. 選擇操作、Stop sharing (停止共用)。

使用 取消共用子網路 AWS CLI

使用 disassociate-resource-share 命令。

識別共用子網路的擁有者

參與者可以使用 Amazon VPC 主控台或命令列工具來檢視已和他們共享的子網路。

使用主控台識別子網路擁有者

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網路)。Owner (擁有者) 資料行會顯示子網路擁有者。

使用 識別子網路擁有者 AWS CLI

使用 describe-subnets 和 describe-vpcs 命令，其包含輸出中的擁有者 ID。

適用於擁有者及參與者的計費和計量

本節包含擁有共用子網路的人員以及使用共用子網路的人員的帳單和計量詳細資訊：

- 在共用 VPC 中，每位參與者都會支付其應用程式資源的費用，包括 Amazon EC2 執行個體、Amazon Relational Database Service 資料庫、Amazon Redshift 叢集和 AWS Lambda 函數。參與者也會支付與可用區域間資料傳輸以及透過 VPC 互連連線、跨網際網路閘道和跨 AWS Direct Connect 閘道進行資料傳輸相關的資料傳輸費用。
- VPC 擁有者會支付 NAT 閘道、虛擬私有閘道、傳輸閘道和 VPC 端點之間的每小時費用 （如適用） AWS PrivateLink、資料處理和資料傳輸費用。此外，共用 VPC 中使用的公有 IPv4 地址會向 VPC 擁有者收費。如需公有 IPv4 地址定價的詳細資訊，請參閱 Amazon VPC 定價頁面中的公有 IPv4 地址。
- 相同可用區域內的資料傳輸 (以 AZ-ID 唯一識別) 是免費的，無論哪個帳戶擁有通訊資源。

擁有者和參與者的責任與許可

本節包含有關擁有共用子網路 (擁有者) 的人員以及使用共用子網路 (參與者) 的人員的責任和許可的詳細資訊。

擁有者資源

擁有者對其擁有的 VPC 資源負責。VPC 擁有者負責建立、管理和刪除與共享 VPC 關聯的資源。這些包括子網路、路由表、網路 ACL、對等連線、閘道端點、介面端點、Route 53 Resolver 端點、網際網路閘道、NAT 閘道、虛擬私有閘道及傳輸閘道連接。

參與者資源

參與者對其擁有的 VPC 資源負責。參與者可以在共享 VPC 中建立有限的 VPC 資源集。例如，參與者可以建立網路介面和安全群組，並且為自己擁有的網路介面啟用 VPC 流量日誌。參與者根據參與者帳戶 (而非擁有者帳戶) 中的 VPC 配額建立的 VPC 資源計數。如需詳細資訊，請參閱VPC 子網路共用。

VPC 資源

使用共用 VPC 子網路時，下列責任和許可套用至 VPC 資源：

流程日誌

- 參與者可以在自己擁有的共用 VPC 子網路中建立、刪除及描述網路界面的流程日誌。
- 參與者無法在自己不擁有的共用 VPC 子網路中建立、刪除或描述網路界面的流程日誌。
- 參與者無法在共用 VPC 子網路中建立、刪除或描述流程日誌。
- VPC 擁有者可以在自己不擁有的共用 VPC 子網路中建立、刪除及描述網路界面的流程日誌。
- VPC 擁有者可以建立、刪除及描述共用 VPC 子網路的流程日誌。
- VPC 擁有者無法描述或刪除由參與者建立的流程日誌。

網際網路閘道和輸出限定網際網路閘道

- 參與者無法在共用 VPC 子網路中建立、連接或刪除網際網路閘道和輸出限定網際網路閘道。參與者可以在共用 VPC 子網路中描述網際網路閘道。參與者無法在共用 VPC 子網路中描述輸出限定網際網路閘道。

NAT 閘道

- 參與者無法在共用 VPC 子網路中建立、刪除或描述 NAT 閘道。

網路存取控制清單 (NACL)

- 參與者無法在共用 VPC 子網路中建立、刪除或取代 NACL。參與者可以描述共用 VPC 子網路中由 VPC 擁有者建立的 NACL。

網路介面

- 參與者可以在共用 VPC 子網路中建立網路介面。參與者無法以任何其他方式 (例如連接、分離或修改網路介面) 使用由 VPC 擁有者在共用 VPC 子網路中建立的網路介面。參與者只能修改或刪除他們在共用 VPC 中建立的網路介面。例如，參與者可以將 IP 地址與他們建立的網路介面關聯或取消關聯。
- VPC 擁有者可以描述共用 VPC 子網路中由參與者所擁有的網路介面。VPC 擁有者無法以任何其他方式使用由參與者擁有的網路介面，例如連接、分離或修改共用 VPC 子網路中由參與者擁有的網路介面。

路由表

- 參與者無法使用共用 VPC 子網路中的路由表 (例如，建立、刪除或關聯路由表)。參與者可描述共用 VPC 子網路中的路由表。

Security groups (安全群組)

- 參與者可以在共用 VPC 子網路中對自己擁有的安全群組進行操作 (如建立、刪除、描述、修改或建立輸入和輸出規則)。如果 VPC 擁有者與參與者共用安全群組，則參與者可以對 VPC 擁有者建立的安全群組進行操作。
- 參與者可以在他們擁有的安全群組中建立規則，這些規則參照屬於其他參與者或 VPC 擁有者的安全群組，例如：account-number/security-group-id
- 參與者無法使用 VPC 預設安全群組來啟動執行個體，因為預設安全群組屬於擁有者。
- 參與者無法使用 VPC 擁有者或其他參與者擁有的非預設安全群組來啟動執行個體，除非該安全群組已與其共用。
- VPC 擁有者可以描述共用 VPC 子網路中參與者建立的安全群組。VPC 擁有者無法以任何其他方式使用由參與者建立的安全群組。例如，VPC 擁有者無法使用參與者建立的安全群組來啟動執行個體。

子網路

- 參與者無法修改共用子網路或其相關屬性。只有 VPC 擁有者可以執行此類作動。參與者可描述共用 VPC 子網路中的子網路。
- VPC 擁有者只能與同一組織中來自 AWS Organizations 的其他帳戶或組織單位共用子網路。VPC 擁有者不能共用預設 VPC 中的子網路。

傳輸閘道

- 只有 VPC 擁有者可以將傳輸閘道連接至共用 VPC 子網路。參與者無法。

VPC

- 參與者無法修改 VPC 或其相關屬性。只有 VPC 擁有者可以執行此類作動。參與者可以描述 VPC 及其屬性和 DHCP 選項集。
- VPC 標籤以及共用 VPC 內資源的標籤不會與參與者共用。
- 參與者可以將自己的安全群組與共用 VPC 建立關聯。這可讓參與者將安全群組與其在共用 VPC 中擁有的彈性網路介面搭配使用。

AWS 資源和共用 VPC 子網路

下列 AWS 服務 支援共用 VPC 子網路中的資源。如需詳細資訊，請依照連結查看對應服務的說明文件。

- Amazon Aurora
- AWS Database Migration Service
- Amazon EC2
- Amazon ECS
- Amazon ElastiCache (Redis OSS)
- Amazon EFS
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Application Load Balancer
  - Gateway Load Balancer

  - Network Load Balancer
- Amazon EMR
- AWS Glue
- AWS Lambda
- 執行 Apache MQ 的 Amazon MQ (非 Rabbit MQ)
- Amazon MSK
- AWS Network Manager
  - AWS 雲端 WAN
  - 網路存取分析器
  - Reachability Analyzer
- Amazon OpenSearch Service
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon Route 53
- Amazon SageMaker Unified Studio
- AWS Transit Gateway
- AWS Verified Access
- Amazon VPC
  - 對等互連
  - 流量鏡射
- Amazon VPC Lattice

† 您可以使用共用 VPC 中的 VPC 端點連線到支援 PrivateLink 的所有 AWS 服務。如需支援 PrivateLink 的服務清單，請參閱《AWS PrivateLink 指南》中的與 AWS 整合的 AWS PrivateLink 服務。

此清單旨在包含所有支援在共用 VPC 子網路中啟動資源的服務。雖然我們已盡最大努力，但仍可能存在部分支援在共用 VPC 子網路中啟動資源但未在此列出的服務 如有任何疑問，歡迎提交文件意見回饋。

將 VPC 擴展至本機區域、Wavelength 區域或 Outpost

您可以在全球多個位置託管 VPC 資源 (例如子網路)。這些位置是由區域、可用區域、Local Zones 和 Wavelength 區域所組成。各個區域為獨立的地理區域。

- 可用區域是每個區域內的多個隔離位置。
- Local Zones 可讓您將資源 (例如運算和儲存) 放置在更靠近最終使用者的多個位置。
- AWS Outposts 將原生 AWS 服務、基礎設施和操作模型帶入幾乎所有資料中心、主機代管空間或內部部署設施。
- Wavelength 區域可讓開發人員為 5G 裝置與最終使用者建立提供極低延遲的應用程式。Wavelength 會將標準 AWS 運算和儲存服務部署到電信業者的 5G 網路邊緣。

AWS 操作state-of-the-art、高可用性的資料中心。儘管故障極為少見，但仍可能影響相同位置內執行個體的可用性。若您將所有執行個體都託管於單一位置，一旦該位置受故障影響，所有執行個體都將無法使用。

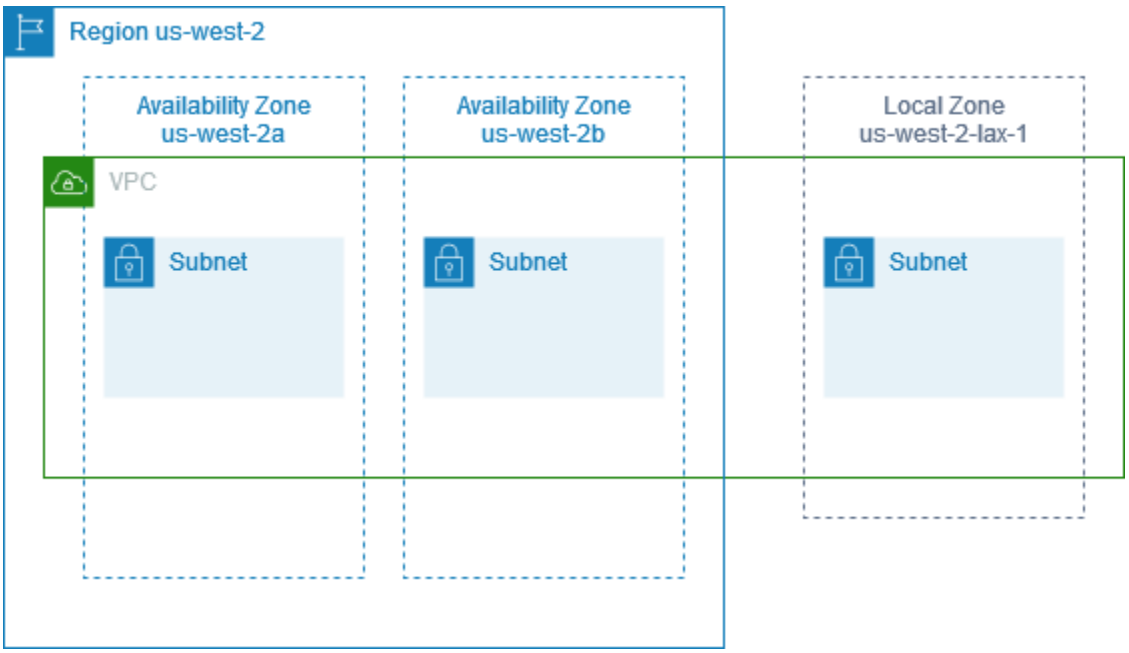
AWS 本機區域中的子網路

AWS Local Zones 可讓您將資源放在更接近使用者的位置，並使用熟悉APIs 和工具集，順暢地連線到 AWS 區域中的完整服務範圍。當您在本機區域中建立子網路時，會將 VPC 擴展到該本機區域。

若要使用本機區域，請使用如下步驟：

- 選擇加入本機區域。
- 在 Local Zone 中建立子網。
- 在本機區域子網路中啟動特定資源，讓您的應用程式更接近使用者。

下圖說明跨越可用區域和本機區域的美國西部 (奧勒岡) (us-west-2) 區域中的 VPC。



當您建立 VPC 時，您可以選擇將一組 Amazon 提供的公用 IP 地址指派給 VPC。您也可以為地址設定網路邊界群組，將地址限制到該群組。設定網路邊界群組後，IP 地址無法在網路邊界群組之間移動。Local Zone 網路流量將直接進入網際網路或連接點 (PoP)，而不會周遊 Local Zone 的父區域，因而可以取用低延遲運算。如需 Local Zones 及相應父區域的完整清單，請參閱《AWS Local Zones 使用者指南》中的可用 Local Zones。

下列規則適用於 Local Zones：

- 本機區域子網路遵循與可用區域子網路相同的路由規則，包括路由表、安全群組，以及網路 ACL。
- 傳出網際網路流量會從本機區域傳出。
- 您必須佈建公有 IP 地址，才能在本機區域中使用。當您配置地址時，可以指定公告 IP 地址的位置。我們將其稱為網路邊界群組，而且您可以設定此參數，將地址限制為此位置。佈建 IP 地址之後，您無法在本機區域和父區域之間移動它們 (例如，從 `us-west-2-lax-1a` 到 `us-west-2`)。
- 如果 Local Zone 支援 IPv6，您可以針對全新或現有的 VPC，使用網路邊界群組以請求 IPv6 Amazon 提供的 IP 地址，並將這些地址建立關聯。如需支援 IPv6 的 Local Zones 清單，請參閱《AWS Local Zones 使用者指南》中的考量
- 您無法在 Local Zone 子網路內建立 VPC 端點。

如需有關使用 Local Zones 的詳細資訊，請參閱 AWS Local Zones 使用者指南。

網際網路閘道的考量事項

當您在 Local Zones 中使用網際網路閘道 (在父區域中) 時，請考慮下列資訊：

- 您可以在 Local Zones 中使用具有彈性 IP 地址或 Amazon 自動指派公有 IP 地址的網際網路閘道。您關聯的彈性 IP 地址必須包含本機區域的網路邊界群組。如需詳細資訊，請參閱 the section called “彈性 IP 位址”。

  您無法關聯為區域設定的彈性 IP 地址。
- 在 Local Zones 中使用的彈性 IP 地址與區域中的彈性 IP 地址具有相同的配額。如需詳細資訊，請參閱 the section called “彈性 IP 位址”。
- 您可以在與本機區域資源相關聯的路由表中使用網際網路閘道。如需詳細資訊，請參閱 the section called “路由至網際網路閘道”。

使用 Direct Connect 閘道存取 Local Zones

請考慮您想要內部部署資料中心存取區域中的資源的案例。您可以使用與本機區域相關聯 VPC 的虛擬私有閘道來連線到 Direct Connect 閘道。Direct Connect 閘道會連線至 區域中的 Direct Connect 位置。內部部署資料中心具有與 Direct Connect 位置的 Direct Connect 連線。

> **Note**
>
> 透過 Direct Connect 傳送至 Local Zone 中子網路的流量不會通過 Local Zone 的父區域。相反地，流量採用最短路徑到達 Local Zone。這樣可以減少延遲，並協助您的應用程式提高回應速度。

您可以為此組態設定下列資源：

- 與本機區域子網路相關聯之 VPC 的虛擬私有閘道。您可以在 Amazon VPC 主控台的子網路詳細資訊頁面上檢視子網路的 VPC 也可使用 describe-subnets 命令進行查詢。

  如需如何建立虛擬私有閘道的詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的建立目標閘道。
- Direct Connect 連線。為了獲得最佳延遲效能， AWS 建議您使用最接近要擴充子網路之 Local Zone 的 Direct Connect 位置。

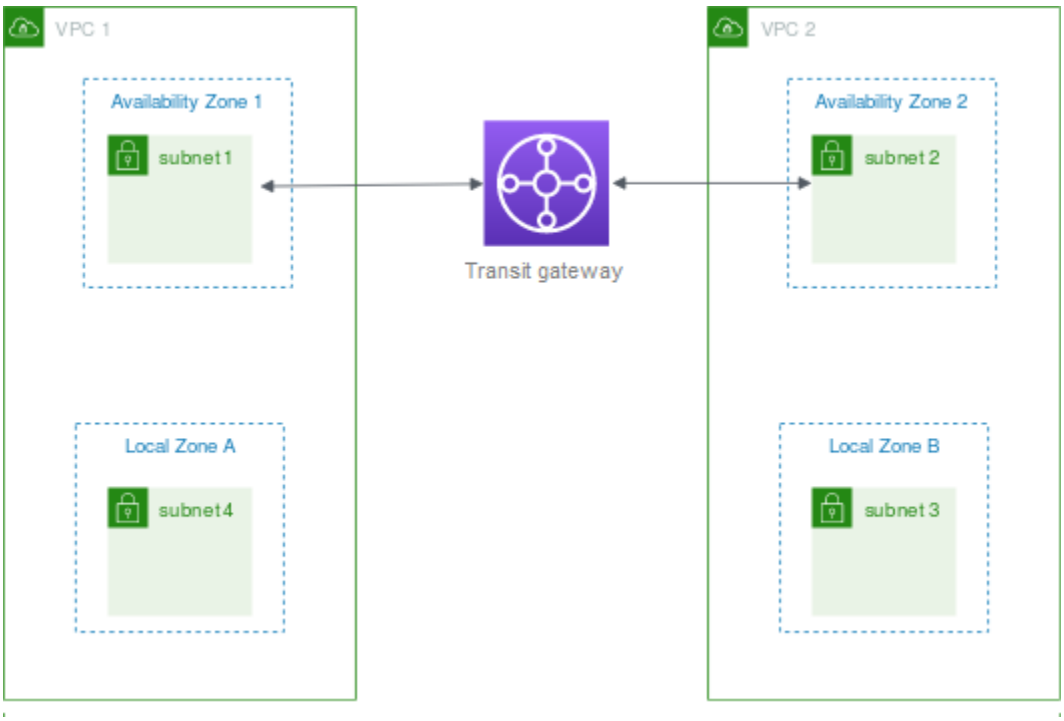
  如需如何排定連線順序的資訊，請參閱《Direct Connect 使用者指南》中的交叉連線。

- Direct Connect 閘道。如需如何建立 Direct Connect 閘道的資訊，請參閱《Direct Connect 使用者指南》中的建立 Direct Connect 閘道。
- 將 VPC 連線至 Direct Connect 閘道的虛擬私有閘道關聯。如需如何建立虛擬私有閘道關聯的資訊，請參閱《Direct Connect 使用者指南》中的建立和解除虛擬私有閘道的關聯。
- 從 Direct Connect 位置到內部部署資料中心的連線上的私有虛擬介面。如需如何建立 Direct Connect 閘道的資訊，請參閱《Direct Connect 使用者指南》中的建立 Direct Connect 閘道的私有虛擬介面。

將 Local Zones 子網路連線至 Transit Gateway

您無法為 Local Zones 中的子網路建立 Transit Gateway 附件。下圖顯示如何配置網路，以便 Local Zone 中的子網路透過父可用區域連線至傳輸閘道。在 Local Zones 中建立子網路，並在父可用區域中建立子網路。將父可用區域中的子網路連線至傳輸閘道，然後在路由表中為每個 VPC 建立一個路由，將目的地為其他 VPC CIDR 的流量路由至傳輸閘道連接的網路介面。

> **Note**
>
> 源自傳輸閘道且目的地為 Local Zone 中子網路的流量會先周遊父區域。



您可以為此案例建立下列資源：

- 每個父可用區域中的子網路。如需詳細資訊，請參閱the section called “建立子網”。
- 傳輸閘道。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的建立傳輸閘道。
- 每個使用父可用區域 VPC 的傳輸閘道連接。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的建立傳輸閘道連接。
- 與傳輸閘道連接相關聯的傳輸閘道路由表。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的傳輸閘道路由表。
- 對於每個 VPC (也就是 Local Zone 子網路中的每個項目)，VPC 路由表都要以其他 VPC CIDR 做為目的地，並以傳輸閘道連接的網路介面 ID 做為目標。若要尋找傳輸閘道連接的網路介面，請在網路介面的描述中搜尋傳輸閘道連接的 ID。如需詳細資訊，請參閱the section called “傳輸閘道的路由”。

以下是 VPC 1 的範例路由表。

目標	Target
VPC 1 CIDR	*##*
VPC 2 CIDR	*vpc1-attachment-network-interface-id*

以下是 VPC 2 的範例路由表。

目標	Target
VPC 2 CIDR	*##*
VPC 1 CIDR	*vpc2-attachment-network-interface-id*

以下是傳輸閘道路由表的範例。每個 VPC 的 CIDR 區塊會傳播至傳輸閘道路由表。

CIDR	連接	路由類型

CIDR	連接	路由類型
VPC 1 CIDR	*VPC 1 ###*	已傳播
VPC 2 CIDR	*VPC 2 ###*	已傳播

中的子網路 AWS Wavelength

AWS Wavelength 可讓開發人員建立提供極低延遲的應用程式給行動裝置與最終使用者。Wavelength 會將標準的 AWS 運算與儲存服務部署至電信業者 5G 網路的邊緣。開發人員可以將虛擬私有雲端 (VPC) 擴展至一或多個 Wavelength 區域，然後使用 Amazon EC2 執行個體之類的 AWS 資源來執行需要超低延遲並連線至 AWS 服務 區域中的應用程式。

若要使用 Wavelength 區域，您必須先選擇加入區域。接著，在 Wavelength 區域中建立一個子網路。您可以在 Wavelength 區域建立 Amazon EC2 執行個體、Amazon EBS 磁碟區以及 Amazon VPC 子網路和電信業者閘道。您也可以使用協調或使用 EC2、EBS 和 VPC 的服務，例如 Amazon EC2 Auto Scaling、Amazon EKS 叢集、Amazon ECS 叢集、Amazon EC2 Systems Manager AWS CloudTrail、Amazon CloudWatch 和 CloudFormation。Wavelength 中的服務是 VPC 的一部分，透過可靠、高頻寬的連線連接到 AWS 區域，以便輕鬆存取 服務，包括 Amazon DynamoDB 和 Amazon RDS。

以下規則適用於 Wavelength 區域：

- 當您在 VPC 中建立子網路並將其與 Wavelength 區域關聯時，VPC 會延伸到 Wavelength 區域。
- 依預設，您在跨越 Wavelength 區域的 VPC 中建立的每個子網路都會繼承主要 VPC 路由表，包括本機路由。
- 當您在 Wavelength 區域的子網路中啟動 EC2 執行個體時，會為其指派一個電信業者 IP 地址。電信業者閘道會使用從介面到網際網路或行動裝置的流量地址。電信業者閘道會使用 NAT 來轉譯地址，然後將流量傳送到目的地。透過電信業者閘道從電信電信業者網路路由傳送的流量。
- 您可以將 VPC 路由表的目標或 Wavelength 區域的子網路路由表設定為電信業者閘道，允許從特定位置的電信業者網路的傳入流量，以及向電信業者網路和網際網路的傳出流量。如需 Wavelength 區域中路由選項的詳細資訊，請參閱 AWS Wavelength 開發人員指南中的路由傳送。
- Wavelength 區域中的子網路與可用區域中的子網路具有相同的網路元件，包括 IPv4 地址、DHCP 選項集和網路 ACL。
- 您無法建立與 Wavelength 區域中子網路的傳輸閘道連接。請改為透過父可用區域中的子網路建立連接，然後透過傳輸閘道將流量路由至所需目的地。如需範例，請參閱下一節。

多個 Wavelength 區域的考量事項

位於相同 VPC 中不同 Wavelength 區域的 EC2 執行個體不允許彼此進行通訊。如果您需要 Wavelength 區域與 Wavelength 區域之間的通訊， AWS 建議您使用多個 VPCs，每個 Wavelength 區域各一個。您可以使用傳輸閘道以連線 VPC。此組態可啟用 Wavelength 區域中執行個體之間的通訊。

Wavelength 區域到 Wavelength 區域流量會透過 AWS 區域路由。如需詳細資訊，請參閱 AWS 傳輸閘道。

下圖顯示如何設定您的網路，以便在兩個不同 Wavelength 區域的執行個體可以進行通訊。您有兩個 Wavelength 區域 (Wavelength 區域 A 和 Wavelength 區域 B)。您需要建立下列資源才能啟用通訊：

- 對於每個 Wavelength 區域，需要有可用區域中的子網路 (該可用區域屬於 Wavelength 區域的父可用區域)。在此範例中，您可以建立子網路 1 和子網路 2。如需建立子網路的相關資訊，請參閱 the section called “建立子網”。使用 describe-availability-zones 命令可查找父區域。
- 傳輸閘道。傳輸閘道會連線 VPC。如需建立傳輸閘道的相關資訊，請參閱 Amazon VPC 傳輸閘道指南中的建立傳輸閘道。
- 對於每個 VPC，與 Wavelength 區域之父可用區域中傳輸閘道的 VPC 連接。如需詳細資訊，請參閱《Amazon VPC 傳輸閘道指南》中的與 VPC 的傳輸閘道連接。
- 傳輸閘道路由表中每個 VPC 的項目。如需建立 Transit Gateway 路由的相關資訊，請參閱 Amazon VPC Transit Gateway 指南中的 Transit Gateway 路由表。
- 對於每個 VPC，需要有 VPC 路由表中的項目，該路由表以其他 VPC CIDR 做為目的地，並以傳輸閘道 ID 做為目標。如需詳細資訊，請參閱 the section called “傳輸閘道的路由”。

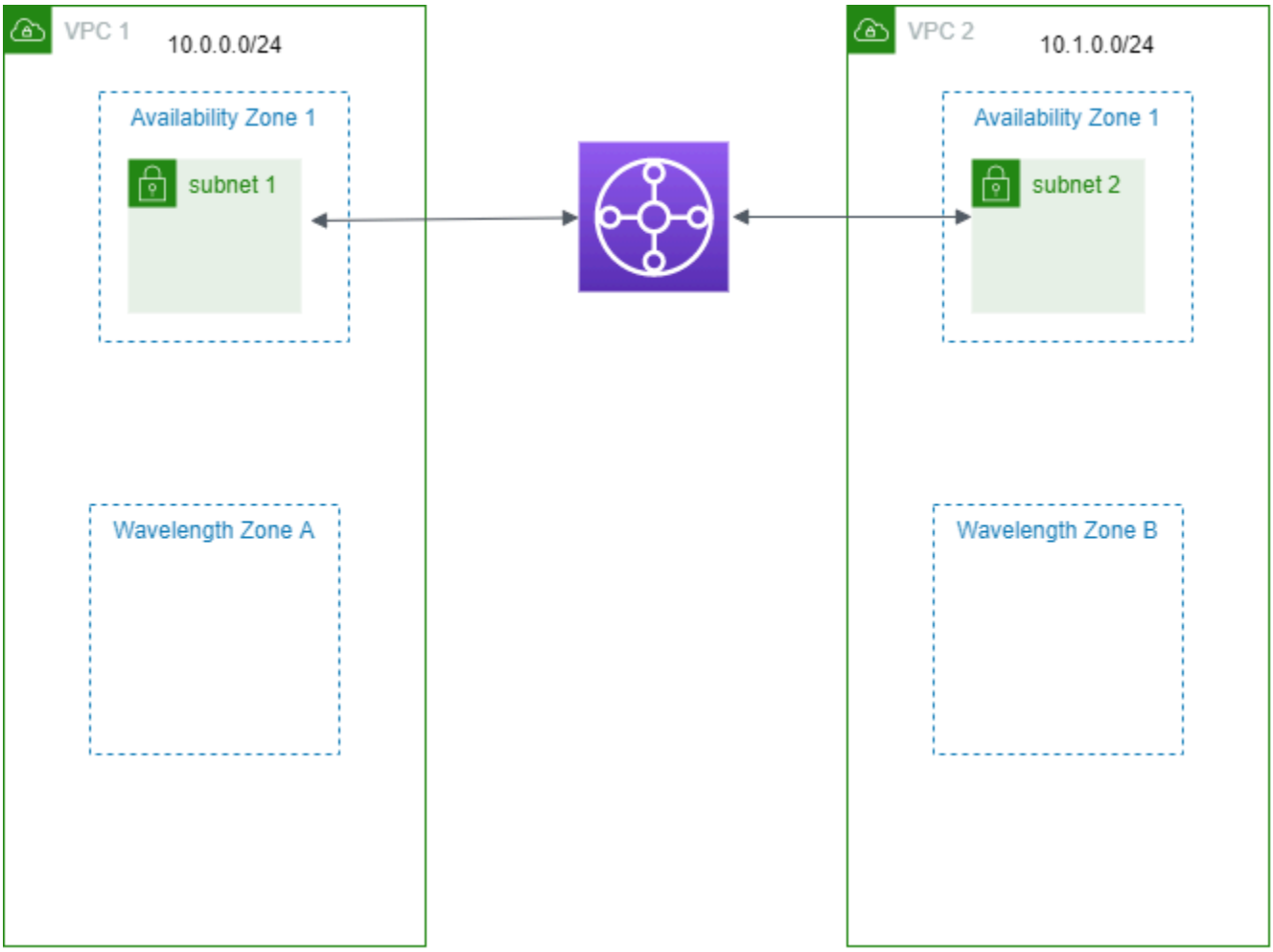
  在範例中，VPC 1 的路由表具有以下項目：

目的地	目標
10.1.0.0/24	tgw-22222222222222222

  VPC 2 的路由表具有以下項目：

目的地	目標
	tgw-22222222222222222

目的地	目標
10.0.0.0/24	



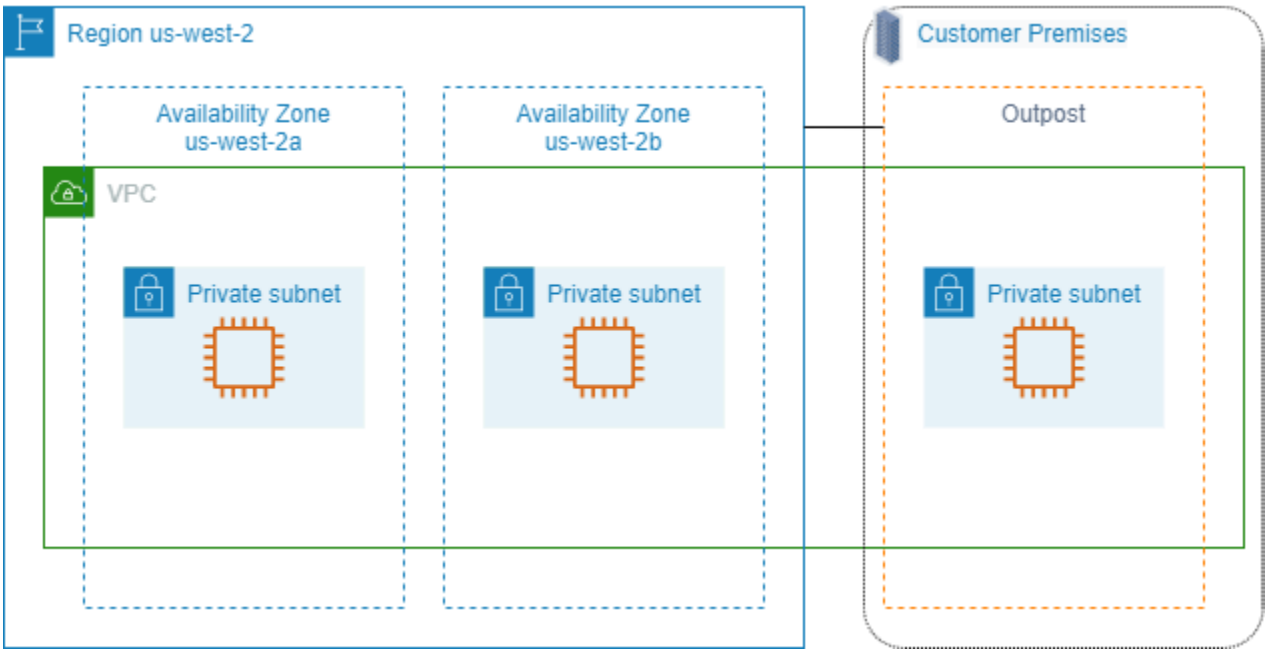
中的子網路 AWS Outposts

AWS Outposts 為您提供相同的 AWS 硬體基礎設施、服務、APIs 和工具，以在內部部署和雲端中建置和執行應用程式。 AWS Outposts 非常適合需要低延遲存取內部部署應用程式或系統的工作負載，以及需要在本機存放和處理資料的工作負載。如需 的詳細資訊 AWS Outposts，請參閱 AWS Outposts。

VPC 跨越 區域中的所有可用區域 AWS 。將 Outpost 連線到其上層區域後，您可以在該 VPC 中為 Outpost 建立子網路，將該區域中的任何 VPC 擴展至您的 Outpost。

下列規則適用於 AWS Outposts：

- 子網路必須位於某個 Outpost 位置。
- 若要為 Outpost 建立子網路，請在建立子網路時指定 Outpost 的 Amazon Resource Name (ARN)。
- Outposts 機架 - 本機閘道會處理 VPC 與內部部署網路之間的網路連線能力。如需詳細資訊，請參閱 Outposts 機架的 AWS Outposts 使用者指南中的本機閘道。
- Outposts 伺服器 - 本機網路介面會處理 VPC 與內部部署網路之間的網路連線能力。如需詳細資訊，請參閱 Outposts 伺服器 AWS Outposts 使用者指南中的本機網路介面。
- 依據預設，您在 VPC 中建立的每個子網路 (包含 Outposts 的子網路) 都會隱含與 VPC 的主路由表建立關聯。或者，您可以明確地將自訂路由表與 VPC 中的子網路建立關聯，並將本機閘道做為目的地為內部部署網路之所有流量的下一個躍點目標。



刪除您的 VPC

VPC 結束使用後即可刪除。

需求

可以刪除 VPC 前，您必須先終止或刪除在 VPC 中建立申請者管理之網路介面的所有資源。例如，您必須終止 EC2 執行個體並刪除您的負載平衡器、NAT 閘道、傳輸閘道 VPC 連接和介面 VPC 端點。

> **Note**
>
> 如果您已為要刪除的 VPC 建立流程日誌，請注意，已刪除 VPC 的流程日誌最終會被自動移除。

目錄

- 使用主控台刪除 VPC
- 使用命令列刪除 VPC

使用主控台刪除 VPC

如果您使用 Amazon VPC 主控台刪除 VPC，我們也會為您刪除下列 VPC 元件：

- DHCP 選項
- 輸出限定網際網路閘道
- 閘道端點
- 網際網路閘道
- 網路 ACL
- 路由表
- 安全群組
- 子網路

使用主控台來刪除您的 VPC

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 終止 VPC 中的所有執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的終止您的執行個體。
3. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
4. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
5. 選取要刪除的 VPC，然後選擇 Actions (動作)、Delete VPC (刪除 VPC)。
6. 如果有您在可以刪除 VPC 之前必須先刪除或終止的資源，我們會顯示這些資源。刪除或終止這些資源，然後再試一次。否則，除了 VPC 以外，還會顯示我們將刪除的其他資源。請檢閱清單，然後繼續進行下一個步驟。

7. (選用) 如果您有 Site-to-Site VPN 連線，您可以選取此選項以將其刪除。若您計劃搭配另一個 VPC 使用客戶閘道，我們建議您保留 Site-to-Site VPN 連線和閘道。否則，您必須在建立新的 Site-to-Site VPN 連線後，再次設定客戶閘道裝置。
8. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

使用命令列刪除 VPC

在您可以使用命令列刪除 VPC 前，必須先終止或刪除在 VPC 中建立申請者管理之網路介面的任何資源。您也必須刪除或分離自己建立的所有 VPC 資源，例如子網路、安全群組、網路 ACL、路由表、網際網路閘道和輸出限定網際網路閘道。您不需要刪除預設安全群組、預設路由表或預設網路 ACL。

下列程序會示範用於刪除常用 VPC 資源與刪除 VPC 的命令。您必須按照此順序使用這些命令。如果您已建立其他 VPC 資源，還需要先使用其對應的刪除命令，才能刪除 VPC。

使用 AWS CLI 刪除 VPC

1. 使用 delete-security-group 命令刪除您的安全群組。

```
aws ec2 delete-security-group --group-id sg-id
```

2. 使用 delete-network-acl 命令刪除每個網路 ACL。

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. 使用 delete-subnet 命令刪除每個子網路。

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. 使用 delete-route-table 命令刪除每個自訂路由表。

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. 使用 detach-internet-gateway 命令將網際網路閘道與 VPC 分離。

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. 使用 delete-internet-gateway 命令刪除網際網路閘道。

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [雙堆疊 VPC] 使用 delete-egress-only-internet-gateway 命令刪除輸出限定網際網路閘道。

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. 使用 delete-vpc 命令刪除 VPC。

```
aws ec2 delete-vpc --vpc-id vpc-id
```

使用 Console-to-Code，從 VPC 主控台操作產生基礎設施即程式碼

該主控台提供建立資源和測試原型的指導路徑。如果您想要大規模建立相同的資源，則需要自動化程式碼。Console-to-Code 是 Amazon Q Developer 的一項功能，可協助您開始使用自動化程式碼。Console-to-Code 會記錄您的主控台動作，包括預設值和相容參數。然後它會使用生成式 AI，以您偏好的基礎設施即程式碼 (IaC) 格式，為您想要的動作建議程式碼。由於主控台工作流程會確保您指定的參數值同時有效，因此您使用 Console-to-Code 產生的程式碼具有相容的參數值。您可以使用該程式碼作為起點，然後對其進行自訂以使其針對特定使用案例準備好投入生產。

例如，使用 Console-to-Code，您可以在 VPC 主控台中記錄建立子網路、安全群組、NACL、定製路由表和網際網路閘道的過程，並產生 CloudFormation JSON 格式的程式碼。然後，您可以複製該程式碼並進行自訂，以便在 CloudFormation 範本中使用。

Console-to-Code 目前可以使用下列語言和格式產生基礎設施即程式碼 (IaC)：

- CDK Java
- CDK Python
- CDK TypeScript
- CloudFormation JSON
- CloudFormation YAML

如需如何使用 Console-to-Code 的詳細資訊和指示，請參閱《Amazon Q Developer 使用者指南》中的使用 Amazon Q Developer Console-to-Code 自動化 AWS 服務。

您 VPC 的子網

子網是您的 VPC 中的 IP 地址範圍。您可以在特定子網路中建立 AWS 資源，例如 EC2 執行個體。

目錄

- 子網基本概念
- 子網安全
- 建立子網
- 從您的子網路中新增或移除 IPv6 CIDR 區塊
- 修改子網路的公有 IP 位址屬性
- 子網路 CIDR 保留
- 設定路由表
- 中間設備路由精靈
- 刪除子網路

子網基本概念

各個子網必須完全位於某一可用區域內，不得跨越多個區域。透過在個別可用區域中啟動 AWS 資源，您可以保護您的應用程式免於單一可用區域的故障。

目錄

- 子網路 IP 地址範圍
- 子網類型
- 子網圖表
- 子網路由
- 子網設定

子網路 IP 地址範圍

建立子網時，您要根據 VPC 的組態指定其 IP 地址：

- 僅 IPv4 – 該子網路具有 IPv4 CIDR 區塊，但沒有 IPv6 CIDR 區塊。僅 IPv4 子網中的資源必須透過 IPv4 進行通訊。

- 雙堆疊 – 該子網路具有 IPv4 CIDR 區塊和 IPv6 CIDR 區塊。VPC 必須具有 IPv4 CIDR 區塊和 IPv6 CIDR 區塊。雙堆疊子網中的資源可透過 IPv4 和 IPv6 進行通訊。
- 僅 IPv6 – 該子網路具有 IPv6 CIDR 區塊，但沒有 IPv4 CIDR 區塊。該 VPC 必須具有 IPv6 CIDR 區塊。僅 IPv6 子網中的資源必須透過 IPv6 進行通訊。

> **Note**
>
> 僅 IPV6 子網路中的資源會獲得從 CIDR 區塊 169.254.0.0/16 指派的 IPv4 連結本地位址。使用這些位址來與僅在 VPC 中使用的服務進行通訊。如需範例，請參閱《Amazon EC2 使用者指南》中的鏈結本端位址。

如需詳細資訊，請參閱您 VPC 和子網路的 IP 定址。

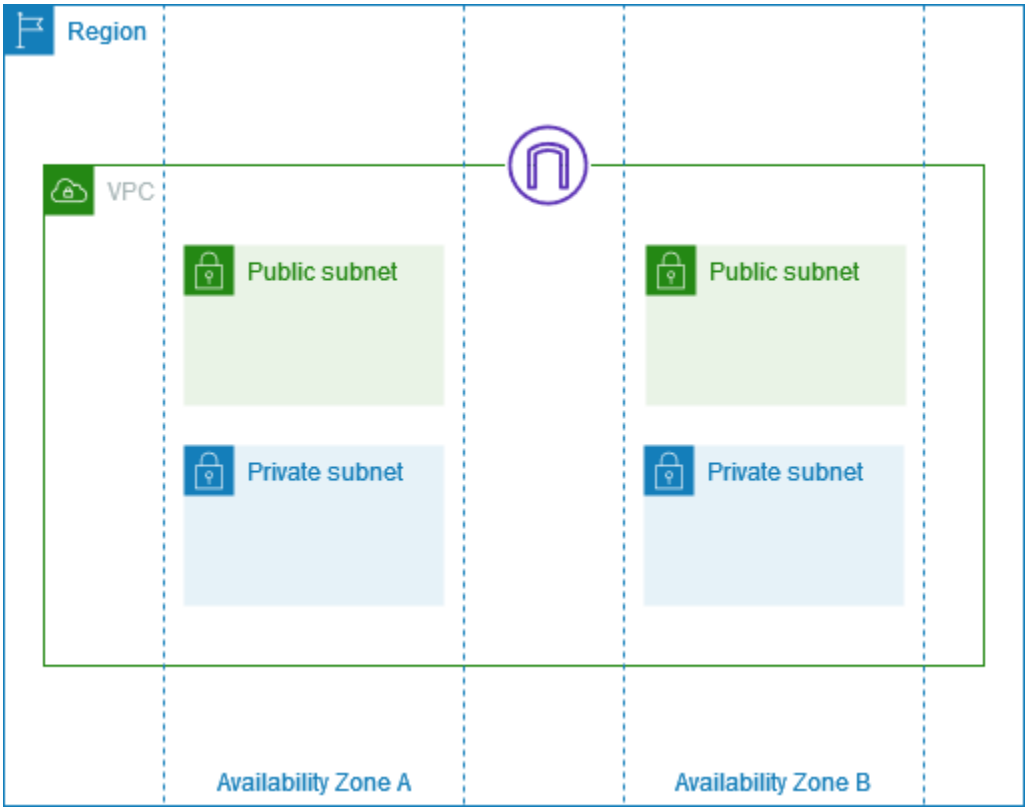
子網類型

子網路類型取決於您如何設定子網路的路由。例如：

- 公有子網路 – 子網路會直接路由至網際網路閘道。公有子網路中的資源可以存取公有網際網路。
- 私有子網路 – 此子網路不會直接路由至網際網路閘道。私有子網路中的資源需要 NAT 裝置才能存取公有網際網路。
- 僅 VPN 子網路 – 子網路會透過虛擬私有閘道路由至 Site-to-Site VPN 連線。子網路不會路由到網際網路閘道。
- 隔離子網路 — 子網路沒有其 VPC 外部目的地的路由。隔離子網路中的資源僅能進行存取，或讓相同 VPC 中的其他資源存取。
- EVS 子網路 – 此類型子網使用 Amazon EVS 建立。如需詳細資訊，請參閱《Amazon EVS 使用者指南》中的 VLAN 子網路。

子網圖表

下圖顯示顯示一個具有兩個可用區域子網路和一個網際網路閘道的 VPC。每個可用區域都有一個公用子網路和一個私有子網路。



如需在 Local Zones 和 Wavelength Zones 中顯示子網路的圖表，請參閱 AWS Local Zones 的運作方式和AWS Wavelength 運作方式。

子網路由

每個子網都必須具有關聯的路由表，指定離開子網之傳出流量的允許路由。每個您建立的子網都會自動與 VPC 的主路由表建立關聯。您可以變更關聯，也可以變更主路由表的內容。如需詳細資訊，請參閱設定路由表。

子網設定

所有子網都有可修改的屬性，決定在該子網中建立的網路界面是否獲派公有 IPv4 地址及 IPv6 地址 (若適用的話)。這包含您在該子網路中啟動執行個體時，為執行個體建立的主要網路介面 (例如 eth0)。無論子網的屬性為何，您仍然可以在啟動時覆寫特定執行個體的此設定。

建立子網路之後，您就可以修改子網路的下列設定。

- 自動指派 IP 設定：可讓您調整自動指派 IP 設定以自動要求此子網中的新網路介面的公有 IPv4 或 IPv6 地址。

- 以資源為基礎的名稱 (RBN) 設定：可讓您指定此子網中 EC2 執行個體的主機名稱類型，以及設定 DNS A 和 AAAA 記錄查詢的處理方式。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體主機名稱類型。

子網安全

為了保護您的 AWS 資源，我們建議您使用私有子網路。使用堡壘託管或 NAT 裝置，以提供網際網路存取權限給私有子網路中的資源 (例如 EC2 執行執行個體)。

AWS 提供您可以用來提高 VPC 中資源安全性的功能。安全群組會允許關聯資源 (例如 EC2 執行個體) 的傳入和傳出流量。網路 ACL 會允許或拒絕子網路層級的傳入和傳出流量。在大多數情況下，安全群組可以滿足您的需求。但是，如果您想多一層安全，可以使用網路 ACL。如需詳細資訊，請參閱the section called “比較安全群組和網路 ACL”。

根據設計，每個子網都必須與一個網路 ACL 相關聯。每個您建立的子網都會自動與 VPC 的預設網路 ACL 建立關聯。預設的網路 ACL 會允許所有外傳和傳入流量。您可以更新預設的網路 ACL，或建立自訂網路 ACL，並將其和您的子網路建立關聯。如需詳細資訊，請參閱使用網路存取控制清單控制子網路流量。

您可以在您的 VPC 或子網上建立流程日誌，以擷取流入或流出您 VPC 或子網中網路界面的流量。您也可以在個別網路界面上建立流程日誌。如需詳細資訊，請參閱使用 VPC 流量日誌來記錄 IP 流量。

建立子網

使用下列步驟為您的虛擬私有雲端 (VPC) 建立子網路。視您所需要的連線能力而定，您可能也需要新增閘道和路由表。

考量事項

- 您必須在 VPC 範圍內指定子網路的 IPv4 CIDR 區塊。若 VPC 有關聯的 IPv6 CIDR 區塊，則您可以選擇性地為子網路指定 IPv6 CIDR 區塊。如需更多詳細資訊，請參閱 您 VPC 和子網路的 IP 定址。
- 如果您建立僅限 IPv6 子網路，請注意以下內容。在僅限 IPv6 之子網路中啟動的 EC2 執行個體會收到 IPv6 地址，而非 IPv4 地址。您在僅限 IPv6 子網路中啟動的任何執行個體，都必須是在 Nitro 系統上建置的執行個體。
- 若要在本機區域或 Wavelength 區域中建立子網路，您必須啟用「區域」。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的區域 (Region) 和區域 (Zone)。

將子網新增至 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選擇 Create subnet (建立子網路)。
4. 在 VPC ID 下，選擇子網路的 VPC。
5. (選用) 對於 Subnet name (子網路名稱)，輸入您的子網路的名稱。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。
6. 對於 Availability Zone (可用區域)，您可以選擇子網路的區域，或保留預設的 No Preference (無偏好設定)，以便讓 AWS 為您選擇。
7. 對於 IPv4 CIDR block (IPv4 CIDR 區塊)，選取 Manual input (手動輸入)，為子網路 (例如 `10.0.1.0/24`) 輸入 IPv4 CIDR 區塊，或選取 No IPv4 CIDR (無 IPv4 CIDR)。如果使用 Amazon VPC IP 位址管理器 (IPAM) 規劃、追蹤和監控 AWS 工作負載的 IP 地址，則在建立子網路時，您可以選擇從 IPAM (IPAM 配置) 配置 CIDR 區塊。如需為子網路 IP 配置規劃 VPC IP 地址空間的詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
8. 對於 IPv6 CIDR block (IPv6 CIDR 區塊)，選取 Manual input (手動輸入)，以選擇要在其中建立子網路的 VPC IPv6 CIDR。此選項唯有在 VPC 具有關聯的 IPv6 CIDR 區塊時才可用。如果使用 Amazon VPC IP 位址管理器 (IPAM) 規劃、追蹤和監控 AWS 工作負載的 IP 地址，則在建立子網路時，您可以選擇從 IPAM (IPAM 配置) 配置 CIDR 區塊。如需為子網路 IP 配置規劃 VPC IP 地址空間的詳細資訊，請參閱《Amazon VPC IPAM 使用者指南》中的教學課程：為子網路 IP 配置規劃 VPC IP 地址空間。
9. 選擇 IPv6 VPC CIDR block (IPv6 VPC CIDR 區塊)。
10. 對於 IPv6 subnet CIDR block (IPv6 子網路 CIDR 區塊)，為等於 VPC CIDR 或比其更為具體的子網路選擇 CIDR。例如，如果 VPC 集區 CIDR 是 /50，您可以為子網路選擇介於 /50 至 /64 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /64 之間 (增量為 /4)。
11. 選擇 Create subnet (建立子網路)。

如何使用 AWS CLI 將子網路新增至您的 VPC

使用 create-subnet 命令。

後續步驟

建立子網路後，您可以按如下方式對其設定：

- 設定路由。然後，您可以建立自訂路由表，以及將流量傳送至與 VPC 關聯的閘道 (如網際網路閘道) 的路由。如需更多詳細資訊，請參閱 設定路由表。
- 修改 IP 地址行為。您可以指定在該子網路中啟動的執行個體是接收公有 IPv4 地址、IPv6 地址，還是兩者。如需更多詳細資訊，請參閱 修改子網路的公有 IP 位址屬性。
- 修改以資源為基礎的名稱 (RBN) 設定。如需詳細資訊，請參閱「Amazon EC2 執行個體主機名稱類型」。
- 建立或修改您的網路 ACL。如需更多詳細資訊，請參閱 使用網路存取控制清單控制子網路流量。
- 與其他帳戶共享子網路。如需更多詳細資訊，請參閱 ???。

從您的子網路中新增或移除 IPv6 CIDR 區塊

您可以建立 IPv6 CIDR 區塊與您 VPC 中現有子網路的關聯。子網路不可擁有任何已和其相關聯的現有 IPv6 CIDR 區塊。

若您不再希望您的子網路支援 IPv6，但您想要繼續使用您的子網路建立 IPv4 資源並與之通訊，您可以移除 IPv6 CIDR 區塊。

您必須先取消指派任何已指派給您子網路中任何執行個體的 IPv6 地址，才能移除 IPv6 CIDR 區塊。

如何在子網路中新增或移除 IPv6 CIDR 區塊

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選取您的子網路，然後選擇 Actions (動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 若要新增 CIDR，選擇 新增 IPv6 CIDR 選擇 VPC CIDR 區塊，輸入 子網路 CIDR 區塊，然後選擇等於 VPC CIDR 網路遮罩長度或其更為具體的網路遮罩長度。例如，如果 VPC 集區 CIDR 是 /50，您可以為子網路選擇介於 /50 至 /64 之間的網路遮罩長度。可能的 IPv6 網路遮罩長度介於 /44 和 /64 之間 (增量為 /4)。
5. 若要移除 CIDR，尋找 IPv6 CIDR 區塊，然後選擇 移除。
6. 選擇儲存。

使用 AWS CLI 建立 IPv6 CIDR 區塊與子網路的關聯

使用 associate-subnet-cidr-block 命令。

使用 AWS CLI 取消 IPv6 CIDR 區塊與子網路的關聯

使用 disassociate-subnet-cidr-block 命令。

修改子網路的公有 IP 位址屬性

根據預設，非預設子網路會將 IPv4 公有定址屬性設為 `false`，而預設子網路會將此屬性設為 `true`。其中一個例外為由 Amazon EC2 啟動執行個體精靈建立的非預設子網路 – 精靈會將屬性設為 `true`。您可以使用 Amazon VPC 主控台來修改此屬性。

根據預設，所有子網路皆會將 IPv6 定址屬性設為 `false`。您可以使用 Amazon VPC 主控台來修改此屬性。若您為您的子網路啟用 IPv6 定址屬性，在子網路中建立的網路界面都會從子網路範圍收到 IPv6 地址。在子網路中啟動的執行個體都會在主要網路界面上收到 IPv6 地址。

您的子網路必須具有關聯的 IPv6 CIDR 區塊。

> **Note**
>
> 若您啟用您子網路的 IPv6 定址功能，您的網路介面或執行個體只會在其使用 `2016-11-15` 版本或更新版本的 Amazon EC2 API 建立時接收到 IPv6 地址。Amazon EC2 主控台使用最新的 API 版本。

修改子網路的公有 IP 位址行為

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選取您的子網路，然後選擇 Actions (動作)、Edit subnet settings (編輯子網路設定)。
4. Enable auto-assign public IPv4 address (啟用自動指派公有 IPv4 地址) 核取方塊若處於選取狀態，便會為所有在選取子網路中啟動的執行個體請求公有 IPv4 地址。視需要選取或清除選取方塊，然後選擇 Save (儲存)。
5. Enable auto-assign IPv6 address (啟用自動指派 IPv6 地址) 核取方塊若處於選取狀態，便會為所有在選取子網路中啟動的執行個體請求 IPv6 地址。視需要選取或清除選取方塊，然後選擇 Save (儲存)。

如何使用 AWS CLI 修改子網路屬性

使用 modify-subnet-attribute 命令。

子網路 CIDR 保留

子網路 CIDR 保留是您預留的 IPv4 或 IPv6 位址範圍，AWS 無法將其指派給網路介面。這可讓您保留 IPv4 或 IPv6 CIDR 區塊 (也稱為「字首」)，以便與網路介面搭配使用。

建立子網 CIDR 保留時，您需要指定使用保留 IP 地址的方式。以下是可用的選項：

- 字首 – 允許將字首指派給單一網路介面。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的為 Amazon EC2 網路界面指派字首。
- 明確 – 允許手動將個別 IP 位址指派給單一網路介面。

下列規則適用於子網路 CIDR 保留：

- 當您建立子網 CIDR 保留時，IP 地址範圍可包含已在使用中的地址。建立子網保留不會取消指派任何已在使用中的 IP 地址。
- 您可以為每個子網路保留多個 CIDR 範圍。當您在同一 VPC 內保留多個 CIDR 範圍時，這些 CIDR 範圍不能重疊。
- 當您在子網中保留多個範圍進行字首委派，且字首委派設定為自動指派時，我們會隨機選擇要指派至網路介面的 IP 地址。
- 刪除子網保留時，未使用的 IP 地址可供 AWS 用來指派至您的網路介面。刪除子網保留不會取消指派任何已在使用中的 IP 地址。
- 保留類型會影響子網路的可用 IP 位址數量。如果建立字首保留，數量會立即減少。如果建立明確的字首保留，數量會在指派 IP 位址時減少。

如需有關無類別域間路由 (CIDR) 表示法的詳細資訊，請參閱 IP 定址。

目錄

- 透過主控台使用子網路 CIDR 保留
- 透過 AWS CLI 使用子網路 CIDR 保留

透過主控台使用子網路 CIDR 保留

您可以建立並管理子網路 CIDR 保留，如下所示。

若要編輯子網路 CIDR 保留

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選擇子網路。
4. 選擇 CIDR reservations (CIDR 保留) 索引標籤以取得任何現有子網路 CIDR 保留的相關資訊。
5. 若要新增或移除子網路 CIDR 保留，請依序選擇 Actions (動作) 和 Edit CIDR reservations (編輯 CIDR 保留)，然後執行以下操作：
   - 若要新增 IPv4 CIDR 保留，請選擇 IPv4、Add IPv4 CIDR reservation (新增 IPv4 CIDR 保留)。選擇保留類型，輸入 CIDR 範圍，然後選擇 Add (新增)。
   - 若要新增 IPv6 CIDR 保留，請選擇 IPv6、Add IPv6 CIDR reservation (新增 IPv6 CIDR 保留)。選擇保留類型，輸入 CIDR 範圍，然後選擇 Add (新增)。
   - 若要移除 CIDR 保留，請針對子網路 CIDR 保留選擇 Remove (移除)。

透過 AWS CLI 使用子網路 CIDR 保留

您可以使用 AWS CLI 來建立並管理子網路 CIDR 保留。

任務

- 建立子網路 CIDR 保留
- 檢視子網路 CIDR 保留
- 刪除子網路 CIDR 保留

建立子網路 CIDR 保留

您可以使用 create-subnet-cidr-reservation 來建立子網路 CIDR 保留。

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

下列為範例輸出。

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
```

```
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
}
```

檢視子網路 CIDR 保留

您可以使用 get-subnet-cidr-reservations 來檢視子網路 CIDR 保留的詳細資訊。

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

刪除子網路 CIDR 保留

您可以使用 delete-subnet-cidr-reservation 來刪除子網路 CIDR 保留。

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

設定路由表

路由表可作為虛擬私有雲端 (VPC) 的流量控制器。每個路由表皆包含一組名為路由的規則，可決定來自子網路或閘道之網路流量的方向。在您建立 VPC 時，我們也會建立 VPC 的主要路由表。您可以為 VPC 建立額外的路由表，從而對 VPC 的網路路徑實現更精細的控制。

您可以使用路由表來指定 VPC 可與哪些網路通訊，例如其他 VPC 或內部部署網路。每個路由皆會指定目的地 (CIDR 區塊或字首清單) 與目標 (例如網際網路閘道、NAT 閘道、VPC 對等互連或 VPN 連線)。流量會根據目的地 IP 位址路由至目標。您可以透過路由表建立包含公有子網路、私有子網路、僅限 VPN 的子網路與隔離子網路的複雜網路架構。

目錄

- 路由表概念
- 子網路由表
- 閘道路由表
- 路由優先順序的運作方式
- 路由選項範例

- 建立 VPC 的路由表
- 管理子網路路由表
- 取代主路由表
- 透過閘道路由表控制進入 VPC 的流量
- 取代或還原本機路由的目標
- VPC 中的進階路由
- 對 VPC 中的連線能力問題進行疑難排解

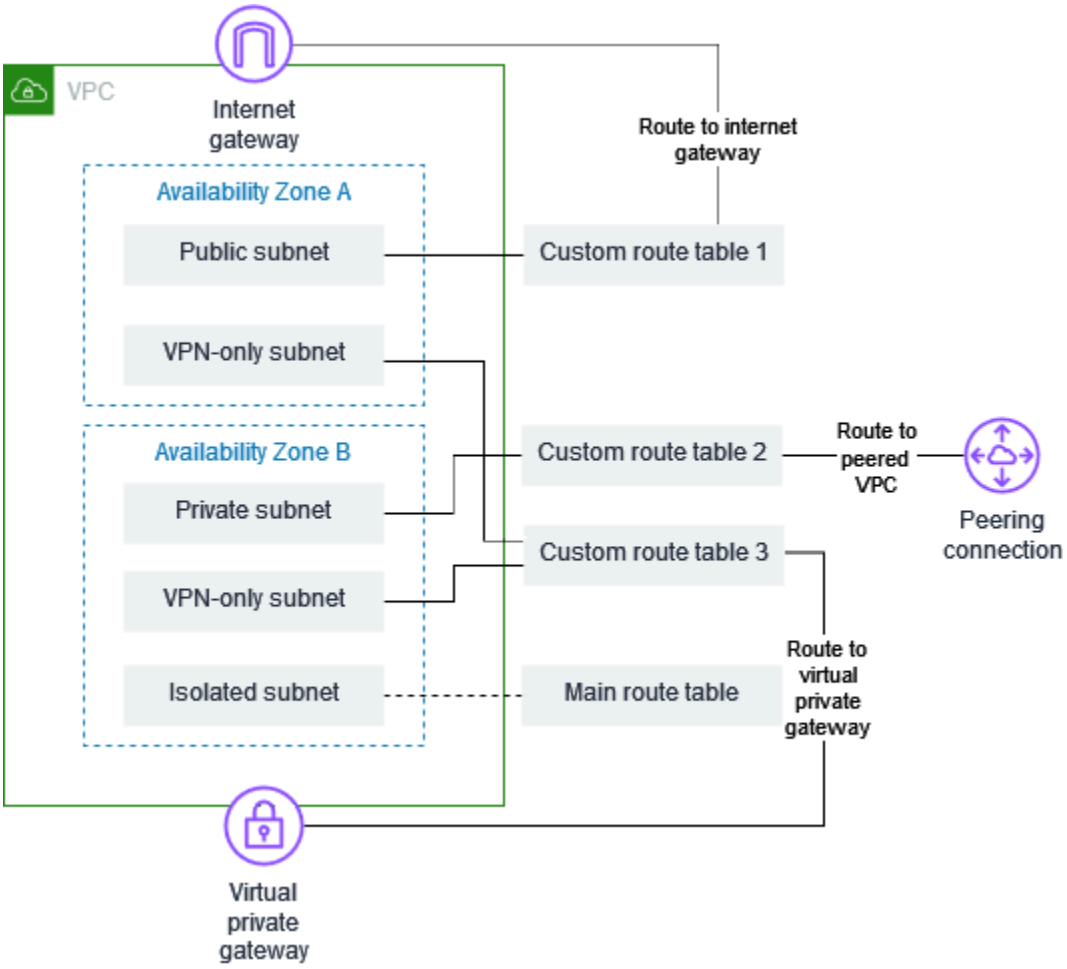
路由表概念

以下是路由表的重要概念：

- 主路由表 — 自動隨附於 VPC 的路由表。它會控制所有並未與任何其他路由表明確建立關聯之子網的路由。
- 自訂路由表 — 您為 VPC 建立的路由表。
- 目的地 — 您想要流量傳送的 IP 地址範圍 (目的地 CIDR)。例如，具有 CIDR `172.16.0.0/12` 的外部公司網路。
- 目標 — 要透過其傳送目的地流量的閘道、網路介面或連線；例如，網際網路閘道。
- 本機路由 — VPC 內用於通訊的預設路由。若 VPC 同時具備 IPv4 與 IPv6 位址，則會存在一條 IPv4 本機路由與一條 IPv6 本機路由。
- 路由表關聯 — 路由表與子網、網際網路閘道或虛擬私有閘道之間的關聯。
- 子網路由表 — 與子網相關聯的路由表。
- 傳播 – 若已將虛擬私有閘道連接至 VPC 並啟用路由傳播，則我們會自動將 VPN 連線的路由新增至子網路路由表。這表示您無需手動新增或移除 VPN 路由。如需詳細資訊，請參閱 Site-to-Site VPN 使用者指南中的 Site-to-Site VPN 路由選項。
- 閘道路由表 — 與網際網路閘道或虛擬私有閘道相關聯的路由表。
- 邊緣關聯 — 您用來將傳入 VPC 流量路由至設備的路由表。您可以將路由表與網際網路閘道或虛擬私有閘道建立關聯，並且將您設備的網路界面指定為 VPC 流量的目標。
- Transit Gateway 路由表 — 與 Transit Gateway 關聯的路由表。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的傳輸閘道路由表。
- 本機閘道路由表 — 與 Outposts 本機閘道相關聯的路由表。如需詳細資訊，請參閱《AWS Outposts 使用者指南》中的本機閘道。

VPC 路由表架構範例

下圖展示了一個包含五個子網路、一個主路由表及三個自訂路由表的 VPC。這四個路由表皆包含本機路由。自訂路由表 1 設有通往網際網路閘道的路由，且與可用區域 A 中的公有子網路關聯。自訂路由表 2 設有通往對等 VPC 的路由，且與可用區域 B 中的私有子網路關聯。自訂路由表 3 設有通往虛擬私有閘道的路由，且同時與兩個可用區域中的僅限 VPN 子網路關聯。



子網路由表

您的 VPC 具有隱含路由器，並且您可以使用路由表，來控制網路流量的方向。您 VPC 中的每個子網都必須與路由表相關聯，此路由表會控制子網的路由 (子網路由表)。您可以明確地將子網與特定路由表建立關聯。否則，子網會隱含地與主路由表相關聯。子網只能一次與一個路由表建立關聯，但您可以將多個子網與相同的子網路由表建立關聯。

目錄

- 路由
- 主路由表

- 自訂路由表
- 子網路由表關聯

路由

路由表中的每個路由都會指定一個目的地和一個目標。例如，若要讓子網能夠透過網際網路閘道存取網際網路，請將下列路由新增至子網路由表。路由的目的地是 `0.0.0.0/0`，它代表所有的 IPv4 地址。目標是連接到 VPC 的網際網路閘道。

目標	目標
0.0.0.0/0	*igw-id*

IPv4 和 IPv6 的 CIDR 區塊會分開處理。例如，目的地 CIDR 為 `0.0.0.0/0` 的路由不會自動包含所有 IPv6 地址。您必須為所有 IPv6 地址建立目的地 CIDR 為 `::/0` 的路由。

如果您經常在 AWS 資源中參考相同的一組 CIDR 區塊，您可以建立客戶受管字首清單，將它們分組在一起。然後，您可以將字首清單指定為路由表項目中的目的地。

每個路由表都包含一個用於在 VPC 內進行通訊的本機路由。此路由預設為新增至所有路由表。若您的 VPC 有超過一個 IPv4 CIDR 區塊，您的路由表便會包含每個 IPv4 CIDR 區塊的本機路由。若您將 IPv6 CIDR 區塊與您的 VPC 建立關聯，您的路由表便會包含 IPv6 CIDR 區塊的本機路由。您可以視需要取代或還原每個本機路由的目標。

規則和考量

- 您可以新增路由至比本機路由更具體的路由表。目的地必須符合 VPC 中子網的整個 IPv4 或 IPv6 CIDR 區塊。目標必須是 NAT 閘道、網路介面或閘道負載平衡器端點。
- 如果您的路由表具有多個路由，我們會使用最具體且符合流量的路由 (最長的字首相符)，從而判斷如何路由流量。
- 無法將路由新增至完全相符的 IPv4 地址或以下範圍的子集：169.254.168.0/22。此範圍位於連結本機地址空間內，並保留供 AWS 服務使用。例如，Amazon EC2 將此範圍內的地址用於只能透過 EC2 執行個體存取的服務，如執行個體中繼資料服務 (IMDS) 和 Amazon DNS 伺服器。您可以使用大於但與 169.254.168.0/22 重疊的 CIDR 區塊，但不會轉傳至指定於 169.254.168.0/22 中地址的封包。
- 無法將路由新增至完全相符的 IPv6 地址或以下範圍的子集：fd00:ec2::/32。此範圍位於唯一的本機地址 (ULA) 空間內，並保留供 AWS 服務使用。例如，Amazon EC2 將此範圍內的地址用於只能透

過 EC2 執行個體存取的服務，如執行個體中繼資料服務 (IMDS) 和 Amazon DNS 伺服器。您可以使用大於但與 fd00:ec2::/32 重疊的 CIDR 區塊，但不會轉傳至指定於 fd00:ec2::/32 中地址的封包。

- 您可以將中間設備新增至 VPC 的路由路徑。如需詳細資訊，請參閱the section called “中間設備的路由”。

範例

在下列範例中，假設 VPC 具有 IPv4 CIDR 區塊以及 IPv6 CIDR 區塊。IPv4 和 IPv6 流量會分開處理，如下列路由表所示。

目標	目標
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- Local 路由涵蓋要在 VPC (10.0.0.0/16) 內路由的 IPv4 流量。
- Local 路由涵蓋要在 VPC (2001:db8:1234:1a00::/56) 內路由的 IPv6 流量。
- 172.31.0.0/16 的路由會將流量傳送至對等連線。
- 所有 IPv4 流量 (0.0.0.0/0) 的路由會將流量傳送至網際網路閘道。因此，除了 VPC 內和傳送到對等連線的流量，所有 IPv4 流量都會路由至網際網路閘道。
- 所有 IPv6 流量 (::/0) 的路由會將流量傳送至輸出限定網際網路閘道。因此，除了 VPC 內的流量，所有 IPv6 流量都會路由至輸出限定網際網路閘道。

主路由表

當您建立 VPC 時，便會自動隨附一個主路由表。當子網未擁有與之關聯的明確路由表，則會根據預設使用主路由表。在 Amazon VPC 主控台中的 Route Tables (路由表) 頁面上，您可以透過尋找 Main (主要) 資料行中的 Yes (是)，檢視 VPC 的主路由表。

依預設，當您建立非預設 VPC 時，主路由表僅包含本機路由。如果您 建立 VPC 並選擇 NAT 閘道，Amazon VPC 會自動將路由新增至閘道的主路由表。

下列規則會套用至主路由表：

- 您可以新增、移除和修改主路由表中的路由。
- 但無法刪除主路由表。
- 您無法將閘道路由表設定為主路由表。
- 您可以透過將自訂路由表與子網路建立關聯來取代主路由表。
- 您可以明確將子網與主路由表建立關聯，即使其已經隱含地建立關聯。

  如果您變更哪個路由表是主路由表，則可能想這樣做。當您變更哪個路由表是主路由表時，它也會變更其他新的子網，或是任何尚未與其他路由表明確建立關聯之子網的預設值。如需詳細資訊，請參閱取代主路由表。

自訂路由表

依預設，每個路由表都包含一個用於在 VPC 內進行通訊的本機路由。如果您 建立 VPC 並選擇公有子網，Amazon VPC 會建立自訂路由表，並將路由新增至網際網路閘道。保護 VPC 的一種方法是將主路由表保留在原始的預設狀態。然後，明確地將您建立的每個新子網與您已建立的其中一個自訂路由表建立關聯。這可確保您明確控制每個子網路由流量的方式。

您可以新增、移除和修改自訂路由表中的路由。僅當自訂路由表格沒有關聯時，才可以刪除它。

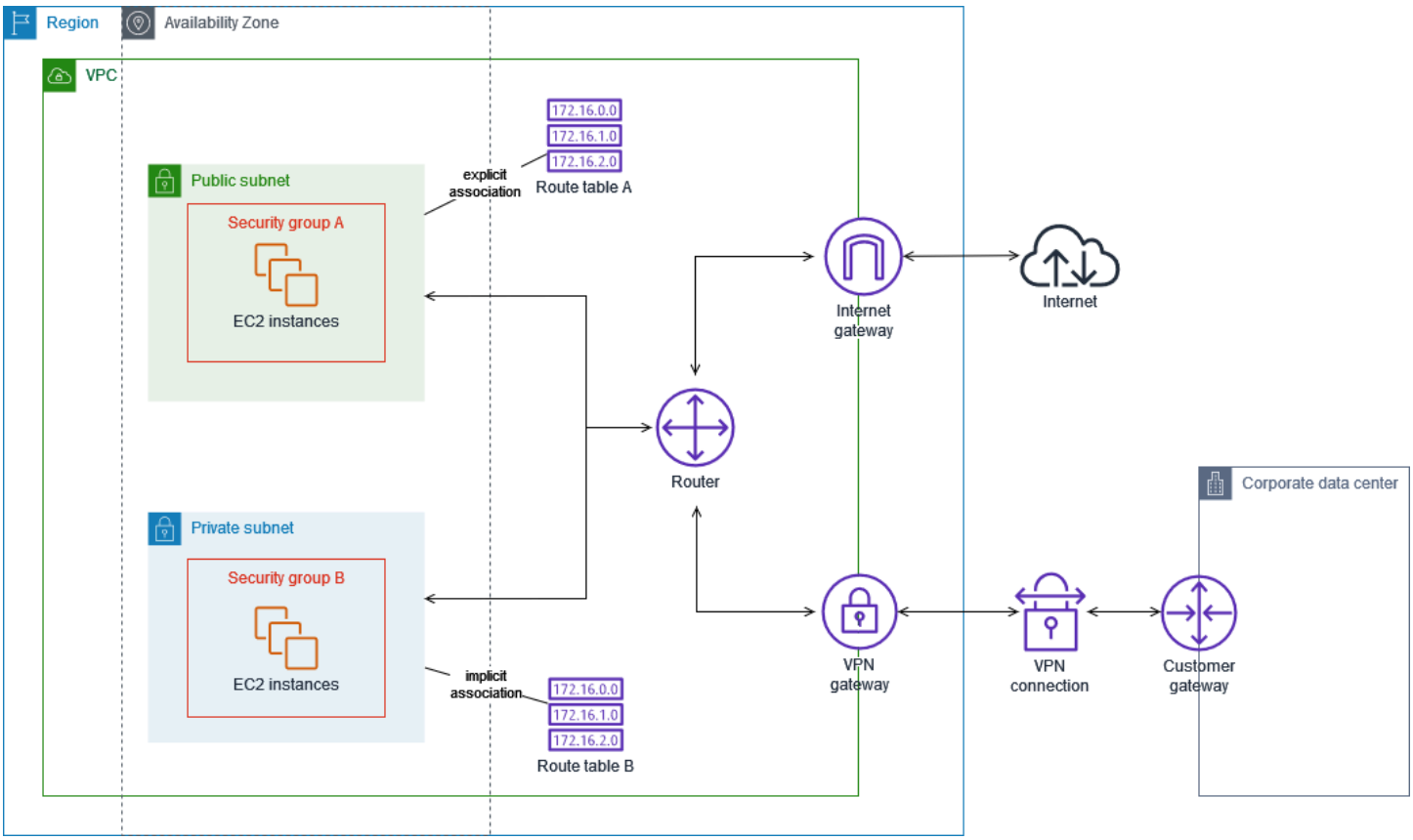
子網路由表關聯

VPC 中的每個子網都必須與路由表建立關聯。子網可以明確地與自訂路由表相關聯，或者隱含或明確地與主路由表相關聯。如需檢視子網和路由表關聯的詳細資訊，請參閱確定明確的關聯關係。

位於與 Outposts 相關聯之 VPC 中的子網可有額外目標類型的本機閘道。這是與非 Outposts 子網的唯一路由差異。

範例 1：隱含和明確的子網關聯

下表顯示具有網際網路閘道、虛擬私有閘道、公有子網路和僅 VPN 子網路的 VPC 路由。



路由表 A 是自訂路由表，明確地與公有子網路關聯。該路由表具有將所有流量傳送至網際網路閘道的路由，這就能讓子網路成為公有子網路。

目標	Target
VPC CIDR	區域
0.0.0.0/0	*igw-id*

路由表 B 是主路由表，隱含地與私有子網路相關聯。該路表具有將所有流量傳送至虛擬私有閘道的路由，但不具有將所有流量傳送至網際網路閘道的路由，這就能讓子網路成為僅 VPN 子網路。如果您在此 VPC 中建立另一個子網路，但未建立與自訂路由表的關聯，則子網路也會隱含地與此路由表相關聯，因為此表是主路由表。

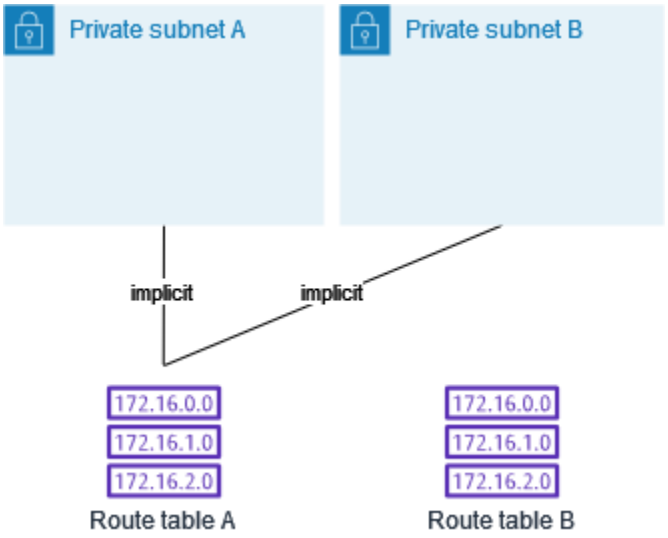
目標	Target
VPC CIDR	區域

目標	Target
0.0.0.0/0	*vgw-id*

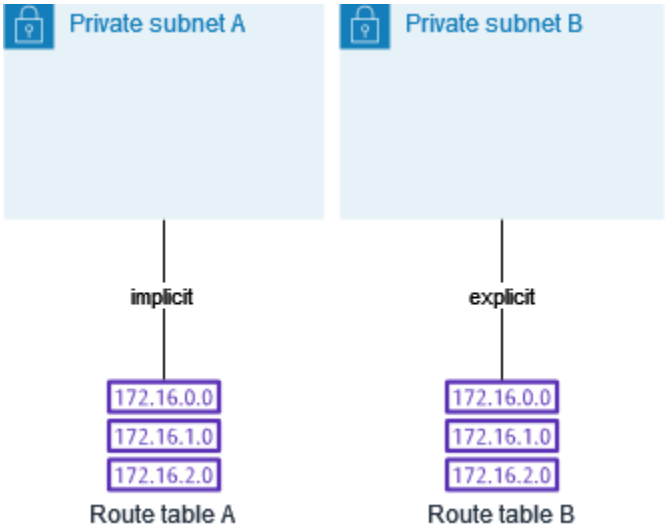
範例 2：取代主路由表

您可能想要對主路由表進行變更。若要避免任何流量中斷，建議您先使用自訂路由表來測試這些路由變更。在您滿意測試之後，便可以使用新的自訂表取代主路由表。

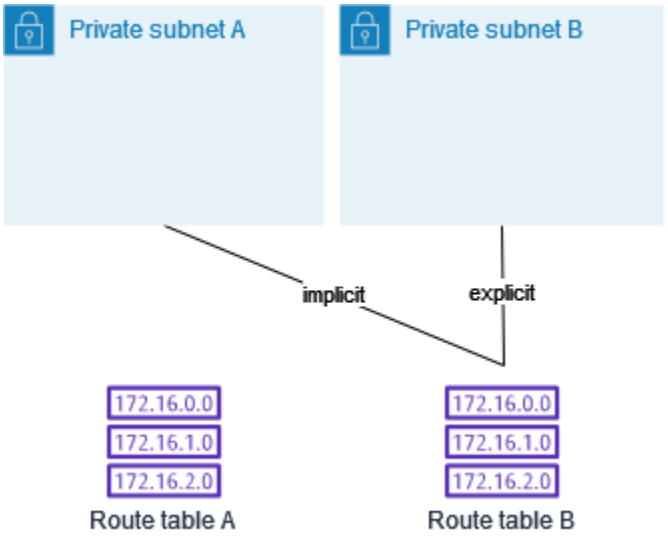
下圖顯示兩個子網路和兩個路由表。子網路 A 隱含地與路由表 A (主路由表) 相關聯。子網路 B 隱含地與路由表 A 相關聯。路由表 B (自訂路由表格) 並未與任何一個子網路相關聯。



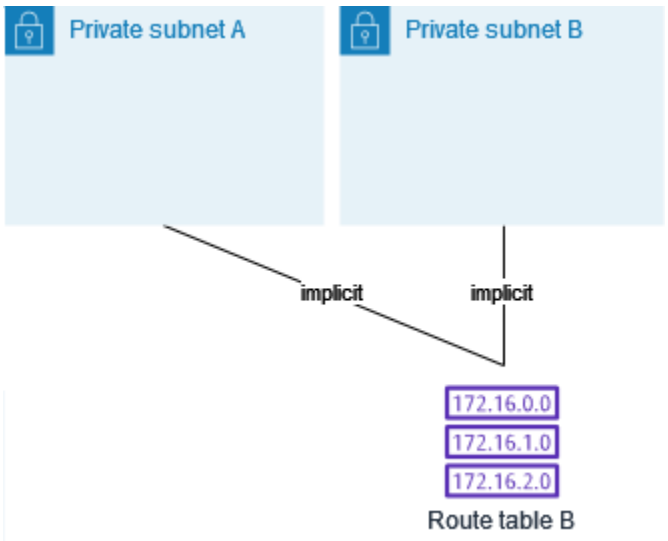
若要取代主路由表，請先在子網路 B 和路由表 B 之間建立明確關聯。然後測試路由表 B。



在測試路由表 B 之後，您可以將之設為主路由表。子網路 B 仍與路由表 B 具有明確關聯。但是，子網路 A 現在與路由表 B 具有隱含關聯，因為路由表 B 為新的主路由表。路由表 A 不再與任何一個子網路相關聯。



(選用) 若您取消子網路 B 與路由表 B 的關聯，子網路 B 和路由表 B 之間仍然具有隱含關聯。若不再需要路由表 A，您可以將其刪除。



閘道路由表

您可以將路由表與網際網路閘道或虛擬私有閘道建立關聯。當路由表與閘道相關聯時，它稱為閘道路由表。您可以建立閘道路由表，以精細控制進入 VPC 的流量路由路徑。例如，您可以透過網際網路閘道攔截進入 VPC 的流量，方法是將該流量重新導向至 VPC 中的中間設備 (例如安全設備)。

目錄

- 閘道路由表路由
- 規則和考量

閘道路由表路由

與網際網路閘道相關聯的閘道路由表可支援具有下列目標的路由：

- 預設的本機路由
- 閘道負載平衡器端點
- 中間設備的網路界面

與虛擬私有閘道相關聯的閘道路由表可支援具有下列目標的路由：

- 預設的本機路由
- 閘道負載平衡器端點
- 中間設備的網路界面

當目標是閘道負載平衡器端點或網路界面時，允許下列目的地：

- VPC 的整個 IPv4 或 IPv6 CIDR 區塊。在此情況下，您可以取代預設本機路由的目標。
- VPC 中子網的整個 IPv4 或 IPv6 CIDR 區塊。這是比預設本機路由更具體的路由。

如果您將閘道路由表中的本機路由目標變更為 VPC 中的網路界面，您可以稍後將其還原為預設 `local` 目標。如需詳細資訊，請參閱取代或還原本機路由的目標。

範例

在下列閘道路由表中，前往具有 `172.31.0.0/20` CIDR 區塊之子網的流量會路由至特定網路介面。前往 VPC 中所有其他子網的流量會使用本機路由。

目的地	目標
172.31.0.0/16	區域
172.31.0.0/20	*eni-id*

範例

在下列閘道路由表中，本機路由的目標會取代為網路界面 ID。前往 VPC 內所有子網的流量會路由至網路界面。

目的地	目標
172.31.0.0/16	*eni-id*

規則和考量

如果下列任一種情況適用，您就無法將路由表與閘道建立關聯：

- 路由表包含具有網路界面、閘道負載平衡器端點或預設本機路由以外目標的現有路由。
- 路由表包含 VPC 範圍外 CIDR 區塊的現有路由。
- 路由表會啟用路由傳播。

此外，下列規則和考量也適用：

- 您無法將路由新增至 VPC 範圍之外的任何 CIDR 區塊，包括大於個別 VPC CIDR 區塊的範圍。
- 您只能將 `local`、閘道負載平衡器端點或網路界面指定為目標。您無法指定任何其他類型的目標，包括個別主機 IP 地址。如需詳細資訊，請參閱the section called “路由選項範例”。
- 您無法將字首清單指定為目的地。
- 您無法使用閘道路由表來控制或攔截 VPC 外的流量，例如通過連接之傳輸閘道的流量。您可以攔截進入 VPC 的流量，並僅將其重新導向至相同 VPC 中的另一個目標。
- 為了確保流量到達您的中間設備，目標網路界面必須連接到執行中的執行個體。對於流經網際網路閘道的流量，目標網路介面也必須具有公有 IP 地址。
- 設定中間設備時，請注意設備的考量。
- 當您透過中間設備路由流量時，來自目的地子網的傳回流量的路由方式必須透過相同的設備。不支援非對稱路由。
- 路由表規則適用於離開子網的所有流量。離開子網的流量會被定義為目的地為該子網閘道路由器之 MAC 地址的流量。目的地為子網中另一個網路界面的 MAC 地址的流量會使用資料連結 (第 2 層) 路由，而非網路 (第 3 層)，因此規則不會套用至此流量。
- 並非所有 Local Zones 都支援與虛擬私有閘道有邊緣關聯。如需有關可用區域的詳細資訊，請參閱《AWS Local Zones 使用者指南》中的考量事項。

路由優先順序的運作方式

一般而言，我們會使用符合流量的最具體路由來引導流量。這就是所謂的最長字首相符。如果您的路由表有重疊或相符的路由，則會套用其他規則。

下列清單顯示路由優先順序摘要，並附有連結至下方各節，這些部分包含更詳細的資訊和範例：

1. 最長字首 (例如，10.10.2.15/32 優先於 10.10.2.0/24)
2. 靜態路由 (例如，VPC 對等互連和網際網路閘道連線)
3. 字首清單路由
4. 傳播路由
   a. Direct Connect BGP 路由 (動態路由)
   b. VPN 靜態路由
   c. VPN BGP 路由 (動態路由) (例如，虛擬私有閘道)

最長字首相符

IPv4 和 IPv6 地址或 CIDR 塊的路由彼此獨立。我們會使用最具體且符合 IPv4 流量或 IPv6 流量的路由，從而判斷如何路由流量。

下列範例子網路由表具有適用於 IPv4 網際網路流量 (`0.0.0.0/0`)，指向網際網路閘道的路由，以及適用於 `172.31.0.0/16` IPv4 流量，指向對等連線 (`pcx-11223344556677889`) 的路由。任何來自子網，前往 `172.31.0.0/16` IP 地址範圍的流量都會使用對等連線，因為這個路由比起網際網路閘道的路由更為具體。任何目標在 VPC (`10.0.0.0/16`) 內的流量都會涵蓋於 `local` 路由之中，因此會在 VPC 內路由。任何來自子網的其他流量都會使用網際網路閘道。

目的地	目標
10.0.0.0/16	本機
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

靜態和動態傳播路由的路由優先順序

若您已將虛擬私有閘道連線至您的 VPC，並在您的子網路由表上啟用路由傳播，則代表您 Site-to-Site VPN 連線的路由會自動做為廣播路由，在您的路由表中出現。

如果傳播路由的目的地與靜態路由的目的地相同，則靜態路由優先：下列資源使用靜態路由：

- 網際網路閘道
- NAT 閘道
- 網路界面
- 執行個體 ID
- 閘道 VPC 端點
- Transit Gateway
- VPC 對等連線
- 閘道負載平衡器端點

如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的路由表和 VPN 路由優先順序。

下列範例路由表具有連向網際網路閘道的靜態路由，以及連向虛擬私有閘道的傳播路由。兩種路由的目標都是 `172.31.0.0/24`。由於通往網際網路閘道的靜態路由優先，因此目的地為 `172.31.0.0/24` 的所有流量會路由至網際網路閘道。

目標	Target	已傳播
10.0.0.0/16	本機	否
172.31.0.0/24	vgw-11223344556677889	是
172.31.0.0/24	igw-12345678901234567	否

字首清單的路由優先順序

如果您的路由表參考字首清單，則適用下列規則：

- 如果您的路由表包含與參考字首清單之路由一致的傳播路由，則參考字首清單的路由優先。請注意，對於重疊的路由，更具體的路由始終優先，無論其是傳播路由、靜態路由還是引用字首清單的路由。

- 如果您的路由表參考多個字首清單，這些清單具有目標不同的重疊 CIDR 區塊，我們會隨機選擇任一路由優先順序。此後，相同的路由一律優先。

路由選項範例

下列主題描述您 VPC 中特定閘道或連線的路由。

目錄

- 路由至網際網路閘道
- 路由至 NAT 裝置
- 路由至虛擬私有閘道
- 路由至 AWS Outposts 本機閘道
- 路由至 VPC 對等連線
- 路由至閘道 VPC 端點
- 路由至輸出限定網際網路閘道
- 傳輸閘道的路由
- 中間設備的路由
- 使用字首清單進行路由
- 路由至閘道負載平衡器端點

路由至網際網路閘道

您可以將子網路由表中的路由新增至網際網路閘道，使子網成為公有子網。若要執行此作業，請將網際網路閘道連接至您的 VPC，然後新增使用 `0.0.0.0/0` (IPv4 流量) 或 `::/0` (IPv6 流量) 做為目的地的路由，以及目的地為網際網路閘道 ID (`igw-xxxxxxxxxxxxxxxxx`) 的目標。

目的地	目標
0.0.0.0/0	*igw-id*
::/0	*igw-id*

如需詳細資訊，請參閱 使用網際網路閘道啟用 VPC 的網際網路存取。

路由至 NAT 裝置

若要讓私有子網中的執行個體連線至網際網路，您可以在公有子網中建立 NAT 閘道或啟動 NAT 執行個體。然後，為私有子網的路由表新增一個路由，將 IPv4 網際網路流量 (`0.0.0.0/0`) 路由至 NAT 裝置。

目的地	目標
0.0.0.0/0	*nat-gateway-id*

您也可以對其他目標建立更具體的路由，以避免使用 NAT 閘道或私自路由特定流量時產生不必要的資料處理費用。在下列範例中，Amazon S3 流量 (pl-xxxxxxxx，包含特定區域中 Amazon S3 IP 地址範圍的字首清單) 會路由至閘道 VPC 端點，而 10.25.0.0/16 流量則會路由至 VPC 對等互連。這些 IP 地址範圍比 0.0.0.0/0 更為具體。當執行個體將流量傳送至 Amazon S3 或互連 VPC 時，流量會傳送至閘道 VPC 端點或 VPC 對等互連連線。所有其他流量都會傳送至 NAT 閘道。

目的地	目標
0.0.0.0/0	*nat-gateway-id*
pl-*xxxxxxxx*	*vpce-id*
10.25.0.0/16	*pcx-id*

如需詳細資訊，請參閱NAT 裝置。

路由至虛擬私有閘道

您可以使用 AWS Site-to-Site VPN 連線，讓 VPC 中的執行個體與您自己的網路通訊。若要這樣做，請建立虛擬私有閘道並將其連接到 VPC。然後，在子網路由表中新增路由，其中包含網路的目的地和虛擬私有閘道的目標 (`vgw-xxxxxxxxxxxxxxxxx`)。

目的地	目標
10.0.0.0/16	*vgw-id*

然後，您可以建立並配置 Site-to-Site VPN 連線。如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的什麼是 AWS Site-to-Site VPN？和路由表和 VPN 路由優先順序。

虛擬私有閘道上的 Site-to-Site VPN 連線不支援 IPv6 流量。但是，我們支援透過虛擬私有閘道前往 Direct Connect 連線的 IPv6 流量。如需詳細資訊，請參閱《Direct Connect 使用者指南》。

路由至 AWS Outposts 本機閘道

本節說明路由至 AWS Outposts 本機閘道的路由表組態。

目錄

- 啟用 Outpost 子網路與內部部署網路之間的流量
- 啟用跨 Outpost 的相同 VPC 中子網路之間的流量

啟用 Outpost 子網路與內部部署網路之間的流量

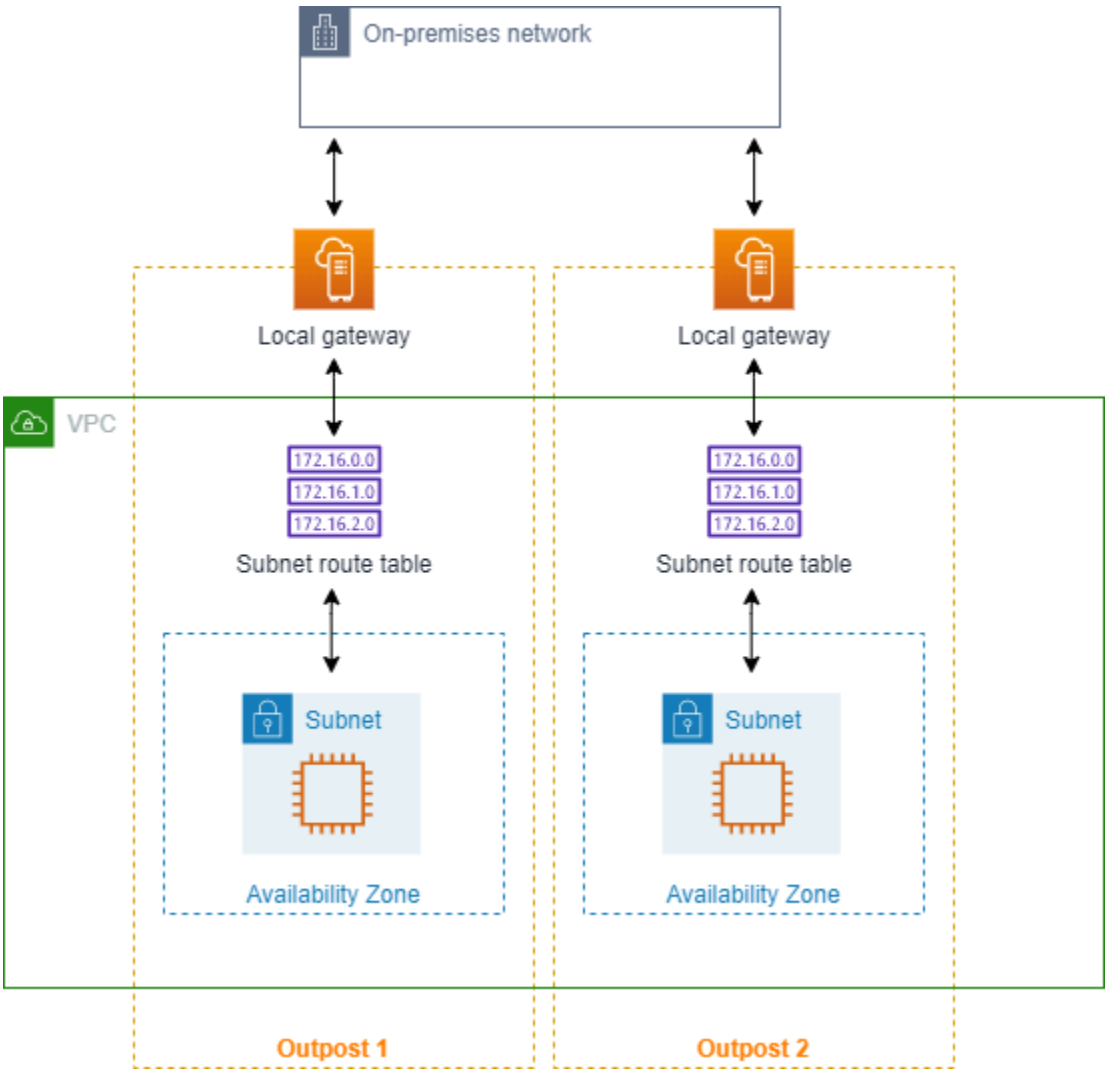
位於與 相關聯VPCs 中的子網路 AWS Outposts 可以具有其他目標類型的本機閘道。請考慮您想要讓本機閘道將目的地地址為 192.168.10.0/24 的流量路由至客戶網路的情況。若要這樣做，請新增下列路由，其中具有目的地網路和本機閘道目標 (`lgw-xxxx`)。

目的地	目標
192.168.10.0/24	*lgw-id*

啟用跨 Outpost 的相同 VPC 中子網路之間的流量

可以使用 Outpost 本機閘道和內部部署網路，在不同 Outpost 的相同 VPC 中的子網路之間建立通訊。

可以使用此功能在錨定到不同可用區域的 Outpost 機架之間建立連線，為在 Outposts 機架上執行的內部部署應用程式建立類似多可用區域 (AZ) 架構的架構。



若要啟用此功能，請將路由新增至 Outpost 機架子網路路由表，該路由比路由表中的本機路由更具體，並且具有本機閘道的目標類型。路由目的地必須與另一個 Outpost 中 VPC 的子網路的整個 IPv4 區塊相符。對需要通訊的所有 Outpost 子網路重複此組態。

Important

- 若要使用此功能，您必須使用直接 VPC 路由。您不能使用自己的客戶擁有的 IP 地址。
- Outpost 本機閘道所連線的內部部署網路必須具有必要的路由，這樣子網路才能互相存取。
- 如果想要為子網路中的資源使用安全群組，則必須使用包含 IP 地址範圍的規則作為 Outpost 子網路中的來源或目的地。您無法使用安全群組 ID。
- 現有的 Outpost 機架可能需要更新，才能支援多個 Outpost 之間的 VPC 內部通訊。如果此功能對您不起作用，請聯絡 AWS 支援。

Example範例

對於 CIDR 為 10.0.0.0/16 的 VPC、CIDR 為 10.0.1.0/24 的 Outpost 1 子網路，以及 CIDR 為 10.0.2.0/24 的 Outpost 2 子網路，Outpost 1 子網路路由表的項目如下所示：

目標	目標
10.0.0.0/16	區域
10.0.2.0/24	*lgw-1-id*

Outpost 2 子網路路由表的項目如下所示：

目標	目標
10.0.0.0/16	區域
10.0.1.0/24	*lgw-2-id*

路由至 VPC 對等連線

VPC 對等互連連線是指兩個 VPC 之間的聯網連線，可讓您使用私有 IPv4 地址路由 VPC 之間的流量。這兩個 VPC 中的執行個體能彼此通訊，有如位於同個網路中。

若要在 VPC 對等連線中的 VPC 之間啟用流量的路由，您必須將路由新增至一或多個子網路由表，指向 VPC 對等連線。這可讓您存取對等連線中其他 VPC 的全部或部分 CIDR 區塊。同樣地，另一個 VPC 的擁有者也必須將路由新增到他們的子網路由表，將流量路由回您的 VPC。

例如，若您有一個介於兩個 VPC 間的 VPC 對等互連連線 (pcx-11223344556677889)，其中包含以下資訊：

- VPC A：CIDR 區塊為 10.0.0.0/16
- VPC B：CIDR 區塊為 172.31.0.0/16

為啟用 VPC 間的流量及允許存取任一個 VPC 的完整 IPv4 CIDR 區塊，VPC A 路由表設定如下。

目的地	目標
10.0.0.0/16	區域
172.31.0.0/16	pcx-11223344556677889

VPC B 路由表設定如下。

目的地	目標
172.31.0.0/16	區域
10.0.0.0/16	pcx-11223344556677889

您的 VPC 對等連線也可支援 VPC 中執行個體之間的 IPv6 通訊 (如果 VPC 和執行個體已啟用 IPv6 通訊的話)。

若要啟用 VPCs 之間的 IPv6 流量路由，請將路由新增至路由表，以指向 VPC 對等互連連線，存取對等 VPC 的全部或部分 IPv6 CIDR 區塊。

例如，使用與上述相同的 VPC 對等互連連線 (`pcx-11223344556677889`)，假設 VPC 具有下列資訊：

- VPC A：IPv6 CIDR 區塊為 `2001:db8:1234:1a00::/56`
- VPC B：IPv6 CIDR 區塊為 `2001:db8:5678:2b00::/56`

若要啟用透過 VPC 對等連線的 IPv6 通訊，請將以下路由新增至 VPC A 的子網路由表。

目的地	目標
10.0.0.0/16	區域
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

將下列路由新增至 VPC B 的路由表。

目的地	目標
172.31.0.0/16	區域
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

如需 VPC 對等互連連線的詳細資訊，請參閱 Amazon VPC 互連指南。

路由至閘道 VPC 端點

閘道 VPC 端點可讓您在 VPC 與其他 AWS 服務之間建立私有連線。建立閘道端點時，您可以在 VPC 中指定閘道端點所使用的子網路由表。路由會自動新增至指定服務前綴清單 ID (`pl-xxxxxxxx`) 之目標 (destination) 以及具有端點 ID 之目標 (target) (`vpce-xxxxxxxxxxxxxxxxx`) 的所有路由表。您無法明確刪除或修改端點路由，但是您可以變更端點使用的路由表。

如需端點路由的詳細資訊，以及前往 AWS 服務之路由的隱含式，請參閱閘道端點的路由。

路由至輸出限定網際網路閘道

您可以為您的 VPC 建立輸出限定網際網路閘道，讓私有子網中的執行個體能初始化對網際網路的傳出通訊，同時防止網際網路啟動與執行個體的連線。輸出限定網際網路閘道僅能用於 IPv6 流量。若要設定輸出限定網際網路閘道的路由，請在私有子網路由表中新增將 IPv6 網際網路流量 (`::/0`) 路由至輸出限定網際網路閘道的路由。

目的地	目標
::/0	*eigw-id*

如需詳細資訊，請參閱 使用輸出限定 (egress-only) 網際網路閘道來啟用傳出 IPv6 流量。

傳輸閘道的路由

當您將 VPC 連線至傳輸閘道時，您需將路由新增至子網路由表，才能透過傳輸閘道路由流量。

請考慮當您有三個 VPC 已連線至傳輸閘道的情況。在此案例中，所有連接會與傳輸閘道路由表相關聯，並且會傳播至傳輸閘道路由表。因此，所有連接都可彼此路由封包，而傳輸閘道則單純做為 Layer 3 IP 中樞。

例如，若您有兩個 VPC，其中包含以下資訊：

- VPC A: 10.1.0.0/16, attachment ID tgw-attach-11111111111111111
- VPC B: 10.2.0.0/16, attachment ID tgw-attach-22222222222222222

為啟用 VPC 間的流量及允許存取傳輸閘道，VPC A 路由表配置如下。

目的地	目標
10.1.0.0/16	區域
10.0.0.0/8	*tgw-id*

下列為 VPC 連接的傳輸閘道路由表項目範例。

目的地	目標
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

如需傳輸閘道路由表的詳細資訊，請參閱 Amazon VPC Transit Gateways 中的路由。

中間設備的路由

您可以將中間設備新增至 VPC 的路由路徑中。下列為可行的使用案例：

- 透過網際網路閘道或虛擬私有閘道攔截進入 VPC 的流量，方法為將該流量導向至 VPC 中的中間設備。您可以使用中間設備路由精靈，讓 AWS 自動為您的閘道、中間設備及目的地子網路設定適當的路由表。如需詳細資訊，請參閱the section called “中間設備路由精靈”。
- 將兩個子網之間的流量導向至中間設備。為此，您可以為符合另一個子網的子網 CIDR 的一個子網路由表建立路由，並將設備的閘道負載平衡器端點、NAT 閘道、Network Firewall 端點或網路界面指定

為目標。或者，若要將所有流量從子網重新引導至任何其他子網，請以閘道負載平衡器端點、NAT 閘道或網路界面取代本機路由的目標。

您可以設定設備以符合您的需求。例如，您可以設定篩選所有流量的安全設備，或 WAN 加速設備。此設備會在 VPC 的子網中部署為 Amazon EC2 執行個體，並以子網中的彈性網路介面 (網路介面) 表示。

如果您啟用目的地子網路由表的路由傳播，請注意路由優先順序。我們優先考慮最具體的路由，如果路由符合，我們優先考慮靜態路由，而不是傳播路由。

檢閱您的路由，以確保流量路由正確，而且如果您啟用或停用路由傳播，不會造成意外後果 （ 例如，支援巨型訊框的 Direct Connect 連線需要路由傳播 ）。

若要將傳入 VPC 流量路由至設備，請將路由表與網際網路閘道或虛擬私有閘道建立關聯，並將您設備的網路界面指定為 VPC 流量的目標。如需詳細資訊，請參閱閘道路由表。您也可以將傳出流量從子網路由至另一個子網中的中間設備。

如需中間設備路由範例，請參閱中間設備案例。

目錄

- 設備考量
- 路由閘道與設備之間的流量
- 將子網間流量路由至設備

設備考量

您可以從 AWS Marketplace 中選擇第三方設備 ，也可以設定自己的設備。建立或設定設備時，請注意下列事項：

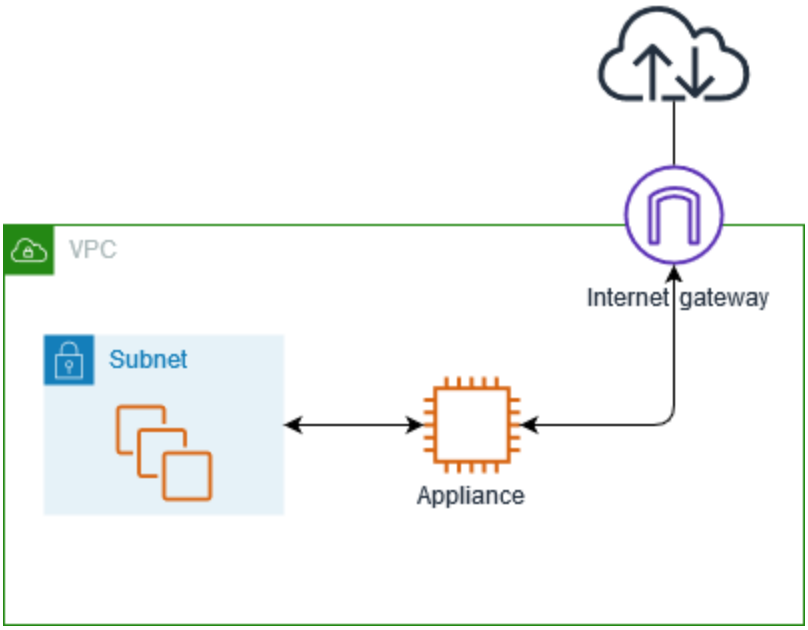
- 設備必須設定在與來源或目的地流量不同的子網中。
- 您必須停用設備上的來源/目的地檢查。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的變更來源或目的地檢查。
- 您無法透過設備在相同子網中的主機之間路由流量。
- 設備不需要執行網路地址轉譯 (NAT)。
- 您可以新增路由至比本機路由更具體的路由表。您可以使用更具體的路由，將 VPC (東西流量) 內子網之間的流量重新引導至中間設備。路由目的地必須符合 VPC 中子網的整個 IPv4 或 IPv6 CIDR 區塊。

- 若要攔截 IPv6 流量，請確定 VPC、子網路和設備可支援 IPv6。
-

> **Important**
>
> 請勿將來自 AWS受管服務的流量，例如傳輸閘道、NAT 閘道或 Network Load Balancer，透過中間設備路由回連接該服務的子網路。此組態會導致無法預測的路由行為，且不受支援。

路由閘道與設備之間的流量

若要將傳入 VPC 流量路由至設備，請將路由表與網際網路閘道或虛擬私有閘道建立關聯，並將您設備的網路界面指定為 VPC 流量的目標。在下列範例中，VPC 具有網際網路閘道、設備以及具有執行個體的子網。來自網際網路的流量會透過設備進行路由。



將此路由表與您的網際網路閘道或虛擬私有閘道建立關聯。第一個項目是本機路由。第二個項目會將目的地為子網的 IPv4 流量傳送至設備的網路界面。這是比本機路由更具體的路由。

目標	Target
VPC CIDR	區域
## CIDR	*###### ID*

或者，您可以將本機路由的目標取代為設備的網路界面。您可以這樣做，以確保所有流量都會自動路由至設備，包括目的地為您未來新增至 VPC 之子網的流量。

目標	Target
VPC CIDR	*###### ID*

若要將流量從子網路由到另一個子網中的設備，請將路由新增到子網路由表，將流量路由至設備的網路界面。此目的地必須比本機路由的目的地更不具體。例如，對於前往網際網路的流量，請為目的地指定 `0.0.0.0/0` (所有 IPv4 地址)。

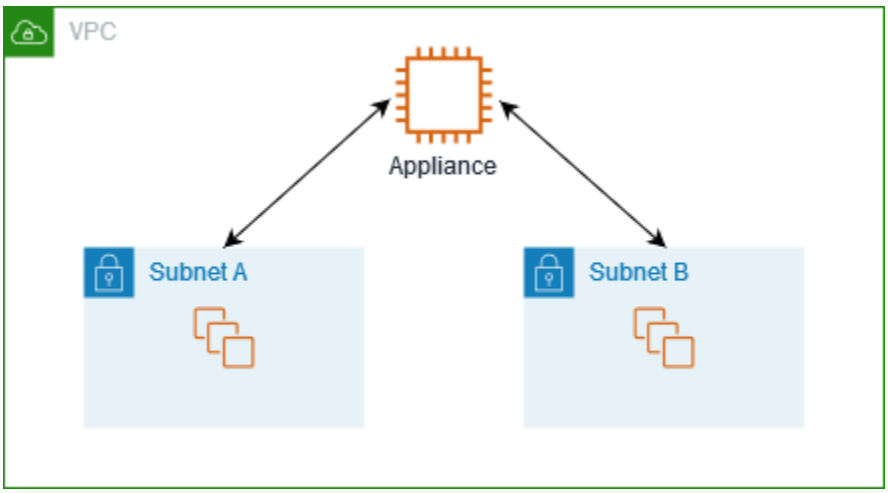
目的地	Target
VPC CIDR	區域
0.0.0.0/0	*###### ID*

然後，在與設備子網相關聯的路由表中，新增一個路由，將流量傳送回網際網路閘道或虛擬私有閘道。

目標	Target
VPC CIDR	區域
0.0.0.0/0	*igw-id*

將子網間流量路由至設備

您可以將目的地為特定子網的流量路由至設備的網路界面。在下列範例中，VPC 包含兩個子網和一個設備。子網之間的流量透過設備進行路由。



Security groups (安全群組)

當您透過中間設備路由不同子網中的執行個體之間的流量時，兩個執行個體的安全群組都必須允許流量在執行個體之間流動。每個執行個體的安全群組都必須參考另一個執行個體的私有 IP 地址，或是包含其他執行個體之子網的 CIDR 範圍作為來源。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。

路由

下列是子網 A 的路由表範例。第一個項目可讓 VPC 中的執行個體彼此通訊。第二個項目會將所有流量從子網 A 路由至子網 B，再路由至設備的網路界面。

目標	Target
VPC CIDR	區域
### B CIDR	*###### ID*

下列是子網 B 的路由表範例。第一個項目可讓 VPC 中的執行個體彼此通訊。第二個項目會將所有流量從子網 B 路由至子網 A，再路由至設備的網路界面。

目標	Target
VPC CIDR	區域
### A CIDR	*###### ID*

或者，您可以將本機路由的目標取代為設備的網路界面。您可以這樣做，以確保所有流量都會自動路由至設備，包括目的地為您未來新增至 VPC 之子網的流量。

目標	Target
VPC CIDR	*###### ID*

使用字首清單進行路由

如果您經常在 AWS 資源中參考相同的一組 CIDR 區塊，您可以建立客戶受管字首清單，將它們分組在一起。然後，您可以將字首清單指定為路由表項目中的目的地。您可以稍後新增或移除字首清單的項目，而不需要更新路由表。

例如，您有一個具有多個 VPC 連接的傳輸閘道。VPC 必須能夠與具有下列 CIDR 區塊的兩個特定 VPC 連接進行通訊：

- 10.0.0.0/16
- 10.2.0.0/16

您可以建立具有兩個項目的字首清單。在子網路由表中，您可以建立路由並指定字首清單作為目的地，並指定傳輸閘道指定為目標。

目的地	目標
172.31.0.0/16	區域
pl-123abc123abc123ab	*tgw-id*

字首清單的項目數目上限等於路由表中的相同項目數。

路由至閘道負載平衡器端點

閘道負載平衡器可讓您將流量散發給虛擬設備 (例如防火牆) 的機群。您可以建立 Gateway Load Balancer、設定 Gateway Load Balancer 端點服務，接著在 VPC 中建立 Gateway Load Balancer 端點，實現與該服務的連線。

若要將流量路由至閘道負載平衡器 (例如，針對安全檢查)，請在路由表中指定閘道負載平衡器端點做為目標。

如需閘道負載平衡器後方的安全設備範例，請參閱the section called “使用安全設備檢查流量”。

若要在路由表中指定閘道負載平衡器端點，請使用 VPC 端點的 ID。例如，若要將 10.0.1.0/24 的流量路由至閘道負載平衡器端點，請新增下列路由。

目標	Target
10.0.1.0/24	*vpc-endpoint-id*

如果將 Gateway Load Balancer 端點作為目標，您無法將字首清單指定為目的地。如果嘗試建立或取代以 VPC 端點為目標的字首清單路由，您將會收到錯誤："Cannot create or replace a prefix list route targeting a VPC Endpoint."

如需詳細資訊，請參閱 Gateway Load Balancer。

建立 VPC 的路由表

完成以下任務，即可為 VPC 建立並設定自訂路由表。依預設，新建立的路由表皆包含允許 VPC 內部通訊的本機路由。您可以新增路由，依據目的地 IP 位址範圍將網路流量導向特定目標。

若要將路由表路由套用至特定子網，您必須將路由表與子網建立關聯。路由表可以和多個子網建立關聯。不過，子網一次只能與一個路由表相關聯。根據預設，所有未與表明確建立關聯的子網都會與主路由表隱含建立關聯。

您可以取消子網與路由表的關聯。直到您將子網與另一個路由表建立關聯之前，子網會與主路由表隱含建立關聯。

> **Note**
>
> 每個 VPC 可以建立的路由表數量有配額。您可以在每個路由表中新增的路由數量也有配額。如需詳細資訊，請參閱Amazon VPC 配額。

任務

- 建立路由表
- 將路由新增至路由表
- 將子網路與路由表建立關聯

建立路由表

使用主控台建立路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選擇 Create route table (建立路由表)。
4. (選用) 針對 Name (名稱)，輸入路由表的名稱。
5. 在 VPC 中，選擇您的 VPC。
6. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤鍵和標籤值。
7. 選擇 Create route table (建立路由表)。

使用 建立路由表 AWS CLI

使用 create-route-table 命令。

將路由新增至路由表

透過主控台將路由新增至路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 選擇 Actions (動作)、Edit routes (編輯路由)。
4. 選擇 Add route (新增路由)。
5. 在目的地欄位中，輸入以下任一內容：
   - IP 位址範圍 – 例如 192.168.0.0/16
   - 單一 IP 位址 – 例如 192.168.10.1/32
   - 字首清單 ID – 例如 pl-0abcdef1234567890
6. 在目標欄位中選取資源類型 (例如網路介面)，然後輸入資源的 ID (例如 eni-11223344556677889)。
7. 選擇儲存變更。

使用 將路由新增至路由表 AWS CLI

使用 create-route 命令。

將子網路與路由表建立關聯

使用主控台將路由表與子網建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 在 Subnet associations (子網關聯) 標籤上，選擇 Edit subnet associations (編輯子網關聯)。
4. 選取子網路的核取方塊以和路由表建立關聯。
5. 選擇 Save associations (儲存關聯)。

使用 將子網路與路由表建立關聯或取消關聯 AWS CLI

- associate-route-table
- disassociate-route-table

管理子網路路由表

依照下列程序透過路由表管理 VPC 路由。

任務

- 判斷子網路的路由表
- 確定明確的關聯關係
- 新增、修改與刪除路由
- 啟用或停用路由傳播
- 變更子網的路由表

判斷子網路的路由表

您可以透過在 Amazon VPC 主控台中查看子網詳細資訊，來判斷與子網關聯的路由表。

透過主控台確定子網路的路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。

3. 選擇子網路。
4. 選擇 Route Table (路由表) 索引標籤以檢視有關路由表及其路由的資訊。若要判斷與主路由表的關聯是否為明確關聯，請參閱 確定明確的關聯關係。

確定明確的關聯關係

您可以判斷有多少及有哪些與路由表明確相關聯的子網或閘道。

主路由表可具有明確及隱含的子網關聯。自訂路由表則只有明確關聯。

並未與任何路由表明確關聯的子網便會和主路由表建立隱含關聯。您可以明確地將子網與主路由表建立關聯。如需您可能這樣做的原因範例，請參閱取代主路由表。

使用主控台判斷哪些子網明確關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 檢查 Explicit subnet association (明確的子網關聯) 資料行，判斷明確關聯的子網以及 Main (主要) 資料行以判斷這是否為主路由表。
4. 選取路由表並選擇 Subnet associations (子網關聯) 標籤。
5. Explicit subnet associations (明確的子網關聯) 下方的子網明確與路由表相關聯。Subnets without explicit associations (沒有明確關聯的子網) 下方的子網屬於與路由表相同的 VPC，但沒有與任何路由表具有關聯，因此它們與 VPC 的主路由表具有隱含關聯。

使用主控台判斷哪些閘道明確關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選取路由表並選擇 Edge associations (邊緣關聯) 標籤。

使用 描述一或多個路由表並檢視其關聯 AWS CLI

使用 describe-route-tables 命令。

新增、修改與刪除路由

您可以新增、修改與刪除路由表中的路由。

如需使用 Site-to-Site VPN 連線的靜態路由的詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的編輯 Site-to-Site VPN 的靜態路由。

考量事項

- 您僅能修改您新增的路由。
- 修改或刪除路由後，使用這些路由的現有連線會受到影響。使用其他路由的連線則不受影響。
- 您可以在每個路由表中新增的路由數量有配額。如需詳細資訊，請參閱Amazon VPC 配額。

使用控制台更新路由表的路由

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 選擇 Actions (動作)、Edit routes (編輯路由)。
4. 若要新增路由，請選擇 Add route (新增路由)。在目的地欄位中輸入 IP 位址範圍、單一 IP 位址或字首清單 ID。在目標欄位中選取資源類型，然後輸入資源 ID。
5. 若要修改路由，輸入新的目的地 CIDR 區塊或字首清單 ID，再選擇目標。
6. 若要刪除路由，請選擇 Remove (移除)。
7. 選擇儲存變更。

使用 更新路由表的路由 AWS CLI

如果您使用命令列工具或 API 新增路由，目的地 CIDR 區塊會自動修改為其正式形式。例如，如果您針對 CIDR 區塊指定 `100.68.0.18/18`，我們會建立目的地 CIDR 區塊為 `100.68.0.0/18` 的路由 。

- create-route
- replace-route
- delete-route

啟用或停用路由傳播

路由傳播允許虛擬私有閘道自動將路由傳播到路由表。這表示您無需手動新增或移除 VPN 路由。

若要完成此程序，您必須擁有虛擬私有閘道。

如需詳細資訊，請參閱 Site-to-Site VPN 使用者指南中的 Site-to-Site VPN 路由選項。

透過主控台啟用或停用路由傳播

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 選擇 Actions (動作)、Edit route propagation (編輯路由傳播)。
4. 選取或取消選取虛擬私有閘道旁邊的啟用核取方塊。
5. 選擇儲存。

使用 啟用或停用路由傳播 AWS CLI

- enable-vgw-route-propagation
- disable-vgw-route-propagation

變更子網的路由表

您可以變更子網的路由表關聯。

當您變更路由表時，除非新路由表包含相同流量通往相同目標的路由，否則會捨棄子網中的現有連線。

使用主控台變更子網路由表關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)，然後選取子網。
3. 從 Route Table (路由表) 標籤中，選擇 Edit route table association (編輯路由表關聯)。
4. 對於 Route table ID (路由表格 ID)，選取新的路由表。
5. 選擇儲存。

使用 變更與子網路相關聯的路由表 AWS CLI

使用 replace-route-table-association 命令。

取代主路由表

本節說明如何變更 VPC 中的主要路由表。

使用控制台取代主路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取新的主路由表。
3. 選擇 Actions (動作)、Set main route table (設定主路由表)。
4. 出現確認提示時，請輸入 **set**，然後選擇 OK (確認)。

使用 取代主路由表 AWS CLI

- 使用 replace-route-table-association 命令。

以下程序說明如何移除子網和主路由表之間的明確關聯。子網和主路由表之間會形成隱含關聯。程序和取消子網與任何路由表的關聯相同。

移除與主路由表的明確關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 從 Subnet associations (子網路關聯) 標籤，選擇 Edit subnet associations (編輯子網路關聯)。
4. 清除子網路的核取方塊。
5. 選擇 Save associations (儲存關聯)。

透過閘道路由表控制進入 VPC 的流量

若要使用閘道路由表控制進入 VPC 的流量，您可以將網際網路閘道或虛擬私有閘道與路由表建立關聯或取消關聯。如需詳細資訊，請參閱閘道路由表。

使用主控台將閘道與路由表建立或取消關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 從 Edge associations (邊緣關聯) 標籤，選擇 Edit edge associations (編輯邊緣關聯)。
4. 選取或取消選取閘道的核取方塊。
5. 選擇儲存變更。

使用 將閘道與路由表建立關聯 AWS CLI

使用 associate-route-table 命令。以下範例將指定路由表與網際網路閘道建立關聯。

```
aws ec2 associate-route-table
    --route-table-id rtb-01234567890123456 \
    --gateway-id igw-11aa22bb33cc44dd1
```

使用 取消閘道與路由表的關聯 AWS CLI

使用 disassociate-route-table 命令。指定路由表與閘道之間的關聯 ID。

```
aws ec2 disassociate-route-table \
    --association-id rtbassoc-0abcdef1234567890
```

取代或還原本機路由的目標

您可以變更預設本機路由的目標。如果取代本端路由的目標，稍後您可以將其還原至預設 `local` 目標。如果您的 VPC 具有 多個 CIDR 區塊，則您的路由表具有多個本機路由 — 每個 CIDR 區塊一個本機路由。您可以視需要取代或還原每個本端路由的目標。

透過主控台取代本機路由

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 從 Routes (路由) 標籤，選擇 Edit routes (編輯路由)。
4. 對於本機路由，請清除目標，然後選擇新目標。
5. 選擇儲存變更。

使用主控台還原本機路由的目標

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 選擇 Actions (動作)、Edit routes (編輯路由)。
4. 對於本機路由，請清除目標，然後選擇本機。
5. 選擇儲存變更。

使用 取代本機路由的目標 AWS CLI

使用 replace-route 命令。下列範例將本機路由的目標取代為指定網路介面。

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --network-interface-id eni-11223344556677889
```

使用 還原本機路由的目標 AWS CLI

以下範例將還原指定路由表的本機目標。

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --local-target
```

VPC 中的進階路由

為 VPC 設定進階路由案例。本節介紹管理流量傳輸的靜態與動態路由方法：

- 靜態傳入路由：設定靜態路由，將目的地為 BYOIP (自有 IP) 位址集區的傳入網際網路流量導向 VPC 內的特定網路介面。
- 使用 VPC 路由伺服器進行動態路由：使用 BGP 型動態路由來自動更新 VPC 與網際網路閘道路由表，為工作負載提供容錯能力與自動容錯移轉。

目錄

- 將網際網路流量路由至單一網路介面
- 透過 VPC 路由伺服器在 VPC 中進行動態路由

將網際網路流量路由至單一網路介面

您可以將目的地為大型公有 IP 位址集區的傳入網際網路流量，路由至 VPC 中的單一彈性網路介面 (ENI)。

以往，網際網路閘道僅接受目的地為 VPC 中網路介面直接關聯之公有 IP 位址的流量。執行個體類型會限制可與網路介面關聯的 IP 位址數量，這對電信與物聯網 (IoT) 等需處理超過該限制之 IP 集區流量的產業構成挑戰。

此路由功能可消除傳入網際網路連線時的複雜位址轉譯作業。您可以攜帶自有公有 IP 集區 (BYOIP)，將 VPC 網際網路閘道設定為接受整個集區的流量並將其路由至單一網路介面。此功能特別適用於：

- 電信業者：可管理大型訂閱用戶 IP 集區，無需承擔位址轉譯開銷
- IoT 應用程式：可彙整來自數千個裝置 IP 位址的流量
- 任何案例：可讓流量路由突破 ENI 關聯限制

您可以將此路由功能與 VPC 路由伺服器整合，在容錯移轉案例中實現動態路由更新。

主要優點

此路由機制具備以下優勢：

- 無需位址轉譯 – 直接路由可消除複雜的 NAT 工作
- 突破 ENI 限制 – 處理超過執行個體關聯限制數量的 IP 集區
- 產業最佳化 – 專為電信業與 IoT 需求打造
- 動態容錯移轉 – 與路由伺服器整合實現自動化更新

可用性

您可以在所有 AWS 商業區域、 AWS 中國區域和 AWS GovCloud 區域使用此功能。

目錄

- 開始之前
- 此功能的運作方式
- 步驟 1：建立 VPC
- 步驟 2：建立並連接網際網路閘道
- 步驟 3：為目標執行個體建立子網路
- 步驟 4：為子網路建立路由表
- 步驟 5：為目標執行個體建立安全群組
- 步驟 6：啟動目標 EC2 執行個體
- 步驟 7：網際網路閘道的路由表
- 步驟 8：將路由表與網際網路閘道建立關聯
- 步驟 9：將 BYOIP 集區與網際網路閘道建立關聯
- 步驟 10：新增指向目標執行個體的靜態路由
- 步驟 11：設定目標執行個體
- 步驟 12：設定執行個體流量處理功能

- 步驟 13：測試連線
- 疑難排解
- 進階選項：整合路由伺服器實現動態路由
- 清除

開始之前

在開始本教學課程之前，請確認已滿足以下條件：

1. BYOIP 集區：您必須已將自己的 IP 地址範圍帶入其中 AWS。完成 Bring your own IP addresses (BYOIP) in Amazon EC2 中的步驟。
2. 驗證 BYOIP 集區：執行如下命令確認集區已就緒：

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1
   ```

   在輸出結果中查找集區，確認 `PoolAddressRanges` 顯示 `Available` 位址。
3. 適當的許可：確保 AWS 您的帳戶具有建立 VPC 資源、EC2 執行個體和管理 BYOIP 集區的許可。

此功能的運作方式

本節將說明網際網路閘道輸入路由背後的技術概念，以及流量從網際網路傳輸至目標執行個體的路徑。

為何使用網際網路閘道輸入路由

以往，因 ENI 關聯數量限制，您需透過位址轉譯才能彙整大量 IP 位址的流量。此增強功能允許 BYOIP 集區直接路由至目標執行個體，從而消除了這種複雜工作。

路由的運作方式

此功能僅適用於您用於 AWS 遵循 BYOIP 程序的公有 IP CIDRs。BYOIP 流程會確保您帳戶擁有該公有 IP CIDR。取得 BYOIP 公有 CIDR 後，執行如下步驟：

1. 將此公有 IP 位址集區與網際網路閘道路由表建立關聯。該網際網路閘道必須已與 VPC 建立關聯。此關聯允許 VPC 接收目的地為該 IP CIDR 的流量。確保網際網路閘道擁有不與任何子網路共用的專用路由表。
2. 完成 BYOIP 集區與網際網路閘道路由表的關聯後，即可在該網際網路閘道路由表中新增目的地為完整 IP CIDR 或其子網段的路由。此路由的目標設定為要接收流量的 ENI。

3. 當您以 BYOIP CIDR 為目標的流量進入時 AWS， AWS 查看網際網路閘道路由表，並相應地將流量路由到相關的 VPC。
4. 在 VPC 中，網際網路閘道會將流量路由至目標 ENI。
5. 目標 (與您工作負載關聯的彈性網路介面) 會處理流量。

最佳實務

- 保持路由表分離：網際網路閘道路由表必須僅專用於網際網路閘道。切勿將此路由表與任何 VPC 子網路建立關聯。子網路路由應使用單獨的路由表。
- 勿直接指派 BYOIP IP：切勿將 BYOIP 集區的公有 IP 位址直接與 EC2 執行個體或網路介面關聯。網際網路閘道輸入路由功能無需直接關聯 IP，即可將流量路由至執行個體。

> **Important**
>
> 如果使用了 VPC 封鎖公開存取 (BPA)，啟用 BPA 後，即使已設定子網路層級 BPA 排除規則，也會封鎖透過輸入路由傳送至子網路的流量。子網路層級排除項目不適用於輸入路由。如要在啟用 BPA 的狀態下允許輸入路由流量：
>
> - 請完全停用 BPA，或
> - 採用 VPC 層級的排除項目

步驟 1：建立 VPC

完成此步驟，即可建立將託管目標執行個體與網際網路閘道的 VPC。

> **Note**
>
> 確認尚未達到 VPC 配額限制。如需詳細資訊，請參閱Amazon VPC 配額。

AWS 主控台

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 在建立資源，選擇僅 VPC。

4. 在名稱標籤欄位中，輸入 VPC 的名稱 (例如 **IGW-Ingress-VPC**)。
5. 在 IPv4 CIDR 區塊欄位中，輸入一個 CIDR 區塊 (例如 **10.0.0.0/16**)。
6. 選擇建立 VPC。

AWS CLI

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=IGW-Ingress-VPC}]' --region us-east-1
```

步驟 2：建立並連接網際網路閘道

完成此步驟，即可建立網際網路閘道並將其連接至 VPC，從而啟用網際網路連線。

AWS 主控台

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 主控台中，選擇網際網路閘道。
3. 選擇建立網際網路閘道。
4. 在名稱標籤欄位中，輸入網際網路閘道的名稱 (例如 **IGW-Ingress-Gateway**)。
5. 選擇建立網際網路閘道。
6. 選取您的網際網路閘道，然後選擇動作、連接至 VPC。
7. 選取您的 VPC，然後選擇連接網際網路閘道。

AWS CLI

```
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=IGW-Ingress-Gateway}]' --region us-east-1

aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1
```

注意：將資源 ID 取代為上一個步驟中的實際 ID。

步驟 3：為目標執行個體建立子網路

完成此步驟，即可建立要部署目標執行個體的子網路。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇 Subnets (子網路)。
2. 選擇 Create subnet (建立子網路)。
3. 在 VPC ID 欄位中，選擇您的 VPC。
4. 在子網路名稱欄位中，輸入一個名稱 (例如 **Target-Subnet**)。
5. 對於可用區域，您可以選擇子網路的區域，或保留預設的無偏好設定，讓 為您 AWS 選擇。
6. 在 IPv4 CIDR 區塊欄位中，選取手動輸入，然後輸入 CIDR 區塊 (例如 **10.0.1.0/24**)。
7. 選擇 Create subnet (建立子網路)。

AWS CLI

```
aws ec2 create-subnet \
    --vpc-id vpc-0123456789abcdef0 \
    --cidr-block 10.0.1.0/24 \
    --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Target-Subnet}]' \
    --region us-east-1
```

步驟 4：為子網路建立路由表

完成此步驟，即可為子網路建立路由表，並將路由表與子網路建立關聯。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇路由表。
2. 選擇 Create route table (建立路由表)。
3. 在名稱欄位中，輸入路由表的名稱 (例如 **Target-Subnet-Route-Table**)。
4. 在 VPC 中，選擇您的 VPC。
5. 選擇 Create route table (建立路由表)。
6. 選取您的路由表，然後依次選擇動作、編輯子網路關聯。
7. 選取您的子網路，然後選擇儲存關聯。

AWS CLI

```
aws ec2 create-route-table \
```

```
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Target-Subnet-
Route-Table}]' \
    --region us-east-1

aws ec2 associate-route-table \
    --route-table-id rtb-0987654321fedcba0 \
    --subnet-id subnet-0123456789abcdef0 \
    --region us-east-1
```

步驟 5：為目標執行個體建立安全群組

完成此步驟，即可建立一個安全群組，用於控制對目標執行個體的網路存取。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇安全群組。
2. 選擇建立安全群組。
3. 在安全群組名稱欄位中，輸入一個名稱 (例如 **IGW-Target-SG**)。
4. 對於 Description (說明)，輸入 **Security group for IGW ingress routing target instance**。
5. 針對 VPC，選取您的 VPC。
6. 若要新增傳入規則，請選擇傳入規則。針對每條規則，請選擇新增規則並指定以下參數：
   - 類型：所有 ICMP – IPv4，來源：0.0.0.0/0 (用於 Ping 測試)。
   - 類型：SSH，連接埠：22，來源：0.0.0.0/0 (用於 EC2 Instance Connect)。

> **Note**
>
> 在本教學課程中，此安全群組會向所有網際網路流量開放 SSH 連接埠。本教學課程用於教育目的，切勿在生產環境中作此設定。在實際生產環境中，應將 SSH 存取限制於特定 IP 範圍。

- 選擇建立安全群組。

AWS CLI

```
aws ec2 create-security-group \
```

```
    --group-name IGW-Target-SG \
    --description "Security group for IGW ingress routing target instance" \
    --vpc-id vpc-0123456789abcdef0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol icmp \
    --port -1 \
    --cidr 0.0.0.0/0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol tcp \
    --port 22 \
    --cidr 0.0.0.0/0 \
    --region us-east-1
```

步驟 6：啟動目標 EC2 執行個體

完成此步驟，即可啟動將接收來自 BYOIP 集區流量的 EC2 執行個體。

AWS 主控台

1. 開啟 Amazon EC2 主控台。
2. 選擇啟動執行個體。
3. 在名稱欄位中，輸入執行個體的名稱 (例如 **IGW-Target-Instance**)。
4. 在應用程式與作業系統映像 (Amazon Machine Image) 欄位中，選擇 Amazon Linux 2023 AMI。
5. 在執行個體類型欄位中，選擇 t2.micro (符合免費方案資格)。
6. 在金鑰對 (登入) 欄位中，選取現有的金鑰對或建立新的金鑰對。
7. 在網路設定欄位中，選擇編輯並設定以下項目：
   - VPC：選取 VPC
   - 子網路：選取子網路
   - 自動指派公有 IP：啟用
   - 防火牆 (安全群組)：選取現有的安全群組並選擇您的安全群組
8. 選擇啟動執行個體。

9. **重要事項：啟動後，前往執行個體詳細資訊，記錄網路介面 ID (以 "eni-" 開頭)，供步驟 10 使用。**

AWS CLI

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name your-key-pair \
    --security-group-ids sg-0123456789abcdef0 \
    --subnet-id subnet-0123456789abcdef0 \
    --associate-public-ip-address \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=IGW-Target-
Instance}]' \
    --region us-east-1
```

若要使用主控台查詢 ENI ID：

1. 在 EC2 主控台中，選取執行個體。
2. 前往聯網索引標籤。
3. 記錄網路介面 ID (例如 `eni-0abcdef1234567890`)。

若要使用 尋找 ENI ID AWS CLI：

```
aws ec2 describe-instances --instance-ids i-0123456789abcdef0 --query
 'Reservations[0].Instances[0].NetworkInterfaces[0].NetworkInterfaceId' --output text
 --region us-east-1
```

步驟 7：網際網路閘道的路由表

完成此步驟，即可為處理輸入路由的網際網路閘道建立專用路由表。

AWS 主控台

1. 在 VPC 主控台中選擇路由表。
2. 選擇 Create route table (建立路由表)。
3. 在名稱欄位中，輸入路由表的名稱 (例如 **`IGW-Ingress-Route-Table`**)。
4. 在 VPC 中，選擇您的 VPC。

5. 選擇 Create route table (建立路由表)。
6. 選取您的路由表並選擇邊緣關聯索引標籤。
7. 選擇編輯邊緣關聯。
8. 選取網際網路閘道，然後選擇儲存變更。

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=IGW-Ingress-
Route-Table}]' \
    --region us-east-1
```

步驟 8：將路由表與網際網路閘道建立關聯

完成此步驟，即可將路由表與網際網路閘道建立關聯，從而啟用輸入路由功能。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇路由表，然後選取您建立的路由表。
2. 從 Edge associations (邊緣關聯) 標籤，選擇 Edit edge associations (編輯邊緣關聯)。
3. 勾選網際網路閘道的核取方塊。
4. 選擇儲存變更。

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --gateway-id igw-0123456789abcdef0 \
    --region us-east-1
```

步驟 9：將 BYOIP 集區與網際網路閘道建立關聯

完成此步驟，即可將 BYOIP 集區與網際網路閘道路由表建立關聯，使 VPC 能夠接收流向您 IP 範圍的流量。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇路由表，然後選取您建立的網際網路閘道路由表。
2. 選擇 IPv4 集區關聯索引標籤。
3. 選擇編輯關聯按鈕。
4. 選取 BYOIP 集區 (例如 pool-12345678901234567)。
5. 選擇儲存關聯按鈕。

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --public-ipv4-pool pool-12345678901234567 \
    --region us-east-1
```

注意：將 rtb-0123456789abcdef0 取代為網際網路閘道路由表 ID，並將 pool-12345678901234567 取代為 BYOIP 集區 ID。

步驟 10：新增指向目標執行個體的靜態路由

完成此步驟，即可新增一條路由，將來自 BYOIP 範圍的流量導向目標執行個體的網路介面。

AWS 主控台

1. 在 VPC 主控台的導覽窗格中，選擇路由表，然後選取您建立的網際網路閘道路由表。
2. 選擇 Actions (動作)、Edit routes (編輯路由)。
3. 選擇 Add route (新增路由)。
4. 在目的地欄位中，輸入 BYOIP CIDR 或子網段 (例如 **203.0.113.0/24**)。字首必須介於 /23 至 /28 之間。
5. 在目標欄位中，選取網路介面，然後輸入執行個體的 ENI ID (例如 eni-0abcdef1234567890)。
6. 選擇儲存變更。

AWS CLI

```
aws ec2 create-route \
    --route-table-id rtb-0123456789abcdef0 \
```

```
    --destination-cidr-block 203.0.113.0/24 \
    --network-interface-id eni-0abcdef1234567890 \
    --region us-east-1
```

步驟 11：設定目標執行個體

完成此步驟，即可設定目標執行個體，從而正確處理目的地為 BYOIP 位址的流量。

重要事項：在測試連線之前完成此執行個體設定步驟 (步驟 12)。執行個體必須設定為回應 BYOIP 位址，輸入路由才能正常運作。

AWS 主控台

1. 透過 EC2 Instance Connect 連線至 Linux 執行個體：
   - 在 EC2 主控台中，選取執行個體。
   - 選擇動作 > 連線。
   - 選取 EC2 Instance Connect 索引標籤。
   - 選擇連線。
2. 將特定 BYOIP IP 位址新增至執行個體介面：

   首先，查詢網路介面的名稱：

   ```
   ip link show
   ```

   接著，新增 IP 位址 (將 `203.0.113.10` 取代為 BYOIP 範圍內的 IP)：

   ```
   sudo ip addr add 203.0.113.10/32 dev eth0
   ```

   注意：將 `203.0.113.10` 取代為要測試的 BYOIP 範圍內的任一 IP 位址。網路介面名稱可能為 `eth0`、`ens5` 或類似名稱，具體取決於執行個體類型。
3. 在 EC2 主控台中，停用來源/目的地檢查：
   - 選取執行個體。
   - 前往聯網索引標籤，選擇網路界面。
   - 依次選擇動作、變更來源/目的地檢查、停用。

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

步驟 12：設定執行個體流量處理功能

完成此步驟，即可將 BYOIP 位址新增至執行個體並停用來源/目的地檢查，從而啟用適當的流量處理功能。

AWS 主控台

1. 透過 EC2 Instance Connect 連線至 Linux 執行個體：
   - 在 EC2 主控台中，選取執行個體。
   - 選擇動作 > 連線。
   - 選取 EC2 Instance Connect 索引標籤。
   - 選擇連線。
2. 將特定 BYOIP IP 位址新增至執行個體介面：

   首先，查詢網路介面的名稱：

   ```
   ip link show
   ```

   接著，新增 IP 位址 (將 ens5 取代為實際介面名稱)：

   ```
   sudo ip addr add 203.0.113.10/32 dev ens5
   ```

   注意：將 203.0.113.10 取代為要測試的 BYOIP 範圍內的任一 IP 位址。網路介面名稱可能為 eth0、ens5 或類似名稱，具體取決於執行個體類型。
3. 在 EC2 主控台中，停用來源/目的地檢查：
   - 選取執行個體。
   - 前往聯網索引標籤，選擇網路界面。
   - 依次選擇動作、變更來源/目的地檢查、停用。

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

步驟 13：測試連線

完成此步驟，即可確認網際網路流量是否已透過 BYOIP 位址正確路由至目標執行個體。

1. 在目標執行個體上，透過 tcpdump 監控傳入流量：

   ```
   sudo tcpdump -i any icmp
   ```

2. 透過另一終端機或電腦，測試與 BYOIP IP 位址的連線：

   ```
   ping 203.0.113.10
   ```

3. 預期結果：

   - Ping 測試應該成功，並顯示 BYOIP IP 位址的回應。
   - tcpdump 應顯示來自 BYOIP 位址的傳入封包，類似於：

     ```
     12:34:56.789012 IP 203.0.113.100 > 203.0.113.10: ICMP echo request, id 1234, seq
      1, length 64
     12:34:56.789123 IP 203.0.113.10 > 203.0.113.100: ICMP echo reply, id 1234, seq 1,
      length 64
     ```

   - 流量應顯示來自外部 IP 位址，證明網際網路閘道輸入路由正在將網際網路流量傳送至您的執行個體。

疑難排解

依照本節內容解決設定網際網路閘道輸入路由時可能遇到的常見問題。

流量無法抵達執行個體

- 驗證路由表是否已將正確的 ENI ID 設定為目標。
- 確認 BYOIP 集區已與網際網路閘道路由表建立關聯。
- 檢查執行個體是否已停用來源/目的地檢查。
- 確保安全群組允許所測試的流量類型。

路由建立失敗

- 驗證 BYOIP 集區是否已正確與路由表建立關聯。
- 確認目的地 CIDR 是否處於 BYOIP 範圍內。
- 檢查目標 ENI 是否存在且已附加至執行中的執行個體。
- 確保 BYOIP 字首介於 /23 至 /28 之間 (不支援超出此範圍的字首)。

Ping/連線失敗

- 驗證 IP 位址是否已新增至執行個體介面。
- 檢查安全群組是否允許 ICMP (用於 ping) 或相關連接埠。
- 確認執行個體是否處於執行中狀態。
- 在多個外部位置進行測試。

進階選項：整合路由伺服器實現動態路由

對於需要自動容錯移轉的環境，此功能可與 VPC 路由伺服器整合，實現以下效果：

- 執行個體故障時動態更新路由。
- 無需手動干預路由管理。
- 為關鍵工作負載提供企業級可用性。

這對於需要高可用性的電信業者與 IoT 使用案例尤其重要。

> **Note**
>
> 需注意，搭配多個 BGP 對等使用路由伺服器時，單一路由表最多容許 32 個 BGP 對等公告相同字首。

對於需要動態路由、自動容錯移轉和跨多個執行個體負載分佈的環境，請考慮與 AWS Route Server 整合。路由伺服器支援 BGP 型動態路由 (而非靜態路由)，提供以下能力：

- 透過 BGP 從執行個體執行動態路由公告。
- 在多個目標執行個體間執行自動容錯移轉。
- 跨多個端點實現負載分佈。

- 透過 BGP 協定執行集中路由管理。

這是企業級部署的重要使用案例，能充分滿足高可用性與動態路由能力需求。如需有關路由伺服器設定的詳細說明，請參閱 AWS 路由伺服器文件。

清除

為避免持續產生費用，您應刪除在本教學課程中建立的資源：

步驟 1：終止 EC2 執行個體

完成此步驟，即可終止 EC2 執行個體，避免運算資源持續產生費用。

AWS 主控台

1. 開啟 Amazon EC2 主控台。
2. 在 EC2 主控台的導覽窗格中，選擇執行個體。
3. 選取您的執行個體，選擇執行個體狀態、終止執行個體。
4. 選擇終止加以確認。

AWS CLI

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 --region us-east-1
```

步驟 2：從 VPC 分離網際網路閘道

完成此步驟，即可從 VPC 分離並刪除網際網路閘道。

AWS 主控台

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 主控台的導覽窗格中，選擇網際網路閘道。
3. 選取您的網際網路閘道，然後選擇動作、從 VPC 分離。
4. 選擇分離網際網路閘道。
5. 完成分離後，選擇動作、刪除網際網路閘道。
6. 選擇刪除網際網路閘道。

AWS CLI

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1

aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --region
 us-east-1
```

步驟 3：刪除 VPC

完成此步驟，即可刪除 VPC 及所有相關資源，從而完成清理程序。

AWS 主控台

1. 在 VPC 主控台中，選擇您的 VPC。
2. 選取您的 VPC，然後選擇動作、刪除 VPC。
3. 輸入 **delete** 進行確認，然後選擇刪除。

AWS CLI

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0 --region us-east-1
```

> **Note**
>
> 刪除 VPC 也會隨之刪除關聯的子網路、路由表與安全群組。

> **Note**
>
> BYOIP 集區仍可供日後使用，不會在此清理程序中刪除。

透過 VPC 路由伺服器在 VPC 中進行動態路由

Amazon VPC 路由伺服器可簡化 VPC 及其網際網路閘道內部署的工作負載之間的流量路由。透過此功能，VPC 路由伺服器可使用您偏好的 IPv4 或 IPv6 路由動態更新 VPC 與網際網路閘道路由表，為這些工作負載實現路由容錯能力。這讓您能夠自動重新路由 VPC 內的流量，進而提高 VPC 路由的可管理性，以及與第三方工作負載的互通性。

路由伺服器支援下列路由表類型：

- 未與子網路關聯的 VPC 路由表
- 子網路由表
- 網際網路閘道路由表

路由伺服器不支援與虛擬私有閘道關聯的路由表。若要將路由傳播至傳輸閘道路由表，請參閱 Transit Gateway Connect。

配額

如需有關 Amazon VPC 路由伺服器相關配額的資訊，請參閱路由伺服器配額。

定價

如需有關 Amazon VPC 路由伺服器相關成本的資訊，請參閱「Amazon VPC 定價」頁面上的 VPC 路由伺服器索引標籤。

目錄

- 術語
- Amazon VPC 路由伺服器的運作方式
- 路由伺服器對等記錄功能
- 入門教學課程

術語

本指南中使用下列術語：

- FIB：轉送資訊庫 (FIB) 作為路由伺服器的轉送表，其中收錄了路由伺服器評估所有可用路由資訊和政策後，從 RIB 中篩選出的最佳路徑路由。安裝在路由表上的 FIB 路由。每當 RIB 發生變更時，系統就會重新計算 FIB。
- RIB：路由資訊庫 (RIB) 作為資料庫，儲存路由器或路由系統收集的所有路由資訊與網路拓撲資料，例如從 BGP 對等收集到的路由。RIB 每當收到新的路由資訊或現有路由變更時，就會更新。這可確保路由伺服器一律具有網路拓撲的最新檢視，並且可以作出最佳的路由決策。
- 路由伺服器：路由伺服器元件會使用轉送資訊庫 (FIB) 中的 IPv4 或 IPv6 路由來更新您的 VPC 與網際網路閘道路由表。路由伺服器代表單一 FIB 和路由資訊庫 (RIB)。
- 路由伺服器關聯：路由伺服器關聯是路由伺服器與 VPC 之間建立的連線。

- 路由伺服器端點：路由伺服器端點是子網路內的 AWS受管元件，可協助路由伺服器與 BGP 對等之間的 BGP （邊界閘道通訊協定） 連線。
- 路由伺服器對等：路由伺服器對等是路由伺服器端點與部署在其中的裝置之間的工作階段 AWS （例如防火牆設備或在 EC2 執行個體上執行的其他網路安全函數）。裝置必須符合下列要求：
  - 在 VPC 中具有彈性網路介面
  - 支援 BGP (邊界閘道協定)
  - 可以啟動 BGP 工作階段
- 路由伺服器傳播：啟用後，路由伺服器傳播會在您指定的路由表中安裝 FIB 中的路由。路由伺服器支援 IPv4 與 IPv6 路由傳播。

Amazon VPC 路由伺服器的運作方式

本節說明 Amazon VPC 路由伺服器的運作方式，並協助您了解其如何為在子網路中執行的工作負載實現路由容錯能力。

目錄

- 概要
- 圖表

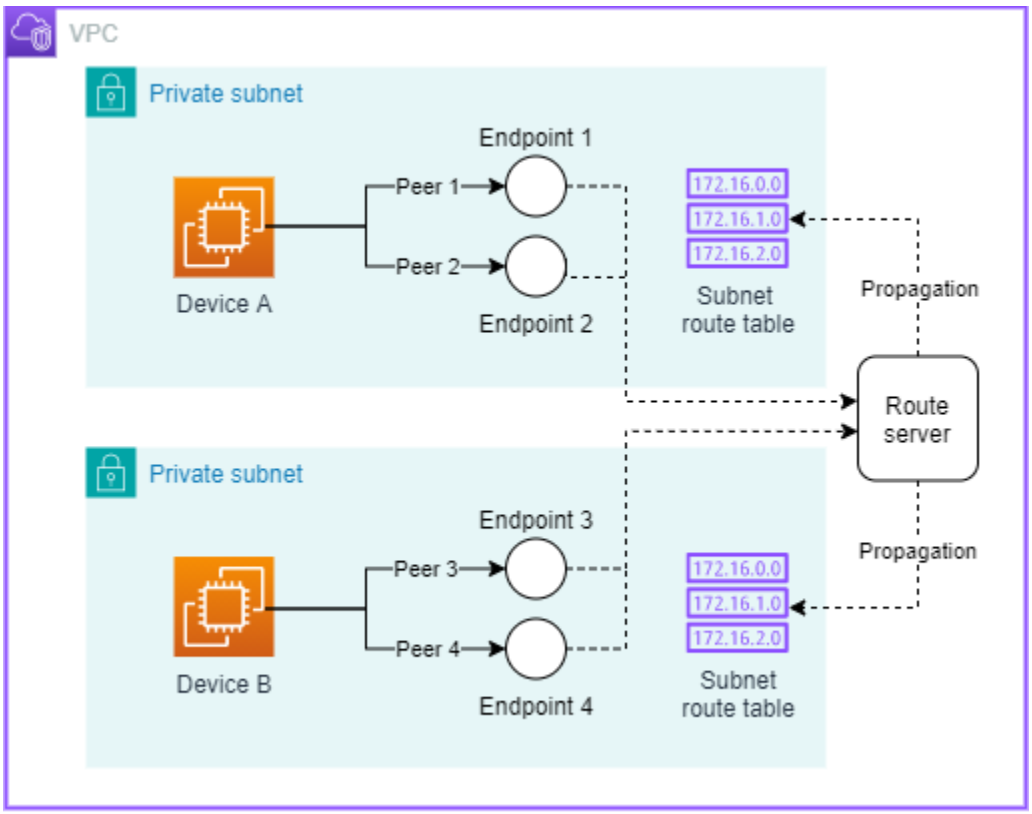
概要

Amazon VPC 路由伺服器的運作方式：

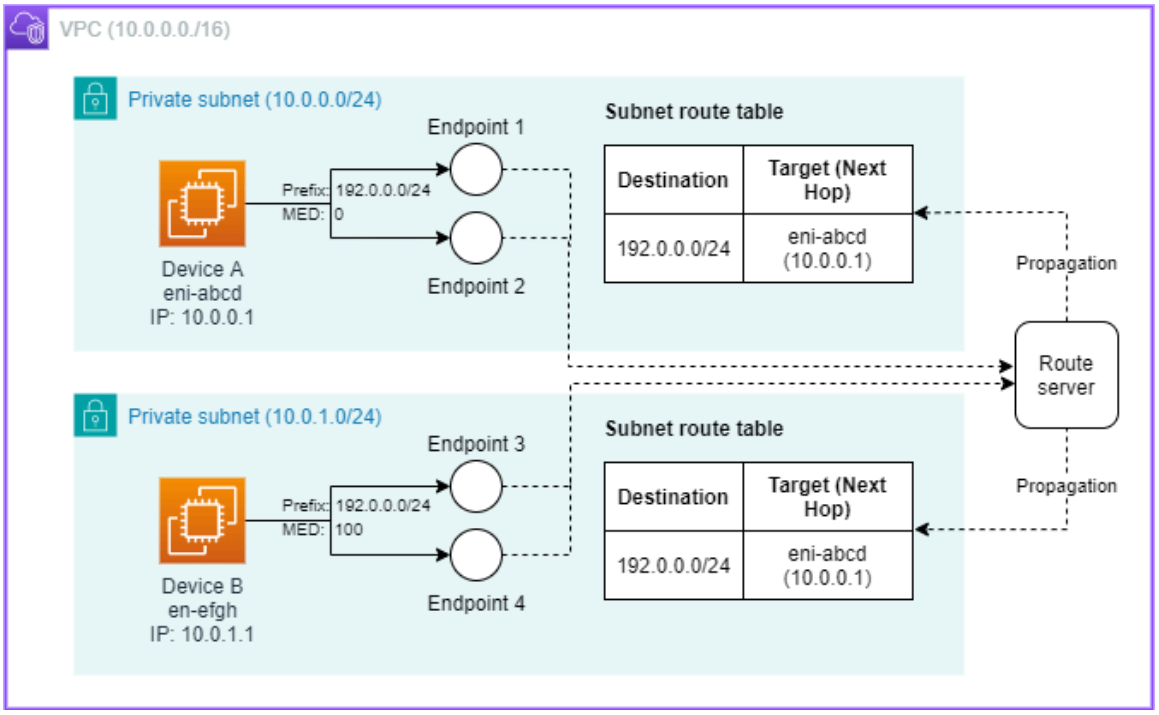
1. 您可以將網路裝置 (例如，在 VPC 中的 EC2 執行個體上執行的防火牆) 設定為使用 Amazon VPC 路由伺服器。
2. 網路裝置失敗。
3. 路由伺服器端點會透過路由伺服器對等上設定的 BFD (雙向轉送偵測) 偵測失敗。
4. 路由伺服器端點會更新路由伺服器，以撤銷路由資訊庫 (RIB) 中失敗的裝置是下一個躍點的路由。
5. 路由伺服器會根據 RIB 運算出轉送資訊庫 (FIB)，並選取最佳可用路由。
6. 路由伺服器會使用來自 FIB 的路由更新設定的路由表。
7. 所有新流量都會轉送至待命裝置。

圖表

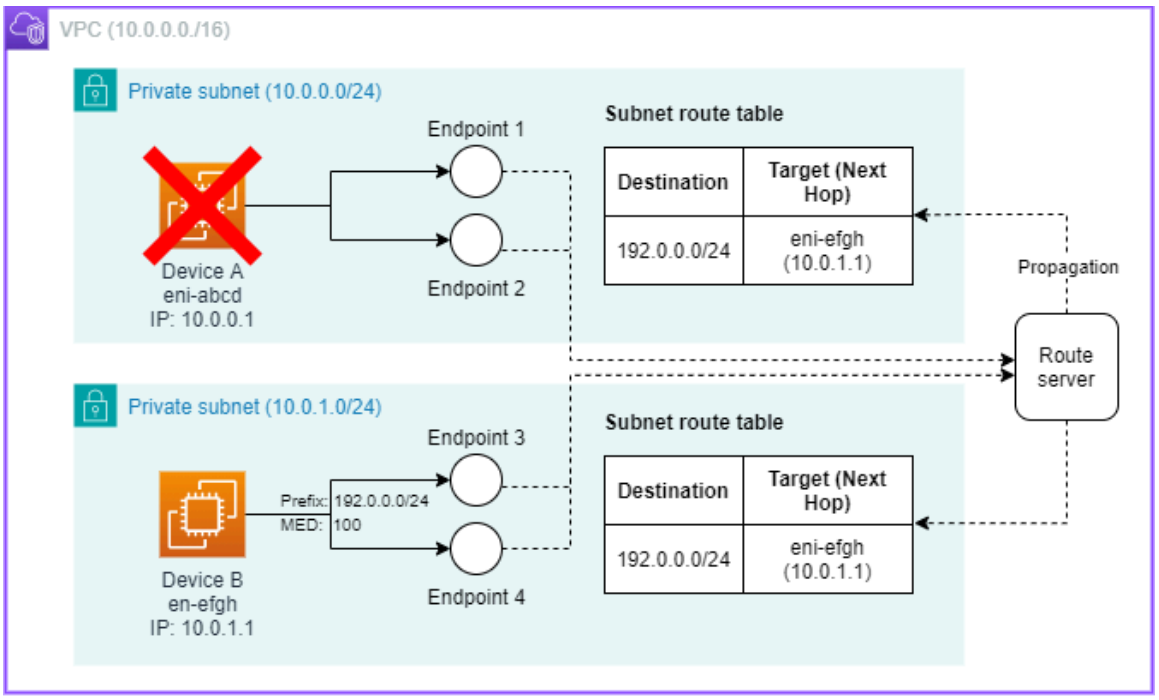
以下是 VPC 路由伺服器的範例圖表，其中已針對兩個子網路中的裝置設定路由伺服器端點。



以上述範例作為基準，以下範例展示了更詳細的設計，其中裝置 A 與裝置 B 都透過 BGP 公告，它們可以接受目的地 IP 在 192.0.0.0/24 (從 192.0.0.0 至 192.0.0.255) 範圍內的任何流量。根據 MED (Multi-Exit Discriminator) 屬性為 0 的情況，路由伺服器可知裝置 A 應優先於裝置 B。路由伺服器會從裝置 A 取得路由與 MED 屬性，並將該路由安裝在子網路路由表中，並以裝置 A 的網路介面作為「下一個躍點」。因此，子網路內目的地 IP 在 192.0.0.0/24 範圍內的任何流量都會傳送至裝置 A。然後，裝置 A 會處理並隨後傳送這些流量。目的地為 192.0.0.0/24 的任一子網路 (10.0.0.0/24 或 10.0.1.0/24) 內的流量，將路由至裝置 A eni-abcd (10.0.0.1) 作為下一個躍點。



以下最後一個範例說明了路由伺服器如何處理容錯移轉。雖然根據 MED 屬性值較高的情況，路由伺服器可知裝置 A 優先於裝置 B，但如果裝置 A eni-abcd (10.0.0.1) 失敗，路由伺服器會更新子網路路由表，目的地為 192.0.0.0/24 的流量會路由至裝置 B eni-efgh (10.0.1.1) 作為下一個躍點。



路由伺服器對等記錄功能

需要執行下列動作時，請使用 VPC 路由伺服器對等記錄功能：

- 監控 BGP 與 BFD 工作階段運作狀態
- 對連線問題進行疑難排解
- 檢閱歷史工作階段變更
- 追蹤網路狀態

定價

- CloudWatch：將路由伺服器對等日誌發布至 CloudWatch Logs 時，會對公開日誌收取資料擷取和存檔費用。
- S3：將路由伺服器對等日誌發布至 Amazon S3 時，會對公開日誌收取資料擷取和存檔費用。
- Data Firehose：會收取標準擷取和傳送費用。

已取代的日誌是來自特定 AWS 服務的日誌，可用於磁碟區分層定價，並交付至 CloudWatch Logs、Amazon S3 或 Amazon Data Firehose。如需詳細資訊，請開啟 Amazon CloudWatch 定價，選取 Logs (日誌)，然後尋找 Vended Logs (付費日誌)。

日誌格式範例

```
{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643505367,
    "type": "RouteStatus",
    "status": "ADVERTISED",
    "message": {
        "prefix": "10.24.34.0/32",
        "asPath": "65000",
        "med": 100,
        "nextHopIp": "10.24.34.1"
    }
}

{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643490000,
    "type": "BGPStatus",
    "status": "UP",
    "message": null
```

```
}
```

其中：

- `resource_arn` 是路由伺服器對等的 ARN。
- `event_timestamp` 是事件的時間戳記。
- 我們產生的日誌事件的 `type` (`RouteStatus`、`BGPStatus`、`BFDStatus`)。
- `status` 欄位是狀態更新。
  - 對於 `RouteStatus` 類型訊息
    - `ADVERTISED` (路由已由對等公告)
    - `UPDATED` (現有路由已由對等更新)
    - `WITHDRAWN` (路由已由對等撤銷)
  - 對於 `BFDStatus` 與 `BGPStatus` 更新
    - UP, DOWN.
- `message` 欄位目前僅用於 RouteStatus 訊息類型的路由屬性，但可能會填入任何類型訊息的相關資訊。

AWS Management Console

若要建立路由伺服器對等日誌：

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中的虛擬私有雲端下，選擇路由伺服器。
3. 在路由伺服器頁面上，選擇路由伺服器對等。
4. 選擇日誌交付索引標籤。
5. 選擇新增日誌交付。
6. 選擇目的地並進行設定：
   - Amazon CloudWatch Logs
     - 日誌類型：要交付的日誌類型。唯一支援的日誌類型是 EVENT_LOGS。
     - 目的地日誌群組：用於接收日誌的 CloudWatch 日誌群組。您可以挑選現有的日誌群組或建立新的日誌群組 (範例：/aws/vpc/route-server-peers)。
     - 欄位選取：要包含在日誌中的資料欄位。
     - 輸出格式：日誌的格式：

- JSON：用於電腦處理的結構化格式
- 文字：純文字格式

- 欄位分隔符號：使用文字格式時，這是分隔欄位的字元 (範例：逗號、製表符、空格)。

- Amazon S3
  - 跨帳戶 - 將日誌傳送至不同的 AWS 帳戶
    - 日誌類型：要交付的日誌類型。唯一支援的日誌類型是 EVENT_LOGS。
    - 交付目的地 ARN：將傳送日誌之另一個 AWS 帳戶中 S3 儲存貯體的 Amazon Resource Name。
    - 欄位選取：要包含在日誌中的資料欄位。
    - 尾碼：新增至日誌檔案名稱的結尾 (範例：.log、.txt)。
    - Hive 相容：開啟後，系統會將日誌整理在資料夾結構中，該資料夾結構可以使用 Hive 型工具，以便於使用 Amazon Athena 等服務進行搜尋。
    - 欄位分隔符號：使用文字格式時，這是分隔欄位的字元。
  - 在目前帳戶中
    - 日誌類型：要交付的日誌類型。唯一支援的日誌類型是 EVENT_LOGS。
    - 目的地 S3 儲存貯體：您帳戶中用於接收日誌的 S3 儲存貯體。您可以指定子資料夾路徑。
    - 欄位選取：要包含在日誌中的資料欄位。
    - 尾碼：新增至日誌檔案名稱的結尾 (範例：.log、.txt)。
    - Hive 相容：開啟後，系統會將日誌整理在資料夾結構中，該資料夾結構可以使用 Hive 型工具以便於進行搜尋。
    - 欄位分隔符號：使用文字格式時，這是分隔欄位的字元。
- Amazon Data Firehose
  - 跨帳戶
    - 日誌類型：要交付的日誌類型。唯一支援的日誌類型是 EVENT_LOGS。
    - 交付目的地 ARN：另一個 AWS 帳戶中 Firehose 交付串流的 Amazon Resource Name。
    - 欄位選取：要包含在日誌中的資料欄位。
    - 欄位分隔符號：使用文字格式時，這是分隔欄位的字元。
  - 在目前帳戶中
    - 日誌類型：要交付的日誌類型。唯一支援的日誌類型是 EVENT_LOGS。

- 交付目的地串流：您帳戶中用於接收日誌的 Firehose 交付串流。該串流必須使用 "Direct Put" 來源類型。
- 欄位選取：要包含在日誌中的資料欄位。
- 輸出格式：日誌的格式：
  - JSON：用於電腦處理的結構化格式
  - 文字：純文字格式
- 欄位分隔符號：使用文字格式時，這是分隔欄位的字元。

Command line

本節中的命令與《AWS CLI 命令參考》連結。本文件旨在詳細說明執行命令時可使用的選項。

若要建立路由伺服器對等日誌：

1. 使用 put-delivery-source 命令。
   - 範例請求

```
aws logs put-delivery-source --name "source-rsp-1234567890abcdef0" --
resource-arn "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0" --log-type "EVENT_LOGS"
```

   - 回應範例

```
{
     "deliverySource": {
        "name": "source-rsp-1234567890abcdef0",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-source:source-
rsp-1234567890abcdef0",
        "resourceArns": [
            "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0"
        ],
        "service": "ec2",
        "logType": "EVENT_LOGS"
    }
}
```

2. 使用 put-delivery-destination 命令。

- 下列 AWS CLI 範例會建立路由伺服器日誌。日誌會傳送至指定的日誌群組。
- 範例請求

```
aws logs put-delivery-destination --name "destination-rsp-abcdef01234567890"
 --destination-resource-arn "arn:aws:logs:us-east-1:111122223333:log-group:/
aws/vendedlogs/ec2/route-server-peer/EVENT_LOGS/rsp-abcdef01234567890"
```

- 回應範例

```
{
     "deliveryDestination": {
        "name": "destination-rsp-abcdef01234567890",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "deliveryDestinationConfiguration": {
            "destinationResourceArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/vendedlogs/ec2/route-server-peer/
EVENT_LOGS/rsp-abcdef01234567890"
        }
    }
}
```

3. 使用 create-delivery 命令。

- 範例請求

```
aws logs create-delivery --delivery-source-name "source-rsp-1234567890abcdef0"
 --delivery-destination-arn "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890"
```

- 回應範例

```
{
     "delivery": {
        "id": "1234567890abcdef0",
        "arn": "arn:aws:logs:us-
east-1:111122223333:delivery:1234567890abcdef0",
        "deliverySourceName": "source-rsp-1234567890abcdef0",
        "deliveryDestinationArn": "arn:aws:logs:us-
east-1:111122223333:delivery-destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
```

```
        "recordFields": [
            "resource_arn",
            "event_timestamp",
            "type",
            "status",
            "message"
        ]
    }
}
```

入門教學課程

本教學課程會逐步引導您設定 VPC 路由伺服器，以在 VPC 中啟用動態路由。您將了解如何建立與設定所有必要的元件、建立 BGP 對等互連，以及驗證適當的操作。本教學課程涵蓋從初始 IAM 設定到測試與清理的所有內容。

在開始本教學課程之前，請確認已滿足以下條件：

- 您 AWS 帳戶的管理存取權
- 要啟用動態路由的 VPC 具備至少兩個子網路
- 具備支援 BGP 且可作為路由伺服器對等裝置的網路裝置 (例如在 EC2 執行個體上執行的防火牆)
- 基本熟悉 BGP 概念和 AWS 聯網

您可以使用 AWS 管理主控台或 來完成這些步驟 AWS CLI。每個步驟都提供這兩種使用方法。

預估完成時間：15-30 分鐘

步驟

- 步驟 1：設定必要的 IAM 角色許可
- 步驟 2：建立路由伺服器
- 步驟 3：將路由伺服器與 VPC 建立關聯
- 步驟 4：建立路由伺服器端點
- 步驟 5：啟用路由伺服器傳播
- 步驟 6：建立路由伺服器對等
- 步驟 7：從裝置啟動 BGP 工作階段
- 步驟 8：清除

步驟 1：設定必要的 IAM 角色許可

若要使用 VPC 路由伺服器，請確保您使用的 IAM 使用者或角色具有必要的 IAM 許可。以下是關於每個 API 需要哪些許可的指南：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:DeleteTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerEndpoint",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*"
        }
    ]
}
```

步驟 2：建立路由伺服器

完成本節中的步驟即可建立路由伺服器。

路由伺服器元件會使用轉送資訊庫 (FIB) 中的 IPv4 或 IPv6 路由來更新您的 VPC 與網際網路閘道路由表。路由伺服器代表單一 FIB 和路由資訊庫 (RIB)。

AWS Management Console

建立路由伺服器

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中的虛擬私有雲端下，選擇路由伺服器。

3. 在路由伺服器頁面上，選擇建立路由伺服器。
4. 在建立路由伺服器頁面上，進行下列設定：

   - 在名稱欄位中，輸入路由伺服器的名稱 (例如 "my-route-server-01")。名稱長度必須小於 255 個字元。
   - 在 Amazon 端 ASN 欄位中，輸入 BGP ASN 值。此值必須介於 1-4294967295 的範圍內。建議使用 64512–65534 (16 位元 ASN) 或 4200000000–4294967294 (32 位元 ASN) 範圍內的私有 ASN。
   - 在持續路由欄位中，選擇啟用或停用。此選項決定在所有 BGP 工作階段終止後是否維持路由：
     - 如果啟用：即使所有 BGP 工作階段都結束，路由仍會保留在路由伺服器的路由資料庫中
     - 如果停用：所有 BGP 工作階段結束後，路由將從路由資料庫中移除
   - 如果已啟用持續路由，請在保持持續時間欄位中輸入 1-5 分鐘之間的值。此持續時間指定 BGP 重新建立之後，路由伺服器取消持久保持路由前的等待時間。例如，如果將此時間設定為 1 分鐘，則裝置在重新建立 BGP 後，有 1 分鐘的時間重新學習並公告其路由，然後路由伺服器才會恢復正常功能。雖然 1 分鐘通常就已足夠，但如果 BGP 網路需要更多時間來完全重新建立與重新學習所有路由，則可以設定最多 5 分鐘。
   - (選用) 若要啟用 BGP 狀態變更的 SNS 通知，請將啟用 SNS 通知開關切換為開啟。啟用 SNS 通知後，可將路由伺服器對等上的 BGP 或 BFD 工作階段狀態變更以及路由伺服器端點的維護通知持續傳送至 AWS佈建的 SNS 主題。如需有關這些通知的詳細資訊，請參閱以下 SNS 通知詳細資訊表。
5. (選用) 若要將標籤新增至路由伺服器，請向下捲動至標籤 – 選用區段，然後選擇新增標籤。輸入每個標籤的索引鍵和選用值。您最多可以新增 50 個標籤。
6. 檢閱設定，然後選擇建立路由伺服器。
7. 等待路由伺服器建立。完成後，系統會將您重新導向至路由伺服器頁面，您可以在其中看到狀態為可用的新路由伺服器。

Command line

依照下列程序建立新的路由伺服器，以管理 VPC 中的動態路由。

在 `--amazon-side-asn` 欄位中輸入 BGP ASN 值。此值必須介於 1-4294967295 的範圍內。建議使用 64512–65534 (16 位元 ASN) 或 4200000000–4294967294 (32 位元 ASN) 範圍內的私有 ASN。

1. 命令：

```
aws ec2 create-route-server --amazon-side-asn 65000
```

回應：

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "pending"
    }
}
```

2. 等待路由伺服器變為可用。

命令：

```
aws ec2 describe-route-servers
```

回應：

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "available"
    }
}
```

SNS 通知詳細資訊

下表顯示 Amazon VPC 路由伺服器將使用 Amazon SNS 傳送之訊息的相關詳細資訊：

標準欄位		訊息屬性 (中繼資料)			
Message	傳送時機	timestamp	eventCode	routeServerEndpointId	affectedRouteServerPeerIds

標準欄位		訊息屬性 (中繼資料)			
路由伺服器端點 [ENDPOINT ID] 正在進行維護。BFD 和 BGP 工作階段可能會受影響。	路由伺服器端點維護	格式：2025-02-17T15:55:00Z	ROUTE_SERVER_ENDPOINT_MAINTENANCE	受影響的端點 ID	受影響的對等 ID 清單
Message	傳送時機	timestamp	eventCode	routeServerPeerId	newBgpStatus
路由伺服器對等 [PEER ID] 的 BGP 現在 [UP/DOWN]。	路由伺服器對等 BGP 狀態變更	格式：2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	受影響的對等 ID	UP 或 DOWN
Message	傳送時機	timestamp	eventCode	routeServerPeerId	newBfdStatus
路由伺服器對等 [PEER ID] 的 BFD 現在 [UP/DOWN]。	路由伺服器對等 BFD 狀態變更	格式：2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	受影響的對等 ID	UP 或 DOWN

步驟 3：將路由伺服器與 VPC 建立關聯

完成本節中的步驟即可將路由伺服器與 VPC 建立關聯。

路由伺服器關聯是指路由伺服器與 VPC 之間建立的連線。此基本組態步驟可讓路由伺服器能夠使用 VPC 中的設備。

建立路由伺服器關聯後：

- 該關聯會將路由伺服器連結至特定 VPC。
- 它可讓路由伺服器與 VPC 子網路內的路由表互動。
- 該關聯可讓路由伺服器在相關聯的 VPC 內接收與傳播路由。
- 該關聯會建立路由伺服器可以操作的範圍。

路由伺服器關聯的關鍵層面：

- 每個路由伺服器可以與一個 VPC 建立關聯。依預設，每個 VPC 最多可以有 5 個不同的路由伺服器關聯。如需有關配額的詳細資訊，請參閱路由伺服器配額。
- 必須先建立關聯，路由伺服器才能管理路由。
- 您可以監控關聯以追蹤其狀態 (例如「正在建立關聯」與「已關聯」)。
- 如果您不再希望路由伺服器在該 VPC 中運作，則可以移除關聯 (取消關聯)。

AWS Management Console

將路由伺服器與 VPC 建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中的虛擬私有雲端下，選擇路由伺服器。
3. 選取要與 VPC 建立關聯的路由伺服器。
4. 在關聯索引標籤上，選擇關聯路由伺服器。
5. 在「關聯路由伺服器」對話方塊中：
   - 路由伺服器 ID 欄位會自動填入所選取的路由伺服器
   - 在 VPC ID 欄位中，從下拉式清單中選擇要關聯的 VPC
6. 選擇關聯路由伺服器。
7. 等待關聯完成。完成後，關聯索引標籤上的狀態會顯示為已關聯。

Command line

依照下列程序將路由伺服器與 VPC 建立關聯。

1. 命令：

```
aws ec2 associate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

回應：

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associating"
    }
}
```

2. 等待關聯完成。

命令：

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

回應：

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associated"
    }
}
```

步驟 4：建立路由伺服器端點

完成本節中的步驟即可建立路由伺服器端點。為每個子網路建立兩個端點以進行備援。

路由伺服器端點是子網路內的 AWS受管元件，可協助路由伺服器與 BGP 對等之間的 BGP（邊界閘道通訊協定）連線。

路由伺服器端點是您的網路裝置與路由伺服器建立 BGP 工作階段的「聯絡點」。它們是實際處理 BGP 連線的元件，而路由伺服器本身只管理路由決策與路由傳播。

> **Note**
>
> 路由伺服器端點的費用為每小時 0.75 USD。

AWS Management Console

建立路由伺服器端點

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中的虛擬私有雲端下，選擇路由伺服器。
3. 選取要為其建立端點的路由伺服器。
4. 在下窗格中，選擇路由伺服器端點索引標籤。
5. 選擇建立路由伺服器端點。
6. 在建立路由伺服器端點頁面上，進行下列設定：
   - 在名稱欄位中，輸入端點的描述性名稱。
   - 在路由伺服器欄位中，確認已選取正確的路由伺服器。
   - 在子網路欄位中，選取要在其中建立端點的子網路。
7. (選用) 若要將標籤新增至路由伺服器端點，請向下捲動至標籤 – 選用區段，然後選擇新增標籤。輸入每個標籤的索引鍵和選用值。
8. 檢閱設定，然後選擇建立路由伺服器端點。
9. 等待端點建立。完成後，您會看到成功訊息。
10. 重複步驟 5-9，使用不同的名稱在相同子網路中建立第二個端點。
11. 針對每個您需要路由伺服器端點的子網路重複步驟 5-10。
12. 建立端點之後，請返回路由伺服器的路由伺服器端點索引標籤。
13. 確認您看到每個子網路有兩個端點。
14. 檢查每個端點的狀態是否為可用。

Command line

依照下列程序建立路由伺服器端點。

1. 命令：

```
aws ec2 create-route-server-endpoint --route-server-id rs-1 --subnet-id subnet-1
```

回應：

```
{
```

```
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending"
    }
}
```

2. 端點建立後可能需要幾分鐘才會完全可用。

   命令：

   ```
   aws ec2 describe-route-server-endpoints
   ```

   回應：

   ```
   {
       "RouteServerEndpoint": {
           "RouteServerId": "rs-1",
           "RouteServerEndpointId": "rse-1",
           "VpcId": "vpc-1",
           "SubnetId": "subnet-1",
           "EniId": "eni-123",
           "EniAddress": "10.1.2.3",
           "State": "available"
       }
   }
   ```

重複以上步驟，使用不同的名稱在同一個子網路中建立第二個端點，並為每個您需要路由伺服器端點的子網路建立端點。

步驟 5：啟用路由伺服器傳播

完成此步驟，即可啟用路由伺服器傳播。

啟用後，路由伺服器傳播會在您指定的路由表中安裝 FIB 中的路由。路由伺服器支援 IPv4 與 IPv6 路由傳播。

路由伺服器傳播機制會自動更新路由表，無需手動更新路由表，路由伺服器會自動根據 FIB 中的路由將適當的路由傳播至已設定的路由表。

路由伺服器傳播的關鍵層面：

- 組態
  - 將路由伺服器連結至特定路由表
  - 決定哪些路由表將接收動態路由更新
  - 可以針對單個路由表啟用或停用
- 功能
  - 使用從 BGP 對等學習到的路由自動更新路由表
  - 根據 BGP 屬性傳播最佳可用路由
  - 維持指定路由表之間的路由一致性
  - 在網路條件變更時動態更新路由
- 州 (States)
  - 可以啟用 (會傳播路由)
  - 可以停用 (不會傳播路由)

AWS Management Console

啟用路由伺服器傳播

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取要啟用傳播的路由伺服器。
3. 在路由伺服器詳細資訊面板中，選擇傳播索引標籤。
4. 選擇啟用傳播。
5. 在啟用傳播對話方塊中：
   - 路由伺服器 ID 將預先填入。
   - 在路由表下，從下拉式功能表中選取新傳播路由的目的地路由表。
6. 選擇啟用傳播進行確認。
7. 等待傳播清單中的傳播狀態變更為「可用」。
8. 確認選取的路由表是否出現在傳播清單中，且狀態為可用。

Command line

依照下列程序啟用路由伺服器傳播。

1. 命令：

```
aws ec2 enable-route-server-propagation --route-table-id rtb-1 --route-server-id
 rs-1
```

回應：

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "pending"
    }
}
```

2. 等待傳播狀態變更為可用。

命令：

```
aws ec2 get-route-server-propagations --route-server-id rs-1
```

回應：

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "available"
    }
}
```

步驟 6：建立路由伺服器對等

路由伺服器對等是路由伺服器端點與部署在其中的裝置之間的工作階段 AWS （例如防火牆設備或在 EC2 執行個體上執行的其他網路安全函數）。裝置必須符合下列要求：

- 在 VPC 中具有彈性網路介面
- 支援 BGP (邊界閘道協定)
- 可以啟動 BGP 工作階段

> **Note**
>
> 建議為每個路由伺服器端點建立一個路由伺服器對等，以進行備援。

AWS Management Console

建立路由伺服器對等

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽路徑中，選擇 VPC > 路由伺服器對等 > 建立路由伺服器對等。
3. 在詳細資訊下，設定下列項目：
   - 名稱：輸入路由伺服器對等的名稱 (最多 255 個字元)。範例：my-route-server-peer-01
   - 路由伺服器端點 ID：從下拉式清單中選擇路由伺服器端點。也可以選擇建立路由伺服器端點來建立新的路由伺服器端點。
   - 對等位址：輸入對等的 IPv4 位址。必須是有效的 IP 位址。對等位址必須可從路由伺服器端點存取。
   - 對等 ASN：輸入 BGP 對等的 ASN (自治系統編號)。值必須介於 1-4294967295 的範圍內。ASN 通常應使用私有範圍 (16 位元的範圍為 64512-65534，32 位元的範圍為 4200000000-4294967294)
   - 對等活動性偵測：
     - BGP 保持連線 (預設)：標準 BGP 保持連線機制
     - BFD：雙向轉送偵測，以實現更快的容錯移轉
   - (選用) 在標籤下，選擇新增標籤以新增鍵值對標籤。標籤有助於識別和追蹤 AWS 資源。
4. 檢閱設定，然後選擇建立路由伺服器對等。

Command line

依照下列程序建立路由伺服器對等。

1. 命令：

```
aws ec2 create-route-server-peer --route-server-endpoint-id rse-1 --peer-address
 10.0.2.3 --bgp-options PeerAsn=65001,PeerLivenessDetection=bfd
```

回應：

在回應中，狀態值可以是 pending|available|deleting|deleted。

```
{
    "RouteServerPeer": {
        "RouteServerPeerId": "rsp-1",
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "Up"
        }
    }
}
```

2. 等待傳播狀態變更為可用。

命令：

```
aws ec2 describe-route-server-peers
```

回應：

```
{
    "RouteServerPeer": {
        "RouteServerPeerId": "rsp-1",
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "available",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
```

```
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "down"
        }
    }
}
```

步驟 7：從裝置啟動 BGP 工作階段

路由伺服器對等的狀態變為可用後，請將工作負載設定為使用路由伺服器端點啟動 BGP 工作階段。

從子網路中的裝置啟動 BGP 工作階段，不在本指南的範圍內。路由伺服器端點不會啟動 BGP 工作階段。

您可以確認路由表是否包含路由伺服器傳播的最佳路由，藉此檢查 VPC 路由伺服器功能是否運作正常。

步驟 8：清除

本教學課程的建置部分已完成。完成本節中的步驟即可移除您建立的 VPC 路由伺服器元件。

7.1：撤銷裝置上的 BGP 公告

撤銷子網路中裝置上的 BGP 公告，不在本指南的範圍內。視需要向第三方廠商洽詢 BGP 組態。

7.2：停用路由伺服器傳播

依照下列程序停用路由伺服器傳播。

AWS Management Console

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取要停用傳播的路由伺服器。
3. 選擇動作 > 修改路由伺服器。
4. 在路由伺服器詳細資訊面板中，選擇傳播索引標籤。
5. 選擇要停用的傳播，然後選擇停用傳播。

6. 在對話方塊中，選擇停用路由伺服器傳播。

Command line

1. 停用傳播：

```
aws ec2 disable-route-server-route-propagation --route-table-id rtb-1 --route-
server-id rs-1
```

2. 確認傳播已刪除：

```
aws ec2 get-route-server-route-propagations --route-server-id rs-1 [--route-
table-id rtb-1]
```

7.3：刪除路由伺服器對等

依照下列程序刪除路由伺服器對等。

AWS Management Console

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽路徑中，選擇路由伺服器 > 路由伺服器對等。
3. 選取路由伺服器對等。
4. 選擇動作 > 刪除路由伺服器對等。

Command line

1. 刪除對等：

```
aws ec2 delete-route-server-peer --route-server-peer-id rsp-1
```

2. 確認刪除：

```
aws ec2 describe-route-server-peers [--route-server-peer-ids rsp-1] [--filters
 Key=RouteServerId|RouteServerEndpointId|VpcId]
```

7.4：刪除路由伺服器端點

依照下列程序刪除路由伺服器端點。

AWS Management Console

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取要刪除端點的路由伺服器。
3. 選擇路由伺服器端點。
4. 選取端點，然後選擇動作 > 刪除路由伺服器端點。
5. 輸入 delete 並選擇刪除。

Command line

1. 描述端點：

```
aws ec2 describe-route-server-endpoints
```

2. 刪除路由伺服器端點：

```
aws ec2 delete-route-server-endpoint --route-server-endpoint-id rse-1
```

3. 確認端點已刪除：

```
aws ec2 describe-route-server-endpoints [--route-server-endpoint-ids rsp-1] [--
filters Key=RouteServerId|VpcId|SubnetId]
```

7.5：取消路由伺服器與 VPC 的關聯

依照下列程序取消路由伺服器與 VPC 的關聯。

AWS Management Console

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取要取消關聯的路由伺服器。
3. 選擇關聯。
4. 選擇取消關聯路由伺服器。
5. 確認要進行的變更，然後選擇取消關聯路由伺服器。

Command line

1. 取消路由伺服器與 VPC 的關聯：

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. 確認取消關聯：

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

7.6 刪除路由伺服器

依照下列程序刪除路由伺服器。

AWS Management Console

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取要刪除的路由伺服器。
3. 選擇動作 > 刪除路由伺服器。
4. 輸入 delete 並選擇刪除。

Command line

1. 刪除路由伺服器：

```
aws ec2 delete-route-server --route-server-id rs-1
```

2. 確認刪除：

```
aws ec2 describe-route-servers [--route-server-ids rs-1] [--filters Key=VpcId]
```

Amazon VPC 路由伺服器教學課程已完成。

對 VPC 中的連線能力問題進行疑難排解

Reachability Analyzer 是一種靜態組態分析工具。使用 Reachability Analyzer 來分析 VPC 中兩項資源之間的網路連線能力並進行偵錯。Reachability Analyzer 會在可連線虛擬路徑時，在這些路徑之間產生

逐個躍點的詳細資訊，並在無法連線時識別導致阻礙的元件。例如，它可以識別遺漏或設定錯誤的路由表路由。

如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

中間設備路由精靈

如果您想要設定對進入或離開 VPC 的流量路由路徑的精細控制，例如，透過將流量重新引導至安全設備，您可以在 VPC 主控台中使用中間設備路由精靈。中間設備路由精靈可協助您自動建立所需的路由表和路由 (躍點)，以視需要重新引導流量。

中間設備路由精靈可協助您設定下列案例的路由：

- 將流量路由至中間設備設備，例如，設定為安全設備的 Amazon EC2 執行個體。
- 將流量路由至閘道負載平衡器。如需詳細資訊，請參閱《Gateway Load Balancers 使用者指南》。

如需詳細資訊，請參閱the section called “中間設備案例”。

目錄

- 中間設備路由精靈的先決條件
- 將 VPC 流量重新導向至安全設備
- 中間設備路由精靈的考量事項
- 中間設備案例

中間設備路由精靈的先決條件

檢閱 the section called “中間設備路由精靈的考量事項”。然後，請確定您有下列資訊，再使用中間設備路由精靈。

- VPC。
- 流量源自 VPC 或進入 VPC 的資源，例如：網際網路閘道、虛擬私有閘道或網路界面。
- 中間設備網路界面或閘道負載平衡器端點。
- 流量的目的地子網。

將 VPC 流量重新導向至安全設備

中間設備路由精靈可在 Amazon VPC 主控台中使用。

目錄

- 1. 使用中間設備路由精靈建立路由
- 2. 修改中間設備路由
- 3. 刪除中間設備路由精靈組態

1. 使用中間設備路由精靈建立路由

若要使用中間設備路由精靈建立路由

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取您的 VPC，然後選擇 Actions (動作)、Manage middlebox routes (管理中間設備路由)。
4. 選擇 Create route (建立路由)。
5. 在 Specify routes (指定路由) 頁面上，執行下列操作：
   - 對於 Source (來源)，選擇流量的來源。如果您選擇虛擬私有閘道，對於 Destination IPv4 CIDR (目的地 IPv4 CIDR)，輸入從虛擬私有閘道進入 VPC 的內部部署流量的 CIDR。
   - 對於 Middlebox (中間設備)，選擇與中間設備相關聯的網路界面 ID，或者當您使用閘道負載平衡器端點時，請選擇 VPC 端點 ID。
   - 對於 Destination subnet (目的地子網)，選擇目的地子網。
6. (選用) 若要新增另一個目的地子網，請選擇 Add additional subnet (新增其他子網)，然後執行下列操作：
   - 對於 Middlebox (中間設備)，選擇與中間設備相關聯的網路界面 ID，或者當您使用閘道負載平衡器端點時，請選擇 VPC 端點 ID。

     您必須針對多個子網使用相同的中間設備。
   - 對於 Destination subnet (目的地子網)，選擇目的地子網。
7. (選用) 若要新增另一個來源，選擇 Add source (新增來源)，然後重複先前的步驟。
8. 選擇 Next (下一步)。
9. 在 Review and create (檢閱和建立) 頁面上，確認路由，然後選擇 Create routes (建立路由)。

2. 修改中間設備路由

您可以透過變更閘道、中間設備或目的地子網來編輯路由組態。

當您進行任何修改時，中間設備路由精靈會自動執行下列操作：

- 為閘道、中間設備和目的地子網建立新的路由表。
- 將所需路由新增至新路由表。
- 取消中間設備路由精靈與資源關聯的現有路由表的關聯。
- 將中間設備路由精靈建立的新路由表與資源建立關聯。

若要使用中間設備路由精靈修改中間設備路由

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取您的 VPC，然後選擇 Actions (動作)、Manage middlebox routes (管理中間設備路由)。
4. 選擇 Edit routes (編輯路由)。
5. 若要變更閘道，請針對 Source (來源) 選擇流量透過其進入 VPC 的閘道。如果您選擇虛擬私有閘道，針對 Destination IPv4 CIDR (目的地 IPv4 CIDR)，輸入目的地子網 CIDR。
6. 若要新增其他目的地子網，請選擇 Add additional subnet (新增其他子網)，然後執行下列操作：
   - 對於 Middlebox (中間設備)，選擇與中間設備相關聯的網路界面 ID，或者當您使用閘道負載平衡器端點時，請選擇 VPC 端點 ID。

     您必須針對多個子網使用相同的中間設備。
   - 對於 Destination subnet (目的地子網)，選擇目的地子網。
7. 選擇下一步。
8. 在 Review and update (檢閱與更新) 頁面上，會顯示由中間設備路由精靈建立的路由表及其路由的清單。確認路由，然後在確認對話方塊中選擇 Update routes (更新路由)。

3. 刪除中間設備路由精靈組態

如果您決定不再需要中間設備路由精靈組態，您必須手動刪除路由表。

若要刪除中間設備路由精靈組態

1. 檢視中間設備路由精靈路由表。

執行操作之後，中間設備路由精靈建立的路由表會顯示在單獨的路由表頁面上。

2. 刪除顯示的每個路由表。

中間設備路由精靈的考量事項

使用中間設備路由精靈時，請考慮下列事項：

- 如果您想檢查流量，您可以針對來源使用網際網路閘道或虛擬私有閘道。
- 如果您在同一 VPC 內的多個中間設備組態中使用相同的中間設備，請確保兩個子網的中間設備位於相同的躍點位置。
- 設備必須設定在與來源或目的地子網不同的子網中。
- 您必須停用設備上的來源/目的地檢查。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的變更來源或目的地檢查。
- 中間設備路由精靈建立的路由表和路由會計入您的配額中。如需詳細資訊，請參閱the section called “路由表”。
- 如果您刪除資源 (例如網路界面)，路由表與該資源的關聯會被移除。如果資源是目標，路由目的地會設定為黑洞。不會刪除路由表。
- 中間設備的子網和目的地子網必須與非預設路由表建立關聯。

> **Note**
>
> 建議您使用中間設備路由精靈來修改或刪除您使用中間設備路由精靈建立的任何路由表。

- 若透過中間設備路由將流量導向安全設備，則不支援在檢查後進行來源與最終目的地間的安全群組參考。

中間設備案例

Amazon Virtual Private Cloud (VPC) 提供廣泛的網路功能，可讓您自訂和控制虛擬網路中的流量路由。這類功能中的其中一項為中間設備路由精靈，可精細控制進出 VPC 的流量路由路徑。

如果您需要將流量重新導向至安全設備、負載平衡器或其他網路裝置，以用於檢查、監控或最佳化，中間設備路由精靈可以簡化程序。此精靈會自動建立必要的路由表和路徑 (躍點)，以視需要重新導向指定的流量，消除設定複雜路由組態所需的手動工作。

中間設備路由精靈支援幾種不同的案例。例如，您可以使用它來檢查目的地為特定子網路的流量、設定整個 VPC 的中間設備流量路由和檢查，或選擇性地檢查特定子網路之間的流量。這種對流量路由的精細控制可讓您實作進階安全政策、啟用集中式網路監控，或最佳化雲端應用程式的效能。

下列範例介紹中間設備路由精靈的案例。

目錄

- 檢查目的地為子網的流量
- 在 VPC 中設定中間設備流量路由和檢查
- 檢查子網之間的流量

檢查目的地為子網的流量

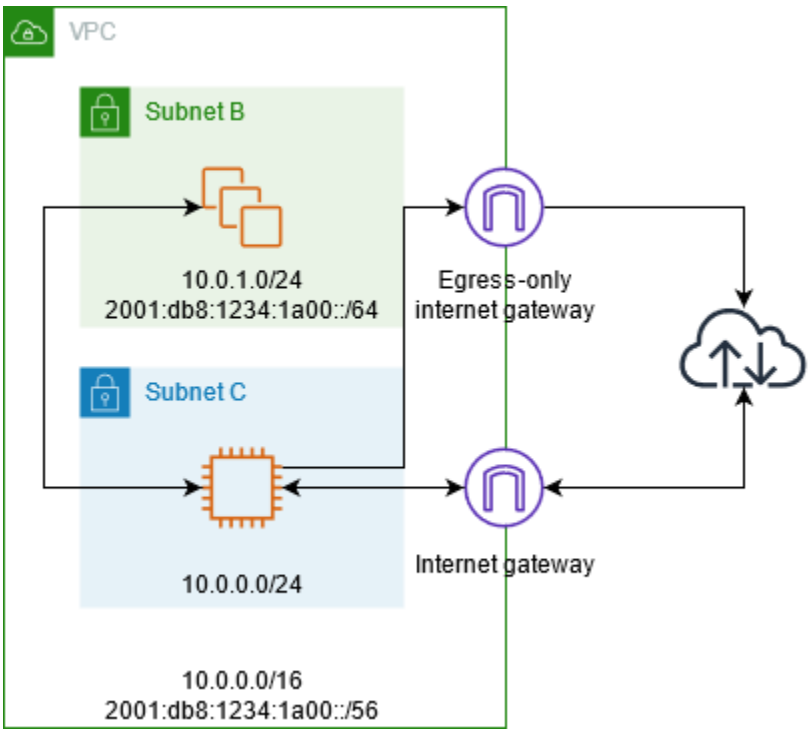
試想這樣一個案例：您的流量透過網際網路閘道進入 VPC，並且您想要使用安裝在 EC2 執行個體上的防火牆設備來檢查目的地為某個子網 (例如子網 B) 的所有流量。應該將防火牆設備安裝和設定在 EC2 執行個體上，且該執行個體位於與 VPC 中子網 B 不同的子網中，例如子網 C。然後您可以使用中間設備路由精靈為子網 B 和網際網路閘道之間的流量設定路由。

中間設備路由精靈會自動執行下列操作：

- 建立下列路由表：
  - 網際網路閘道的路由表
  - 目的地子網的路由表
  - 中間設備子網的路由表
- 將所需路由新增至新路由表，如下列章節所述。
- 將與網際網路閘道、子網 B 和子網 C 相關聯的目前路由表取消關聯。
- 將路由表 A 與網際網路閘道 (中間設備路由精靈中的 Source (來源))、路由表 C 與子網 C (中間設備路由精靈中的 Middlebox (中間設備)) 以及路由表 B 與子網 B (中間設備路由精靈中的 Destination (目的地)) 建立關聯。
- 建立一個標籤，指出其是由中間設備路由精靈建立，並建立指出建立日期的標籤。

中間設備路由精靈不會修改現有的路由表。它會建立新的路由表，然後將其與閘道和子網資源建立關聯。如果您的資源已經明確與現有路由表相關聯，則現有路由表會先被取消關聯，然後新路由表會與您的資源相關聯。系統不會刪除您現有的路由表。

如果您不使用中間設備路由精靈，則您必須手動設定，然後將路由表指派給子網和網際網路閘道。



網際網路閘道路由表

新增以下路由至網際網路閘道的路由表：

目標	Target	用途
10.0.0.0/16	區域	IPv4 的本機路由
10.0.1.0/24	*appliance-eni*	將目的地為子網 B 的 IPv4 流量路由到中間設備
2001:db8:1234:1a00::/56	區域	IPv6 的本機路由
2001:db8:1234:1a00::/64	*appliance-eni*	將目的地為子網 B 的 IPv6 流量路由到中間設備

網際網路閘道和 VPC 之間存在邊緣關聯。

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"

- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

目的地子網路由表

將以下路由新增至目的地子網的路由表中 (範例圖表中的子網 B)。

目標	Target	用途
10.0.0.0/16	區域	IPv4 的本機路由
0.0.0.0/0	*appliance-eni*	將目的地為網際網路的 IPv4 流量路由至中間設備
2001:db8:1234:1a00::/56	區域	IPv6 的本機路由
::/0	*appliance-eni*	將目的地為網際網路的 IPv6 流量路由至中間設備

中間設備子網有子網關聯。

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

中間設備子網路由表

將以下路由新增至中間設備子網的路由表中 (範例圖表中的子網 B)。

目標	Target	用途
10.0.0.0/16	區域	IPv4 的本機路由
0.0.0.0/0	*igw-id*	將 IPv4 流量路由至網際網路閘道
2001:db8:1234:1a00::/56	區域	IPv6 的本機路由

目標	Target	用途
::/0	*eigw-id*	將 IPv6 流量路由至僅輸出網際網路閘道

目的地子網有子網關聯。

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

在 VPC 中設定中間設備流量路由和檢查

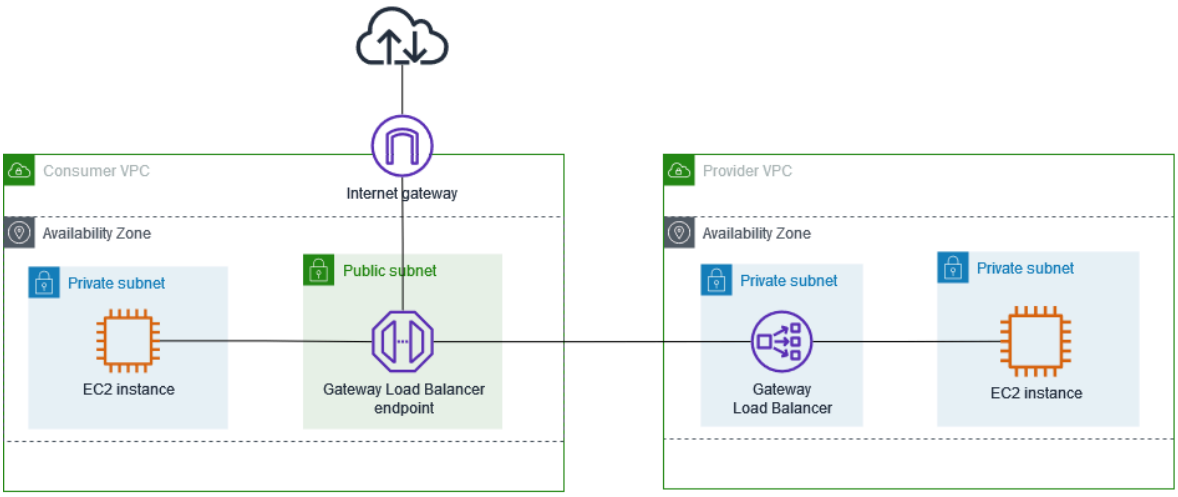
試想這樣一個案例：您需要使用在 Gateway Load Balancer 後方設定的安全設備機群，檢查從網際網路閘道進入 VPC 且目的地為子網路的流量。服務消費者 VPC 的擁有者會在其 VPC (由端點網路介面表示) 的子網中建立 Gateway Load Balancer 端點。所有透過網際網路閘道進入 VPC 的流量會先路由至 Gateway Load Balancer 端點，以便進行檢查，然後再路由至應用程式子網。同樣地，離開應用程式子網的所有流量會先路由至 Gateway Load Balancer 端點，以便進行檢查，然後再路由至網際網路。

中間設備路由精靈會自動執行下列操作：

- 建立路由表。
- 將所需路由新增至新路由表。
- 取消與子網關聯之目前路由表的關聯。
- 將中間設備路由精靈建立的路由表與子網建立關聯。
- 建立一個標籤，指出其是由中間設備路由精靈建立，並建立指出建立日期的標籤。

中間設備路由精靈不會修改現有的路由表。它會建立新的路由表，然後將其與閘道和子網資源建立關聯。如果您的資源已經明確與現有路由表相關聯，則現有路由表會先被取消關聯，然後新路由表會與您的資源相關聯。系統不會刪除您現有的路由表。

如果您不使用中間設備路由精靈，則您必須手動設定，然後將路由表指派給子網和網際網路閘道。



網際網路閘道路由表

網際網路閘道路由表具備下列路由。

目標	Target	用途
### VPC CIDR	區域	本機路由
###### CIDR	*endpoint-id*	將目的地為應用程式子網路的流量路由至 Gateway Load Balancer 端點

與閘道有邊緣關聯。

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

應用程式子網路由表

應用程式子網的路由表具備下列路由。

目標	Target	用途
### VPC CIDR	區域	本機路由

目標	Target	用途
0.0.0.0/0	*endpoint-id*	將流量從應用程式伺服器路由至 Gateway Load Balancer 端點，然後再路由至網際網路

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

提供者子網路由表

提供者子網的路由表具備下列路由。

目標	Target	用途
### VPC CIDR	區域	本機路由。確保源自網際網路的流量會路由至應用程式伺服器
0.0.0.0/0	*igw-id*	將所有流量路由至網際網路閘道

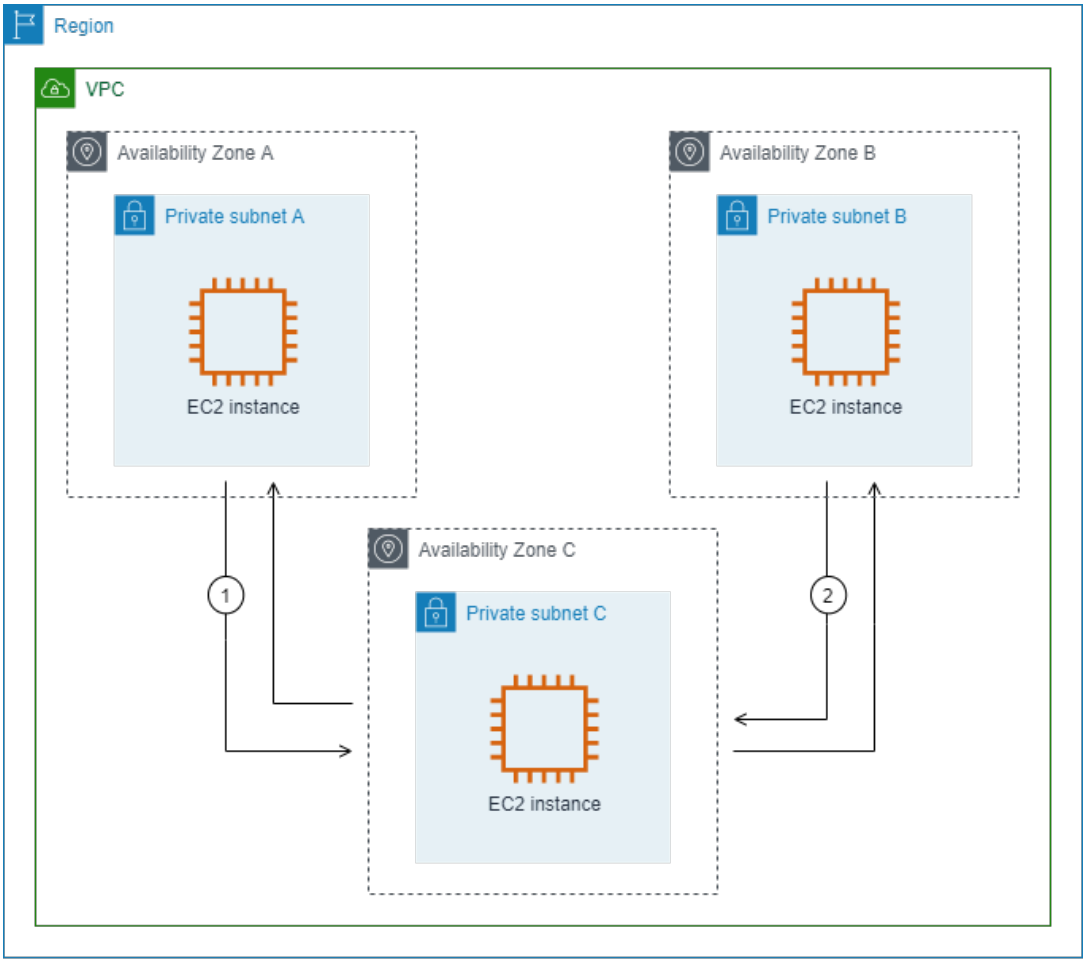
當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

檢查子網之間的流量

試想這樣一個案例：在 VPC 中有多個子網，並且您想要使用防火牆設備來檢查子網之間的流量。在 VPC 之單獨子網中的 EC2 執行個體上設定和安裝防火牆設備。

下圖顯示安裝在子網 C 中 EC2 執行個體上的防火牆設備。該設備可檢查從子網 A 到子網 B (請參閱 1) 以及從子網 B 到子網 A (請參閱 2) 的所有流量。



您可以將主要路由表用於 VPC 和中間設備子網。子網 A 和 B 各有一個自訂路由表。

中間設備路由精靈會自動執行下列操作：

- 建立路由表。
- 將所需路由新增至新路由表。
- 取消與子網關聯之目前路由表的關聯。
- 將中間設備路由精靈建立的路由表與子網建立關聯。
- 建立一個標籤，指出其是由中間設備路由精靈建立，並建立指出建立日期的標籤。

中間設備路由精靈不會修改現有的路由表。它會建立新的路由表，然後將其與閘道和子網資源建立關聯。如果您的資源已經明確與現有路由表相關聯，則現有路由表會先被取消關聯，然後新路由表會與您的資源相關聯。系統不會刪除您現有的路由表。

如果您不使用中間設備路由精靈，則您必須手動設定，然後將路由表指派給子網和網際網路閘道。

自訂子網 A 路由表

子網 A 的路由表具備下列路由。

目標	Target	用途
VPC CIDR	區域	本機路由
### B CIDR	*appliance-eni*	將目的地為子網 B 的流量路由至中間設備

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

自訂子網 B 路由表

子網 B 的路由表具備下列路由。

目標	Target	用途
VPC CIDR	區域	本機路由
### A CIDR	*appliance-eni*	將目的地為子網 A 的流量路由至中間設備

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

主路由表

子網 C 使用主路由表。主路由表具備下列路由。

目標	Target	用途
VPC CIDR	區域	本機路由

當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 索引鍵是 "Origin"，值是 "Middlebox wizard"
- 索引鍵是 "date_created"，值是建立時間 (例如 "2021-02-18T22:25:49.137Z")

刪除子網路

若您不再需要子網路，您可以將其刪除。如果子網路包含任何網路介面，則無法刪除子網路。例如，您必須先終止子網路中的任何執行個體，才能刪除子網路。

當您刪除子網路時，與該子網路相關聯的 CIDR 區塊會返回至 VPC 的可用 IP 位址集區。這表示子網路 CIDR 範圍內的 IP 位址可以重新配置到相同 VPC 內的其他子網路或資源。

請務必注意，刪除子網路不會自動刪除其中的資源。您必須先終止所有 EC2 執行個體、刪除所有網路介面，並移除與子網路相關聯的所有其他資源，才能繼續刪除子網路。

如何使用主控台刪除子網路

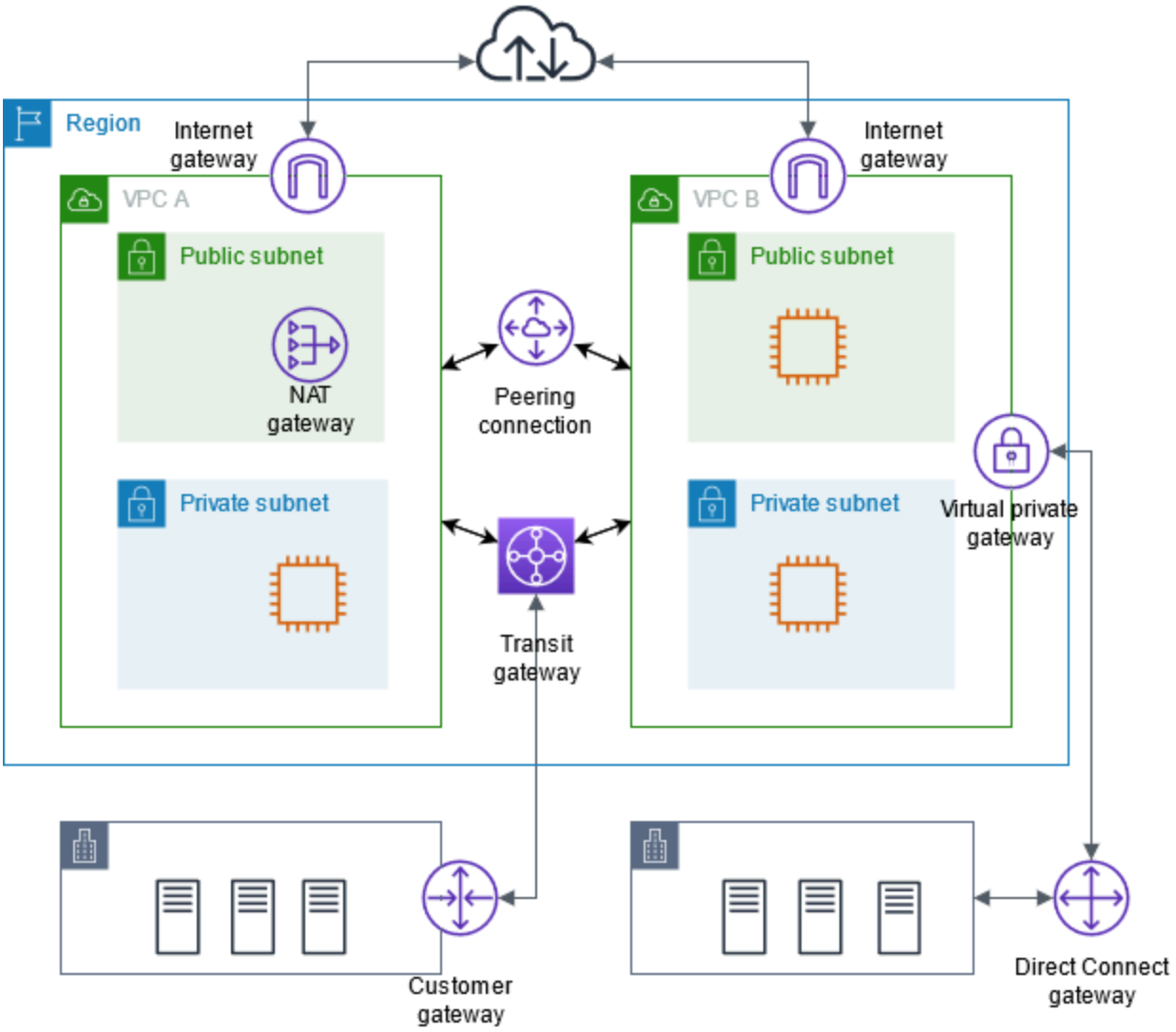
1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 終止子網路中的所有執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的終止您的執行個體。
3. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
4. 在導覽窗格中，選擇 Subnets (子網)。
5. 選取子網路，然後選擇 Actions (動作)、Delete subnet (刪除子網路)。
6. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

如何使用 AWS CLI 刪除子網路

使用 delete-subnet 命令。

將 VPC 連線至其他網路

您可以將虛擬私有雲端 (VPC) 連接到其他網路，例如其他 VPC、網際網路或內部部署網路。



您可以將虛擬私有雲端 (VPC) 連接到其他網路，例如其他 VPC、網際網路或內部部署網路。

該圖示範了其中一些連線選項。VPC A 透過網際網路閘道連接到網際網路，私有子網路中的 EC2 執行個體可以使用公有子網路中一個 NAT 閘道連接到網際網路。VPC B 也連接至網際網路，但透過直接網際網路閘道，允許公有子網路中的 EC2 執行個體存取網際網路。

此外，VPC A 和 VPC B 透過 VPC 對等互連和傳輸閘道互連。傳輸閘道具有與資料中心的 VPN 連接，而 VPC B 具有與相同資料中心的 Direct Connect 連線。這種互連性可讓組織將其雲端資源與內部部署基礎設施整合，進而建立混合雲端環境。

將 VPC 連接到其他網路，是在 AWS內建置雲端基礎設施的重要層面。它為組織提供彈性並控制其聯網組態，讓他們能夠設計符合其業務需求和安全性需求的 VPC 架構。這些連線選項有助於分散式 IT 環境各種元件之間的有效資料流程，無論是在雲端還是內部部署。

AWS 提供各種工具和功能來啟用這些 VPC 連線，包括網際網路閘道、NAT 閘道、VPC 對等互連、傳輸閘道和 Direct Connect。透過使用這些功能，組織可以建立安全且整合的雲端環境，與其現有的 IT 基礎設施無縫整合。

您可以將 Virtual Private Cloud (VPC) 連線至其他網路。例如，其他 VPC、網際網路或內部部署網路。

如需詳細資訊，請參閱 Amazon Virtual Private Cloud 連線選項。

目錄

- 使用網際網路閘道啟用 VPC 的網際網路存取
- 使用輸出限定 (egress-only) 網際網路閘道來啟用傳出 IPv6 流量
- 使用 NAT 裝置連線至網際網路或其他網路
- 將彈性 IP 地址與 VPC 中的資源建立關聯
- 使用傳輸閘道將您的 VPC 連線至其他 VPC 和網路
- 使用 AWS Virtual Private Network 將 VPC 連線至遠端網路
- 使用 VPC 對等互連來連線 VPC

使用網際網路閘道啟用 VPC 的網際網路存取

網際網路閘道是一種水平擴展、備援且高可用性的 VPC 元件，允許 VPC 與網際網路之間的通訊。它支援 IPv4 和 IPv6 流量。它不會對您的網路流量造成可用性風險或頻寬限制。

如果資源具有公有 IPv4 地址或 IPv6 地址，則網際網路閘道可讓公有子網中的資源 (如 EC2 執行個體) 連線至網際網路。同樣地，網際網路上的資源可以使用公有 IPv4 地址或 IPv6 地址來初始化子網中資源的連線。例如，網際網路閘道可讓您 AWS 使用本機電腦連線到 中的 EC2 執行個體。

網際網路閘道會在您的 VPC 路由表中為可由網際網路路由的流量提供目標。針對使用 IPv4 的通訊，網際網路閘道也會執行網路位址轉譯 (NAT)。如需詳細資訊，請參閱 IP 地址和 NAT。

定價

網際網路閘道不收費，但使用網際網路閘道的 EC2 執行個體需支付資料傳輸費用。如需詳細資訊，請參閱 Amazon EC2 隨需定價。

目錄

- 網際網路閘道基礎知識
- 將網際網路存取新增至子網路
- 刪除網際網路閘道

網際網路閘道基礎知識

若要使用網際網路閘道，必須將其連接至 VPC 並設定路由。

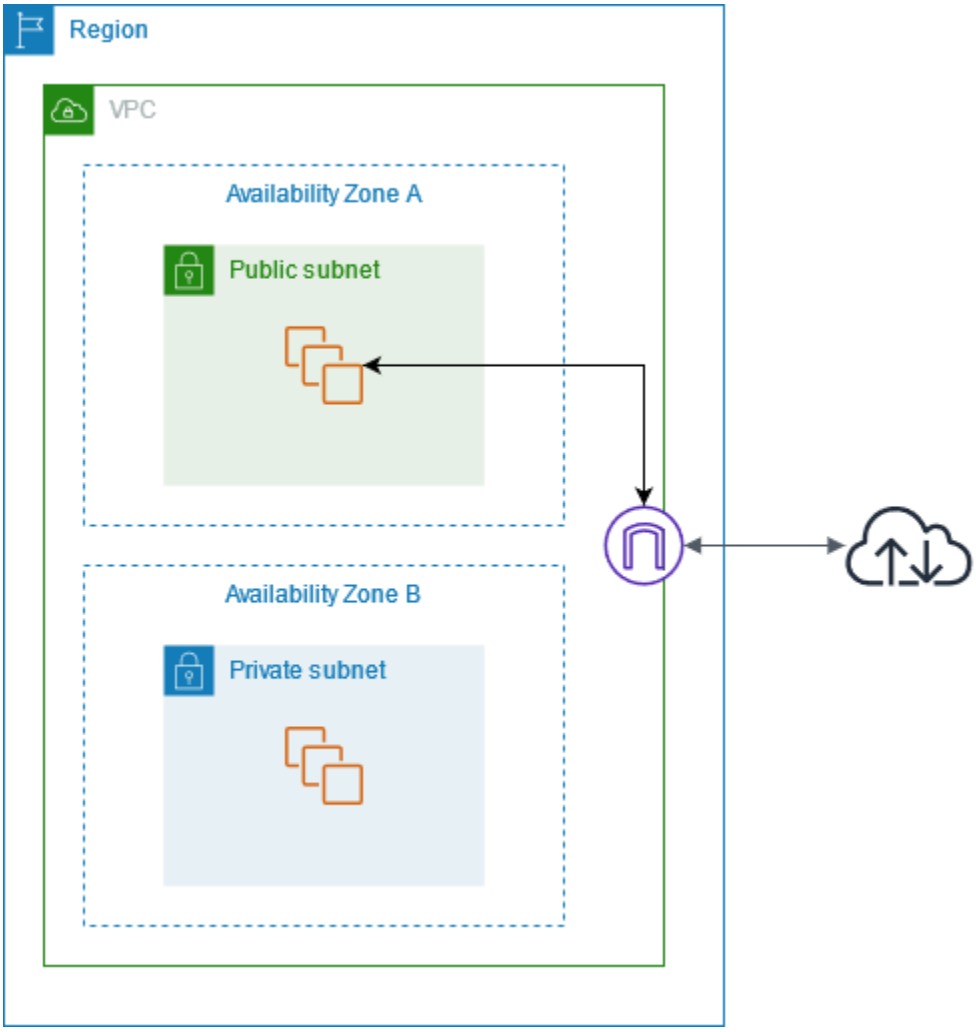
路由組態

如果子網與路由至網際網路閘道的路由表建立關聯，即稱為公有子網。如果子網與未路由至網際網路閘道的路由表建立關聯，則稱為私有子網。

在公有子網路由表中，您可為網際網路閘道指定路由至路由表無法明確辨識的所有目的地 (IPv4 為 0.0.0.0/0，IPv6 為 ::/0)。或者，您可以將路由範圍限制為較窄範圍的 IP 地址；例如，公司外部公有端點的公有 IPv4 地址 AWS，或 VPC 外部其他 Amazon EC2 執行個體的彈性 IP 地址。

網際網路閘道圖表

在下方圖表中，可用區域 A 中的子網路是公有子網路，因為其路由表包含一條路由，可將所有前往網際網路的 IPv4 流量傳送至網際網路閘道。公有子網中的執行個體必須具有公有 IP 地址或彈性 IP 地址，才能透過網際網路閘道與網際網路通訊。相較之下，可用區域 B 中的子網為私有子網，因其路由表沒有通往網際網路閘道的路由。由於沒有通往網際網路閘道的路由，即使具有公有 IP 位址，私有子網路中的執行個體也無法與網際網路通訊。



IP 地址和 NAT

若要針對 IPv4 啟用透過網際網路的通訊，您的執行個體必須具有公有 IPv4 地址。您可以將 VPC 設定為自動指派公有 IPv4 地址給執行個體，或是指派彈性 IP 地址給執行個體。您的執行個體只能辨識 VPC 和子網內定義的私有 (內部) IP 地址空間。網際網路閘道邏輯上會代您的執行個體提供一對一 NAT，因此流量離開 VPC 子網並前往網際網路時，回覆地址欄位會設定成您執行個體的公有 IPv4 地址或彈性 IP 地址，而非私有 IP 地址。相反地，目標設為您執行個體的公有 IPv4 地址或彈性 IP 地址的流量，會將其目標地址轉譯為執行個體的私有 IPv4 地址，再將流量交付給 VPC。

若要針對 IPv6 啟用透過網際網路的通訊，您的 VPC 和子網必須具有相關聯的 IPv6 CIDR 區塊，而且必須有來自子網範圍的 IPv6 地址指派到您的執行個體。IPv6 地址是全域唯一的，因此預設是公開的。

預設和非預設 VPC 的網際網路存取

下表概述 VPC 是否自動隨附透過 IPv4 或 IPv6 存取網際網路所需的元件。

元件	預設 VPC	非預設 VPC
網際網路閘道	是	否
將 IPv4 流量 (0.0.0.0/0) 路由至網際網路閘道的路由表	是	否
將 IPv6 流量 (::/0) 路由至網際網路閘道的路由表	否	否
自動指派給子網中所啟動之執行個體的公有 IPv4 地址	是 (預設子網)	否 (非預設子網)
自動指派給子網中所啟動之執行個體的 IPv6 地址	否 (預設子網)	否 (非預設子網)

將網際網路存取新增至子網路

下文說明如何透過網際網路閘道，支援從非預設 VPC 中的子網路存取網際網路。您必須建立網際網路閘道，將其連接至 VPC，並為子網路設定路由。

在為子網路設定網際網路存取之後，必須確保子網路中的資源能夠存取網際網路。例如，EC2 執行個體必須具備公有 IPv4 或 IPv6 位址，且執行個體的安全群組必須允許往返網際網路的特定流量。

或者，如要為執行個體提供網際網路存取，但不為其指派公有 IP 位址，可以改用 NAT 裝置。如需詳細資訊，請參閱NAT 裝置。

若要移除網際網路存取，您可以將網際網路閘道與您的 VPC 分開，然後將其刪除。如需詳細資訊，請參閱the section called “刪除網際網路閘道”。

任務

- 步驟 1：建立網際網路閘道
- 步驟 2：將網際網路閘道連接至 VPC
- 步驟 3：在子網路路由表中新增路由

步驟 1：建立網際網路閘道

使用下列程序建立網際網路閘道。

透過主控台建立網際網路閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Internet gateways (網際網路閘道)。
3. 選擇建立網際網路閘道。
4. (可選) 輸入網際網路閘道的名稱。
5. (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。
6. 選擇建立網際網路閘道。
7. (可選) 若要立即將網際網路閘道連接至 VPC，請從畫面頂端的橫幅中選擇 Attach to a VPC (連接至 VPC)，選取可用的 VPC，然後選擇 Attach internet gateway (連接網際網路閘道)。否則，您可以在其他時間將網際網路閘道連接至 VPC。

透過命令列建立網際網路閘道

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

步驟 2：將網際網路閘道連接至 VPC

若要使用網際網路閘道，必須將其連接至 VPC。

透過主控台將網際網路閘道連接至 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Internet gateways (網際網路閘道)。
3. 勾選網際網路閘道的核取方塊。
4. 若要連接它，請選擇動作、連接至 VPC、選取可用的 VPC，然後選擇連線網際網路閘道。
5. 若要將其分離，請選擇動作、從 VPC 分離，然後選擇分離網際網路閘道。出現確認提示時，選擇 Detach internet gateway (分離網際網路閘道)。

透過命令列將網際網路閘道連接至 VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

步驟 3：在子網路路由表中新增路由

子網路的路由表必須具有路由，能將網際網路的流量傳送至網際網路閘道。

透過主控台設定子網路路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選取子網路的路由表。依預設，子網路會使用 VPC 的主路由表。或者，您可以建立路由表，然後將子網路與新路由表建立關聯。
4. 在路由標籤上，選擇編輯路由，然後選擇新增路由。
5. 在目的地欄位中輸入 0.0.0.0/0，然後在目標欄位中選取網際網路閘道。
6. 選擇儲存變更。

透過命令列設定子網路路由表

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)

刪除網際網路閘道

若某個 VPC 不再需要網際網路存取，您可以從該 VPC 分離網際網路閘道，然後將其刪除。只要網際網路閘道仍然連接至 VPC，您就無法刪除網際網路閘道。如果 VPC 的資源具有相關聯的公有 IP 地址或彈性 IP 地址，則您無法分離網際網路閘道。

透過主控台從 VPC 分離網際網路閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Internet gateways (網際網路閘道)。
3. 勾選網際網路閘道的核取方塊。
4. 若要連接它，請選擇動作、連接至 VPC、選取可用的 VPC，然後選擇連線網際網路閘道。
5. 若要將其分離，請選擇動作、從 VPC 分離，然後選擇分離網際網路閘道。出現確認提示時，選擇 Detach internet gateway (分離網際網路閘道)。

透過命令列描述網際網路閘道 (包括連接項目)

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

透過命令列從 VPC 分離網際網路閘道

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

透過主控台刪除網際網路閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Internet gateways (網際網路閘道)。
3. 勾選網際網路閘道的核取方塊。
4. 選擇 Actions (動作)、Delete internet gateway (刪除網際網路閘道)。
5. 出現確認提示時，輸入 **`delete`**，然後選擇 Delete internet gateway (刪除網際網路閘道)。

透過命令列刪除網際網路閘道

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

使用輸出限定 (egress-only) 網際網路閘道來啟用傳出 IPv6 流量

輸出限定網際網路閘道是一種水平擴展、備援且高可用性的 VPC 元件，允許透過 IPv6 從 VPC 中的執行個體到網際網路的傳出通訊，並防止網際網路啟動與您執行個體的 IPv6 連線。

輸出限定網際網路閘道僅與 IPv6 流量搭配使用。若要啟用透過 IPv4 的傳出限定網際網路通訊，請改為使用 NAT 閘道。如需詳細資訊，請參閱NAT 閘道。

定價

輸出限定網際網路閘道不收費，但使用網際網路閘道的 EC2 執行個體需支付資料傳輸費用。如需詳細資訊，請參閱 Amazon EC2 隨需定價。

目錄

- 輸出限定網際網路閘道基本概念
- 將僅輸出網際網路存取新增至子網路

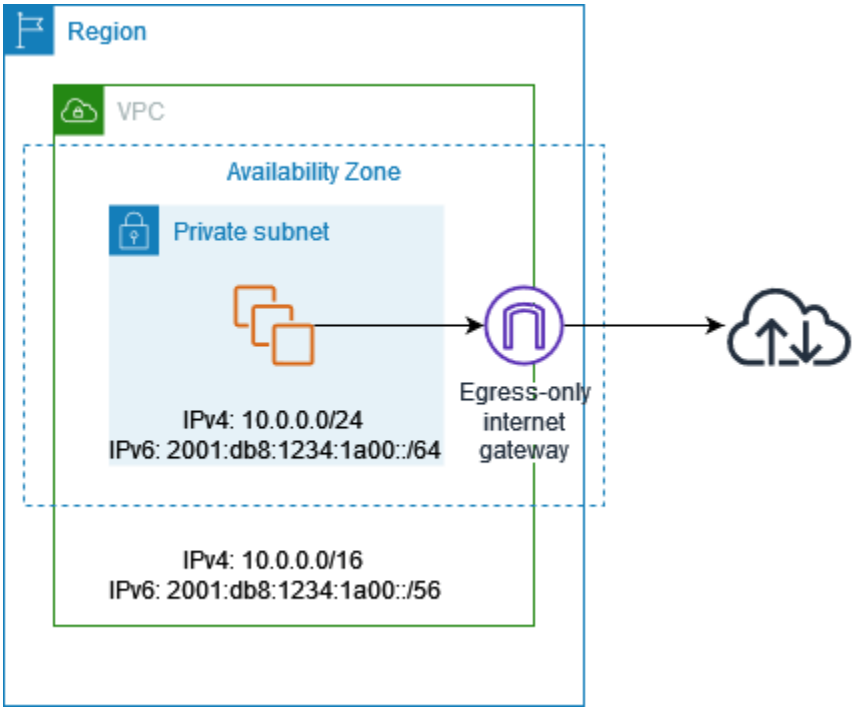
輸出限定網際網路閘道基本概念

IPv6 地址是全域唯一的，因此預設是公開的。如果您想要執行個體可以存取網際網路，但想要防止網際網路上的資源啟動與您執行個體的通訊，則可以使用輸出限定網際網路閘道。若要執行此作業，請在 VPC 中建立輸出限定網際網路閘道，然後將路由新增至路由表，以將所有 IPv6 流量 (`::/0`) 或特定範圍的 IPv6 地址指向輸出限定網際網路閘道。與路由表建立關聯之子網路中的 IPv6 流量會遞送至輸出限定網際網路閘道。

輸出限定網際網路閘道具有狀態：它會將流量從子網路中的執行個體轉送到網際網路或其他 AWS 服務，然後將回應傳回給執行個體。

您無法將安全群組與輸出限定網際網路閘道建立關聯，以控制允許存取或離開輸出限定網際網路閘道的流量。您可以使用網路 ACL，來控制進出輸出限定網際網路閘道路由其流量之子網路的流量。

在下圖中，VPC 同時具有 IPv4 和 IPv6 CIDR 區塊，且子網路同時具有 IPv4 和 IPv6 CIDR 區塊。VPC 具有輸出限定網際網路閘道。



下面是與子網路關聯的路由表範例。存在一個路由，可將所有網際網路繫結 IPv6 流量 (::/0) 傳送至輸出限定網際網路閘道。

目標	目標
10.0.0.0/16	區域
2001:db8:1234:1a00:/64	區域
::/0	*eigw-id*

將僅輸出網際網路存取新增至子網路

下列任務說明如何建立私有子網路的輸出限定網際網路閘道，以及設定子網路的路由。

任務

- 1. 建立輸出限定網際網路閘道
- 2. 建立自訂路由表
- 3. 刪除輸出限定網際網路閘道
- 命令列概觀

1. 建立輸出限定網際網路閘道

您可以使用 Amazon VPC 主控台來建立 VPC 的輸出限定網際網路閘道。

建立輸出限定網際網路閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Egress Only Internet Gateways (輸出限定網際網路閘道)。
3. 選擇 Create Egress Only Internet Gateway (建立輸出限定網際網路閘道)。
4. (選用) 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值欄位中，輸入金鑰值。

   【移除標籤】 選擇標籤索引鍵和值右側的移除。
5. 選取要在其中建立輸出限定網際網路閘道的 VPC。

6. 選擇建立。

2. 建立自訂路由表

若要將目標設為 VPC 外部的流量傳送至輸出限定網際網路閘道，您必須建立自訂路由表，並新增路由以將流量傳送給閘道，然後建立與您子網路的關聯。

建立自訂路由表並新增輸出限定網際網路閘道的路由

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)、Create route table (建立路由表)。
3. 在 Create route table (建立路由表) 對話方塊中，選擇性地命名您的路由表，並選取您的 VPC，然後選擇 Create route table (建立路由表)。
4. 選取您剛建立的自訂路由表。詳細資訊窗格會顯示用於使用其路由、關聯和路由傳播的標籤。
5. 在 Routes (路由) 標籤上，選擇 Edit routes (編輯路由)，並在 Destination (目標) 方塊中指定 `::/0`，然後在 Target (目標) 清單中選取輸出限定網際網路閘道 ID，再選擇 Save changes (儲存變更)。
6. 在 Subnet associations (子網路關聯) 標籤上，選擇 Edit subnet associations (編輯子網路關聯)，然後選取子網路的關聯核取方塊。選擇 Save (儲存)。

或者，您可以將路由新增至與子網路建立關聯的現有路由表。選取現有路由表，並遵循上方的步驟 5 和 6，新增輸出限定網際網路閘道的路由。

如需路由表的詳細資訊，請參閱設定路由表。

3. 刪除輸出限定網際網路閘道

如果您不再需要輸出限定網際網路閘道，可以予以刪除。除非您手動刪除或更新路由表中指向已刪除的輸出限定網際網路閘道的任何路由，否則該路由會保持 `blackhole` 狀態。

刪除輸出限定網際網路閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇輸出限定網際網路閘道，然後選取輸出限定網際網路閘道。
3. 選擇 Delete (刪除)。
4. 在確認對話方塊中，選擇 Delete Egress Only Internet Gateway (刪除輸出限定網際網路閘道)。

命令列概觀

您可以使用命令列執行此頁面所述的任務。

建立輸出限定網際網路閘道

- create-egress-only-internet-gateway (AWS CLI)
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

說明輸出限定網際網路閘道

- describe-egress-only-internet-gateways (AWS CLI)
- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

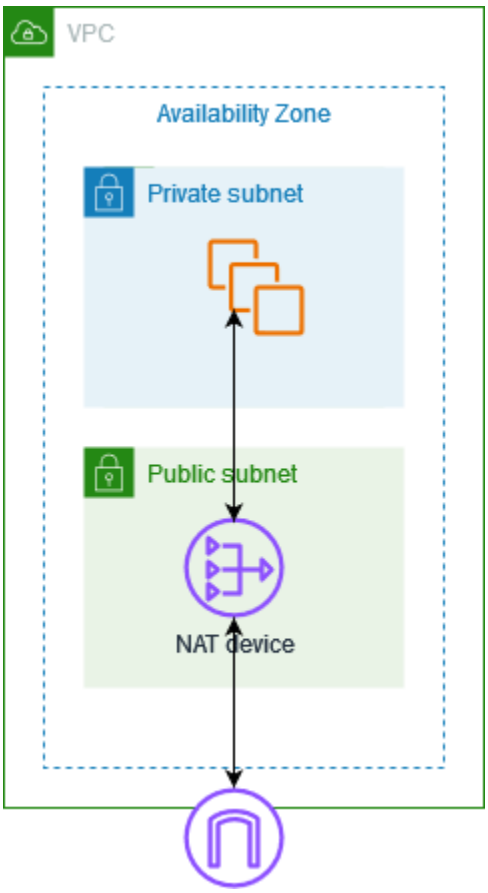
刪除輸出限定網際網路閘道

- delete-egress-only-internet-gateway (AWS CLI)
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

使用 NAT 裝置連線至網際網路或其他網路

您可以使用 NAT 裝置，允許私有子網中的資源連線到網際網路、其他 VPC 或內部部署網路。這些執行個體可以與 VPC 外部的服務進行通訊，但無法接收來路不明的連線請求。

例如，下圖顯示公有子網路中的 NAT 裝置，允許私有子網路中的 EC2 執行個體透過網際網路閘道連線至網際網路。NAT 裝置會以 NAT 裝置的地址取代執行個體的來源 IPv4 地址。傳送回應流量至執行個體時，NAT 裝置會將地址轉譯回原始來源 IPv4 地址。



Important

- 我們在此文件中使用 NAT 以遵循通用 IT 實務，但是 NAT 裝置的實際角色同時包含地址轉換和連接埠地址轉換 (PAT)。
- 您可以使用 提供的受管 NAT 裝置 AWS，稱為 NAT 閘道，也可以在稱為 NAT 執行個體的 EC2 執行個體上建立自己的 NAT 裝置。我們建議您使用 NAT 閘道，因為它們提供更好的可用性和頻寬，而且您的管理負擔較輕。

目錄

- NAT 閘道
- NAT 執行個體
- 比較 NAT 執行個體和 NAT 閘道

NAT 閘道

NAT 閘道是網路地址轉譯 (NAT) 服務。您可以使用 NAT 閘道，使私有子網路中的執行個體可以連線至 VPC 外部的服務，但外部服務無法啟動與這些執行個體的連線。

當您建立 NAT 閘道時，您可以指定下列其中一種連線類型：

- 公有 – (預設) 私有子網路中的執行個體可以透過公有 NAT 閘道連線至網際網路，但無法接收來自網際網路的未經請求的傳入連線。您在公有子網路中建立公有 NAT 閘道時，必須在建立之時為其關聯一個彈性 IP 位址。您可以將流量從 NAT 閘道路由傳送到 VPC 的網際網路閘道。或者，您可以使用公有 NAT 閘道來連線到其他 VPC 或內部部署網路。在此情況下，您可以透過傳輸閘道或虛擬私有閘道路由傳送來自 NAT 閘道的流量。
- 私有 – 私有子網路中的執行個體可以透過私有 NAT 閘道連線至其他 VPC 或內部部署網路，但執行個體無法接收來自其他 VPC 或內部部署網路的未經請求的傳入連線。您可以透過傳輸閘道或虛擬私有閘道路由傳送來自 NAT 閘道的流量。您無法將彈性 IP 位址與私有 NAT 閘道建立關聯。您可以將網際網路閘道連接到具有私有 NAT 閘道的 VPC，但是如果您將流量從私有 NAT 閘道路由傳送到網際網路閘道，網際網路閘道會捨棄流量。

NAT 閘道適用於 IPv4 或 IPv6 流量 (使用 DNS64 和 NAT64)。若要啟用透過 IPv6 的僅限傳出網際網路通訊，請使用僅限輸出網際網路閘道。

私有和公有 NAT 閘道都會將執行個體的來源私有 IPv4 地址映射至 NAT 閘道的私有 IPv4 地址。對於公有 NAT 閘道，網際網路閘道接著會將公有 NAT 閘道的私有 IPv4 地址映射至與 NAT 閘道相關聯的彈性 IP 地址。

傳送回應流量至執行個體時，無論是公有或私有 NAT 閘道，NAT 閘道都會將地址轉譯回原始來源 IP 地址。

考量事項

- 連線必須一律從包含 NAT 閘道的 VPC 內部啟動。
- 您可以使用公有或私有 NAT 閘道，將流量路由至傳輸閘道和虛擬私有閘道。
- 如果您使用私有 NAT 閘道連線至傳輸閘道或虛擬私有閘道，則前往目的地的流量會來自私有 NAT 閘道的私有 IP 地址。
- 如果您使用公有 NAT 閘道連線至傳輸閘道或虛擬私有閘道，則前往目的地的流量會來自公有 NAT 閘道的私有 IP 位址。公有 NAT 閘道僅會在與同一 VPC 中的網際網路閘道搭配使用時，才會將其彈性 IP 位址作為來源 IP 位址。

目錄

- NAT 閘道基本概念
- 使用 NAT 閘道
- 用於自動多可用區域擴展的區域 NAT 閘道
- API 閘道使用案例
- DNS64 和 NAT64
- 檢查來自 NAT 閘道的流量
- 使用 Amazon CloudWatch 監控 NAT 閘道
- 疑難排解 NAT 閘道
- NAT 閘道的定價

NAT 閘道基本概念

每個 NAT 閘道都是在特定的可用區域內建立，並且使用該區域中的備援實作。您能夠在每個可用區域中建立的 NAT 閘道數量具有配額。如需詳細資訊，請參閱閘道。

如果您在多個可用區域中有資源，而且它們共用一個 NAT 閘道，而且如果 NAT 閘道的可用區域關閉，則其他可用區域中的資源會失去網際網路存取。若要提高彈性，請在每個可用區域中建立 NAT 閘道，然後設定您的路由，確保資源使用相同可用區域內的 NAT 閘道。

下列特性和規則適用於 NAT 閘道：

- NAT 閘道支援以下通訊協定：TCP、UDP 和 ICMP。
- IPv4 或 IPv6 流量支援 NAT 閘道。對於 IPv6 流量，NAT 閘道會執行 NAT64。搭配 DNS64 (可在 Route 53 解析器上使用) 一起使用此功能，Amazon VPC 中子網中的 IPv6 工作負載就可以與 IPv4 資源通訊。這些 IPv4 服務可能存在於相同的 VPC (在個別的子網中) 或不同的 VPC、您的內部部署環境或網際網路上。
- NAT 閘道支援 5 Gbps 的頻寬，並可自動擴展至 100 Gbps。若您需要更多頻寬，您可以將您的資源分割到多個子網，並在每個子網中建立 NAT 閘道。
- NAT 閘道每秒可以處理一百萬個封包，並自動擴展至每秒最多 1，000 萬個封包。超出此限制，NAT 閘道便會捨棄封包。若要防止封包遺失，請將您的資源分割為多個子網，並為每個子網建立單獨的 NAT 閘道。
- 每個 IPv4 地址可支援最多 55,000 個連至每個唯一目標的同時連線。唯一目的地由目的地 IP 地址、目的地連接埠以及通訊協定 (TCP/UDP/ICMP) 的唯一組合來識別。您可以將最多 8 個 IPv4 位址與

NAT 閘道關聯 (1 個主要 IPv4 位址與 7 個次要 IPv4 位址) 來提高此限制。依預設，您只能將 2 個彈性 IP 地址與公有 NAT 閘道相關聯。您可以透過請求調整配額來提高此限制。如需詳細資訊，請參閱彈性 IP 位址。

- 建立 NAT 閘道時，您需選取要指派給 NAT 閘道的主要私有 IPv4 位址。否則，我們會代為從子網路的 IPv4 位址範圍中選取一個。您無法變更或移除主要私有 IPv4 位址。您可以視需要新增次要私有 IPv4 位址。
- 您無法建立安全群組與 NAT 閘道的關聯。您可以將安全群組與您的執行個體建立關聯，來控制傳入和傳出流量。
- 我們會為您的 NAT 閘道建立申請者受管網路介面。您可以透過 Amazon EC2 主控台檢視此網路介面。在描述中搜尋 NAT 閘道的 ID。您可以將標籤新增至網路介面，但無法修改此網路介面的其他屬性。
- 您可以使用網路 ACL 控制流入及流出您 NAT 閘道子網的流量。NAT 閘道使用連接埠 1024–65535。如需詳細資訊，請參閱網路 ACL。
- 您無法透過 VPC 對等互連將流量路由至 NAT 閘道。不過，從 NAT 閘道透過 VPC 對等互連傳送至對等 VPC 目的地的流量，支援「回傳至傳送著」行為，即使目的地 VPC 未設定回傳路由，返回流量仍會自動路由回原始 NAT 閘道。此行為僅適用於 NAT 閘道，不適用於標準 EC2 執行個體。若要防止這種情況，可使用 NACL 來封鎖回傳流量。

  不支援：

  ```
  Client # Peering # NAT # Internet
  ```

  支援：

  ```
  Client # NAT # Peering # Destination
  ```

- 您無法透過虛擬私有閘道，將來自 Site-to-Site VPN 或 Direct Connect 的流量路由至 NAT 閘道。如果您使用傳輸閘道而非虛擬私有閘道，則可以從 Site-to-Site VPN 或 Direct Connect 路由流量至 NAT 閘道。
- NAT 閘道支援最大傳輸單位 (MTU) 為 8500 的流量，但請務必注意下列事項：
  - 網路連線的 MTU 係允許通過該連線的最大封包大小 (以位元組為單位)。連線的 MTU 越大，單一封包能傳遞的資料也越多。
  - 抵達 NAT 閘道且大於 8500 位元組的封包會被丟棄 (或在適用時進行分段處理)。
  - 為了防止使用公有 NAT 閘道透過網際網路與資源通訊時潛在的封包遺失，EC2 執行個體的 MTU 設定不應超過 1500 個位元組。如需在執行個體上檢查和設定 MTU 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 EC2 執行個體的網路 MTU。

- NAT 閘道支援透過 FRAG_NEEDED ICMPv4 封包和 Packet Too Big (PTB) ICMPv6 封包的路徑 MTU 探索 (PMTUD)。
- NAT 閘道會強制執行所有封包的最大區段大小 (MSS) 限制。如需詳細資訊，請參閱 RFC879。

使用 NAT 閘道

您可以使用 Amazon VPC 主控台來建立和管理您的 NAT 閘道。

任務

- 控制 NAT 閘道的使用
- 建立 NAT 閘道
- 編輯次要 IP 地址關聯
- 為 NAT 閘道新增標籤
- 刪除 NAT 閘道
- 命令列概觀

控制 NAT 閘道的使用

根據預設， 使用者沒有使用 NAT 閘道的許可。您可以建立 IAM 角色，確保其連接的政策會將建立、描述和刪除 NAT 閘道的許可授予使用者。如需詳細資訊，請參閱Amazon VPC 的身分和存取管理。

建立 NAT 閘道

使用下列程序建立 NAT 閘道。

相關配額

- 如果您已用盡配置給帳戶的彈性 IP 位址，將無法建立公有 NAT 閘道。如需詳細資訊，請參閱彈性 IP 位址。
- 您可以將最多 8 個私有 IPv4 位址指派給私有 NAT 閘道。此限制不可調整。
- 依預設，您只能將 2 個彈性 IP 地址與公有 NAT 閘道相關聯。您可以透過請求調整配額來提高此限制。如需詳細資訊，請參閱彈性 IP 位址。

建立 NAT 閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇 NAT 閘道。
3. 選擇建立 NAT 閘道。
4. (選擇性) 指定 NAT 閘道的名稱。這會建立一個標籤，其中金鑰為 **Name**，而值是您指定的名稱。
5. 選取要在其中建立 NAT 閘道的子網。
6. 針對連線類型，保留預設公有選擇以建立公有 NAT 閘道，或選擇私有以建立私有 NAT 閘道。如需有關公有和私有 NAT 閘道之間差異的詳細資訊，請參閱 NAT 閘道。
7. 如果您選擇公有，請執行下列動作；否則，請跳至步驟 8：

   1. 選擇彈性 IP 配置 ID，將彈性 IP 位址指派給 NAT 閘道；也可以選擇配置彈性 IP，為公有 NAT 閘道自動配置彈性 IP。依預設，您只能將 2 個彈性 IP 地址與公有 NAT 閘道相關聯。您可以透過請求調整配額來提高此限制。如需詳細資訊，請參閱彈性 IP 位址。

      > **Important**
      >
      > 將彈性 IP 位址指派給公有 NAT 閘道時，EIP 的網路邊界群組必須與您要啟動公有 NAT 閘道之可用區域 (AZ) 的網路邊界群組相符。如果不相同，NAT 閘道將無法啟動。您可以檢視子網路的詳細資料，查看子網路 AZ 的網路邊界群組。同樣地，您可以檢視 EIP 地址的詳細資料，檢視 EIP 的網路邊界群組。如需詳細資訊，請參閱1. 配置彈性 IP 位址。

   2. (選用) 選擇其他設定，並在私有 IP 地址 - 選用下，輸入 NAT 閘道的私有 IPv4 地址。如果您未輸入地址， AWS 會從 NAT 閘道所在的子網路隨機將私有 IPv4 地址指派給 NAT 閘道。
   3. 跳至步驟 11。
8. 如果您選擇私有，請在其他設定、私有 IPv4 地址指派方法，選擇下列其中一項：

   - 自動指派： AWS 選擇 NAT 閘道的主要私有 IPv4 地址。對於自動指派的私有 IPv4 地址數量，您可以選擇指定 NAT 閘道的次要私有 IPv4 地址數量。 會從 NAT 閘道的子網路隨機 AWS 選擇這些 IP 地址。
   - 自訂：請在主要私有 IPv4 地址，選擇 NAT 閘道的主要私有 IPv4 地址。對於次要私有 IPv4 地址，您可以選擇性地為 NAT 閘道指定最多 7 個次要私有 IPv4 地址。
9. 如果在步驟 8 中選擇自訂，則請略過此步驟。如果您選擇自動指派，請在自動指派的私有 IP 地址數量下，選擇您要 AWS 指派給此私有 NAT 閘道的次要 IPv4 地址數量。您最多可以選擇 7 個 IPv4 地址。

> **Note**
>
> 次要 IPv4 位址是選用項目，當使用 NAT 閘道的工作負載與單一目的地 (相同的目的地 IP、目的地連接埠和通訊協定) 的並行連線超過 55,000 條時，應進行指派或配置。次要 IPv4 地址會增加可用連接埠的數目，因此會增加工作負載可使用 NAT 閘道建立之並行連線數目的限制。

10. 如果在步驟 9 中選擇自動指派，則請略過此步驟。如果選擇自訂，請執行下列操作：
    1. 在主要私有 IPv4 地址中，輸入私有 IPv4 地址。
    2. 在次要私有 IPv4 地址中，輸入最多 7 個次要私有 IPv4 地址。
11. (選用) 若要新增標籤至 NAT 閘道，請選擇 Add new tag (新增標籤)，然後輸入鍵名稱和值。您最多可以新增 50 個標籤。
12. 選擇建立 NAT 閘道。
13. NAT 閘道的初始狀態為 `Pending`。狀態變更為後 `Available`，NAT 閘道即可供您使用。請務必視需要更新您的路由表。如需範例，請參閱 the section called “使用案例”。

若 NAT 閘道的狀態變更為 `Failed`，表示在建立過程中發生錯誤。如需詳細資訊，請參閱NAT 閘道建立失敗。

編輯次要 IP 地址關聯

每個 IPv4 地址可支援最多 55,000 個連至每個唯一目標的同時連線。唯一目的地由目的地 IP 地址、目的地連接埠以及通訊協定 (TCP/UDP/ICMP) 的唯一組合來識別。您可以將最多 8 個 IPv4 位址與 NAT 閘道關聯 (1 個主要 IPv4 位址與 7 個次要 IPv4 位址) 來提高此限制。依預設，您只能將 2 個彈性 IP 地址與公有 NAT 閘道相關聯。您可以透過請求調整配額來提高此限制。如需詳細資訊，請參閱彈性 IP 位址。

您可以使用 NAT 閘道 CloudWatch 指標 ErrorPortAllocation 和 PacketsDropCount 來判斷您的 NAT 閘道是否產生連接埠配置錯誤或捨棄封包。若要解決此問題，請將次要 IPv4 地址新增至 NAT 閘道。

考量事項

- 您可以在建立私有 NAT 閘道時或使用本節中的程序建立 NAT 閘道後，新增次要私有 IPv4 地址。只有在使用本節中的程序建立 NAT 閘道之後，您才可以將彈性 IP 位址新增至公有 NAT 閘道。

- NAT 閘道最多擁有 8 個與其關聯的 IPv4 地址 (1 個主要 IPv4 地址和 7 個次要 IPv4 地址)。您可以將最多 8 個私有 IPv4 位址指派給私有 NAT 閘道。依預設，您只能將 2 個彈性 IP 地址與公有 NAT 閘道相關聯。您可以透過請求調整配額來提高此限制。如需詳細資訊，請參閱彈性 IP 位址。

編輯次要 IPv4 地址關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 NAT 閘道。
3. 選取您要編輯其次要 IPv4 地址關聯的 NAT 閘道。
4. 選擇動作，然後選擇編輯次要 IP 地址關聯。
5. 如果您要編輯私有 NAT 閘道的次要 IPv4 地址關聯，則請在動作下選擇指派新 IPv4 地址或取消指派現有 IPv4 地址。如果您要編輯公有 NAT 閘道的次要 IPv4 地址關聯，請在動作下選擇關聯新 IPv4 地址或取消關聯現有 IPv4 地址。
6. 執行以下任意一項：

   - 如果您選擇指派或關聯新 IPv4 地址，則請執行下列操作：

     1. 此步驟為必要。您必須選取私有 IPv4 地址。選擇私有 IPv4 地址指派方法：
        - 自動指派： AWS 自動選擇主要私有 IPv4 地址，如果您 AWS 想要指派最多 7 個次要私有 IPv4 地址來指派給 NAT 閘道，請選擇此選項。 AWS 會自動從您的 NAT 閘道所在的子網路隨機選擇並指派這些地址。
        - 自訂：選擇要指派給 NAT 閘道的主要私有 IPv4 地址和最多 7 個次要私有 IPv4 地址。
     2. 在彈性 IP 配置 ID 下，選擇要新增為次要 IPv4 位址的彈性 IP 位址。此步驟為必要。您必須同時選取一個彈性 IP 位址與一個私有 IPv4 位址。如果將私有 IP 位址指派方法選為自訂，則您也必須為新增的每個彈性 IP 位址輸入私有 IPv4 位址。

     > **Important**
     >
     > 將次要 EIP 指派給公有 NAT 閘道時，EIP 的網路邊界群組必須符合公有 NAT 閘道所在之可用區域 (AZ) 的網路邊界群組。如果不相同，EIP 將無法指派。您可以檢視子網路的詳細資料，查看子網路 AZ 的網路邊界群組。同樣地，您可以檢視 EIP 地址的詳細資料，檢視 EIP 的網路邊界群組。如需詳細資訊，請參閱1. 配置彈性 IP 位址。

     NAT 閘道最多可以擁有 8 個與其相關聯的 IP 地址。如果這是公有 NAT 閘道，則每個區域的彈性 IP 位址都有預設配額限制。如需詳細資訊，請參閱彈性 IP 位址。

   - 如果您選擇取消指派或取消關聯新 IPv4 地址，請執行下列操作：

1. 在要取消指派的現有次要 IP 地址下，選取您要取消指派的次要 IP 地址。
2. (選用) 在連接耗盡持續時間下，輸入如果連接仍在進行中，則強制釋出 IP 地址之前等待的時間上限 (以秒為單位)。如果不輸入值，則預設值為 350 秒。

7. 選擇儲存變更。

若 NAT 閘道的狀態變更為 `Failed`，表示在建立過程中發生錯誤。如需詳細資訊，請參閱 NAT 閘道建立失敗。

為 NAT 閘道新增標籤

您可為您的 NAT 閘道新增標籤，以利您根據組織需求識別或分類。如需使用標籤的資訊，請參閱《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源。

NAT 閘道支援成本分配標籤。因此，您也可以使用標籤來整理 AWS 帳單，並反映您自己的成本結構。如需詳細資訊，請參閱《AWS Billing 使用者指南》中的使用成本分配標籤。如需使用標籤設定成本分配報告的詳細資訊，請參閱關於 AWS 帳戶帳單中的每月成本分配報告。

標記 NAT 閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 NAT 閘道。
3. 選取要標記的 NAT 閘道，然後選擇動作。然後選擇管理標籤。
4. 選擇新增新標籤，並定義標籤的索引鍵和值。您最多可以新增 50 個標籤。
5. 選擇儲存。

刪除 NAT 閘道

若您不再需要 NAT 閘道，您可以予以刪除。在您刪除 NAT 閘道之後，其項目仍會在 Amazon VPC 主控台中顯示約一小時)，之後便會自動移除。您無法自行移除此項目。

刪除 NAT 閘道會取消關聯其彈性 IP 地址，但不會從您的帳戶釋出地址。若您刪除 NAT 閘道，NAT 閘道路由會繼續處於 `blackhole` 狀態，直到您刪除或更新路由。

刪除 NAT 閘道

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 NAT 閘道。
3. 選取 NAT 閘道選項按鈕，然後選擇 Actions (動作)、Delete NAT Gateway (刪除 NAT 閘道)。

4. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。
5. 如果您不再需要與公有 NAT 閘道相關聯的彈性 IP 地址，建議您將其釋出。如需詳細資訊，請參閱5. 釋出彈性 IP 位址。

命令列概觀

您可以使用命令列執行此頁面所述的任務。

將私有 IPv4 地址指派給私有 NAT 閘道

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

將彈性 IP 位址 和私有 IPv4 位址與公有 NAT 閘道建立關聯

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

建立 NAT 閘道

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

刪除 NAT 閘道

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

描述 NAT 閘道

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

取消次要彈性 IP 位址 與公有 NAT 閘道的關聯

- disassociate-nat-gateway-address (AWS CLI)

- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

為 NAT 閘道新增標籤

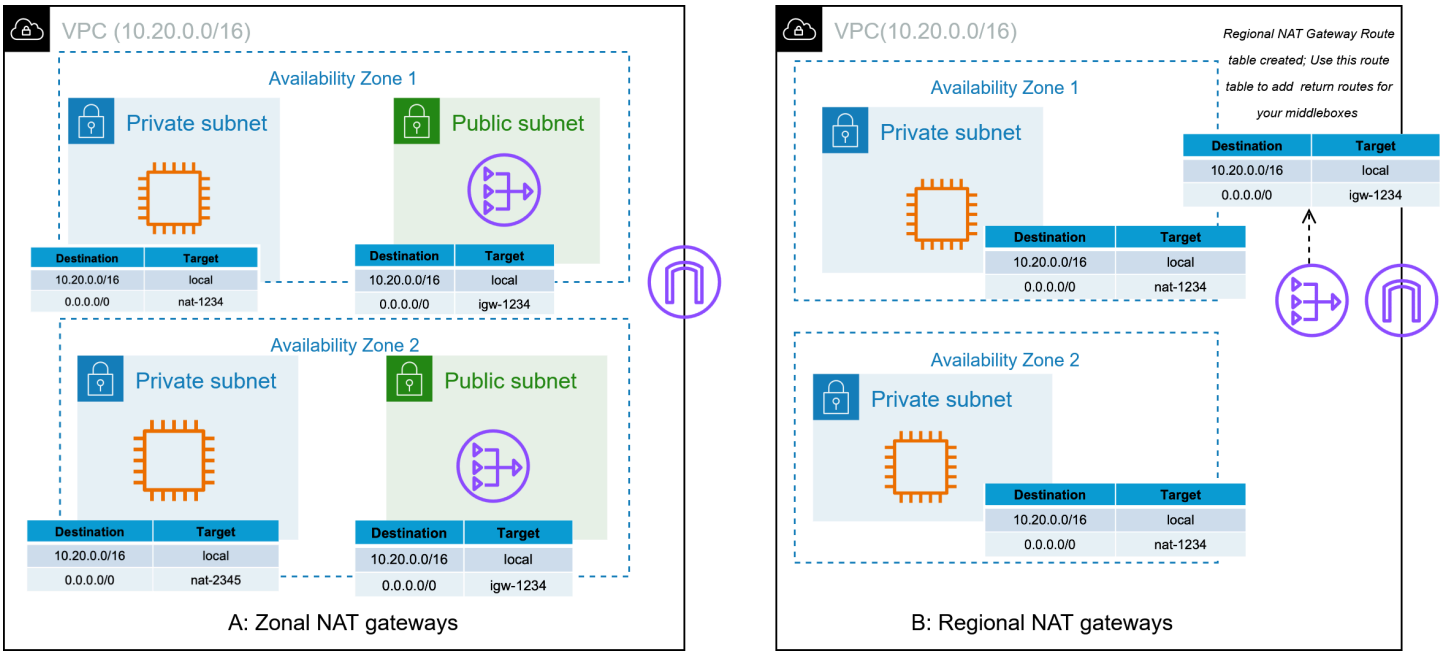
- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

從私有 NAT 閘道中取消指派次要 IPv4 地址

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

用於自動多可用區域擴展的區域 NAT 閘道

當您想要簡化網路架構、改善安全狀態，以及預設設定高可用性時，請使用區域 NAT 閘道。區域 NAT 閘道會根據您的工作負載存在情況，自動跨可用區域擴展。與在單一可用區域中運作的標準 NAT 閘道（稱為區域 NAT 閘道）不同，區域 NAT 閘道會跟隨您的工作負載以提供自動高可用性。



左側圖表 A 代表使用區域 NAT Gateway 的目前設定。您首先為每個可用區域建立區域 NAT 閘道，並將您的 NATs 託管在公有子網路中。然後，您可以為每個可用區域設定從私有子網路到該可用區域中 NAT 的個別路由。您每次將工作負載擴展到新的可用區域時都會重複此步驟，以獲得高可用性。此外，您需要在每個可用區域的 NAT 子網路路由表中新增網際網路閘道的路由。

另一方面，使用區域 NAT Gateway，您不需要建立公有子網路來託管它。您也不必在每次工作負載擴展到新的可用區域時建立和刪除 NAT 閘道並編輯路由表。相反地，您只需使用區域模式建立 NAT Gateway，選擇您的 VPC，並根據工作負載的存在，自動在所有AZs之間擴展和簽訂合約，以提供高可用性。如圖表 B 所示，您可以將所有 AZs 中私有子網路中的資源流量路由到此單一區域 NAT Gateway ID，或使用 AZ 中子網路之間的相同路由表來執行網路位址轉譯。建立區域 NAT Gateway 後， AWS 會自動為其建立路由表，並隨附預先設定的網際網路閘道路由。您可以使用此路由表，將傳回路由新增至中間設備。

優勢

區域 NAT 閘道提供下列優點：

- 簡化設定 – 在具有網路介面的所有可用區域中使用單一 NAT ID，因此您可以對不同可用區域的子網路使用相同的路由項目。
- 增強安全性 – 不需要公有子網路。區域 NAT Gateway 是具有自己的路由表的獨立資源，您不需要 VPC 中的公有子網路來託管區域 NAT Gateway，這樣可以降低在具有公有連線的子網路中設定私有資源的機率。
- 自動高可用性 – 自動擴展工作負載足跡並與其簽訂合約，以維持區域親和性，依預設可提供高可用性。
- 更高的連接埠和 IP 限制 – 您的區域 NAT 閘道每個可用區域最多支援 32 個 IP 地址 （區域 NAT 閘道則為 8)。每個 IP 地址都會將與熱門目的地 （透過目的地 IP、目的地連接埠和通訊協定的唯一組合來識別） 的並行連線限制增加 55，000。

何時使用區域 NAT 閘道

考慮在所有使用案例中使用區域 NAT 閘道，但需要私有連線的情況除外。區域 NAT 閘道不提供私有連線，建議您在區域可用性模式中將 NAT 閘道用於私有 NAT 使用案例。

區域 NAT 閘道的運作方式

當您在新的可用區域中啟動資源時，區域 NAT 閘道會偵測該可用區域中是否存在網路介面 (ENI)，並自動擴展至該區域。同樣地，NAT Gateway 會從沒有作用中工作負載的可用區域簽訂合約。

資源執行個體化後，您的區域 NAT Gateway 最多可能需要 60 分鐘才能擴展到新的可用區域。在此擴展完成之前，來自此資源的相關流量將由區域 NAT Gateway 在其中一個現有可用區域中跨區域處理。

區域 NAT 閘道支援兩種模式：

- 自動模式 – 在此模式中， AWS 會自動管理 IP 地址和可用區域擴展 （ 建議 ）。如果您想要在此模式下使用自己的 IP 地址，並使用 Amazon VPC IPAM，請參閱《Amazon VPC IPAM 使用者指南》中的使用 IPAM 政策定義公有 IPv4 配置策略。
- 手動模式 – 在此模式中，您可以手動管理每個可用區域的 IP 地址和控制網路地址轉譯。在手動模式下，您有責任跨可用區域擴展和收縮 NAT 閘道。

> **Important**
>
> 區域 NAT 閘道支援 AWS Transit Gateway 做為區域 NAT 閘道路由表中的有效路由。區域 NAT 閘道不支援私有 NAT。如果您需要私有 NAT，請改用區域 NAT 閘道。受限的可用區域不支援區域 NAT 閘道。

定價

如需定價資訊，請參閱 Amazon VPC 定價。

建立區域 NAT 閘道

使用主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 NAT 閘道。
3. 選擇建立 NAT 閘道。
4. 針對可用性模式，選擇區域性。選擇區域可用性時，您不需要指定任何子網路
5. 選擇 VPC。
6. 完成剩餘的組態，然後選擇建立 NAT 閘道。

使用 AWS CLI

建立區域 NAT 閘道

```
aws ec2 create-nat-gateway --vpc-id vpc-12345678 --availability-mode regional
```

檢視 NAT 閘道詳細資訊

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-12345678
```

新增 IP 地址（手動模式）

```
aws ec2 associate-nat-gateway-address --nat-gateway-id nat-12345678 --availability-zone
 us-east-1b --allocation-ids eipalloc-12345678
```

移除 IP 地址

```
aws ec2 disassociate-nat-gateway-address --nat-gateway-id nat-12345678 --association-
ids eipassoc-12345678
```

刪除區域 NAT 閘道

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-12345678
```

從區域轉換為區域 NAT 閘道

> **Important**
>
> 這將重設您現有的連線。我們建議您在維護時段中完成這些步驟。

您可以使用下列兩種方法之一，將現有的區域 NAT 閘道轉換為區域 NAT 閘道：

如果您可以使用具有新 IP 地址的區域 NAT 閘道：

1. 建立新的區域 NAT 閘道
2. 更新路由表以指向區域 NAT 閘道
3. 刪除舊區域 NAT 閘道

此方法使用新的 IP 地址，並在路由更新時重設現有的連線。

如果您想要在區域 NAT 閘道中重複使用現有的 IP 地址：

1. 刪除現有的區域 NAT 閘道以釋出其 IP 地址
2. 使用發行的 IP 地址建立區域 NAT 閘道
3. 更新路由表以指向區域 NAT 閘道

此方法會保留 IP 地址，但需要維護時段，因為流量會在轉換期間中斷。

API 閘道使用案例

以下是公有和私有 NAT 閘道的範例使用案例。

案例

- 從私有子網存取網際網路
- 使用允許清單中的 IP 地址存取您的網路
- 實現重疊網路之間的通訊

從私有子網存取網際網路

您可以使用公有 NAT 閘道讓私有子網中的執行個體能將傳出流量傳送到網際網路，同時阻止網際網路建立與執行個體的連線。

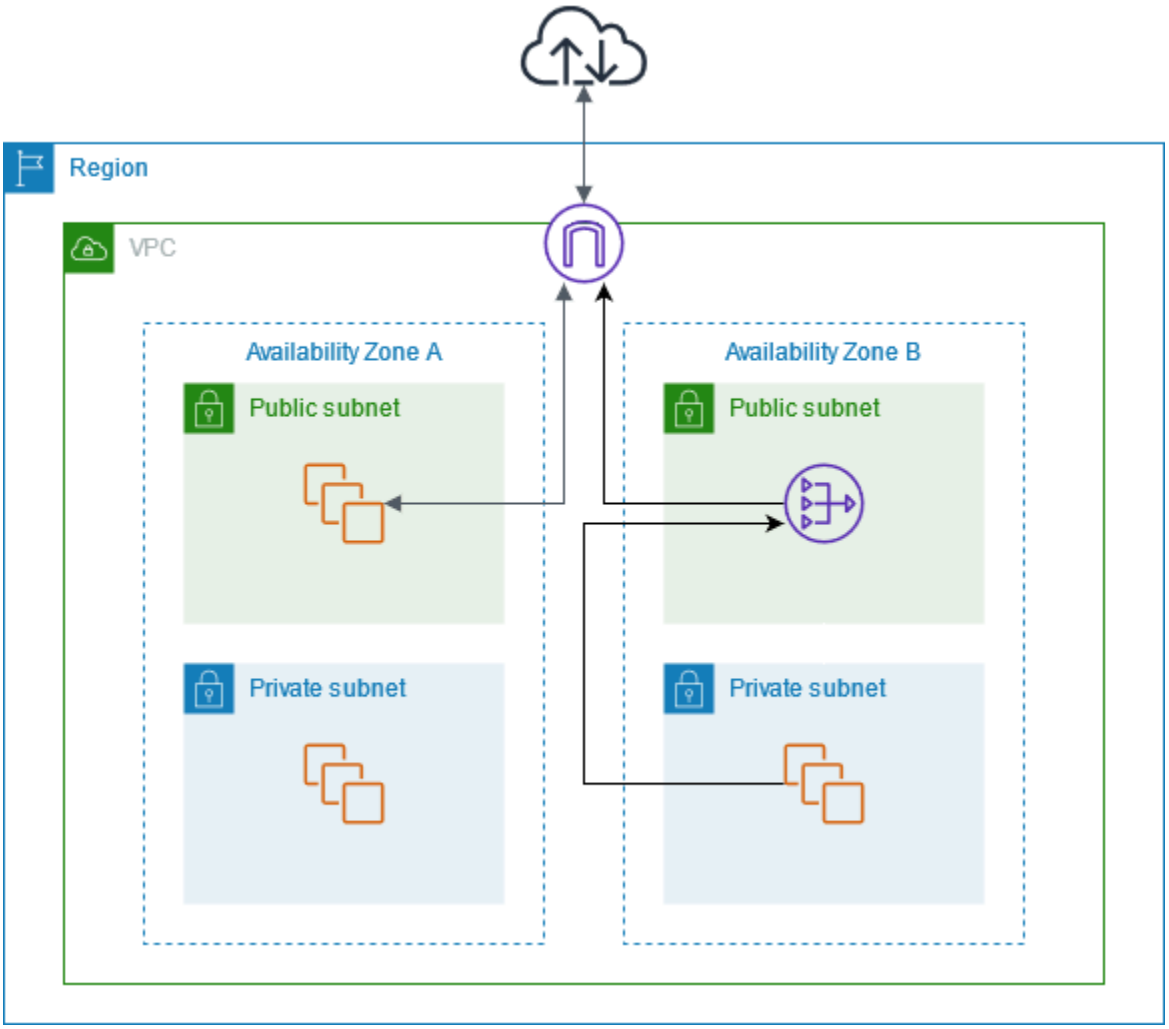
目錄

- 概要
- 路由
- 測試公有 NAT 閘道

概要

以下圖表說明此使用案例。有兩個可用區域，每個可用區域中皆有兩個子網。每個子網的路由表決定流量的路由方式。在可用區域 A 中，公有子網中的執行個體可以經由通往網際網路閘道的路由到達網際網路，而私有子網中的執行個體沒有通往網際網路的路由。在可用區域 B 中，公有子網包含一個 NAT 閘道，私有子網中的執行個體可經由通往公有子網中 NAT 閘道的路由到達網際網路。

私有與公有 NAT 閘道皆會將執行個體的來源私有 IPv4 位址映射至私有 NAT 閘道的私有 IPv4 位址；但如果是公有 NAT 閘道，網際網路閘道會將公有 NAT 閘道的私有 IPv4 位址映射至與 NAT 閘道相關聯的彈性 IP 位址。傳送回應流量至執行個體時，無論是公有或私有 NAT 閘道，NAT 閘道都會將地址轉譯回原始來源 IP 地址。



請注意，如果可用區域 A 的私有子網路中的執行個體也需要連線至網際網路，您可以建立從此子網路到可用區域 B 的 NAT 閘道的路由。或者，您也可以在每個包含需要網際網路存取資源的可用區域中建立 NAT 閘道，以提高彈性。如需範例圖表，請參閱the section called “私有伺服器”。

路由

與可用區域 A 中公有子網相關聯的路由表如下。第一個項目是本機路由；讓子網中的執行個體能使用私有 IP 地址與 VPC 中的其他執行個體通訊。第二個項目會將所有其他子網流量傳送到網際網路閘道，使子網中的執行個體能夠存取網際網路。

目標	Target
VPC CIDR	區域
0.0.0.0/0	*internet-gateway-id*

與可用區域 A 中私有子網相關聯的路由表如下。項目是本機路由，讓子網中的執行個體能使用私有 IP 地址與 VPC 中的其他執行個體通訊。此子網中的執行個體無法存取網際網路。

目標	Target
VPC CIDR	本機

與可用區域 B 中公有子網相關聯的路由表如下。第一個項目是本機路由，讓子網中的執行個體能使用私有 IP 地址與 VPC 中的其他執行個體通訊。第二個項目會將所有其他子網流量傳送到網際網路閘道，使子網中的 NAT 閘道能夠存取網際網路。

目標	Target
VPC CIDR	區域
0.0.0.0/0	*internet-gateway-id*

與可用區域 B 中私有子網相關聯的路由表如下。第一個項目是本機路由；讓子網中的執行個體能使用私有 IP 地址與 VPC 中的其他執行個體通訊。第二個項目會將所有其他子網的流量傳送到 NAT 閘道。

目標	Target
VPC CIDR	區域
0.0.0.0/0	*nat-gateway-id*

如需詳細資訊，請參閱the section called “管理子網路路由表”。

測試公有 NAT 閘道

在您建立 NAT 閘道並更新您的路由表之後，您可以從您私有子網中的執行個體 ping 網際網路上的遠端地址，測試其是否能連線到網際網路。如需如何執行此作業的範例，請參閱 測試網際網路連線。

若您可以連線到網際網路，您也可以測試網際網路流量是否透過 NAT 閘道路由傳送：

- 從私有子網中的執行個體追蹤流量的路由。若要執行此作業，請從您私有子網中的 Linux 執行個體執行 `traceroute` 命令。在輸出中，您會在其中一個躍點 (通常是第一個躍點) 看見 NAT 閘道的私有 IP 地址。
- 在您從私有子網中的執行個體連線到來源 IP 地址時，使用可顯示地址的第三方網站或工具。來源 IP 位址應為 NAT 閘道的彈性 IP 位址。

如果這些測試失敗，請參閱疑難排解 NAT 閘道。

測試網際網路連線

以下範例會示範私有子網中的執行個體可否連線到網際網路的測試方式。

1. 在您的公有子網中啟動執行個體 (以此做為堡壘主機)。在啟動精靈中，確認您已選取 Amazon Linux AMI，並指派一個公有 IP 地址給您的執行個體。

   確保您的安全群組規則允許從本機網路 IP 地址範圍的傳入 SSH 流量，以及傳出 SSH 流量到私有子網路的 IP 地址範圍。您也可以針對此測試`0.0.0.0/0`的傳入和傳出 SSH 流量使用 。
2. 在您的私有子網中啟動執行個體。在啟動精靈中，確認您已選取 Amazon Linux AMI。請勿指派公有 IP 地址給您的執行個體。確認您的安全群組規則允許來自您在公有子網中啟動之執行個體私有 IP 地址的傳入 SSH 流量，以及所有傳出 ICMP 流量。您所選擇的金鑰對必須與您用來在公有子網中啟動執行個體的金鑰對相同。
3. 在本機電腦上設定 SSH 代理程式轉送，然後連線到公有子網中的堡壘主機。如需詳細資訊，請參閱設定 Linux 或 macOS 的 SSH 代理程式轉送 或 設定 Windows 的 SSH 代理程式轉送。
4. 從您的堡壘主機連線到您私有子網中的執行個體，然後從您私有子網中的執行個體測試網際網路連線。如需詳細資訊，請參閱 測試網際網路連線。

設定 Linux 或 macOS 的 SSH 代理程式轉送

1. 從您的本機電腦，將您的私有金鑰新增至身分驗證代理程式。

   針對 Linux，請使用以下命令。

   ```
   ssh-add -c mykeypair.pem
   ```

   針對 macOS，請使用以下命令。

   ```
   ssh-add -K mykeypair.pem
   ```

2. 使用 -A 選項連線到您公有子網中的執行個體，以啟用 SSH 代理程式轉送，並使用執行個體的公有地址，如下列範例所示：

```
ssh -A ec2-user@54.0.0.123
```

設定 Windows 的 SSH 代理程式轉送

您可以使用 Windows 中可用的 OpenSSH 用戶端，或安裝您偏好的 SSH 用戶端 (例如 PuTTY)。

OpenSSH

如本文所述，安裝 OpenSSH for Windows：OpenSSH for Windows 入門。然後將您的金鑰新增到身分驗證代理程式。如需詳細資訊，請參閱《OpenSSH for Windows 中的金鑰型身分驗證》。

PuTTY

1. 如果您尚未安裝 Pageant，請轉至 PuTTY 下載頁面下載及安裝。
2. 將您的私有金鑰轉換成 .ppk 格式。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 PuTTYgen 轉換私有金鑰。
3. Start Pageant，開啟任務列上 Pageant 圖示的內容選單（可能隱藏），然後選擇新增金鑰。選取您建立的 .ppk 檔案，如需要則輸入密碼短語，然後選擇 Open (開啟)。
4. 啟動 PuTTY 工作階段，並使用其公有 IP 地址連線至您公有子網中的執行個體。如需詳細資訊，請參閱使用 PuTTY 連線至 Linux 執行個體。在 Auth (身分驗證) 類別中，確認您已選取 Allow agent forwarding (允許代理程式轉送) 選項，並將 Private key file for authentication (身分驗證的私有金鑰檔案) 方塊維持空白。

測試網際網路連線

1. 從您公有子網中的執行個體，使用其私有 IP 地址連線到您私有子網中的執行個體，如下列範例所示：

```
ssh ec2-user@10.0.1.123
```

2. 從私有執行個體，針對啟用 ICMP 的網站執行 ping 命令，以測試您是否能連線至網際網路。

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

按下鍵盤上的 Ctrl+C 取消 ping 命令。若 ping 命令失敗，請參閱 執行個體無法存取網路。

3. (選用) 若您不再需要您的執行個體，請予以終止。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的終止您的執行個體。

使用允許清單中的 IP 地址存取您的網路

您可以使用私有 NAT 閘道，利用允許清單中的地址集區，實現從 VPC 對內部部署網路的通訊。

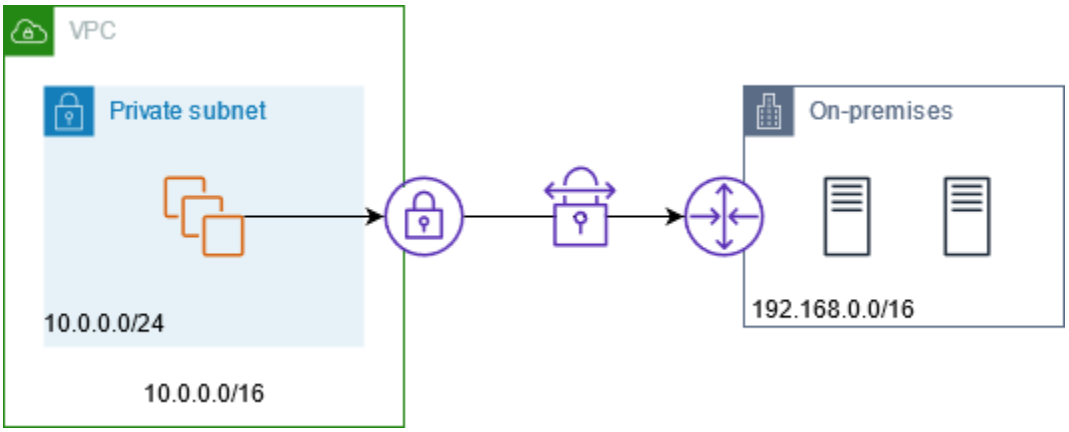
您可以利用允許列出範圍中的 IP 地址，透過私有 NAT 閘道路由來自子網路的流量，而不是將個別 IP 地址指派給每個執行個體。

目錄

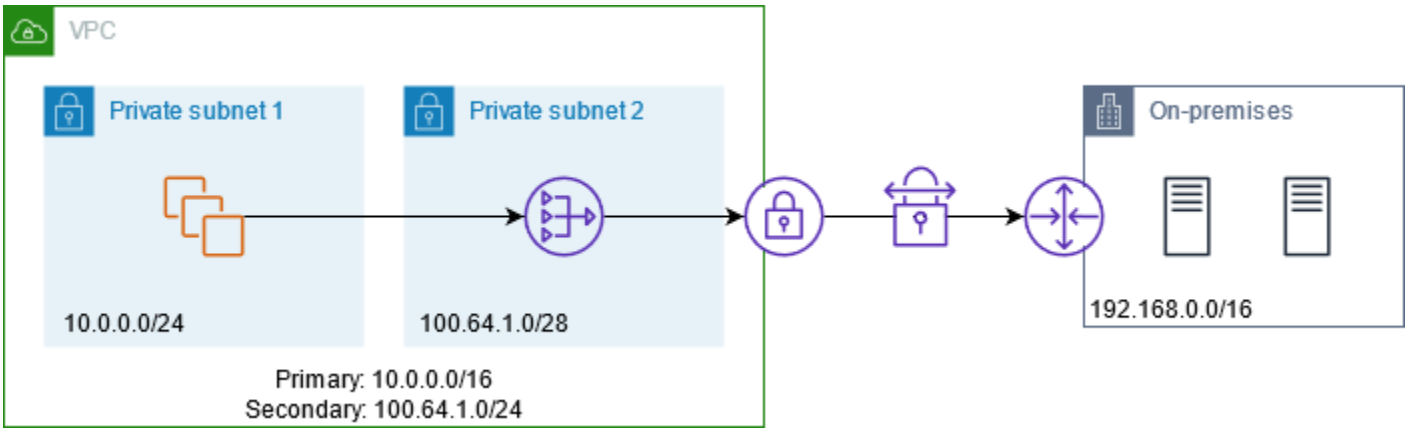
- 概要
- Resources
- 路由

概要

下圖顯示執行個體如何透過 存取內部部署資源 Site-to-Site VPN。來自執行個體的流量透過 VPN 連接路由到虛擬私有閘道、客戶閘道，然後到內部部署網路中的目的地。但是，假設目的地僅允許來自特定 IP 地址範圍 (例如 100.64.1.0/28) 的流量，此將阻止來自這些執行個體的流量到達內部部署網路。



下圖顯示此案例組態的重要元件。VPC 具有其原始 IP 地址範圍和允許的 IP 地址範圍。VPC 具有來自允許 IP 地址範圍的子網以及一個私有 NAT 閘道。會將來自以內部部署網路為目的地的執行個體的流量發送至 NAT 閘道，然後再路由到 VPN 連接。內部部署網路會接收來自具有 NAT 閘道來源 IP 地址 (來自允許的 IP 地址範圍內) 的執行個體的流量。



Resources

建立或更新資源，如下所示：

- 將允許的 IP 地址範圍關聯至 VPC。
- 從允許的 IP 地址範圍內在 VPC 中建立子網。
- 在新子網中建立私有 NAT 閘道。
- 使用執行個體更新子網的路由表，以便將以內部部署網路為目的地的流量發送至 NAT 閘道。將路由新增至具有私有 NAT 閘道的子網的路由表，其會將以內部部署網路為目的地的流量發送至虛擬私有閘道。

路由

以下為與第一個子網相關聯的路由表。每個 VPC CIDR 都有一個本地路由。本地路由讓子網中的資源能使用私有 IP 地址與 VPC 中的其他資源通訊。第三個條目將以內部部署網路為目的地的流量發送至私有 NAT 閘道。

目標	目標
10.0.0.0/16	本機
100.64.1.0/24	本機

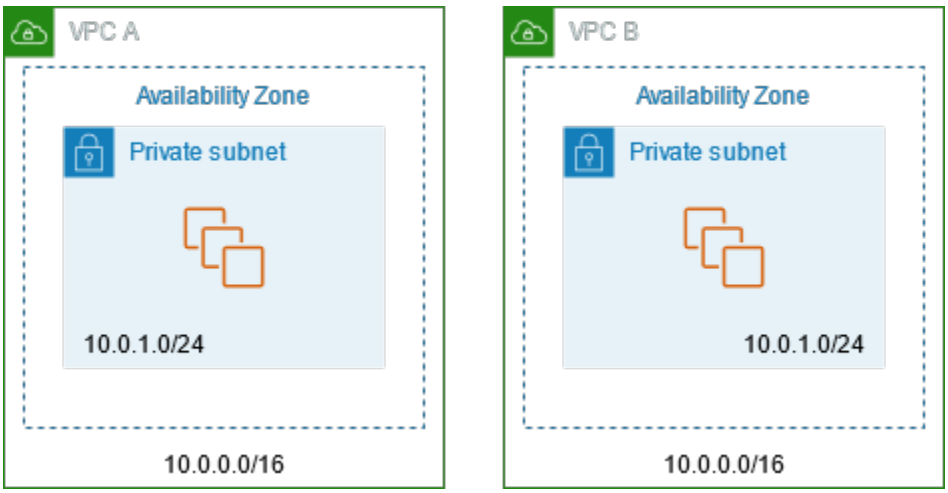
目標	目標
192.168.0.0/16	*nat-gateway-id*

以下為與第二個子網相關聯的路由表。每個 VPC CIDR 都有一個本地路由。本地路由讓子網中的資源能使用私有 IP 地址與 VPC 中的其他資源通訊。第三個條目將以內部部署網路為目的地的流量發送至虛擬私有閘道。

目標	目標
10.0.0.0/16	本機
100.64.1.0/24	本機
192.168.0.0/16	*vgw-id*

實現重疊網路之間的通訊

您可以使用私有 NAT 閘道實現網路之間的通訊，即使網路具有重疊的 CIDR 範圍。例如，假設 VPC A 中的執行個體需要存取由 VPC B 中執行個體提供的服務。



目錄

- 概要
- Resources
- 路由

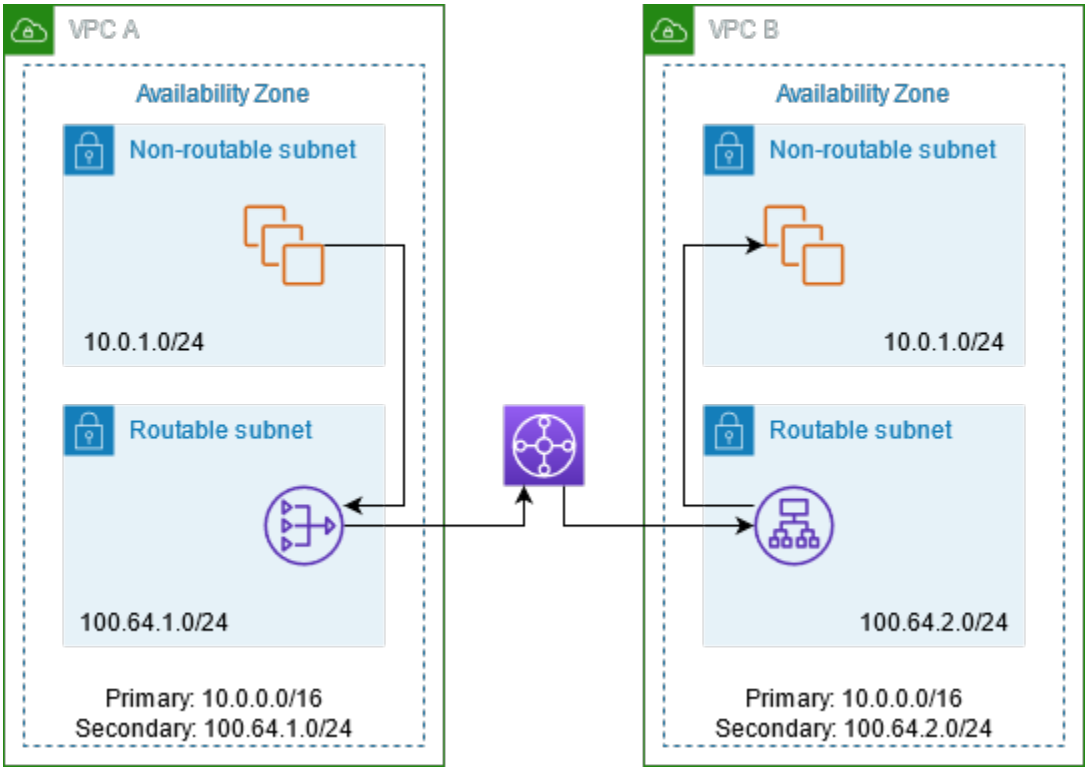
概要

下圖顯示此案例組態的重要元件。首先，IP 管理團隊要決定哪些位址範圍可以重疊 (不可路由位址範圍)，哪些範圍不能重疊 (可路由位址範圍)。IP 管理團隊根據請求，從可路由地址範圍的集區中將地址分配給專案。

每個 VPC 都有其不可路由的原始 IP 地址範圍，以及 IP 管理團隊指派給該 VPC 的可路由 IP 地址範圍。VPC A 具有一個來自其可路由範圍的子網以及一個私有 NAT 閘道。私有 NAT 閘道從其子網取得其 IP 地址。VPC B 具有一個來自其可路由範圍的子網以及一個 Application Load Balancer。Application Load Balancer 從其子網取得其 IP 地址。

來自 VPC A 不可路由子網路中執行個體的流量，其目的地為 VPC B 不可路由子網路中的執行個體，會透過私有 NAT 閘道傳送。然後，它會路由到傳輸閘道。

傳輸閘道將流量發送至 Application Load Balancer，由其將流量路由至 VPC B 不可路由子網中的其中一個目標執行個體。從轉換閘道到 Application Load Balancer 的流量具有私有 NAT 閘道的來源 IP 地址。因此，來自負載平衡器的回應流量使用私有 NAT 閘道的地址作為其目的地。將回應流量發送至傳輸閘道，然後路由至私有 NAT 閘道，其會將目的地轉換為 VPC A 不可路由子網中的執行個體。



Resources

建立或更新資源，如下所示：

- 將分派到的可路由 IP 地址範圍與其各自的 VPC 相關聯。
- 在 VPC A 中從其可路由 IP 地址範圍中建立子網，並在此新子網中建立私有 NAT 閘道。
- 在 VPC B 中從其可路由 IP 地址範圍中建立子網，並在此新子網中建立 Application Load Balancer。註冊不可路由子網中的執行個體以及目標群組，以便用於負載平衡器。
- 建立傳輸閘道以連接至 VPC。確認停用路由傳播。將每個 VPC 連接至傳輸閘道時，應使用 VPC 的可路由地址範圍。
- 更新 VPC A 中不可路由子網的路由表，以便將以 VPC B 可路由地址範圍為目的地的所有流量發送至私有 NAT 閘道。更新 VPC A 中可路由子網的路由表，以便將以 VPC B 可路由地址範圍為目的地的所有流量發送至傳輸閘道。
- 更新 VPC B 中可路由子網的路由表，以便將以 VPC A 可路由地址範圍為目的地的所有流量發送至傳輸閘道。

路由

以下為 VPC A 中不可路由子網的路由表。

目標	目標
10.0.0.0/16	本機
100.64.1.0/24	本機
100.64.2.0/24	*nat-gateway-id*

以下為 VPC A 中可路由子網的路由表。

目標	目標
10.0.0.0/16	本機
100.64.1.0/24	本機
100.64.2.0/24	*transit-gateway-id*

以下為 VPC B 中不可路由子網的路由表。

目標	目標
10.0.0.0/16	本機
100.64.2.0/24	本機

以下為 VPC B 中可路由子網的路由表。

目標	目標
10.0.0.0/16	本機
100.64.2.0/24	本機
100.64.1.0/24	*transit-gateway-id*

以下為傳輸閘道路由表。

CIDR	連接	路由類型
100.64.1.0/24	*VPC A ###*	靜態
100.64.2.0/24	*VPC B ###*	靜態

DNS64 和 NAT64

NAT 閘道支援從 IPv6 到 IPv4 的網路地址轉譯，通常稱為 NAT64。NAT64 可協助您的 IPv6 AWS 資源與相同 VPC 或不同 VPC 中的 IPv4 資源、內部部署網路或網際網路進行通訊。您可以搭配 Amazon Route 53 Resolver 上的 DNS64 來使用 NAT64，或使用您自己的 DNS64 伺服器。

目錄

- 什麼是 DNS64？
- 什麼是 NAT64？
- 設定 DNS64 與 NAT64

什麼是 DNS64？

在 VPC 中執行的僅限 IPv6 工作負載只能傳送和接收 IPv6 網路封包。如果沒有 DNS64，純 IPv4 服務的 DNS 查詢將產生 IPv4 目的地位址作為回應，而純 IPv6 服務無法與其通訊。若要橋接此通訊間隙，您可以為子網路啟用 DNS64，並將其套用至該子網路中的所有 AWS 資源。透過 DNS64，Amazon Route 53 Resolver 會查找您所查詢之服務的 DNS 記錄，並執行下列其中一項作業：

- 如果記錄包含 IPv6 地址，就會傳回原始記錄且會建立沒有任何透過 IPv6 轉譯的連線。
- 如果沒有與 DNS 記錄中的目的地關聯的 IPv6 地址，Route 53 Resolver 會合成一個 IPv6 地址，方法是在記錄中的 IPv4 地址預先加上已知的 /96 字首 (在 RFC6052 (64:ff9b::/96) 中定義)。

  您的僅限 IPv6 服務會將網路封包傳送到合成的 IPv6 地址。然後，您透過 NAT 閘道路由此流量，它會對流量執行必要的轉譯，以允許子網路中的 IPv6 服務存取該子網路外的 IPv4 服務。

您可以使用 modify-subnet-attribute 來啟用或停用子網路上的 DNS64，方法是使用 AWS CLI 或透過 VPC 主控台選取子網路，然後選擇動作 > 編輯子網路設定。

什麼是 NAT64？

NAT64 可讓 Amazon VPC 中的僅限 IPv6 服務與相同 VPC (位於不同子網中) 或連線的 VPC、現場部署網路或透過網際網路的僅限 IPv4 服務通訊。

NAT64 會自動在您現有的 NAT 閘道或您建立的任何新 NAT 閘道上提供。您無法啟用或停用此功能。NAT 閘道所在的子網路不需要是雙堆疊子網路 NAT64 才能運作。

啟用 DNS64 後，如果僅限 IPv6 的服務透過 NAT 閘道將網路封包傳送至合成的 IPv6 地址，就會發生下列情況：

- NAT 閘道會從 64:ff9b::/96 字首辨識原始目的地是 IPv4，並將 IPv6 封包轉譯為 IPv4，方法是取代：
  - 具有自己的私有 IP 之來源 IPv6，由網際網路閘道轉譯為彈性 IP 地址。
  - 目的地 IPv6 到 IPv4 (藉由截斷 64:ff9b::/96 字首的方式)。
- NAT 閘道會透過網際網路閘道、虛擬私有閘道或傳輸閘道，將轉譯的 IPv4 封包傳送至目的地並啟動連線。
- 僅限 IPv4 主機會傳回 IPv4 回應封包。建立連線後，NAT 閘道就會接受來自外部主機的回應 IPv4 封包。

- 回應 IPv4 封包的目的地為 NAT 閘道，它會接收封包，並透過將其 IP （目的地 IP) 取代為主機的 IPv6 地址，並附加64:ff9b::/96回來源 IPv4 地址來取消 NATs 封包。然後，封包會依照本機路由流向主機。

這樣，子網路中僅限 IPv6 的工作負載就可以透過 NAT 閘道與子網路外僅限 IPv4 的服務通訊。

設定 DNS64 與 NAT64

請依照本節中的步驟設定 DNS64 和 NAT64，以啟用與僅限 IPv4 的服務之通訊。

目錄

- 使用 CLI 在網際網路上啟用與IPv4-only AWS 服務的通訊
- 在您的內部部署環境啟用中啟用與僅限 IPv4 的服務之通訊

使用 CLI 在網際網路上啟用與IPv4-only AWS 服務的通訊

如果您的子網具有僅限 IPv6 的工作負載，而且需要與子網外僅限 IPv4 的服務通訊，此範例會示範如何啟用這些僅限 IPv6 的服務來與網際網路上僅限 IPv4 的服務通訊。

您應該先在公有子網中設定 NAT 閘道 (與包含僅限 IPv6 的工作負載之子網分開)。例如，包含 NAT 閘道的子網應該有指向網際網路閘道的 0.0.0.0/0 路由。

請完成下列步驟，讓這些僅限 IPv6 的服務與網際網路上僅限 IPv4 的服務連接：

1. 將下列三個路由新增至包含僅限 IPv6 的工作負載之子網的路由表：

   - 指向 NAT 閘道的 IPv4 路由 (如果有的話)。
   - 指向 NAT 閘道的 64:ff9b::/96 路由。這將允許來自僅限 IPv6 的服務之工作負載的流量，透過 NAT 閘道路由傳送至僅限 IPv4 的服務。
   - 指向僅傳出之網際網路閘道 (或網際網路閘道) 的 IPv6 ::/0 路由。

   請注意，指向 ::/0 到網際網路閘道將允許外部 IPv6 主機 (VPC 外部) 透過 IPv6 啟動連線。

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
```

```
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. 在包含僅限 IPv6 的工作負載之子網中啟用 DNS64 功能。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

現在，私有子網中的資源可以同時與網際網路上的 IPv4 和 IPv6 服務建立狀態連線。妥善設定您的安全群組和 NACL 來允許 64:ff9b::/96 流量的傳出與傳入。

在您的內部部署環境啟用中啟用與僅限 IPv4 的服務之通訊

Amazon Route 53 Resolver 可讓您將 DNS 查詢從 VPC 轉發到內部部署網路，反之亦然。若要這麼做，請執行下列操作：

- 您可以在 VPC 中建立 Route 53 Resolver 輸出端點，並將其指派至您要 Route 53 Resolver 轉發查詢的來源 IPv4 地址。對於您的內部部署 DNS 解析程式而言，這些是 DNS 查詢產生來源的 IP 地址，因此應該是 IPv4 地址。
- 您要建立一或多項規則，指定您希望 Route 53 Resolver 轉送到您內部部署解析程式之 DNS 查詢的網域名稱。您也要指定內部部署解析程式的 IPv4 地址。
- 現在您已設定 Route 53 Resolver 傳出端點，您需要在包含IPv6-only6 工作負載的子網路上啟用 DNS64。您也需要透過 NAT 閘道路由任何目的地為內部部署網路的資料。

DNS64 針對內部部署網路中僅限 IPv4 的目的地之運作方式：

1. 您可以將 IPv4 地址指派給 VPC 中 Route 53 Resolver 的輸出端點。
2. 從您的 IPv6 服務的 DNS 查詢，會透過 IPv6 進入 Route 53 Resolver。Route 53 Resolver 會比對轉送規則的查詢，並取得內部部署解析程式的 IPv4 地址。
3. Route 53 Resolver 會將查詢封包從 IPv6 轉換為 IPv4，並將其轉送到輸出端點。端點的每個 IP 地址都代表一個 ENI，會將要求轉送至 DNS 解析程式的內部部署 IPv4 地址。
4. 內部部署解析程式會透過 IPv4 將回應封包藉由輸出端點傳回 Route 53 Resolver。
5. 假設查詢是從啟用了 DNS64 的子網提出，Route 53 Resolver 會執行兩件事：

a. 檢查回應封包的內容。如果記錄中有 IPv6 地址，它會保持內容不變，但如果它只包含 IPv4 記錄。就合成一個 IPv6 記錄，並且在 IPv4 地址前面加上 `64:ff9b::/96`。

b. 重新包裝內容，並透過 IPv6 將其傳送至 VPC 中的服務。

檢查來自 NAT 閘道的流量

您可以將 Network Firewall Proxy 連接至 NAT Gateway，以檢查和篩選 NAT Gateway 上的流量。此安全控制可讓您防止資料在信任的周邊外洩漏，並封鎖任何不需要的傳入回應。

運作方式

建立 Network Firewall Proxy 時，您必須選取要連接 Proxy 的現有 NAT Gateway。建立之後，代理：

- Proxy 隨附完整網域名稱，您需要將應用程式設定為將 http 和 https 連線請求傳送至 Proxy。代理會先根據客戶輸入的規則，篩選連線請求中的網域名稱。如果客戶允許，代理會進行 DNS 查詢以取得網域的 IP 地址。然後，它建立了與最終目的地的 TCP 連線。根據是否啟用 TLS 解密，代理接著會篩選 IP 地址和標頭屬性上的 TLS 連線，並且只有在政策允許 IP 和標頭屬性（包括標頭動作和 URL 路徑）時，才會建立與目的地的 TLS 連線。
- 設備會檢查和篩選流量。
- 允許流量繼續流向目的地（在網際網路或內部部署環境或其他 VPC 中）。

連接設備

設備會透過 AWS Network Firewall 連接到 NAT Gateway。如需建立和連接設備的步驟，請參閱 Network Firewall Proxy 開發人員指南。

檢視連接的設備

若要檢視連接至 NAT Gateway 的設備，請使用 describe-nat-gateways 命令：

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-1234567890abcdef0
```

回應包含顯示下列項目`AttachedAppliances`的欄位：

- 類型 – 設備類型（例如 `network-firewall-proxy`)
- ApplianceArn – 連接的設備的 ARN
- AttachmentState – 目前的連接狀態 (`attached`、`detaching`、`detached`、`attach_failed`、`detach_failed`)

- ModificationState – 目前的修改狀態 (`modifying`、`completed`、`failed`)
- VpcEndpointId – 用來將流量從應用程式 VPC 路由到代理以進行檢查和篩選VPCs 端點 ID
- FailureCode – 設備連接或修改操作失敗時的失敗代碼
- FailureMessage – 如果設備連接或修改操作失敗，說明失敗的描述性訊息

使用 Amazon CloudWatch 監控 NAT 閘道

您可以使用 CloudWatch 監控 NAT 閘道以收集來自 NAT 閘道的原始資料，並處理為可讀且近乎即時的指標。您可以使用此資訊來監控 NAT 閘道並進行故障診斷。這些指標可讓您了解 NAT 閘道的運作狀態和效能，讓您密切監控其操作並快速疑難排解任何問題。

CloudWatch 收集的 NAT 閘道指標包括處理位元組、封包計數、連線計數和錯誤率等資料點。這可讓您徹底了解流經 NAT 閘道的流量，並識別任何異常或瓶頸。CloudWatch 每隔 1 分鐘提供此指標資料，讓您精細地查看 NAT 閘道的行為。

此外，CloudWatch 會保留此 NAT 閘道指標資料 15 個月，讓您分析一段時間內的趨勢和模式。您可以使用此歷史資料進行容量規劃、效能最佳化，以及了解 NAT 閘道用量的長期演變。

若要使用這些強大的監控功能，您可以根據特定需求建立自訂 CloudWatch 儀表板和警示。例如，您可以設定提醒，以便在 NAT 閘道的傳出資料傳輸超過特定閾值時通知您，讓您主動解決潛在的頻寬限制。

如需定價的詳細資訊，請參閱 Amazon CloudWatch 定價。

目錄

- NAT 閘道指標和維度
- 檢視 NAT 閘道 CloudWatch 指標
- 建立 CloudWatch 警報以監控 NAT 閘道

NAT 閘道指標和維度

以下指標可用於您的 NAT 閘道。描述欄包括每個指標以及單位和統計資料的描述。

指標	描述
`ActiveConnectionCount`	通過 NAT 閘道的並行作用中 TCP 連線的總數。 0 值表示沒有作用中連線通過 NAT 閘道。

指標	描述
	單位：計數 統計資訊：最實用的統計資訊是 Max。
BytesInFromDestination	NAT 閘道接收到來自目的地的位元組數量。 如果 BytesOutToSource 的值小於 BytesInFromDestination 的值，可能有資料在 NAT 閘道處理期間流失，或有流量被 NAT 閘道主動封鎖。 單位：位元組 統計資訊：最實用的統計資訊是 Sum。
BytesInFromSource	NAT 閘道接收到來自您的 VPC 中的用戶端的位元組數量。 如果 BytesOutToDestination 的值小於 BytesInFromSource 的值，可能有資料在 NAT 閘道處理期間流失。 單位：位元組 統計資訊：最實用的統計資訊是 Sum。
BytesOutToDestination	透過 NAT 閘道送出至目的地的位元組數量。 大於 0 的值表示，有流量從 NAT 閘道之後的用戶端流出至網際網路。如果 BytesOutToDestination 的值小於 BytesInFromSource 的值，可能有資料在 NAT 閘道處理期間流失。 單位：位元組 統計資訊：最實用的統計資訊是 Sum。

指標	描述
BytesOutToSource	透過 NAT 閘道送出至您的 VPC 中的用戶端的位元組數量。 大於 0 的值表示，有流量從網際網路流入至 NAT 閘道之後的用戶端。如果 BytesOutToSource 的值小於 BytesInFromDestination 的值，可能有資料在 NAT 閘道處理期間流失，或有流量被 NAT 閘道主動封鎖。 單位：位元組 統計資訊：最實用的統計資訊是 Sum。
ConnectionAttemptCount	透過 NAT 閘道嘗試連線的數量。這僅包含初始 SYN。在某些情況下，ConnectionAttemptCount 可能會因為 SYN 重新傳輸而低於 ConnectionEstablishedCount 。 如果 ConnectionEstablishedCount 的值小於 ConnectionAttemptCount 的值，表示 NAT 閘道之後的用戶端嘗試建立新的連線，但沒有回應。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
ConnectionEstablishedCount	透過 NAT 閘道建立的連線數量。這包含 SYN 與 SYN 重新傳輸。 如果 ConnectionEstablishedCount 的值小於 ConnectionAttemptCount 的值，表示 NAT 閘道之後的用戶端嘗試建立新的連線，但沒有回應。 單位：計數 統計資訊：最實用的統計資訊是 Sum。

指標	描述
ErrorPortAllocation	NAT 閘道無法配置來源連接埠的次數。 大於 0 的值表示，有過多的並行連線透過 NAT 閘道開啟。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
IdleTimeoutCount	從作用中狀態轉換為閒置狀態的連線數量。作用中連線若未正常關閉，而且過去 350 秒皆無活動，將轉換為閒置狀態。 大於 0 的值表示，有連線已移至閒置狀態。如果 IdleTimeoutCount 的值增加，可能表示 NAT 閘道後面的用戶端正在重新使用過時的連線。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
PacketsDropCount	NAT 閘道捨棄的封包數量。 若要以整體封包流量的百分比計算捨棄的封包數量，請使用此公式：PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*100 。如果此值超過 NAT 閘道上總流量的 0.01%，則 Amazon VPC 服務可能有問題。使用 AWS 服務運作狀態儀表板來識別任何可能導致 NAT 閘道捨棄封包的服務問題。 單位：Count 統計資訊：最實用的統計資訊是 Sum。

指標	描述
PacketsInFromDestination	NAT 閘道接收到來自目的地的封包數量。 如果 PacketsOutToSource 的值小於 PacketsInFromDestination 的值，可能有資料在 NAT 閘道處理期間流失，或有流量被 NAT 閘道主動封鎖。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
PacketsInFromSource	NAT 閘道接收到來自您的 VPC 中的用戶端的封包數量。 如果 PacketsOutToDestination 的值小於 PacketsInFromSource 的值，可能有資料在 NAT 閘道處理期間流失。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
PacketsOutToDestination	透過 NAT 閘道送出至目的地的封包數量。 大於 0 的值表示，有流量從 NAT 閘道之後的用戶端流出至網際網路。如果 PacketsOutToDestination 的值小於 PacketsInFromSource 的值，可能有資料在 NAT 閘道處理期間流失。 單位：計數 統計資訊：最實用的統計資訊是 Sum。

指標	描述
PacketsOutToSource	透過 NAT 閘道送出至您的 VPC 中的用戶端的封包數量。 大於 0 的值表示，有流量從網際網路流入至 NAT 閘道之後的用戶端。如果 PacketsOutToSource 的值小於 PacketsInFromDestination 的值，可能有資料在 NAT 閘道處理期間流失，或有流量被 NAT 閘道主動封鎖。 單位：計數 統計資訊：最實用的統計資訊是 Sum。
PeakBytesPerSecond	此指標報告一分鐘內每秒最高 10 秒位元組的平均值。 單位：Count 統計資訊：最實用的統計資訊是 Maximum。
PeakPacketsPerSecond	此指標會每 10 秒計算 60 秒的平均封包速率 (每秒處理的封包數)，然後報告六個速率的最大值 (最高平均封包速率)。 單位：Count 統計資訊：最實用的統計資訊是 Maximum。

若要篩選指標資料，請使用下列維度。

維度	描述
NatGatewayId	可藉由 NAT 閘道 ID 來篩選指標資料。區域 NAT 閘道只會使用此維度。區域 NAT 閘道會搭配 使用此維度AvailabilityZone 。

維度	描述
AvailabilityZone	依可用區域篩選指標資料。區域 NAT 閘道會搭配 使用此維度NatGatewayId 。區域 NAT 閘道不會使用此維度。

檢視 NAT 閘道 CloudWatch 指標

NAT 閘道指標每間隔 1 分鐘傳送至 CloudWatch。指標會先依服務命名空間分組，再依各命名空間內可能的維度組合分組。您可以下列步驟來檢視 NAT 閘道的指標。

使用 CloudWatch 主控台檢視指標

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Metrics (指標)、All metrics (所有指標)。
3. 選擇 NATGateway 指標命名空間。
4. 選擇指標維度。

使用 檢視指標 AWS CLI

在命令提示中，使用下列命令來列出可用於 NAT 閘道服務的指標。

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

建立 CloudWatch 警報以監控 NAT 閘道

您可以建立 CloudWatch 警報，在警示變更狀態時傳送 Amazon SNS 訊息。警示會在您指定的期間監看單一指標。警報會根據在數個期間與指定閾值相關的指標值，傳送通知給 Amazon SNS 主題。

例如，您可以建立警示來監控傳入或傳出 NAT 閘道的流量。下列警示會監控來自您 VPC 中的用戶端，透過 NAT 閘道，傳送至網際網路的傳出流量。如果位元組數在 15 分鐘期間內達到 5,000,000 閾值，將會傳送通知。

建立透過 NAT 閘道的傳出流量警示

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Alarms (警示)、All alarms (所有警示)。

3. 選擇 Create alarm (建立警示)。
4. 選擇 Select metric (選取指標)。
5. 選擇 NATGateway 指標命名空間，然後選擇指標維度。移至指標時，請選取 NAT 閘道的 BytesOutToDestination 指標旁邊的核取方塊，然後選擇 Select metric (選取指標)。
6. 如下設定警示，然後選擇 Next (下一步)。
   - 在 Statistic (統計資料) 中選擇 Sum (總和)。
   - 對於 Period (時段)，選擇 15 Minute (15 分鐘)。
   - 對於 Whenever (隨時)，選擇 Greater/Equal (大於/等於)，然後輸入 5000000 作為閾值。
7. 對於 Notification (通知)，請選取現有的 SNS 主題，或選擇 Create new topic (建立新主題) 來建立新主題。選擇下一步。
8. 輸入警示的名稱和說明，然後選擇 Next (下一步)。
9. 當您完成設定警示時，請選擇 Create alarm (建立警示)。

作為另一個範例，您可以建立警示來監控連接埠配置錯誤，並在連續三個 5 分鐘期間內值大於零 (0) 時傳送通知。

建立警示以監控連接埠配置錯誤

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Alarms (警示)、All alarms (所有警示)。
3. 選擇 Create alarm (建立警示)。
4. 選擇 Select metric (選取指標)。
5. 選擇 NATGateway 指標命名空間，然後選擇指標維度。移至指標時，請選取 NAT 閘道的 ErrorPortAllocation 指標旁邊的核取方塊，然後選擇 Select metric (選取指標)。
6. 如下設定警示，然後選擇 Next (下一步)。
   - 對於 Statistic (統計數字)，選擇 Maximum (最大值)。
   - 對於 Period (時段)，選擇 5 Minute (5 分鐘)。
   - 對於 Whenever (隨時)，選擇 Greater (大於)，然後輸入 0 作為閾值。
   - 對於 Additional configuration (其他組態) 下的 Datapoints to alarm (要警示的資料點)，輸入 3。
7. 對於 Notification (通知)，請選取現有的 SNS 主題，或選擇 Create new topic (建立新主題) 來建立新主題。選擇下一步。
8. 輸入警示的名稱和說明，然後選擇 Next (下一步)。

9. 完成設定警示之後，請選擇 Create alarm (建立警示)。

如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。

疑難排解 NAT 閘道

以下主題可協助您在建立或使用 NAT 閘道時可能遇到的常見問題進行疑難排解。

問題

- NAT 閘道建立失敗
- NAT 閘道配額
- 彈性 IP 地址配額
- 不支援此可用區域
- NAT 閘道無法顯示
- NAT 閘道沒有回應 ping 命令
- 執行個體無法存取網路
- TCP 連線到目標失敗
- Traceroute 輸出沒有顯示 NAT 閘道私有 IP 地址
- 網際網路連線在 350 秒之後卸除
- 無法建立 IPsec 連線
- 無法初始化更多的連線

NAT 閘道建立失敗

問題

您建立 NAT 閘道並進入 `Failed` 狀態。

> **Note**
>
> 失敗的 NAT 閘道會自動刪除 (通常是在大約一小時內)。

原因

建立 NAT 閘道時發生錯誤。回傳的狀態訊息提供錯誤的原因。

解決方案

若要檢視錯誤訊息，請開啟 Amazon VPC 主控台，然後選擇 NAT 閘道。選取 NAT 閘道的選項按鈕，然後在 Details (詳細資訊) 索引標籤上尋找 State message (狀態訊息)。

下表列出導致 Amazon VPC 主控台中指出之錯誤的可能原因。在您套用任何指示的補救步驟之後，您可以嘗試再次建立 NAT 閘道。

顯示的錯誤	原因	解決方案
子網路擁有的可用地址數不足以建立此 NAT 閘道	您指定的子網路中沒有任何可用的私有 IP 地址。NAT 閘道需要網路界面具備從子網路的範圍配置的私有 IP 地址。	透過 Amazon VPC 主控台的子網路頁面檢查您的子網路中有多少可用的 IP 地址。您可以在詳細窗格中檢視子網路的 可用的 IPs。若要在您的子網路中建立可用的 IP 地址，您可以刪除未使用的網路界面，或是終止您不再需要的執行個體。
網路 vpc-xxxxxxxx 沒有連接的網際網路閘道	NAT 閘道必須在具備網際網路閘道的 VPC 中建立。	建立網際網路閘道並連接到您的 VPC。如需詳細資訊，請參閱將網際網路存取新增至子網路。
彈性 IP 地址 eipalloc-xxxxxxxx 已建立關聯	您指定的彈性 IP 地址已與其他資源建立關聯，因此無法與此 NAT 閘道建立關聯。	檢查與彈性 IP 地址關聯的資源。到 Amazon VPC 主控台的彈性 IP 頁面，檢視執行個體 ID 或網路介面 ID 指定的值。若您不需要針對該資源使用彈性 IP 地址，您可以取消其關聯。或者，將新的彈性 IP 地址配置到您的帳戶。如需詳細資訊，請參閱開始使用彈性 IP 位址。

NAT 閘道配額

當您嘗試建立 NAT 閘道時，得到下列錯誤。

```
Performing this operation would exceed the limit of 5 NAT gateways
```

原因

您已達到該可用區域 NAT 閘道的數量配額。

解決方案

如果您已達到帳戶的此 NAT 閘道配額，您可以執行下列其中一項動作：

- 使用 Service Quotas 主控台要求增加每個可用區域配額的 NAT 閘道。
- 檢查您 NAT 閘道的狀態。Pending、Available 或 Deleting 狀態都會計入您的配額。如果您最近刪除 NAT 閘道，等待數分鐘待其狀態從 Deleting 變為 Deleted。然後嘗試建立新的 NAT 閘道。
- 若您在特定可用區域中不需要 NAT 閘道，請嘗試在您尚未到達配額的可用區域內建立 NAT 閘道。

如需詳細資訊，請參閱 Amazon VPC 配額。

彈性 IP 地址配額

問題

當您嘗試為公有 NAT 閘道配置彈性 IP 地址時，會發生以下錯誤。

```
The maximum number of addresses has been reached.
```

原因

您已達到該區域帳戶彈性 IP 地址的數量配額。

解決方案

如果您已達彈性 IP 地址的配額，您可以從其他資源取消與彈性 IP 地址的關聯。或者，您可以使用 Service Quotas 主控台要求增加彈性 IP 配額。

不支援此可用區域

問題

當您嘗試建立 NAT 閘道時，得到下列錯誤：`NotAvailableInZone`。

原因

您可能會在受到限制的可用區域 (即擴展功能受限的區域) 中嘗試建立 NAT 閘道。

解決方案

我們無法支援這些可用區域內的 NAT 閘道。您可以在不同的可用區域中建立 NAT 閘道，並將其用於受限制區域中的私有子網路。您也可以將您的資源移動到未受限制的可用區域，讓您的資源及 NAT 閘道位於相同的區域內。

NAT 閘道無法顯示

問題

您已建立 NAT 閘道，但無法在 Amazon VPC 主控台中顯示。

原因

建立 NAT 閘道期間可能發生錯誤，建立失敗。大約一小時後，您便可在 Amazon VPC 主控台中看見狀態為 `Failed` 的 NAT 閘道。在一小時後，會自動刪除。

解決方案

請檢閱 NAT 閘道建立失敗 中的資訊，並嘗試建立新的 NAT 閘道。

NAT 閘道沒有回應 ping 命令

問題

當您嘗試從網際網路 (例如您的家用電腦) 或您 VPC 中的執行個體 ping NAT 閘道的彈性 IP 地址或私有 IP 地址時，您將無法取得回應。

原因

NAT 閘道只會將來自私有子網路中執行個體的流量傳遞至網際網路。

解決方案

若要測試您的 NAT 閘道是否正常運作，請參閱 測試公有 NAT 閘道。

執行個體無法存取網路

問題

您已建立公有 NAT 閘道並依照步驟測試，但 ping 指令錯誤，或您的執行個體在私有子網路中無法存取網路。

原因

導致此問題的原因可能為下列其中一項：

- NAT 閘道尚未準備好服務流量。
- 您的路由表未正確設定。
- 您的安全群組或網路 ACLs 正阻擋輸入或傳輸流量。
- 您正在使用不支援的通訊協定。

解決方案

檢查下列資訊：

- 檢查 NAT 閘道處於 Available 狀態。在 Amazon VPC 主控台中，前往 NAT 閘道頁面並在詳細資訊窗格中檢視狀態資訊。若 NAT 閘道處於失敗狀態，表示在建立時可能發生錯誤。如需詳細資訊，請參閱 NAT 閘道建立失敗。
- 確認您已正確設定路由表：
  - NAT 閘道必須位於具備可將網際網路流量路由至網際網路閘道之路由表的公有子網路中。
  - 您的執行個體必須位於具備可將網際網路流量路由至 NAT 閘道之路由表的私有子網路中。
  - 檢查是否沒有其他路由表項目將所有或部分的網際網路流量路由至其他非 NAT 閘道的裝置。
- 確認您私有執行個體的安全群組規則允許傳出網際網路流量。若要使 ping 命令正常運作，規則也必須允許傳出 ICMP 流量。

  NAT 閘道本身允許所有傳出流量及接收傳出請求之回應所產生的流量 (因此其具有狀態)。
- 確認與私有子網路和公有子網路關聯的網路 ACL 沒有封鎖傳入或傳出網際網路流量的規則。若要使 ping 命令正常運作，規則也必須允許傳入和傳出 ICMP 流量。

  您可以啟用流程日誌，協助您診斷因網路 ACL 或安全群組規則而遭到卸除的連線。如需詳細資訊，請參閱 使用 VPC 流量日誌來記錄 IP 流量。
- 若您使用 ping 命令，請確認您要 ping 的主機已啟用 ICMP。如果 ICMP 沒有啟用，您將無法接收回覆封包。若要測試此作業，請從您電腦的命令列終端機執行相同的 ping 命令。

- 檢查您的執行個體是否能夠 ping 其他資源，例如：位於私有子網路內的其他執行個體 (假設安全群組規則允許此行為)。
- 確認您的連線只使用 TCP、UDP 或 ICMP 通訊協定。

TCP 連線到目標失敗

問題

您的部分執行個體 TCP 連線位於私有子網路，透過 NAT 閘道指定到特定目標成功，但是有部分失敗或逾時。

原因

導致此問題的原因可能為下列其中一項：

- 目標端點正在回應分段的 TCP 封包。NAT 閘道不支援 TCP 或 ICMP 的 IP 分段。如需詳細資訊，請參閱 比較 NAT 執行個體和 NAT 閘道。
- `tcp_tw_recycle` 選項可在遠端伺服器上啟用，已知當 NAT 裝置後方有多個連線時會導致問題。

解決方案

驗證您正在嘗試連線的端點以分散的 TPC 封包回應，執行以下步驟：

1. 在公有子網路 IP 地址使用執行個體來從特定端點觸發大小足以引發分散的回應。
2. 使用 `tcpdump` 公用程式驗證端點傳送分散式封包。

> **Important**
>
> 您必須使用位於公有子網路中的執行個體執行這些檢查。您無法使用原始連線失敗的執行個體，或是位於 NAT 閘道或 NAT 執行個體後方私有子網路內的執行個體。

   傳送或接收大型 ICMP 封包的診斷工具會報告封包遺失。例如，`ping -s 10000 example.com` 命令無法在 NAT 閘道後方正常運作。
3. 若端點傳送的是分散式 TCP 封包，您可以改為使用 NAT 執行個體而非 NAT 閘道。

如果能存取遠端伺服器，您可以透過執行下列步驟驗證 `tcp_tw_recycle` 選項是否啟用：

1. 從伺服器端，執行下列命令：

```
cat /proc/sys/net/ipv4/tcp_tw_recycle
```

   如果輸出是 1，則 tcp_tw_recycle 選項已啟用。

2. 如果 tcp_tw_recycle 已啟用，我們建議將其停用。如果您需要重新使用連線，tcp_tw_reuse 是更安全的選項。

如果您無法存許遠端伺服器，您可以透過在私有子網路中暫時停用執行個體的 tcp_timestamps 選項進行測試。然後再一次連線至遠端伺服器。如果連線成功，則先前錯誤的原因可能是因為 tcp_tw_recycle 在遠端伺服器上已啟用。如果可能，聯繫遠端伺服器的擁有者來驗證此選項已啟用，然後要求將其停用。

Traceroute 輸出沒有顯示 NAT 閘道私有 IP 地址

問題

您的執行個體可存取網際網路，但當您執行 traceroute 命令時，輸出沒有顯示 NAT 閘道的私有 IP 地址。

原因

您的執行個體會使用不同閘道存取網際網路，例如網際網路閘道。

解決方案

在您執行個體所在子網路的路由表中，檢查下列資訊：

- 確認其中有將網際網路流量傳送至 NAT 閘道的路由。
- 確認其中沒有更明確的路由，將網際網路流量傳送至其他裝置 (例如虛擬私有閘道或網際網路閘道)。

網際網路連線在 350 秒之後卸除

問題

您的執行個體可以存取網路，但連線在 350 秒後卸除。

原因

若使用 NAT 閘道的連線閒置達 350 秒或以上，連線便會逾時。

如果連線逾時，NAT 閘道會對 NAT 閘道後的任何資源傳回 RST 封包來嘗試繼續連線 (不會傳送 FIN 封包)。

解決方案

您可以在連線上初始化更多流量來防止連線遭到卸除。或者，您可以在執行個體上啟用 TCP 存留並且值小於 350 秒。

無法建立 IPsec 連線

問題

您無法建立 IPsec 連線至目標。

原因

NAT 閘道目前不支援 IPsec 通訊協定。

解決方案

您可以使用 NAT-Traversal (NAT-T) 將 IPsec 流量封裝於 UDP 中。NAT 閘道支援 UDP 通訊協定。請務必測試您的 NAT-T 和 IPsec 組態，確認您的 IPsec 流量並未遭到卸除。

無法初始化更多的連線

問題

您有透過 NAT 閘道的現有目標連線，但您無法建立更多連線。

原因

您可能已達單一 NAT 閘道同時連線的上限。如需詳細資訊，請參閱 NAT 閘道基本概念。若您私有子網路中的執行個體建立大量的連線，您便可能達到此限制。

解決方案

執行以下任意一項：

- 在每個可用區域建立 NAT 閘道，將您的用戶端分配至這些區域。

- 在公有子網路中建立額外的 NAT 閘道，將您的用戶端分割到多個私有子網路中，並且每個都具有連至不同 NAT 閘道的路由。
- 限制您用戶端可連線到目標的建立連線數。
- 使用 CloudWatch 中的 `IdleTimeoutCount` 指標來監控閒置連線的增量。關閉閒置連線已釋出容量。
- 建立具有多個 IP 位址的 NAT 閘道，或將次要 IP 位址新增至現有的 NAT 閘道。每個新 IPv4 地址可支援最多 55,000 個並行連線。如需詳細資訊，請參閱 建立 NAT 閘道 或 編輯次要 IP 地址關聯 。

NAT 閘道的定價

當您佈建 NAT 閘道時，需支付 NAT 閘道可用時數及其處理每 GB 資料的費用。如需詳細資訊，請參閱 Amazon VPC 定價。

下列策略可協助您降低 NAT 閘道的資料傳輸費用：

- 如果您的 AWS 資源跨可用區域傳送或接收大量流量，請確定資源與 NAT 閘道位於相同的可用區域。或者，您也可以在每個可用區域中建立包含資源的 NAT 閘道。
- 如果大多數透過 NAT 閘道的流量是針對支援介面端點或閘道端點 AWS 的服務，請考慮為這些服務建立介面端點或閘道端點。如需有關潛在成本節省的詳細資訊，請參閱 AWS PrivateLink 定價。

NAT 執行個體

NAT 執行個體提供網路位址轉譯 (NAT)。若您使用 NAT 執行個體，即可允許私有子網路中的資源與虛擬私有雲端 (VPC) 外部的目的地通訊，例如與網際網路或內部部署網路通訊。私有子網路中的資源可以啟動流向網際網路的傳出 IPv4 流量，但無法接收在網際網路上啟動的傳入流量。

> **Important**
>
> NAT AMI 建立在最新版本的 Amazon Linux AMI, 2018.03 上，該版本已於 2020 年 12 月 31 日終止標準支援，並於 2023 年 12 月 31 日結束維護支援。如需詳細資訊，請參閱下列部落格文章：Amazon Linux AMI end of life。
> 如果您使用現有的 NAT AMI， AWS 建議您遷移到 NAT 閘道。NAT 閘道可提升可用性，提高頻寬並可減輕管理負擔。如需詳細資訊，請參閱比較 NAT 執行個體和 NAT 閘道。
> 如果與 NAT 閘道相比，NAT 執行個體更符合您的使用案例，您可以從 the section called “3. 建立 NAT AMI” 中所述的當前版本的 Amazon Linux 建立自己的 NAT AMI。

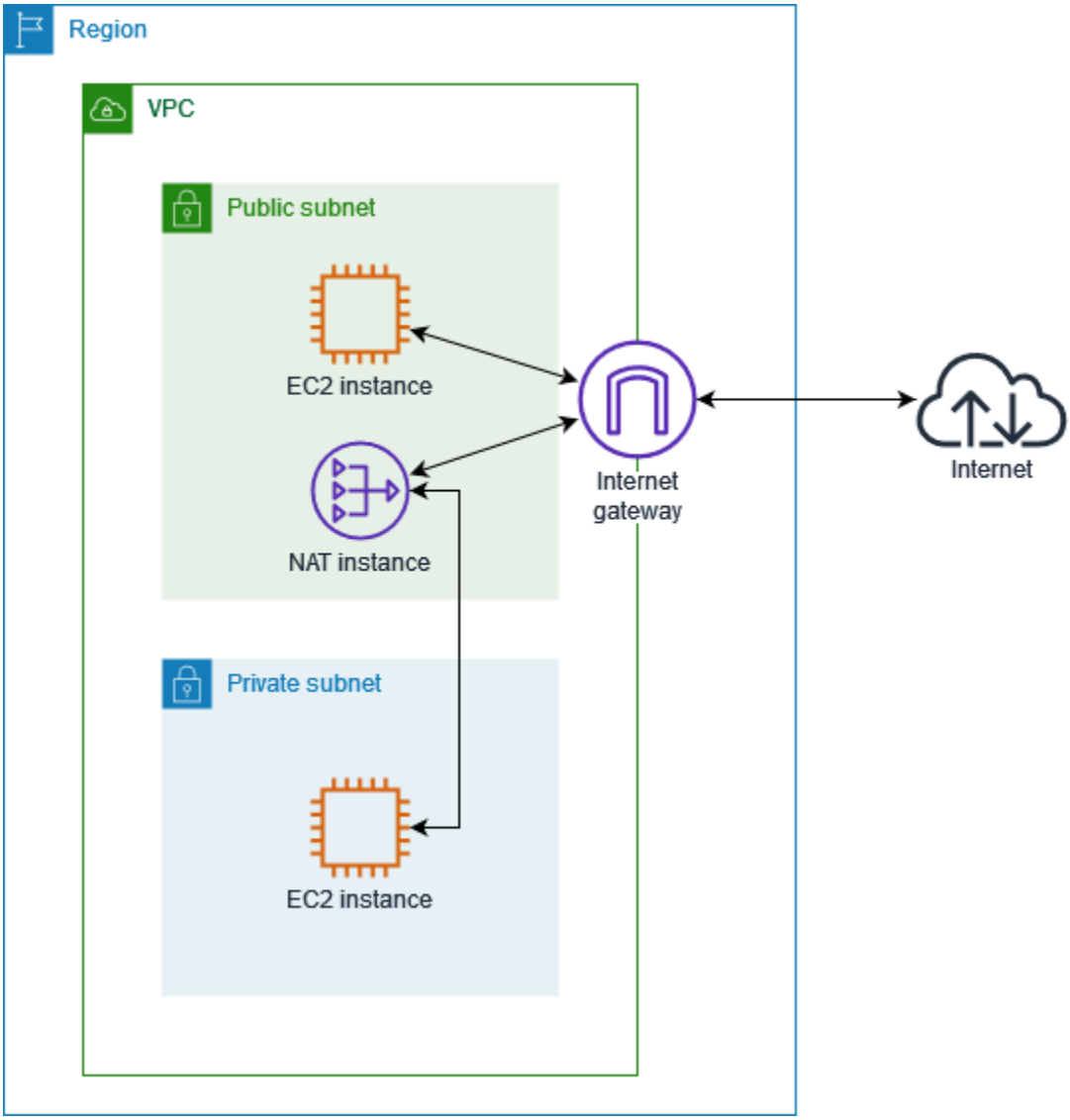
目錄

- NAT 執行個體基本概念
- 啟用私有資源以在 VPC 外部通訊

NAT 執行個體基本概念

下圖說明 NAT 執行個體基本概念。路由表與私有子網路相關聯，將網際網路流量從私有子網路的執行個體傳送至公有子網路的 NAT 執行個體。NAT 執行個體之後會將流量傳送至網際網路閘道。流量歸屬於 NAT 執行個體的公有 IP 地址。NAT 執行個體指定高連接埠號碼用於回應，如果傳回回應，NAT 執行個體會根據回應的連接埠號碼將它傳送到私有子網路的執行個體。

NAT 執行個體必須具有網際網路存取權，因此其必須位於公有子網路 (即具有路由表且具有通往網際網路閘道的子網路) 中，且必須具有公有 IP 地址或彈性 IP 地址。



若要開始使用 NAT 執行個體，請先建立 NAT AMI，再為 NAT 執行個體建立安全群組，然後在 VPC 中啟動 NAT 執行個體。

您的 NAT 執行個體配額取決於該區域的執行個體配額。如需詳細資訊，請參閱《AWS 一般參考》中的 Amazon EC2 Service Quotas。

啟用私有資源以在 VPC 外部通訊

本節說明如何建立和使用 NAT 執行個體，以啟用私有子網路中的資源，以在虛擬私有雲端外部進行通訊。

任務

- 1. 為 NAT 執行個體建立 VPC
- 2. 為 NAT 執行個體建立安全群組
- 3. 建立 NAT AMI
- 4. 啟動 NAT 執行個體
- 5. 停用來源/目標檢查
- 6. 更新路由表
- 7. 測試 NAT 執行個體

1. 為 NAT 執行個體建立 VPC

按照以下程序建立包含公有子網路和私有子網路的 VPC。

若要建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇建立 VPC。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 針對自動產生名稱標籤，輸入 VPC 的名稱。
5. 若要設定子網路，請執行下列動作：
    a. 對於 Number of Availability Zones (可用區域數量)，請根據您的需求選擇 1 或 2。
    b. 針對 Number of public subnets (公用子網路數量)，請確定每個可用區域有一個公用子網路。
    c. 針對 Number of private subnets (私有子網路數量)，請確定每個可用區域有一個私有子網路。

6. 選擇建立 VPC。

2. 為 NAT 執行個體建立安全群組

按照下表所述的規則建立安全群組。這些規則可讓 NAT 執行個體接收從私有子網路中執行個體流向網際網路的流量，以及來自您網路的 SSH 流量。NAT 執行個體也可以傳送流量到網際網路，讓私有子網路中的執行個體能取得軟體更新。

下列是建議的傳入規則。

來源	通訊協定	連接埠範圍	評論
##### CIDR	TCP	80	允許來自私有子網路伺服器的傳入 HTTP 流量
##### CIDR	TCP	443	允許來自私有子網路伺服器的傳入 HTTPS 流量
###### IP ####	TCP	22	允許傳入 SSH 從您的網路存取 NAT 執行個體 (透過網際網路閘道)

下列是建議的傳出規則。

目標	通訊協定	連接埠範圍	評論
0.0.0.0/0	TCP	80	允許傳出 HTTP 存取網際網路。
0.0.0.0/0	TCP	443	允許傳出 HTTPS 存取網際網路。

建立安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組。
3. 選擇 Create Security Group (建立安全群組)。
4. 輸入安全群組的名稱和說明。
5. 在 VPC 欄位中選取 NAT 執行個體的 VPC ID。

6. 在傳入規則下新增傳入流量的規則，如下所示：

   a. 選擇新增規則。在類型欄位中選擇 HTTP，然後在來源欄位中輸入私有子網路的 IP 地址範圍。

   b. 選擇新增規則。在類型欄位中選擇 HTTPS，然後在來源欄位中輸入私有子網路的 IP 地址範圍。

   c. 選擇新增規則。在類型欄位中選擇 SSH，然後在來源欄位中輸入網路的 IP 地址範圍。

7. 在傳出規則下新增傳出流量的規則，如下所示：

   a. 選擇新增規則。在類型欄位中選擇 HTTP，然後在目的地欄位中輸入 0.0.0.0/0。

   b. 選擇新增規則。在類型欄位中選擇 HTTPS，然後在目的地欄位中輸入 0.0.0.0/0。

8. 選擇 Create Security Group (建立安全群組)。

如需詳細資訊，請參閱Security groups (安全群組)。

3. 建立 NAT AMI

將 NAT AMI 設定為在 EC2 執行個體上執行 NAT。您必須先建立 NAT AMI，然後才能使用 NAT AMI 啟動 NAT 執行個體。

如果您計劃將 Amazon Linux 以外的作業系統用於 NAT AMI，則請參閱相應作業系統的說明文件，從中了解如何設定 NAT。請務必儲存這些設定，以便這些設定在執行個體重新啟動後仍然存在。

為 Amazon Linux 建立一個 NAT AMI

1. 啟動執行 AL2023 或 Amazon Linux 2 的 EC2 執行個體。請務必指定您為 NAT 執行個體建立的安全群組。
2. 連線到執行個體，並在執行個體上執行下列命令以啟用 iptables。

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. 在執行個體上執行下列操作以啟用 IP 轉送，以便在重新開機後持續進行：

   a. 使用 nano 或 vim 等文字編輯器，建立以下組態檔案：`/etc/sysctl.d/custom-ip-forwarding.conf`。

   b. 將以下行新增至組態檔案。

```
net.ipv4.ip_forward=1
```

c. 儲存組態檔案並關閉文字編輯器。

d. 執行以下命令，套用組態檔案。

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. 在執行個體上執行以下命令，並記下主要網路介面的名稱。下一個步驟您將需要這項資訊。

```
netstat -i
```

在下面的範例輸出中，docker0 是由 Docker 建立的網絡介面，eth0 是主要網路介面，lo 是迴路介面。

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

在下列範例輸出中，主要網路介面為 enX0。

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

在下列範例輸出中，主要網路介面為 ens5。

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. 在執行個體上執行下列命令以設定 NAT。如果主要網路介面不是 eth0，則使用您在上一個步驟中記下的主要網路介面來取代 *eth0*。

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. 從 EC2 執行個體建立 NAT AMI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的從執行個體建立 Linux AMI。

4. 啟動 NAT 執行個體

按照下列步驟操作，透過您建立的 VPC、安全群組和 NAT AMI 來啟動 NAT 執行個體。

啟動 NAT 執行個體

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在儀表板上，選擇啟動執行個體。
3. 在名稱欄位中輸入 NAT 執行個體名稱。
4. 在應用程式和作業系統映像欄位中，選取 NAT AMI (依序選擇瀏覽更多 AMI、我的 AMI)。
5. 在執行個體類型欄位中，選擇提供 NAT 執行個體所需運算、記憶體和儲存資源的執行個體類型。
6. 對於金鑰對，請選取現有的金鑰對或選擇建立新的金鑰對。
7. 針對 Network settings (網路設定)，執行下列操作：
   a. 選擇編輯。
   b. 在 VPC 欄位選擇您建立的 VPC。
   c. 對於子網路，請選擇先前建立的公有子網路。
   d. 在 Auto-assign public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。此外，也可在啟動 NAT 執行個體之後，配置彈性 IP 地址並將其指派給 NAT 執行個體。
   e. 對於防火牆，請選擇選取現有的安全群組，然後選擇先前建立的安全群組。
8. 選擇啟動執行個體。選擇執行個體 ID 以開啟執行個體詳細資訊頁面。等待執行個體狀態變更為執行中，並等待狀態檢查成功。
9. 停用 NAT 執行個體的來源/目的地檢查 (請參閱 5. 停用來源/目標檢查)。
10. 更新路由表以將流量傳送至 NAT 執行個體 (請參閱 6. 更新路由表)。

5. 停用來源/目標檢查

每個 EC2 執行個體預設都會執行來源/目標檢查。這表示執行個體必須是其傳送或接收流量的來源或目標。但當它本身不是來源或目標時，NAT 執行個體必須能夠傳送並接收流量。因此，您必須停用 NAT 執行個體的來源/目標檢查。

停用來源/目的地檢查

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選取 NAT 執行個體。
4. 選擇動作、聯網、變更來源/目的地檢查。
5. 在來源/目的地檢查欄位中選取停止。
6. 選擇 Save (儲存)。
7. 如果 NAT 執行個體具有次要網路介面，請從 Networking (聯網) 索引標籤的 Network interfaces (網路介面) 對其進行選擇。選擇界面 ID 以移至網路界面頁面。選擇 Actions (動作)、Change source/dest. check (變更來源/目標檢查)，清除 Enable (啟用)，選擇 Save (儲存)。

6. 更新路由表

私有子網路的路由表必須具有路由，能將網際網路的流量傳送至 NAT 執行個體。

更新路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選取私有子網路的路由表。
4. 在路由標籤上，選擇編輯路由，然後選擇新增路由。
5. 在目的地欄位中輸入 0.0.0.0/0，在目標欄位中輸入 NAT 執行個體的執行個體 ID。
6. 選擇儲存變更。

如需詳細資訊，請參閱設定路由表。

7. 測試 NAT 執行個體

在啟動 NAT 執行個體並完成上述設定步驟後，您就可以執行測試，檢查私有子網路中的執行個體是否可以將 NAT 執行個體作為堡壘伺服器使用，透過 NAT 執行個體存取網際網路。

任務

- 步驟 1：更新 NAT 執行個體安全群組
- 步驟 2：在私有子網路中啟動測試執行個體
- 步驟 3：Ping 到啟用 ICMP 的網站

- 步驟 4：清理

步驟 1：更新 NAT 執行個體安全群組

若要允許私有子網路中的執行個體傳送 ping 流量至 NAT 執行個體，請新增規則以允許傳入和傳出 ICMP 流量。若要允許 NAT 執行個體做為堡壘伺服器，請新增規則以允許傳出 SSH 流量至私有子網路。

更新您的 NAT 執行個體安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組。
3. 選取與 NAT 執行個體關聯之安全群組的核取方塊。
4. 在傳入規則索引標籤上，選擇編輯傳入規則。
5. 選擇 Add rule (新增規則)。選擇 Type (類型) 的 All ICMP - IPv4 (所有 ICMP - IPv4)。在來源欄位中選擇自訂，然後輸入私有子網路的 IP 地址範圍。選擇儲存規則。
6. 在傳出規則標籤上，選擇編輯傳出規則。
7. 選擇 Add rule (新增規則)。選擇 Type (類型) 的 SSH。在目的地欄位中選擇自訂，然後輸入私有子網路的 IP 地址範圍。
8. 選擇 Add rule (新增規則)。選擇 Type (類型) 的 All ICMP - IPv4 (所有 ICMP - IPv4)。對於 Destination (目的地) 選擇 Anywhere - IPv4 (隨處 - IPv4)。選擇儲存規則。

步驟 2：在私有子網路中啟動測試執行個體

在您的私有子網路中啟動執行個體。您必須允許來自 NAT 執行個體的 SSH 存取，而且必須使用您用於 NAT 執行個體的相同金鑰對。

在私有子網路中啟動測試執行個體

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在儀表板上，選擇啟動執行個體。
3. 選取您的私有子網路。
4. 請勿將公有 IP 地址指派給此執行個體。
5. 務必確保此執行個體的安全群組允許來自 NAT 執行個體或公有子網路 IP 地址範圍的傳入 SSH 存取，以及傳出 ICMP 流量。
6. 選取用於 NAT 執行個體的相同金鑰對。

步驟 3：Ping 到啟用 ICMP 的網站

若要確認私有子網路中的執行個體是否可以使用 NAT 執行個體與網際網路通訊，請執行 ping 命令。

測試來自私有執行個體的網際網路連線

1. 從您的本機電腦設定 SSH 代理程式轉送，讓您可以使用 NAT 執行個體作為堡壘伺服器。

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   下載並安裝 Pageant (如果尚未安裝)。

   使用 PuTTYgen 轉換私有金鑰。

   Start Pageant，開啟任務列上 Pageant 圖示的內容選單（可能隱藏），然後選擇新增金鑰。選取您建立的 .ppk 檔案，如需要，則輸入密碼短語，然後選擇 Open (開啟)。
2. 從本機電腦連線到 NAT 執行個體。

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   使用 PuTTY 連線到 NAT 執行個體 針對 Auth (驗證)，您必須選取 Allow agent forwarding (允許代理程式轉送)，並將 Private key file for authentication (要驗證的私有金鑰檔案) 留空。
3. 在 NAT 執行個體中，執行 ping 命令，並指定啟用 ICMP 的網站。

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

   若要確認您的 NAT 執行個體可以存取網際網路，請確認您收到如下的輸出，然後按 Ctrl+C 以取消 ping 命令。否則，請確認 NAT 執行個體位於公有子網路中 (其路由表具有通往網際網路閘道的路由)。

   ```
   PING ietf.org (104.16.45.99) 56(84) bytes of data.
   64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
   ```

```
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
...
```

4. 從您的 NAT 執行個體，使用其私有 IP 地址連線到您私有子網路中的執行個體。

```
[ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
```

5. 從您的私有執行個體執行 ping 命令，測試能否連線到網際網路。

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

若要確認您的私有執行個體可以透過 NAT 執行個體存取網際網路，請確認您收到如下的輸出，然後按 Ctrl+C 以取消 ping 命令。

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

疑難排解

如果從私有子網路中的伺服器執行 ping 命令失敗，請使用下列步驟對問題進行故障診斷：

- 確認您是否已對啟用了 ICMP 的網站執行 Ping 動作。若未執行，伺服器則無法接收回覆封包。若要測試此作業，請從您電腦的命令列終端機執行相同的 ping 命令。
- 確認 NAT 執行個體的安全群組是否允許來自您私有子網路的傳入 ICMP 流量。如不允許，您的 NAT 執行個體無法接收私有執行個體的 ping 命令。
- 確認您是否已停用 NAT 執行個體的來源/目的地檢查。如需詳細資訊，請參閱5. 停用來源/目標檢查。
- 確認您是否已正確設定路由表。如需詳細資訊，請參閱6. 更新路由表。

步驟 4：清理

如果私有子網路中不再需要測試伺服器，請終止該執行個體，這樣您就不再需要支付該執行個體的費用。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的終止您的執行個體。

如果您不再需要 NAT 執行個體，您可以停止或終止該執行個體，這樣您就不再需要支付該執行個體的費用。如果您已建立 NAT AMI，則可以在需要時建立新的 NAT 執行個體。

比較 NAT 執行個體和 NAT 閘道

下列是 NAT 閘道和 NAT 執行個體之間差異的高階摘要。我們建議您使用 NAT 閘道，因為它們提供更好的可用性和頻寬，而且您的管理負擔較輕。

屬性	NAT 閘道	NAT 執行個體
可用性	高可用性。每個可用區域中的 NAT 閘道都使用備援來實作。在每個可用區域中建立 NAT 閘道，可確保架構獨立於區域之外。	使用指令碼管理執行個體間的容錯移轉。
頻寬	最高可擴展到 100 Gbps。	取決於執行個體類型的頻寬。
Maintenance (維護)	受管者 AWS。您不需要執行任何維護。	由您管理，例如為執行個體安裝軟體更新或作業系統修補程式。
效能	軟體已最佳化，以便處理 NAT 流量。	設定執行 NAT 的一般 AMI。
費用	費用取決於您使用的 NAT 閘道數目、使用持續時間以及您透過 NAT 閘道傳送的資料量。	費用取決於您使用的 NAT 執行個體數目、使用持續時間以及執行個體類型和大小。
類型和大小	統一方案；您不需要決定類型或大小。	根據您的預測工作負載，選擇適當的執行個體類型和大小。
公有 IP 地址	在建立時選擇彈性 IP 地址，以便與公有 NAT 閘道建立關聯。	為 NAT 執行個體使用彈性 IP 地址或公有 IP 地址。您可以隨時透過將新的彈性 IP 地址與執行個體建立關聯，以變更公有 IP 地址。
私有 IP 地址	當您建立閘道時，自動從子網的 IP 地址範圍內選取。	當您啟動執行個體時，從子網 IP 地址範圍內指派特定的私有 IP 地址。

屬性	NAT 閘道	NAT 執行個體
安全群組	您無法將安全群組與 NAT 閘道建立關聯，但可以將安全群組與 NAT 閘道後的資源建立關聯，以控制傳入和傳出流量。	與您的 NAT 執行個體和 NAT 執行個體後的資源建立關聯，以控制傳入和傳出流量。
網路 ACL	使用網路 ACL 來控制進出 NAT 閘道所在子網的流量。	使用網路 ACL 來控制進出 NAT 執行個體所在子網的流量。
流程日誌	使用流程日誌來擷取流量。	使用流程日誌來擷取流量。
網路埠轉送	不支援.	手動自訂組態以支援網路埠轉送。
堡壘伺服器	不支援.	做為堡壘伺服器使用。
流量指標	檢視 NAT 閘道的 CloudWatch 指標。	檢視執行個體的 CloudWatch 指標。
逾時行為	如果連線逾時，NAT 閘道會對 NAT 閘道後的任何資源傳回 RST 封包來嘗試繼續連線 (不會傳送 FIN 封包)。	如果連線逾時，NAT 執行個體會對 NAT 執行個體後的資源傳送 FIN 封包來關閉連線。
IP 分段	支援轉送 UDP 通訊協定的 IP 分段封包。 不支援 TCP 和 ICMP 通訊協定的分段。這些通訊協定的分段封包會遭刪除。	支援 UDP、TCP 和 ICMP 通訊協定 IP 分段封包的重組。

從 NAT 執行個體遷移至 NAT 閘道

若您已在使用 NAT 執行個體，我們建議您使用 NAT 閘道予以取代。您可以在相同子網中建立 NAT 閘道作為您的 NAT 執行個體，然後使用指向 NAT 閘道的路由取代您路由表中指向 NAT 執行個體的現有路由。若要針對 NAT 閘道使用您目前用於 NAT 執行個體的相同彈性 IP 地址，您必須先取消與 NAT 執行個體之彈性 IP 地址的關聯，然後在建立閘道時將其與您的 NAT 閘道建立關聯。

若您將您的路由從 NAT 執行個體變更為 NAT 閘道，或者您取消彈性 IP 地址與您 NAT 執行個體的關聯，則任何目前連線都會遭到卸除，需要重新建立。請確認您沒有任何執行中的關鍵任務 (或其他透過 NAT 執行個體操作的任務)。

將彈性 IP 地址與 VPC 中的資源建立關聯

彈性 IP 位址是一個靜態的公有 IPv4 地址，專為雲端運算的動態特性而設計。此功能可讓您將彈性 IP 地址與您 AWS 帳戶中任何虛擬私有雲端 (VPC) 內的任何執行個體或網路介面建立關聯。透過使用彈性 IP 地址，您可以釋放許多好處，簡化雲端基礎設施的管理和彈性。

彈性 IP 位址的主要優點之一是能夠遮罩執行個體的故障。如果執行個體發生非預期的中斷或需要取代，您可以將相關聯的彈性 IP 位址重新映射到 VPC 中的另一個執行個體。此容錯移轉程序可確保您的應用程式和服務維持一致且可靠的公有端點，將停機時間降至最低，並提供卓越的使用者體驗。

此外，彈性 IP 位址可讓您靈活管理網路資源。您可以視需要以程式設計方式建立和取消這些地址的關聯，讓您根據不斷變化的業務需求，將流量導向至不同的執行個體。這種公有 IP 位址的動態配置可讓您適應不斷變化的需求、擴展基礎設施，以及實作創新架構，而不受靜態 IP 指派的限制。

除了用於執行個體容錯移轉之外，彈性 IP 位址也可以做為雲端資源的穩定識別碼。這在設定外部服務時很有幫助，例如 DNS AWS記錄或防火牆規則，以與您託管的應用程式通訊。透過建立持久性公有 IP 位址的關聯，您可以為聯網組態做好準備，並避免在替換或擴展基礎執行個體時更新外部參考。

目錄

- 彈性 IP 位址概念和規則
- 開始使用彈性 IP 位址

彈性 IP 位址概念和規則

若要使用彈性 IP 位址，請先分配給帳戶使用。然後，您可以將其與 VPC 中的執行個體或網路介面相關聯。您的彈性 IP 地址仍會配置給 AWS 您的帳戶，直到您明確釋出為止。

彈性 IP 地址是網路界面的屬性。您可以透過更新連接至執行個體的網路界面，將彈性 IP 地址與執行個體建立關聯。將彈性 IP 位址與網路介面 (而不是直接與執行個體) 建立關聯的好處在於只要一個步驟，即可將網路介面的所有屬性從一個執行個體移至另一個執行個體。如需詳細，請參閱《Amazon EC2 使用者指南》中的彈性網絡介面。

適用的規定如下：

- 彈性 IP 位址可以一次與單一執行個體或網路介面相關聯。
- 您可以將彈性 IP 位址從一個執行個體或網路介面移動到另一個執行個體或網路介面。
- 如果您將彈性 IP 位址與執行個體的主要網路介面建立關聯，即會向公有 IP 位址集區釋出其目前的公有 IPv4 位址 (如果有的話)。如果您取消彈性 IP 位址的關聯，則會在幾分鐘內自動將新的公有 IPv4 位址指派給主要網路介面。如已將第二個網路界面連接至您的執行個體，則不適用。
- 您只能使用五個彈性 IP 位址。為了協助保存這些位址，您可以使用 NAT 裝置。如需更多詳細資訊，請參閱 使用 NAT 裝置連線至網際網路或其他網路。
- 不支援 IPv6 的彈性 IP 位址。
- 您可以標記配置用於 VPC 的彈性 IP 位址，但不支援成本配置標籤。如果您復原彈性 IP 地址，不會復原標籤。
- 當安全群組和網路 ACL 允許來自來源 IP 地址的流量時，您可以從網際網路存取彈性 IP 地址。從 VPC 內回到網際網路的回覆流量需有網際網路閘道。如需詳細資訊，請參閱Security groups (安全群組)及網路 ACL。
- 您可以針對彈性 IP 地址使用下列任一選項：
  - 讓 Amazon 提供彈性 IP 地址。當您選取此選項時，您可以將彈性 IP 地址與網路邊界群組建立關聯。這是我們公告 CIDR 區塊的位置。設定網路邊界群組會將 CIDR 區塊限制在此群組。
  - 使用您自己的 IP 地址。如需自攜 IP 位址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的自攜 IP 位址 (BYOIP)。
- 公有 IPv4 地址支援成本分配標籤。如果您將標籤套用至彈性 IP 位址，則可以使用這些標籤來追蹤 AWS Cost Explorer中的公有 IPv4 地址成本。

  您必須先啟用標籤，才能使用標籤做為成本分配標籤。如需詳細資訊，請參閱《AWS Billing 使用者指南》中的啟用使用者定義的成本配置標籤。請注意，在您建立使用者定義的標籤並套用至資源之後，標籤索引鍵最多可能需要 24 小時才會出現在成本分配標籤頁面上供您啟用。

  成本分配標籤啟用後...
  - 對於與彈性網路介面相關聯的所有公有 IPv4 地址 (包括指派給 EC2 執行個體和彈性 IP 位址的公有 IPv4 地址)，您可以選擇用量類型 > PublicIPv4InUseAddress (Hrs)，在 Cost Explorer 中檢視公有 IPv4 地址的相關成本。
  - 如果已標記的彈性 IP 位址未與 ENI 相關聯，或與已停止的資源相關聯 (例如已停止的 EC2 執行個體)，則視為閒置 IPv4 地址。您可以在 Cost Explorer 中選擇用量類型 > PublicIPv4IdleAddress (Hrs)，檢視與閒置 IPv4 地址相關聯的成本。

  如需有關 Cost Explorer 的更多資訊，請參閱《AWS Billing 使用者指南》的使用 AWS Cost Explorer 分析您的成本。

彈性 IP 地址為區域性。如需有關使用 Global Accelerator 佈建全域 IP 地址的詳細資訊，請參閱 AWS Global Accelerator 開發人員指南中的使用全域靜態 IP 地址而非區域靜態 IP 地址。

如需彈性 IP 位址定價的詳細資訊，請參閱 Amazon VPC 定價中的公有 IPv4 地址。

開始使用彈性 IP 位址

下列各節說明如何開始使用彈性 IP 位址。

任務

- 1. 配置彈性 IP 位址
- 2. 建立彈性 IP 地址的關聯
- 3. 取消彈性 IP 地址的關聯
- 4. 轉移彈性 IP 地址
- 5. 釋出彈性 IP 位址
- 6. 復原彈性 IP 地址
- 命令列概觀

1. 配置彈性 IP 位址

在使用彈性 IP 之前，您必須配置一個用於 VPC 中的彈性 IP。

配置彈性 IP 位址

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選擇 Allocate Elastic IP address (配置彈性 IP 位址)。
4. (選用) 配置彈性 IP 地址 (EIP) 時，您可以選擇要配置 EIP 的網路邊界群組。網路邊界群組是可用區域 (AZs)、本機區域或 Wavelength 區域的集合，可從中 AWS 公告公有 IP 地址。Local Zones 和 Wavelength Zones 的網路邊界群組可能與區域中AZs 不同，以確保 AWS 網路和存取這些區域中資源的客戶之間的最低延遲或實體距離。

> **Important**
>
> 您必須在與 EIP 相關聯的 AWS 資源相同的網路邊界群組中配置 EIP。一個網路邊界群組中的 EIP 只能在該網路邊界群組中的區域中進行公告，而不能在其他網路邊界群組所代表的任何其他區域中進行公告。

如果您已啟用 Local Zones 或 Wavelength Zones (如需詳細資訊，請參閱啟用 Local Zone 或啟用 Wavelength Zones)，您可以為 AZ、Local Zones 或 Wavelength Zones 選擇網路邊界群組。仔細選擇網路邊界群組，因為 EIP 與其相關聯的 AWS 資源必須位於相同的網路邊界群組中。您可以使用 EC2 主控台檢視可用區域、Local Zones 或 Wavelength Zones 所在的網路邊界群組 (請參閱 Local Zones)。一般而言，區域中的所有可用區域屬於相同的網路邊界群組，而 Local Zones 或 Wavelength Zones 則屬於其各自的網路邊界群組。

如果您沒有啟用 Local Zones 或 Wavelength Zones，則當您配置 EIP 時，代表該區域所有 AZ 的網路邊界群組 (例如 `us-west-2`) 會為您預先定義，且您無法予以變更。這表示您配置給此網路邊界群組的 EIP 會在您所在區域的所有 AZ 中進行公告。

5. (僅限 VPC 範圍) 對於公用 IPv4 地址集區，請選擇下列其中一項：
   - Amazon 的 IP 地址集區 — 若您要從 Amazon IP 地址集區配置一個 IPv4 地址。
   - 我的公有 IPv4 地址集區 - 如果您想要從已帶到 AWS 帳戶的 IP 地址集區配置 IPv4 地址。如果您沒有任何 IP 地址集區，則會停用此選項。
   - Customer owned pool of IPv4 addresses (客戶擁有的 IPv4 地址集區) — 若您要從內部部署網路建立的集區配置 IPv4 地址，以搭配使用 Outpost。僅當您有 Outpost 時才能使用此選項。
6. (選用) 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：
   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值欄位中，輸入金鑰值。

   【移除標籤】 選擇標籤索引鍵和值右側的移除。
7. 選擇 Allocate (配置)。

2. 建立彈性 IP 地址的關聯

您可以將彈性 IP 與 VPC 中正在執行的執行個體或網路介面相關聯。

在您將彈性 IP 位址與您執行個體建立關聯後，如果啟用 DNS 主機名稱，執行個體就會收到公用 DNS 主機名稱。如需更多詳細資訊，請參閱 VPC 的 DNS 屬性。

將彈性 IP 位址與執行個體或網路介面建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選取配置用於 VPC 的彈性 IP 位址 (Scope (範圍) 欄有 vpc 值)，依序選擇 Actions (動作)、Associate Elastic IP address (與彈性 IP 位址建立關聯)。
4. 選擇 Instance (執行個體) 或 Network interface (網路界面)，然後選取執行個體或網路界面 ID。選取要與彈性 IP 地址建立關聯的私有 IP 地址。選擇 Associate (關聯)。

3. 取消彈性 IP 地址的關聯

若要變更與彈性 IP 位址相關聯的資源，您必須先將其與目前關聯的資源取消關聯。

取消與彈性 IP 地址的關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選取彈性 IP 位址，接著選擇 Actions (動作)、Disassociate Elastic IP address (解除彈性 IP 位址的關聯)。
4. 出現提示時，請選擇 Disassociate (取消關聯)。

4. 轉移彈性 IP 地址

本節旨在說明如何將彈性 IP 地址從一個 AWS 帳戶 轉移到另一個。轉移彈性 IP 地址適用於下列情況：

- 組織重組 – 使用彈性 IP 地址傳輸，快速將工作負載從一個移動 AWS 帳戶 到另一個。您無須等待新的彈性 IP 地址列在安全群組和 NACL 的允許清單中。
- 集中式安全管理 – 使用集中式 AWS 安全帳戶來追蹤和轉移已經過安全合規審核的彈性 IP 地址。

- 災難復原 – 發生緊急事故時，使用彈性 IP 地址轉移可快速重新對應 IP，以處理公開網站的工作負載。

轉移彈性 IP 位址無需付費。

任務

- 啟用彈性 IP 位址轉移
- 停用彈性 IP 地址轉移
- 接受轉移後的彈性 IP 地址

啟用彈性 IP 位址轉移

本節旨在說明如何接受轉移後的彈性 IP 位址。請注意下列與啟用彈性 IP 位址轉移的相關限制：

- 您可以將彈性 IP 地址從任何 AWS 帳戶（來源帳戶）轉移到相同 AWS 區域中的任何其他 AWS 帳戶（轉移帳戶）。
- 當您轉移彈性 IP 位址時， AWS 帳戶之間會發生兩步驟交握。來源帳戶開始轉移時，轉移帳戶有七天時間可以接受彈性 IP 位址轉移。在這七天內，來源帳戶可以檢視待處理的轉移（例如，在 AWS 主控台中或使用 describe-address-transfers AWS CLI 命令）。七天後轉移將到期，屆時彈性 IP 位址的擁有權會回到來源帳戶。
- 接受的轉移會在接受轉移後 14 天內顯示給來源帳戶（例如，在 AWS 主控台中或使用 describe-address-transfers AWS CLI 命令）。
- AWS 不會通知轉移帳戶有關待定的彈性 IP 地址轉移請求。來源帳戶的擁有者必須通知轉移帳戶的擁有者，有必須接受的彈性 IP 位址轉移的請求。
- 轉移完成時，會重設與要轉移之彈性 IP 位址相關的所有標籤。
- 您無法從公有 IPv4 地址集區中配置的彈性 IP 地址傳輸到 AWS 帳戶 – 通常稱為使用自有 IP (BYOIP) 地址集區。
- 如果您嘗試轉移具有與其相關聯之反向 DNS 記錄的彈性 IP 地址，您可以開始轉移程序。不過，在移除相關聯的 DNS 記錄之前，轉移帳戶無法接受轉移。
- 如果您已啟用並設定 AWS Outposts，您可能已從客戶擁有的 IP 地址集區 (CoIP) 配置彈性 IP 地址。您無法轉移從 CoIP 配置的彈性 IP 位址。不過，您可以使用 與其他帳戶 AWS RAM 共用 CoIP。如需詳細資訊，請參閱AWS Outposts 使用者指南中的客戶擁有的 IP 位址。
- 您可使用 Amazon VPC IPAM 來追蹤彈性 IP 位址在 AWS Organizations組織中的帳戶之間轉移的情況。如需詳細資訊，請參閱 View IP address history (檢視 IP 位址歷程記錄)。如果將彈性 IP 位址轉移至組織外部的 AWS 帳戶 ，就會失去彈性 IP 位址的 IPAM 稽核歷史記錄。

這些步驟必須由來源帳戶完成。

啟用彈性 IP 位址轉移

1. 請確定您使用的是來源 AWS 帳戶。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
4. 選取要啟用轉移的一或多個彈性 IP 位址，然後選擇 Actions (動作)、Enable transfer (啟用轉移)。
5. 如果您要轉移多個彈性 IP 地址，您會看到轉移類型選項。請選擇下列其中一個選項：
   - 如果您要將彈性 IP 地址轉移到單一帳戶，請選擇單一 AWS 帳戶。
   - 如果您要將彈性 IP 地址轉移到多個帳戶，請選擇多個 AWS 帳戶。
6. 在 Transfer account ID (轉移帳戶 ID) 底下，輸入您要將彈性 IP 位址轉移至哪個 AWS 帳戶 ID。
7. 在文字方塊中輸入 **`enable`**，以便確認轉移。
8. 選擇提交。
9. 若要接受轉移，請參閱接受轉移後的彈性 IP 地址。若要停用轉移，請參閱 停用彈性 IP 地址轉移。

停用彈性 IP 地址轉移

本節旨在說明如何在啟用轉移後停用彈性 IP 轉移。

這些步驟必須由啟用轉移的來源帳戶完成。

停用彈性 IP 位址轉移

1. 請確定您使用的是來源 AWS 帳戶。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
4. 在彈性 IP 的資源清單中，確保您已啟用顯示 Transfer status (轉移狀態) 欄位的屬性。
5. 選取 Transfer status (轉移狀態) 為 Pending (待定) 的一或多個彈性 IP 位址，然後選擇 Actions (動作)、Disable transfer (停用轉移)。
6. 在文字方塊中輸入 **`disable`**，以便進行確認。
7. 選擇提交。

接受轉移後的彈性 IP 地址

本節旨在說明如何接受轉移後的彈性 IP 位址。

當您轉移彈性 IP 位址時， AWS 帳戶之間會發生兩步驟交握。來源帳戶開始轉移時，轉移帳戶有七天時間可以接受彈性 IP 位址轉移。在這七天內，來源帳戶可以檢視待處理的轉移（例如，在 AWS 主控台中或使用 describe-address-transfers AWS CLI 命令）。七天後轉移將到期，屆時彈性 IP 位址的擁有權會回到來源帳戶。

接受轉移時，請注意下列可能發生的異常情況，以及如何解決這些異常問題：

- AddressLimitExceeded：如果轉移帳戶超過彈性 IP 位址配額，則來源帳戶仍可啟用彈性 IP 位址轉移，但是如果轉移帳戶嘗試接受轉移，就會發生此異常情況。根據預設，所有 AWS 帳戶每個區域限制為 5 個彈性 IP 地址。如需提高上限的說明，請參閱《Amazon EC2 使用者指南》中的彈性 IP 位址上限。
- InvalidTransfer.AddressCustomPtrSet：您嘗試傳輸的彈性 IP 地址設定為使用反向 DNS 查詢。來源帳戶可以啟用彈性 IP 地址的轉移。不過，當轉移帳戶嘗試接受轉移時，就會發生此例外狀況。若要解決這個問題，來源帳戶必須移除該彈性 IP 位址的 DNS 記錄。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的移除反向 DNS 記錄。
- InvalidTransfer.AddressAssociated：如果彈性 IP 位址與 ENI 或 EC2 執行個體有關，則來源帳戶仍可啟用該彈性 IP 位址的轉移，但是如果轉移帳戶嘗試接受轉移，就會發生此異常情況。若要解決這個問題，來源帳戶必須取消與該彈性 IP 位址的關聯。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的取消彈性 IP 位址的關聯。

如有任何其他異常情況，請聯絡 支援。

這些步驟必須由轉移帳戶完成。

接受彈性 IP 位址轉移

1. 確保您使用的是轉移帳戶。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
4. 選擇 Actions (動作)、Accept transfer (接受轉移)。
5. 當您接受轉移時，與該彈性 IP 位址有關的所有標籤都不會隨著該彈性 IP 位址轉移。如果您要為接受的彈性 IP 位址定義 Name (名稱) 標籤，請選取 Create a tag with a key of 'Name' and a value that you specify (建立索引鍵為 'Name' 並具有您指定值的標籤)。

6. 輸入您要轉移的彈性 IP 位址。
7. 如果您要接受多個轉移的彈性 IP 位址，請選擇 Add address (新增位址)，以輸入其他彈性 IP 位址。
8. 選擇提交。

5. 釋出彈性 IP 位址

如果您不再需要彈性 IP 位址，我們建議您將其釋出。配置用於 VPC 但未與執行個體相關聯的任何彈性 IP 位址都會產生費用。彈性 IP 位址不得與執行個體或網路介面相關聯。

釋出彈性 IP 地址

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選取要釋出的彈性 IP 位址，然後依序選擇 Actions (動作)、Release Elastic IP addresses (公佈彈性 IP 地址)。
4. 出現提示時，請選擇 Release (釋出)。

6. 復原彈性 IP 地址

如果您在釋出彈性 IP 地址後反悔，您或許能夠予以復原。如果彈性 IP 地址已配置給另一個 AWS 帳戶，或如果復原會導致您超過彈性 IP 地址配額，則無法復原彈性 IP 地址。

您可以使用 Amazon EC2 API 或命令列工具來復原彈性 IP 地址。

使用 復原彈性 IP 地址 AWS CLI

使用 allocate-address 命令，並使用 `--address` 參數來指定 IP 地址。

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

命令列概觀

您可以使用命令列或 API 執行這一小節所述的任務。如需命令列介面的詳細資訊與可用的 API 動作清單，請參閱使用 Amazon VPC。

接受彈性 IP 地址轉移

- accept-address-transfer (AWS CLI)

- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

配置彈性 IP 位址

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

建立彈性 IP 地址與執行個體或網路介面的關聯

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

說明彈性 IP 地址轉移

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

停用彈性 IP 地址轉移

- disable-address-transfer (AWS CLI)
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

取消彈性 IP 位址的關聯

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

啟用彈性 IP 地址轉移

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

釋出彈性 IP 位址

- release-address (AWS CLI)

- Remove-EC2Address (AWS Tools for Windows PowerShell)

為彈性 IP 地址套用標籤

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

檢視您的彈性 IP 地址

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

使用傳輸閘道將您的 VPC 連線至其他 VPC 和網路

您可以使用傳輸閘道來連線 Virtual Private Cloud (VPC) 和內部部署網路，它可充當中樞，在 VPC、VPN 連接和 Direct Connect 連接之間路由流量。

使用傳輸閘道的主要好處之一是能夠集中和簡化 VPC 與內部部署網路之間的連線管理。您可以使用傳輸閘道做為單一整合點，而不是設定多個 VPN 連線或 Direct Connect 連結，這有助於降低網路架構的整體複雜性和營運開銷。

使用傳輸閘道的費用是根據透過閘道傳輸的資料量來計算的。傳輸閘道進出資料的費用按每 GB 計算，傳輸閘道資源本身也有單獨的每小時費用。特定定價可能因 AWS 區域而異，可能會有所變更，因此請務必參閱目前的 AWS Transit Gateway 定價頁面以取得up-to-date。透過了解傳輸閘道的定價模式，您可以更好地規劃和預算與此 AWS 聯網服務相關的持續成本。這結合了營運效率和連線效益，使傳輸閘道成為希望建置可擴展且具成本效益混合雲端解決方案的組織的理想選擇。

下表說明了傳輸閘道的部分常見使用案例。如需每個使用案例的詳細資訊，請參閱《AWS Transit Gateway 使用者指南》中的傳輸閘道案例示例。

範例	用量
集中式路由器	將傳輸閘道設定為連接所有 VPCs、 AWS Direct Connect和 AWS Site-to-Site VPN 連線的集中式路由器。
隔離的 VPC	將傳輸閘道設定為多個隔離路由器。這就類似於使用多個傳輸閘道，但更具彈性，可讓路由和附件變更。

範例	用量
隔離 VPC 與共享服務	將傳輸閘道設定為使用共用服務的多個隔離路由器。這就類似於使用多個傳輸閘道，但更具彈性，可讓路由和附件變更。

如需詳細資訊，請參閱 AWS 傳輸閘道。

使用 AWS Virtual Private Network 將 VPC 連線至遠端網路

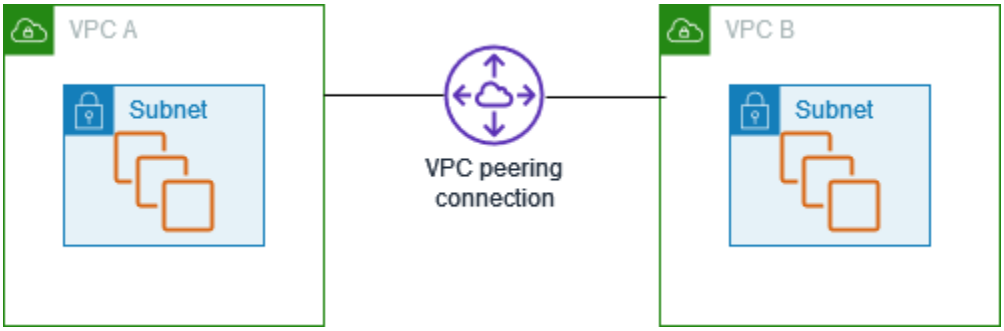
您可以使用下列 VPN 連線選項將您的 VPC 連線到遠端網路和使用者。

VPN 連線選項	描述
AWS Site-to-Site VPN	您可在您的 VPC 與您的遠端網路之間建立 IPsec VPN 連接。在 Site-to-Site VPN 連接的 AWS 端上，虛擬私有閘道或傳輸閘道會提供兩個 VPN 端點 (通道) 用於自動容錯移轉。您在 Site-to-Site VPN 連線的遠端配置您的客戶閘道裝置。如需詳細資訊，請參閱《AWS Site-to-Site VPN使用者指南》。
AWS Client VPN	AWS Client VPN 是以用戶端為基礎的受管 VPN 服務，能讓您安全地存取您的 AWS 資源或您的內部部署網路。您可以藉由 AWS Client VPN 來設定使用者可以連線的端點，以建立安全 TLS VPN 工作階段。如此可讓用戶端使用以 OpenVPN 為基礎的 VPN 用戶端，從任何位置存取 AWS 或內部部署中的資源。如需詳細資訊，請參閱 AWS Client VPN 管理員指南。
AWS VPN CloudHub	如有多個遠端網路 (例如多間分公司)，您可透過虛擬私有閘道建立多個 AWS Site-to-Site VPN 連線，讓這些網路能彼此通訊。如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的使用 VPN CloudHub 提供網站間的安全通訊。
第三方軟體 VPN 應用裝置	您可使用您 VPC 中執行第三方軟體 VPN 應用裝置的 Amazon EC2 執行個體，建立遠端網路的 VPN 連接。AWS 不提供或維護第三方軟體 VPN 應用裝置，但您可在合作夥伴和開源社群提供的產品中選擇。在 AWS Marketplace 中尋找第三方軟體 VPN 應用裝置。

您也可以使用 Direct Connect 建立遠端網路到您 VPC 的專用私有連線。您可結合此連線與 AWS Site-to-Site VPN，以建立 IPsec 加密的連線。如需詳細資訊，請參閱《Direct Connect 使用者指南》中的什麼是 Direct Connect？。

使用 VPC 對等互連來連線 VPC

VPC 互連連線是一種聯網功能，可在 AWS 基礎設施內的兩個虛擬私有雲端 (VPCs) 之間進行安全且直接的通訊。此私有連線可讓對等 VPC 中的資源彼此互動，彷彿它們屬於相同的網路，從而免去必須經過公有網際網路的需求。



建立 VPC 互連連線的程序會使用現有的 VPC 基礎設施來建立此連線，而不需要閘道 AWS Site-to-Site VPN或任何其他實體硬體。此設計可確保沒有單一故障點或頻寬瓶頸。

VPC 互連連線的主要優點之一是能夠跨不同 AWS 帳戶或甚至不同 AWS 區域連接 VPCs。這種靈活性可讓組織無縫整合其雲端資源，無論它們是否位於同一帳戶內，還是分散在多個帳戶和地理位置。連線的私有性質也可確保對等 VPCs 之間的所有資料流量都保留在 AWS 網路中，而不會周遊公有網際網路。

VPC 對等互連的使用案例範圍廣泛。組織可以使用此功能在應用程式的不同層（例如 Web 伺服器和資料庫伺服器）之間啟用安全通訊、協助在多個團隊或業務單位之間共用資源，甚至透過將內部部署網路連接到其 AWS VPCs 來啟用混合雲端架構。

VPC 互連連線是指兩個 VPC 之間的聯網連線，透過此機制，您可以私下在兩者間路由流量。對等 VPC 中的資源能彼此通訊，有如位於相同網路中一樣。您可以在自己的 VPCs 之間建立 VPC 對等互連、在另一個 VPC 中建立 VPC AWS 帳戶，或在不同的 AWS 區域中建立 VPC。對等 VPC 之間的流量不會周遊公用網際網路。

如需詳細資訊，請參閱 Amazon VPC 對等連線指南。

監控 VPC

您可以使用下列工具，來監控 Virtual Private Cloud (VPC) 中的流量或網路存取。

VPC 流量日誌

您可以使用 VPC 流量日誌，來擷取 VPC 中傳入和傳出網路介面的流量詳細資訊。

Amazon CloudWatch 網路監視器

您可以使用網路監視器來了解網際網路問題如何影響 上託管的應用程式與最終使用者之間的效能 AWS 和可用性。您也可以近乎即時地探索如何透過切換到使用其他 服務，或透過不同的方式將流量重新路由到工作負載，來改善應用程式的預計延遲 AWS 區域。如需詳細資訊，請參閱使用 Amazon CloudWatch 網路監視器。

Amazon VPC IP 地址管理員 (IPAM)

您可以使用 IPAM 來規劃、追蹤和監控您工作負載的 IP 地址。如需詳細資訊，請參閱 IP 地址管理員。

流量鏡射

您可以使用此功能從 Amazon EC2 執行個體的網路介面複製網路流量，並將其傳送至頻外安全和監控設備，以進行深度封包檢查。您可以偵測網路和安全異常狀況，取得營運洞察，實作合規與安全控制，並排解問題。如需詳細資訊，請參閱流量鏡射。

Reachability Analyzer

您可以使用此工具來分析 VPC 中兩項資源之間的網路連線能力並進行偵錯。指定來源和目的地資源後，Reachability Analyzer 會在可連線虛擬路徑時，在這些路徑之間產生逐個躍點的詳細資訊，並在無法連線時識別導致阻礙的元件。如需詳細資訊，請參閱 Reachability Analyzer。

Network Access Analyzer

您可以使用 Network Access Analyzer 了解對資源的網路存取。這有助於您識別網路安全狀態的改善，並證明您的網路符合特定的合規要求。如需詳細資訊，請參閱 Network Access Analyzer。

CloudTrail 日誌

AWS CloudTrail 會記錄 Amazon VPC 的 API 呼叫，例如：

- 執行了哪些 API 呼叫 (例如建立或修改 VPC 資源等動作)
- 呼叫的來源 IP 位址
- 呼叫發起者身分

- 呼叫的執行時間

系統會為 CreateVpc、DeleteVpc、CreateDefaultVpc 動作分別建立單獨的日誌。這些日誌也包含隨 VPC 自動建立並關聯的預設資源 (例如任何預設網際網路閘道或預設安全群組)。

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 AWS CloudTrail記錄 Amazon EC2 API 呼叫。

使用 VPC 流量日誌來記錄 IP 流量

VPC 流量日誌是一項可讓您擷取傳入及傳出您 VPC 中網路介面之 IP 流量相關資訊的功能。流量日誌資料可以發佈至下列位置：Amazon CloudWatch Logs、Amazon S3 或 Amazon Data Firehose。將網路流量日誌傳送至 CloudWatch Logs 或 S3 等目的地的設定傳輸路徑與許可稱為訂閱。建立流程日誌之後，您可以在您設定的日誌群組、儲存貯體或交付串流中擷取和檢視流程日誌記錄。

流量日誌可協助您處理多項任務，例如：

- 診斷過於嚴苛的安全群組規則
- 監控進入執行個體的流量
- 判斷網路介面往來流量的方向

流量日誌資料是在網路流量路徑之外收集，因此不會影響網路輸送量或延遲。您可以建立或刪除流量日誌，而不會影響網路效能。

> **Note**
>
> 本節僅討論 VPC 的流量日誌。如需版本 6 中引入之傳輸閘道的流量日誌相關資訊，請參閱《Amazon VPC 傳輸閘道使用者指南》中的使用傳輸閘道流量日誌記錄網路流量。

目錄

- 流量日誌基礎知識
- 流量日誌記錄
- 流量日誌記錄範例
- 流量日誌限制
- 定價

- 使用流量日誌工作
- 將流量日誌發佈至 CloudWatch Logs
- 將流量日誌發佈到 Amazon S3
- 將流量日誌發布至 Amazon Data Firehose
- 使用 Amazon Athena 查詢流量日誌
- VPC 流程日誌中的身分和存取管理
- 疑難排解 VPC 流量日誌

流量日誌基礎知識

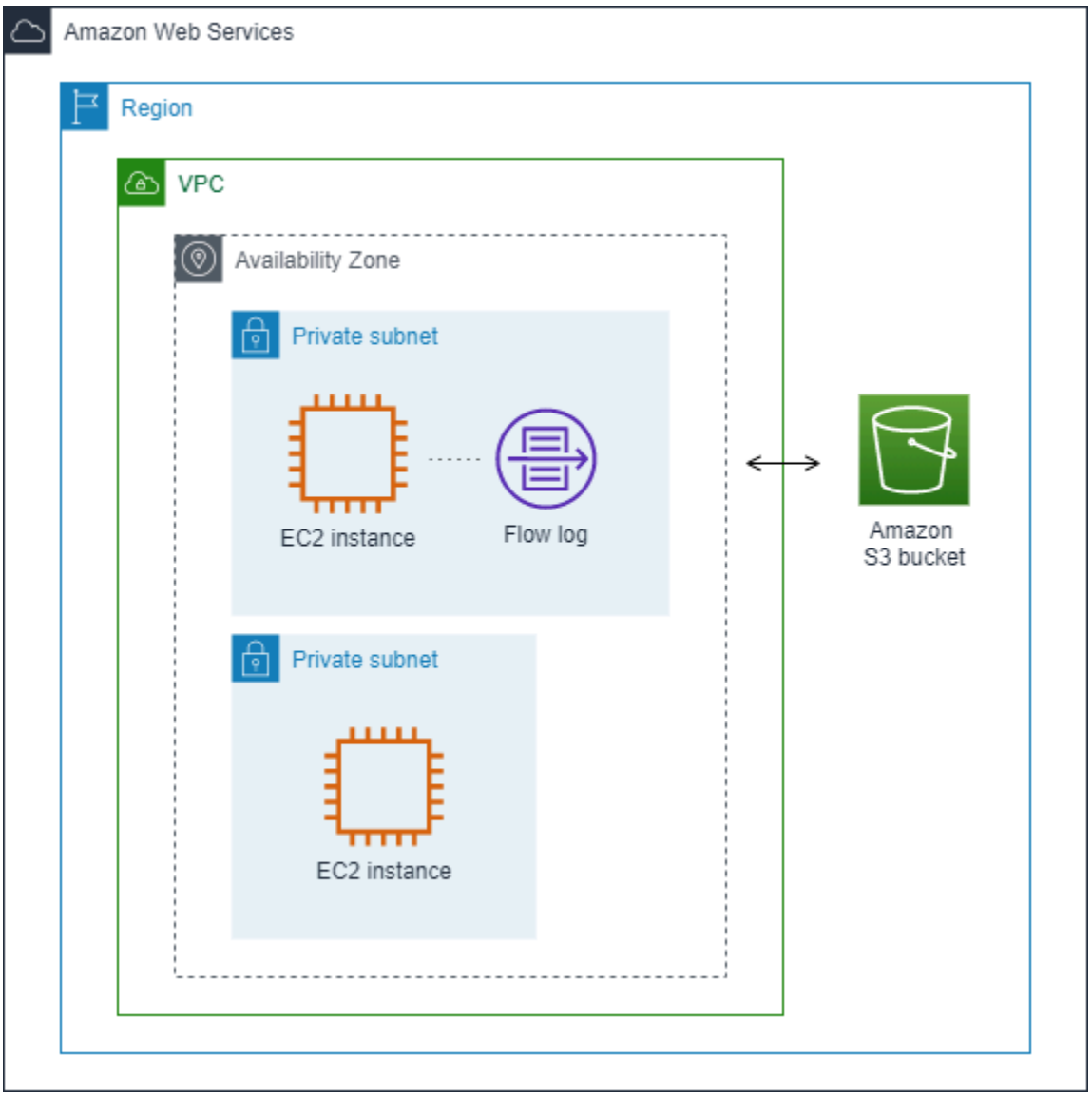
您可以建立 VPC、子網或網路介面的流量日誌。如果建立子網或 VPC 的流量日誌，則會監控該子網或 VPC 中的每個網路介面。

監控之網路介面的流量日誌將記錄為流量日誌記錄，即由描述流量之欄位組成的日誌事件。如需更多詳細資訊，請參閱 流量日誌記錄。

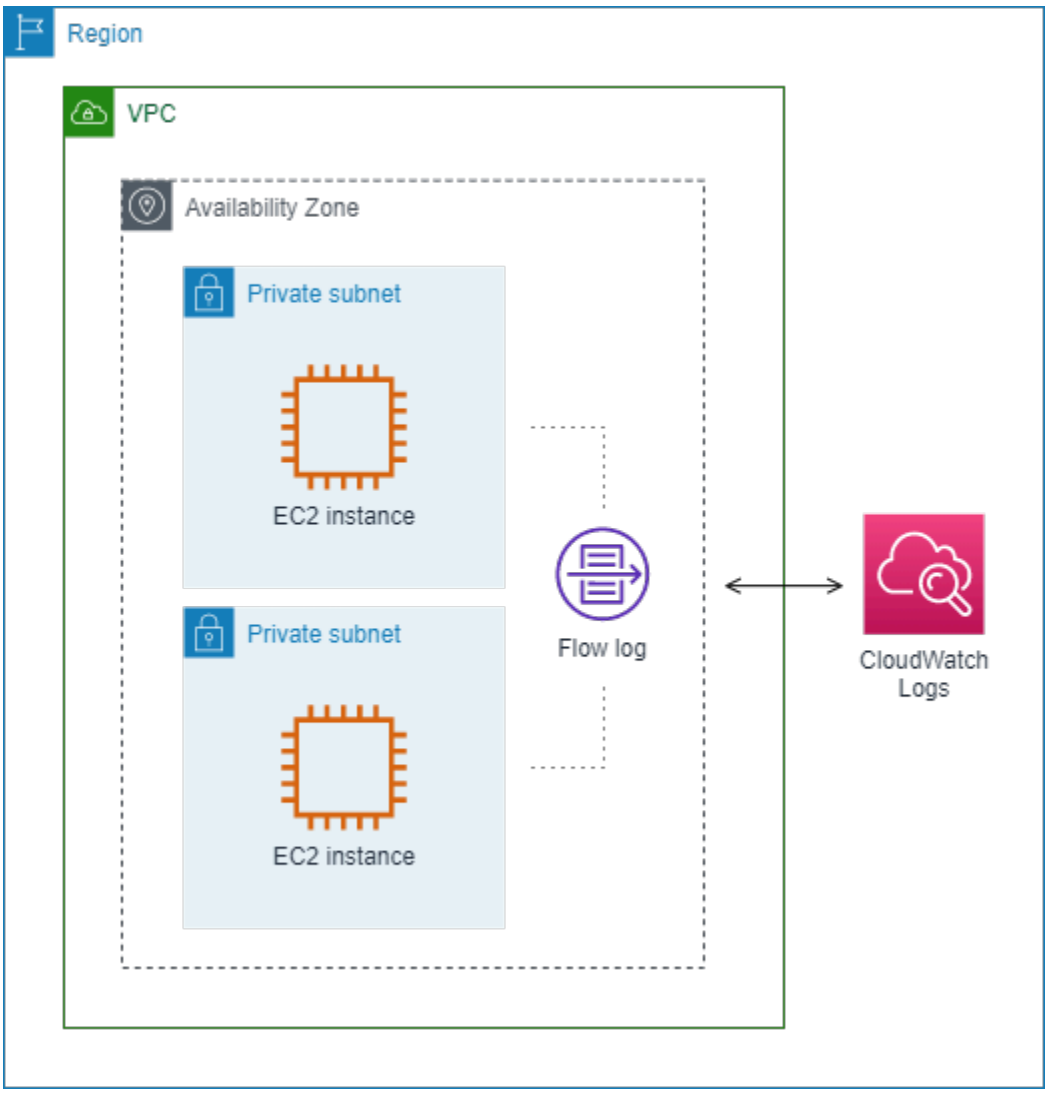
若要建立流量日誌，您要指定：

- 要建立流量日誌的資源
- 要擷取的流量類型 (接受的流量、拒絕的流量，或全部流量)
- 流量日誌資料的發佈目標

在下列範例中，您將為私有子網中的其中一個 EC2 執行個體建立流量日誌，以擷取網路介面的接受流量，並將流量日誌記錄發佈至 Amazon S3 儲存貯體。



在以下範例中，流量日誌擷取子網的所有流量，並將流量日誌記錄發佈至 Amazon CloudWatch Logs。流量日誌擷取子網中所有網路介面的流量。



在您建立流量日誌之後，其可能需要數分鐘的時間，才會開始收集資料並將資料發佈至選擇的目的地。流量日誌不會擷取您網路介面的即時日誌串流。如需詳細資訊，請參閱2. 建立流量日誌。

如果您在為子網路或 VPC 建立流程日誌之後在子網路中啟動執行個體，我們會為新的網路介面建立日誌串流（適用於 CloudWatch Logs) 或日誌檔案物件（適用於 Amazon S3)。一旦在界面上發生網路流量，就會建立日誌串流或檔案物件。

您可以為其他 AWS 服務建立的網路介面建立流量日誌，例如：

- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift

- Amazon WorkSpaces
- NAT 閘道
- 傳輸閘道

無論網路介面的類型為何，您都必須使用 Amazon EC2 主控台或 Amazon EC2 API 建立網路介面的流量日誌。

您可以將標籤套用至流量日誌。每個標籤皆包含由您定義的一個索引鍵與一個選用值。標籤可協助您整理流量日誌，例如依據用途或擁有者整理日誌。

如果您不再需要流量日誌，即可將其刪除。刪除流程日誌會停用資源的流程日誌服務，因此將不會再建立和發佈新的流程日誌記錄。刪除流程日誌並不會刪除任何現有的流程日誌資料。刪除流程日誌之後，您可以在完成操作後直接從目的地刪除流程日誌資料。如需詳細資訊，請參閱4. 刪除流量日誌。

流量日誌記錄

流量日誌記錄代表您 VPC 中的網路流。根據預設，每筆記錄會擷取發生在彙總時間間隔 (也稱為擷取時段) 內的網際網路通訊協定 (IP) 流量 (特徵為每個網路介面一個 5 元組)。

每筆記錄都是包含欄位的字串，其中欄位會由空格分隔。記錄包含 IP 流程不同元件的值，例如來源、目標和通訊協定。

建立流量日誌時，您可以使用流量日誌記錄的預設格式，或指定自訂格式。

內容

- 彙總時間間隔
- 預設格式
- 自訂格式
- 可用的欄位

彙總時間間隔

彙總時間間隔是指擷取特定流程並彙總至流量日誌記錄的一段期間。根據預設，最大彙總時間間隔為 10 分鐘。建立流量日誌時，您可以選擇指定最大彙總時間間隔為 1 分鐘。最大彙總時間間隔 1 分鐘的流量日誌所產生的流量日誌記錄量會高於最大彙總時間間隔 10 分鐘的流量日誌。

當網路介面連線至 Nitro 型執行個體時，無論指定的最大彙總時間間隔為何，彙總時間間隔一律為 1 分鐘或更短。

在彙總時間間隔內擷取資料之後，需要額外的時間來處理和發佈資料至 CloudWatch Logs 或 Amazon S3。流量日誌服務通常會在大約 5 分鐘內將日誌傳遞給 CloudWatch Logs，並在大約 10 分鐘內將日誌傳遞給 Amazon S3。不過，日誌傳遞是最大努力的基礎，而您的日誌可能會延遲超過一般傳遞時間。

預設格式

使用預設格式時，流量日誌記錄會依照可用欄位表格中顯示的順序，包括版本 2 欄位。您無法自訂或變更預設格式。若要擷取其他欄位或不同的欄位子集，請改為指定自訂格式。

自訂格式

使用自訂格式時，您可以指定流量日誌記錄中包含哪些欄位以及順序。這樣可讓您建立專門針對需求的流量日誌，省略不相關的欄位。使用自訂格式可以減少個別處理程序從已發佈的流量日誌擷取特定資訊的需求。您可指定任何數量的可用流量日誌欄位，但至少必須指定一個。

可用的欄位

下表描述流量日誌記錄的所有可用欄位。版本欄表示導入此欄位的 VPC 流量日誌版本。預設格式包括所有版本 2 欄位，其顯示順序與表格中的順序相同。

將流量日誌資料發佈到 Amazon S3 時，欄位的資料類型取決於流量日誌格式。如果格式為純文字，則所有欄位均為 STRING 類型。如果格式為 Parquet，請參閱欄位資料類型的資料表。

如果欄位不適用或無法計算特定記錄，則記錄會針對該項目顯示一個 '-' 符號。非直接來自封包標頭的中繼資料欄位是最佳近似值，而且它們的值可能會遺失或不正確。

欄位	描述	版本
version	VPC 流量日誌版本。如果您使用預設格式，則版本為 2。如果您使用自訂格式，則版本為指定欄位中的最高版本。例如，如果您只指定版本 2 中的欄位，則版本為 2。如果您指定的欄位混合了版本 2、3 和 4 的欄位，則版本為 4。 Parquet 資料類型：INT_32	2
account-id	記錄流量之來源網路介面擁有者 AWS 的帳戶 ID。如果網路介面是由 AWS 服務建立，例如在建立 VPC 端點或 Network Load Balancer 時，可能會unknown顯示此欄位的記錄。	2

欄位	描述	版本
	Parquet 資料類型：STRING	
interface-id	要記錄流量的網路介面 ID。對於與區域 NAT 閘道相關聯的流程，傳回 '-' 符號。 Parquet 資料類型：STRING	2
srcaddr	對於傳入流量，此欄位顯示流量的來源 IP 位址。對於傳出流量，此欄位顯示傳送流量之網路介面的私有 IPv4 位址或 IPv6 位址。對於來自區域 NAT 閘道的傳出流量，這是與 中相同的封包層級來源 IP 地址pkt-srcaddr。另請參閱pkt-srcaddr。 Parquet 資料類型：STRING	2
dstaddr	網路介面上傳出流量的目標地址，或傳入流量網路介面的 IPv4 或 IPv6 地址。網路介面的 IPv4 地址永遠都是其私有 IPv4 地址。對於傳入區域 NAT 閘道的流量，這是與 中相同的封包層級目的地 IP 地址pkt-dstaddr。另請參閱pkt-dstaddr。 Parquet 資料類型：STRING	2
srcport	流量的來源連接埠。 Parquet 資料類型：INT_32	2
dstport	流量的目標連接埠。 Parquet 資料類型：INT_32	2
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。 Parquet 資料類型：INT_32	2
packets	在流量期間傳輸的封包數。 Parquet 資料類型：INT_64	2

欄位	描述	版本
bytes	在流量期間傳輸的位元組數。 Parquet 資料類型：INT_64	2
start	彙總時間間隔內接收到第一個流量封包的時間 (以 Unix 秒為單位)。這可能是在網路界面上接收封包前最多 60 秒，或在傳輸封包後最多 60 秒。 Parquet 資料類型：INT_64	2
end	彙總時間間隔內接收到最後一個流量封包的時間 (以 Unix 秒為單位)。這個時間最長可能是在網路介面上傳送或接收封包之後 60 秒。 Parquet 資料類型：INT_64	2
action	與流量相關聯的動作： • ACCEPT – 已接受流量。 • REJECT – 已拒絕流量。例如，安全群組或網路 ACL 不允許流量，或封包在連線關閉後到達。 Parquet 資料類型：STRING	2

欄位	描述	版本
log-status	流量日誌的記錄狀態： • OK – 資料正常記錄至選擇的目的地。 • NODATA – 在彙總時間間隔內沒有任何流入或流出網路介面的網路流量。 • SKIPDATA – 在彙總時間間隔內曾跳過一部分流量日誌記錄。這可能是因為內部容量的條件約束，或是內部錯誤。 在彙總時間間隔內可能跳過一部分流量日誌記錄 (請參閱可用的欄位中的 log-status)。這可能是由於內部 AWS 容量限制或內部錯誤所造成。如果您使用 AWS Cost Explorer 來檢視 VPC 流程日誌費用，且在流程日誌彙總間隔期間略過某些流程日誌，則 中報告的流程日誌數目 AWS Cost Explorer 會高於 Amazon VPC 發佈的流程日誌數目。 Parquet 資料類型：STRING	2
vpc-id	包含要記錄流量之網路介面的 VPC ID。 Parquet 資料類型：STRING	3
subnet-id	包含要記錄流量之網路介面的子網 ID。傳回與區域 NAT 閘道相關聯之流程的 '-' 符號。 Parquet 資料類型：STRING	3
instance-id	如果您擁有執行個體，則為與要記錄流量之網路介面相關聯的執行個體 ID。傳回請求者管理網路介面的 '-' 符號，例如 NAT 閘道的網路介面。 Parquet 資料類型：STRING	3

欄位	描述	版本
tcp-flags	下列 TCP 標記的位元遮罩值： • FIN – 1 • SYN – 2 • RST – 4 • SYN-ACK – 18 如果沒有記錄支援的旗標，TCP 旗標值則為 0。例如，由於 tcp-flags 不支援記錄 ACK 或 PSH 旗標，具有這些不支援旗標的流量紀錄會導致 tcp-flags 值 0。但是，如果不支援的旗標附帶支援的旗標，我們將報告支援旗標的值。例如，如果 ACK 是 SYN-ACK 的一部分，則會報告 18。如果有 SYN+ECE 等紀錄，由於 SYN 是支援的旗標，而 ECE 不是，TCP 旗標值是 2。如果由於某種原因旗標組合無效且無法計算值，則值為 '-'。如果沒有傳送旗標，則 TCP 旗標值為 0。 彙總時間間隔內的 TCP 標記可用 OR 運算彙總。針對短暫連線，標記可能和流量日誌記錄設在同一行，例如，SYN-ACK 和 FIN 為 19，而 SYN 和 FIN 為 3。如需範例，請參閱TCP 標記序列。 如需有關 TCP 標記的一般資訊 (如 FIN、SYN 和 ACK 等標記的含義)，請參閱 Wikipedia 上的 TCP segment structure (TCP 區段結構)。 Parquet 資料類型：INT_32	3
type	流量類型。可能的值為：IPv4 | IPv6 | EFA。如需詳細資訊，請參閱 Elastic Fabric Adapter。 Parquet 資料類型：STRING	3

欄位	描述	版本
pkt-srcaddr	流量的封包層級 (原始) 來源 IP 地址。使用此欄位搭配 srcaddr 欄位來分辨流量流經之中繼 layer 的 IP 地址，以及流量的原始來源 IP 地址。 例如，流量可能會流經 NAT 閘道的網路界面。另一種情況是 Amazon EKS 中 Pod 的 IP 地址與執行 Pod 之執行個體節點的網路介面 IP 地址不同 （用於 VPC 內的通訊）。 Parquet 資料類型：STRING	3
pkt-dstaddr	流量的封包層級 (原始) 目標 IP 地址。使用此欄位搭配 dstaddr 欄位來分辨流量流經之中繼 layer 的 IP 地址，以及流量的最終目標 IP 地址。 例如，流量可能會流經 NAT 閘道的網路界面。另一種情況是 Amazon EKS 中 Pod 的 IP 地址與執行 Pod 之執行個體節點的網路介面 IP 地址不同 （用於 VPC 內的通訊）。 Parquet 資料類型：STRING	3
region	包含記錄流量之網路介面的區域。 Parquet 資料類型：STRING	4
az-id	可用區域的 ID，其中包含記錄流量的網路介面。如果流量來自子位置，記錄會顯示此欄位的 '-' 符號。 Parquet 資料類型：STRING	4
sublocation-type	在 sublocation-id 欄位中傳回的子位置類型。可能的值為：波長 | outpost | 本機區域。如果流量不是來自子位置，則記錄會在此欄位顯示 '-' 符號。 Parquet 資料類型：STRING	4

欄位	描述	版本
sublocation-id	包含要記錄流量之網路介面的子位置 ID。如果流量不是來自子位置，則記錄會在此欄位顯示 '-' 符號。 Parquet 資料類型：STRING	4
pkt-src-aws-service	如果來源 IP 地址適用於 AWS 服務，pkt-srcaddr 欄位的 IP 地址範圍的子集名稱。如果來源 IP 地址屬於重疊的範圍，則 只會pkt-src-aws-service顯示其中一個 AWS 服務代碼。可能的值為：AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS 。 Parquet 資料類型：STRING	5
pkt-dst-aws-service	如果目的地 IP 地址是 AWS 服務，則pkt-dstaddr欄位的 IP 地址範圍子集名稱。如需可能值的清單，請參閱 pkt-src-aws-service 欄位。 Parquet 資料類型：STRING	5
flow-direction	關於擷取流量的介面的流程方向。可能的值為：ingress | egress。 Parquet 資料類型：STRING	5

欄位	描述	版本
traffic-path	出口流量前往目的地的路徑。若要判斷流量是否為出口流量，請查看 flow-direction 欄位。可能的值如下。如果沒有任何值套用，則欄位會設定為 -。 • 1 — 透過相同 VPC 中的另一個資源，包括 AWS受管網路介面或 Outpost 本機閘道 • 2 – 透過網際網路閘道或閘道 VPC 端點 • 3 – 透過虛擬私有閘道 • 4 – 透過區域內 VPC 對等連線 • 5 – 透過區域間 VPC 對等連線 • 6 – 透過 Local Zone 或 Wavelength Zone • 7 — 透過閘道 VPC 端點 • 8 — 透過網際網路閘道 Parquet 資料類型：INT_32	5
ecs-cluster-arn	AWS 如果流量來自執行中的 ECS 任務，則為 ECS 叢集的資源名稱 (ARN)。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 的許可。 Parquet 資料類型：STRING	7
ecs-cluster-name	如果流量來自正在執行的 ECS 任務，則此欄位表示 ECS 叢集的名稱。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 的許可。 Parquet 資料類型：STRING	7
ecs-container-instance-arn	如果流量來自 EC2 執行個體上正在執行的 ECS 任務，則此欄位表示 ECS 容器執行個體的 ARN。如果容量提供者為 AWS Fargate，則此欄位將為 '-'。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 和 ecs:ListContainerInstances 的許可。 Parquet 資料類型：STRING	7

欄位	描述	版本
ecs-container-instance-id	如果流量來自 EC2 執行個體上正在執行的 ECS 任務，則此欄位表示 ECS 容器執行個體的 ID。如果容量提供者為 AWS Fargate，則此欄位將為 '-'。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 和 ecs:ListContainerInstances 的許可。 Parquet 資料類型：STRING	7
ecs-container-id	如果流量來自正在執行的 ECS 任務，則此欄位表示容器的 Docker 執行時期 ID。如果 ECS 任務中有一個或多個容器，則此欄位將顯示第一個容器的 Docker 執行時期 ID。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 的許可。 Parquet 資料類型：STRING	7
ecs-second-container-id	如果流量來自正在執行的 ECS 任務，則此欄位表示容器的 Docker 執行時期 ID。如果 ECS 任務中有多個容器，則此欄位將顯示第二個容器的 Docker 執行時期 ID。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 的許可。 Parquet 資料類型：STRING	7
ecs-service-name	如果流量來自正在執行的 ECS 任務，且 ECS 任務由 ECS 服務啟動，則此欄位表示 ECS 服務的名稱。如果 ECS 服務未啟動 ECS 任務，此欄位將為 '-'。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 和 ecs:ListServices 的許可。 Parquet 資料類型：STRING	7
ecs-task-definition-arn	如果流量來自正在執行的 ECS 任務，則此欄位表示 ECS 任務定義的 ARN。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 和 ecs:ListTaskDefinitions 的許可。 Parquet 資料類型：STRING	7
ecs-task-arn	如果流量來自正在執行的 ECS 任務，則此欄位表示 ECS 任務的 ARN。若要在訂閱中包含此欄位，您需要擁有呼叫 ecs:ListClusters 和 ecs:ListTasks 的許可。 Parquet 資料類型：STRING	7

欄位	描述	版本
ecs-task-id	如果流量來自正在執行的 ECS 任務，則此欄位表示 ECS 任務的 ID。若要在訂閱中包含此欄位，您需要呼叫 ecs:ListClusters 和 ecs:ListTasks 的許可。 Parquet 資料類型：STRING	7
reject-reason	流量遭拒的原因。可能的值：BPA、EC。對於其他任何拒絕原因，傳回 '-'。 • BPA — 如需 VPC 封鎖公開存取 (BPA) 的詳細資訊，請參閱封鎖對 VPC 和子網路的公開存取。 • EC：由於加密控制，VPC 端點拒絕流程。如需 VPC 加密控制的詳細資訊，請參閱 強制執行傳輸中的 VPC 加密。 Parquet 資料類型：STRING	8
resource-id	區域 NAT 閘道的 ID，其中包含記錄流量的網路界面。對於與區域 NAT 閘道無關的流量，傳回 '-' 符號。如需區域 NAT 閘道的詳細資訊，請參閱 用於自動多可用區域擴展的區域 NAT 閘道。 Parquet 資料類型：STRING	9

欄位	描述	版本

encryption-status	流程的加密狀態。如需 VPC 加密控制的詳細資訊，請參閱 強制執行傳輸中的 VPC 加密。可能值如下：
	• 0 — 未加密。
	• 1 — nitro 加密。它由 Nitro 系統硬體加密。
	• 2 — 應用程式加密。只有下列項目會被視為應用程式加密：
	  • TCP 連接埠 443 上的流程，用於介面端點到 AWS 服務*
	  • 閘道端點的 TCP 連接埠 443 上的流程*
	  • 透過 VPC 端點傳送至加密 Redshift 叢集**
	• 3 — nitro 加密和應用程式加密。
	
	如果未啟用 VPC 加密控制，或 FlowLog 無法取得狀態，則值為 '-'。
	
	Note
	* 對於介面和閘道端點， AWS 不會查看封包資料來判斷加密狀態，而是依賴用來取得加密狀態的連接埠。
	** 對於指定的 AWS 受管端點， 會根據服務組態中的 TLS 需求來 AWS 確定加密狀態。
	
	Parquet 資料類型：INT_32
		10

instance-tag	TagFieldSpecifications 中包含的第一個執行個體標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 ec2：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11

欄位	描述	版本
instance-tag-2	TagFieldSpecifications 中包含的第二個執行個體標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 ec2：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11
interface-tag	TagFieldSpecifications 中包含的第一個網路界面標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 ec2：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11
interface-tag-2	TagFieldSpecifications 中包含的第二個網路界面標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 ec2：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11
asg-tag	TagFieldSpecifications 中包含的第一個auto-scaling-group標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 autoscaling：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。您的帳戶中必須至少有一個啟用的 CloudTrail 追蹤，才能即時正確追蹤和更新 Auto Scaling 群組標籤值。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11

欄位	描述	版本
asg-tag-2	TagFieldSpecifications 中包含的第二個auto-scaling-group標籤的標籤值。標籤值會顯示為使用 UTF-8% 編碼翻譯所有特殊字元。若要在訂閱中包含此欄位，您需要呼叫 autoscaling：DescribeTags 和 iam：CreateServiceLinkedRole 的許可。您的帳戶中必須至少有一個啟用的 CloudTrail 追蹤，才能即時正確追蹤和更新 Auto Scaling 群組標籤值。如需流程日誌 Amazon EC2 標籤服務連結角色的詳細資訊，請參閱 使用 VPC 流程日誌的服務連結角色。 Parquet 資料類型：STRING	11
interface-type	擷取流程的本機網路界面類型。支援的值為： `nat_gateway` | `network_load_balancer` | `regional_nat_gateway` | `transit_gateway` | `vpc_endpoint` 。如果網路界面沒有關聯服務，或不支援該服務，則值為 '-'。 Parquet 資料類型：STRING	11
next-hop-interface-id	下一個躍點網路界面的 ID。對於輸出流量，這是接收流量的界面。對於輸入流量，這是傳送流量的界面。 Parquet 資料類型：STRING	11
next-hop-subnet-id	包含下一個躍點網路界面的子網路 ID。 Parquet 資料類型：STRING	11
next-hop-az-id	包含下一個躍點網路界面的可用區域 ID。 Parquet 資料類型：STRING	11
next-hop-vpc-id	包含下一個躍點網路界面的 VPC ID。 Parquet 資料類型：STRING	11
next-hop-interface-type	下一個躍點網路界面的類型。如需可能值的清單，請參閱 interface-type 欄位 Parquet 資料類型：STRING	11

流量日誌記錄範例

以下是擷取特定流量的流量日誌記錄範例。

如需流量日誌記錄格式的資訊，請參閱 流量日誌記錄。如需如何建立流程記錄的相關資訊，請參閱使用流量日誌工作。

內容

- 已接受和已拒絕的流量
- 無任何資料及略過的記錄
- 安全群組及網路 ACL 規則
- IPv6 流量
- TCP 標記序列
- 透過區域 NAT 閘道的流量
- 透過區域 NAT 閘道的流量
- 通過傳輸閘道的流量
- 服務名稱、流量路徑和流向

已接受和已拒絕的流量

以下是預設流量日誌記錄的範例。

在此範例中，允許從 IP 位址 172.31.16.139 到私有 IP 位址為 172.31.16.21，ID 為 eni-1235b8ca123456789 且屬於帳戶 123456789010 之網路介面的 SSH 流量 (目的地連接埠 22、TCP 通訊協定)。

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

在本範例中，拒絕帳戶 123456789010 中網路介面 eni-1235b8ca123456789 的 RDP 流量（目標連接埠 3389，TCP 通訊協定）。

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

無任何資料及略過的記錄

以下是預設流量日誌記錄的範例。

在此範例中，彙總時間間隔內沒有記錄任何資料。

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

VPC Flow Logs 在無法在彙總間隔期間擷取流量日誌資料時，會跳過記錄，因為超過內部容量。跳過的單個記錄可代表在彙總間隔期間內未對網路介面擷取的多個流程。

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

> **Note**
>
> 在彙總時間間隔內可能跳過一部分流量日誌記錄 (請參閱可用的欄位中的 log-status)。這可能是由於內部 AWS 容量限制或內部錯誤所造成。如果您使用 AWS Cost Explorer 來檢視 VPC 流程日誌費用，且在流程日誌彙總間隔期間略過某些流程日誌，則 中報告的流程日誌數目 AWS Cost Explorer 會高於 Amazon VPC 發佈的流程日誌數目。

安全群組及網路 ACL 規則

如使用流量日誌診斷過於嚴苛或寬鬆的安全群組規則或網路 ACL 規則，請注意這些資源的狀態性。安全群組具有狀態，這表示針對允許流量的回應也會獲得允許，即使您安全群組中的規則不允許。相反的，網路 ACL 無狀態，因此針對允許流量的回應仍會受制於網路 ACL 規則。

例如，您從您的家用電腦（IP 地址為 203.0.113.12）對您的執行個體（網路介面的私有 IP 地址為 172.31.16.139）使用 ping 命令。您的安全群組傳入規則允許 ICMP 流量，但傳出規則不允許 ICMP 流量。因為安全群組有狀態，所以允許來自您執行個體的回應 ping。您的網路 ACL 允許傳入 ICMP 流量，但不允許傳出 ICMP 流量。因為網路 ACL 無狀態，回應 ping 會遭到卸除，因而不會觸達您的家用電腦。在預設的流量日誌中，這會顯示為兩筆流量日誌記錄：

- 同時獲得網路 ACL 及安全群組允許，因此可觸達您執行個體之原始 ping 的 ACCEPT 記錄。
- 網路 ACL 拒絕之回應 ping 的 REJECT 記錄。

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

若您的網路 ACL 允許傳出 ICMP 流量，則流量日誌會顯示兩個 ACCEPT 記錄 (其中一個為原始 ping，另一個則為回應 ping)。若您的安全群組拒絕傳入 ICMP 流量，則流量日誌會顯示單一 REJECT 記錄，因為流量未獲准能觸達您的執行個體。

IPv6 流量

以下是預設流量日誌記錄的範例。在此範例中，允許使用帳戶 123456789010 內從 IPv6 地址 2001:db8:1234:a100:8d6e:3477:df66:f105 至網路介面 eni-1235b8ca123456789 的 SSH 流量（連接埠 22）。

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

TCP 標記序列

本節所述的自訂流量日誌範例，可依以下順序擷取下列欄位。

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

本節範例中的 tcp-flags 欄位以流量日誌中的倒數第二個值表示。TCP 標記可協助您識別流量方向，例如哪部伺服器啟動了連線。

> **Note**
>
> 如需有關 tcp-flags 選項的詳細資訊和每個 TCP 標記的說明，請參閱 可用的欄位。

在下列記錄中 (下午 7:47:55 開始，下午 7:48:53 結束)，用戶端向在連接埠 5001 執行的伺服器啟動了兩條連線。用戶端伺服器收到來自用戶端不同來源連接埠（43416 和 43418）的兩個 SYN 標記 (2)。對每個 SYN 而言，SYN-ACK 是從伺服器傳送至對應連接埠的用戶端 (18)。

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
```

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

在第二個彙總時間間隔內，上個流程期間建立的其中一條連線現已關閉。伺服器針對 43418 連接埠的連線，向用戶端傳送了 FIN 旗標 (1)。用戶端隨後經由 43418 連接埠向伺服器回應了 FIN。

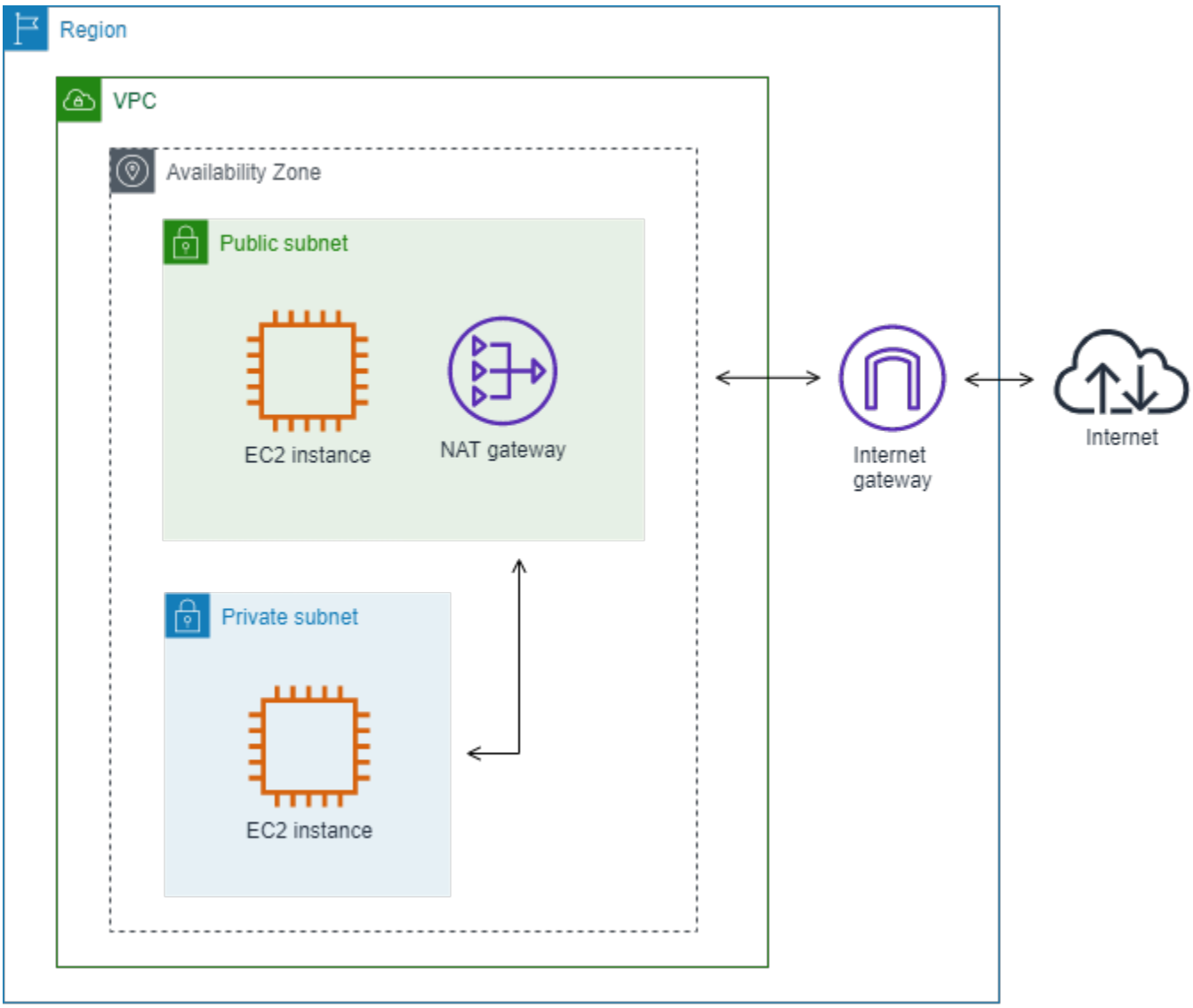
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

對於在單一彙總間隔內開啟和關閉的短連線，旗標可能會在相同方向的流量日誌記錄中的同一行上設定。在以下範例中，連線在同一彙總時間間隔內建立及結束。在第一行中，TCP 標記值是 3，指出曾有 SYN 和 FIN 訊息自用戶端傳送至伺服器。在第二行中，TCP 標記值是 19，指出曾有 SYN-ACK 和 FIN 訊息自伺服器傳送至用戶端。

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

透過區域 NAT 閘道的流量

在此範例中，私有子網路中的執行個體會透過公有子網路中的區域 NAT 閘道存取網際網路。



下列區域 NAT 閘道網路介面的自訂流程日誌會依下列順序擷取下列欄位。

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

流程日誌顯示流量從執行個體 IP 地址 (10.0.1.5) 透過區域 NAT 閘道網路界面流向網際網路上的主機 (203.0.113.5)。區域 NAT 閘道網路界面是申請者管理的網路界面，因此流程日誌記錄會顯示 instance-id 欄位的「-」符號。下行顯示從來源執行個體到區域 NAT 閘道網路介面的流量。dstaddr 和 pkt-dstaddr 欄位的值不一樣。dstaddr 欄位會顯示區域 NAT 閘道網路界面的私有 IP 地址，而 pkt-dstaddr 欄位會顯示網際網路上主機的最終目的地 IP 地址。

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

下兩行顯示從區域 NAT 閘道網路界面到網際網路上目標主機的流量，以及從主機到 NAT 閘道網路界面的回應流量。

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

下行顯示從區域 NAT 閘道網路界面到來源執行個體的回應流量。srcaddr 和 pkt-srcaddr 欄位的值不一樣。srcaddr 欄位會顯示區域 NAT 閘道網路界面的私有 IP 地址，而 pkt-srcaddr 欄位會顯示網際網路上主機的 IP 地址。

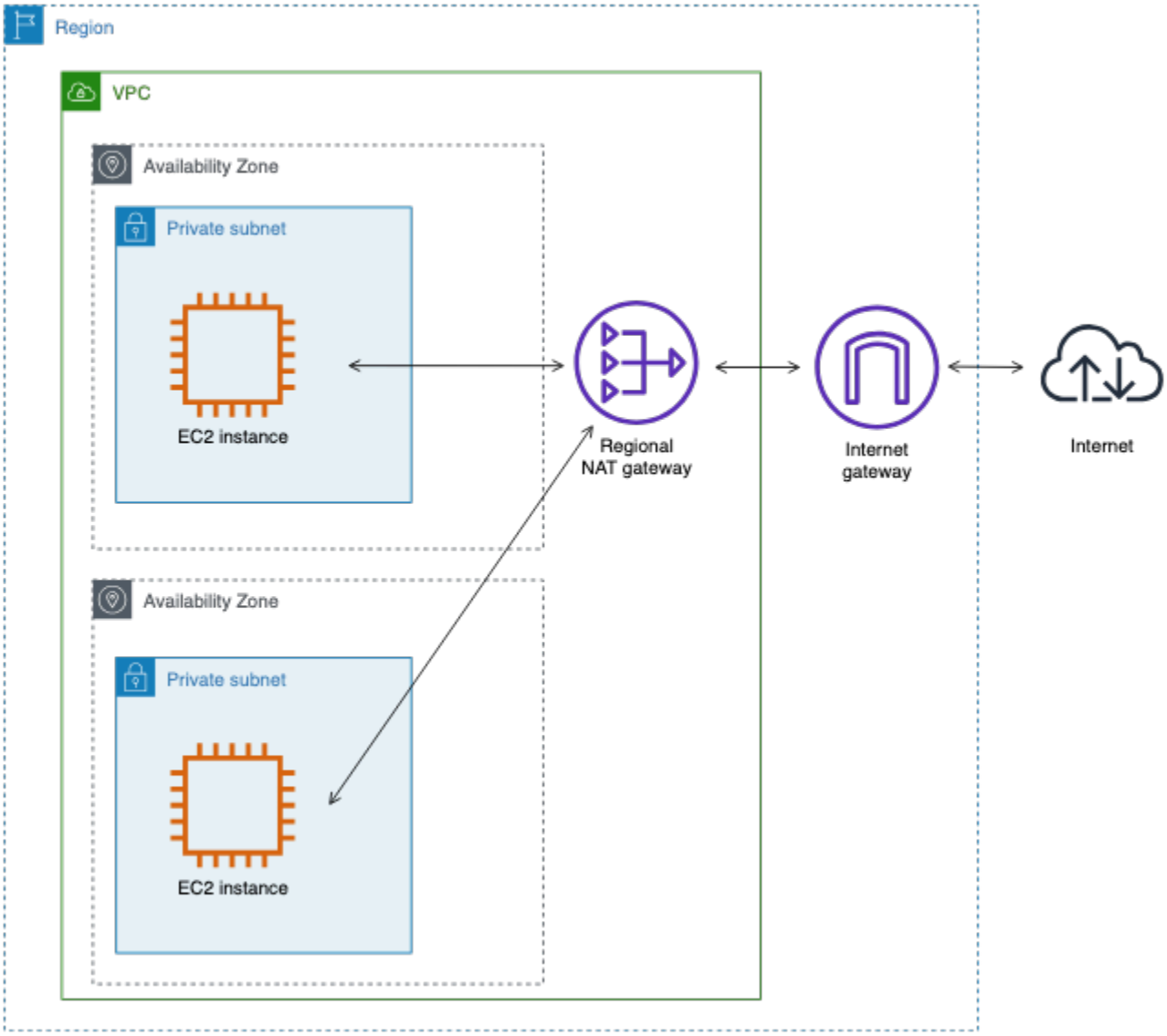
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

您使用上文中的同一欄位集，建立另一個自訂流量日誌。您為私有子網中的執行個體建立網路介面的流量日誌。在此情況下， instance-id 欄位會傳回與網路界面相關聯的執行個體 ID。dstaddr 和 pkt-dstaddr 欄位或 srcaddr和 pkt-srcaddr 欄位之間沒有差異。與區域 NAT 閘道的網路界面不同，此網路界面不是流量的中繼網路界面。

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

透過區域 NAT 閘道的流量

區域 NAT 閘道可以連接到不同可用區域的多個子網路。在此範例中，來自兩個不同可用區域的兩個私有子網路執行個體會透過相同的區域 NAT 閘道存取網際網路。下列流程日誌顯示透過區域 NAT 閘道從其中一個執行個體到網際網路的流量。



下列區域 NAT 閘道的自訂流程日誌會依下列順序擷取下列欄位。

```
resource-id instance-id interface-id subnet-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

流程日誌顯示流量從執行個體 IP 地址 (10.0.1.5) 透過區域 NAT 閘道流向網際網路上的主機 (203.0.113.5)。interface-id、 instance-id和 subnet-id不適用於區域 NAT 閘道。因此，流程日誌記錄會顯示這些欄位的 '-' 符號。反之， resource-id 欄位會顯示區域 NAT 閘道的 ID。dstaddr 和 pkt-dstaddr 欄位會顯示網際網路上主機的最終目的地 IP 地址。

```
nat-1234567890abcdef - - - 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
```

下兩行顯示從區域 NAT 閘道（公有 IP 地址 107.22.182.139) 到網際網路上目標主機的流量。它們也會顯示從主機到區域 NAT 閘道的回應流量。

```
nat-1234567890abcdef - - - 107.22.182.139 203.0.113.5 107.22.182.139 203.0.113.5
nat-1234567890abcdef - - - 203.0.113.5 107.22.182.139 203.0.113.5 107.22.182.139
```

下行顯示從區域 NAT 閘道到來源執行個體的回應流量。srcaddr 和 pkt-srcaddr 欄位會顯示網際網路上主機的 IP 地址。

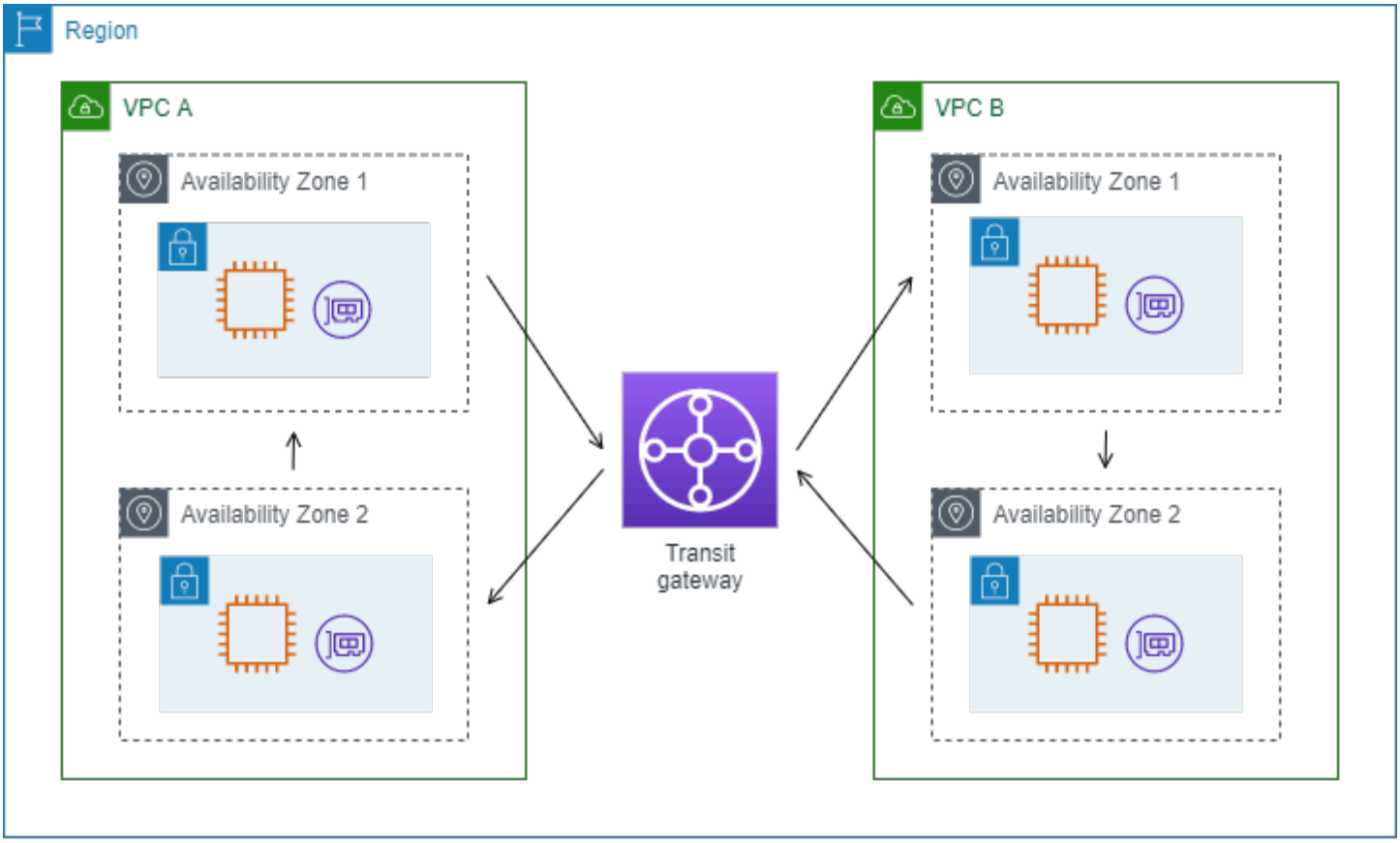
```
nat-1234567890abcdef - - - 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

您使用上文中的同一欄位集，建立另一個自訂流量日誌。您為私有子網中的執行個體建立網路介面的流量日誌。在此情況下， instance-id 欄位會傳回與網路界面相關聯的執行個體 ID，且 resource-id為'-'。dstaddr 和 pkt-dstaddr 欄位與 srcaddr和 pkt-srcaddr 欄位之間沒有差異。

```
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 10.0.1.5
 203.0.113.5 10.0.1.5 203.0.113.5 #Traffic from the source instance to host on the
 internet
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 203.0.113.5
 10.0.1.5 203.0.113.5 10.0.1.5 #Response traffic from host on the internet to the
 source instance
```

通過傳輸閘道的流量

在本範例中，VPC A 中的用戶端透過傳輸閘道連線至 VPC B 的 Web 伺服器。用戶端和伺服器位於不同的可用區域。流量使用一個彈性網路介面 ID (在此範例中，假設 ID 為 eni-11111111111111111) 到達 VPC B 中的伺服器，並使用另一個 (例如 eni-22222222222222222) 離開 VPC B。



您使用以下格式建立 VPC B 的自訂流量日誌。

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

下列數行流量日誌記錄示範 Web 伺服器網路介面上的流量。第一行是來自用戶端的請求流量，而最後一行是來自 Web 伺服器的回應流量。

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

下行是子網 subnet-11111111aaaaaaaaa 中，傳輸閘道申請者管理網路介面在 eni-11111111111111111 上的請求流量。因此，流量日誌記錄在 instance-id 欄位會顯示 '-' 符

號。srcaddr 欄位顯示傳輸閘道網路介面的私有 IP 地址，而 pkt-srcaddr 欄位則顯示 VPC A 中用戶端的 IP 地址。

```
3 eni-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

下行是子網 subnet-22222222bbbbbbbbb 中，傳輸閘道申請者管理網路介面在 eni-22222222222222222 上的回應流量。dstaddr 欄位顯示傳輸閘道網路介面的私有 IP 地址，而 pkt-dstaddr 欄位則顯示 VPC A 中用戶端的 IP 地址。

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

服務名稱、流量路徑和流向

以下是自訂流量日誌記錄的欄位範例。

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

在下列範例中，版本為 5，因為記錄包含版本 5 欄位。一個 EC2 執行個體呼叫 Amazon S3 服務。會在執行個體的網路介面上擷取流量日誌。第一筆記錄的流動方向為 ingress，第二個記錄的流動方向為 egress。對於 egress 記錄，traffic-path 為 8，表示流量通過網際網路閘道。此 traffic-path 欄位不支援 ingress 流量。當 pkt-srcaddr 或 pkt-dstaddr 是公用 IP 地址時，會顯示服務名稱。

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

流量日誌限制

若要使用流量日誌，您必須注意下列限制：

- 建立流量日誌之後，除非您選擇的網路介面、子網路或 VPC 有作用中流量，否則您不會看到流量日誌資料。
- 您無法為已和您 VPC 互連之 VPC 啟用流量日誌，除非對等 VPC 位於您的帳戶中。
- 建立流量日誌之後，您即無法變更其組態或流量日誌記錄格式。例如，您無法建立不同 IAM 角色與流量日誌的關聯，或新增或移除流量日誌記錄的欄位。但是您可以刪除流量日誌，並使用需要的組態建立新的流量日誌。
- 您的網路介面如有多個 IPv4 地址，且流量會傳送到輔助私有 IPv4 地址，則流量日誌會在 `dstaddr` 欄位中顯示主要私有 IPv4 地址。若要擷取原始目標 IP 地址，請建立具有 `pkt-dstaddr` 欄位的流量日誌。
- 如果流量要傳送到網路介面，但目標不是任一網路介面的 IP 地址，則流量日誌會在 `dstaddr` 欄位中顯示主要私有 IPv4 地址。若要擷取原始目標 IP 地址，請建立具有 `pkt-dstaddr` 欄位的流量日誌。
- 如果流量是從網路介面傳送，且來源不是網路介面的任何 IP 地址，則行為取決於流程方向。對於輸出流程，流程日誌會在 `srcaddr` 欄位中顯示主要私有 IPv4 地址。若要擷取原始來源 IP 地址，請建立具有 `pkt-srcaddr` 欄位的流量日誌。

  如果日誌記錄對應進入網路介面的輸入流量，則 `srcaddr` 欄位不會顯示網路介面的主要私有 IP。
- 當您的網路介面連線至 Nitro 型執行個體時，無論指定的最大彙總時間間隔為何，彙總時間間隔一律為 1 分鐘或更短。
- 對於 `pkt-srcaddr` 和 `pkt-dstaddr` 欄位，如果中繼層啟用了用戶端 IP 位址保留，則此欄位可能會顯示保留的用戶端 IP，而不是中繼層的 IP 位址。
- 對於 `traffic-path` 欄位，流經同一 VPC 中資源的流量與流經 Outpost 本機閘道的流量，其欄位值相同。
- 在彙總時間間隔內可能跳過一部分流量日誌記錄 (請參閱可用的欄位中的 log-status)。這可能是由於內部 AWS 容量限制或內部錯誤所造成。如果您使用 AWS Cost Explorer 來檢視 VPC 流程日誌費用，且在流程日誌彙總間隔期間略過某些流程日誌，則 中報告的流程日誌數目 AWS Cost Explorer 將高於 Amazon VPC 發佈的流程日誌數目。
- 如果您使用 VPC 封鎖公開存取 (BPA)：
  - VPC BPA 的流量日誌不包含跳過的記錄。
  - 即使您在流量日誌中包含 `bytes` 欄位，VPC BPA 的流量日誌也不會包含 `bytes`。
- VPC 流程日誌支援每個帳戶每個資源最多 250 個訂閱。若要在已達到此限制的資源上建立其他訂閱，您必須先刪除現有的訂閱。

流量日誌不會擷取所有 IP 流量。以下流量類型的日誌不會記錄：

- 由執行個體在與 Amazon DNS 伺服器聯絡時產生的流量。若您使用您自己的 DNS 伺服器，則會記錄所有流向該 DNS 伺服器的流量。
- 由 Windows 執行個體針對 Amazon Windows 授權啟用所產生的流量。
- 針對執行個體中繼資料，流入及流出 169.254.169.254 的流量。
- 針對 Amazon Time Sync Service，流入及流出 169.254.169.123 的流量。
- DHCP 流量。
- 鏡映流量的來源流量。您只會看到鏡映流量的目標流量。
- 流入預設 VPC 路由器預留 IP 地址的流量。
- 端點網路介面和 Network Load Balancer 網路介面之間的流量。
- 位址解析通訊協定 (ARP) 流量。
- 短期區域 NAT 閘道上的流量會在建立幾分鐘後刪除。

特定於第 7 版中可用 ECS 欄位的限制：

- 如果流量日誌訂閱的擁有者未擁有基礎 ECS 任務，則不會計算 ECS 欄位。

  例如，假設您與其他帳戶 (SubnetA) 共用子網路 (AccountB)，然後為 建立流程日誌訂閱SubnetA。如果 在共用子網路中AccountB啟動 ECS 任務，您的訂閱會從這些任務接收流量日誌。不過，由於安全性考量，系統不會計算這些日誌的 ECS 欄位。
- 如果您在 VPC/子網路資源層級建立包含 ECS 欄位的流量日誌訂閱，則系統會為訂閱傳送針對非 ECS 網路介面所產生的任何流量。非 ECS IP 流量的 ECS 欄位值將為 '-'。例如，您擁有子網路 (subnet-000000)，且為此子網路建立了包含 ECS 欄位 (fl-00000000) 的流量日誌訂閱。在 subnet-000000 中，您啟動了連線至網際網路且主動產生 IP 流量的 EC2 執行個體 (i-0000000)。您還在同一個子網路中啟動了正在執行的 ECS 任務 (ECS-Task-1)。由於 i-0000000 和 ECS-Task-1 都產生 IP 流量，您的流量日誌訂閱 fl-00000000 將傳送這兩個實體的流量日誌。不過，只有 ECS-Task-1 才會擁有您在 logFormat 中所包含的 ECS 欄位的實際 ECS 中繼資料。對於 i-0000000 相關的流量，這些欄位的值為 '-'。
- 根據 VPC 流量日誌服務從 ECS 事件串流中接收到的順序對 ecs-container-id 和 ecs-second-container-id 進行排列。不保證它們與您在 ECS 主控台或 DescribeTask API 呼叫中看到的順序相同。如果容器在任務仍在執行時進入「已停止」狀態，它可能會繼續出現在您的日誌中。
- ECS 中繼資料和 IP 流量日誌來自兩個不同的來源。我們從上游相依項取得所有必要資訊後，即會開始計算您的 ECS 流量。

  啟動新任務後，我們會在滿足下列兩個條件時開始計算您的 ECS 欄位：我們會收到基礎網路界面的 IP 流量，而且我們會收到包含 ECS 任務中繼資料的 ECS 事件，以指出任務現在正在執行中。

在您停止任務後，我們會在滿足下列兩個條件時停止計算 ECS 欄位：我們不再接收基礎網路界面的 IP 流量（或我們接收延遲超過一天的 IP 流量），而且我們會收到包含 ECS 任務中繼資料的 ECS 事件，以指出您的任務不再執行。

- 僅支援以 awsvpc 網路模式啟動的 ECS 任務。

`encryption-status` 欄位特定的限制：

- 由於某些網路設備報告加密狀態的限制，某些流程中的加密狀態可能是 '-'（無法使用）。使用者可以在分析中忽略這些流程。
- 在監控模式中顯示為加密，並不表示流程會在強制執行模式中被允許。反之亦然。
  - 如果流程是在監控模式中加密，則在強制執行模式中可能不合規：
    - 如果流程涉及 AWS 服務建立的 ENI，則服務需要支援加密控制。
    - 如果流程通過 VPC 對等互連，對等 VPC 可能不會強制加密控制。
  - 如果流程未在監控模式下加密，則由於與流程相關的服務已新增為排除，因此在強制執行模式下可能仍然合規。

適用於第 11 版之 Flow Logs Amazon EC2 標籤欄位的特定限制：

- 如果資源上的標籤不是流程日誌訂閱擁有者所擁有，則不會計算標籤欄位。

  例如，假設您與其他帳戶 (SubnetA) 共用子網路 (AccountB)，然後為 在網路界面上建立SubnetA具有標籤欄位的 流程日誌訂閱。如果 使用您設定的金鑰AccountB啟動標記的網路界面，您的訂閱會收到由 啟動之網路界面的流量日誌AccountB，但由於安全性考量，不會計算您訂閱設定的標籤欄位。您可以標記 啟動的該網路界面AccountB，以在需要時顯示標籤。
- 如果您在 VPC/子網路資源層級使用標籤欄位建立流程日誌訂閱，則針對未標記的網路介面所產生的任何流量也會交付給您的訂閱。對於未標記的資源，標籤欄位的值將為 '-'。
- 如果標籤名稱為 '-'，Auto Scaling 群組將無法顯示任何標籤，因為這是表示缺少/沒有值的預留字元。
- 使用標籤欄位建立任何流程日誌訂閱將導致代表客戶建立幾個資源。為了使用標籤值的更新，將建立 EventBridge 受管規則，以將標籤變更傳送至 Flow Logs 服務。如果刪除具有標籤欄位的所有訂閱，這些 EventBridge 受管規則將自動清除。請勿手動刪除這些 EventBridge 受管規則。這樣做會導致大幅延遲更新標籤值。為了控制此建立/清除並提供標籤值的存取權，將在您的帳戶中建立服務連結角色。如需詳細資訊，請參閱使用 VPC 流程日誌的服務連結角色。

- 由於 Amazon CloudWatch Logs 剖析和 Athena 剖析限制，標籤值中的所有特殊字元都會使用 UTF-8% 編碼進行編碼。這可以在 Athena 中原生解碼，`url_decode`也可以由任何 URL 或 URI 解碼器解碼。
- 建立新訂閱後的第一個小時，標籤值可能遺失或不準確。第一個小時之後，標籤值將能夠以 1 分鐘的精細程度準確反映已標記資源的值。
- 如果在同一秒內對相同資源進行多個標籤變更，則可能會遺失更新，導致高達一小時的過時標籤值。
- 對於 Auto Scaling 群組標籤欄位，您的帳戶中必須至少有一個已啟用的 CloudTrail 追蹤。如果沒有啟用線索，Auto Scaling 群組標籤值可能會過時或不準確。

`next-hop-` 欄位特定的限制：

- 如果流程日誌訂閱的擁有者不擁有下一個躍點網路介面，則不會計算下一個躍點欄位，但 除外`next-hop-az-id`。
- 如果下一個躍點沒有網路介面，則無法使用下一個躍點欄位（例如，網際網路閘道的流量）。
- 下一個跳轉欄位不適用於跨區域流量。
- 下一個跳轉欄位不適用於來自某些網路服務的輸入流量（例如，傳輸閘道和 Network Load Balancer)。
- 如果流量通過中間設備（例如傳輸閘道或 Network Load Balancer)，則下一個跳轉網路界面是與中間設備（例如傳輸閘道連接）相關聯的界面，而不是流量的最終目的地

定價

當您發佈流程日誌時，會套用付費日誌的資料擷取和存檔費用。如需發佈付費記錄時的定價詳細資訊，請開啟 Amazon CloudWatch 定價，選取日誌並尋找付費記錄。

若要追蹤發佈流程日誌的費用，您可以將成本分配標籤套用至目的地資源。之後，您的 AWS 成本分配報告會包含這些標籤彙總的用量和成本。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，請參閱下列內容：

- AWS Billing User Guide 中的 Using Cost Allocation Tags
- Amazon CloudWatch Logs User Guide 中的 Tag log groups in Amazon CloudWatch Logs
- Amazon Simple Storage Service User Guide 中的 Using cost allocation S3 bucket tags
- Amazon Data Firehose Developer Guide 中的 Tagging Your Delivery Streams

使用流量日誌工作

您可以使用 Amazon EC2 和 Amazon VPC 的主控台來處理流程日誌。

任務

- 1. 使用 IAM 控制流量日誌的使用方式
- 2. 建立流量日誌
- 3. 標記流程日誌
- 4. 刪除流量日誌
- 命令列概觀

1. 使用 IAM 控制流量日誌的使用方式

根據預設，使用者沒有使用流程日誌的許可。您可以建立 IAM 角色，確保其連接的政策會將建立、描述和刪除流量日誌的許可授予使用者。

以下是授予使用者建立、描述、刪除流量日誌等完整許可的範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

如需詳細資訊，請參閱the section called “Amazon VPC 如何與 IAM 搭配運作”。

2. 建立流量日誌

您可以建立 VPC、子網或網路介面的流量日誌。建立流程日誌時，您必須指定流程日誌的目的地。如需詳細資訊，請參閱下列內容：

- the section called “建立發佈至 CloudWatch Logs 的流量日誌”
- the section called “建立發佈到 Amazon S3 的流量日誌”
- the section called “建立發布至 Amazon Data Firehose 的流量日誌”

3. 標記流程日誌

您可以隨時新增或移除流程日誌的標籤。

管理流程日誌的標籤

1. 執行以下任意一項：
   - 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)。選取網路介面的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)。選取 VPC 的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)。選取子網路的核取方塊。
2. 選擇 Flow Logs (流程日誌)。
3. 選擇 Actions (動作)、Manage tags (管理標籤)。
4. 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入金鑰和值。若要移除標籤，請選擇 Remove (移除)。
5. 當您完成新增或移除標籤時，請選擇 Save (儲存)。

4. 刪除流量日誌

您可以隨時刪除流程日誌。在您刪除流程日誌之後，它可能需要數分鐘的時間，才會停止收集資料。

刪除流程日誌並不會刪除目的地中的日誌資料或修改目的地資源。您必須使用目的地服務的主控台直接從目的地刪除現有流程日誌資料，並清理目的地資源。

刪除流程日誌

1. 執行以下任意一項：
   - 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)。選取網路介面的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)。選取 VPC 的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)。選取子網路的核取方塊。
2. 選擇 Flow Logs (流程日誌)。
3. 選擇 Actions (動作) 和 Delete flow logs (刪除流程日誌)。
4. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

命令列概觀

您可以使用命令列執行此頁面所述的任務。

建立流量日誌

- create-flow-logs (AWS CLI)
- 新的 EC2 流量日誌 (AWS Tools for Windows PowerShell)

描述流程日誌

- describe-flow-logs (AWS CLI)
- 獲得 EC2 流量日誌 (AWS Tools for Windows PowerShell)

標記流程日誌

- create-tags 和 delete-tags (AWS CLI)
- New-EC2Tag 和 Remove-EC2Tag (AWS Tools for Windows PowerShell)

刪除流量日誌

- delete-flow-logs (AWS CLI)
- 移除 EC2 流量日誌 (AWS Tools for Windows PowerShell)

將流量日誌發佈至 CloudWatch Logs

流量日誌可以將流量日誌資料直接發佈到 Amazon CloudWatch。Amazon CloudWatch 是全方位的監控和可觀測性服務。它從各種 AWS 資源以及您自己的應用程式和服務收集和追蹤指標、日誌和事件資料。CloudWatch 提供對資源使用率、應用程式效能和運作狀態的可見性，幫助您偵測和回應整個系統的效能變更和潛在問題。使用 CloudWatch，您可以設定警示、視覺化日誌和指標，並自動做出反應以收集和最佳化您的雲端資源。它是確保雲端基礎設施和應用程式的可靠性、可用性和效能的重要工具。

發佈至 CloudWatch Logs 時，流量日誌資料會發佈至日誌群組，以及該日誌群組中每個具有唯一日誌串流的網路介面。日誌串流包含流量日誌記錄。您可以建立多個流量日誌，將資料發佈至相同的日誌群組。若相同日誌群組中的一或多個流量日誌內存在相同的網路介面，它便會擁有一個合併日誌串流。若您指定其中一個流程日誌應擷取拒絕流量，並且指定其他流程日誌應擷取接受流量，則合併日誌串流便會擷取所有流量。

在 CloudWatch Logs 中，timestamp 欄位對應到流程日誌記錄中擷取的開始時間。ingestionTime 欄位指出 CloudWatch Logs 收到流量日誌記錄的日期和時間。這個時間戳記晚於流量日誌記錄中擷取的結束時間。

如需 CloudWatch Logs 的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的傳送至 CloudWatch Logs 的日誌。

定價

當您將流量日誌發佈到 CloudWatch Logs 時，會套用付費日誌的資料擷取和存檔費用。如需詳細資訊，請開啟 Amazon CloudWatch 定價，選取 Logs (日誌)，然後尋找 Vended Logs (付費日誌)。

目錄

- 用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色
- 建立發佈至 CloudWatch Logs 的流量日誌
- 檢視 CloudWatch Logs 中的流量日誌記錄
- 搜尋流量日誌記錄
- 處理 CloudWatch Logs 中的流量日誌記錄

用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色

與您流量日誌關聯的 IAM 角色必須具有足夠的許可，將流量日誌發佈到 CloudWatch Logs 中指定的日誌群組。IAM 角色必須屬於 AWS 您的帳戶。

與您 IAM 角色連線的 IAM 政策必須包含至少下列任一許可：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

確保您的角色具有下列信任政策，以允許流程日誌服務擔任角色。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

建議您使用 aws:SourceAccount 和 aws:SourceArn 條件金鑰，保護自己免受混淆代理人問題的困擾。例如，您可以將下列條件區塊新增至先前的信任政策。來源帳戶是流量日誌的擁有者，且來源

ARN 是流量日誌 ARN。如果您不清楚流量日誌 ID，您可以使用萬用字元 (*) 取代該部分的 ARN，然後在建立流量日誌之後更新政策。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

建立流程日誌的 IAM 角色

您可以如上所述更新現有的角色。或者，您可以使用下列程序建立新的角色以搭配流程日誌使用。您將在建立流程日誌時指定此角色。

建立流量日誌的 IAM 角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 在 Create policy (建立政策) 頁面上，執行下列動作：
   a. 選擇 JSON。
   b. 將此視窗的內容取代為本節開頭的許可政策。
   c. 選擇下一步。
   d. 輸入您的政策的名稱，以及可選的描述和標籤，然後選擇 建立政策。
5. 在導覽窗格中，選擇 Roles (角色)。
6. 選擇 Create Role (建立角色)。
7. 對於 Trusted entity type (信任的實體類型)，選擇 Custom trust policy (自訂信任政策)。對於 Custom trust policy (自訂信任政策)，將 `"Principal": {},` 取代為下列內容，然後選擇 Next (下一步)。

   ```
   "Principal": {
      "Service": "vpc-flow-logs.amazonaws.com"
   },
   ```

8. 在 Add permissions (新增許可) 頁面上，選取您先前在此程序中建立的政策的核取方塊，然後選擇 Next (下一步)。
9. 輸入您角色的名稱，然後選擇性提供描述。
10. 選擇 Create Role (建立角色)。

建立發佈至 CloudWatch Logs 的流量日誌

您可以建立 VPC、子網或網路介面的流量日誌。如果您以使用者身分使用特定 IAM 角色執行這些步驟，請確定此角色擁有使用 `iam:PassRole` 動作的許可。

先決條件

確認您用來發出請求的 IAM 主體擁有呼叫 `iam:PassRole` 動作的許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

使用主控台建立流程日誌

1. 執行以下任意一項：
   - 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)。選取網路介面的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)。選取 VPC 的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)。選取子網路的核取方塊。

2. 選擇 Actions (動作)、Create flow log (建立流量日誌)。
3. 對於 Filter (篩選條件)，請指定要記錄的流量類型。選擇 All (全部) 以記錄已接受和已拒絕的流量，選擇 Reject (拒絕) 以記錄僅拒絕的流量，或選擇 Accept (接受) 以記錄僅接受的流量。
4. 針對 Maximum aggregation interval (最大彙總時間間隔)，選擇擷取流量並彙總至一個流量日誌記錄的最長期間。
5. 針對 Destination (目標)，選擇 Send to CloudWatch Logs (傳送至 CloudWatch Logs)。
6. 對於 目的地日誌群組，請選擇現有日誌群組的名稱，或輸入新日誌群組名稱。如果您輸入名稱，我們會在需要記錄流量時建立日誌群組。
7. 在服務存取欄位中，選擇一個具備將日誌發布至 CloudWatch Logs 之許可的現有 IAM 服務角色，或選擇建立一個新的服務角色。
8. 對於 Log record format (日誌記錄格式)，請選取流量日誌記錄的格式。
   - 若要使用預設格式，請選擇 AWS default format (預設格式)。
   - 若要使用自訂格式，請選擇 Custom format (自訂格式)，然後從 Log format (日誌格式) 選取欄位。
9. 如果您想要包含 Amazon ECS 的日誌格式中繼資料，請選取其他中繼資料。
10. (選用) 選擇 Add new tag (新增標籤) 將標籤套用至流量日誌。
11. 選擇 Create flow log (建立流量日誌)。

使用命令列建立流量日誌

請使用下列其中一個命令。

- create-flow-logs (AWS CLI)
- 新的 EC2 流量日誌 (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立流程日誌，擷取指定子網路的所有已接受流量。流程日誌會交付至指定的日誌群組。`--deliver-logs-permission-arn` 參數指定發佈至 CloudWatch Logs 所需的 IAM 角色。

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

檢視 CloudWatch Logs 中的流量日誌記錄

您可以使用 CloudWatch Logs 主控台檢視流程日誌記錄。在您建立流程日誌之後，可能需要數分鐘的時間，才能在主控台中看到它。

使用主控台檢視發佈至 CloudWatch Logs 的流程日誌記錄

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中依序選擇 Logs (日誌)、Log groups (日誌群組)。
3. 選取包含您流程日誌的日誌群組的名稱，以開啟其詳細資訊頁面。
4. 選取包含流程日誌記錄的日誌串流的名稱。如需詳細資訊，請參閱流量日誌記錄。

使用命令列檢視發佈至 CloudWatch Logs 的流程日誌記錄

- get-log-events (AWS CLI)
- 獲得 CWL 日誌事件 (AWS Tools for Windows PowerShell)

搜尋流量日誌記錄

您可以使用 CloudWatch Logs 主控台，搜尋發佈至 CloudWatch Logs 的流程日誌記錄。您可以使用指標篩選條件來篩選流量日誌記錄。流量日誌記錄是以空格分隔。

使用 CloudWatch Logs 主控台搜尋流量日誌記錄

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中依序選擇 Logs (日誌)、Log groups (日誌群組)。
3. 如果您知道要搜尋的網路介面，請選取包含您流程日誌的日誌群組，然後選取日誌串流。或者，選擇 Search log group (搜尋日誌群組)。如果您的日誌群組中有許多網路介面，這可能需要一些時間，視您選取的時間範圍而定。
4. 在篩選事件下，輸入下面的字串。這會假設流量日誌記錄使用預設格式。

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
 packets, bytes, start, end, action, logstatus]
```

5. 根據需要透過指定欄位值來修改篩選條件。下列範例會依特定來源 IP 地址進行篩選。

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

```
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

下列範例會依目標連接埠、位元組數目，以及是否拒絕流量進行篩選。

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

處理 CloudWatch Logs 中的流量日誌記錄

在處理流量日誌記錄時，您可以您使用其他由 CloudWatch Logs 收集之日誌事件的相同方式。如需有關監控日誌資料與指標篩選條件的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用篩選條件根據日誌事件建立指標。

範例：建立流量日誌的 CloudWatch 指標篩選條件和警報

在此範例中，您有一個 `eni-1a2b3c4d` 的流量日誌。您希望建立警示，在 1 個小時期間內嘗試透過 TCP 連接埠 22 (SSH) 連線到您的執行個體，其中有 10 次或超過 10 次嘗試遭到拒絕時提醒您。首先，您必須建立符合要建立警示之流量模式的指標篩選條件。然後，您可以建立指標篩選條件的警示。

建立拒絕 SSH 流量的指標篩選條件，及建立篩選條件的警示

1. 前往 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中依序選擇 Logs (日誌)、Log groups (日誌群組)。
3. 選取日誌群組的核取方塊，然後選擇 Actions (動作)、Create metric filter (建立指標篩選條件)。
4. 針對 Filter Pattern (篩選條件模式)，請輸入下列字串。

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",
 packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. 對於 Select Log Data to Test (選取要測試的日誌資料)，選取網路介面的日誌串流。(選用) 若要檢視符合篩選條件模式的日誌資料行，請選擇 Test Pattern (測試模式)。
6. 就緒後，請選擇 Next (下一步)。
7. 輸入篩選條件名稱、指標命名空間和指標名稱。將指標值設定為 1。完成後，請選擇 Next (下一步)，然後選擇 Create metric filter (建立指標篩選條件)。

8. 在導覽窗格中，選擇 Alarms (警示)、All alarms (所有警示)。
9. 選擇 Create alarm (建立警示)。
10. 選取您建立的指標名稱，然後選擇 選取指標。
11. 如下設定警示，然後選擇 Next (下一步)。
    - 在 Statistic (統計資料) 中選擇 Sum (總和)。這可確保您擷取的是指定時間段的資料點總數。
    - 在 Period (時段) 中選擇 1 hour (1 小時)。
    - 在 只要 TimeSinceLastActive 為… 中，選擇 大於/等於，然後輸入 10 作為閾值。
    - 對於 Additional configuration (其他組態)、Datapoints to alarm (要警示的資料點)，保留預設值 1。
12. 選擇下一步。
13. 對於 Notification (通知)，請選取現有的 SNS 主題，或選擇 Create new topic (建立新主題) 來建立新主題。選擇下一步。
14. 輸入警示的名稱和說明，然後選擇 Next (下一步)。
15. 完成預覽警示之後，請選擇 建立警示。

將流量日誌發佈到 Amazon S3

流量日誌現在可將流量日誌資料發佈至 Amazon S3。Amazon S3 (Simple Storage Service) 是一項高度可擴展且持久的物件儲存服務。它旨在從 Web 上的任意位置儲存和擷取任何數量的資料。S3 提供業界領先的持久性和可用性，並內建資料版本控制、加密以及存取控制等功能。

當發佈至 Amazon S3 時，流程日誌資料將發佈至您指定的現有 Amazon S3 儲存貯體。所有受監控之網路介面的流量日誌記錄，都將發佈至存放在該儲存貯體的一系列日誌檔案物件。如果流量日誌擷取 VPC 的資料，該流量日誌將發佈所選擇之 VPC 中所有網路介面的流量日誌記錄。

若要建立用於流量日誌的 Amazon S3 儲存貯體，請參閱《Amazon S3 使用者指南》中的建立儲存貯體。

如需了解有關簡化 VPC 流量日誌擷取、流量日誌處理和流量日誌視覺化的詳細資訊，請參閱 AWS 解決方案程式庫中的使用 OpenSearch 的集中式日誌。

如需 CloudWatch Logs 的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的傳送至 Simple Storage Service (Amazon S3) 的日誌。

定價

當您將流量日誌發佈到 Amazon S3 時，會套用付費日誌的資料擷取和存檔費用。如需詳細資訊，請開啟 Amazon CloudWatch 定價，選取 Logs (日誌)，然後尋找 Vended Logs (付費日誌)。

目錄

- 流量日誌檔
- 流量日誌的 Amazon S3 儲存貯體許可
- 搭配 SSE-KMS 使用的必要金鑰政策
- Amazon S3 日誌檔案許可
- 建立發佈到 Amazon S3 的流量日誌
- 使用 Amazon S3 檢視流量日誌記錄

流量日誌檔

VPC 流量日誌會將進出您 VPC 的 IP 流量資料收集到日誌記錄，然後將這些記錄彙整成日誌檔案，並每隔 5 分鐘將日誌檔案發布至 Amazon S3 儲存貯體。可能會發布多個檔案，每個日誌檔案可能包含先前 5 分鐘內記錄之 IP 流量的部分或全部流量日誌記錄。

在 Amazon S3 中，流量日誌檔案的上次修改欄位指出檔案上傳至 Amazon S3 儲存貯體的日期和時間。這個時間晚於檔案名稱中的時間戳記，並且會因檔案上傳至 Amazon S3 儲存貯體所花費的時間而有所不同。

日誌檔案格式

可為日誌檔案指定下列其中一種格式。每個檔案都會壓縮到單一 Gzip 檔案中。

- Text – 純文字。此為預設格式。
- Parquet – Apache Parquet 是一種單欄資料格式。與純文字的資料查詢相比，Parquet 格式的資料查詢速度快 10 到 100 倍。採用 Gzip 壓縮的 Parquet 格式的資料佔用的儲存空間比使用 Gzip 壓縮的純文字要少 20%。

> **Note**
>
> 如果每個彙總期間採用 Gzip 壓縮的 Parquet 格式之資料小於 100 KB，由於採用 Parquet 檔案記憶體的要求，採用 Parquet 格式儲存的資料可能會比 Gzip 壓縮的純文字檔案佔用更多的空間。

日誌檔案選項

您可以選擇指定下列項目。

- Hive 兼容的 S3 前綴 – 啟用 Hive 相容的前置詞，而不是將分割區匯入 Hive 相容的工具。在執行查詢之前，請使用 MSCK REPAIR TABLE 命令。
- 每小時分割 – 如果您有大量的日誌，而且通常針對特定小時進行查詢，則透過每小時分割日誌，可獲得更快的結果並節省查詢成本。

日誌檔案 S3 儲存貯體結構

使用基於流量日誌的 ID、區域、建立日期以及目標選項的資料夾架構，將日誌檔案儲存至指定的 Amazon S3 儲存貯體。

根據預設，檔案會傳遞至下列位置。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

如果您啟用 Hive 相容的 S3 字首，檔案會傳遞至下列位置。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

如果您啟用每小時分割，檔案會傳遞到下列位置。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

如果您啟用 Hive 相容的分割，並且每小時分割流量日誌，檔案會傳遞至下列位置。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

日誌檔案名稱

日誌檔案的檔案名稱以流量日誌 ID、區域以及建立日期和時間為基礎。檔案名稱使用下列格式。

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

以下是 AWS 帳戶 123456789012 針對 us-east-1 區域中的資源，在 June 20, 2018 的 16:20 UTC 建立的流量日誌的日誌檔案範例。檔案包含結束時間介於 16:20:00 和 16:24:59 的流量日誌記錄。

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

流量日誌的 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，將存取權授予其他資源和使用者。

如果建立流量日誌的使用者擁有儲存貯體且具有該儲存貯體的 PutBucketPolicy 和 GetBucketPolicy 許可，我們就會自動將以下政策連接至該儲存貯體。此政策會覆寫附加至儲存貯體的任何現有政策。

否則，儲存貯體擁有者必須將此政策新增至儲存貯體、指定流量日誌建立者的 AWS 帳戶 ID，否則流量日誌會建立失敗。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的「使用儲存貯體政策」。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

您為 *my-s3-arn* 指定的 ARN 取決於您是否使用與 Hive 相容的 S3 字首。

- 預設字首

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- 與 Hive 相容的 S3 字首

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

最佳實務是將這些許可授予日誌交付服務委託人，而不是個別 AWS 帳戶 ARNs。這也是使用 `aws:SourceAccount` 和 `aws:SourceArn` 條件金鑰來保護自己免受混淆代理人問題的困擾之最佳實務。來源帳戶是流量日誌的擁有者，且來源 ARN 是日誌服務的萬用字元 (*) ARN。

請注意，日誌交付服務會呼叫 `HeadBucket` Amazon S3 API 動作，驗證 S3 儲存貯體的存續狀態與位置。您不需要授予日誌交付服務呼叫此動作的許可。即使無法確認 S3 儲存貯體是否存在，服務仍會交付 VPC 流程日誌。不過，CloudTrail 日誌中會針對該次 `HeadBucket` 呼叫，記錄一項 `AccessDenied` 錯誤。

搭配 SSE-KMS 使用的必要金鑰政策

透過在 S3 儲存貯體上，啟用採用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密，或採用 KMS 金鑰 (SSE-KMS) 的伺服器端加密，您可以保護 Amazon S3 儲存貯體中的資料。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的使用伺服器端加密保護資料。

如果您選擇 SSE-S3，則不需要其他組態。Amazon S3 會處理加密金鑰。

若您選擇 SSE-KMS，則必須使用客戶受管金鑰 ARN。如果您使用金鑰 ID，您可能會在建立流程日誌時遇到 LogDestination 無法傳遞 錯誤。此外，您必須更新客戶受管金鑰的金鑰政策，以讓日誌傳遞帳戶能夠寫入您的 S3 儲存貯體。如需有關 SSE-KMS 所需金鑰政策的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的 Amazon S3 儲存貯體伺服器端加密。

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) 來管理流量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《Amazon S3 使用者指南》中的存取控制清單 (ACL) 概覽。

建立發佈到 Amazon S3 的流量日誌

建立並設定您的 Amazon S3 儲存貯體後，您可以建立網路介面、子網以及 VPC 的流量日誌。

必要條件

建立流量日誌的 IAM 主體必須使用具有以下許可的 IAM 角色，才能將流量日誌發佈至目的地 Amazon S3 儲存貯體。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

使用主控台建立流程日誌

1. 執行以下任意一項：
   - 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)。選取網路介面的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)。選取 VPC 的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)。選取子網路的核取方塊。
2. 選擇 Actions (動作)、Create flow log (建立流量日誌)。
3. 在 Filter (篩選條件) 中指定要記錄的 IP 流量資料類型。
   - 接受 – 僅記錄接受的流量
   - 拒絕 – 僅記錄拒絕的流量
   - 全部 – 記錄已接受和已拒絕的流量。
4. 針對 Maximum aggregation interval (最大彙總時間間隔)，選擇擷取流程並彙總至一個流程日誌記錄的最長期間。
5. 針對目的地，選擇傳送至 Amazon S3 儲存貯體。
6. 針對 S3 儲存貯體 ARN，指定現有 Amazon S3 儲存貯體的 Amazon Resource Name (ARN)。您可以選擇包含子資料夾。例如，若要指定名為 `my-logs` 之儲存貯體中的 `my-bucket` 子資料夾，請使用以下 ARN 格式：

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

   儲存貯體不可使用 `AWSLogs` 做為子資料夾名稱，因為這是保留項目。

   若您擁有儲存貯體，我們會自動建立資源政策並將它連接至儲存貯體。如需詳細資訊，請參閱流量日誌的 Amazon S3 儲存貯體許可。
7. 對於 Log record format (日誌記錄格式)，請指定流量日誌記錄的格式。
   - 若要使用預設的流量日誌紀錄格式，請選擇 AWS default format (預設格式)。
   - 若要建立自訂格式，請選擇 Custom format (自訂格式)。針對 Log format (日誌格式)，請選擇要包含在流量日誌記錄中的欄位。

8. 如果您想要包含 Amazon ECS 的日誌格式中繼資料，請選取其他中繼資料。
9. 對於 Log file format (日誌檔案格式)，指定日誌檔案的格式。
   - Text – 純文字。此為預設格式。
   - Parquet – Apache Parquet 是一種單欄資料格式。與純文字的資料查詢相比，Parquet 格式的資料查詢速度快 10 到 100 倍。採用 Gzip 壓縮的 Parquet 格式的資料佔用的儲存空間比使用 Gzip 壓縮的純文字要少 20%。
10. (選用) 若要使用 Hive 相容的 S3 字首，請選擇 Hive-compatible S3 prefix (Hive 相容的 S3 字首)、Enable (啟用)。
11. (選用) 若要每小時分割流量日誌，請選擇 Every 1 hour (60 mins) (每 1 小時 (60 分鐘))。
12. (選用) 若要新增標籤至流量日誌，請選擇 Add new tag (新增新標籤)，並指定標籤金鑰和值。
13. 選擇 Create flow log (建立流程日誌)。

透過命令列建立可發布至 Amazon S3 的流量日誌

請使用以下其中一個命令：

- create-flow-logs (AWS CLI)
- 新的 EC2 流量日誌 (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立流程日誌，擷取指定 VPC 的所有流量，並將流程日誌交付至指定的 Amazon S3 儲存貯體。`--log-format` 參數會指定流量日誌記錄的自訂格式。

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

使用 Amazon S3 檢視流量日誌記錄

您可以使用 Amazon S3 主控台檢視您的流程日誌記錄。在您建立流程日誌之後，可能需要數分鐘的時間，才能在主控台中看到它。

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，並顯示流量日誌記錄。如果您下載這些檔案，則必須解壓縮才能檢視流量日誌記錄。

檢視發佈至 Amazon S3 的流量日誌記錄

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選取儲存貯體的名稱，開啟其詳細資訊頁面。
3. 導覽至包含日誌檔的資料夾。例如，*prefix*/AWSLogs/*account_id*/vpcflowlogs/*region*/*year*/*month*/*day*/。
4. 選取檔案名稱旁邊的核取方塊，然後選擇 Download (下載)。

您也可以使用 Amazon Athena 查詢日誌檔案中的流量日誌記錄。Amazon Athena 是一種互動式查詢服務，可讓您使用標準 SQL 輕鬆分析 Amazon S3 中的資料。如需詳細資訊，請參閱《Amazon Athena 使用者指南》中的查詢 Amazon VPC 流量日誌。

將流量日誌發布至 Amazon Data Firehose

流量日誌可以將流量日誌資料直接發佈至 Amazon Data Firehose。Amazon Data Firehose 是一項全受管服務，可收集、轉換並交付即時資料串流至各種 AWS 資料存放區和分析服務。它還能代表您處理資料擷取。

當涉及 VPC 流量日誌時，Firehose 是非常實用的工具。VPC 流量日誌可擷取您 VPC 中傳入和傳出網路界面之 IP 流量資訊。這些資料對於安全監控、效能分析以及遵循法規要求至關重要。然而，管理這種連續的日誌資料流的儲存和處理可能是一項複雜且佔用資源的任務。

透過將 Firehose 與 VPC 流量日誌整合起來，您可以將這些資料交付至偏好的目的地，例如 Amazon S3 或 Amazon Redshift。Firehose 能夠擴展以處理 VPC 流量日誌的擷取、轉換和交付工作，減輕您的營運負擔。這讓您可以專注於分析日誌和取得洞察，而不用擔心基礎設施。

此外，Firehose 提供資料轉換、壓縮和加密等功能，可提升 VPC 流量日誌處理管道的效率和安全性。使用 Firehose 來處理 VPC 流量日誌，可以簡化資料管理，幫助您從網路流量資料中取得洞察。

發布至 Amazon Data Firehose 時，流程日誌資料會以純文字格式發佈至 Amazon Data Firehose 交付串流。

定價

需支付標準擷取和交付費用。如需詳細資訊，請開啟 Amazon CloudWatch 定價，選取 Logs (日誌)，然後尋找 Vended Logs (付費日誌)。

目錄

- 跨帳戶交付的 IAM 角色

- 建立發布至 Amazon Data Firehose 的流量日誌

跨帳戶交付的 IAM 角色

發佈至 Amazon Data Firehose 時，您可以選擇與要監控的資源位於同一帳戶 (來源帳戶) 或不同帳戶 (目的地帳戶) 中的交付串流。若要啟用跨帳戶將流程日誌交付至 Amazon Data Firehose，必須在來源帳戶中建立 IAM 角色，並在目的地帳戶中建立 IAM 角色。

角色

- 來源帳戶角色
- 目的地帳戶角色

來源帳戶角色

在來源帳戶中，建立授予下列許可的角色。在此範例中，角色的名稱是 `mySourceRole`，但您可以為此角色選擇其他名稱。最後一個陳述式允許目的地帳戶中的角色擔任此角色。條件陳述式可確保此角色僅傳遞至日誌交付服務，而且只有在監控指定的資源時才會傳遞。建立政策時，請使用條件金鑰 `iam:AssociatedResourceARN` 指定要監控的 VPC、網路介面或子網路。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-00112233344556677"
                    ]
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

確保此角色具有下列信任政策，以允許日誌交付服務擔任角色。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

在來源帳戶，使用下列程序建立角色。

建立來源帳戶角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 在 Create policy (建立政策) 頁面上，執行下列動作：
   a. 選擇 JSON。
   b. 將此視窗的內容取代為本節開頭的許可政策。
   c. 選擇下一步。
   d. 輸入您的政策的名稱，以及可選的描述和標籤，然後選擇 建立政策。
5. 在導覽窗格中，選擇 Roles (角色)。
6. 選擇 Create Role (建立角色)。
7. 對於 Trusted entity type (信任的實體類型)，選擇 Custom trust policy (自訂信任政策)。對於 Custom trust policy (自訂信任政策)，將 `"Principal": {},` 取代為下列內容，以指定日誌交付服務。選擇下一步。

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. 在 Add permissions (新增許可) 頁面上，選取您先前在此程序中建立的政策的核取方塊，然後選擇 Next (下一步)。
9. 輸入您角色的名稱，然後選擇性提供描述。
10. 選擇 Create Role (建立角色)。

目的地帳戶角色

在目的地帳戶中，建立名稱開頭為 AWSLogDeliveryFirehoseCrossAccountRole 的角色。此角色必須授予下列許可。

JSON

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

請確保此角色具有下列信任政策，可讓您在來源帳戶中建立的角色擔任此角色。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

透過目的地帳戶，使用下列程序建立角色。

建立目的地帳戶角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 在 Create policy (建立政策) 頁面上，執行下列動作：

    a. 選擇 JSON。

b. 將此視窗的內容取代為本節開頭的許可政策。

c. 選擇下一步。

d. 輸入您政策的名稱 (開頭為 AWSLogDeliveryFirehoseCrossAccountRole)，然後選擇 Create policy (建立政策)。

5. 在導覽窗格中，選擇 Roles (角色)。
6. 選擇 Create Role (建立角色)。
7. 對於 Trusted entity type (信任的實體類型)，選擇 Custom trust policy (自訂信任政策)。對於 Custom trust policy (自訂信任政策)，將 `"Principal": {},` 取代為下列內容，以指定來源帳戶角色。選擇下一步。

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. 在 Add permissions (新增許可) 頁面上，選取您先前在此程序中建立的政策的核取方塊，然後選擇 Next (下一步)。
9. 輸入您角色的名稱，然後選擇性提供描述。
10. 選擇 Create Role (建立角色)。

建立發布至 Amazon Data Firehose 的流量日誌

您可以建立 VPC、子網或網路介面的流量日誌。

先決條件

- 建立目的地 Amazon Data Firehose 交付串流。使用 Direct Put 作為來源。如需詳細資訊，請參閱建立 Amazon Data Firehose 交付串流。
- 建立流程日誌的帳戶必須使用授予下列許可的 IAM 角色，以將流程日誌發佈至 Amazon Data Firehose。

  JSON

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

```
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "iam:CreateServiceLinkedRole",
                "firehose:TagDeliveryStream"
            ],
            "Resource": "*"
        }
    ]
}
```

- 如果您要將流程日誌發佈至其他帳戶，請如 the section called “跨帳戶交付的 IAM 角色” 所述建立所需的 IAM 角色。

建立發佈至 Amazon Data Firehose 的流量日誌

1. 執行以下任意一項：
   - 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)。選取網路介面的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)。選取 VPC 的核取方塊。
   - 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)。選取子網路的核取方塊。
2. 選擇 Actions (動作)、Create flow log (建立流量日誌)。
3. 對於 Filter (篩選條件)，請指定要記錄的流量類型。
   - Accept (接受) – 僅記錄接受的流量
   - Reject (拒絕) – 僅記錄拒絕的流量
   - All (全部) – 記錄已接受和已拒絕的流量
4. 針對 Maximum aggregation interval (最大彙總時間間隔)，選擇擷取流量並彙總至一個流量日誌記錄的最長期間。
5. 針對 Destination (目的地)，選擇下列其中一個選項：
   - 在同一帳戶中傳送至 Amazon Data Firehose – 交付串流和要監控的資源在同一帳戶中。
   - 在不同帳戶中傳送至 Amazon Data Firehose – 交付串流和要監控的資源在不同帳戶中。
6. 在 Amazon Data Firehose 串流名稱中，選擇您建立的交付串流。
7. 【僅限跨帳戶交付】 針對服務存取，選擇具有發佈日誌許可的現有 IAM 服務角色進行跨帳戶交付。或者，選擇設定許可以開啟 IAM 主控台並建立服務角色。

8. 對於 Log record format (日誌記錄格式)，請指定流量日誌記錄的格式。
   - 若要使用預設的流量日誌紀錄格式，請選擇 AWS default format (預設格式)。
   - 若要建立自訂格式，請選擇 Custom format (自訂格式)。針對 Log format (日誌格式)，請選擇要包含在流量日誌記錄中的欄位。
9. 如果您想要包含 Amazon ECS 的日誌格式中繼資料，請選取其他中繼資料。
10. (可選) 選擇 標籤 將標籤套用至流量日誌。
11. 選擇 Create flow log (建立流量日誌)。

透過命令列建立可發布至 Amazon Data Firehose 的流量日誌

請使用以下其中一個命令：

- create-flow-logs (AWS CLI)
- 新的 EC2 流量日誌 (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立流程日誌，擷取指定 VPC 的所有流量，並將流程日誌交付至相同帳戶中指定的 Amazon Data Firehose 交付串流。

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream
```

下列 AWS CLI 範例會建立流程日誌，擷取指定 VPC 的所有流量，並將流程日誌交付至不同帳戶中指定的 Amazon Data Firehose 交付串流。

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

由於您已建立流量日至，您可以從為交付串流設定的目的地取得流量日誌資料。

使用 Amazon Athena 查詢流量日誌

Amazon Athena 是一種互動式查詢服務，可讓您使用標準 SQL 分析 Amazon S3 中的資料，例如流量日誌。您可以將 Athena 與 VPC 流量日誌搭配使用，以快速取得關於流經 VPC 流量的可行見解。例如，您可以識別 Virtual Private Cloud (VPC) 中的哪些資源是最受歡迎者，或識別具有最多拒絕 TCP 連線的 IP 地址。

選項

- 您可以簡化和自動化 VPC 流程日誌與 Athena 的整合。產生 CloudFormation 範本，建立必要的 AWS 資源和預先定義的查詢，以取得流經 VPC 之流量的洞見。
- 您可以使用 Athena 建立自己的查詢。如需詳細資訊，請參閱《Amazon Athena 使用者指南》中的「使用 Amazon Athena 查詢流量日誌」。

定價

您需要針對執行查詢產生標準的 Amazon Athena 費用。Lambda 函數會產生標準的 AWS Lambda 費用，該函數會按照週期性排程載入新的分割區（當您指定分割區載入頻率，但未指定開始和結束日期時）。

使用預先定義的查詢

- 使用主控台產生 CloudFormation 範本
- 使用 產生 CloudFormation 範本 AWS CLI
- 執行預先定義的查詢

使用主控台產生 CloudFormation 範本

在第一個流程記錄傳遞至 S3 儲存貯體後，您可以產生 CloudFormation 範本並使用範本建立堆疊，與 Athena 整合。

要求

- 選取的區域必須支援 AWS Lambda 和 Amazon Athena。
- Amazon S3 儲存貯體必須位於選取的區域。
- 流量日誌的日誌記錄格式必須包含您想要執行的特定預先定義查詢所用的欄位。

使用主控台產生範本

1. 請執行下列其中一項：
   - 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Your VPCs (您的 VPC)，然後選擇您的 VPC。
   - 開啟 Amazon VPC 主控台。在導覽窗格中，選擇 Subnets (子網)，然後選取您的子網。
   - 開啟 Amazon EC2 主控台。在導覽窗格中，選擇 Network Interfaces (網路介面)，然後選取網路介面。
2. 在 Flow logs (流量日誌)索引標籤上，選取發佈至 Amazon S3 的流量日誌，然後選擇 Actions (動作)、Generate Athena integration (產生 Athena 整合)。
3. 指定分割區載入頻率。如果您選擇 None (無)，則必須使用過去的日期來指定分割區的開始日期和結束日期。如果您選擇 Daily (每日)、Weekly (每週) 或 Monthly (每月)，分割區的開始日期和結束日期是選擇性的。如果您沒有指定開始和結束日期，CloudFormation 範本會建立 Lambda 函式，在週期性排程載入新的分割區。
4. 為產生的範本選取或建立 S3 儲存貯體，並為查詢結果選取或建立 S3 儲存貯體。
5. 選擇 Generate Athena integration (產生 Athena 整合)。
6. （選擇性）在成功訊息中，選擇連結以瀏覽至您為 CloudFormation 範本指定的儲存貯體，然後自訂範本。
7. 在成功訊息中，選擇建立 CloudFormation 堆疊以在 CloudFormation 主控台中開啟建立堆疊精靈。產生的 CloudFormation 範本的 URL 會在 Template (範本) 區段中指定。完成精靈以建立範本中指定的資源。

由 CloudFormation 範本建立的資源

- Athena 資料庫。資料庫名為 vpcflowlogsathenadatabase<flow-logs-subscription-id>。
- Athena 工作群組。工作群組名稱為 <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup
- 分割的 Athena 資料表，對應至您的流量日誌記錄。資料表名稱為 <flow-log-subscription-id><partition-load-frequency><start-date><end-date>。
- 一組以 Athena 命名的查詢。如需更多詳細資訊，請參閱 預先定義的查詢。
- Lambda 函數，可將新的磁碟分割載入至表格，依照指定的排程（每日、每週或每月）。
- 授與執行 Lambda 函數的許可的 IAM 角色。

使用 產生 CloudFormation 範本 AWS CLI

在第一個流量日誌傳遞至 S3 儲存貯體後，您可以產生並使用 CloudFormation 範本來與 Athena 整合。

使用下列 get-flow-logs-integration-template 命令產生 CloudFormation 範本。

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

以下是 config.json 檔案的範例。

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
        ]
    }
}
```

使用下列 create-stack 命令，使用產生的 CloudFormation 範本建立一個堆疊。

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

執行預先定義的查詢

產生的 CloudFormation 範本提供一組預先定義的查詢，您可以執行這些查詢，以便快速取得關於 AWS 網路中流量的有意義洞見分析。建立堆疊並確認已正確建立所有資源之後，您可以執行其中一個預先定義的查詢。

使用主控台執行預先定義的查詢

1. 開啟 Athena 主控台。

2. 在左邊導覽中，選擇 Query Editor (查詢編輯器)。在 Workgroups (工作群組) 下，選取由 CloudFormation 範本建立的工作群組。
3. 選取已儲存的查詢，選取一個查詢，視需要修改參數，然後執行查詢。如需可用的預先定義查詢清單，請參閱預先定義的查詢。
4. 在查詢結果下，檢視查詢結果。

預先定義的查詢

以下是 Athena 命名查詢的完整清單。產生範本時提供的預先定義查詢，視流量日誌記錄格式中的一部分欄位而定。因此，範本可能未包含所有這些預先定義的查詢。

- VpcFlowLogsAcceptedTraffic - 根據您的安全群組和網路 ACL 所允許的 TCP 連線。
- VpcFlowLogsAdminPortTraffic – 在管理連接埠上服務請求的應用程式所記錄之流量最多的前 10 個 IP 地址。
- VpcFlowLogsIPv4Traffic - 所記錄的 IPv4 流量總位元組數。
- VpcFlowLogsIPv6Traffic - 記錄 IPv6 流量的總位元組數。
- VpcFlowLogsRejectedTCPTraffic - 根據您的安全群組或網路 ACL 拒絕的 TCP 連線。
- VpcFlowLogsRejectedTraffic - 根據您的安全群組或網路 ACL 拒絕的流量。
- VpcFlowLogsSshRdpTraffic - SSH 和 RDP 流量。
- VpcFlowLogsTopTalkers - 記錄流量最多的 50 個 IP 地址。
- VpcFlowLogsTopTalkersPacketLevel - 50 個封包層級的 IP 地址，其記錄的流量最多。
- VpcFlowLogsTopTalkingInstances - 擁有記錄最多流量的 50 個執行個體的 ID。
- VpcFlowLogsTopTalkingSubnets - 擁有記錄最多流量的 50 個子網的 ID。
- VpcFlowLogsTopTCPTraffic - 針對來源 IP 地址所記錄的所有 TCP 流量。
- VpcFlowLogsTotalBytesTransferred - 已記錄最多位元組數的 50 組來源和目的地 IP 地址。
- VpcFlowLogsTotalBytesTransferredPacketLevel - 50 對的封包層級來源和目的地 IP 地址，其中記錄了最多位元組數。
- VpcFlowLogsTrafficFrmSrcAddr - 針對特定來源 IP 地址所記錄的流量。
- VpcFlowLogsTrafficToDstAddr - 針對特定目的地 IP 地址所記錄的流量。

VPC 流程日誌中的身分和存取管理

AWS 使用安全登入資料來識別您的身分，並授予您存取 資源 AWS 的權限。您可以使用 AWS Identity and Access Management (IAM) 的功能，允許其他使用者、服務和應用程式完整或有限地使用您的 AWS 資源，而無需共用您的安全登入資料。

本節說明專為 VPC Flow Logs 建立 AWS 的服務連結角色，以及連接至 VPC Flow Logs 服務連結角色的受管政策。如需有關 AWS IAM 角色和政策的詳細資訊，請參閱《IAM 使用者指南》中的角色術語和概念。

如需有關 VPC 身分與存取管理的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 的身分和存取管理。

目錄

- 使用 VPC 流程日誌的服務連結角色
- AWS VPC 流程日誌的 受管政策

使用 VPC 流程日誌的服務連結角色

VPC 流程日誌使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 VPC 流程日誌的唯一 IAM 角色類型。服務連結角色由 VPC 流程日誌預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 VPC 流程日誌，因為您不必手動新增必要的許可。VPC Flow Logs 會定義其服務連結角色的許可，除非另有定義，否則只有 VPC Flow Logs 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 VPC Flow Logs 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

VPC 流程日誌的服務連結角色許可

VPC Flow Logs 使用名為 AWSServiceRoleForVPCFlowLogs 的服務連結角色 – 此服務連結角色可讓 VPC Flow Logs 建立和管理 EventBridge 受管規則，並代您呼叫 DescribeTag APIs以在包含標籤欄位的 Flow Logs 訂閱下自動追蹤與資源相關聯的 EC2 標籤值更新。

AWSServiceRoleForVPCFlowLogs 服務連結角色信任下列服務擔任該角色：

- `vpc-flow-logs.amazonaws.com`

名為 AWSVPCFlowLogsServiceRolePolicy 的角色許可政策允許 VPC 流程日誌對指定的資源完成下列動作：

- 動作：在 EC2 Autoscaling 群組`autoscaling:DescribeTags`上驗證標籤值。

  動作：在 EC2 執行個體和 ElasticNetworkInterfaces `tag:GetResources`上驗證標籤值。

  動作：針對來自來源`events:PutRule`的新受管規則`aws.autoscaling`，`aws.tag`以及與標籤變更事件相關的詳細資訊類型。

  動作：在名為 VPCFlowLogsEC2TagsManagedRule和/或 的 VPC 流程日誌建立的受管規則`events:DeleteRule`上VPCFlowLogsASGTagsManagedRule。

  動作：在名為 VPCFlowLogsEC2TagsManagedRule和/或 的 VPC 流程日誌建立的受管規則`events:DescribeRule`上VPCFlowLogsASGTagsManagedRule。

  動作：在名為 VPCFlowLogsEC2TagsManagedRule和/或 的 VPC 流程日誌建立的受管規則`events:PutTargets`上VPCFlowLogsASGTagsManagedRule。

  動作：在名為 VPCFlowLogsEC2TagsManagedRule和/或 的 VPC 流程日誌建立的受管規則`events:RemoveTargets`上VPCFlowLogsASGTagsManagedRule。

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 VPC 流程日誌建立服務連結角色

您不需要手動建立服務連結角色，當您使用日誌格式的標籤欄位和 AWS CLI、 或 AWS API AWS 管理主控台中的相關聯 TagFieldSpecifications 參數CreateFlowLogs時，VPC Flow Logs 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 中出現的新角色 AWS 帳戶。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您使用日誌格式的標籤欄位和相關聯的 TagFieldSpecifications 參數來 CreateFlowLogs 時，VPC Flow Logs 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台建立具有 AWSServiceRoleForVPCFlowLogs 使用案例的服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立`vpc-flow-logs.amazonaws.com`服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 VPC 流程日誌的服務連結角色

VPC 流程日誌不允許您編輯 AWSServiceRoleForVPCFlowLogs 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。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 VPC 流程日誌的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果您嘗試刪除資源時，VPC Flow Logs 服務正在使用 角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForVPCFlowLogs 使用的 VPC 流程日誌資源

1. 刪除以日誌格式使用標籤欄位的所有 VPC Flow Logs 訂閱。
2. 等待至少一個小時讓 VPC 流程日誌處理您帳戶的所有標籤訂閱都已刪除，並自動清除為支援日誌擴充而建立的 EventBridge 受管規則。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForVPCFlowLogs 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

VPC Flow Logs 服務連結角色的支援區域

VPC 流程日誌不支援在提供服務的每個區域中使用服務連結角色。您可以在下列區域中使用 AWSServiceRoleForVPCFlowLogs 角色。

區域名稱	區域身分	VPC 流程日誌中的支援
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
Africa (Cape Town)	af-south-1	是
亞太地區 (香港)	ap-east-1	是
亞太地區 (雅加達)	ap-southeast-3	是
亞太區域 (孟買)	ap-south-1	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (米蘭)	eu-south-1	是
歐洲 (巴黎)	eu-west-3	是
Europe (Stockholm)	eu-north-1	是

區域名稱	區域身分	VPC 流程日誌中的支援
Middle East (Bahrain)	me-south-1	是
中東 (阿拉伯聯合大公國)	me-central-1	是
南美洲 (聖保羅)	sa-east-1	是
AWS GovCloud (US-East)	us-gov-east-1	是
AWS GovCloud （美國西部）	us-gov-west-1	是

AWS VPC 流程日誌的 受管政策

如果您使用 VPC 流程日誌，並建立具有標籤欄位和相關聯 TagFieldSpecifications 參數的訂閱，則 AWSVPCFlowLogsServiceRolePolicy 受管政策會自動建立在您的 IAM 帳戶中，並連接到 AWSServiceRoleForVPCFlowLogs 服務連結角色。

此受管政策可讓 VPC 流程日誌執行下列動作：

- 建立和管理 EventBridge 受管規則，將標籤更新事件傳送至 VPC Flow Logs 服務。
- 代表客戶呼叫 APIs，以驗證日誌擴充的標籤值新鮮度。

下例顯示建立之受管政策的詳細資訊。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
            "Effect": "Allow",
            "Action": "events:PutRule",
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
```

```
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.tag",
                        "aws.autoscaling"
                    ],
                    "events:detail-type": [
                        "AWS API Call via CloudTrail",
                        "Tag Change on Resource"
                    ]
                },
                "Null": {
                    "events:source": "false",
                    "events:detail-type": "false"
                },
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowDescribeTagsOnAllEC2Resources",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources",
                "autoscaling:DescribeTags"
```

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

上述範例中的第一個陳述式可讓 VPC Flow Logs 在 AWS 您的帳戶中為來源aws.tag和標籤變更事件相關的詳細資訊類型建立 EventBridge aws.autoscaling 受管規則。

上述範例中的第二個陳述式可讓 VPC Flow Logs 控制您 AWS 帳戶中建立的受管規則生命週期，以取得名為 VPCFlowLogsEC2TagsManagedRule和/或 的資源VPCFlowLogsASGTagsManagedRule。

上述範例中的第三個陳述式可讓 VPC Flow Logs 代表客戶呼叫標籤 APIs，以驗證日誌擴充的標籤值新鮮度。

AWS 受管政策：AWSVPCFlowLogsServiceRolePolicy

您可將 AWSVPCFlowLogsServiceRolePolicy 政策連接到 IAM 身分。此政策授予許可，讓 VPC Flow Logs 能夠建立和管理 EventBridge 受管規則，並代表您呼叫 DescribeTag APIs，以自動追蹤與包含標籤欄位之 Flow Logs 訂閱下資源相關聯的 EC2 標籤值更新。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AWSVPCFlowLogsServiceRolePolicy。

AWS 受管政策的更新

檢視自此服務開始追蹤這些變更以來，VPC Flow Logs AWS 受管政策更新的詳細資訊。

變更	描述	日期
the section called “AWSVPCFlowLogsServiceRolePolicy ” – 新政策	新的 AWSVPCFlowLogsServiceRolePolicy 政策可讓 VPC Flow Logs 建立和管理 EventBridge 受管規則，並代表您呼叫 DescribeTag APIs，以在包含標籤欄位的 Flow Logs 訂閱下自動追蹤與資源相關聯的 EC2 標籤值更新。	2026 年 3 月 31 日
VPC 流程日誌已開始追蹤變更	VPC Flow Logs 開始追蹤其 AWS 受管政策的變更。	2026 年 3 月 31 日

疑難排解 VPC 流量日誌

以下是使用流量日誌時可能會遇到的問題。

問題

- 不完整的流量日誌記錄
- 流量日誌作用中，但沒有任何流量日誌記錄或日誌群組
- 'LogDestinationNotFoundException' 或 'Access Denied for LogDestination' 錯誤
- 超過 Amazon S3 儲存貯體原則限制
- LogDestination 無法傳遞
- 流量日誌資料大小與帳單資料不相符

不完整的流量日誌記錄

問題

您的流量日誌記錄不完整，或已不再發布。

原因

流量日誌可能存在無法交付至 CloudWatch Logs 日誌群組的問題，或日誌中可能存在 SkipData 項目。

解決方案

檢查 VPC、子網路或網路介面的流量日誌索引標籤。您無法描述與您共用的 VPC 或子網路的流程日誌。不過，您可以描述您在與您共用的 VPC 或子網路中建立之網路介面的流程日誌。若存在任何錯誤，即會出現在狀態欄位中。或者，使用 describe-flow-logs 命令，然後檢查在 `DeliverLogsErrorMessage` 欄位中傳回的值。

以下是狀態可能出現的錯誤值：

- `Rate limited`：當網路界面的流程日誌記錄數量超過在特定時間範圍內可發佈的最大數量時，可能會發生此錯誤。在您到達您可以建立的 CloudWatch Logs 日誌群組數配額時，也可能會發生此錯誤。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的 CloudWatch 服務配額。
- `Access error`：此錯誤可能的發生原因如下：
  - 您流量日誌的 IAM 角色沒有足夠的許可將流量日誌記錄發佈到 CloudWatch 日誌群組。

- IAM 角色與流量日誌服務沒有信任關係
- 信任關係不指定流量日誌服務為委託人

如需詳細資訊，請參閱用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色。

- `Unknown error`：流量日誌服務發生內部錯誤。

流量日誌作用中，但沒有任何流量日誌記錄或日誌群組

問題

您已建立流量日誌，且 Amazon VPC 或 Amazon EC2 主控台顯示流量日誌狀態為 `Active`。但是，您無法在 Amazon S3 儲存貯體中看到 CloudWatch Logs 或日誌檔案中的任何日誌串流。

可能原因

- 系統仍在建立流量日誌。在某些情況下，建立日誌群組的流程日誌以及顯示資料後，可能需要 10 分鐘或更長時間。
- 尚未記錄到任何網路介面的流量。只有在記錄流量時，才會建立 CloudWatch Logs 中的日誌群組。

解決方案

等待幾分鐘建立日誌群組或記錄流量。

'LogDestinationNotFoundException' 或 'Access Denied for LogDestination' 錯誤

問題

當您建立流量記錄檔時，會收到 `Access Denied for LogDestination` 或 `LogDestinationNotFoundException` 錯誤。

可能原因

- 建立將資料發佈至 Amazon S3 儲存貯體的流程日誌時，此錯誤表示找不到指定的 S3 儲存貯體。這也表示儲存貯體政策不允許將日誌交付至儲存貯體。
- 建立將資料發佈到 Amazon CloudWatch Logs 的流量記錄檔時若發生此錯誤，表示 IAM 角色不允許將記錄檔傳送到記錄檔群組。

解決方案

- 將資料發佈到 Amazon S3 儲存貯體時，請確保現有的 S3 儲存貯體已有指定的 ARN，而且該 ARN 的格式正確。如果您未擁有 S3 儲存貯體，則請確認儲存貯體政策具有所需的許可，並在 ARN 中使用正確的帳戶 ID 和儲存貯體名稱。
- 發佈至 CloudWatch Logs 時，請確認 IAM 角色具有所需的許可。

超過 Amazon S3 儲存貯體原則限制

問題

當您嘗試建立流量日誌時，得到下列錯誤：`LogDestinationPermissionIssueException`。

可能原因

此外，Amazon S3 儲存貯體原則的大小限制為 20 KB。

每次您建立流量日誌發布到 Amazon S3 儲存貯體時，我們都會自動將包括資料夾路徑的指定儲存貯體 ARN 新增到儲存貯體原則的 `Resource` 元素中。

建立多個發布到相同儲存貯體的流量日誌可能造成您超過儲存貯體政策限制。

解決方案

- 移除不再需要的流量記錄檔項目以清除儲存貯體的政策。
- 以下列內容取代個別的流量日誌項目，將許可授予整個儲存貯體。

```
arn:aws:s3:::bucket_name/*
```

若您授予許可給整個儲存貯體，新的流量日誌訂閱不會將新的許可加入到儲存貯體政策。

LogDestination 無法傳遞

問題

當您嘗試建立流量日誌時，得到下列錯誤：`LogDestination <bucket name> is undeliverable`。

可能原因

使用伺服器端加密搭配 AWS KMS (SSE-KMS) 加密目標 Amazon S3 儲存貯體，儲存貯體的預設加密是 KMS 金鑰 ID。

解決方案

此值必須為 KMS 金鑰 ARN。將預設 S3 加密類型從 KMS 金鑰 ID 變更為 KMS 金鑰 ARN。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的設定預設加密。

流量日誌資料大小與帳單資料不相符

問題

流量日誌的總資料大小與帳單資料報告的大小不相符。

可能原因

流量日誌中可能存在 SKIPDATA 項目。如需 SKIPDATA 項目的說明，請參閱無任何資料及略過的記錄。

解決方案

透過查詢日誌中 log-status 欄位的不同取值，確認日誌項目中是否存在 SKIPDATA 項目。

用於檢查 SKIPDATA 的查詢範例：

CW Insights：

```
fields @timestamp, @message, @logStream, @log
| filter interfaceId = 'eni-123'
| stats count(*) by interfaceId, logStatus
| sort by interfaceId, logStatus
```

Athena：

```
SELECT log_status, interface_id, count(1)
FROM vpc_flow_logs
WHERE interface_id IN ('eni-1', 'eni-2', 'eni-3')
GROUP BY log_status, interface_id
```

VPC 的 CloudWatch 指標

Amazon VPC 將有關 VPC 的資料發佈至 Amazon CloudWatch。您可以擷取有關您的 VPC 的統計資料，作為一組按順序排列的時間序列資料，亦即指標。您可以將指標視為要監控的變數，且資料是該變數在不同時間的值。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

目錄

- NAU 指標與維度
- 啟用或停用 NAU 監控
- NAU CloudWatch 警示範例

NAU 指標與維度

網路地址使用 (NAU) 是套用至虛擬網路中資源的指標，可協助您規劃和監控 VPC 大小。監控 NAU 無需支付任何費用。監控 NAU 很有幫助，因為如果您用盡 VPC 的 NAU 或對等 NAU 配額，則無法啟動新的 EC2 執行個體或佈建新資源，例如 Network Load Balancer、VPC 端點、Lambda 函數、傳輸閘道連接和 NAT 閘道。

如果您已針對 VPC 啟用網路地址使用監控，Amazon VPC 會將與 NAU 相關的指標傳送至 Amazon CloudWatch。VPC 的大小根據 VPC 包含的網路地址使用 (NAU) 單位數量來衡量。

您可以使用這些指標來了解 VPC 成長率、預測 VPC 何時會達到大小限制，或在超過大小閾值時建立警示。

AWS/EC2 命名空間包含下列用於監控 NAU 的指標。

指標	說明
NetworkAddressUsage	每個 VPC 的 NAU 計數。 報告準則 • 每 24 小時。 維度：、 • 名稱：Per-VPC Metrics，值：VPC ID。

指標	說明
NetworkAddressUsagePeered	VPC 和與之對等的所有 VPC 的 NAU 計數。 報告準則 • 每 24 小時。 維度：、 • 名稱：Per-VPC Metrics，值：VPC ID。

AWS/Usage 命名空間包含下列用於監控 NAU 的指標。

指標	說明
ResourceCount	每個 VPC 的 NAU 計數。 報告準則 • 每 24 小時。 維度：、 • 名稱：Service，值：EC2 • 名稱：Type，值：Resource • 名稱：Resource，值：VPC ID。 • 名稱：Class，值：NetworkAddressUsage
ResourceCount	VPC 和與之對等的所有 VPC 的 NAU 計數。 報告準則 • 每 24 小時。 維度：、

指標	說明
	• 名稱：Service，值：EC2 • 名稱：Type，值：Resource • 名稱：Resource，值：VPC ID。 • 名稱：Class，值：NetworkAddressUsagePeered
ResourceCount	VPC 之間 NAU 使用的組合視圖。 報告準則 • 每 24 小時。 維度：、 • 名稱：Service，值：EC2 • 名稱：Type，值：Resource • 名稱：Resource，值：VPC • 名稱：Class，值：NetworkAddressUsage
ResourceCount	對等 VPC 之間 NAU 使用的組合視圖。 報告準則 • 每 24 小時。 維度：、 • 名稱：Service，值：EC2 • 名稱：Type，值：Resource • 名稱：Resource，值：VPC • 名稱：Class，值：NetworkAddressUsagePeered

啟用或停用 NAU 監控

若要在 CloudWatch 中檢視 NAU 指標，您必須先啟用要監控的每個 VPC 上的監控功能。

啟用或停用監控 NAU

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC 的核取方塊。
4. 選取 Actions (動作) 和 Edit VPC settings (編輯 VPC 設定)。
5. 執行以下任意一項：
   - 若要啟用監控，請選取 Network mapping units metrics settings (網路映射單元指標設定) 和 Enable network address usage metrics (啟用網路地址使用指標)。
   - 若要停用監控，請清除 Network mapping units metrics settings (網路映射單元指標設定) 和 Enable network address usage metrics (啟用網路地址使用指標)。

使用命令列啟用或停用監控

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

NAU CloudWatch 警示範例

您可以使用下列 AWS CLI 命令和範例 `.json` 來建立 Amazon CloudWatch 警示和 SNS 通知，以追蹤 VPC 的 NAU 使用率，並以 50,000 個 NAU 作為閾值。此範例要求您先建立 Amazon SNS 主題。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

以下是 `nau-alarm.json` 的範例。

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
```

```
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

了解帳單和用量報告中的 Amazon VPC 代碼

當您使用 Amazon VPC 時，我們會在您的 AWS 帳單和用量報告中包含相關代碼。檢閱這些代碼有助於了解 Amazon VPC 的成本和使用模式。追蹤和管理您的支出費用對於成本的最佳化至關重要。

下表說明在帳單和用量報告中顯示的 Amazon VPC 代碼。如需帳單和用量報告中使用的區域代碼清單，請參閱 AWS Region billing codes。

下列項目的帳單代碼：

- IP 位址管理
- VPC 端點
- 傳輸閘道
- 網路分析
- 流量鏡射
- VPC Lattice
- 跨帳戶/區域資源數量

相關資源

- Amazon VPC 定價
- AWS PrivateLink 定價
- AWS Transit Gateway 定價
- Amazon VPC Lattice 定價

IP 位址管理

代碼	說明	個單位	精細程度
region-PublicIPv4:InUseAddress	資源使用公有 IPv4 位址的時間長度。	小時	每秒
region-PublicIPv4:IdleAddress	資源未使用公有 IPv4 位址的時間長度。	小時	每秒
region-PublicIPv4:ContiguousBlock	在 Amazon 提供的連續 IPv4 區塊中使用公有 IPv4 位址的時間長度。	小時	每小時
region-IPAddressManager-IP-Hours	IPAM 進階方案管理 IP 位址的時間長度。	小時	每小時

VPC 端點

代碼	說明	個單位	精細程度
region-VpcEndpoint-Hours	介面 VPC 端點的佈建時間長度。	小時	每小時
region-VpcEndpoint-Bytes	介面 VPC 端點處理的資料量。	GB	每小時

代碼	說明	個單位	精細程度
region-VpcEndpoint-GWLBE-Hours	Gateway Load Balancer 端點的佈建時間長度。	小時	每小時
region-VpcEndpoint-GWLBE-Bytes	Gateway Load Balancer 端點處理的資料量。	GB	每小時

傳輸閘道

代碼	說明	個單位	精細程度
region-TransitGateway-Hours	傳輸閘道連接的使用時間。	小時	每小時
region-TransitGateway-Bytes	傳輸閘道處理的資料量。	GB	每小時
region-TGW-Multicast-Consumer-Bytes	多播接收者執行個體處理的資料量。	GB	每小時

網路分析

代碼	說明	個單位	精細程度
region-Analysis-Runs	Reachability Analyzer 分析的網路路徑數量。	計數	每次分析
region-NetworkInterface-Assessment	網路存取分析器分析的網路介面數量。	計數	每次評估

流量鏡射

代碼	說明	個單位	精細程度
region-ENI-Mirror	為 Traffic Mirroring 設定的網路介面的時間長度。	小時	每小時

VPC Lattice

代碼	說明	個單位	精細程度
region-VPCLattice-Service-Hourly	VPC Lattice 服務的執行時間長度。	小時	每小時
region-VPCLattice-DataProcessing-Bytes	VPC Lattice 服務處理的資料量。	GB	每小時

代碼	說明	個單位	精細程度
region-VPCLattice-RequestCount-Free	免費的 HTTP 請求與 TCP 連線數量。	計數	每小時
region-VpcLattice-Service-Network-Resource-Hours	VPC Lattice 服務網路的執行時間長度。	小時	每小時

跨帳戶/區域資源數量

代碼	說明	個單位	精細程度
region-VpcResource-Provider-Bytes	跨帳戶或區域的提供者資源傳輸的資料量。	GB	每小時
region-VpcResource-Consumer-Bytes	跨帳戶或區域的取用者資源傳輸的資料量。	GB	每小時

描述 VPC 網路架構

Amazon VPC 可讓您在 AWS 雲端中定義邏輯隔離的虛擬網路，稱為虛擬私有雲端 (VPC)。建立單獨的 VPC，依工作負載或組織實體來隔離基礎結構。您可以選取 IP 位址範圍、設定路由以及新增網路閘

道 (VPC 互連的網路閘道、VPC 與網際網路連線的網路閘道、VPC 與您自己的企業網路連線的網路閘道)，來設定 VPC。您可以在 VPCs 中啟動 AWS 資源，例如 EC2 執行個體或 RDS 執行個體。

下表描述了 VPC 網路的關鍵特性。網路管理員可依據此指引來描述 VPC 網路的架構與組態。掌握這些資訊，管理員便能在內部部署環境或透過其他雲端服務供應商，建立功能等效的網路。

特性	說明
地理位置	Amazon VPC 託管於全球所有 AWS 區域。您可以為您的 VPC 網路選取最接近您客戶的 AWS 資源區域。
子網路	您為 VPCs 定義的子網路會定義網路邊界，並判斷 AWS 資源的 IP 地址。您可以在多個可用區域中新增子網路，提高資源的可用性。
網路連線能力	您連接至 VPC 或子網路的閘道，可提供 VPC 網路與其他網路 (例如其他 VPC 或子網路、網際網路或內部部署網路) 之間的連線能力。
安全控制項	您為 VPC 建立的安全群組會控管進出相關聯資源 (例如運算資源、資料庫資源與負載平衡器) 的流量。每個子網路皆具備網路 ACL，可控管進出子網路的流量。
流量管理	路由規則可控管子網路、VPC 與外部位置之間的流量傳輸。Elastic Load Balancing 提供的負載平衡器會將傳入流量分配至多個目標，例如 EC2 執行個體、容器與 Lambda 函式。

地理位置

Amazon VPC 適用於全球每個 AWS 區域。各個 區域為獨立的地理區域。當您在接近大多數使用者的區域中為資源建立 VPC 時，可降低網路延遲。

您可以使用 Amazon EC2 全域檢視功能，透過圖形化使用者介面列出所有區域中的 VPC (目前沒有等效的程式設計介面)。使用 Amazon VPC 主控台、 AWS API 和 AWS 命令列界面，您必須個別列出每個區域的 VPCs 和 VPC 資源。

為什麼這很重要

確認 VPC 的部署位置後，您可根據需求決定是否在相同或不同位置設定功能等效的網路環境。

跨所有區域取得 VPC 的摘要資訊

1. 前往 https://console.aws.amazon.com/ec2globalview/home 開啟 Amazon EC2 全域檢視主控台。
2. 在區域總管索引標籤的摘要下，查看 VPC 的資源數量，其中包括 VPC 數量與區域數量。這包括代表您 AWS 建立的預設 VPCs，以及您建立的非預設 VPCs。選擇底線文字，查看 VPC 計數如何分散到各個區域。如果某個區域只有一個 VPC，該 VPC 很可能是該區域的預設 VPC。
3. 在全域搜尋索引標籤上，選取用戶端篩選條件資源類型 = Vpc。您可以透過指定區域或標籤進一步篩選結果。

使用 取得區域中VPCs AWS CLI

使用如下 describe-vpcs 命令。您必須在每個您有 VPC 的區域中執行此命令。`--query` 參數僅包含輸出中的 VPC ID。您可以視需要包含其他欄位。

```
aws ec2 describe-vpcs \
    --region us-east-2 \
    --query "Vpcs[*].VpcId"
```

每個區域均附帶預設 VPC。如果不使用預設 VPC，可新增如下篩選條件，將這些 VPC 從結果中排除。

```
--filters Name=is-default,Values=false
```

子網路

子網路是 VPC 中的邏輯網路邊界。建立子網路時，需指派 IP 位址區塊。在子網路中啟動的資源，將被指派該子網路 IP 位址區塊中的 IP 位址。IP 位址使資源能夠透過區域網路或網際網路相互通訊。

Amazon VPC 主控台中的資源地圖會以視覺化方式呈現 VPC 內子網路的分佈情況。

重要性說明

子網路可使網路管理員實作安全邊界，並控管不同應用程式層之間的流量。記錄子網路的 IP 位址有助確保功能等效網路中的資源，能與 VPC 網路中相同外部用戶端或應用程式維持通訊。

透過資源地圖檢視 VPC 的子網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 VPCs (VPC)。
3. 選取 VPC 的核取方塊。
4. 選擇資源地圖索引標籤。
5. 在 VPC 窗格中，選擇顯示詳細資訊。子網路窗格會列出 VPC 中的所有子網路，也會顯示各子網路的 IP 位址範圍。將滑鼠游標暫留在子網路上，可反白顯示其相關聯的路由表與網路連線。如需詳細資訊，請選擇連結以開啟子網路詳細資訊頁面。

使用 描述 VPC 的子網路 AWS CLI

使用如下 describe-subnets 命令。`--filters` 參數會將搜尋範圍限定於描述指定 VPC 的子網路。`--query` 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-subnets \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query Subnets[*].
[SubnetId,AvailabilityZoneId,CidrBlock,Ipv6CidrBlockAssociationSet[0].Ipv6CidrBlock] \
    --output table
```

以下為範例輸出。這些欄位分別是子網路 ID、可用區域 ID、IPv4 位址範圍，以及首個 IPv6 位址範圍 (如有)。

```
-------------------------------------------------------------------------------------
|                                  DescribeSubnets                                  |
+---------------------------+-----------+----------------+---------------------------+
|  subnet-0d2d1b81e0bc9c6d4 |  usw2-az1 |  10.0.144.0/20 |  2600:1f14:1e6e:a003::/64  |
|  subnet-0e01d500780bb7468 |  usw2-az1 |  10.0.16.0/20  |  2600:1f14:1e6e:a001::/64  |
|  subnet-0eb17d85f5dfd33b1 |  usw2-az2 |  10.0.128.0/20 |  2600:1f14:1e6e:a002::/64  |
|  subnet-0e990c67809773b19 |  usw2-az2 |  10.0.0.0/20   |  2600:1f14:1e6e:a000::/64  |
+---------------------------+-----------+----------------+---------------------------+
```

網路連線

Amazon VPC 提供的連線選項，能讓您建立囊括多個帳戶、多個區域與遠端網路中 VPC 的網路。

您可以透過 Amazon VPC 主控台中的資源地圖，探索 VPC 是否使用網際網路閘道、僅限輸出網際網路閘道、NAT 閘道或閘道 VPC 端點。資源地圖不會顯示任何正在使用的傳輸閘道、對等互連、虛擬私

有閘道或其他類型 VPC 端點。若要取得某個 VPC 的所有閘道與對等互連的完整清單，您可以使用主控台、API 或命令列介面逐一描述。

重要性說明

了解 VPC 網路提供的連線能力後，您可確保功能等效網路中的資源，能與相同的本機及遠端資源維持通訊。

透過資源地圖檢視 VPC 的網路連線

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 VPCs (VPC)。
3. 選取 VPC 的核取方塊。
4. 選擇資源地圖索引標籤。
5. 在 VPC 窗格中，選擇顯示詳細資訊。網路連線窗格會列出所有網際網路閘道、僅限輸出網際網路閘道、NAT 閘道與閘道 VPC 端點。如果資源類型不明確，將滑鼠游標暫留在網路連線的連結圖示上，即可檢視對應的 URL。此 URL 是該資源在主控台中的連結，包含資源類型與資源 ID (例如 internetGatewayId=igw-0123456780abcdef)。

使用 取得 VPCs的網路連線 AWS CLI

1. 使用如下 describe-internet-gateways 命令，取得指定區域的網際網路閘道。`--query` 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-internet-gateways \
    --region us-east-2 \
    --query InternetGateways[*].[Attachments[0].VpcId,InternetGatewayId] \
    --output table
```

以下為範例輸出。這些欄位顯示 VPC ID 與網際網路閘道 ID。

```
-------------------------------------------------------
|             DescribeInternetGateways              |
+-------------------------+-------------------------+
|  None                   |  igw-04c61dba10EXAMPLE  |
|  vpc-0bf4c2739bEXAMPLE  |  igw-09737a4029EXAMPLE  |
|  vpc-060415a18fEXAMPLE  |  igw-0c562bd22aEXAMPLE  |
|  vpc-0ea9d41094EXAMPLE  |  igw-0e06f7033dEXAMPLE  |
|  vpc-03b86de356EXAMPLE  |  igw-0a9ff72d05EXAMPLE  |
```

```
+------------------------+-------------------------+
```

2. 使用如下 describe-egress-only-internet-gateways 命令，取得指定區域的僅限輸出網際網路閘道。--query 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-egress-only-internet-gateways \
    --region us-east-2 \
    --query EgressOnlyInternetGateways[*].
[Attachments[0].VpcId,EgressOnlyInternetGatewayId] \
    --output table
```

以下為範例輸出。這些欄顯示 VPC ID 與僅限輸出網際網路閘道 ID。

```
-----------------------------------------------------
|        DescribeEgressOnlyInternetGateways         |
+------------------------+--------------------------+
|  vpc-060415a18fEXAMPLE |  eigw-0b8ca558acEXAMPLE  |
+------------------------+--------------------------+
```

3. 使用如下 describe-nat-gateways 命令，取得指定區域的 NAT 閘道。--query 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-nat-gateways \
    --region us-east-2 \
    --query NatGateways[*].[VpcId,NatGatewayId,SubnetId] \
    --output table
```

以下為範例輸出。這些欄位顯示 VPC ID、NAT 閘道 ID 與子網路 ID。

```
-------------------------------------------------------------------------------
|                            DescribeNatGateways                              |
+------------------------+-------------------------+---------------------------+
|  vpc-060415a18fEXAMPLE |  nat-026316334aEXAMPLE  |  subnet-0eb17d85f5EXAMPLE  |
|  vpc-060415a18fEXAMPLE |  nat-0f08bc5f52EXAMPLE  |  subnet-0d2d1b81e0EXAMPLE  |
+------------------------+-------------------------+---------------------------+
```

4. 使用如下 describe-transit-gateway-vpc-attachments 命令，取得指定區域的傳輸閘道 VPC 連接項目。--query 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-transit-gateway-vpc-attachments \
    --region us-east-2 \
```

```
    --query TransitGatewayVpcAttachments[*].
[VpcId,TransitGatewayId,length(SubnetIds[])] \
    --output table
```

以下為範例輸出。這些欄位顯示 VPC ID、傳輸閘道 ID 與子網路數量。

```
-------------------------------------------------------------
|         DescribeTransitGatewayVpcAttachments              |
+-------------------------+-------------------------+-----+
|  vpc-0bf4c2739bEXAMPLE |  tgw-055dc4e47bEXAMPLE  |  4 |
|  vpc-0ea9d41094EXAMPLE |  tgw-055dc4e47bEXAMPLE  |  2 |
+-------------------------+-------------------------+-----+
```

5. 使用如下 describe-vpc-peering-connections 命令，取得指定區域中 VPC 的對等連線。`--query` 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-vpc-peering-connections \
    --region us-east-2 \
    --query VpcPeeringConnections[*].[AccepterVpcInfo.VpcId,RequesterVpcInfo.VpcId]
 \
    --output table
```

以下為範例輸出。這些欄位顯示接受者 VPC ID、接受者 VPC 擁有者、申請者 VPC ID 與申請者 VPC 擁有者。

```
-------------------------------------------------------------------------------------
|                          DescribeVpcPeeringConnections
 |
+-------------------------+--------------+-------------------------+---------------
+
|  vpc-0ea9d41094EXAMPLE |  123456789012 |  vpc-03b86de356EXAMPLE |  123456789012
 |
+-------------------------+--------------+-------------------------+---------------
+
```

6. 使用如下 describe-vpn-gateways 命令，取得指定區域的虛擬私有閘道。`--query` 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-vpn-gateways \
    --region us-east-2 \
    --query VpnGateways[*].[VpcAttachments[0].VpcId,VpnGatewayId] \
```

```
    --output table
```

以下為範例輸出。這些欄位顯示 VPC ID 與虛擬私有閘道 ID。

```
-----------------------------------------------------
|                DescribeVpnGateways                |
+-------------------------+-------------------------+
|  vpc-0bf4c2739bEXAMPLE |  vgw-0cb3226c4aEXAMPLE  |
+-------------------------+-------------------------+
```

7. 使用如下 describe-vpc-endpoints 命令，取得指定區域的 VPC 端點。--query 參數僅包含輸出中的指定欄位。您可以視需要包含其他欄位。

```
aws ec2 describe-vpc-endpoints \
    --region us-east-2 \
    --query 'VpcEndpoints[*].[VpcId,VpcEndpointType,ServiceName||
ServiceNetworkArn||ResourceConfigurationArn]' \
    --output table
```

以下為範例輸出。第一個欄位顯示 VPC ID，第二個欄位顯示 VPC 端點類型。第三個欄位取決於端點類型，顯示的內容可能是服務名稱、資源組態 ARN 或服務網路 ARN。

```
-----------------------------------------------------------------------------------------------
|                                                    DescribeVpcEndpoints
                                                 |
+-------------------------+-----------------
+-----------------------------------------------------------------------------------------------
+
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                                |
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                                |
|  vpc-0bf4c2739bc05a694 |  Gateway        |  com.amazonaws.us-west-2.s3
                                                |
|  vpc-0ea9d410947d27b7d |  Interface      |  com.amazonaws.us-west-2.logs
                                                |
|  vpc-0bf4c2739bc05a694 |  Resource       |  arn:aws:vpc-lattice:us-
east-2:123456789012:resourceconfiguration/rcfg-07129f3acded87625  |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
```

```
+------------------------+-----------------
+-------------------------------------------------------------------------------------------------------
+
```

安全控制項

Amazon VPC 提供的安全控制項會決定對 VPC 的網路存取，以及 VPC 中部署的資源。

重要性說明

確定允許抵達子網路與資源的傳入流量，以及允許離開子網路與資源的傳出流量後，即可規劃功能等效網路所需的防火牆規則。

安全控制項

- Security groups (安全群組)
- 網路 ACL

Security groups (安全群組)

安全群組允許在資源層級控管特定的傳入與傳出流量。安全群組是控制存取 VPC 內資源的主要機制。

取得 VPC 的安全群組

使用如下 describe-security-groups 命令，顯示指定 VPC 的安全群組。

```
aws ec2 describe-security-groups \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query SecurityGroups[*].GroupId
```

取得安全群組的傳入規則

使用如下 describe-security-group-rules 命令，顯示指定安全群組的規則，其中 `IsEgress` 為 `false`。

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

取得安全群組的傳出規則

使用如下 describe-security-group-rules 命令，顯示指定安全群組的規則，其中 IsEgress 為 true。

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

網路 ACL

網路存取控制清單 (ACL) 會允許或拒絕子網路層級的特定傳入與傳出流量。您可以將網路 ACL 用作深度防禦措施，因應資源部署時未設定正確安全群組的情況。

取得子網路的網路 ACL

使用如下 describe-network-acls 命令，顯示指定 VPC 的網路 ACL 及其子網路關聯。

```
aws ec2 describe-network-acls \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "NetworkAcls[*].{ID:NetworkAclId,Subnets:Associations[].SubnetId}"
```

取得網路 ACL 的傳入規則

使用如下 describe-network-acls 命令，顯示指定網路 ACL 的規則，其中 Egress 為 false。

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`false`]'
```

取得網路 ACL 的傳出規則

使用如下 describe-network-acls 命令，顯示指定網路 ACL 的規則，其中 Egress 為 true。

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`true`]'
```

流量管理

有效的流量管理需結合路由表提供的網路層級路由決策，以及負載平衡機制提供的應用程序層級分配策略。

重要性說明

網路管理員必須設計子網路、路由、DNS 解析與負載平衡機制，在維持安全邊界與效能需求的同時，實現流量傳輸最佳化。記錄 VPC 網路中這些元件的組態有助確保功能等效網路中的資源，能與 VPC 網路中相同外部用戶端或裝置維持通訊。

流量管理

- 路由表
- DHCP 選項集
- 負載平衡器

路由表

路由表會決定網路流量如何跨子網路、VPC、內部部署網路與網際網路等網路邊界傳輸。

Amazon VPC 主控台中的資源地圖提供 VPC 路由表的視覺化呈現。

透過資源地圖檢視 VPC 的路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 VPCs (VPC)。
3. 選取 VPC 的核取方塊。
4. 選擇資源地圖索引標籤。
5. 路由表窗格會列出 VPC 的所有路由表。將滑鼠游標暫留在路由表上，可反白顯示其相關聯的子網路與網路連線。如需詳細資訊，請選擇連結以開啟路由表詳細資訊頁面。

描述路由表

使用 describe-route-tables 命令，描述指定 VPC 的路由表及其子網路關聯。

```
aws ec2 describe-route-tables \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "RouteTables[*].{ID:RouteTableId,Subnets:Associations[].SubnetId}"
```

取得路由表的路由

使用 describe-route-tables 命令，描述指定路由表的路由。

```
aws ec2 describe-route-tables \
    --route-table-ids rtb-02ec01715bEXAMPLE \
```

```
    --query RouteTables[*].Routes
```

DHCP 選項集

您的 VPC 具備 DHCP 選項集，可用於設定各種網路。例如，您可以設定自訂 DNS 伺服器，讓 EC2 執行個體可以透過現有的 DNS 基礎結構解析內部主機名稱。如需詳細資訊，請參閱the section called “DHCP 選項集概念”。

描述 VPC 的 DHCP 選項

使用 describe-dhcp-options 命令，描述指定的 DHCP 選項。此範例也可使用 describe-vpcs 命令，取得指定 VPC 的 DHCP 選項 ID。

```
aws ec2 describe-dhcp-options \
    --dhcp-options-id "$(aws ec2 describe-vpcs \
        --vpc-id vpc-1234567890abcdef0 \
        --query Vpcs[].DhcpOptionsId --output text)"
```

以下是使用預設 DHCP 選項的 VPC 輸出範例。

```
{
    "DhcpOptions": [
        {
            "OwnerId": "415546850671",
            "Tags": [],
            "DhcpOptionsId": "dopt-1234567890abcdef0",
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-west-2.compute.internal"
                        }
                    ]
                },
                {
                    "Key": "domain-name-servers",
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
```

```
                }
            ]
        }
    ]
}
```

負載平衡器

負載平衡機制會將來自用戶端的傳入流量分配至多個目標。負載平衡器會監控目標的運作狀態，也會自動從流量分配中移除運作狀態不良的目標，確保僅使用運作狀態良好的目標。這有助於提高應用程式的可用性與效能，最佳化資源使用率。如需詳細資訊，請參閱《Elastic Load Balancing 使用者指南》。

描述負載平衡器

使用 describe-load-balancers 命令，顯示指定 VPC 的負載平衡器。

```
aws elbv2 describe-load-balancers \
    --query 'LoadBalancers[?VpcId==`vpc-1234567890abcdef0`].LoadBalancerArn'
```

相關資源

以下是 VPC 網路中可能正在使用的選用服務或功能：

- Direct Connect
- AWS Network Firewall
- IPAM
- 流量鏡射
- VPC 流程日誌

管理 Amazon Virtual Private Cloud 的安全責任

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模式將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也提供您可以安全使用的服務。在AWS 合規計劃中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon Virtual Private Cloud 的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Amazon VPC 時套用共同責任模型。下列各主題將說明如何配置 Amazon VPC，以達成您的安全性與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon VPC 資源。

目錄

- 確保 Amazon Virtual Private Cloud 中的資料保護
- 強制執行傳輸中的 VPC 加密
- Amazon VPC 的身分和存取管理
- Amazon VPC 的基礎設施安全性
- 使用安全群組控制 AWS 資源的流量
- 使用網路存取控制清單控制子網路流量
- Amazon Virtual Private Cloud 的恢復能力
- Amazon Virtual Private Cloud 的合規驗證
- 封鎖對 VPC 和子網路的公開存取
- VPC 的安全最佳實務

確保 Amazon Virtual Private Cloud 中的資料保護

共同責任模型適用於 AWS Amazon Virtual Private Cloud 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負

責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。 如需歐洲資料保護的詳細資訊，請參閱一般資料保護規則 (GDPR) 中心。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Amazon VPC 或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

確保 Amazon VPC 中的網際網路流量隱私權

Amazon Virtual Private Cloud 提供可用來提高和監控 Virtual Private Cloud (VPC) 安全的功能：

- 安全群組：安全群組會允許資源層級 (例如 EC2 執行個體) 的特定傳入與傳出流量。啟動執行個體時，您可將其與一個或多個安全群組建立關聯。VPC 中的每個執行個體可能隸屬不同的安全群組。若您並未在啟動執行個體時指定安全群組，則執行個體會自動與其 VPC 的預設安全群組建立關聯。如需詳細資訊，請參閱Security groups (安全群組)。
- 網路存取控制清單 (ACL)：網路 ACL 會允許或拒絕子網層級的特定傳入與傳出流量。如需詳細資訊，請參閱使用網路存取控制清單控制子網路流量。
- 流量日誌：流量日誌可擷取您 VPC 中傳入和傳出網路介面之 IP 流量資訊。您可以建立 VPC、子網路或個別網路介面的流量日誌。流量日誌資料會發佈至 CloudWatch Logs 或 Amazon S3，並可協助您診斷過度限制或過度寬鬆的安全群組和網路 ACL 規則。如需詳細資訊，請參閱 使用 VPC 流量日誌來記錄 IP 流量。

- 流量鏡射：您可以從 Amazon EC2 執行個體的彈性網路介面複製網路流量。然後，您可以將流量傳送至頻外安全性和監控設備。如需詳細資訊，請參閱流量鏡射指南。

強制執行傳輸中的 VPC 加密

VPC 加密控制是一項安全與合規功能，可讓您集中進行授權控制，以監控流量的加密狀態、協助您識別允許純文字通訊的資源，並最終為您提供機制，以強制執行區域內跨 VPCs傳輸中的加密

VPC Encryption Controls 同時使用應用程式層加密和 nitro AWS 系統硬體的內建傳輸中加密功能，以確保加密強制執行。此功能也會將原生硬體層加密延伸至現代 Nitro 執行個體以外的 AWS 其他服務，包括 Fargate、Application Load Balancer、Transit Gateways 等。

此功能專為想要確保可見性和控制所有流量加密狀態的任何人而設計。在資料加密對於符合 HIPAA、FedRamp 和 PCI DSS 等合規標準至關重要的產業中特別有用。安全管理員和雲端架構師可以使用它，在其 AWS 環境中集中執行傳輸政策中的加密

此功能可用於兩種模式：監控模式和強制執行模式。

加密控制模式

監控模式

在監控模式中，加密控制可讓您了解 VPC 內部和跨 VPCs 之間 AWS 資源之間流量流程的加密狀態。它還可協助您識別未強制執行傳輸中加密的 VPC 資源。您可以設定 VPC 流程日誌以發出富集欄位 - `encryption-status` -，告知您的流量是否已加密。您也可以使用主控台或`GetVpcResourcesBlockingEncryptionEnforcement`命令來識別未強制執行傳輸中加密的資源。

> **Note**
>
> 現有的 VPCs 只能先在監控模式中啟用。這可讓您了解允許或可能允許純文字流量的資源。只有在這些資源開始強制執行加密 （或您為其建立排除） 時，您才能在 VPC 上開啟強制執行模式。

強制執行模式

在強制執行模式中，VPC 加密控制可防止您使用允許 VPC 邊界內未加密流量的任何功能或服務。您無法在現有 VPCs 上直接在強制模式下啟用加密控制。您必須先在監控模式中開啟加密控制、識別和

修改不合規的資源，以強制執行傳輸中的加密，然後開啟強制執行模式。不過，您可以在建立新 VPCs 期間，以強制模式開啟加密控制。

啟用時，強制模式會防止您建立或連接未加密的 VPC 資源，例如不支援原生內建加密的舊 EC2 執行個體，或網際網路閘道等。如果您想要在加密強制執行的 VPC 中執行不合規的資源，您必須建立該資源的排除。

監控流量流程的加密狀態

您可以使用 VPC 流程日誌中的 `encryption-status` 欄位，稽核 VPC 內流量的加密狀態。可包含下列值：

- `0` = 未加密
- 1 = nitro 加密 （ 由 VPC 加密控制管理 ）
- 2 = 應用程式加密
  - 界面端點到 AWS 服務的 TCP 連接埠 443 上的流程 *
  - 閘道端點 TCP 連接埠 443 上的流程 *
  - 透過 VPC 端點流向加密 Redshift 叢集 **
- 3 = 同時加密 nitro AND 應用程式
- (-) = 加密狀態未知或 VPC 加密控制已關閉

請注意：

* 對於介面和閘道端點， AWS 不會查看封包資料來判斷加密狀態，而是依賴用來取得加密狀態的連接埠。

** 對於指定的 AWS 受管端點， 會根據服務組態中的 TLS 需求來 AWS 確定加密狀態。

VPC 流程日誌限制

- 若要啟用 VPC Encryption Controls 的流程日誌，您需要使用 encryption-status 欄位手動建立新的流程日誌。加密狀態欄位不會自動新增至現有的流程日誌。
- 建議您將 ${traffic-path} 和 ${flow-direction} 欄位新增至流程日誌，以取得流程日誌中更多詳細資訊。

  範例：

```
aws ec2 create-flow-logs \
```

```
--resource-type VPC \
--resource-ids vpc-12345678901234567 \
--traffic-type ALL \
--log-group-name my-flow-logs \
--deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs
--log-format '${encryption-status} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${protocol} ${traffic-path} ${flow-direction} ${reject-reason}'
```

VPC 加密控制排除

VPC 加密控制強制執行模式需要 VPC 中的所有資源強制執行加密。這可確保區域中 AWS 內的加密。不過，您可能有網際網路閘道、NAT 閘道或虛擬私有閘道等資源，允許在負責設定和維護end-to-end加密 AWS的網路外部進行連線。若要在加密強制執行VPCs 中執行這些資源，您可以建立資源排除。排除會為資源建立可稽核的例外狀況，其中客戶負責維護加密 （通常是在應用程式層）。

VPC 加密控制僅支援 8 個排除。如果您的 VPC 中有這些資源，並且想要移至強制執行模式，則必須在從監視器切換到強制執行模式時新增這些排除。不可排除其他資源。您可以遷移 VPC 以強制執行模式，方法是建立這些資源的排除。您負責加密進出這些資源的流量

- 網際網路閘道
- NAT 閘道
- 僅限輸出的網際網路閘道
- 加密未強制執行 VPC VPCs VPC 對等互連 （詳細案例請參閱 VPC 對等互連支援一節）
- 虛擬私有閘道
- VPC 內的 Lambda 函數
- VPC Lattice
- 彈性檔案系統

實作工作流程

1. 啟用監控 - 在監控模式下建立 VPC 加密控制
2. 分析流量 - 檢閱流程日誌以監控流量的加密狀態
3. 分析資源 - 使用主控台或`GetVpcResourcesBlockingEncryptionEnforcement`命令來識別未強制執行傳輸中加密的資源。
4. 準備 【選用】 - 如果您想要開啟強制執行模式，請規劃資源遷移和必要的排除項目

5. 強制執行 【選用】 - 切換為強制執行模式並設定必要的排除
6. 稽核 - 透過流程日誌持續監控合規

如需詳細設定說明，請參閱部落格介紹 VPC 加密控制：強制執行區域內 VPCs內和之間傳輸中的加密。

VPC 加密控制狀態

VPC 加密控制可以具有下列其中一種狀態：

建立

正在 VPC 上建立 VPC 加密控制。

modify-in-progress

正在 VPC 上修改 VPC 加密控制項

正在刪除

正在 VPC 上刪除 VPC 加密控制項

有用

VPC 加密控制在 VPC 上成功實作監控模式或強制執行模式

AWS 服務支援和相容性

若要符合加密規範，資源必須一律在硬體層或應用程式層強制執行傳輸中的加密。對於大多數資源，您不需要採取任何動作。

具有自動合規的服務

PrivateLink 支援的大多數 AWS 服務，包括跨區域 PrivateLinks，都會接受在應用程式層加密的流量。您不需要對這些資源進行任何變更。 AWS 會自動捨棄任何未經application-layer-encrypted流量。某些例外狀況包括 Redshift 叢集 （已佈建和無伺服器 - 您需要在其中手動遷移基礎資源）

自動遷移的資源

Network Load Balancer、Application Load Balancer、Fargate 叢集、EKS 控制平面會在您開啟監控模式後自動遷移至原生支援加密的硬體。您不需要修改這些資源。 會自動 AWS 處理遷移。

需要手動遷移的資源

某些 VPC 資源和服務要求您選取基礎執行個體類型。所有現代 EC2 執行個體都支援傳輸中加密。如果您的服務已使用現代 EC2 執行個體，則不需要進行任何變更。您可以使用 主控台或 GetVpcResourcesBlockingEncryptionEnforcement 命令來識別是否有任何這些服務正在使用較舊的執行個體。如果您識別這類資源，則必須將其升級至支援 nitro 系統硬體原生加密的任何現代 EC2 執行個體。這些服務包括 EC2 執行個體、Auto Scaling 群組、RDS（所有資料庫和文件資料庫）、Elasticache 佈建、Amazon Redshift 佈建叢集、EKS、ECS-EC2、OpenSearch 佈建和 EMR。

相容資源：

下列資源與 VPC 加密控制相容：

- Nitro 型 EC2 執行個體
- Network Load Balancer（有限制）
- Application Load Balancer
- AWS Fargate 叢集
- Amazon Elastic Kubernetes Service (EKS)
- Amazon EC2 Auto Scaling 群組
- Amazon Relational Database Service (RDS - 所有資料庫）
- Amazon ElastiCache 節點型叢集
- Amazon Redshift 佈建和無伺服器叢集
- Amazon Elastic Container Service (ECS) - EC2 容器執行個體
- Amazon OpenSearch Service
- Amazon Elastic MapReduce (EMR)
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- VPC 加密控制會對透過 PrivateLink 存取的所有 AWS 服務在應用程式層強制執行加密。任何未在應用程式層加密的流量，都會由託管在 VPC 內的 PrivateLink 端點捨棄，且加密控制處於強制執行模式

服務特定的限制

Network Load Balancer 限制

TLS 組態：在包含 VPC 的 上強制執行加密控制時，您無法使用 TLS 接聽程式將加密和解密的工作卸載至負載平衡器。不過，您可以將目標設定為執行 TLS 加密和解密

Redshift 佈建和無伺服器

客戶無法在具有現有叢集/端點的 VPC 上移至強制執行模式。若要搭配 Redshift 使用 VPC 加密控制，您必須從快照還原叢集或命名空間。對於佈建叢集，建立現有 Redshift 叢集的快照，然後使用叢集快照操作的還原，從快照還原。對於無伺服器，建立現有命名空間的快照，然後使用無伺服器工作群組上快照操作的還原，從快照還原。請注意，在未執行快照和還原程序的情況下，無法在現有叢集或命名空間上啟用 VPC 加密控制。如需建立快照，請參閱 Amazon Redshift 文件。

Amazon MSK (Apache Kafka 的受管串流）

4.1 的新叢集在其自己的 VPC 中支援此功能。下列步驟將協助您搭配 MSK 使用 VPC 加密。

- 客戶在沒有其他 MSK 叢集的 VPC 上啟用 VPC 加密
- 客戶使用 Kafka 4.1 版建立叢集，並將執行個體類型建立為 M7g

Gateway Load Balancer 和 AWS Network Firewall

強制模式下VPCs 不支援 Gateway Load Balancer 和 AWS Network Firewall。如果您的 VPC 中存在這些資源，您必須在監控模式下執行 VPC。

區域和區域限制

- 本機區域子網路：強制執行模式中不支援 - 必須從 VPC 刪除

VPC 對等互連支援

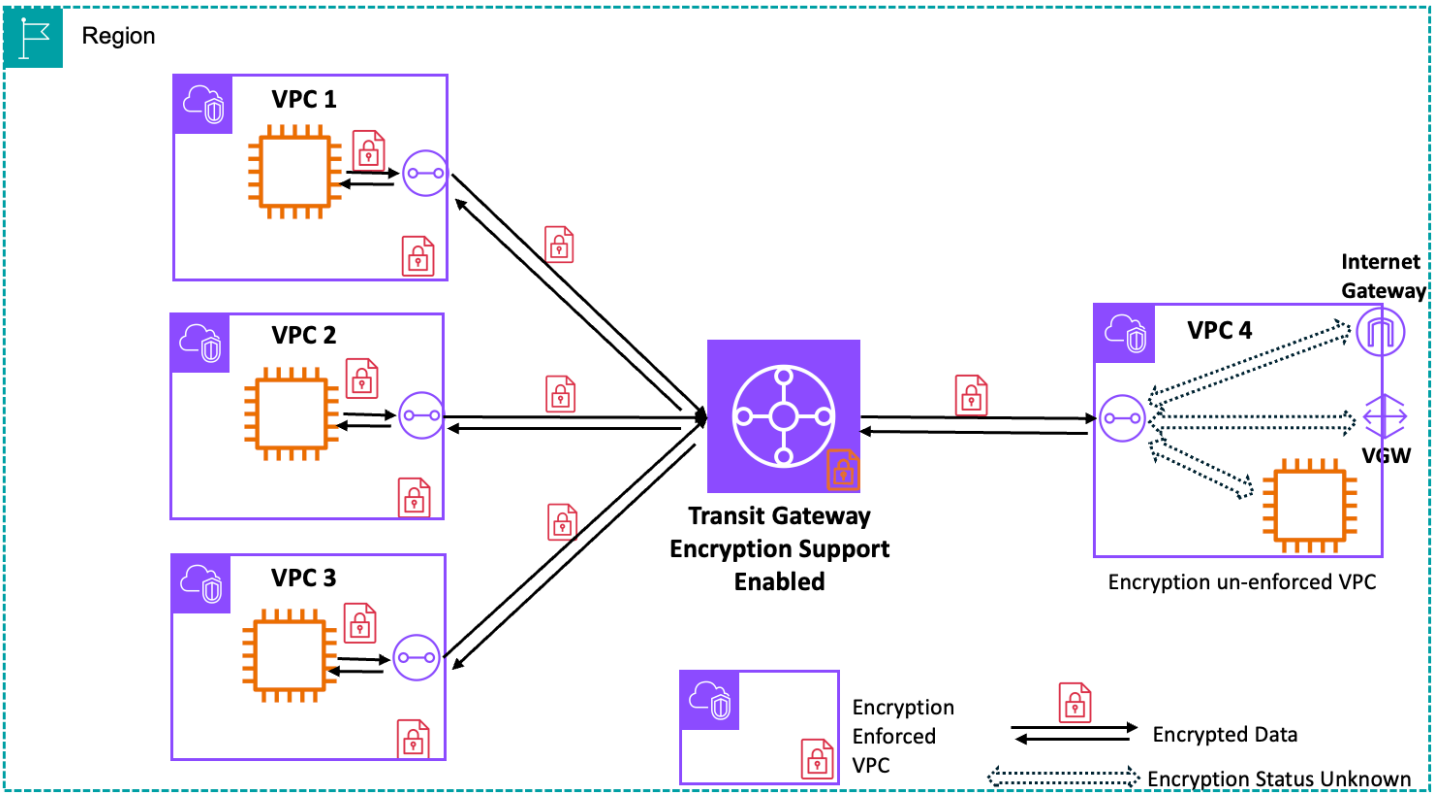
為了確保兩個 VPCs 之間使用 VPC 對等互連傳輸中的加密，兩個 VPCs 必須位於相同區域，並在沒有任何排除的情況下以強制執行模式開啟加密控制。如果您想要將加密強制執行的 VPC 與位於不同區域或未啟用強制執行模式的加密控制項的另一個 VPC 對等互連排除項目（不含排除項目），則必須建立對等互連排除項目。

如果兩個 VPCs處於強制執行模式並彼此對等，您無法將模式從強制執行變更為監控。您必須先建立對等排除，才能修改要監控的 VPC 加密控制模式。

傳輸閘道加密支援

您必須在 Transit Gateway 上明確啟用加密支援，以加密已開啟加密控制的 VPCs之間的流量。在現有的 Transit Gateway 上啟用加密不會對現有的流量造成干擾，而且 VPC 連接遷移到加密通道將順暢自動發生。兩個處於強制模式（不含排除） VPCs 透過 Transit Gateway 周遊 100% 加密通道之間

的流量。傳輸閘道上的加密也可讓您連接兩個處於不同加密控制模式VPCs。當您想要在連接到non-encryption-enforced加密強制執行 VPC 的 VPC 中強制執行加密控制時，您應該使用它。在這種情況下，加密強制執行 VPC 內的所有流量都會加密，包括 VPC 間流量。加密強制執行 VPC 中的資源與 Transit Gateway 之間的 VPC 間流量會加密。除此之外，加密取決於流量在非強制執行 VPC 中傳送至的資源，且不保證會加密（因為 VPC 未處於強制執行模式）。所有 VPCs 都必須位於相同的區域。（請參閱此處的詳細資訊）。



- 在此圖表中，VPC 1、VPC 2 和 VPC3 在強制模式下具有加密控制，並且它們連接到在監控模式下執行加密控制的 VPC 4。
- VPC1、VPC2 和 VPC3 之間的所有流量都會加密。
- 為了詳細說明，VPC 1 中的資源與 VPC 4 中的資源之間的任何流量都會加密，直到 Transit Gateway 使用 nitro 系統硬體提供的加密為止。除了加密狀態之外， 還取決於 VPC 4 中的資源，且不保證會加密。

如需 Transit Gateway 加密支援的詳細資訊，請參閱傳輸閘道文件。

在帳戶層級啟用 VPC 加密控制

帳戶層級 VPC 加密控制可讓您設定套用至您帳戶中所有 VPCs加密控制模式和資源排除。這可提供加密政策的集中式管理，而不需要個別設定每個 VPC。

帳戶層級加密控制支援與 VPC 層級控制相同的八個資源排除：網際網路閘道、NAT 閘道、輸出限定網際網路閘道、VPC 對等互連、虛擬私有閘道、Lambda、VPC Lattice 和彈性檔案系統。

帳戶層級加密控制模式

您可以在帳戶層級設定下列模式：

未受管

VPC 加密控制會維持在目前的模式，並且可以在 VPC 層級進行管理。

嘗試監控

嘗試將帳戶中的所有 VPCs轉換為監控模式。識別未加密的資源，而不會封鎖建立。

嘗試強制執行

嘗試轉換帳戶中的所有 VPCs以強制執行模式。封鎖未加密資源的建立。

帳戶層級加密控制狀態

帳戶層級 VPC 加密控制可以有下列其中一種狀態：

default-state

帳戶層級 VPC 加密控制尚未啟用。

transitions-in-progress

帳戶中VPCs 正在轉換至指定的模式。

transitions-partially-successful

一或多個 VPCs未轉換為預期的模式。

轉換成功

所有 VPCs都已成功轉換為預期的模式。

轉換失敗

所有 VPCs都無法轉換為預期的模式。

在組織層級啟用 VPC 加密控制

如果您使用 AWS Organizations 來管理組織中的帳戶，則可以使用 AWS Organizations 宣告政策在組織中的帳戶強制執行 VPC 加密控制。如需 VPC 加密控制宣告政策的詳細資訊，請參閱 AWS Organizations 使用者指南中的支援的宣告政策。

定價

如需定價資訊，請參閱 Amazon VPC 定價。

AWS CLI 命令參考

設定與組態

- aws ec2 create-vpc-encryption-control
- aws ec2 modify-vpc-encryption-control
- aws ec2 modify-account-vpc-encryption-control
- aws ec2 describe-account-vpc-encryption-control
- aws ec2 tgw modify-transit-gateway

監控和疑難排解

- aws ec2 describe-vpc-encryption-controls
- aws ec2 get-vpc-resources-blocking-encryption-enforcement
- aws ec2 create-flow-logs
- aws ec2 describe-flow-logs
- aws 日誌查詢

清除

- aws ec2 delete-vpc-encryption-control

其他資源

如需詳細設定說明，請參閱部落格介紹 VPC 加密控制：強制執行區域內 VPCs內和之間傳輸中的加密。

如需更詳細的 API 資訊，請參閱 EC2 API 參考指南。

Amazon VPC 的身分和存取管理

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。IAM 管理員可以控制驗證 (已登入) 和授權 (具有許可) 來使用 Amazon VPC 資源。IAM 是 AWS 服務 您可以免費使用的 。

目錄

- 目標對象
- 使用身分進行驗證
- 使用政策管理存取權
- Amazon VPC 如何與 IAM 搭配運作
- Amazon VPC 原則範例
- Amazon VPC 身分識別和存取疑難排解
- AWS Amazon Virtual Private Cloud 的 受管政策
- 使用 VPC 的服務連結角色

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Amazon VPC 中執行的工作。

服務使用者 – 若您使用 Amazon VPC 來執行您的任務，您的管理員可以提供您需要的登入資料和許可。隨著您為了執行作業而使用的 Amazon VPC 功能數量變多，您可能會需要額外的許可。了解存取的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon VPC 中的功能，請參閱 Amazon VPC 身分識別和存取疑難排解。

服務管理員 – 若您在公司負責管理 Amazon VPC 資源，您應該具備服務使用的完整存取權限。您的任務是要判斷員工應存取哪些 Amazon VPC 功能和資源。接著必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司可搭配 Amazon VPC 使用 IAM 的方式，請參閱 Amazon VPC 如何與 IAM 搭配運作。

IAM 管理員 – 如果您是 IAM 管理員，建議您掌握如何撰寫原則以管理 Amazon VPC 存取權的詳細資訊。若要檢視範例原則，請參閱Amazon VPC 原則範例。

使用身分進行驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon VPC 如何與 IAM 搭配運作

在您使用 IAM 管理對 Amazon VPC 的存取權之前，您應該瞭解哪些 IAM 功能可以與 Amazon VPC 搭配使用。若要全面了解 Amazon VPC 和其他 AWS 服務如何與 IAM 搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

目錄

- 動作
- Resources
- 條件索引鍵
- 以 Amazon VPC 資源為基礎的原則
- 以標籤為基礎的授權
- IAM 角色

使用 IAM 身分型原則，您可以指定允許或拒絕的動作。對於某些動作，您可以指定允許或拒絕動作的資源和條件。Amazon VPC 支援特定動作、資源和條件金鑰。若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

Amazon VPC 與 Amazon EC2 共享其 API 命名空間。Amazon VPC 中的原則動作會在動作之前使用下列前綴：`ec2:`。例如，若要授予使用 `CreateVpc` API 操作建立 VPC 的許可，請授予 `ec2:CreateVpc` 動作的存取權。政策陳述式必須包含 `Action` 或 `NotAction` 元素。

若要在單一陳述式中指定多個動作，請以逗號分隔它們，如下列範例所示。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，如需指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "ec2:Describe*"
```

若要查看 Amazon VPC 動作的清單，請參閱《服務授權參考》中的 Amazon EC2 定義的動作。

Resources

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

VPC 資源具有下列範例所示的 ARN。

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

例如，若要在陳述式中指定 `vpc-1234567890abcdef0` VPC，請使用下列範例中顯示的 ARN。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

若要指定屬於特定帳戶之特定區域中的所有 VPC，請使用萬用字元 (*)。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

有些 Amazon VPC 動作無法對特定資源執行，例如用來建立資源的動作。在這些情況下，您必須使用萬用字元 (*)。

```
"Resource": "*"
```

許多 Amazon EC2 API 動作都涉及多個資源。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
]
```

若要查看 Amazon VPC 資源類型及其 ARN 的清單，請參閱《服務授權參考》中的 Amazon EC2 定義的資源類型。

條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

所有 Amazon EC2 操作都支援 `aws:RequestedRegion` 和 `ec2:Region` 條件索引鍵。如需詳細資訊，請參閱範例：將存取限制在特定區域。

Amazon VPC 會定義自己的一組條件金鑰，也支援使用一些全域條件金鑰。若要查看 Amazon VPC 條件金鑰的清單，請參閱《服務授權參考》中的 Amazon EC2 的條件金鑰。若要了解您可以搭配哪些動作和資源使用條件金鑰，請參閱 Amazon EC2 定義的動作。

以 Amazon VPC 資源為基礎的原則

資源型原則是 JSON 原則文件，這些文件會指定指定的委託人可對 Amazon VPC 資源以及在怎樣的條件下執行哪些動作。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型原則的委託人。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同的 AWS 帳戶中時，您還必須授予委託人實體存取資源的許可。透過將身分型政策連接到實體來授予許可。不過，如果資源型政策會為相同帳戶中的委託人授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

以標籤為基礎的授權

您可以將標籤連線到 Amazon VPC 資源，或是在請求中傳遞標籤。若要根據標籤控制存取，請使用條件金鑰，在政策的條件元素中提供標籤資訊。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的在建立過程中向標籤資源授予許可。

若要檢視身分型原則範例，以根據該資源上的標籤來限制存取資源，請參閱在特定 VPC 中啟動執行個體。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的實體。

使用暫時性憑證

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 AssumeRole 或 GetFederationToken 等 AWS STS API 操作來取得臨時安全登入資料。

Amazon VPC 支援使用臨時登入資料。

服務連結角色

服務連結角色可讓 AWS 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。

傳輸閘道支援服務連結角色。

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，這樣可能會破壞此服務的功能。

Amazon VPC 支援流程日誌的服務角色。建立流程日誌時，您必須選擇允許流程日誌服務存取 CloudWatch Logs 的角色。如需詳細資訊，請參閱the section called “用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色”。

Amazon VPC 原則範例

根據預設，IAM 角色不具備建立或修改 VPC 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。IAM 管理員建立的 IAM 政策必須授予角色在指定資源上執行特定 API 操作的許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

目錄

- 政策最佳實務
- 使用 Amazon VPC 主控台
- 建立包含公有子網的 VPC
- 修改和刪除 VPC 資源
- 管理安全群組
- 管理安全群組規則
- 在特定子網中啟動執行個體
- 在特定 VPC 中啟動執行個體
- 封鎖對 VPC 和子網路的公開存取
- 其他 Amazon VPC 原則範例

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Amazon VPC 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並轉向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作

AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 Amazon VPC 主控台

若要存取 Amazon VPC 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視 AWS 帳戶中 Amazon VPC 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (IAM 角色) 而言，主控台就無法如預期運作。

下列政策會授與角色在 VPC 主控台中列出資源的許可，但不會建立、更新或刪除這些資源。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
```

```
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

對於僅呼叫 AWS CLI 或 AWS API 的角色，您不需要允許最低主控台許可。反之，只需允許存取符合角色所需執行之 API 操作的動作就可以了。

建立包含公有子網的 VPC

下列範例可讓角色建立 VPC、子網路、路由表和網際網路閘道。角色也可以將網際網路閘道連接至 VPC，並在路由表中建立路由。此 `ec2:ModifyVpcAttribute` 動作可讓角色啟用 VPC 的 DNS 主機名稱，以便啟動至 VPC 的每個執行個體都會收到一個 DNS 主機名稱。

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource": "*"
    }
   ]
}
```

上述政策還可讓角色在 Amazon VPC 主控台中建立 VPC。

修改和刪除 VPC 資源

您可能想要控制角色可以修改或刪除的 VPC 資源。例如，下列政策允許角色使用和刪除具有標籤 `Purpose=Test` 的路由表。此政策也會指定角色只能刪除具有標籤 `Purpose=Test` 的網際網路閘道。角色無法使用沒有此標籤的路由表或網際網路閘道。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteInternetGateway",
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

管理安全群組

下列政策可讓角色管理安全群組。第一個陳述式允許角色刪除任何具有標籤 Stack=test 的安全群組並管理具有標籤 Stack=test 的任何安全群組的傳入和傳出規則。第二個陳述式要求角色使用標籤 Stack=Test 來標記每一個他們建立的安全群組。第三個陳述式允許角色在建立安全群組時建立標籤。第四個陳述式允許角色檢視任何安全群組和安全群組規則。第五個陳述式允許角色在 VPC 中建立安全群組。

> **Note**
>
> AWS CloudFormation 服務無法使用此政策來建立具有必要標籤的安全群組。如果您移除需要標記之 `ec2:CreateSecurityGroup` 動作上的條件，則該政策會有效。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

若要允許角色變更與執行個體相關聯的安全群組，請將 `ec2:ModifyInstanceAttribute` 動作新增至您的政策。

若要允許角色變更網路介面的安全群組，請將 `ec2:ModifyNetworkInterfaceAttribute` 動作新增至您的政策。

管理安全群組規則

下列政策會授予角色許可，以允許角色檢視所有安全群組和安全群組規則、為特定 VPC 的安全群組新增和移除傳入和傳出規則，以及修改指定 VPC 的規則描述。第一個陳述式使用 `ec2:Vpc` 條件金鑰將許可範圍設定為特定 VPC。

第二個陳述式會授予角色許可，以允許角色描述所有安全群組、安全群組規則和標籤。這可讓角色檢視安全群組規則，以便進行修改。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:ModifySecurityGroupRules"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:security-group/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySecurityGroupRules"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:security-group-rule/
*"
        }
    ]
```

```
}
```

在特定子網中啟動執行個體

下列政策會授予角色許可，以允許角色在特定子網路中啟動執行個體以及在請求中使用特定安全群組。此政策執行這項作業的方式是指定子網路的 ARN 和安全群組的 ARN。如果角色嘗試在不同的子網路中啟動執行個體，或使用不同的安全群組來啟動執行個體，則請求會失敗 (除非另一個政策或陳述式授予了角色執行此作業的許可)。

此政策也會授予許可來使用網路界面資源。在子網路中啟動時，根據預設，RunInstances 請求會建立主要網路介面，因此角色需要在啟動執行個體時建立此資源的許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1::image/ami-*",
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-
east-1:123456789012:subnet/subnet-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-
group/sg-0abcdef1234567890"
            ]
        }
    ]
}
```

在特定 VPC 中啟動執行個體

下列政策會授予角色許可，以允許角色在特定 VPC 的任何子網路中啟動執行個體。此政策執行這項作業的方式是將條件金鑰 (ec2:Vpc) 套用至子網路資源。

此政策也會授予角色許，以允許角色僅使用具有 "department=dev" 標籤的 AMI 啟動執行個體。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:subnet/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-group/*"
            ]
        }
    ]
}
```

封鎖對 VPC 和子網路的公開存取

下列政策範例授予角色許可，以使用 VPC 封鎖公開存取 (BPA) 功能，以封鎖對 VPC 和子網路中資源的公開存取。

範例 1 – 允許唯讀存取 VPC BPA 全帳戶設定和 VPC BPA 排除。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

範例 2 – 允許完整讀取和寫入存取 VPC BPA 全帳戶設定和 VPC BPA 排除。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
```

```
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

範例 3 – 允許存取所有 EC2 API，但修改 VPC BPA 設定和建立排除除外。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EC2FullAccess",
            "Action": [
                "ec2:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "VPCBPAPartialAccess",
            "Action": [
                "ec2:ModifyVpcBlockPublicAccessOptions",
                "ec2:CreateVpcBlockPublicAccessExclusion"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }
    ]
}
```

其他 Amazon VPC 原則範例

您可以在下列文件中找到與 Amazon VPC 相關的其他 IAM 政策範例：

- 受管理的字首清單
- 流量鏡射

- 傳輸閘道
- VPC 端點與 VPC 端點服務 (AWS PrivateLink)
- VPC 對等互連

Amazon VPC 身分識別和存取疑難排解

請使用以下資訊來協助您診斷和修正使用 Amazon VPC 和 IAM 時可能遇到的常見問題。

問題

- 我未獲授權，不得在 Amazon VPC 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 Amazon VPC 資源

我未獲授權，不得在 Amazon VPC 中執行動作

如果 AWS 管理主控台 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是您的登入憑證提供者。

如果 `mateojackson` IAM 使用者嘗試使用主控台檢視子網路的詳細資訊，但但該子網路卻屬於沒有 `ec2:DescribeSubnets` 許可的 IAM 角色，會發生以下範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

在此情況下，Mateo 會請求管理員更新政策，以允許他存取子網路。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 Amazon VPC。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 Amazon VPC 中執行動作時，發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 Amazon VPC 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

若要進一步了解，請參閱以下內容：

- 若要了解 Amazon VPC 是否支援這些功能，請參閱 Amazon VPC 如何與 IAM 搭配運作。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

AWS Amazon Virtual Private Cloud 的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 （ 使用者、群組和角色 ）。當新的 啟動或新的 API 操作可供現有 服務使用時， AWS 最有可能更新 AWS 服務 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：AmazonVPCFullAccess

您可以將 AmazonVPCFullAccess 政策連接到 IAM 身分。此政策授與允許 Amazon VPC 完整權限的許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 AmazonVPCFullAccess。

AWS 受管政策：AmazonVPCReadOnlyAccess

您可以將 AmazonVPCReadOnlyAccess 政策連接到 IAM 身分。此政策授與允許 Amazon VPC 唯讀權限的許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 AmazonVPCReadOnlyAccess。

AWS 受管政策：AmazonVPCCrossAccountNetworkInterfaceOperations

您可將 AmazonVPCCrossAccountNetworkInterfaceOperations 政策連接到 IAM 身分。此策略授予允許身分建立網路介面並將其連接至跨帳戶資源的許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 AmazonVPCCrossAccountNetworkInterfaceOperations。

AWS 受管政策：AWSServiceRoleForNATGateway

您可將 AWSServiceRoleForNATGateway 政策連接到 IAM 身分。此政策會授予許可，允許身分代表您自動擴展區域 NAT 閘道。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AWSServiceRoleForNATGateway。

AWS 受管政策的 Amazon VPC 更新

檢視自此服務於 2021 年 3 月開始追蹤 Amazon VPC AWS 受管政策更新以來的詳細資訊。

變更	描述	日期
the section called “AmazonVPCFullAccess” – 更新現有政策	新增至 AWSIPAMServiceRolePolicy 受管政策 (ec2:ModifyManagedPrefixList、ec2:DescribeManagedPrefixLists 和 ec2:GetManagedPrefixListEntries) 的動作	2025 年 10 月 31 日

變更	描述	日期
	讓 IPAM 能夠修改與讀取受管字首清單。	
the section called “AWSServiceRoleForNATGateway ” – 新政策	新的 AWSServiceRoleForNATGateway 政策允許身分自動擴展區域 NAT 閘道。	2025 年 11 月 19 日
the section called “AmazonVPCFullAccess” – 更新現有政策	新增了 AssociateSecurityGroupVpc、DescribeSecurityGroupVpcAssociations 和 DisassociateSecurityGroupVpc 動作，讓您可以建立、取消與檢視 VPC 的安全群組關聯。	2024 年 12 月 9 日
the section called “AmazonVPCReadOnlyAccess” – 更新現有政策	新增了 DescribeSecurityGroupVpcAssociations 動作，讓您可以檢視與 VPC 的安全群組關聯。	2024 年 12 月 9 日
the section called “AmazonVPCFullAccess” – 更新現有政策	新增 GetSecurityGroupsForVpc 動作，可讓您取得可在 VPC 中使用的安全群組。	2024 年 2 月 8 日
the section called “AmazonVPCReadOnlyAccess” – 更新現有政策	新增 GetSecurityGroupsForVpc 動作，可讓您取得可在 VPC 中使用的安全群組。	2024 年 2 月 8 日
the section called “AmazonVPCCrossAccountNetworkInterfaceOperations” – 更新現有政策	已新增 AssignIpv6Addresses 和 UnassignIpv6Addresses 動作，可讓您管理與網路介面關聯的 IPv6 地址。	2023 年 9 月 25 日
the section called “AmazonVPCReadOnlyAccess” – 更新現有政策	新增了 DescribeSecurityGroupRules 動作，可讓您檢視安全群組規則。	2021 年 8 月 2 日

變更	描述	日期
the section called “AmazonVPCFullAccess” – 更新現有政策	新增了 DescribeSecurityGroupRules 和 ModifySecurityGroupRules 動作，可讓您檢視和修改安全群組規則。	2021 年 8 月 2 日
the section called “AmazonVPCFullAccess” – 更新現有政策	新增了針對電信業者閘道、IPv6 集區、本機閘道和本機閘道路由表的動作。	2021 年 6 月 23 日
the section called “AmazonVPCReadOnlyAccess” – 更新現有政策	新增了針對電信業者閘道、IPv6 集區、本機閘道和本機閘道路由表的動作。	2021 年 6 月 23 日

使用 VPC 的服務連結角色

Amazon VPC 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 VPC 的唯一 IAM 角色類型。服務連結角色由 VPC 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 VPC，因為您不必手動新增必要的許可。VPC 定義其服務連結角色的許可，除非另有定義，否則只有 VPC 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 VPC 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

VPC 的服務連結角色許可

VPC 使用名為 AWSServiceRoleForNATGateway 的服務連結角色 – 此服務連結角色可讓 Amazon VPC 代表您配置彈性 IP 地址，以自動擴展區域 NAT 閘道、將現有彈性 IPs 與區域 NAT 閘道建立關聯，以及描述網路界面，以識別要自動擴展至新可用區域。

AWSServiceRoleForNATGateway 服務連結角色信任下列服務擔任該角色：

- ec2-nat-gateway.amazonaws.com

名為 AWSNATGatewayServiceRolePolicy 的角色許可政策可讓 VPC 對指定的資源完成下列動作：

- 動作：在服務受管 EIPs AllocateAddress上代表您配置 EIPs。服務受管 EIPs會自動使用服務受管標籤和 ReleaseAddress 處理後續標記。
- 動作：在您預先存在的彈性 IP 地址AssociateAddress上，依您的請求手動將它們與區域 NAT Gateway 建立關聯。
- 動作：在您預先存在的彈性 IP 地址DisassociateAddress上，依您的請求從區域 NAT Gateway 移除它們。
- 動作：從關聯上客戶提供EIPs 取得公DescribeAddresses有 IP 地址資訊。
- 動作：在現有的網路界面DescribeNetworkInterface上，自動識別基礎設施所在的可用區域，以自動擴展到新區域。

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 VPC 建立服務連結角色

您不需要手動建立服務連結角色，當您在 AWS CLI、 或 AWS API 中建立具有「區域」可用模式的 NAT 閘道 AWS 管理主控台時，VPC 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。此外，如果您在 2017 年 1 月 1 日之前使用 VPC 服務，則當 VPC 開始支援服務連結角色時，VPC 會在您的帳戶中建立 AWSServiceRoleForNATGateway 角色。若要進一步了解，請參閱我的 中出現的新角色 AWS 帳戶。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您使用「區域」可用性模式建立 NAT 閘道時，VPC 會再次為您建立服務連結角色。

您也可以使用 IAM 主控台建立具有 AWSServiceRoleForNATGateway 使用案例的服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立ec2-nat-gateway.amazonaws.com服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 VPC 的服務連結角色

VPC 不允許您編輯 AWSServiceRoleForNATGateway 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。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 VPC 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果 VPC 服務在您嘗試刪除資源時使用角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForNATGateway 使用的 VPC 資源

- 刪除所有已部署區域的所有區域 NAT 閘道。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForNATGateway 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

VPC 服務連結角色支援的 區域

VPC 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Regions and endpoints。

VPC 不支援在提供服務的每個區域中使用服務連結角色。您可以在下列區域中使用 AWSServiceRoleForNATGateway 角色。

區域名稱	區域身分	VPC 中的支援
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是

區域名稱	區域身分	VPC 中的支援
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
Africa (Cape Town)	af-south-1	是
亞太地區 (香港)	ap-east-1	是
亞太區域 (台北)	ap-east-2	是
亞太地區 (雅加達)	ap-southeast-3	是
亞太區域 (孟買)	ap-south-1	是
亞太地區 (海德拉巴)	ap-south-2	是
亞太區域 (大阪)	ap-northeast-3	是
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
亞太區域 (東京)	ap-northeast-1	是
亞太地區 (墨爾本)	ap-southeast-4	是
亞太地區 (馬來西亞)	ap-southeast-5	是
亞太區域 (紐西蘭)	ap-southeast-6	是
亞太區域 (泰國)	ap-southeast-7	是
加拿大 (中部)	ca-central-1	是
加拿大西部 (卡加利)	ca-west-1	是
歐洲 (法蘭克福)	eu-central-1	是

區域名稱	區域身分	VPC 中的支援
歐洲 (蘇黎世)	eu-central-2	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	是
歐洲 (米蘭)	eu-south-1	是
歐洲 (西班牙)	eu-south-2	是
歐洲 (巴黎)	eu-west-3	是
Europe (Stockholm)	eu-north-1	是
以色列 (特拉維夫)	il-central-1	是
Middle East (Bahrain)	me-south-1	是
中東 (阿拉伯聯合大公國)	me-central-1	是
中東 (沙烏地阿拉伯)	me-west-1	是
墨西哥 (中部)	mx-central-1	是
南美洲 (聖保羅)	sa-east-1	是
AWS GovCloud (US-East)	us-gov-east-1	否
AWS GovCloud （美國西部）	us-gov-west-1	否

Amazon VPC 的基礎設施安全性

Amazon Virtual Private Cloud 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Amazon VPC。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。

- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

網路隔離

虛擬私有雲端 (VPC) 是 AWS 雲端中您自己的邏輯隔離區域中的虛擬網路。使用不同的 VPC，依工作負載或組織實體來隔離基礎設施。

子網是您的 VPC 中的 IP 地址範圍。啟動執行個體時，您會在 VPC 的子網中啟動它。使用子網來隔離單一 VPC 內的應用程式層 (例如，Web、應用程式及資料庫)。如果不應該從網際網路直接存取，則針對您的執行個體使用私有子網。

您可以使用 AWS PrivateLink讓 VPC 中的資源 AWS 服務 使用私有 IP 地址連線至 ，就像這些服務直接託管在 VPC 中一樣。因此，您不需要使用網際網路閘道或 NAT 裝置來存取 AWS 服務。

控制網路流量

請考慮下列選項來控制您 VPC 中的資源 (例如 EC2 執行個體) 的網路流量：

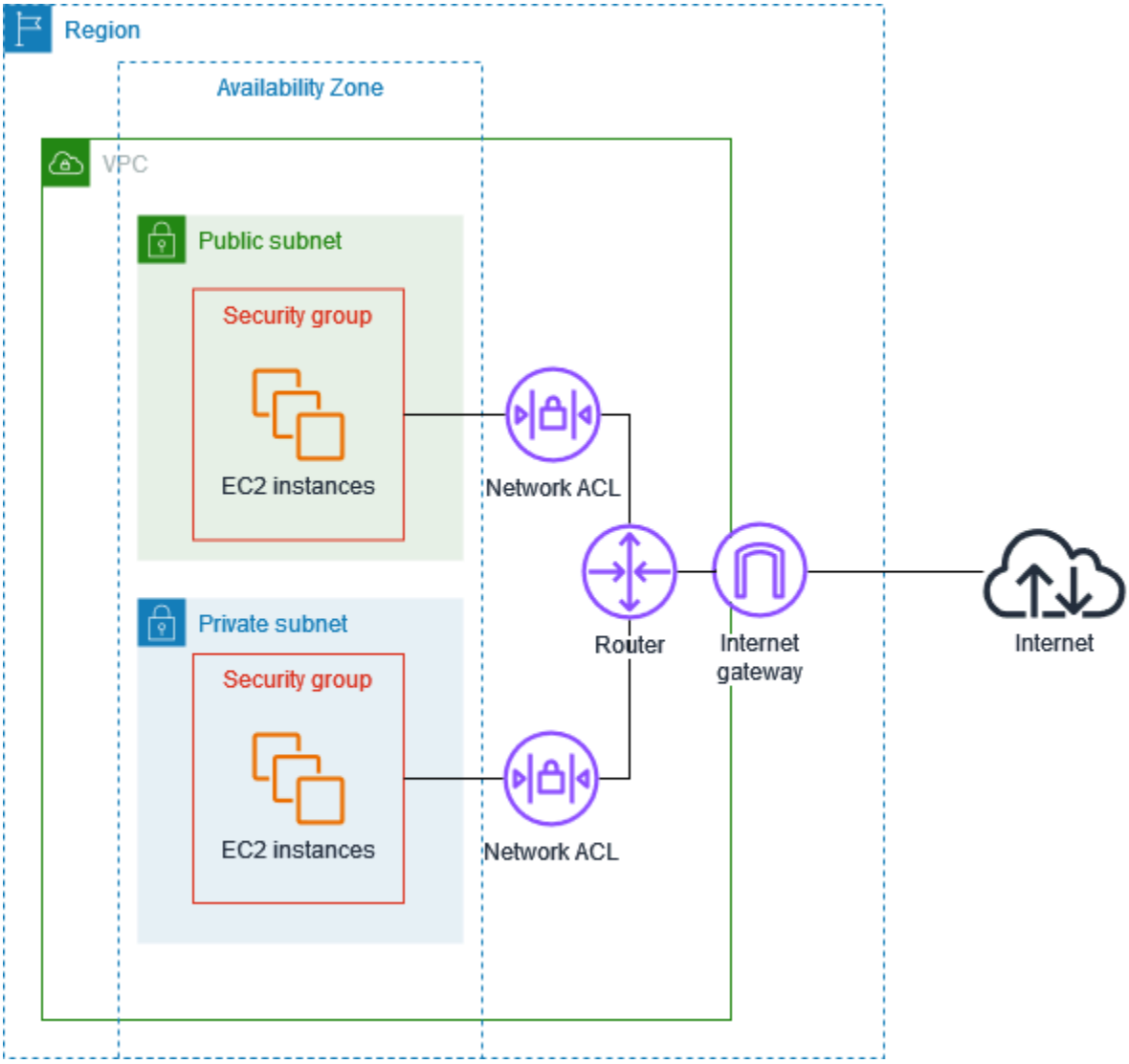
- 使用安全群組做為控制網路存取 VPC 的主要機制。必要時，請使用 網路 ACL 來提供無狀態、粗糙的網路控制。安全群組比網路 ACL 更多用途，因為它們能夠執行有狀態封包篩選，並建立參考其他安全群組的規則。網路 ACL 可以有效地作為次要控制項 (例如拒絕特定流量子集) 或作為高階子網路防護護欄。此外，因為網路 ACL 會套用至整個子網路，所以執行個體若在沒有正確安全群組的情況下啟動，它們可以用作深度防禦。
- 如果不應該從網際網路直接存取，則針對您的執行個體使用私有子網。使用堡壘主機或 NAT 閘道，以取得來自私有子網路中執行個體的網際網路存取權限。
- 設定具有最少網路路由的子網路路由表，以支援連線需求。
- 請考慮使用其他安全群組或網路界面，來控制和稽核 Amazon EC2 執行個體管理流量，並與一般應用程式流量分開。因此，您可以實作變更控制的特殊 IAM 政策，讓稽核安全群組規則或自動規則驗證指令碼的變更變得更輕鬆。多個網路介面也提供控制網路流量的其他選項，包括能夠建立以主機為基礎的路由政策，或根據指派給子網路的網路介面使用不同的 VPC 子網路路由規則。
- 使用 AWS Virtual Private Network 或 Direct Connect 建立從遠端網路到 VPCs私有連線。如需詳細資訊，請參閱 Network-to-Amazon VPC 連線選項。
- 使用 VPC 流程日誌監控到達您執行個體的流量。
- 使用 AWS Security Hub CSPM 檢查來自您執行個體的意外網路存取性。
- 使用 AWS Network Firewall 保護 VPC 中的子網路，以免遭受常見網路威脅的侵害。

比較安全群組和網路 ACL

下表總結了安全群組與網路 ACL 之間的基本差異。

特性	安全群組	網路 ACL
操作層級	執行個體層級	子網路層級
Scope (範圍)	適用於與安全群組相關聯的所有執行個體	適用於關聯子網路中的所有執行個體
規則類型	僅支援允許規則	支援允許與拒絕規則
規則評估	在決定是否允許流量前，先評估所有規則	以遞增順序評估規則，直至找到流量的相符項為止
傳回流量	自動允許 (具狀態)	必須明確允許 (無狀態)

下表說明安全群組和網路 ACL 提供的安全 layer。例如，網際網路閘道傳出的流量會透過路由表中的路由來路由至適合的子網路。與子網路相關聯的網路 ACL 規則會控制允許哪些流量傳入子網路。與執行個體相關聯的安全群組規則會控制允許哪些流量傳入執行個體。



您只能使用安全群組來保護執行個體。不過，您可以新增網路 ACL 做為額外的防禦層。如需詳細資訊，請參閱範例：控制對子網路中執行個體的存取。

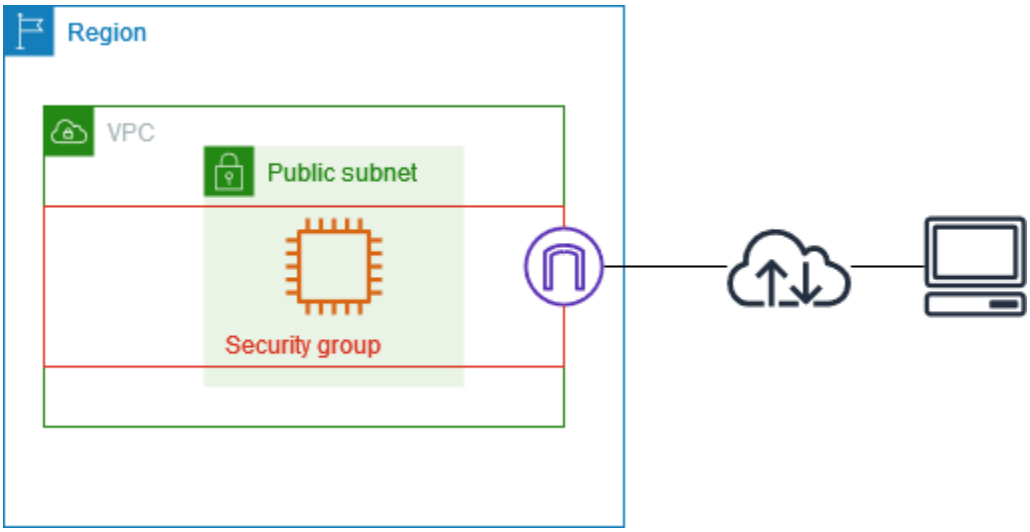
使用安全群組控制 AWS 資源的流量

安全群組負責控制允許到達和離開其關聯資源的流量。例如，將安全群組與 EC2 執行個體相關聯後，就會控制執行個體的傳入和傳出流量。

當您建立 VPC 時，其具有一個預設的安全群組。您可以為 VPC 建立額外的安全群組，每個群組都有自己的傳入及傳出規則。您可以為每個傳入規則指定來源、連接埠範圍和通訊協定。您可以為每個傳出規則指定目的地、連接埠範圍和通訊協定。

下圖顯示具有子網路、網際網路閘道和安全群組的 VPC。子網路包含 EC2 執行個體。指派給執行個體的安全群組。安全群組會做為虛擬防火牆。僅有安全群組規則允許的流量才能到達執行個體。例如，如

果安全群組包含允許 ICMP 流量從您的網路傳輸至執行個體的規則，您即可從電腦 ping 執行個體。如果安全群組不包含允許 SSH 流量的規則，則您無法使用 SSH 連線至執行個體。



目錄

- 安全群組基礎知識
- 安全群組範例
- 安全群組規則
- VPC 的預設安全群組
- 為 VPC 建立安全群組
- 設定安全群組規則
- 刪除安全群組
- 將安全群組與多個 VPC 建立關聯
- 與 AWS Organizations 共用安全群組

定價

使用安全群組無需額外收費。

安全群組基礎知識

- 如果使用安全群組 VPC 關聯功能將安全群組與相同區域中的其他 VPC 建立關聯，可以將安全群組指派給在與該安全群組相同的 VPC 中建立的資源，或指派給其他 VPC 中的資源。還可以將多個安全群組指派單個資源。
- 當您建立安全群組時，您必須提供名稱和描述。適用的規定如下：

  - 安全群組名稱在 VPC 中必須是唯一的。
  - 安全群組名稱不區分大小寫。
  - 名稱和描述的長度最多可達 255 個字元。
  - 名稱和描述僅能使用下列字元：a-z、A-Z、0-9、空格，以及 ._-:/()#,@[]+=&;{}!$*。
  - 當名稱包含結尾空格時，我們會裁剪名稱結尾處的空格。例如，如果您輸入「測試安全群組」做為名稱，我們會將其儲存為「測試安全群組」。
  - 安全群組名稱的開頭不能是 `sg-`。
- 安全群組具狀態。例如，若您從執行個體傳送請求，則允許該請求的回應流量到達執行個體，不論傳入安全群組規則為何。都會允許對允許傳入流量的回應離開執行個體，不論傳出規則為何。
- 安全群組不會篩選往返下列位置的流量：
  - Amazon 網域名稱服務 (DNS)
  - Amazon 動態主機設定通訊協定 (DHCP)
  - Amazon EC2 執行個體中繼資料
  - Amazon ECS 任務中繼資料端點
  - Windows 執行個體的授權啟動
  - Amazon Time Sync Service
  - 預設 VPC 路由器使用的保留 IP 地址
- 您可以為每個 VPC 建立的安全群組數、每個安全群組可新增的規則數，以及您可以與網路介面建立關聯的安全群組數都具有配額。

  如需詳細資訊，請參閱Amazon VPC 配額。

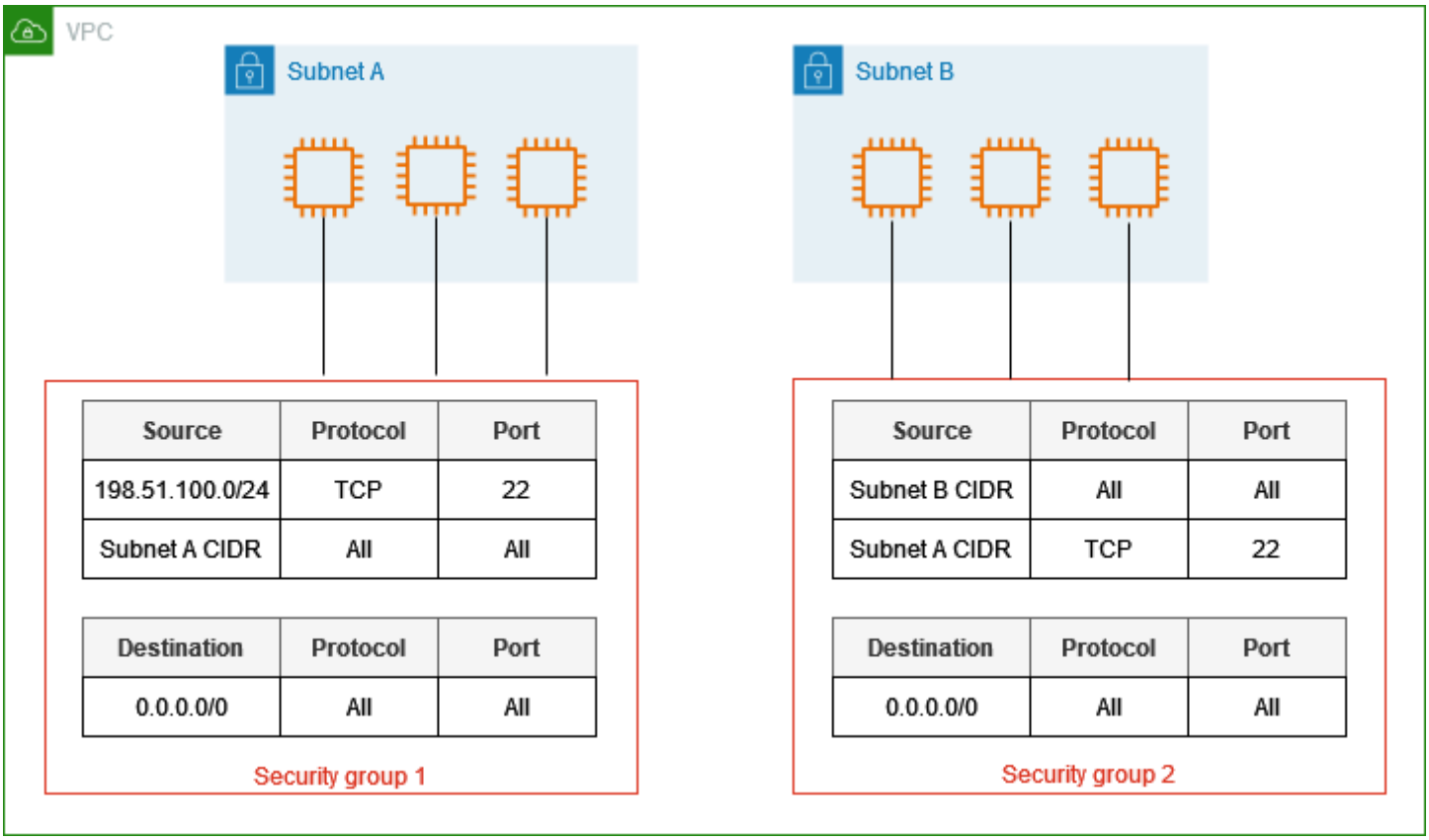
最佳實務

- 僅授權特定 IAM 主體建立和修改安全群組。
- 建立您需要的最小數量的安全群組，以降低發生錯誤的風險。使用每個安全群組來管理對具有類似功能和安全要求之資源的存取權。
- 在您為連接埠 22 (SSH) 或 3389 (RDP) 新增傳入規則以便可以存取 EC2 執行個體時，僅授權特定 IP 地址範圍。如果您指定 0.0.0.0/0 (IPv4) 和 ::/ (IPv6)，這可讓任何人使用指定的通訊協定從任何 IP 地址存取您的執行個體。
- 請勿開啟較大的連接埠範圍。確保透過每個連接埠進行的存取僅限於需要連接埠的來源或目的地。
- 考慮使用與您的安全群組相似的規則來建立網路 ACL，以為您的 VPC 新增額外的安全層。如需有關安全群組與網路 ACL 間差異的詳細資訊，請參閱比較安全群組和網路 ACL。

安全群組範例

下圖顯示了具有兩個安全群組和兩個子網路的 VPC。子網路 A 中的執行個體具有相同的連線需求，因此與安全群組 1 相關聯。子網路 B 中的執行個體具有相同的連線需求，因此與安全群組 2 相關聯。安全群組規則允許流量如下：

- 安全群組 1 中的第一個輸入規則允許從指定地址範圍 (例如，您自己網路中的範圍) 傳輸至子網路 A 中執行個體的 SSH 流量。
- 安全群組 1 中的第二個輸入規則允許子網路 A 中的執行個體使用任何通訊協定和連接埠相互通訊。
- 安全群組 2 中的第一個輸入規則允許子網路 B 中的執行個體使用任何通訊協定和連接埠相互通訊。
- 安全群組 2 中的第二個輸入規則允許子網路 A 中的執行個體使用 SSH 與子網路 B 中的執行個體通訊。
- 兩個安全群組均使用預設傳出規則，允許所有流量。



安全群組規則

安全群組的規則可控制允許到達與安全群組相關聯之資源的傳入流量。規則也會控制允許離開的對外流量。

您可以新增或移除安全群組的規則 (也稱為授權或撤銷傳入或傳出存取)。規則會套用至傳入流量 (輸入) 或傳出流量 (輸出)。您可以授予特定來源或目的地的存取權。

目錄

- 安全群組規則基礎知識
- 安全群組規則的元件
- 安全群組參考
- 安全群組大小
- 過時的安全群組規則

安全群組規則基礎知識

以下為安全群組規則的特性：

- 您可以指定允許規則，但無法指定拒絕規則。
- 當您首次建立安全群組時，它沒有傳入規則。因此，在您將傳入規則新增到安全群組之前，都不會允許傳入流量。
- 當您首次建立安全群組時，該安全群組會具有允許來自該資源的所有傳出流量的傳出規則。您可以移除規則並新增只允許特定傳出流量的傳出規則。若您的安全群組沒有傳出規則，將不會允許傳出流量。
- 當您將多個安全群組與資源建立關聯時，會將每個安全群組的規則彙總以構成一組規則，並使用這組規則來決定是否允許存取。
- 當您新增、更新或移除規則時，您的變更會自動套用至與安全群組相關聯的所有資源。如需說明，請參閱設定安全群組規則。
- 有些規則變更的效果可取決於追蹤流量的方式。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線追蹤。
- 當您建立安全群組規則時， 會 AWS 為規則指派唯一的 ID。當您使用 API 或 CLI 修改或刪除規則時，可以使用規則的 ID。

限制

安全群組無法封鎖有時稱為「VPC+2 IP 位址」(請參閱《Amazon Route 53 開發人員指南》中的 Amazon Route 53 Resolver) 或 AmazonProvidedDNS 的 Route 53 Resolver 所接收或發出的 DNS 請求。若要透過 Route 53 Resolver 篩選 DNS 請求，請使用 Route 53 Resolver DNS Firewall。

安全群組規則的元件

以下是傳入和傳出安全群組規則的組成部分：

- 通訊協定：要允許的通訊協定。最常見的通訊協定為 6 (TCP)、17 (UDP) 和 1 (ICMP)。
- 連接埠範圍：適用於 TCP、UDP 或自訂通訊協定，要允許的連接埠範圍。您可以指定單一連接埠號碼 (例如，22)，或是連接埠號碼的範圍 (例如，7000-8000)。
- ICMP 類型及代碼：適用於 ICMP，為 ICMP 的類型及代碼。例如，使用類型 8 代表「ICMP Echo 請求」，輸入 128 則代表「ICMPv6 Echo 請求」。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Ping/ICMP 的規則。
- 來源或目的地：允許流量的來源 (傳入規則) 或目的地 (傳出規則)。請指定下列其中一項：
  - 單一 IPv4 地址。您必須使用 /32 的字首長度。例如 203.0.113.1/32。
  - 單一 IPv6 地址。您必須使用 /128 的字首長度。例如 2001:db8:1234:1a00::123/128。
  - IPv4 地址範圍，以 CIDR 區塊標記法表示。例如 203.0.113.0/24。
  - IPv6 地址範圍，以 CIDR 區塊標記法表示。例如 2001:db8:1234:1a00::/64。
  - 字首清單的 ID。例如 pl-1234abc1234abc123。如需詳細資訊，請參閱受管理的字首清單。
  - 安全群組的 ID。例如 sg-1234567890abcdef0。如需詳細資訊，請參閱the section called “安全群組參考”。
- (Optional) Description ((選用) 描述)：您可以為規則新增描述，這可協助您在稍後更容易識別它。描述的長度最高可達 255 個字元。允許的字元為 a-z、A-Z、0-9、空格鍵和 ._-:/()#,@[]+=;{}!$*。

如需範例，請參閱《Amazon EC2 使用者指南》中的不同使用案例的安全群組規則。

安全群組參考

當您將安全群組指定為規則的來源或目的地時，規則會影響所有與安全群組相關聯的執行個體。執行個體可透過指定的通訊協定和連接埠，使用執行個體的私有 IP 地址，以指定的方向進行通訊。

例如，以下內容表示參考安全群組 sg-0abcdef1234567890 的安全群組傳入規則。此規則允許來自與 sg-0abcdef1234567890 關聯的執行個體的傳入 SSH 流量。

來源	通訊協定	連接埠範圍
sg-0abcdef1234567890	TCP	22

在安全群組規則中參考安全群組時，請注意下列事項：

- 如果下列任一情況為 true，您可以在另一個安全群組的傳入規則中參考安全群組：
  - 與同一 VPC 關聯的安全群組。
  - 與安全群組相關聯的 VPC 之間有互連連線。
  - 與安全群組相關聯的 VPC 之間有傳輸閘道。
- 如果下列任一情況為 true，您可以在傳出規則中參考安全群組：
  - 與同一 VPC 關聯的安全群組。
  - 與安全群組相關聯的 VPC 之間有互連連線。
- 所參考安全群組中的規則不會新增至參考該安全群組的安全群組。
- 對於傳入規則，與安全群組關聯的 EC2 執行個體可以從與參考安全群組相關聯之 EC2 執行個體的網路介面中的私有 IP 位址接收傳入流量。
- 對於傳出規則，與安全群組關聯的 EC2 執行個體可以將傳出流量傳送至與參考安全群組相關聯之 EC2 執行個體的網路介面中的私有 IP 位址。
- 我們不會在下列動作中對參考的安全群組進行授權：`AuthorizeSecurityGroupIngress`、`AuthorizeSecurityGroupEgress`、`RevokeSecurityG` 與 `RevokeSecurityGroupEgress`。我們只會檢查安全群組是否存在。此舉會導致以下情形：
  - 在 IAM 政策中為這些動作指定參考的安全群組沒有作用。
  - 當另一個帳戶擁有參考的安全群組時，擁有者帳戶不會收到這些動作的 CloudTrail 事件。

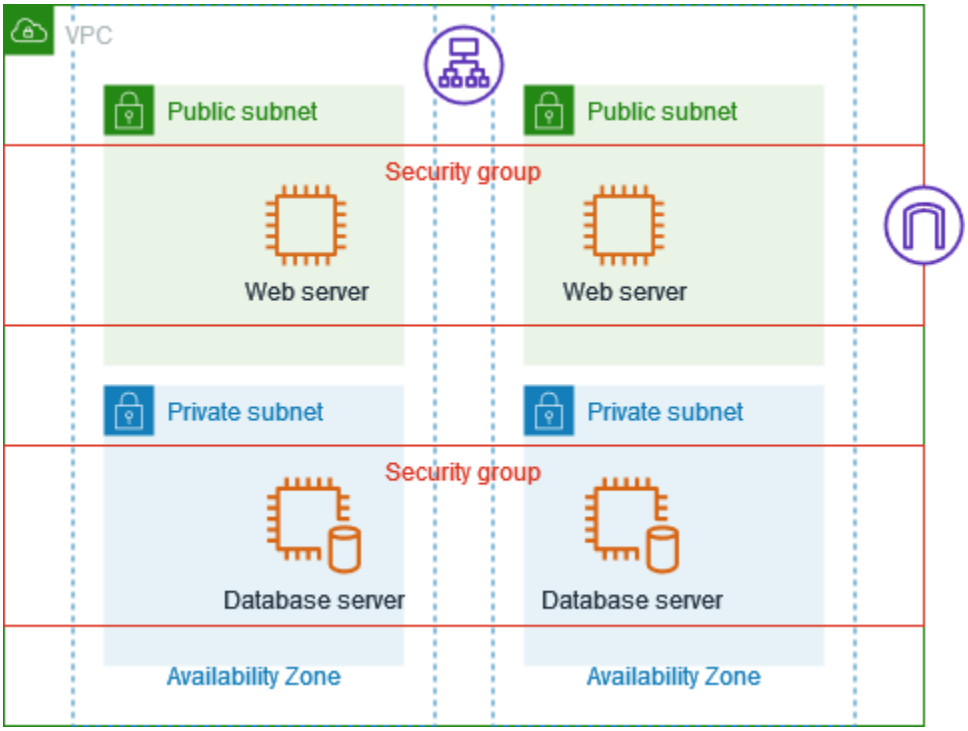
限制

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群組都必須參考另一個執行個體的私有 IP 地址，或是包含其他執行個體之子網路的 CIDR 範圍作為來源。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。

範例

下圖顯示在兩個可用區域中具有子網路、一個網際網路閘道和一個 Application Load Balancer 的 VPC。每個可用區域都有一個用於 Web 伺服器的公用子網路，以及一個用於資料庫伺服器的私有子網路。負載平衡器、Web 伺服器和資料庫伺服器有個別的安全群組。建立下列安全群組規則以允許流量。

- 將規則新增至負載平衡器的安全群組以允許來自網際網路的 HTTP 和 HTTPS 流量。來源是 0.0.0.0/0。
- 將規則新增至 Web 伺服器的安全群組，以僅允許來自負載平衡器的 HTTP 和 HTTPS 流量。來源是負載平衡器的安全群組。
- 將規則新增至資料庫伺服器的安全群組，以允許來自 Web 伺服器的資料庫請求。來源是 Web 伺服器的安全群組。



安全群組大小

來源或目的地類型會決定每個規則如何計入每個安全群組可擁有的規則數目上限。

- 參考 CIDR 區塊的規則會計為一個規則。
- 參考另一個安全群組的規則會計為一個規則，無論參考之安全群組的大小為何。
- 參考客戶管理之字首清單的規則會計為字首清單的大小上限。例如，如果字首清單的大小上限為 20，則參考此字首清單的規則會計為 20 個規則。

- 參考 AWS受管字首清單的規則會計入字首清單的權重。例如，如果字首清單的權重為 10，則參考此字首清單的規則會計為 10 個規則。如需詳細資訊，請參閱the section called “可用的 AWS受管字首清單”。

過時的安全群組規則

若 VPC 和另一個 VPC 之間有 VPC 對等互連連線或與其他帳戶共用一個 VPC，則 VPC 的安全群組規則會參考該對等 VPC 或共用 VPC 中的安全群組規則。這可讓與被參考安全群組相關聯的資源，以及與參考安全群組相關聯的執行個體彼此通訊。如需詳細資訊，請參閱《Amazon VPC 互連指南》中的更新您的安全群組，使其參考互連安全群組。

如果您有參考對等 VPC 或共用 VPC 中安全群組的安全群組規則，則在刪除參考的安全群組或刪除 VPC 對等連線時，規則會標記為過時。如同任何其他的安全群組規則，您可以刪除過時的安全群組規則。

VPC 的預設安全群組

您的預設 VPC 和您建立的任何 VPC 皆隨附預設的安全群組。預設安全群組的名稱為「default」。

建議您為特定資源或資源群組建立安全群組，而非使用預設安全群組。但是，如果您未在建立資源時關聯安全群組，則資源會關聯至預設安全群組。例如，如果您未在啟動 EC2 執行個體時指定安全群組，執行個體會與 VPC 的預設安全群組建立關聯。

預設安全群組基本概念

- 您可以變更預設安全群組的規則。
- 您無法刪除預設安全群組。若您嘗試刪除預設安全群組，我們會傳回下列錯誤代碼：`Client.CannotDelete`。

預設規則

下表說明預設安全群組的預設傳入規則。

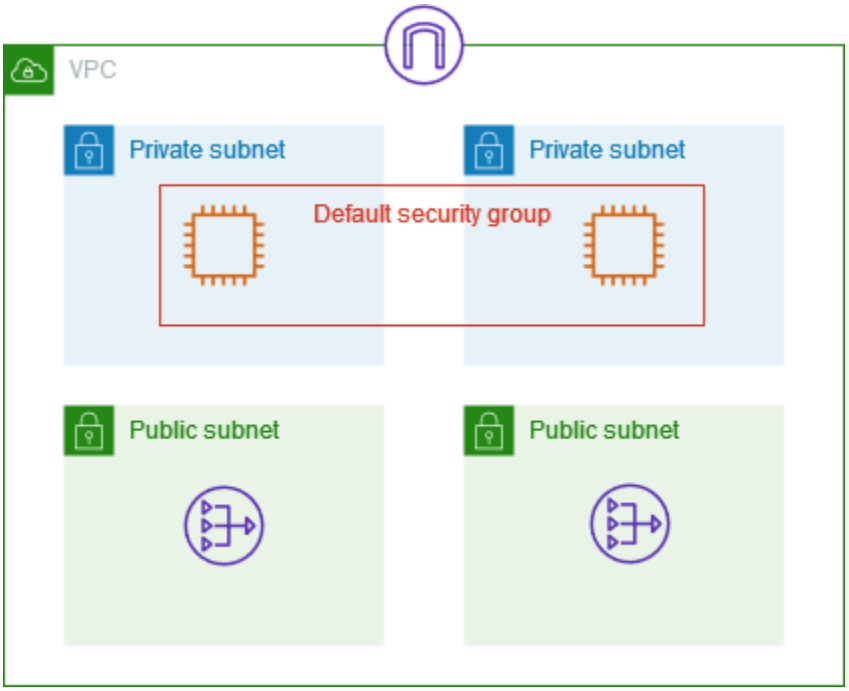
來源	通訊協定	連接埠範圍	說明
sg-1234567890abcdef0	全部	全部	允許來自指派給此安全群組的所有資源的傳入流量。來源為此安全群組的 ID。

下表說明預設安全群組的預設傳出規則。

目標	通訊協定	連接埠範圍	描述
0.0.0.0/0	全部	全部	允許所有傳出 IPv4 流量。
::/0	全部	全部	允許所有傳出 IPv6 流量。只有在 VPC 有相關聯的 IPv6 CIDR 區塊時，才會新增此規則。

範例

下圖顯示具有一個預設安全群組、一個網際網路閘道和一個 NAT 閘道的 VPC。預設安全措施僅包含其預設規則，並且它會與在 VPC 中執行的兩個 EC2 執行個體建立關聯。在此案例中，每個執行個體都可以從所有連接埠和通訊協定上的其他執行個體接收傳入流量。預設規則不允許執行個體從網際網路閘道或 NAT 閘道接收流量。如果您的執行個體必須接收額外流量，建議您建立一個具有所需規則的安全群組，並將新的安全群組與執行個體建立關聯，而不是與預設安全群組建立關聯。



為 VPC 建立安全群組

您的虛擬私有雲端 (VPC) 隨附預設安全群組。您可以建立額外的安全群組。安全群組只能在建立該群組的 VPC 的資源中使用。

根據預設，新的安全群組一開始只有允許流量離開資源的傳出規則。您必須新增規則啟用任何傳入流量，或是限制傳出流量。您可以在建立安全群組時新增規則，或稍後再新增。如需詳細資訊，請參閱安全群組規則。

所需的 許可

開始之前，請務必備妥必要的許可。如需詳細資訊，請參閱下列內容：

- 管理安全群組
- 管理安全群組規則

使用主控台建立安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組。
3. 選擇 Create Security Group (建立安全群組)。
4. 輸入安全群組的名稱和說明。您無法在建立安全群組之後變更安全群組的名稱和說明。
5. 對於 VPC，選擇您要建立與安全群組建立關聯的資源的 VPC。
6. (選用) 若要新增傳入規則，請選擇傳入規則。針對每個規則，選擇新增規則並指定通訊協定、連接埠和來源。如需詳細資訊，請參閱設定安全群組規則。
7. (選用) 若要新增傳出規則，請選擇傳出規則。針對每個規則，選擇新增規則並指定通訊協定、連接埠和目的地。
8. (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。
9. 選擇建立安全群組。

使用 建立安全群組 AWS CLI

使用 create-security-group 命令。

此外，您可以複製現有安全群組，以建立新的安全群組。當您複製安全群組時，我們會自動新增與原始安全群組相同的傳入和傳出規則，並使用與原始安全群組相同的 VPC。您可以輸入新安全群組的名稱和說明。您可以選擇不同的 VPC，也可以視需要修改傳入和傳出規則。但是，您無法將安全群組從一個區域複製到另一個區域。

根據現有的安全群組建立安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇安全群組。
3. 選取安全群組。
4. 選擇動作，複製到新的安全群組。
5. 輸入安全群組的名稱和說明。
6. (選用) 視需要選擇不同的 VPC。
7. (選用) 視需要新增、移除或編輯安全群組規則。
8. 選擇建立安全群組。

設定安全群組規則

建立安全群組之後，您可以新增、更新和刪除其安全群組規則。當您新增、更新或刪除規則時，變更會自動套用至與安全群組相關聯的任何資源。

所需的許可

開始之前，請務必備妥必要的許可。如需詳細資訊，請參閱管理安全群組規則。

通訊協定與連接埠

- 在主控台中選取預先定義的類型後，系統會為您指定通訊協定與連接埠範圍。如需輸入連接埠範圍，必須選取以下自訂類型之一：自訂 TCP 或自訂 UDP。
- 使用 AWS CLI，您可以使用 `--protocol`和 `--port`選項新增具有單一連接埠的單一規則。如需新增多項規則，或具有連接埠範圍的規則，請改用 `--ip-permissions` 選項。

資料來源和目的地

- 透過主控台，可指定下列內容作為傳入規則的來源，或傳出規則的目的地：
  - 自訂 – IPv4 CIDR 區塊、IPv6 CIDR 區塊、安全群組或字首清單。
  - Anywhere-IPv4 – 0.0.0.0/0 IPv4 CIDR 區塊。
  - Anywhere-IPv6 – ::/0 IPv6 CIDR 區塊。
  - 我的 IP：自動新增您本機電腦的公有 IPv4 地址。
- 透過 AWS CLI，您可以使用 `--cidr`選項指定 IPv4 CIDR 區塊，或使用 `--source-group`選項指定安全群組。若要指定字首清單或 IPv6 CIDR 區塊，請使用 `--ip-permissions` 選項。

> **Warning**
>
> 如果您選擇任何位置-IPv4，則會允許來自所有 IPv4 地址的流量。如果您選擇任何位置-IPv6，則會允許來自所有 IPv6 地址的流量。最佳實務是僅授權需要存取資源的特定 IP 位址範圍。

使用主控台為安全群組配置規則

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組。
3. 選取安全群組。
4. 若要編輯傳入規則，請從動作或傳入規則索引標籤中選擇編輯傳入規則。
   a. 若要新增規則，請選擇新增規則，並輸入規則的類型、通訊協定、連接埠和來源。

      針對 TCP 或 UDP，您必須輸入要允許的連接埠範圍。針對自訂 ICMP，則必須從 Protocol (通訊協定) 中選擇 ICMP 類型名稱，然後再從 Port Range (連接埠範圍) 中選擇代碼名稱 (若適用)。如果是任何其他類型，則系統會自動為您設定通訊協定和連接埠範圍。
   b. 若要更新規則，請視需要變更其通訊協定、描述和來源。不過，您無法變更來源類型。例如，如果來源是 IPv4 CIDR 區塊，則無法指定 IPv6 CIDR 區塊、字首清單或安全群組。
   c. 若要刪除規則，請選擇其刪除按鈕。
5. 若要編輯傳出規則，請從動作或傳出規則索引標籤中選擇編輯傳出規則。
   a. 若要新增規則，請選擇新增規則，並輸入規則的類型、通訊協定、連接埠和目的地。您也可以選擇輸入描述。

      針對 TCP 或 UDP，您必須輸入要允許的連接埠範圍。針對自訂 ICMP，則必須從 Protocol (通訊協定) 中選擇 ICMP 類型名稱，然後再從 Port Range (連接埠範圍) 中選擇代碼名稱 (若適用)。如果是任何其他類型，則系統會自動為您設定通訊協定和連接埠範圍。
   b. 若要更新規則，請視需要變更其通訊協定、描述和來源。不過，您無法變更來源類型。例如，如果來源是 IPv4 CIDR 區塊，則無法指定 IPv6 CIDR 區塊、字首清單或安全群組。
   c. 若要刪除規則，請選擇其刪除按鈕。
6. 選擇儲存規則。

使用 設定安全群組規則 AWS CLI

- 使用 authorize-security-group-ingress 和 authorize-security-group-egress 命令。
- 使用 revoke-security-group-ingress 和 revoke-security-group-egress 命令。
- 修改 – 使用 modify-security-group-rules、update-security-group-rule-descriptions-ingress 和 update-security-group-rule-descriptions-egress 命令。

刪除安全群組

當您完成建立的安全群組後，您可以將其刪除。

要求

- 安全群組無法與任何資源建立關聯。
- 安全群組不能被其他安全群組中的規則參考。
- 安全群組不能是 VPC 的預設安全群組。

使用主控台刪除安全群組

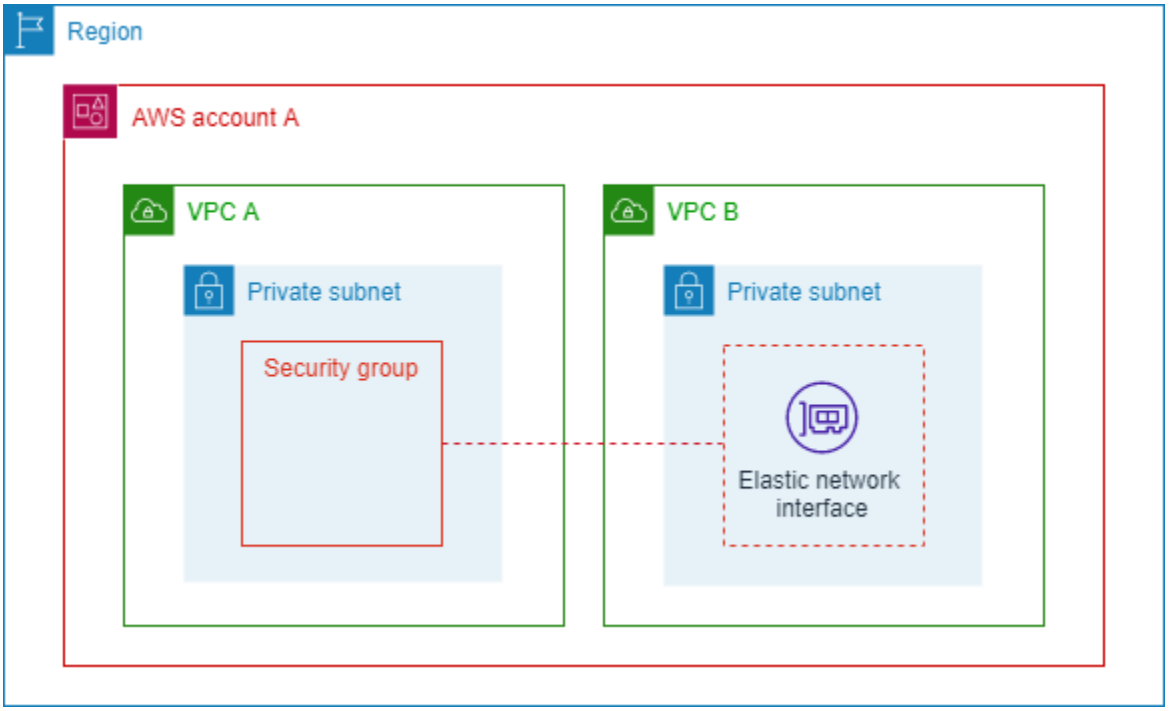
1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇安全群組。
3. 選取安全群組，然後選擇動作、刪除安全群組。
4. 如果您選擇多個安全群組，系統會提示您進行確認。如果無法刪除某些安全群組，我們會顯示每個安全群組的狀態，指出是否要刪除。若要確認刪除，請輸入刪除。
5. 選擇 刪除。

使用 刪除安全群組 AWS CLI

使用 delete-security-group 命令。

將安全群組與多個 VPC 建立關聯

如果您有工作負載在共用網路安全需求的多個 VPC 中執行，您可以使用安全群組 VPC 關聯功能，將安全群組與相同區域中的 VPC 建立關聯。這可讓您管理和維護您帳戶中多個 VPC 的安全群組。



上圖顯示帳戶 AWS A，其中包含兩個 VPCs。每個 VPC 都有在私有子網路中執行的工作負載。在此情況下，VPC A 和 B 子網路中的工作負載共用相同的網路流量需求，因此帳戶 A 可以使用安全群組 VPC 關聯功能，將 VPC A 中的安全群組與 VPC B 建立關聯。對相關安全群組所做的任何更新都會自動套用至 VPC B 子網路中的工作負載。

安全群組 VPC 關聯功能的需求

- 您必須擁有 VPC 或與您共用其中一個 VPC 子網路，才能將安全群組與 VPC 建立關聯。
- VPC 和安全群組必須位於相同的 AWS 區域。
- 您無法將預設安全群組與其他 VPC 建立關聯，或將安全群組與預設 VPC 建立關聯。
- 安全群組擁有者和 VPC 擁有者都可以檢視安全群組 VPC 關聯。

支援此功能的服務

- Amazon API Gateway (僅限 REST API)
- AWS Auto Scaling
- CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS

- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

將安全群組與另一個 VPC 建立關聯

本節說明如何使用 AWS 管理主控台 和 AWS CLI 將安全群組與 VPCs建立關聯。

AWS Management Console

為安全群組與另一個 VPC 建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左導覽窗格中，選擇安全群組。
3. 選擇安全群組，檢視其詳細資訊。
4. 選擇 VPC 關聯標籤。
5. 選擇 Associate VPC (關聯 VPC)。
6. 在 VPC ID 下，選擇要與安全群組建立關聯的 VPC。
7. 選擇 Associate VPC (關聯 VPC)。

Command line

將安全群組與另一個 VPC 建立關聯

1. 建立與 associate-security-group-vpc 的 VPC 關聯。
2. 檢查 VPC 與 describe-security-group-vpc-associations 的關聯狀態，並等待狀態變為 `associated`。

VPC 現在已與安全群組關聯。

將 VPC 與安全群組建立關聯後，例如，您可以在 VPC 中啟動執行個體，然後選擇此新的安全群組，或在現有的安全群組規則中參考此安全群組。

取消安全群組與另一個 VPC 的關聯

本節說明如何使用 AWS 管理主控台 和 AWS CLI 取消安全群組與 VPCs關聯。如果您的目標是刪除安全群組，您可能想要這麼做。如果安全群組已關聯，則無法刪除。只有在關聯的 VPC 中沒有網路介面使用該安全群組時，您才能取消關聯安全群組。

AWS Management Console

取消安全群組與 VPC 的關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左導覽窗格中，選擇安全群組。
3. 選擇安全群組，檢視其詳細資訊。
4. 選擇 VPC 關聯標籤。
5. 選擇取消關聯 VPC。
6. 在 VPC ID 下，選擇要與安全群組取消關聯的 VPC。
7. 選擇取消關聯 VPC。
8. 在 VPC 關聯標籤中檢視取消關聯的狀態，並等待狀態變為 `disassociated`。

Command line

取消安全群組與 VPC 的關聯

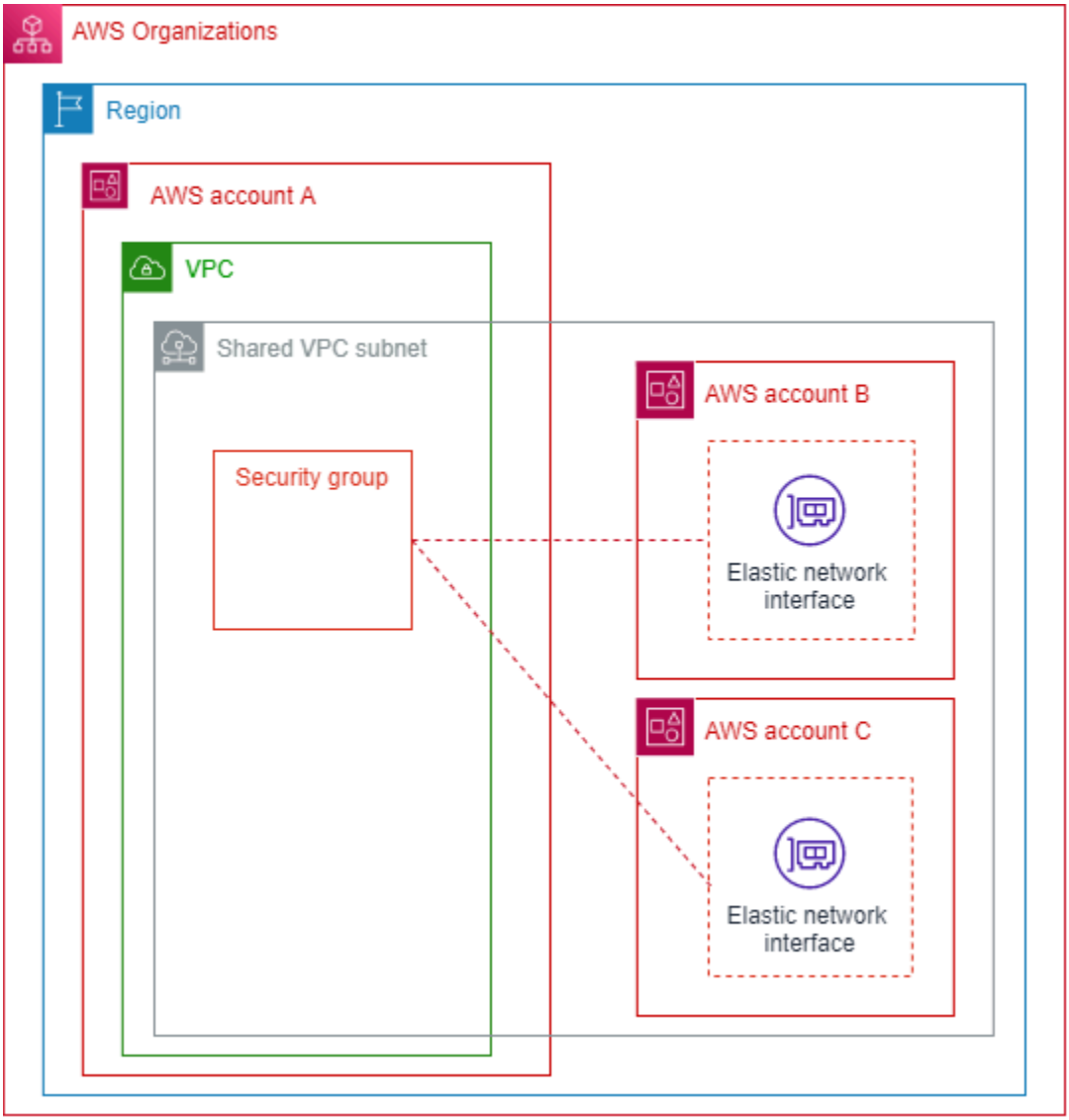
1. 取消 VPC 與 disassociate-security-group-vpc 的關聯。
2. 檢查 VPC 與 describe-security-group-vpc-associations 取消關聯的狀態，並等待狀態變為 `disassociated`。

VPC 現在已與安全群組取消關聯。

與 AWS Organizations 共用安全群組

共用安全群組功能可讓您與相同 AWS 區域內的其他 AWS Organizations 帳戶共用安全群組，並讓安全群組可供這些帳戶使用。

下圖示範如何使用共用安全群組功能來簡化 AWS Organizations 中跨帳戶的安全群組管理：



此圖表顯示三個屬於相同組織的帳戶。帳戶 A 與帳戶 B 和 C 共用 VPC 子網路。帳戶 A 使用共用安全群組功能與帳戶 B 和 C 共用安全群組。帳戶 B 和 C 接著會在共用子網路中啟動執行個體時使用該安全群組。這可讓帳戶 A 管理安全群組；安全群組的任何更新都會套用至帳戶 B 和 C 在共用 VPC 子網路中執行的資源。

共用安全群組功能的需求

- 此功能僅適用於 AWS Organizations 中相同組織中的帳戶。資源共用必須在 AWS Organizations 中啟用。
- 共用安全群組的帳戶必須同時擁有 VPC 和安全群組。
- 您無法共用預設安全群組。
- 您無法共用預設 VPC 中的安全群組。

- 參與者帳戶可以在共用 VPC 中建立安全群組，但無法共用這些安全群組。
- IAM 主體需要一組最低許可，才能與之共用安全群組 AWS RAM。使用 `AmazonEC2FullAccess` 和 `AWSResourceAccessManagerFullAccess` 受管 IAM 政策，確保您的 IAM 主體擁有共用和使用共用安全群組所需的許可。如果您使用自訂 IAM 政策，則需要 `c2:PutResourcePolicy` 和 `ec2:DeleteResourcePolicy` 動作。這些是僅限許可的 IAM 動作。如果 IAM 主體未授予這些許可，則嘗試使用 共用安全群組時發生錯誤 AWS RAM。

支援此功能的服務

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Elastic Load Balancing
  - Application Load Balancer
  - Network Load Balancer

此功能如何影響現有的配額

安全群組配額適用。不過，對於「每個網路介面的安全群組」配額，如果參與者在彈性網路介面 (ENI) 上使用擁有和共用的群組，則適用擁有者和參與者配額的最小值。

示範配額如何受到此功能影響的範例：

- 擁有者帳戶配額：每個介面 4 個安全群組
- 參與者帳戶配額：每個介面 5 個安全群組。

- 擁有者與參與者共用群組 SG-O1、SG-O2、SG-O3、SG-O4、SG-O5。參與者已在 VPC 中擁有自己的群組：SG-P1、SG-P2、SG-P3、SG-P4、SG-P5。
- 如果參與者建立 ENI 並僅使用其擁有的群組，他們可以關聯所有 5 個安全群組 (SG-P1、SG-P2、SG-P3、SG-P4、SG-P5)，因為這是他們的配額。
- 如果參與者建立 ENI 並使用其中的任何共用群組，則他們最多只能關聯 4 個群組。在這種情況下，此類 ENI 的配額是擁有者和參與者配額的最小值。可能的有效組態如下所示：
  - SG-O1、SG-P1、SG-P2、SG-P3
  - SG-O1、SG-O2、SG-O3、SG-O4

共用安全群組

本節說明如何使用 AWS 管理主控台 和 AWS CLI 與 Organization 中的其他帳戶共用安全群組。

AWS Management Console

共用安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左導覽窗格中，選擇安全群組。
3. 選擇安全群組，檢視其詳細資訊。
4. 選擇 Sharing (共用) 標籤 。
5. 選擇共用安全群組。
6. 選擇 Create resource share (建立資源共用)。因此， AWS RAM 主控台會開啟，您將在其中為安全群組建立資源共享。
7. 輸入共用資源的名稱。
8. 在資源 – 選用下，選擇安全群組。
9. 選擇安全群組。安全群組不能是預設安全群組，也不能與預設 VPC 相關聯。
10. 選擇下一步。
11. 檢閱允許主體執行的動作，然後選擇下一步。
12. 在主體 – 選用下，選擇僅允許在組織內共用。
13. 在主體下，選擇下列其中一個主體類型，然後輸入適當的數字：
    - AWS 帳戶：您 Organization 中帳戶的帳戶號碼。
    - Organization： AWS Organizations ID。

- 組織單位 (OU)：組織中的 OU 的 ID。
- IAM 角色：IAM 角色的 ARN。建立角色的帳戶必須與建立此資源共享的帳戶是相同組織的成員。
- IAM 使用者：IAM 使用者的 ARN。建立使用者的帳戶必須與建立此資源共享的帳戶是相同組織的成員。
- 服務主體：您無法與服務主體共用安全群組。

14. 選擇新增。
15. 選擇下一步。
16. 選擇 Create resource share (建立資源共用)。
17. 在共用資源下，等待以查看 `Associated` 的狀態。如果有安全群組關聯失敗，可能是因為上述其中一個限制。檢視安全群組的詳細資訊，以及詳細資訊頁面上的共用標籤，以查看與安全群組無法共用原因相關的任何訊息。
18. 返回 VPC 主控台安全群組清單。
19. 選擇您共用的安全群組。
20. 選擇 Sharing (共用) 標籤 。您的 AWS RAM 資源應該會在那裡顯示。如果不是，資源共享建立可能失敗，您可能需要重新建立。

Command line

共用安全群組

1. 您必須先為要共用的安全群組建立資源共用 AWS RAM。如需如何使用 在 中建立資源共享的步驟 AWS RAM AWS CLI，請參閱AWS RAM 《 使用者指南》中的在 中建立資源共享 AWS RAM
2. 若要檢視建立的資源共用關聯，請使用 get-resource-share-associations。

安全群組現在已共用。您可以在相同 VPC 內的共用子網路中啟動 EC2 執行個體時選取安全群組。

停止共用安全群組

本節說明如何使用 AWS 管理主控台 和 AWS CLI 來停止與 Organization 中的其他帳戶共用安全群組。

AWS Management Console

停止共用安全群組

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左導覽窗格中，選擇安全群組。
3. 選擇安全群組，檢視其詳細資訊。
4. 選擇 Sharing (共用) 標籤 。
5. 選擇安全群組資源共用，然後選擇停止共用。
6. 選擇是，停止共用。

Command line

停止共用安全群組

使用 delete-resource-share 刪除資源共用。

安全群組不再共用。擁有者停止共用安全群組後，適用下列規則：

- 現有參與者彈性網絡介面 (ENI) 會繼續取得對未共用安全群組所做的任何安全群組規則更新。取消共用只會防止參與者與未共用的群組建立新的關聯。
- 參與者無法再將未共用的安全群組與其擁有的任何 ENI 建立關聯。
- 參與者可以描述和刪除仍然與未共用安全群組相關聯的 ENI。
- 如果參與者仍有與未共用安全群組相關聯的 ENI，則擁有者無法刪除未共用的安全群組。擁有者只能在參與者取消安全群組與其所有 EN 的關聯 (移除) 之後，才能刪除安全群組。
- 參與者無法使用與未共用安全群組相關聯的 ENI 啟動新的 EC2 執行個體。

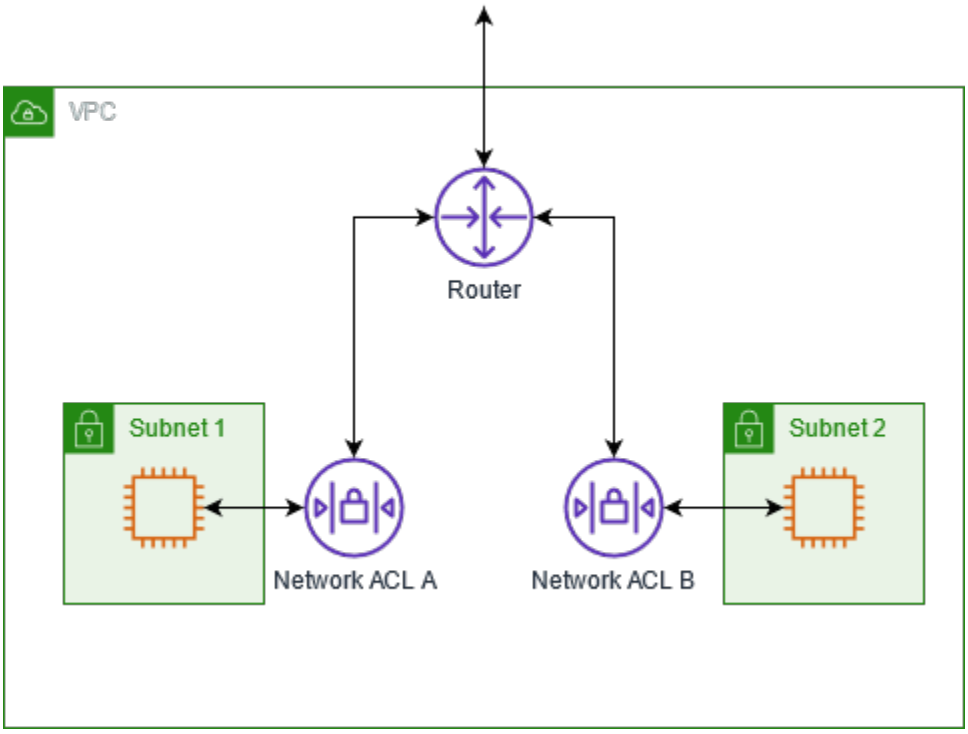
使用網路存取控制清單控制子網路流量

網路存取控制清單 (ACL) 會允許或拒絕子網層級的特定傳入或傳出流量。您可以使用 VPC 的預設網路 ACL，也可以使用類似於安全群組規則的規則為 VPC 建立自訂網路 ACL。自訂網路 ACLs為您的 VPC 新增額外的安全層。

使用網路 ACL 無需額外收費。

下圖顯示具有兩個子網路的 VPC。每個子網路都具有網路 ACL。當流量進入 VPC (例如，從對等 VPC、VPN 連線或網際網路) 時，路由器會將流量傳送至其目的地。網路 ACL A 會判斷哪些目的地為

子網路 1 的流量允許進入子網路 1，以及哪些目的地為子網路 1 以外位置的流量允許離開子網路 1。同樣地，網路 ACL B 會判斷哪些流量允許進入和離開子網路 2。



如需安全群組與網路 ACL 間差異的相關資訊，請參閱比較安全群組和網路 ACL。

目錄

- 網路 ACL 基本概念
- 網路 ACL 規則
- VPC 的預設網路 ACL
- VPC 的自訂網路 ACL
- 路徑 MTU 探索與網路 ACL
- 為您的 VPC 建立網路 ACL
- 管理 VPC 的網路 ACL 關聯
- 刪除 VPC 的網路 ACL
- 範例：控制對子網路中執行個體的存取

網路 ACL 基本概念

下列是開始之前需要了解的網路 ACL 基本事項。

網路 ACL 關聯

- VPC 中的每個子網路都必須與一個網路 ACL 建立關聯。如果您未明確將子網路與網路 ACL 建立關聯，子網路就會自動與預設網路 ACL 建立關聯。
- 您可以建立自訂網路 ACL 並將其與子網路關聯，以允許或拒絕子網路層級的特定傳入或傳出流量。
- 您可以將網路 ACL 與多個子網路建立關聯。不過，子網路一次只能與一個網路 ACL 相關聯。當您為網路 ACL 與子網路建立關聯時，系統就會移除先前的關聯。

網路 ACL 規則

- 網路 ACL 具有傳入規則和傳出規則。每個網路 ACL 擁有的規則數量有配額 (或限制)。每個規則都可以允許或拒絕流量。每個規則都有一個從 1 至 32766 的數字。在決定是允許還是拒絕流量時，我們會依序評估規則，從編號最低的規則開始。如果流量符合規則，則會套用規則，我們不會評估任何其他規則。我們建議您先以增量方式建立規則 (例如 10 或 100 的增量)，以便稍後可在需要時插入新規則。
- 當流量進入和離開子網路時，我們會評估網路 ACL 規則，而不是在子網路內路由時。
- NACL 為無狀態，這表示不會儲存有關先前傳送或接收的流量資訊。例如，如果您建立了允許子網路之特定輸入流量的 NACL 規則，則不會自動允許對該流量的回應。這與安全群組的工作方式相反。安全群組為無狀態，這表示會儲存有關先前傳送或接收的流量資訊。例如，如果安全群組允許 EC2 執行個體的輸入流量，則無論輸出安全群組規則如何，都會自動允許回應。

限制

- 網路 ACL 有配額 (也稱為限制)。如需詳細資訊，請參閱網路 ACL。
- 網路 ACL 無法封鎖傳送至 Route 53 Resolver (也稱為 VPC+2 IP 地址或 AmazonProvidedDNS) 或從其傳送的 DNS 請求。若要透過 Route 53 Resolver 篩選 DNS 請求，請啟用 Route 53 Resolver DNS 防火牆。
- 網路 ACL 無法封鎖傳送至執行個體中繼資料服務 (IMDS) 的流量。若要管理對 IMDS 的存取權限，請參閱《Amazon EC2 使用者指南》中的設定執行個體中繼資料選項。
- 網路 ACL 不會篩選往返下列位置的流量：
  - Amazon 網域名稱服務 (DNS)
  - Amazon 動態主機設定通訊協定 (DHCP)
  - Amazon EC2 執行個體中繼資料
  - Amazon ECS 任務中繼資料端點

- Windows 執行個體的授權啟動
- Amazon Time Sync Service
- 預設 VPC 路由器使用的保留 IP 地址

網路 ACL 規則

您可以在預設網路 ACL 中新增或移除規則，或為您的 VPC 建立額外的網路 ACL。當您在網路 ACL 中新增或移除規則時，系統會自動將變更套用至與網路 ACL 建立關聯的子網路。

下列為部分網路 ACL 規則：

- 規則編號。規則評估順序是從最低的編號規則開始。只要規則符合流量，即會套用規則，不論是否有任何編號更高的規則可能與其抵觸均同。
- 類型。流量類型；例如 SSH。您也可以指定所有流量或自訂範圍。
- Protocol (通訊協定)。您可以指定任何具有標準通訊協定號碼的通訊協定。如需詳細資訊，請參閱 Protocol Numbers。若您指定 ICMP 為通訊協定，您可以指定任何或所有的 ICMP 類型及代碼。
- 連接埠範圍。流量的接聽連接埠或連接埠範圍。例如，80 代表 HTTP 流量。
- 來源。[僅限傳入規則] 流量的來源 (CIDR 範圍)。
- Destination (目的地)。[僅限傳出規則] 流量的目的地 (CIDR 範圍)。
- 允許/拒絕。允許還是拒絕指定的流量。

如需規則範例，請參閱 the section called “範例：控制對子網路中執行個體的存取”。

考量事項

- 每個網路 ACL 的規則數量有配額 (亦稱為限制)。如需詳細資訊，請參閱Amazon VPC 配額。
- 當您新增或刪除 ACL 的規則時，任何與該 ACL 相關聯的子網路都會套用變更。這些變更在很短時間後便會生效。
- 如果您使用命令列工具或 Amazon EC2 API 新增規則，CIDR 範圍會自動修改為其標準形式。例如，如果您指定 CIDR 範圍為 `100.68.0.18/18`，我們會建立具有 `100.68.0.0/18` CIDR 範圍的規則。
- 如果您必須開放範圍很廣的連接埠，但該範圍內有要拒絕的特定連接埠，則您可能想要新增拒絕規則。請務必為拒絕規則設定比允許更廣連接埠流量範圍的規則更小的編號。

- 如果同時從網路 ACL 新增與刪除規則，請多加小心。如果您刪除傳入或傳出規則，然後新增的新項目數量超過允許的數量 (請參閱 Amazon VPC 配額)，則選擇要刪除的項目將會被移除，而新項目則不會新增。這可能會導致未預期的連線問題，並且阻止進出 VPC 的存取行為。

VPC 的預設網路 ACL

虛擬私有雲端 (VPC) 自動隨附預設網路 ACL。系統會將預設網路 ACL 設定為允許所有流量流進和流出其相關聯的子網路。每個網路 ACL 也包括規則編號為星號 (*) 的規則。這些規則可確保在封包未符合任何其他編號規則時拒絕該封包。

您可以透過新增規則或移除預設編號規則來修改預設網路 ACL。您無法刪除規則編號為星號的規則。

預設傳入規則

下表顯示預設網路 ACL 的預設傳入規則。只有在建立具有關聯 IPv6 CIDR 區塊的 VPC，或將 IPv6 CIDR 區塊與 VPC 建立關聯後，才能新增 IPv6 規則。不過，如果您已修改預設網路 ACL 的傳入規則，我們就不會在您將 IPv6 區塊與 VPC 建立關聯時新增允許所有傳入 IPv6 流量的規則。

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允許
101	所有 IPv6 流量	全部	全部	::/0	允許
*	所有流量	全部	全部	0.0.0.0/0	拒絕
*	所有 IPv6 流量	全部	全部	::/0	拒絕

預設傳出規則

下表顯示預設網路 ACL 的預設傳出規則。只有在建立具有關聯 IPv6 CIDR 區塊的 VPC，或將 IPv6 CIDR 區塊與 VPC 建立關聯後，才能新增 IPv6 規則。不過，如果您已修改預設網路 ACL 的傳出規則，我們就不會在您將 IPv6 區塊與 VPC 建立關聯時新增允許所有傳出 IPv6 流量的規則。

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕
100	所有流量	全部	全部	0.0.0.0/0	允許
101	所有 IPv6 流量	全部	全部	::/0	允許
*	所有流量	全部	全部	0.0.0.0/0	拒絕
*	所有 IPv6 流量	全部	全部	::/0	拒絕

VPC 的自訂網路 ACL

您可以建立自訂網路 ACL 並將其與子網路關聯，以允許或拒絕子網路層級的特定傳入或傳出流量。如需詳細資訊，請參閱the section called “建立網路 ACL”。

每個網路 ACL 都包含規則編號為星號 (*) 的預設傳入規則和預設傳出規則。這些規則可確保在封包未符合任何其他規則時拒絕該封包。

可以透過新增或移除規則來修改網路 ACL。您無法刪除規則編號為星號的規則。

對於每個新增的規則，必須設有允許回應流量的傳入或傳出規則。如需如何選取適當的暫時性連接埠範圍的詳細資訊，請參閱暫時性連接埠。

傳入規則範例

下表顯示網路 ACL 的傳入規則。僅當 VPC 具有關聯的 IPv6 CIDR 區塊時，才能新增 IPv6 規則。IPv4 和 IPv6 流量會分別評估。因此，IPv4 流量的任何規則都不適用於 IPv6 流量。您可以在對應的 IPv4 規則旁新增 IPv6 規則，或在最後一個 IPv4 規則後新增 IPv6 規則。

在封包前往子網路時，系統會依據與子網路相關聯的網路 ACL 傳入規則評估該封包 (從編號最小的規則開始)。例如，假設有目的地為 HTTPS 連接埠 (443) 的 IPv4 流量。該封包不符合規則 100 或 105。但該封包符合規則 110，而該規則允許流量進入子網路。如果封包的目的地是連接埠 139 (NetBIOS)，它就不符合任何編號規則，因此 IPv4 流量的 * 規則最終也會拒絕該封包。

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕	說明
100	HTTP	TCP	80	0.0.0.0/0	允許	允許來自任何 IPv4 地址的傳入 HTTP 流量。
105	HTTP	TCP	80	::/0	允許	允許來自任何 IPv6 地址的傳入 HTTP 流量。
110	HTTPS	TCP	443	0.0.0.0/0	允許	允許來自任何 IPv4 地址的傳入 HTTPS 流量。
115	HTTPS	TCP	443	::/0	允許	允許來自任何 IPv6 地址的傳入 HTTPS 流量。
120	SSH	TCP	22	*192.0.2.0 /24*	允許	允許來自您家用網路公有 IPv4 地址範圍的傳入 SSH 流量 (透過網際網路閘道)。
140	自訂 TCP	TCP	*32768-655 35*	0.0.0.0/0	允許	允許來自網際網路的傳入回傳 IPv4 流量 (針對出自子網路的請求)。
145	自訂 TCP	TCP	*32768-655 35*	::/0	允許	允許來自網際網路的傳入回傳 IPv6 流量 (針對出自子網路的請求)。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv4 流量。

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕	說明
*	所有流量	全部	全部	::/0	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。

傳出規則範例

下表顯示自訂網路 ACL 的傳出規則範例。僅當 VPC 具有關聯的 IPv6 CIDR 區塊時，才能新增 IPv6 規則。IPv4 和 IPv6 流量會分別評估。因此，IPv4 流量的任何規則都不適用於 IPv6 流量。您可以在對應的 IPv4 規則旁新增 IPv6 規則，或在最後一個 IPv4 規則後新增 IPv6 規則。

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕	說明
100	HTTP	TCP	80	0.0.0.0/0	允許	允許傳出 IPv4 HTTP 流量從子網路流向網際網路。
105	HTTP	TCP	80	::/0	允許	允許傳出 IPv6 HTTP 流量從子網路流向網際網路。
110	HTTPS	TCP	443	0.0.0.0/0	允許	允許傳出 IPv4 HTTPS 流量從子網路流向網際網路。
115	HTTPS	TCP	443	::/0	允許	允許傳出 IPv6 HTTPS 流量從子網路流向網際網路。
120	自訂 TCP	TCP	*1024-655 5*	*192.0.2.(/24*	允許	允許對來自家用網路的 SSH 流量進行傳出回應。
140	自訂 TCP	TCP	*32768-65 35*	0.0.0.0/0	允許	允許對網際網路上的用戶端進行傳出 IPv4

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕	說明
						回應 (例如，提供網頁服務)。
145	自訂 TCP	TCP	32768-65535	::/0	允許	允許對網際網路上的用戶端進行傳出 IPv6 回應 (例如，提供網頁服務)。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕上述規則尚未處理的所有傳出 IPv4 流量。
*	所有流量	全部	全部	::/0	拒絕	拒絕上述規則尚未處理的所有傳出 IPv6 流量。

暫時性連接埠

上節的範例網路 ACL 是使用 32768-65535 暫時性連接埠範圍。不過，建議您依據所使用的用戶端類型或要通訊的目標，為您的網路 ACL 使用不同範圍。

初始化請求的用戶端會選擇暫時性連接埠範圍。範圍需視用戶端作業系統而定。

- 許多 Linux 核心 (包括 Amazon Linux 核心) 使用的連接埠 32768-61000。
- 來自 Elastic Load Balancing 的請求會使用連線埠 1024-65535。
- Windows 作業系統到 Windows Server 2003 使用連接埠 1025-5000。
- Windows Server 2008 和更新版本使用連接埠 49152-65535。
- NAT 閘道使用連接埠 1024-65535。
- AWS Lambda 函數使用連接埠 1024-65535。

例如，如果送達 VPC 之 Web 伺服器的請求是來自網際網路的 Windows 10 用戶端，您的網路 ACL 就必須具有傳出規則以讓流量通往連接埠 49152-65535。

如果啟動請求的用戶端是您 VPC 中的執行個體，您的網路 ACL 就必須具有傳入規則以讓流量通往特定執行個體作業系統的暫時性連接埠。

實際操作時，為了涵蓋各種可能初始化流量至 VPC 中公開執行個體的不同用戶端類型，您可以開啟暫時性連接埠 1024-65535。不過，您也可以新增規則至 ACL 以拒絕該範圍內任何惡意連接埠上的流量。請務必比開啟廣泛暫時性連接埠的允許規則更早在資料表中放入拒絕規則。

自訂網路 ACLs和其他 AWS 服務

如果您建立自訂網路 ACL，請注意它如何影響您使用其他 AWS 服務建立的資源。

透過 Elastic Load Balancing，如果您已在後端執行個體子網路的網路 ACL 中，針對來源為 `0.0.0.0/0` 或子網路 CIDR 的所有流量新增拒絕規則，您的負載平衡器就無法對執行個體執行運作狀態檢查。

如需有關負載平衡器與後端執行個體之建議網路 ACL 規則的詳細資訊，請參閱下列主題：

- Application Load Balancer 的網路 ACL
- Network Load Balancer 的網路 ACL
- Classic Load Balancer 的網路 ACL

對連線能力問題進行疑難排解

Reachability Analyzer 是一種靜態組態分析工具。使用 Reachability Analyzer 來分析 VPC 中兩項資源之間的網路連線能力並進行偵錯。Reachability Analyzer 會在可連線虛擬路徑時，在這些路徑之間產生逐個躍點的詳細資訊，並在無法連線時識別導致阻礙的元件。例如，它可以識別遺失或設定錯誤的網路 ACL 規則。

如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

路徑 MTU 探索與網路 ACL

路徑 MTU 探索可用於確認兩個裝置間的路徑 MTU。路徑 MTU 是原始主機和接收主機之間的路徑上支援的最大封包尺寸。

對於 IPv4，當主機沿著路徑傳送大於接收主機或裝置的 MTU 封包時，接收主機或裝置會捨棄封包。接著會傳回下列 ICMP 訊息： `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (類型 3，代碼 4)。

這會指示傳輸主機將承載分割成多個較小的封包，然後重新傳輸它們。

IPv6 通訊協定不支援網路中的分段。當主機沿著路徑傳送大於接收主機或裝置的 MTU 的封包時，接收主機或裝置會捨棄封包。接著會傳回下列 ICMP 訊息： `ICMPv6 Packet Too Big (PTB)` (類型 2)。

這會指示傳輸主機將承載分割成多個較小的封包，然後重新傳輸它們。

如果子網路中主機之間的最大傳輸單位 (MTU) 不同，或您的執行個體透過網際網路進行對等通訊，則您必須新增下列網路 ACL 規則，同時適用於傳入和傳出。這可確保路徑 MTU 探索能夠正確運作，並防止封包遺失。為類型選取 Custom ICMP Rule (自訂 ICMP 規則)，而且若 Destination Unreachable (無法連接目的地)，則為連接埠範圍 (類型 3，代碼 4) 選取需要分段並設定 DF 旗標。如果您使用追蹤路由，也必須新增以下規則：為連接埠範圍 (類型 11、代碼 0) 選取 Custom ICMP Rule (自訂 ICMP 規則) 類型，以及 Time Exceeded (超過時間)、TTL expired transit (TTL 過期傳輸)。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 EC2 執行個體的網路最高傳輸裝置 (MTU)。

為您的 VPC 建立網路 ACL

下列任務說明如何建立網路 ACL、將規則新增至網路 ACL，然後將網路 ACL 與子網路建立關聯。

任務

- 步驟 1：建立網路 ACL
- 步驟 2：新增規則
- 步驟 3：將子網路與網路 ACL 建立關聯
- (選用) 透過 Firewall Manager 管理網路 ACL

步驟 1：建立網路 ACL

您可以為 VPC 建立自訂網路 ACL。自訂網路 ACL 的初始規則會封鎖所有傳入與傳出流量。您的新自訂網路 ACL 預設不會與子網路建立關聯，但必須與子網路明確建立關聯。

透過主控台建立網路 ACL

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選擇建立網路 ACL。
4. (選用) 在名稱欄位中，輸入網路 VPC 的名稱。
5. 在 VPC 欄位中選取 VPC。
6. (選用) 在標籤欄位中選擇新增標籤，然後輸入標籤索引鍵與標籤值。

7. 選擇建立網路 ACL。

透過命令列建立網路 ACL

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

步驟 2：新增規則

您可以新增允許或拒絕傳入或傳出流量的規則。

我們會從最小的編號開始，按照順序來處理規則。建議您在規則編號之間保留間隔 (例如 100、200、300)，而不是使用連續編號 (101、102、103)。這麼做可讓您更輕鬆地新增規則，而不需要重新編號現有的規則。

如果您使用的是 Amazon EC2 API 或命令列工具，則無法修改規則。您只能新增和刪除規則。如果您使用的是 Amazon VPC 主控台，則可以修改現有規則的項目。主控台會移除現有的規則，並為您新增規則。如果您需要變更 ACL 中的規則順序，您必須使用新的規則編號來新增規則，然後刪除原始規則。

透過主控台將規則新增至網路 ACL

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選擇網路 ACL。
4. 若要新增傳入規則，請執行下列動作：
   a. 選擇 Inbound Rules (傳入規則) 索引標籤。
   b. 依次選擇編輯傳入規則、新增規則。
   c. 輸入尚未使用的規則編號、類型、通訊協定、連接埠範圍、來源，以及是否允許或拒絕流量。對於某些類型，我們會為您填寫通訊協定與連接埠。如果系統提示您輸入連接埠範圍，請輸入連接埠編號或連接埠範圍 (例如 49152-65535)。

      若要使用未列出的通訊協定，請選擇自訂通訊協定類型，然後選取通訊協定。如需詳細資訊，請參閱 IANA 通訊協定編號。
   d. 選擇儲存變更。
5. 若要新增傳出規則，請執行下列動作：

a. 選擇 Outbound rules (傳出規則) 索引標籤。

b. 依次選擇編輯傳出規則、新增規則。

c. 輸入尚未使用的規則編號、類型、通訊協定、連接埠範圍、來源，以及是否允許或拒絕流量。對於某些類型，我們會為您填寫通訊協定與連接埠。如果系統提示您輸入連接埠範圍，請輸入連接埠編號或連接埠範圍 (例如 49152-65535)。

若要使用未列出的通訊協定，請選擇自訂通訊協定類型，然後選取通訊協定。如需詳細資訊，請參閱 IANA 通訊協定編號。

d. 選擇儲存變更。

透過命令列將規則新增至網路 ACL

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

透過命令列取代網路 ACL 中的規則

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

透過命令列刪除網路 ACL 中的規則

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

步驟 3：將子網路與網路 ACL 建立關聯

若要將網路 ACL 的規則套用至特定子網路，您必須將子網路與網路 ACL 建立關聯。您可以將網路 ACL 與多個子網路建立關聯。不過，一個子網路只能與一個網路 ACL 相關聯。根據預設，如果有任何未與特定 ACL 相關聯的子網路，系統會將其與預設網路 ACL 建立關聯。

將子網路與網路 ACL 建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)，然後選取網路 ACL。

3. 在詳細資訊窗格中，在 Subnet Associations (子網路關聯) 標籤上，選擇 Edit (編輯)。選取子網路的 Associate (關聯) 核取方塊以與網路 ACL 建立關聯，然後選擇 Save (儲存)。

(選用) 透過 Firewall Manager 管理網路 ACL

AWS Firewall Manager 簡化跨多個帳戶和子網路的網路 ACL 管理和維護任務。您可以使用 Firewall Manager 來監控組織中的帳戶和子網路，並自動套用您定義的網路 ACL 組態。當您想要保護整個組織，或者您經常新增要從中央系統管理員帳戶自動保護的新子網路時，Firewall Manager 特別有用。

使用 Firewall Manager 網路 ACL 政策，您可以使用單一管理員帳戶來設定、監控和管理您想要在組織中使用的網路 ACL 中定義的最小規則集。您可以指定組織中哪些帳戶和子網路在 Firewall Manager 政策的範圍內。Firewall Manager 會報告範圍內子網路的網路 ACL 合規狀態，而且您可以設定 Firewall Manager 來自動修復不合規的網路 ACL。

如需詳細資訊，請參閱《AWS Firewall Manager 開發人員指南》中的下列資源：

- AWS Firewall Manager 先決條件
- 設定 AWS Firewall Manager 網路 ACL 政策
- 搭配 Firewall Manager 使用網路 ACL 政策

管理 VPC 的網路 ACL 關聯

每個子網路皆與一個網路 ACL 相關聯。您首次建立子網路時，它就會與 VPC 的預設網路 ACL 建立關聯。您可以建立自訂網路 ACL，並將其與一或多個子網路建立關聯，取代先前的網路 ACL 關聯。

任務

- 描述網路 ACL 關聯
- 變更與網路 ACL 相關聯的子網路
- 變更與子網路相關聯的網路 ACL。

描述網路 ACL 關聯

您可以描述與子網路相關聯的網路 ACL，也可以描述哪些子網路與網路 ACL 相關聯。

透過主控台描述與子網路相關聯的網路 ACL

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選擇子網路。
4. 選擇網路 ACL 索引標籤。

使用 描述與子網路相關聯的網路 ACL AWS CLI

使用下列 describe-network-acls 命令列出與指定子網路相關聯的網路 ACL。

```
aws ec2 describe-network-acls --filters Name=association.subnet-
id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkAclId
```

以下為範例輸出。

```
[
    "acl-03701d1f82d8c3fd6"
]
```

透過主控台描述與網路 ACL 相關聯的子網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選擇網路 ACL。
4. 選取子網路關聯索引標籤。

使用 描述與網路 ACL 相關聯的子網路 AWS CLI

使用下列 describe-network-acls 命令列出與指定網路 ACL 相關聯的子網路。

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query
 NetworkAcls[*].Associations[].SubnetId
```

以下為範例輸出。

```
[
    "subnet-0d2d1b81e0bc9c6d4",
    "subnet-0e990c67809773b19",
    "subnet-0eb17d85f5dfd33b1",
    "subnet-0e01d500780bb7468"
```

```
]
```

變更與網路 ACL 相關聯的子網路

您可以取消自訂網路 ACL 與子網路的關聯。您取消子網路與自訂網路 ACL 的關聯後，我們會自動將其與 VPC 的預設網路 ACL 建立關聯。這些變更在很短時間後便會生效。

將子網路與網路 ACL 建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選擇網路 ACL。
4. 依次選擇動作、編輯子網路關聯。
5. 從選取的子網路中移除子網路。
6. 選擇儲存變更。

變更與子網路相關聯的網路 ACL。

您可以變更與子網路相關聯的網路 ACL。例如，當您建立子網路時，它一開始就會與 VPC 的預設網路 ACL 建立關聯。如果建立自訂網路 ACL，可以將網路 ACL 與一個或多個子網路建立關聯來套用網路 ACL 規則。

變更子網路的網路 ACL 之後，變更在很短時間後便會生效。

變更與子網路相關聯的網路 ACL

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Subnets (子網)。
3. 選擇子網路。
4. 依次選擇動作、編輯網路 ACL 關聯。
5. 在網路 ACL ID 欄位中，選取要與子網路建立關聯的網路 ACL，並檢閱所選網路 ACL 的傳入與傳出規則。
6. 選擇儲存。

透過命令列取代網路 ACL 關聯

- replace-network-acl-association (AWS CLI)

- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

刪除 VPC 的網路 ACL

網路 ACL 結束使用後即可予以刪除。不能刪除與子網路相關聯的網路 ACL。您無法刪除預設網路 ACL。

透過主控台從網路 ACL 移除子網路關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。關聯對象資料欄會指出與每個網路 ACL 相關聯的子網路數量。如果沒有相關聯的子網路，則此資料欄為 -。
3. 選擇網路 ACL。
4. 依次選擇動作、編輯子網路關聯。
5. 移除子網路關聯。
6. 選擇儲存變更。

透過命令列描述您的網路 ACL (包括關聯)

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

透過命令列取代網路 ACL 關聯

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

透過主控台刪除網路 ACL

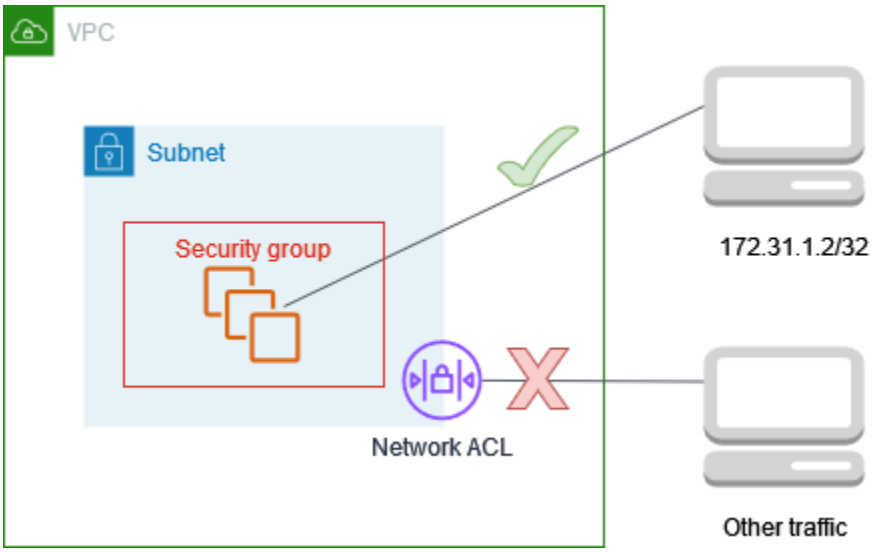
1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選擇網路 ACL。
4. 依次選擇動作、刪除網路 ACL。
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

透過命令列刪除網路 ACL

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

範例：控制對子網路中執行個體的存取

在此範例中，子網路中的執行個體可以彼此通訊，而且可以從信任的遠端電腦存取，以執行管理任務。遠端電腦可能是區域網路中的電腦 (如圖中所示)，也可能是位於不同子網路或 VPC 中的執行個體。子網路的網路 ACL 規則和執行個體的安全群組規則允許來自遠端電腦 IP 位址的存取。其他所有來自網際網路或其他網路的流量都會遭拒。



使用網路 ACL，可讓您彈性變更執行個體的安全群組或安全群組規則，並將網路 ACL 作為備份防禦層。

例如，如果您不小心更新安全群組以允許來自任何地方的傳入 SSH 存取，網路 ACL 仍會限制存取遠端電腦的 IP 地址範圍。網路 ACL 拒絕來自任何其他 IP 地址的傳入 SSH 流量。

網路 ACL 規則

以下是與子網路關聯的網路 ACL 的傳入規則範例。這些規則會套用至子網路中的所有執行個體。

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕	說明
100	SSH	TCP	22	*172.31.1.2/32*	允許	允許來自遠端電腦的傳入流量。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕所有其他傳入流量。

以下是與子網路關聯的網路 ACL 的傳出規則範例。網路 ACL 無狀態。因此，您必須包含允許回應傳入流量的規則。

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕	說明
100	自訂 TCP	TCP	1024-65535	*172.31.1.2/32*	允許	允許對遠端電腦的傳出回應。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕所有其他傳出流量。

安全群組規則

以下是與執行個體關聯的安全群組的傳入規則範例。這些規則適用於與安全群組相關聯的所有執行個體。如果使用者具有與執行個體相關聯的金鑰對的私有金鑰，則可以使用 SSH 從遠端電腦連線至執行個體。

通訊協定類型	通訊協定	連接埠範圍	來源	評論
所有流量	全部	全部	*sg-1234567890abcdef0*	允許與此安全群組相關聯之執行個體間的通訊。

通訊協定類型	通訊協定	連接埠範圍	來源	評論
SSH	TCP	22	*172.31.1.2/32*	允許來自遠端電腦的傳入 SSH 存取。

以下是與執行個體關聯的安全群組的傳出規則範例。安全群組具狀態。因此，您不需要允許回應傳入流量的規則。

通訊協定類型	通訊協定	連接埠範圍	目的地	評論
所有流量	全部	全部	*sg-1234567890abcdef0*	允許與此安全群組相關聯之執行個體間的通訊。

網路 ACL 與安全群組之間的差異

下表總結了網路 ACL 與安全群組之間的基本差異。

特性	網路 ACL	安全群組
操作層級	子網路層級	執行個體層級
Scope (範圍)	適用於關聯子網路中的所有執行個體	適用於與安全群組相關聯的所有執行個體
規則類型	支援允許與拒絕規則	僅支援允許規則
規則評估	以遞增順序評估規則，直至找到流量的相符項為止	在決定是否允許流量前，先評估所有規則
傳回流量	必須明確允許 (無狀態)	自動允許 (具狀態)

Amazon Virtual Private Cloud 的恢復能力

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些可用區域使用低延遲、高輸送量和高度備援聯網進行連接。透過可用區域，您可以設計與操作的應用程式和資料庫，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、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

AWS 區域 是主要建置區塊，每個區塊代表不同的地理位置，其中包含多個實體分隔和隔離的可用區域。這些可用區域是透過低延遲、高輸送量和高備援網路連線結構來連接，因此可在它們之間進行無縫通訊和資料傳輸。

可用區域的架構是關鍵差異因素，因為它們的設計比傳統的單一或多個資料中心設定更強大且容錯能力更高。透過將資源分散到區域內的多個可用區域，應用程式和資料庫可以設計成在區域之間自動容錯移轉，而不會中斷服務。此備援和高可用性層級是關鍵任務工作負載的關鍵需求，可讓組織建置彈性的雲端原生解決方案。

此外， AWS 基礎設施的擴展和全球觸角讓客戶能夠更接近最終使用者部署其應用程式，從而減少延遲並改善整體使用者體驗。全球多個區域的可用性也允許有效的資料主權和合規，因為客戶可以在其特定法規和業務需求所需的地理範圍內存放和處理資料。

透過使用 AWS 全球基礎設施，組織可以將其雲端環境建構為高可用性、容錯性和可擴展性，並靈活地適應不斷變化的需求和不斷變化的業務需求。此穩固的基礎是成功實作現代雲端型應用程式和服務的關鍵推動因素。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

您可以設定 VPC 以符合工作負載的彈性需求。如需詳細資訊，請參閱下列內容：

- 了解彈性模式和權衡 (AWS 架構部落格)
- 規劃您的網路拓撲 (AWS Well-Architected Framework)
- Amazon Virtual Private Cloud Connectivity Options (AWS 白皮書)

Amazon Virtual Private Cloud 的合規驗證

我們的新 AWS 註冊體驗並非針對受管制的工作負載而設計。如果您正在使用我們新的 AWS 註冊體驗，但想要將 AWS 用於受管制的工作負載，您可以註冊 AWS （進階） 或為您的 AWS 環境啟用進階功能。

若要了解 是否 AWS 服務 在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

封鎖對 VPC 和子網路的公開存取

VPC 封鎖公開存取 (BPA) 是一種集中式安全功能，可授權防止公開網際網路存取整個 AWS 帳戶的 VPC 資源。它可確保符合安全要求，同時為特定例外狀況和稽核功能提供靈活性。

VPC BPA 功能具有下列模式：

- 雙向：此區域中往返網際網路閘道和僅輸出網際網路閘道 (排除 VPC 和子網路除外) 的所有流量都會遭到封鎖。
- 僅輸入：此區域中 VPC 的所有網際網路流量 (排除 VPC 或子網路除外) 都會遭到封鎖。僅允許進出 NAT 閘道和僅輸出網際網路閘道的流量，因為這些閘道僅允許建立傳出連線。

您也可以針對您不想封鎖的流量，為此功能建立「排除」。排除項目是可套用至單一 VPC 或子網路的模式，其會將其從帳戶的 VPC BPA 模式排除，並允許雙向或僅限輸出存取。

排除項目可以有下列其中一種模式：

- 雙向：允許進出排除 VPC 和子網路的所有網際網路流量。
- 僅輸出：允許來自排除 VPC 和子網路的傳出網際網路流量。已封鎖對排除 VPC 和子網路的傳入網際網路流量。這僅適用於 VPC BPA 設定為雙向時。

目錄

- VPC BPA 基礎知識
- 評估 VPC BPA 的影響並監控 VPC BPA
- 進階範例

VPC BPA 基礎知識

本節涵蓋 VPC BPA 的重要詳細資訊，包括哪些服務支援它，以及如何使用它。

目錄

- 區域可用性
- AWS 服務影響和支援
- VPC BPA 的限制
- 使用 IAM 政策控制對 VPC BPA 的存取
- 為您的帳戶啟用 VPC BPA 雙向模式
- 將 VPC BPA 模式變更為僅輸入
- 建立和刪除排除項目
- 在組織層級啟用 VPC BPA

區域可用性

VPC BPA 適用於所有商業 AWS 區域，包括 GovCloud 和中國區域。

在本指南中，您還可以找到有關將網路存取分析器和 Reachability Analyzer 與 VPC BPA 搭配使用的資訊。請注意，並非所有商業區域都提供網路存取分析器和 Reachability Analyzer。如需有關網路存取分析器和 Reachability Analyzer 區域可用性的資訊，請參閱《網路存取分析器指南》中的限制和《Reachability Analyzer 指南》中的考量。

AWS 服務影響和支援

下列資源和服務支援 VPC BPA，而這些服務和資源的流量會受到 VPC BPA 的影響：

- 網際網路閘道：會封鎖所有傳入和傳出流量。
- 僅輸出網際網路閘道：封鎖所有傳出流量。僅輸出網際網路閘道不允許傳入流量。
- Gateway Load Balancer (GWLB)：除非排除包含 GWLB 端點的子網路，否則會封鎖所有傳入和傳出流量。
- NAT 閘道：會封鎖所有傳入和傳出流量。NAT 閘道需要網際網路閘道才能進行網際網路連線。
- 面向網際網路的 Network Load Balancer：會封鎖所有傳入和傳出流量。面向網際網路的 Network Load Balancer 需要網際網路閘道才能進行網際網路連線。
- 面向網際網路的 Application Load Balancer：會封鎖所有傳入和傳出流量。面向網際網路的 Application Load Balancer 需要網際網路閘道才能進行網際網路連線。
- Amazon CloudFront VPC 來源：所有傳入與傳出流量都會遭到封鎖。
- Direct Connect：使用公有虛擬介面 (公有 IPv4 位址或全域單播 IPv6 位址) 的所有傳入與傳出流量都會遭到封鎖。此流量會使用網際網路閘道 (或僅限輸出網際網路閘道) 進行連線。

- AWS Global Accelerator：無論目標是否可從網際網路存取，都會封鎖傳入 VPCs 的流量。
- AWS Network Firewall：除非排除包含防火牆端點的子網路，否則會封鎖所有傳入和傳出流量。
- AWS Wavelength 電信業者閘道：所有傳入和傳出流量都會遭到封鎖。

VPC BPA 不會封鎖或影響與私有連線相關的流量，例如下列服務和資源的流量：

- AWS Client VPN
- AWS CloudWAN
- AWS Outposts 本機閘道
- AWS Site-to-Site VPN
- Transit Gateway
- AWS Verified Access

Important

- 如果您使用 VPC 傳入路由，透過在子網路中 EC2 執行個體上執行的設備 （例如第三方安全或監控工具） 路由傳入和傳出流量，您必須從 VPC 封鎖公開存取中排除工作負載子網路。工作負載子網路是子網路，其中包含其流量透過設備路由的執行個體。包含設備的子網路不需要排除。
- 即使 VPC BPA 未透過 VPC 中的網際網路閘道開啟，也允許從 VPC 中的資源私下傳送至 VPC 中執行之其他服務的流量，例如 Route 53 Resolver。這些服務可能會代表您向 VPC 外部的資源提出請求，例如解析 DNS 查詢，如果未透過其他安全控制緩解，則可能會公開 VPC 內資源活動的相關資訊。
- 如果您有面向網際網路的負載平衡器，而且只為其其中一個子網路建立 VPC BPA 排除，則負載平衡器仍然可以在排除的子網路中接收公有流量，並將其私下路由到未排除的子網路中的目標。為了確保 VPC BPA 完全封鎖對目標的公開存取，請確保不會排除任何負載平衡器子網路。

VPC BPA 的限制

不允許 NAT 閘道和僅輸出網際網路閘道的 Local Zones (LZ) 不支援 VPC BPA 僅輸入模式。

使用 IAM 政策控制對 VPC BPA 的存取

如需允許/拒絕存取 VPC BPA 功能的 IAM 政策範例，請參閱 封鎖對 VPC 和子網路的公開存取。

為您的帳戶啟用 VPC BPA 雙向模式

VPC BPA 雙向模式會封鎖此區域中往返網際網路閘道和僅輸出網際網路閘道的所有流量 (排除 VPC 和子網路除外)。如需排除的更多相關資訊，請參閱建立和刪除排除項目。

> **Important**
> 強烈建議您在生產帳戶中啟用 VPC BPA 之前，先徹底檢閱需要網際網路存取的工作負載。

> **Note**
> - 若要在帳戶中的 VPC 和子網路上啟用 VPC BPA，您必須擁有 VPC 和子網路。
> - 如果您目前與其他帳戶共用 VPC 子網路，子網路擁有者強制執行的 VPC BPA 模式也適用於參與者流量，但參與者無法控制影響共用子網路的 VPC BPA 設定。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇編輯公開存取設定。
4. 選擇開啟「封鎖公開存取」和雙向，然後選擇儲存變更。
5. 等待狀態變更為開啟。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

VPC BPA 雙向模式現已開啟。

AWS CLI

1. 開啟 VPC BPA：

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

2. 檢視 VPC BPA 的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

將 VPC BPA 模式變更為僅輸入

VPC BPA 僅輸入模式會封鎖此區域中 VPC 的所有網際網路流量 (排除 VPC 或子網路除外)。僅允許進出 NAT 閘道和僅輸出網際網路閘道的流量，因為這些閘道僅允許建立傳出連線。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇編輯公開存取設定。
4. 將方向變更為僅限輸入。
5. 儲存變更並等待狀態更新。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

AWS CLI

1. 修改 VPC BPA 區塊方向：

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

2. 檢視 VPC BPA 的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

建立和刪除排除項目

VPC BPA 排除是一種模式，可套用至單一 VPC 或子網路，以將其從帳戶的 VPC BPA 模式排除，並允許雙向或僅輸出存取。即使帳戶未啟用 VPC BPA，您也可以為 VPC 和子網路建立 VPC BPA 排除

項目，以確保在開啟 VPC BPA 時，排除項目不會發生流量中斷。VPC 的排除會自動套用至 VPC 中的所有子網路。

您最多可以建立 50 個排除。如需有關請求提高限制的資訊，請參閱 Amazon VPC 配額 中每個帳戶的 VPC BPA 排除。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在封鎖公開存取索引標籤的排除項目下，執行下列其中一項動作：
   - 若要刪除排除項目，請選取排除項目，然後選擇動作 > 刪除排除項目。
   - 若要建立排除項目，請選擇建立排除項目並繼續後續步驟。
4. 選擇區塊方向：
   - 雙向：允許所有往返排除 VPC 和子網路的網際網路流量。
   - 僅輸出：允許來自排除 VPC 和子網路的傳出網際網路流量。封鎖對排除 VPC 和子網路的傳入網際網路流量。當 VPC BPA 設定為雙向時，此設定適用。
5. 選擇 VPC 或子網路。
6. 選擇建立排除。
7. 等待排除狀態變更為作用中。您可能需要重新整理排除資料表才能查看變更。

已建立排除。

AWS CLI

1. 修改排除允許方向：

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. 可能需要一些時間才能更新排除狀態。檢視排除的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

在組織層級啟用 VPC BPA

如果您使用 AWS Organizations 來管理組織中的帳戶，則可以使用 AWS Organizations 宣告政策在組織中的帳戶強制執行 VPC BPA。如需 VPC BPA 宣告政策的詳細資訊，請參閱《AWS Organizations 使用者指南》中的支援宣告政策。

> **Note**
>
> - 您可以使用 VPC BPA 宣告政策來設定是否允許排除，但無法使用政策建立排除。若要建立排除，您仍然必須在擁有 VPC 的帳戶中建立排除。如需有關建立 VPC BPA 排除的詳細資訊，請參閱建立和刪除排除項目。
> - 如果已啟用 VPC BPA 宣告政策，則在封鎖公開存取設定中，您會看到依宣告政策管理，而且您將無法在帳戶層級修改 VPC BPA 設定。

評估 VPC BPA 的影響並監控 VPC BPA

本節包含有關您可以在開啟 VPC BPA 之前評估其影響的資訊，以及如何在開啟流量之後監控流量是否遭到封鎖的資訊。

目錄

- 使用網路存取分析器評估 VPC BPA 的影響
- 使用流量日誌監控 VPC BPA 影響
- 使用 CloudTrail 追蹤排除刪除
- 使用 Reachability Analyzer 確認連線已封鎖

使用網路存取分析器評估 VPC BPA 的影響

在本節中，您將使用網路存取分析器檢視帳戶中使用網際網路閘道的資源，然後再啟用 VPC BPA 和封鎖存取。使用此分析來了解在帳戶中開啟 VPC BPA 並封鎖流量的影響。

> **Note**
>
> - 網路存取分析器不支援 IPv6；因此您將無法使用它來檢視 VPC BPA 對僅限輸出網際網路閘道傳出 IPv6 流量的潛在影響。

- 您需要為使用網路存取分析器執行的分析付費。如需詳細資訊，請參閱《網路存取分析器指南》中的定價。
- 如需有關網路存取分析器區域可用性的資訊，請參閱《網路存取分析器指南》中的限制。

AWS 管理主控台

1. 在 開啟 AWS Network Insights 主控台https://console.aws.amazon.com/networkinsights/。
2. 選擇網路存取分析器。
3. 選擇建立網路存取範圍。
4. 選擇評估 VPC 封鎖公開存取的影響，然後選擇下一步。
5. 範本已設定為分析您帳戶中網際網路閘道的往返流量。您可以在來源和目的地下檢視。
6. 選擇下一步。
7. 選擇建立網路存取範圍。
8. 選擇您剛建立的範圍，然後選擇分析。
9. 等候分析完成。
10. 檢視分析的調查結果。調查結果下的每一列都顯示了封包在網路中往返於您帳戶中的網際網路閘道的網路路徑。在此情況下，如果您開啟 VPC BPA，且這些調查結果中出現的任何 VPC 和/或子網路都未設定為 VPC BPA 排除項目，則流向這些 VPC 和子網路的流量將受到限制。
11. 分析每個調查結果，了解 VPC BPA 對您 VPC 資源的影響。

影響分析已完成。

AWS CLI

1. 建立網路存取範圍：

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. 開始範圍分析：

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. 取得分析的結果：

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

結果會顯示您帳戶中所有 VPC 中往返網際網路閘道的流量。結果會組織為「調查結果」。"FindingId": "AnalysisFinding-1" 表示這是分析中的第一個調查結果。請注意，有多個調查結果，每個調查結果都表示流量流程會因為開啟 VPC BPA 而受到影響。第一個調查結果會顯示從網際網路閘道 ("SequenceNumber": 1) 開始的流量，傳遞至 NACL ("SequenceNumber": 2) 給安全群組 ("SequenceNumber"： 3)，並在執行個體 ("SequenceNumber": 4) 結束。

4. 分析調查結果，了解 VPC BPA 對 VPC 資源的影響。

影響分析已完成。

使用流量日誌監控 VPC BPA 影響

VPC 流程日誌是一項可讓您擷取傳入及傳出您 VPC 中彈性網路介面之 IP 流量相關資訊的功能。您可以使用此功能來監控 VPC BPA 封鎖到達執行個體網路介面的流量。

使用 使用流量日誌工作 中的步驟為您的 VPC 建立流程日誌。

當您建立流程日誌時，請務必使用包含欄位 `reject-reason` 的自訂格式。

當您檢視流量日誌時，如果流向 ENI 的流量因 VPC BPA 而遭到拒絕，您會在流量日誌項目中看到 BPA 的 `reject-reason`。

除了 VPC 流程日誌的標準限制之外，請注意 VPC BPA 特有的下列限制：

- VPC BPA 的流量日誌不包含跳過的記錄。
- 即使您在流量日誌中包含 `bytes` 欄位，VPC BPA 的流量日誌也不會包含 `bytes`。

使用 CloudTrail 追蹤排除刪除

本節說明如何使用 AWS CloudTrail 來監控和追蹤 VPC BPA 排除的刪除。

AWS 管理主控台

您可以在透過 https://console.aws.amazon.com/cloudtrailv2/ 存取 AWS CloudTrail 主控台，在其中查詢資源類型 > `AWS::EC2::VPCBlockPublicAccessExclusion`，以檢視 CloudTrail 事件歷史記錄中任何已刪除的排除。

AWS CLI

您可以使用 `lookup-events` 命令來檢視與刪除排除項目相關的事件：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

使用 Reachability Analyzer 確認連線已封鎖

VPC Reachability Analyzer 可用來評估是否可以根據您的網路組態達到特定網路路徑，包括 VPC BPA 設定。

如需 Reachability Analyzer 區域可用性的相關資訊，請參閱《Reachability Analyzer 指南》中的考量。

AWS 管理主控台

1. 在 開啟 AWS Network Insights 主控台https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer。
2. 選擇建立和分析路徑。
3. 針對來源類型，選擇網際網路閘道，然後從來源下拉式清單中選擇您要封鎖流量的網際網路閘道。
4. 針對目的地類型，選擇執行個體，然後從目的地下拉式清單中選擇您要封鎖流量的執行個體。
5. 選擇建立和分析路徑。
6. 等候分析完成。這可能需要幾分鐘的時間。
7. 完成後，您應該會看到連線性狀態為無法連線，而且路徑詳細資訊顯示 `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` 是造成此連線能力問題的原因。

AWS CLI

1. 使用您要封鎖來自 (來源) 的流量的網際網路閘道 ID 和您要封鎖流向 (目的地) 執行個體的 ID 建立網路路徑：

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. 在網路路徑上開始分析：

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. 檢索分析的結果：

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. 確認 VPC_BLOCK_PUBLIC_ACCESS_ENABLED 為 ExplanationCode，無法連線。

進階範例

本節包含進階範例，可協助您了解 VPC 封鎖公開存取功能在不同案例中的運作方式。每個案例都會先建立案例，因此依序完成步驟非常重要。

Important

請勿在生產帳戶中瀏覽此範例。強烈建議您在生產帳戶中啟用 VPC BPA 之前，先徹底檢閱需要網際網路存取的工作負載。

Note

若要完全了解 VPC BPA 功能，您需要帳戶中的特定資源。在本節中，我們提供 CloudFormation 範本，您可以用來佈建所需的資源，以完全了解此功能的運作方式。您使用 CloudFormation 範本佈建的資源，以及您使用網路存取分析器和 Reachability Analyzer 執行的分析，會有相關的成本。如果您使用本節中的範本，請確定您在完成此範例時完成清除步驟。

目錄

- 部署 CloudFormation 範本 (選用)

- 使用網路存取分析器檢視 VPC BPA 的影響
- 案例 1 – 連線至未開啟 VPC BPA 的執行個體
- 案例 2 – 開啟 VPC BPA 雙向模式
- 案例 3 – 將 VPC BPA 變更為僅限輸入模式
- 案例 4 – 建立排除
- 案例 5 – 修改排除模式
- 案例 6 – 修改 VPC BPA 模式
- 清除

部署 CloudFormation 範本 (選用)

若要示範此功能的運作方式，您需要 VPC、子網路、執行個體和其他資源。為了讓您更輕鬆地完成此示範，我們提供以下 CloudFormation 範本，您可以用來快速啟動此示範中案例所需的資源。此步驟為選用，您可能只想檢視本節案例中的圖表。

> **Note**
>
> - 與您在本節中建立的 CloudFormation 範本資源相關聯的成本，例如 NAT 閘道和公有 IPv4 地址的成本。為了避免成本過高，請確定您完成清除步驟，以移除為本範例所建立的所有資源。
> - 此 CloudFormation 範本會建立 VPC BPA 所需的基礎資源，但不會啟用 VPC BPA 功能本身。此處部署的資源旨在協助您在選擇單獨啟用 VPC BPA 功能之後，了解與測試該功能。

範本會在您的帳戶中建立下列資源：

- 出口限定網際網路閘道
- 網際網路閘道
- NAT 閘道
- 兩個公有子網路
- 一個私有子網路
- 兩個具有公有及私有 IPv4 地址的 EC2 執行個體
- 一個具有 IPv6 地址和私有 IPv4 地址的 EC2 執行個體
- 一個僅具有私有 IPv4 地址的 EC2 執行個體

- 允許 SSH 和 ICMP 傳入流量以及允許所有傳出流量的安全群組
- VPC 流程日誌
- 子網路 B 中的一個 EC2 執行個體連線端點

複製下面的範本，並將其儲存至 .yaml 檔案。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
  VPCBPAIpv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
```

```
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
  VPCBPAInternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: VPC BPA Internet Gateway

  VPCBPAInternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref VPCBPA
      InternetGatewayId: !Ref VPCBPAInternetGateway

  # Egress-Only Internet Gateway
  VPCBPAEgressOnlyInternetGateway:
    Type: AWS::EC2::EgressOnlyInternetGateway
    Properties:
      VpcId: !Ref VPCBPA

  # Subnets
  VPCBPAPublicSubnetA:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.1.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
          Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetB:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.2.0/24
      MapPublicIpOnLaunch: true
      Tags:
        - Key: Name
```

```
        Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetC:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref VPCBPA
      CidrBlock: 10.0.3.0/24
      MapPublicIpOnLaunch: false
      Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
      AssignIpv6AddressOnCreation: true
      Tags:
        - Key: Name
          Value: VPC BPA Private Subnet C

  # NAT Gateway
  VPCBPANATGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
      SubnetId: !Ref VPCBPAPublicSubnetB
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway

  VPCBPANATGatewayEIP:
    Type: AWS::EC2::EIP
    Properties:
      Domain: vpc
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway EIP

  # Route Tables
  VPCBPAPublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Public Route Table

  VPCBPAPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: VPCBPAInternetGatewayAttachment
```

```
    Properties:
      RouteTableId: !Ref VPCBPAPublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref VPCBPAInternetGateway

  VPCBPAPublicSubnetARouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetA
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPublicSubnetBRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table

  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable
```

```
# EC2 Instances Security Group
VPCBPAInstancesSecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    GroupName: VPC BPA Instances Security Group
    GroupDescription: Allow SSH and ICMP access
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: 0.0.0.0/0
      - IpProtocol: icmp
        FromPort: -1
        ToPort: -1
        CidrIp: 0.0.0.0/0
    VpcId: !Ref VPCBPA
    Tags:
      - Key: Name
        Value: VPC BPA Instances Security Group

# EC2 Instances
VPCBPAInstanceA:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref InstanceAMI
    InstanceType: t2.micro
    KeyName: !Ref VPCBPAKeyPair
    SubnetId: !Ref VPCBPAPublicSubnetA
    SecurityGroupIds:
      - !Ref VPCBPAInstancesSecurityGroup
    Tags:
      - Key: Name
        Value: VPC BPA Instance A

VPCBPAInstanceB:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: !Ref InstanceAMI
    InstanceType: !Ref InstanceType
    KeyName: !Ref VPCBPAKeyPair
    SubnetId: !Ref VPCBPAPublicSubnetB
    SecurityGroupIds:
      - !Ref VPCBPAInstancesSecurityGroup
```

```
      Tags:
        - Key: Name
          Value: VPC BPA Instance B

  VPCBPAInstanceC:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
        - DeviceIndex: '0'
          GroupSet:
            - !Ref VPCBPAInstancesSecurityGroup
          SubnetId: !Ref VPCBPAPrivateSubnetC
          Ipv6AddressCount: 1
      Tags:
        - Key: Name
          Value: VPC BPA Instance D

  # Flow Logs IAM Role
  VPCBPAFlowLogRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service: vpc-flow-logs.amazonaws.com
            Action: 'sts:AssumeRole'
```

```
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs Role

  VPCBPAFlowLogPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: VPC-BPA-FlowLogsPolicy
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action:
              - 'logs:CreateLogGroup'
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
              - 'logs:DescribeLogGroups'
              - 'logs:DescribeLogStreams'
            Resource: '*'
      Roles:
        - !Ref VPCBPAFlowLogRole

  # Flow Logs
  VPCBPAFlowLog:
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
```

```
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id

  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetAName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB

  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C

  VPCBPAInstanceAId:
    Description: The ID of instance A
    Value: !Ref VPCBPAInstanceA

  VPCBPAInstanceBId:
    Description: The ID of instance B
    Value: !Ref VPCBPAInstanceB
```

```
  VPCBPAInstanceCId:
    Description: The ID of instance C
    Value: !Ref VPCBPAInstanceC

  VPCBPAInstanceDId:
    Description: The ID of instance D
    Value: !Ref VPCBPAInstanceD
```

AWS 管理主控台

1. 在 開啟 CloudFormation 主控台https://console.aws.amazon.com/cloudformation/。
2. 選擇建立堆疊並上傳 .yaml 範本檔案。
3. 完成啟動範本的步驟。您需要輸入映像 ID 和執行個體類型 (例如 t2.micro)。您也需要允許 CloudFormation 為您建立 IAM 角色，以建立流量日誌，並取得登入 CloudWatch 的許可。
4. 啟動堆疊後，請檢視事件標籤以檢視進度，並確保完成堆疊後再繼續。

AWS CLI

1. 執行下列命令來建立 CloudFormation 堆疊：

   ```
   aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
    file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
   ```

   輸出：

   ```
   {
       "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
   stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
   }
   ```

2. 檢視進度，並確保完成堆疊後再繼續：

   ```
   aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-
   east-2
   ```

使用網路存取分析器檢視 VPC BPA 的影響

在本節中，您將使用網路存取分析器來檢視帳戶中使用網際網路閘道的資源。使用此分析來了解在帳戶中開啟 VPC BPA 並封鎖流量的影響。

如需有關網路存取分析器區域可用性的資訊，請參閱《網路存取分析器指南》中的限制。

AWS 管理主控台

1. 在 開啟 AWS Network Insights 主控台https://console.aws.amazon.com/networkinsights/。
2. 選擇網路存取分析器。
3. 選擇建立網路存取範圍。
4. 選擇評估 VPC 封鎖公開存取的影響，然後選擇下一步。
5. 範本已設定為分析您帳戶中網際網路閘道的往返流量。您可以在來源和目的地下檢視。
6. 選擇下一步。
7. 選擇建立網路存取範圍。
8. 選擇您剛建立的範圍，然後選擇分析。
9. 等候分析完成。
10. 檢視分析的調查結果。調查結果下的每一列都顯示了封包在網路中往返於您帳戶中的網際網路閘道的網路路徑。在此情況下，如果您開啟 VPC BPA，且這些調查結果中出現的任何 VPC 和/或子網路都未設定為 VPC BPA 排除項目，則流向這些 VPC 和子網路的流量將受到限制。
11. 分析每個調查結果，了解 VPC BPA 對您 VPC 資源的影響。

影響分析已完成。

AWS CLI

1. 建立網路存取範圍：

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

輸出：

```
{
```

```
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      }
    ]
  }
}
```

2. 開始範圍分析：

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

輸出：

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
```

```
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. 取得分析的結果：

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

輸出：

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
```

```
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
```

```
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
```

```
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```


結果會顯示您帳戶中所有 VPC 中往返網際網路閘道的流量。結果會組織為「調查結果」。"FindingId": "AnalysisFinding-1" 表示這是分析中的第一個調查結果。請注意，有多個調查結果，每個調查結果都表示流量流程會因為開啟 VPC BPA 而受到影響。第一個調查結果會顯示從網際網路閘道 ("SequenceNumber": 1) 開始的流量，傳遞至 NACL ("SequenceNumber": 2) 給安全群組 ("SequenceNumber"： 3)，並在執行個體 ("SequenceNumber": 4) 結束。

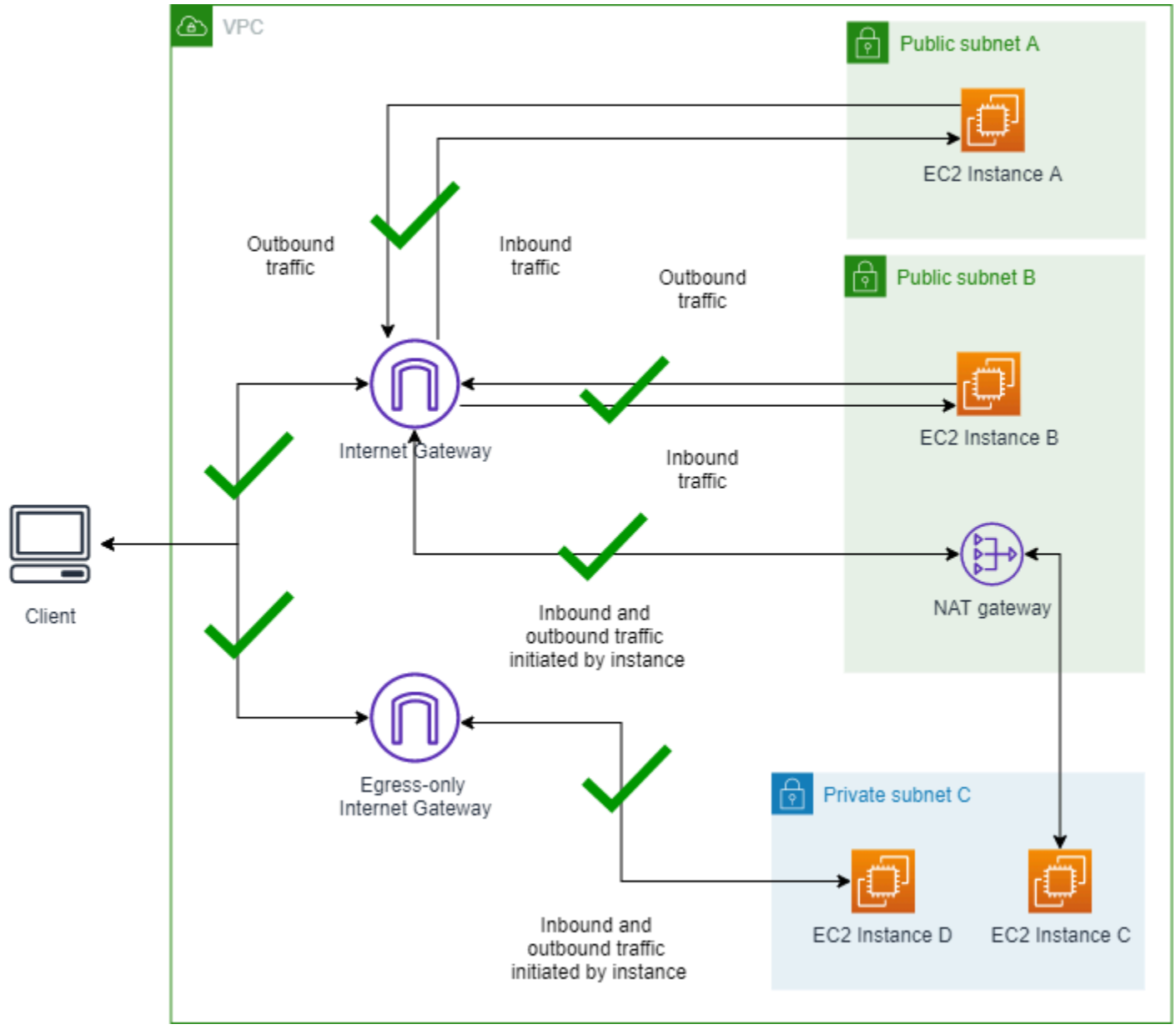
4. 分析調查結果，了解 VPC BPA 對 VPC 資源的影響。

影響分析已完成。

案例 1 – 連線至未開啟 VPC BPA 的執行個體

在本節中，公有子網路 A 與 B 中的 EC2 執行個體可透過網際網路閘道從網際網路連線，同時允許傳入與傳出流量。私有子網路中的執行個體 C 與 D 可以透過 NAT 閘道或僅限輸出網際網路閘道啟動傳出流量，但無法直接從網際網路連線。此設定提供對某些資源的網際網路存取，同時保護其他資源。此設定旨在設定基準，並確保在啟用 VPC BPA 之前，可以連接所有執行個體，並 Ping 公有 IP 位址。

未開啟 VPC BPA 的 VPC 圖表：



1.1 連線至執行個體

完成本節，在 VPC BPA 關閉的情況下連線至您的執行個體，以確保您可以順利連線。此範例中使用 CloudFormation 建立的所有執行個體的名稱都類似於「VPC BPA 執行個體 A」。

AWS 管理主控台

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 開啟執行個體 A 詳細資訊。
3. 使用 EC2 執行個體連線 > 連線 EC2 執行個體連線端點選項連線至執行個體 A。
4. 選擇連線。成功連線至執行個體後，請 Ping www.amazon.com 以確認您可以將傳出請求傳送至網際網路。
5. 使用您用來連線至執行個體 A 的相同方法，連線至執行個體 B、C 和 D。從每個執行個體中，Ping www.amazon.com 以確認您可以將傳出請求傳送至網際網路。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

   ```
   ping 18.225.8.244
   ```

   輸出：

   ```
   Pinging 18.225.8.244 with 32 bytes of data:

   Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
   Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
   ```

   請注意，Ping 成功且流量未遭到封鎖。
2. 使用私有 IPv4 地址來連線和檢查傳出流量：

   ```
   aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
   east-2 --connection-type eice
   ```

   輸出：

   ```
   A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
   Run "/usr/bin/dnf check-release-update" for full release and version update info
   ```

```
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

請注意，Ping 成功且流量未遭到封鎖。

3. 使用公有 IPv4 地址 Ping 執行個體 B 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

請注意，Ping 成功且流量未遭到封鎖。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
```

```
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

請注意，Ping 成功且流量未遭到封鎖。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

請注意，Ping 成功且流量未遭到封鎖。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

輸出：

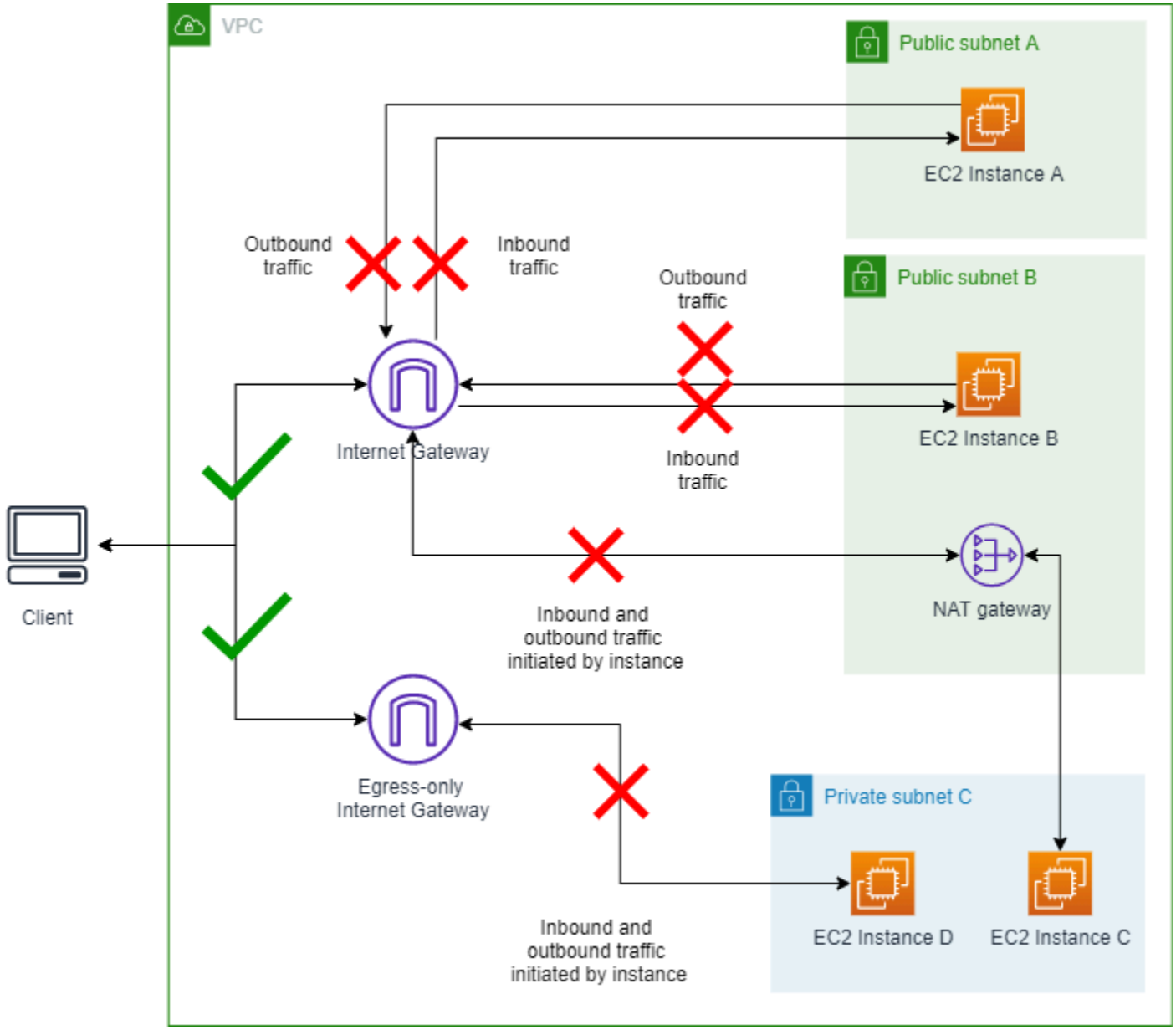
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

請注意，Ping 成功且流量未遭到封鎖。

案例 2 – 開啟 VPC BPA 雙向模式

在本節中，您將開啟 VPC BPA，並封鎖您帳戶中網際網路閘道的往返流量。

圖表，顯示已開啟 VPC BPA 雙向模式：



2.1 啟用 VPC BPA 雙向模式

完成本節以啟用 VPC BPA。VPC BPA 雙向模式會封鎖此區域中往返網際網路閘道和僅輸出網際網路閘道的所有流量 (排除 VPC 和子網路除外)。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇編輯公開存取設定。

4. 選擇開啟「封鎖公開存取」和雙向，然後選擇儲存變更。
5. 等待狀態變更為開啟。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

VPC BPA 現已開啟。

AWS CLI

1. 使用 modify-vpc-block-public-access-options 命令來開啟 VPC BPA：

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

2. 檢視 VPC BPA 的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 連線至執行個體

完成本節以連線至您的執行個體。

AWS 管理主控台

1. Ping 執行個體 A 和執行個體 B 的公有 IPv4 地址，如您在案例 1 中所執行的一樣。請注意，流量會遭到封鎖。
2. 使用 EC2 執行個體連線 > 連線 EC2 執行個體連線端點選項連線至執行個體 A，如您在案例 1 中所執行的一樣。請確定您使用端點選項。
3. 選擇連線。成功連線至執行個體後，請 Ping https：//www.amazon.com。請注意，所有傳出流量都會遭到封鎖。
4. 使用您用來連線至執行個體 A 的相同方法，連線至執行個體 B、C 和 D，並測試傳出請求到網際網路。請注意，所有傳出流量都會遭到封鎖。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 18.225.8.244
```

輸出：

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

2. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

3. 使用公有 IPv4 地址 Ping 執行個體 B 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

輸出：

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

請注意，Ping 會失敗並封鎖流量。

2.3 選用：使用 Reachability Analyzer 確認連線已封鎖

VPC Reachability Analyzer 可用來了解是否可以根據您的網路組態達到特定網路路徑，包括 VPC BPA 設定。在此範例中，您將分析先前嘗試的相同網路路徑，以確認 VPC BPA 是連線失敗的原因。

AWS 管理主控台

1. 透過 https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer 前往 Network Insights 主控台。
2. 選擇建立和分析路徑。
3. 在來源類型欄位中，選擇網際網路閘道，然後從來源下拉式清單中選取標記為 VPC BPA 網際網路閘道的網際網路閘道。
4. 在目的地類型欄位中，選擇執行個體，然後從目的地下拉式清單中選取標記為 VPC BPA 執行個體 A 的執行個體。
5. 選擇建立和分析路徑。
6. 等候分析完成。這可能需要幾分鐘的時間。
7. 完成後，您應該會看到連線性狀態為無法連線，而且路徑詳細資訊顯示 `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` 為原因。

AWS CLI

1. 使用標記為 VPC BPA 網路閘道的網際網路閘道 ID 和標記為 VPC BPA 執行個體 A 的執行個體 ID 建立網路路徑：

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. 在網路路徑上開始分析：

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. 檢索分析的結果：

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

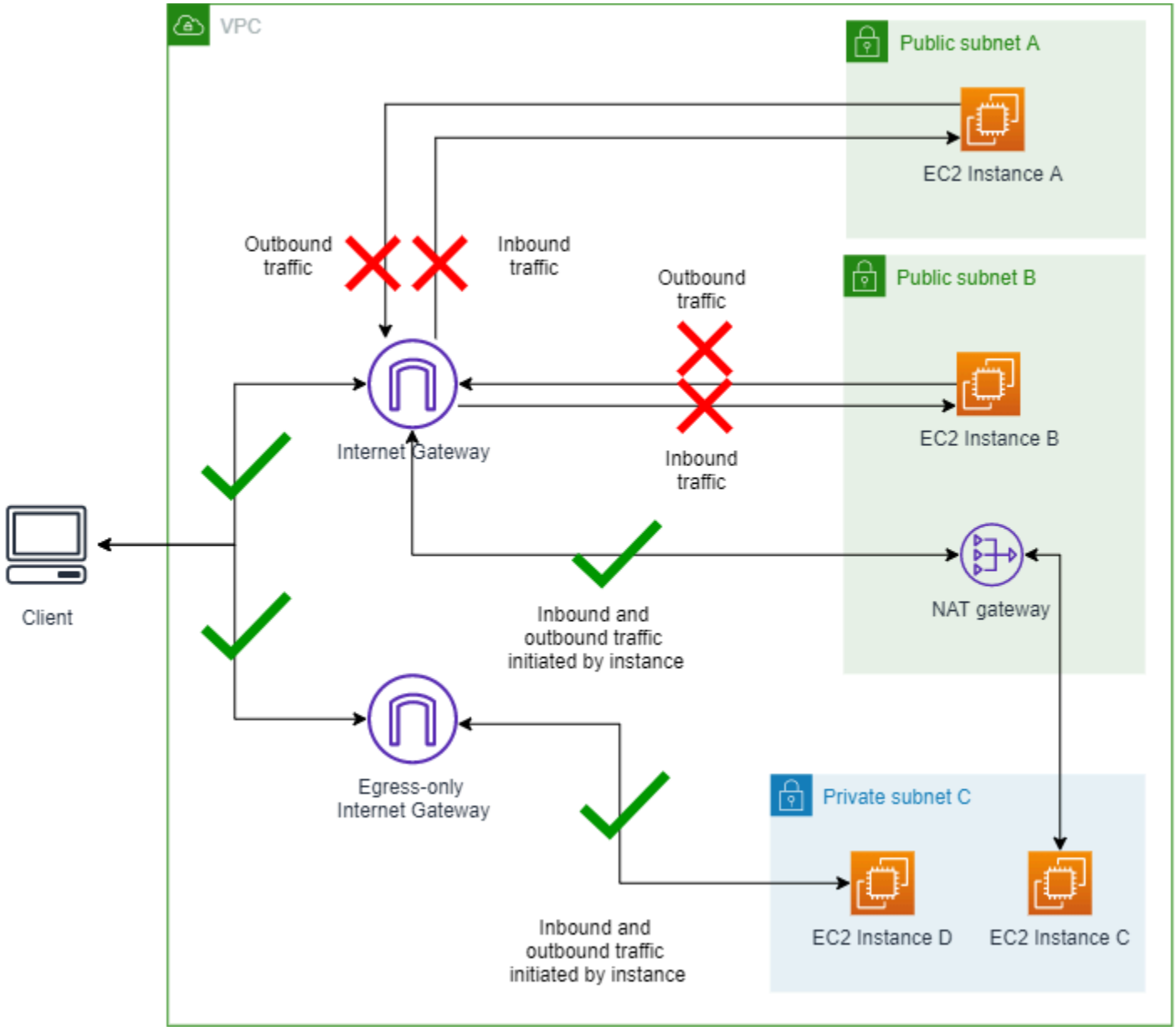
4. 確認 `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` 為 `ExplanationCode`，無法連線。

請注意，您也可以使用流量日誌監控 VPC BPA 影響。

案例 3 – 將 VPC BPA 變更為僅限輸入模式

在本節中，您將變更 VPC BPA 流量方向，並只允許使用 NAT 閘道或僅輸出網際網路閘道的流量。公有子網路中的 EC2 執行個體 A 與 B 將無法從網際網路連線，因為 BPA 會封鎖透過網際網路閘道傳入的流量。私有子網路中的執行個體 C 與 D 仍可透過 NAT 閘道和僅限輸出網際網路閘道啟動傳出流量，因此仍然可以連線網際網路。

開啟的 VPC BPA 僅輸入模式的圖表：



3.1 將模式變更為僅輸入

完成本節以變更模式。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在封鎖公開存取索引標籤中，選擇編輯公開存取設定。
4. 在 VPC 主控台中修改公開存取設定，並將方向變更為僅輸入。
5. 儲存變更並等待狀態更新。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

AWS CLI

1. 修改 VPC BPA 模式：

   ```
   aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
   gateway-block-mode block-ingress
   ```

   VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。
2. 檢視 VPC BPA 的狀態：

   ```
   aws ec2 --region us-east-2 describe-vpc-block-public-access-options
   ```

3.2 連線至執行個體

完成本節以連線至執行個體。

AWS 管理主控台

1. Ping 執行個體 A 和執行個體 B 的公有 IPv4 地址，如您在案例 1 中所執行的一樣。請注意，流量會遭到封鎖。
2. 使用 EC2 執行個體連線連線至執行個體 A 和 B，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您無法從執行個體 A 或 B 在網際網路上 Ping 公有網站，且流量會遭到封鎖。

3. 使用 EC2 執行個體連線連線至執行個體 C 和 D，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您可以從執行個體 C 或 D 對網際網路上 Ping 公有網站，並允許流量。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 18.225.8.244
```

輸出：

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

2. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
```

```
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

3. 使用公有 IPv4 地址 Ping 執行個體 B 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

輸出：

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

請注意，Ping 成功且流量未遭到封鎖。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
```

```
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

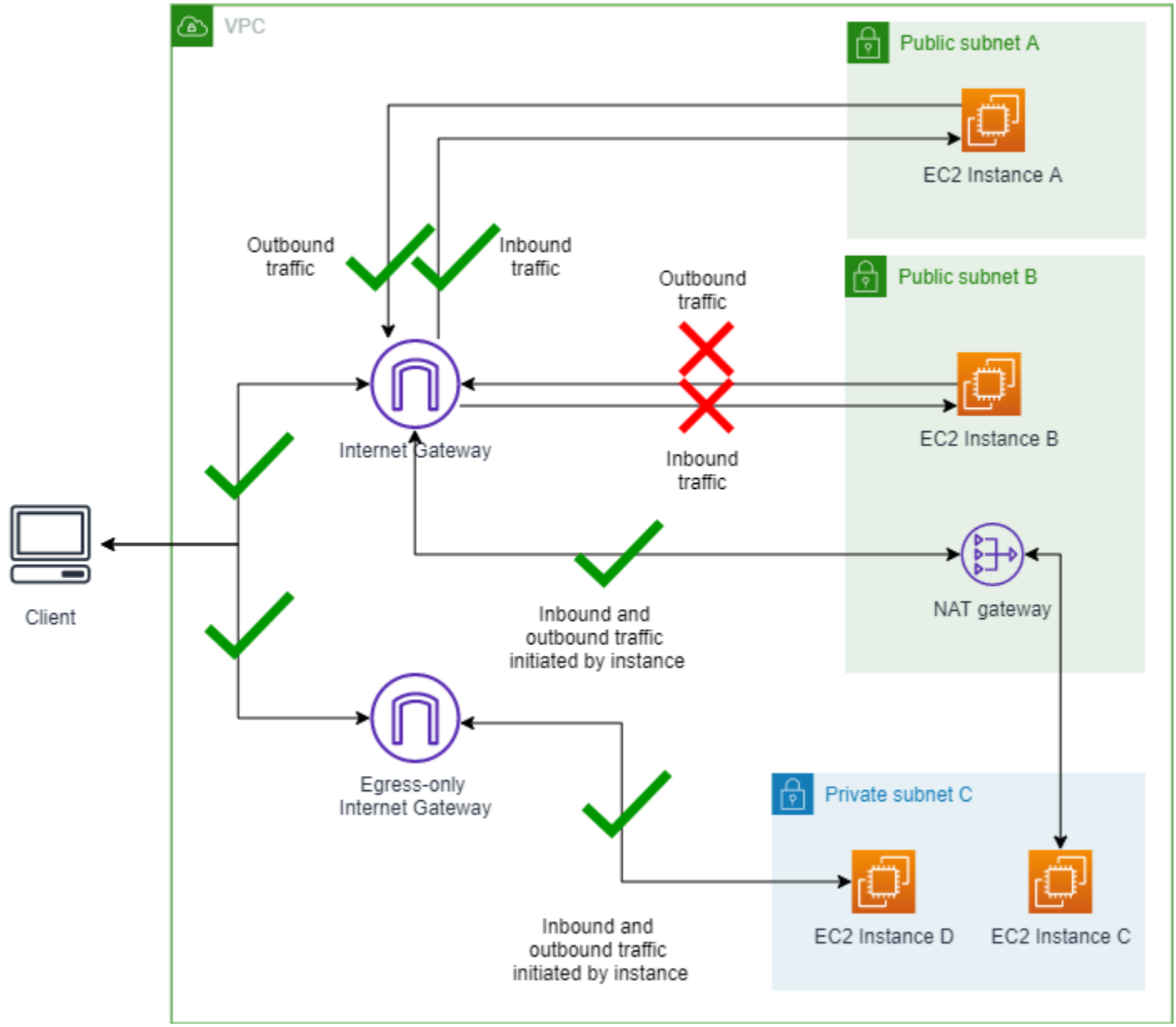
請注意，Ping 成功且流量未遭到封鎖。

案例 4 – 建立排除

在本節中，您會建立排除項目。然後，VPC BPA 只會封鎖沒有排除項目的子網路上的流量。VPC BPA 排除是一種模式，可套用至單一 VPC 或子網路，以將其從帳戶的 VPC BPA 模式排除，並允許雙向或僅輸出存取。即使帳戶未啟用 VPC BPA，您也可以為 VPC 和子網路建立 VPC BPA 排除項目，以確保在開啟 VPC BPA 時，排除項目不會發生流量中斷。

在此範例中，我們將建立子網路 A 的排除，以顯示到排除的流量受到 VPC BPA 的影響。

開啟 VPC BPA 僅輸入模式和開啟雙向模式的子網路 A 排除的圖表：



4.1 建立子網路 A 的排除

完成本節以建立排除。VPC BPA 排除是一種模式，可套用至單一 VPC 或子網路，以將其從帳戶的 VPC BPA 模式排除，並允許雙向或僅輸出存取。即使帳戶未啟用 VPC BPA，您也可以為 VPC 和子網路建立 VPC BPA 排除項目，以確保在開啟 VPC BPA 時，排除項目不會發生流量中斷。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在封鎖公開存取標籤的排除下，選擇建立排除。

4. 選擇 VPC BPA 公有子網路 A，確保選取允許方向雙向，然後選擇建立排除。
5. 等待排除狀態變更為作用中。您可能需要重新整理排除資料表才能查看變更。

已建立排除。

AWS CLI

1. 修改排除允許方向：

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. 可能需要一些時間才能更新排除狀態。檢視排除的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 連線至執行個體

完成本節以連線至執行個體。

AWS 管理主控台

1. Ping 執行個體 A 的公有 IPv4 地址。請注意，允許流量。
2. Ping 執行個體 B 的公有 IPv4 地址。請注意，流量已封鎖。
3. 使用 EC2 執行個體連線連線至執行個體 A，如同您在案例 1 中所做的，並 Ping www.amazon.com。請注意，您可以從執行個體 A 在網際網路上 Ping 公有網站。允許流量。
4. 使用 EC2 執行個體連線連線至執行個體 B，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您無法從執行個體 B 在網際網路上 Ping 公有網站。流量會遭到封鎖。
5. 使用 EC2 執行個體連線連線至執行個體 C 和 D，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您可以從執行個體 C 或 D 對網際網路上 Ping 公有網站。允許流量。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 18.225.8.244
```

輸出：

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

請注意，Ping 成功且流量未遭到封鎖。

2. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

請注意，Ping 成功且流量未遭到封鎖。

3. 使用公有 IPv4 地址 Ping 執行個體 B 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

請注意，Ping 成功且流量未遭到封鎖。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
```

```
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

請注意，Ping 成功且流量未遭到封鎖。

4.3 選用：驗證與 Reachability Analyzer 的連線

使用案例 2 中的 Reachability Analyzer 中建立的相同網路路徑，您現在可以執行新的分析，並確認現在已為公有子網路 A 建立排除項目，即可連線該路徑。

如需 Reachability Analyzer 區域可用性的相關資訊，請參閱《Reachability Analyzer 指南》中的考量。

AWS 管理主控台

1. 從您先前在 Network Insights 主控台中建立的網路路徑中，選擇重新執行分析。
2. 等候分析完成。這可能需要幾分鐘的時間。
3. 確認路徑現在可連線。

AWS CLI

1. 使用先前建立的網路路徑 ID，開始新的分析：

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

2. 檢索分析的結果：

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

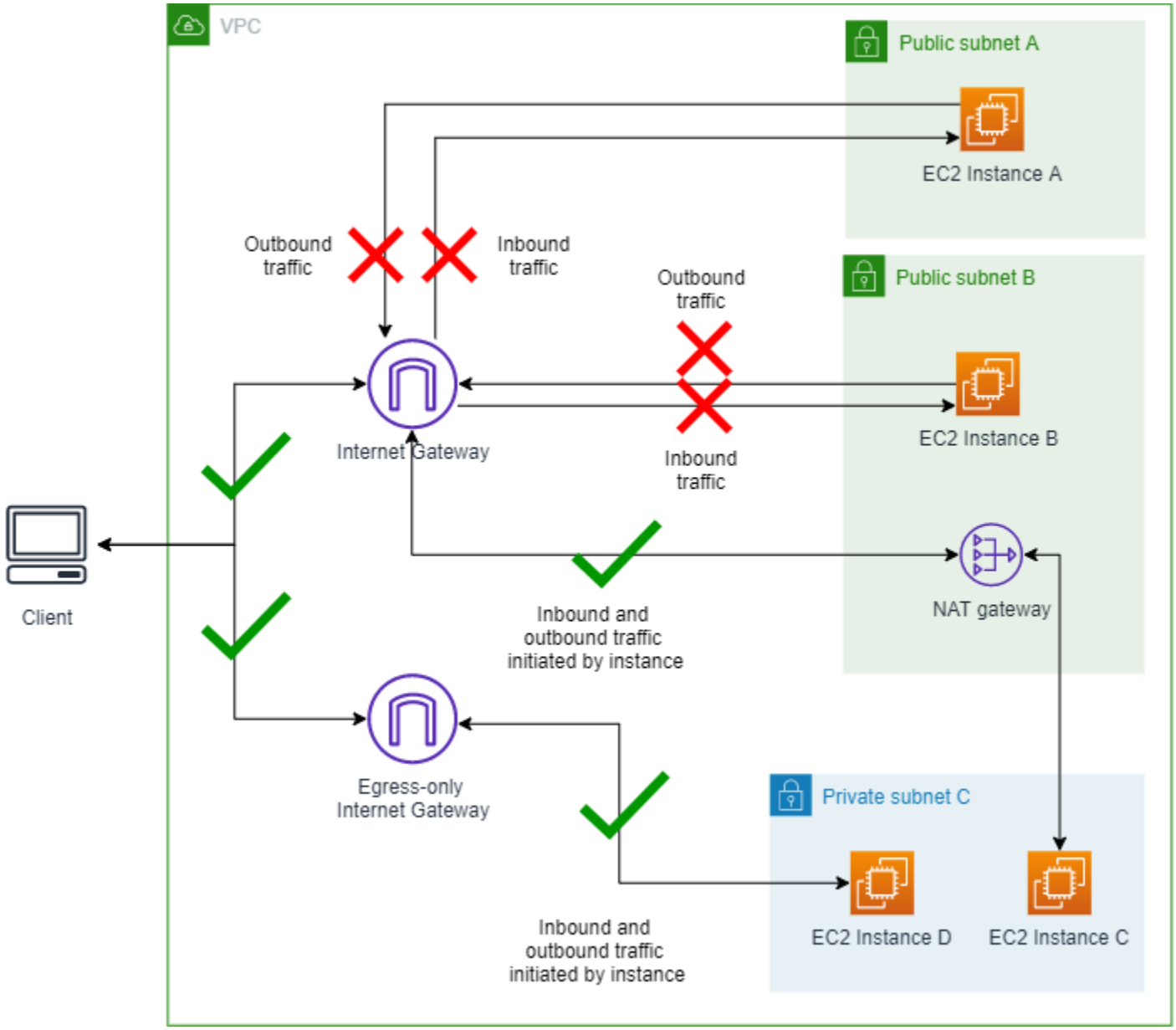
3. 確認 VPC_BLOCK_PUBLIC_ACCESS_ENABLED 說明代碼不再存在。

案例 5 – 修改排除模式

在本節中，您將變更排除的允許流量方向，以查看它如何影響 VPC BPA。

> **Note**
>
> 在此案例中，您会將排除模式變更為僅限輸出。請注意，當您執行此操作時，子網路 A 上的輸出限定排除不允許傳出流量，這違反直覺，因為您預期它允許傳出流量。不過，由於帳戶層級 BPA 是僅限輸入，因此會忽略僅限輸出的排除，且子網路 A 路由至網際網路閘道受到 VPC BPA 的限制，以封鎖傳出流量。若要在子網路 A 上啟用傳出流量，您必須將 VPC BPA 切換為雙向模式。

開啟 VPC BPA 僅輸入模式和開啟僅輸出模式的子網路 A 排除的圖表：



5.1 將排除允許方向變更為僅輸出

完成本節以變更排除允許方向。

AWS 管理主控台

1. 編輯您在案例 4 中建立的排除，並將允許方向變更為僅輸出。
2. 選擇儲存變更。
3. 等待排除狀態變更為作用中。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。您可能需要重新整理排除資料表才能查看變更。

AWS CLI

1. 修改排除允許方向：

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

2. 可能需要一些時間才能更新排除狀態。檢視排除的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 連線至執行個體

完成本節以連線至執行個體。

AWS 管理主控台

1. Ping 執行個體 A 和 B 的公有 IPv4 地址。請注意，流量已封鎖。
2. 使用 EC2 執行個體連線連線至執行個體 A 和 B，如同您在案例 1 中所做的，並 Ping www.amazon.com。請注意，您無法從執行個體 A 或 B 在網際網路上 Ping 公有網站。流量會遭到封鎖。
3. 使用 EC2 執行個體連線連線至執行個體 C 和 D，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您可以從執行個體 C 或 D 對網際網路上 Ping 公有網站。允許流量。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 18.225.8.244
```

   輸出：

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

2. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

3. 使用公有 IPv4 地址 Ping 執行個體 B 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
```

```
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

請注意，Ping 成功且流量未遭到封鎖。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

輸出：

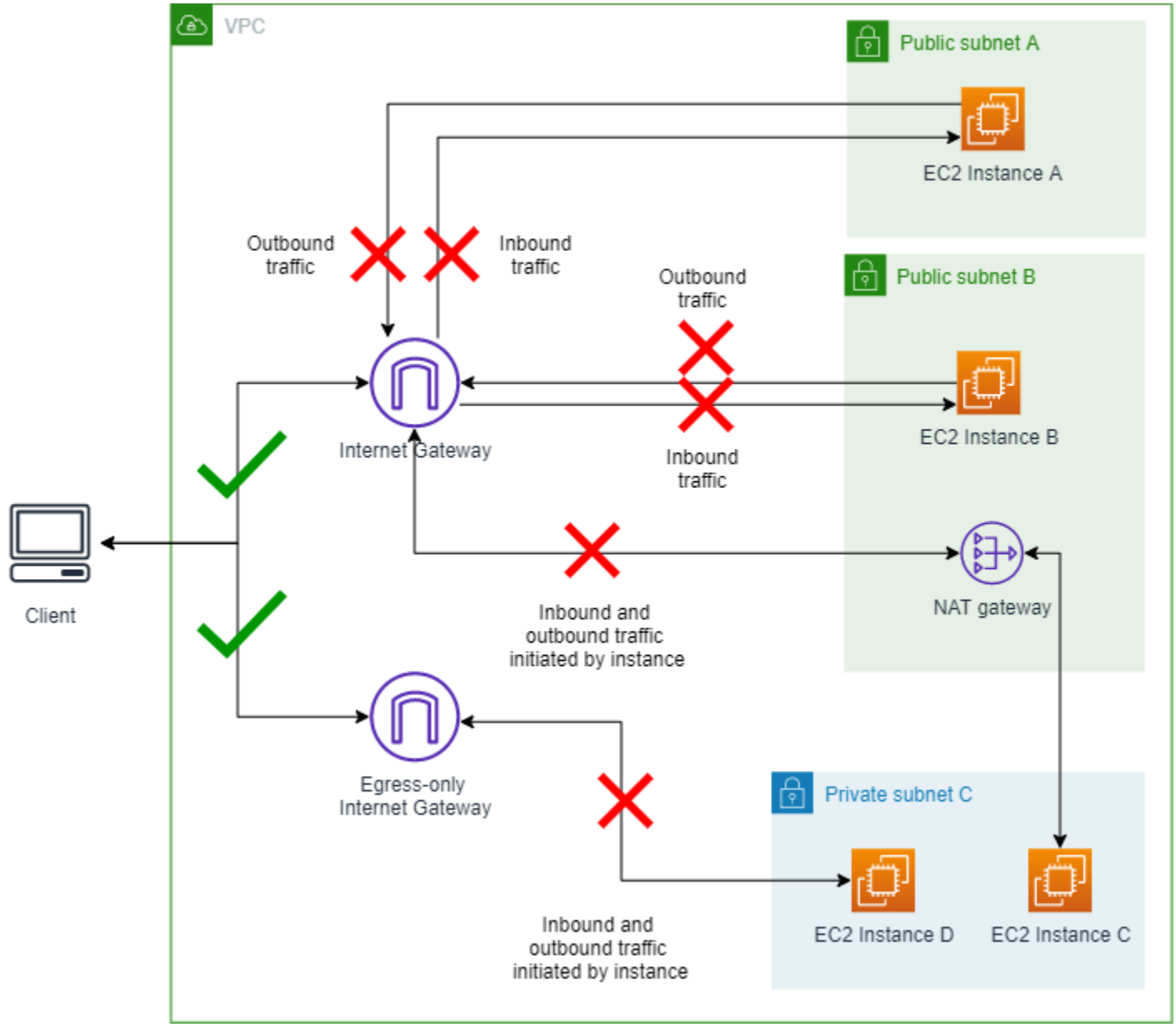
```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

請注意，Ping 成功且流量未遭到封鎖。

案例 6 – 修改 VPC BPA 模式

在本節中，您將變更 VPC BPA 區塊方向，以查看其如何影響流量。在此案例中，在雙向模式中啟用 VPC BPA 會封鎖所有流量，就像案例 1 一樣。除非排除可存取 NAT 閘道或僅輸出網際網路閘道，否則會封鎖流量。

開啟 VPC BPA 雙向模式和開啟僅輸出模式的子網路 A 排除的圖表：



6.1 將 VPC BPA 變更為雙向模式

完成本節以變更 VPC BPA 模式。

AWS 管理主控台

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇編輯公開存取設定。
4. 將區塊方向變更為雙向，然後選擇儲存變更。

5. 等待狀態變更為開啟。VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

AWS CLI

1. 修改 VPC BPA 區塊方向：

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

VPC BPA 設定可能需要幾分鐘的時間才會生效，並更新狀態。

2. 檢視 VPC BPA 的狀態：

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 連線至執行個體

完成本節以連線至執行個體。

AWS 管理主控台

1. Ping 執行個體 A 和 B 的公有 IPv4 地址。請注意，流量已封鎖。
2. 使用 EC2 執行個體連線連線至執行個體 A 和 B，如同您在案例 1 中所做的，並 Ping www.amazon.com。請注意，您無法從執行個體 A 或 B 在網際網路上 Ping 公有網站。流量會遭到封鎖。
3. 使用 EC2 執行個體連線連線至執行個體 C 和 D，如同您在案例 1 中所做的，並從中 Ping www.amazon.com。請注意，您無法從執行個體 C 或 D 在網際網路上 Ping 公有網站。流量會遭到封鎖。

AWS CLI

1. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 18.225.8.244
```

輸出：

```
Pinging 18.225.8.244 with 32 bytes of data:
```

```
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

2. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

3. 使用公有 IPv4 地址 Ping 執行個體 A 以檢查傳入流量：

```
ping 3.18.106.198
```

輸出：

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

請注意，Ping 會失敗並封鎖流量。

4. 使用私有 IPv4 地址來連線和檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

請注意，Ping 會失敗並封鎖流量。

5. 連線至執行個體 C。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
```

```
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

請注意，Ping 會失敗並封鎖流量。

6. 連線至執行個體 D。由於沒有公有 IP 位址可供 Ping，請使用「EC2 執行個體連線」連線執行個體，然後從執行個體 Ping 公有 IP 來檢查傳出流量：

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

輸出：

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

請注意，Ping 會失敗並封鎖流量。

清除

在本節中，您將刪除為此進階範例建立的所有資源。請務必清理資源，以避免帳戶中建立的資源產生過多的額外費用。

刪除 CloudFormation 資源

完成本節以刪除您使用 CloudFormation 範本建立的資源。

AWS 管理主控台

1. 在 開啟 CloudFormation 主控台https://console.aws.amazon.com/cloudformation/。
2. 選擇 VPC BPA 堆疊。
3. 選擇 刪除。
4. 開始刪除堆疊後，請檢視事件標籤以檢視進度，並確保堆疊已刪除。您可能需要強制刪除堆疊，才能將其完全刪除。

AWS CLI

1. 刪除 CloudFormation 堆疊。您可能需要強制刪除堆疊，才能將其完全刪除。

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. 檢視進度並確保堆疊已刪除。

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

使用 CloudTrail 追蹤排除項目刪除

完成本節以使用 追蹤排除刪除 AWS CloudTrail。當您刪除排除時，會顯示 CloudTrail 項目。

AWS 管理主控台

您可以在 的 CloudTrail 主控台中查詢資源類型 > AWS::EC2::VPCBlockPublicAccessExclusion，以檢視 AWS CloudTrail 事件歷史記錄中任何已刪除的排除https://console.aws.amazon.com/cloudtrailv2/。

AWS CLI

您可以使用 lookup-events 命令來檢視與刪除排除相關的事件：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

進階範例已完成。

VPC 的安全最佳實務

以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

- 將子網路新增至 VPC 以託管應用程式時，在多個可用區域中建立子網路。可用區域是一個或多個離散的資料中心，在 AWS 區域中具有備援電源、聯網和連線能力。使用多個可用區域可使生產應用程式具備高可用性、容錯能力和可擴展性。
- 使用安全群組來控制到子網路中 EC2 執行個體的流量。如需詳細資訊，請參閱Security groups (安全群組)。
- 使用網路 ACL 來控制子網路層級的傳出和傳入流量。如需詳細資訊，請參閱使用網路存取控制清單控制子網路流量。
- 使用 AWS Identity and Access Management (IAM) 聯合身分、使用者和角色管理對 VPC 中 AWS 資源的存取。如需詳細資訊，請參閱Amazon VPC 的身分和存取管理。
- 使用 VPC 流量日誌以監控從 VPC、子網路或網路介面傳入和傳出的 IP 流量。如需詳細資訊，請參閱VPC 流程日誌。
- 使用網路存取分析器識別對 VPC 中資源的意外網路存取。如需詳細資訊，請參閱 Network Access Analyzer Guide (《網路存取分析器指南》)。
- AWS Network Firewall 使用 透過篩選傳入和傳出流量來監控和保護您的 VPC。如需詳細資訊，請參閱 AWS Network Firewall 指南。
- 使用 Amazon GuardDuty 偵測您 AWS 環境中帳戶、容器、工作負載和資料的潛在威脅。基礎威脅偵測包括監控與您的 Amazon EC2 執行個體相關聯的 VPC 流程日誌。如需詳細資訊，請參閱《Amazon GuardDuty 使用者指南》中的 VPC 流程日誌。

如需 VPC 安全常見問答集的解答，請參閱 Amazon VPC 常見問答集中的安全和篩選。

搭配其他 使用 Amazon VPC AWS 服務

Amazon Virtual Private Cloud (VPC) 是一項基礎 AWS 服務，為您的雲端基礎設施提供安全、可自訂的網路環境。除了建立和管理您自己的 VPC 之外，您還可以使用 VPC 與其他 AWS 服務之間的整合，來建置符合您特定需求的全方位解決方案。

您可以使用 將 VPC 連線至各種 AWS 服務 AWS PrivateLink。這可讓您在 VPC 與支援的 AWS 服務或內部部署應用程式之間進行私有連線，保持 AWS 網路內的網路流量，並避免暴露於公有網際網路。這對於維護嚴格的安全界限和合規要求尤為重要。

若要進一步增強 VPC 的安全性，您可以使用 AWS Network Firewall。此受管防火牆服務允許您定義並強制執行網路層級的安全政策，篩選 VPC 內的南北向流量和東西向流量。透過將 Network Firewall 與您的 VPC 配對，您可以強化防禦策略，並保護您的雲端資源免受未經授權的存取或惡意活動。

此外，您可以使用 Route 53 Resolver DNS Firewall 篩選 VPC 內的 DNS 流量。此功能允許您建立自訂 DNS 篩選規則，控制您的 VPC 資源可以解析的網域，進而提供額外的安全層和合規強制執行。

如果您在 VPC 內的資源之間或連線至 VPC 時遇到連線能力問題，您可以使用 Reachability Analyzer。Reachability Analyzer 會執行虛擬連線測試，提供詳細的逐跳路徑資訊，並識別任何封鎖元件。此故障診斷工具可協助您快速識別並解決網路連線問題。

透過將這些補充 AWS 服務與您的 VPC 整合，您可以建置功能強大、安全且具彈性的雲端解決方案，以因應您獨特的業務和架構需求。

目錄

- 使用 將您的 VPC 連接到 服務 AWS PrivateLink
- 使用 AWS Network Firewall 篩選網路流量
- 使用 Route 53 Resolver DNS Firewall 來篩選 DNS 流量
- 使用 Reachability Analyzer 進行連線能力問題故障診斷

使用 將您的 VPC 連接到 服務 AWS PrivateLink

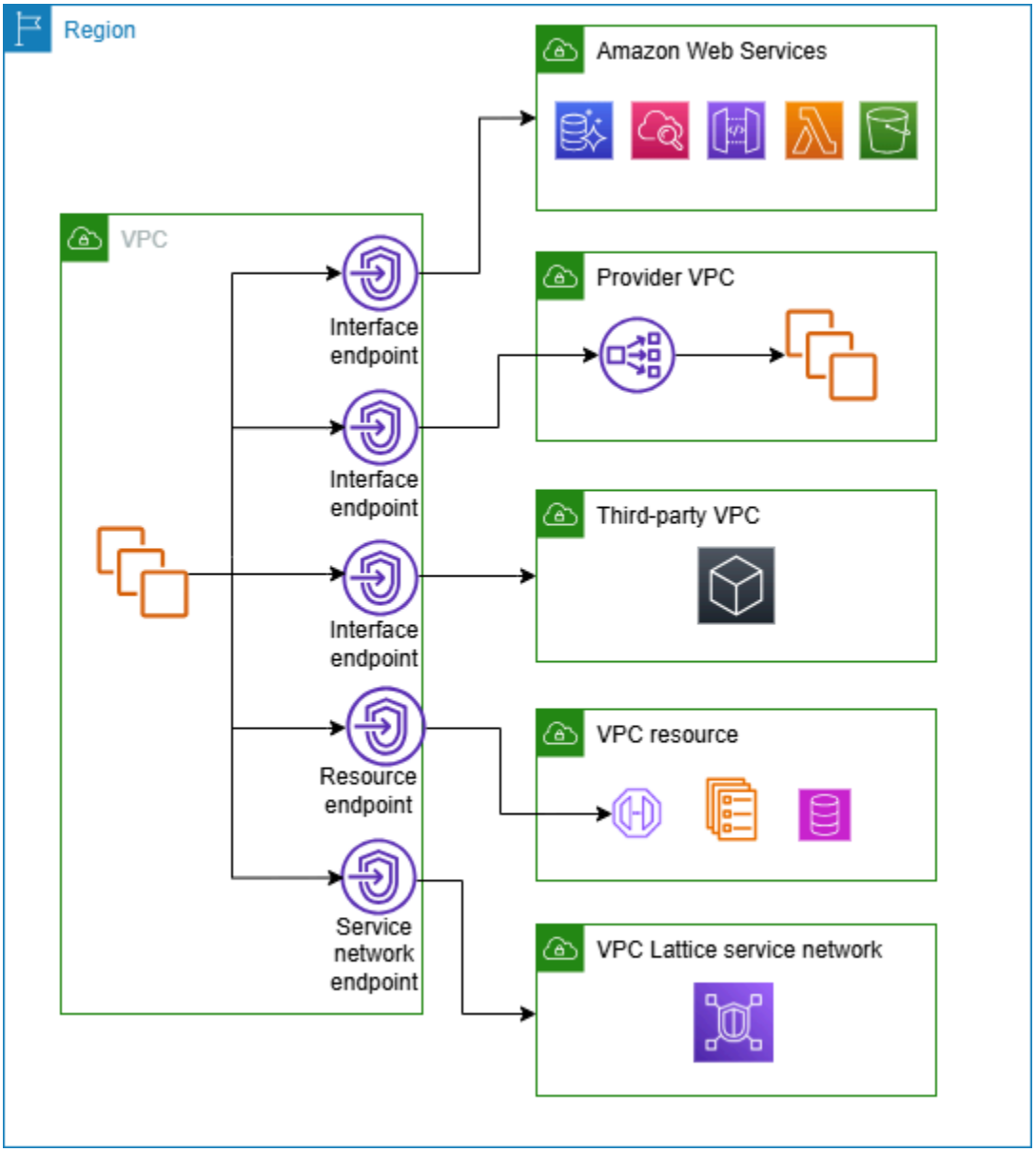
AWS PrivateLink 在虛擬私有雲端 (VPC) 與支援的 AWS 服務服務、其他託管的服務 AWS 帳戶、支援的 AWS Marketplace 服務和支援的 資源之間建立私有連線。您不需要使用網際網路閘道、NAT 裝置 Direct Connect 、連線或 AWS Site-to-Site VPN 連線來與服務或資源通訊。

若要使用 AWS PrivateLink，請在您需要從中存取服務或資源的任何子網路中建立 VPC 端點。這會在指定子網路中建立彈性網絡介面，作為通往目標服務或資源的流量進入點。

您也可以建立自己的 VPC 端點服務，由 提供支援 AWS PrivateLink ，並讓其他 AWS 客戶存取您的服務。PrivateLink 可建立私有 API 端點，讓組織安全地向其他 AWS 客戶公開自己的服務。這可讓企業從內部功能獲利、培養協作生態系統，並維持對存取和使用其服務方式的控制。

使用 的主要優點之一 AWS PrivateLink 是能夠建立安全的私有連線，而不需要網際網路閘道、NAT 裝置或 VPN 連線等傳統聯網建構。這有助於簡化網路架構、減少受攻擊面，並透過將資料流量限制在 AWS 網路內來改善整體安全性。

下圖顯示 的常見使用案例 AWS PrivateLink。VPC 的私有子網路中有多個 EC2 執行個體可透過五個 VPC 端點存取資源。其中包括三個介面 VPC 端點、一個資源 VPC 端點與一個服務網路 VPC 端點。



如需詳細資訊，請參閱AWS PrivateLink。

使用 AWS Network Firewall 篩選網路流量

您可以使用 AWS Network Firewall 篩選 VPC 周邊的網路流量。Network Firewall 是一種可設定狀態、受管理的網路防火牆和入侵偵測與預防服務。如需詳細資訊，請參閱 AWS Network Firewall 開發人員指南。

您可以使用下列 AWS 資源實作 Network Firewall。

Network Firewall 資源	描述
防火牆	防火牆會將防火牆政策的網路流量篩選行為連線到您要保護的 VPC。防火牆組態包含可用區域和防火牆端點所在子網路的規格。它還定義了高階設定，如防火牆記錄組態和 AWS 防火牆資源上的標記。 如需詳細資訊，請參閱 AWS Network Firewall 中的防火牆。
防火牆政策	防火牆政策定義防火牆的監控和防護行為。行為的詳細資料定義在您新增至政策的規則群組中，以及某些政策預設設定中。若要使用防火牆政策，請將其與一或多個防火牆建立關聯。 如需詳細資訊，請參閱 AWS Network Firewall 中的防火牆政策。
規則群組	規則群組是一組可重複使用的準則，用於檢查和處理網路流量。您可以將一或多個規則群組新增至防火牆政策，做為政策組態的一部分。您可以定義無狀態規則群組，以隔離檢查每個網路封包。無狀態規則群組的行為和使用方式與 Amazon VPC 網路存取控制清單 (ACL) 類似。您也可以定義可設定狀態的規則群組，以便在封包流量的內容中檢查封包。可設定狀態規則群組的行為和使用方式與 Amazon VPC 安全群組類似。 如需詳細資訊，請參閱 AWS Network Firewall 中的規則群組。

您也可以使用 AWS Firewall Manager 來集中設定和管理 AWS Organizations 中的帳戶和應用程式之間的 Network Firewall 資源。您可以使用 Firewall Manager 中的單一帳戶來管理多個帳戶的防火牆。如需詳細資訊，請參閱 AWS WAF、AWS Firewall Manager 和 AWS Shield Advanced 開發人員指南中的 AWS Firewall Manager。

使用 Route 53 Resolver DNS Firewall 來篩選 DNS 流量

使用 DNS 防火牆，您可以在與 VPC 關聯的規則群組中定義網域名稱篩選規則。您可以指定要允許或封鎖的網域名稱清單，也可以自訂要封鎖的 DNS 查詢的回應。如需詳細資訊，請參閱 Route 53 Resolver DNS Firewall 文件。

您可以使用下列 AWS 資源實作 DNS Firewall。

DNS Firewall 資源	描述
DNS Firewall 規則群組	DNS Firewall 規則群組是具名、可重複使用的 DNS Firewall 規則集合，用於篩選 DNS 查詢。您可以使用篩選規則填入規則群組，然後將規則群組與 Amazon VPC 中的一或多個 VPC 建立關聯。當您將規則群組與 VPC 建立關聯時，即啟用 VPC 的 DNS Firewall 篩選。然後，當 Resolver 收到具有與其相關聯的規則群組的 VPC 的 DNS 查詢時，Resolver 會將查詢傳遞至 DNS Firewall 進行篩選。 規則群組中的每個規則都會指定一個網域清單，以及要對其網域符合清單中網域規格的 DNS 查詢採取的動作。您可以允許、封鎖或提醒相符查詢。您也可以為封鎖的查詢定義自訂回應。 如需詳細資訊，請參閱 Route 53 Resolver DNS Firewall 中的規則群組和規則。
網域清單	網域清單是一組可重複使用的網域規格，可在規則群組的 DNS Firewall 規則中使用。 如需詳細資訊，請參閱 Route 53 Resolver DNS Firewall 中的網域清單。

您也可以使用 AWS Firewall Manager 來集中設定和管理 AWS Organizations 中的帳戶和組織之間的 DNS Firewall 資源。您可以使用 Firewall Manager 中的單一帳戶來管理多個帳戶的防火牆。如需詳細資訊，請參閱 AWS WAF、AWS Firewall Manager 和 AWS Shield Advanced 開發人員指南中的 AWS Firewall Manager。

使用 Reachability Analyzer 進行連線能力問題故障診斷

Reachability Analyzer 是一種靜態組態分析工具。使用 Reachability Analyzer 來分析 VPC 中兩項資源之間的網路連線能力並進行偵錯。Reachability Analyzer 會在可連線虛擬路徑時，在這些路徑之間產生逐個躍點的詳細資訊，並在無法連線時識別導致阻礙的元件。

您可以使用 Reachability Analyzer 來分析下列資源之間的連線能力：

- 執行個體
- 網際網路閘道
- 網路介面
- 傳輸閘道
- 傳輸閘道連接
- VPC 端點服務
- VPC 端點
- VPC 對等連線
- VPN 閘道

如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

VPC 範例

Amazon 虛擬私有雲端 (VPC) 是 AWS 生態系統中的基本建置區塊，可讓您佈建專為特定需求量身打造的隔離虛擬網路。透過建立和管理您自己的 VPC，您可以完全控制聯網環境，包括定義 IP 位址範圍、子網路、路由表和連線選項的能力。

本節包含三個虛擬私有雲端 (VPC) 的範例組態，每個範例組態的設計都是為了滿足不同的需求：

- 測試環境的 VPC：此組態顯示如何建立 VPC，供您用於開發或測試環境。
- 用於 Web 和資料庫伺服器的 VPC：此組態說明如何建立 VPC，供您用於生產環境中的無提示架構。
- VPC 搭配私有子網路和 NAT 的伺服器：在此進階組態中，所有 EC2 執行個體都會佈建在私有子網路中，並透過 NAT 閘道提供安全的網際網路傳出存取。這是一個範例，您需要限制資源的直接網際網路連線，同時仍然啟用必要的傳出通訊。

透過提供這些範例 VPC 組態，我們希望能說明設計雲端聯網環境時可用的彈性和自訂選項。您選擇的特定 VPC 設定應基於應用程式的架構、安全需求和整體業務目標。仔細規劃 VPC 基礎設施可協助您建立強大、可擴展且安全的虛擬網路，以支援雲端工作負載的成長與演變。

範例

- 範例：測試環境的 VPC
- 範例：適用於 Web 和資料庫伺服器的 VPC
- 範例：在私有子網路和 NAT 具有伺服器的 VPC

相關範例

- 若要讓 VPC 彼此連線，請參閱《Amazon VPC 對等互連指南》中的 VPC 對等互連組態。
- 若要將 VPC 連線至自己的網路，請參閱 AWS Site-to-Site VPN User Guide 中的 Site-to-Site VPN scenarios。
- 若要讓 VPC 彼此連線並連線至您自己的網路，請參閱 Amazon VPC Transit Gateways 中的 Example transit gateway scenarios。

其他資源

- 了解恢復模式和權衡取捨 (AWS 架構部落格)

- 規劃您的網路拓撲 (AWS Well-Architected Framework)
- Amazon Virtual Private Cloud 連線選項 (AWS 白皮書)

範例：測試環境的 VPC

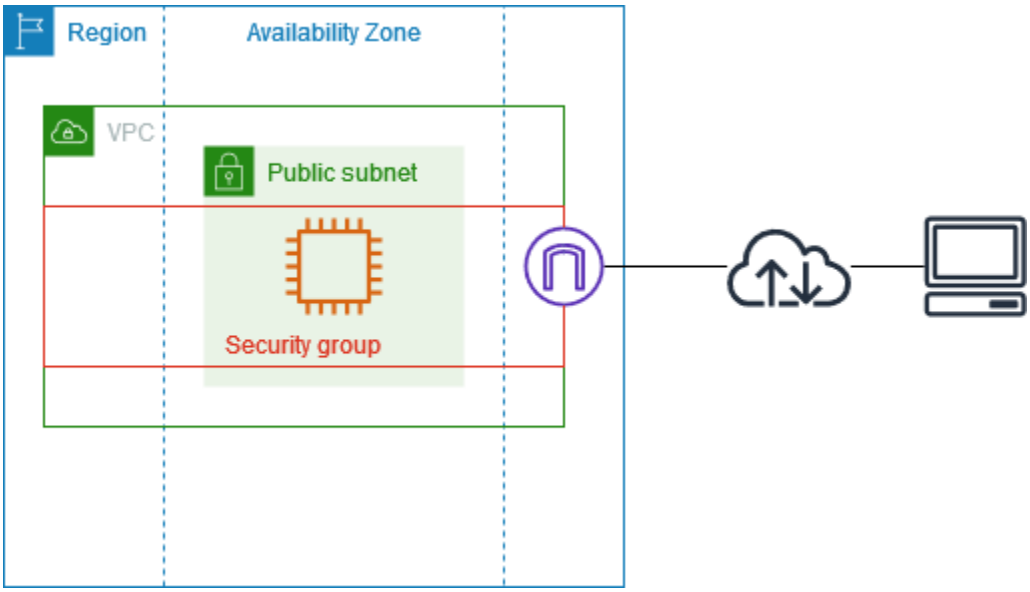
此範例示範如何建立可用作開發或測試環境的 VPC。由於此 VPC 並非用於生產，因此不需要在多個可用區域中部署伺服器。若要維持低成本和複雜性，您可以在單一可用區域中部署伺服器。

目錄

- 概要
- 1. 建立 VPC
- 2. 部署您的應用程式
- 3. 測試組態
- 4. 清除

概要

下圖提供此範例所包含的資源概觀。VPC 在單一可用區域和網際網路閘道中有一個公有子網路。伺服器是在公有子網路中執行的 EC2 執行個體。執行個體的安全群組允許來自您自己電腦的 SSH 流量，以及開發或測試活動特別需要的任何其他流量。



路由

當您使用 Amazon VPC 主控台建立此 VPC 時，我們會為具有本機路由和網際網路閘道之路由的公有子網路建立路由表。以下是具有 IPv4 和 IPv6 路由的路由表範例。如果您建立僅限 IPv4 的子網路 (而不是雙堆疊子網路)，則路由表只會有 IPv4 路由。

目標	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	*igw-id*
::/0	*igw-id*

安全

對於此範例組態，您必須為您的執行個體建立允許您應用程式所需流量的安全群組。例如，您可能需要新增規則，以允許來自電腦的 SSH 流量或來自網路的 HTTP 流量。

以下是安全群組的傳入規則範例，其中包含 IPv4 和 IPv6 的規則。如果您建立僅限 IPv4 子網路 (而不是雙堆疊子網路)，則僅需要 IPv4 的規則。

來源	通訊協定	連接埠範圍	描述
0.0.0.0/0	TCP	80	允許來自所有 IPv4 地址的傳入 HTTP 存取
::/0	TCP	80	允許來自所有 IPv6 地址的傳入 HTTP 存取
0.0.0.0/0	TCP	443	允許來自所有 IPv4 地址的傳入 HTTPS 存取
::/0	TCP	443	允許來自所有 IPv6 地址的傳入 HTTPS 存取

來源	通訊協定	連接埠範圍	描述
###### IPv4 ####	TCP	22	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 SSH 存取
###### IPv6 ####	TCP	22	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 SSH 存取
###### IPv4 ####	TCP	3389	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 RDP 存取
###### IPv6 ####	TCP	3389	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 RDP 存取

1. 建立 VPC

使用下列程序建立在一個可用區域具有公有子網路的 VPC。此組態適用於開發或測試環境。

若要建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在儀表板上，選擇建立 VPC。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 設定 VPC
   a. 針對自動產生名稱標籤，輸入 VPC 的名稱。
   b. 對於 IPv4 CIDR 區塊，您可以保留預設建議，或者您也可以輸入應用程式或網路所需的 CIDR 區塊。如需詳細資訊，請參閱the section called “VPC CIDR 區塊”。
   c. (選用) 如果您的應用程式使用 IPv6 位址進行通訊，請選擇 IPv6 CIDR 區塊 > Amazon 提供的 IPv6 CIDR 區塊。
5. 設定子網路
   a. 對於可用區域 (AZ) 的數量，請選擇 1。您可以保留預設的可用區域，或者也可以展開自訂 AZ 並選取可用區域。
   b. 對於 Number of public subnet (公有子網的數量)，選擇 1。
   c. 對於 Number of private subnet (私有子網的數量)，選擇 0。

d. 您可以保留公有子網路的預設 CIDR 區塊，或者您也可以展開自訂子網路 CIDR 區塊並輸入 CIDR 區塊。如需詳細資訊，請參閱the section called “子網路 CIDR 區塊”。

6. 若為 NAT 閘道，請保留預設值無。
7. 對於 VPC endpoints (VPC 端點)，選擇 None (無)。S3 的閘道 VPC 端點僅用於從私有子網路存取 Amazon S3。
8. 保持選取 DNS 選項中的兩個選項。因此，您的執行個體將收到與其公有 IP 地址對應的公有 DNS 主機名稱。
9. 選擇建立 VPC。

2. 部署您的應用程式

您可透過各種不同方式部署 EC2 執行個體。例如：

- Amazon EC2 啟動執行個體精靈
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

部署 EC2 執行個體後，您可以連線至執行個體、安裝應用程式所需的軟體，然後建立映像以供日後使用。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的建立 AMI。或者，您也可以使用 EC2 Image Builder 來建立和管理您的 Amazon Machine Image (AMI)。

3. 測試組態

完成應用程式部署後，您可以對其進行測試。如果您無法連線至 EC2 執行個體，或如果您的應用程式無法傳送或接收預期的流量，您可以使用 Reachability Analyzer 來協助您進行疑難排解。例如，Reachability Analyzer 可以識別路由表或安全群組的組態問題。如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

4. 清除

此組態結束使用後即可刪除。您必須先終止執行個體，才能刪除 VPC。如需詳細資訊，請參閱the section called “刪除您的 VPC”。

範例：適用於 Web 和資料庫伺服器的 VPC

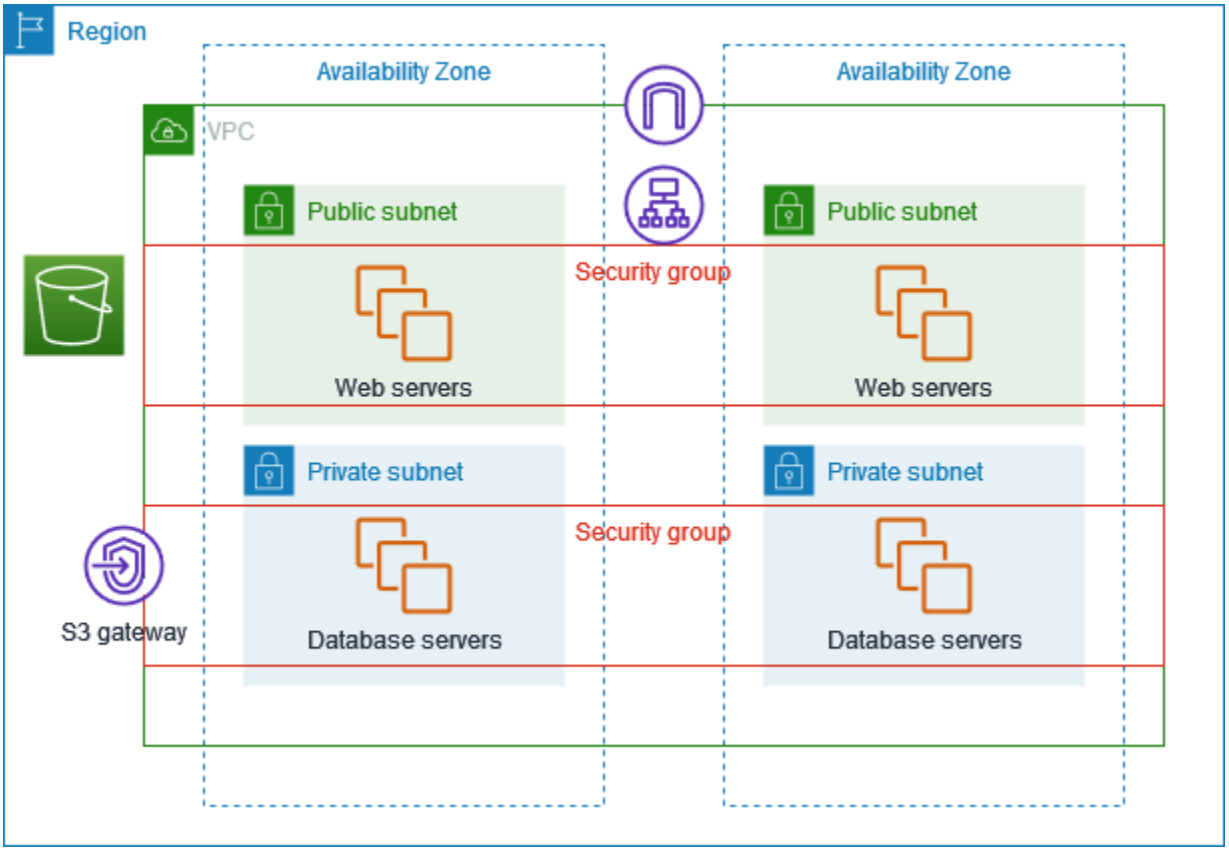
此範例示範如何建立 VPC，以便用於生產環境中的雙層架構。若要提升彈性，您可以在兩個可用區域中部署伺服器。

目錄

- 概要
- 1. 建立 VPC
- 2. 部署您的應用程式
- 3. 測試組態
- 4. 清除

概要

下圖提供此範例所包含的資源概觀。VPC 具有兩個可用區域中的公有子網路和私有子網路。Web 伺服器會在公有子網路中執行，並透過負載平衡器接收來自用戶端的流量。Web 伺服器的安全群組會允許來自負載平衡器的流量。資料庫伺服器會在私有子網路中執行，並從 Web 伺服器接收流量。資料庫伺服器的安全群組會允許來自 Web 伺服器的流量。資料庫伺服器可以使用閘道 VPC 端點連線至 Amazon S3。



路由

當您使用 Amazon VPC 主控台建立此 VPC 時，我們會為具有本機路由和網際網路閘道之路由的公有子網路建立路由表，並為具有本機路由和閘道 VPC 端點之路由的每個私有子網路建立路由表。

以下是具有 IPv4 和 IPv6 路由之公有子網路的路由表範例。如果您建立僅限 IPv4 的子網路 (而不是雙堆疊子網路)，則路由表只會有 IPv4 路由。

目標	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	*igw-id*
::/0	*igw-id*

以下是具有 IPv4 和 IPv6 本機路由之私有子網路的路由表範例。如果您建立了僅限 IPv4 的子網路，則路由表只會有 IPv4 路由。最後一個路由會將目的地 Amazon S3 的流量傳送至閘道 VPC 端點。

目標	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	本機
s3- #### ID	*S3 #####*

安全

對於此範例組態，您要為負載平衡器建立安全群組、為 Web 伺服器建立安全群組，並為資料庫伺服器建立安全群組。

負載平衡器

Application Load Balancer 或 Network Load Balancer 的安全群組必須允許負載平衡器接聽程式連接埠上用戶端的傳入流量。若要接受來自網際網路上任何位置的流量，請指定 0.0.0.0/0 作為來源。負載平衡器安全群組也必須允許執行個體接聽程式連接埠和運作狀態檢查連接埠上從負載平衡器到目標執行個體的傳出流量。

Web 伺服器

下列安全群組規則可讓 Web 伺服器接收來自負載平衡器的 HTTP 和 HTTPS 流量。您可以選擇允許 Web 伺服器從您的網路接收 SSH 或 RDP 流量。Web 伺服器可將 SQL 或 MySQL 流量傳送至您的資料庫伺服器。

來源	通訊協定	連接埠範圍	Description
########## ID	TCP	80	允許來自負載平衡器的傳入 HTTP 存取
########## ID	TCP	443	允許來自負載平衡器的傳入 HTTPS 存取
###### IPv4 ####	TCP	22	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 SSH 存取

來源	通訊協定	連接埠範圍	Description
###### IPv6 ####	TCP	22	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 SSH 存取
###### IPv4 ####	TCP	3389	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 RDP 存取
###### IPv6 ####	TCP	3389	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 RDP 存取

目標	通訊協定	連接埠範圍	Description
## Microsoft SQL Server ########## ID	TCP	1433	允許傳出 Microsoft SQL Server 存取資料庫伺服器。
## MySQL ######### # ID	TCP	3306	允許傳出 MySQL 存取資料庫伺服器。

資料庫伺服器

下列安全群組規則允許資料庫伺服器接收來自 Web 伺服器的讀取和寫入請求。

來源	通訊協定	連接埠範圍	評論
Web ######## ID	TCP	1433	允許來自 Web 伺服器的傳入 Microsoft SQL Server 存取
Web ######## ID	TCP	3306	允許來自 Web 伺服器的傳入 MySQL Server 存取

目標	通訊協定	連接埠範圍	評論
0.0.0.0/0	TCP	80	允許傳出 HTTP 透過 IPv4 存取網際網路
0.0.0.0/0	TCP	443	允許傳出 HTTPS 透過 IPv4 存取網際網路

如需 Amazon RDS 資料庫執行個體安全群組的詳細資訊，請參閱《Amazon RDS 使用者指南》中的透過安全群組控制存取權限。

1. 建立 VPC

使用下列程序建立在兩個可用區域具有公有子網路和私有子網路的 VPC。

若要建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在儀表板上，選擇建立 VPC。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 設定 VPC：
   a. 保持選取 自動產生名稱標籤 以建立 VPC 資源的「名稱」標籤，或將其清除以提供您自己的 VPC 資源「名稱」標籤。
   b. 對於 IPv4 CIDR 區塊，您可以保留預設建議，或者您也可以輸入應用程式或網路所需的 CIDR 區塊。如需詳細資訊，請參閱the section called “VPC CIDR 區塊”。
   c. (選用) 如果您的應用程式使用 IPv6 位址進行通訊，請選擇 IPv6 CIDR 區塊 > Amazon 提供的 IPv6 CIDR 區塊。
   d. 選擇租用選項。此選項會定義啟動至 VPC 的 EC2 執行個體，是否會在與其他 AWS 帳戶 共用的硬體上執行，或是在僅供您使用的硬體上執行。如果您選擇 VPC 的租用為 `Default`，則在此 VPC 中啟動的 EC2 執行個體將使用啟動執行個體時指定的租用屬性。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用定義參數啟動執行個體。如果您選擇 VPC 的租用為 `Dedicated`，則執行個體將會一律以硬體上之專用預留執行個體 (專供您使用) 的形式執行。
5. 設定子網路：

a. 對於可用區域數量，請選擇 2，以便在兩個可用區域中啟動執行個體，以提高彈性。
b. 針對公用子網路數量，選擇 2。
c. 在 Number of private subnet (私有子網路數量) 中，選擇 2。
d. 您可以保留子網路的預設 CIDR 區塊，或者您也可以展開 自訂子網路 CIDR 區塊 並輸入 CIDR 區塊。如需詳細資訊，請參閱the section called “子網路 CIDR 區塊”。

6. 若為 NAT 閘道，請保留預設值無。
7. 若為 VPC 端點，請保留預設值 S3 閘道。雖然沒有任何效果 (除非您存取 S3 儲存貯體)，但啟用此 VPC 端點無須支付任何費用。
8. 保持選取 DNS 選項中的兩個選項。因此，您的 Web 伺服器將收到與其公有 IP 地址對應的公有 DNS 主機名稱。
9. 選擇建立 VPC。

2. 部署您的應用程式

在理想的情況下，您已在開發或測試環境中完成 Web 伺服器和資料庫伺服器測試，並建立了用於在生產環境中部署應用程式的指令碼或映像。

您可以將 EC2 執行個體用於 Web 伺服器。您可透過各種不同方式部署 EC2 執行個體。例如：

- Amazon EC2 啟動執行個體精靈
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

若要提高可用性，您可以使用 Amazon EC2 Auto Scaling 在多個可用區域中部署伺服器，並維持應用程式所需的最低伺服器容量。

您可以使用 Elastic Load Balancing 來將流量平均分配至伺服器之間。您可以將負載平衡器連接至 Auto Scaling 群組。

您可以將 EC2 執行個體用於資料庫伺服器，或是我們的專用資料庫類型之一。如需詳細資訊，請參閱上的資料庫 AWS：如何選擇。

3. 測試組態

完成應用程式部署後，您可以對其進行測試。如果您的應用程式無法傳送或接收預期的流量，您可以使用 Reachability Analyzer 來協助您進行疑難排解。例如，Reachability Analyzer 可以識別路由表或安

全群組的組態問題。如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

4. 清除

此組態結束使用後即可刪除。您必須先終止執行個體並刪除負載平衡器，才能刪除 VPC。如需詳細資訊，請參閱the section called “刪除您的 VPC”。

範例：在私有子網路和 NAT 具有伺服器的 VPC

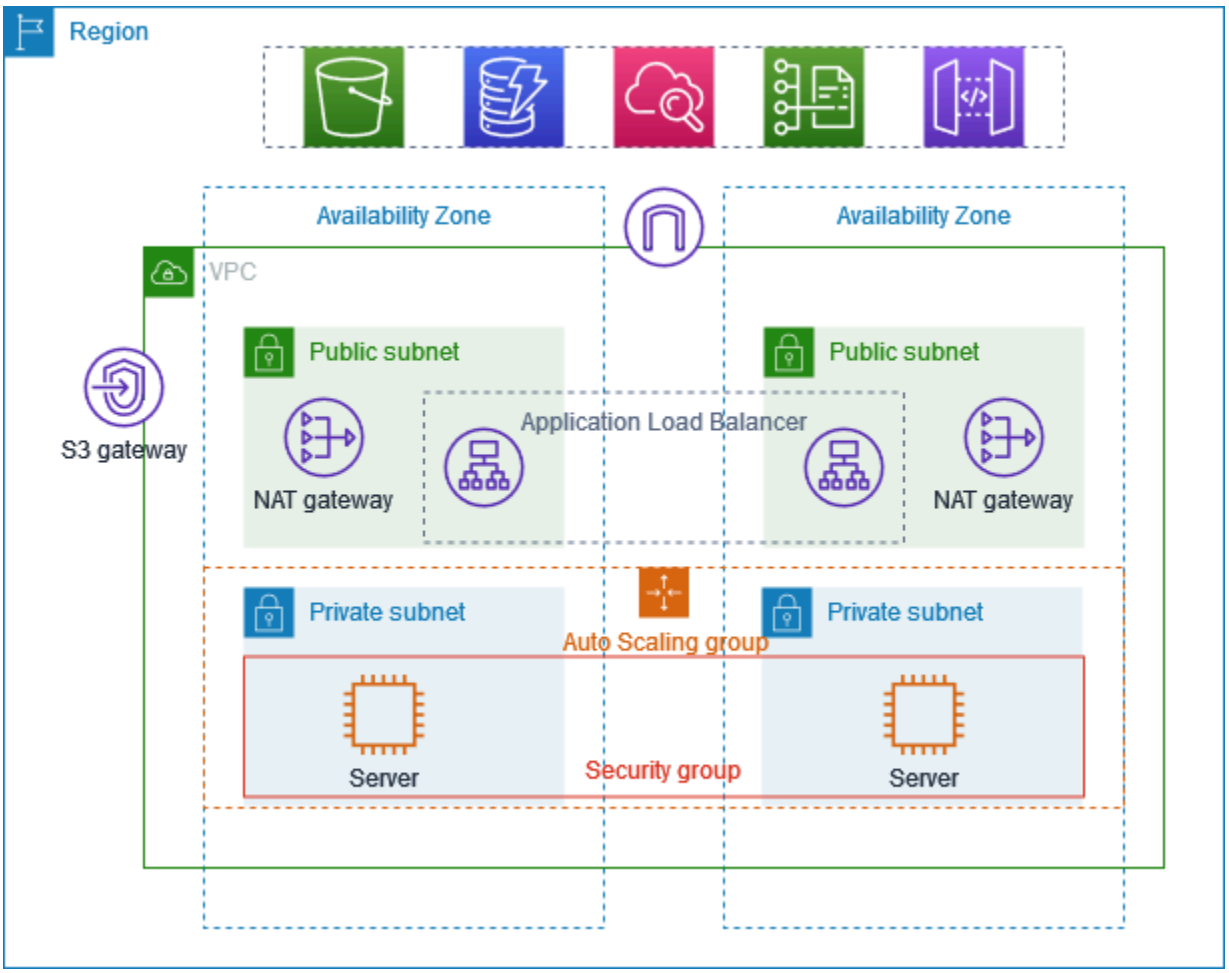
此範例示範如何建立 VPC，以便用於生產環境中的伺服器。若要提升彈性，您可以使用 Auto Scaling 群組和 Application Load Balancer，在兩個可用區域中部署伺服器。若要提高安全性，您可以在私有子網路中部署伺服器。伺服器會透過負載平衡器接收要求。伺服器可以使用 NAT 閘道連線至網際網路。若要提升彈性，您可以在兩個可用區域中部署 NAT 閘道。

目錄

- 概要
- 1. 建立 VPC
- 2. 部署您的應用程式
- 3. 測試組態
- 4. 清除

概要

下圖提供此範例所包含的資源概觀。VPC 具有兩個可用區域中的公有子網路和私有子網路。每個公有子網路都包含一個 NAT 閘道和一個負載平衡器節點。在私有子網路中執行的伺服器會使用 Auto Scaling 群組啟動和終止，並從負載平衡器接收流量。伺服器可以使用 NAT 閘道連線至網際網路。伺服器可以使用閘道 VPC 端點連線至 Amazon S3。



路由

當您使用 Amazon VPC 主控台建立此 VPC 時，我們會為具有本機路由和網際網路閘道之路由的公有子網路建立路由表。我們也會為具有本機路由以及 NAT 閘道、僅限輸出網際網路閘道和閘道 VPC 端點之路由的私有子網路建立路由表。

以下是具有 IPv4 和 IPv6 路由之公有子網路的路由表範例。如果您建立僅限 IPv4 的子網路 (而不是雙堆疊子網路)，則路由表只會包含 IPv4 路由。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	*igw-id*

目的地	目標
::/0	*igw-id*

以下是其中一個具有 IPv4 和 IPv6 路由之私有子網路的路由表範例。如果您建立了僅限 IPv4 的子網路，則路由表只會包含 IPv4 路由。最後一個路由會將目的地 Amazon S3 的流量傳送至閘道 VPC 端點。

目標	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
s3- #### ID	*S3 #####*

安全

以下是您可能為與伺服器相關聯之安全群組建立的規則範例。安全群組必須在接聽程式連接埠和通訊協定上允許來自負載平衡器的流量。它還必須允許運作狀態檢查流量。

來源	通訊協定	連接埠範圍	評論
########## ID	*########*	*#######*	在接聽程式連接埠上允許來自負載平衡器的所有傳入流量
########## ID	*##########*	*#########*	允許來自負載平衡器的傳入運作狀態檢查流量

1. 建立 VPC

使用下列程序建立在兩個可用區域具有公有子網路和私有子網路並在每個可用區域具有 NAT 閘道的 VPC。

若要建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在儀表板上，選擇建立 VPC。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 設定 VPC
   a. 針對自動產生名稱標籤，輸入 VPC 的名稱。
   b. 對於 IPv4 CIDR 區塊，您可以保留預設建議，或者您也可以輸入應用程式或網路所需的 CIDR 區塊。
   c. 如果您的應用程式使用 IPv6 地址進行通訊，請選擇 IPv6 CIDR 區塊 > Amazon 提供的 IPv6 CIDR 區塊。
5. 設定子網路
   a. 對於可用區域數量，請選擇 2，以便在多個可用區域中啟動執行個體，以提高彈性。
   b. 針對公用子網路數量，選擇 2。
   c. 在 Number of private subnet (私有子網路數量) 中，選擇 2。
   d. 您可以保留公有子網路的預設 CIDR 區塊，或者您也可以展開自訂子網路 CIDR 區塊並輸入 CIDR 區塊。如需詳細資訊，請參閱the section called “子網路 CIDR 區塊”。
6. 若為 NAT 閘道，請選擇每個 AZ 1 個以提高彈性。
7. 如果您的應用程式使用 IPv6 地址進行通訊，則針對輸出限定網際網路閘道，請選擇是。
8. 針對 VPC 端點，如果您的執行個體必須存取 S3 儲存貯體，請保留 S3 閘道預設值。否則，私有子網路中的執行個體將無法存取 Amazon S3。此選項無須支付任何費用，因此如果您未來可能使用 S3 儲存貯體，則可以保留預設值。如果您選擇無，您稍後可以隨時新增閘道 VPC 端點。
9. 對於 DNS 選項，請清除啟用 DNS 主機名稱。
10. 選擇建立 VPC。

2. 部署您的應用程式

在理想的情況下，您已在開發或測試環境中完成伺服器測試，並建立了用於在生產環境中部署應用程式的指令碼或映像。

您可以使用 Amazon EC2 Auto Scaling 在多個可用區域中部署伺服器，並維持應用程式所需的最低伺服器容量。

使用 Auto Scaling 群組啟動執行個體

1. 建立啟動範本，以指定使用 Amazon EC2 Auto Scaling 啟動 EC2 執行個體所需的組態資訊。如需逐步指示，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的建立 Auto Scaling 群組的啟動範本。
2. 建立 Auto Scaling 群組，該群組是具有最小、最大以及所需大小的 EC2 執行個體集合。如需逐步指示，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的使用啟動範本建立 Auto Scaling 群組。
3. 建立負載平衡器，以將流量平均分配在您 Auto Scaling 群組的各執行個體之間，然後將負載平衡器連接至 Auto Scaling 群組。如需詳細資訊，請參閱《Elastic Load Balancing 使用者指南》https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/以及《Amazon EC2 Auto Scaling 使用者指南》中的使用 Elastic Load Balancing。

3. 測試組態

完成應用程式部署後，您可以對其進行測試。如果您的應用程式無法傳送或接收預期的流量，您可以使用 Reachability Analyzer 來協助您進行疑難排解。例如，Reachability Analyzer 可以識別路由表或安全群組的組態問題。如需詳細資訊，請參閱 Reachability Analyzer Guide (《Reachability Analyzer 指南》)。

4. 清除

此組態結束使用後即可刪除。刪除 VPC 之前，您必須先刪除 Auto Scaling 群組、終止執行個體、刪除 NAT 閘道，以及刪除負載平衡器。如需詳細資訊，請參閱the section called “刪除您的 VPC”。

VPC 教學課程

Amazon Virtual Private Cloud (VPC) 是您在 AWS 中網路基礎結構的根基。雖然 AWS 管理主控台提供易於使用的介面，但 AWS 命令列介面 (CLI) 在建立與管理 VPC 資源面向具備更強的彈性與自動化能力。

本指南介紹兩種重要的 VPC 部署案例：

- 含公有子網路的基礎 VPC 設定，適用於簡單 Web 應用程式
- 採用 NAT 閘道且含私有與公有子網路的進階 VPC 組態，適用於多層級應用程式

透過如下教學課程，您將了解如何：

- 建立具有不同子網路組態的 VPC
- 設定網際網路與 NAT 閘道
- 設定路由表與安全群組
- 使用 AWS CLI 命令管理網路基礎結構
- 實作 AWS 網路最佳實務

接下來，我們就可以透過命令列開始建置 AWS 網路基礎結構。

教學課程

- 使用 CLI AWS 開始使用 Amazon VPC
- 透過 AWS CLI 建立包含私有子網路與 NAT 閘道的 VPC

使用 CLI AWS 開始使用 Amazon VPC

本教學課程將引導您使用 AWS 命令列界面 () 建立虛擬私有雲端 (VPC AWS CLI)。您將了解如何設定具備公有與私有子網路的 VPC、設定網際網路連線，以及部署 EC2 執行個體，來示範常見的 Web 應用程式架構。

先決條件

在開始本教學課程之前，請確認已滿足以下條件：

1. AWS CLI。若需安裝，請根據 AWS CLI 安裝指南進行操作。

2. AWS CLI 使用適當的登入資料設定您的 。若尚未設定憑證，請執行 `aws configure`。
3. 掌握聯網概念的基本知識。
4. Amazon VPC 的身分和存取管理 在 AWS 帳戶中建立和管理 VPC 資源。

成本考量

本教學課程會建立可能會在您的帳戶中產生成本 AWS 的資源。主要費用源自 NAT 閘道 (每小時 0.045 USD 外加資料處理費用) 與 EC2 執行個體 (t2.micro，每個執行個體每小時約 0.0116 USD)。若在一小時內完成本教學課程，隨後及時清理所有資源，總成本約為 0.07 USD。為最佳化開發環境的成本，建議使用 NAT 執行個體而非 NAT 閘道，因為這能大幅降低費用。

讓我們先確認您的 AWS CLI 已正確設定，再繼續。

```
aws configure list
```

您應該會看到您的 AWS 存取金鑰、私密金鑰和預設區域。另需驗證您擁有建立 VPC 資源所需的許可。

```
aws sts get-caller-identity
```

此命令會顯示 AWS 您的帳戶 ID、使用者 ID 和 ARN，確認您的登入資料有效。

建立 VPC

Virtual Private Cloud (VPC) 是專屬於您 AWS 帳戶的虛擬網路。在本節中，您將建立 CIDR 區塊為 10.0.0.0/16 的 VPC，最多可提供 65,536 個 IP 位址。

建立 VPC

以下命令會建立新的 VPC 並為其指派名稱標籤。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]'
```

記錄輸出中的 VPC ID。後續命令會用到該 ID。在本教學課程中，我們會將 "vpc-0123456789abcdef0" 用作範例 VPC ID。在所有命令中，將該 ID 取代為實際的 VPC ID。

啟用 DNS 支援與主機名稱

依預設，新 VPC 中會停用 DNS 解析與 DNS 主機名稱。啟用這些功能，允許 VPC 中的執行個體解析網域名稱。

```
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-support
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-hostnames
```

如果執行成功，這些命令不會產生輸出。您的 VPC 此時已啟用 DNS 支援與主機名稱解析。

建立子網路

子網路是 VPC IP 位址範圍的細分區段，可用於置放一組相互隔離的資源。在本節中，為實現高可用性，您需在兩個可用區域中建立公有與私有子網路。

取得可用的可用區域

首先，擷取所在區域中可用的可用區域。

```
aws ec2 describe-availability-zones
```

在本教學課程中，我們會使用前兩個可用區域。記錄輸出中的名稱 (例如 "us-east-1a" 與 "us-east-1b")。

建立公有子網路

公有子網路用於需要透過網際網路存取的資源，例如 Web 伺服器。

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ1}]'
```

記錄輸出中的子網路 ID。在本教學課程中，我們會將 "subnet-0123456789abcdef0" 用作第一個公有子網路的範例 ID。

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ2}]'
```

記錄輸出中的子網路 ID。在本教學課程中，我們會將 "subnet-0123456789abcdef1" 用作第二個公有子網路的範例 ID。

建立私有子網路

私有子網路用於不應直接透過網際網路存取的資源，例如資料庫。

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ1}]'
```

記錄輸出中的子網路 ID。在本教學課程中，我們會將 "subnet-0123456789abcdef2" 用作第一個私有子網路的範例 ID。

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ2}]'
```

記錄輸出中的子網路 ID。在本教學課程中，我們會將 "subnet-0123456789abcdef3" 用作第二個私有子網路的範例 ID。

此時已建立四個子網路：兩個公有子網路與兩個私有子網路，分佈在兩個可用區域中。

提示：規劃 CIDR 區塊時，確認這些區塊不會與現有的網路重疊。用於生產環境時，需配置足夠的 IP 位址因應未來擴展需求，同時保持子網路規模適中，兼顧安全與管理效率。

設定網際網路連線

若要允許 VPC 中的資源與網際網路通訊，需建立並連接網際網路閘道。在本節中，您需為 VPC 設定網際網路連線。

建立網際網路閘道

網際網路閘道可實現 VPC 與網際網路通訊。

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
```

記錄輸出中的網際網路閘道 ID。在本教學課程中，我們會將 "igw-0123456789abcdef0" 用作範例 ID。

將網際網路閘道連接至 VPC

建立網際網路閘道後，即可將其連接至 VPC。

```
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
```

建立與設定路由表

路由表包含規則 (路由)，可決定網路流量導向何處。首先，為公有子網路建立路由表。

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
```

記錄輸出中的路由表 ID。在本教學課程中，我們會將 "rtb-0123456789abcdef0" 用作公有路由表的範例 ID。

在公有路由表中新增通往網際網路閘道的路由。

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef0 --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-0123456789abcdef0
```

將公有子網路與公有路由表建立關聯。

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef0
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef1
```

現在，為私有子網路建立路由表。

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
```

記錄輸出中的路由表 ID。在本教學課程中，我們會將 "rtb-0123456789abcdef1" 用作私有路由表的範例 ID。

將私有子網路與私有路由表建立關聯。

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef2
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef3
```

建立 NAT 閘道

NAT 閘道允許私有子網路中的執行個體啟動前往網際網路的傳出流量，同時阻止來自網際網路的傳入流量。此機制對於需要下載更新或存取外部服務的執行個體至關重要。

配置彈性 IP

首先，為 NAT 閘道配置彈性 IP 位址。

```
aws ec2 allocate-address --domain vpc
```

記錄輸出中的配置 ID。在本教學課程中，我們會將 "eipalloc-0123456789abcdef0" 用作範例 ID。

建立 NAT 閘道

使用配置的彈性 IP，在您某一個公有子網路中建立 NAT 閘道。

```
aws ec2 create-nat-gateway \
  --subnet-id subnet-0123456789abcdef0 \
  --allocation-id eipalloc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]'
```

記錄輸出中的 NAT 閘道 ID。在本教學課程中，我們會將 "nat-0123456789abcdef0" 用作範例 ID。

等待 NAT 閘道變得可用，然後再繼續。

```
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-0123456789abcdef0
```

新增通往 NAT 閘道的路由

在私有路由表中新增通往 NAT 閘道的路由，允許私有子網路中的執行個體存取網際網路。

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef1 --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id nat-0123456789abcdef0
```

注意：若用於生產環境，建議在具備私有子網路的每個可用區域中建立 NAT 閘道，用以消除單點故障。

設定子網路

設定公有子網路，使之自動為於其中啟動的執行個體指派公有 IP 位址。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef0 --map-public-ip-
on-launch
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef1 --map-public-ip-
on-launch
```

此設定能確保在公有子網中啟動的執行個體預設取得公有 IP 位址，從而可透過網際網路存取這些執行個體。

建立安全群組

安全群組會作為執行個體的虛擬防火牆，控管傳入及傳出流量。在本節中，您需為 Web 伺服器與資料庫伺服器建立安全群組。

建立 Web 伺服器的安全群組

```
aws ec2 create-security-group \
  --group-name WebServerSG \
  --description "Security group for web servers" \
  --vpc-id vpc-0123456789abcdef0
```

記錄輸出中的安全群組 ID。在本教學課程中，我們會將 "sg-0123456789abcdef0" 用作 Web 伺服器安全群組的範例 ID。

允許 HTTP 與 HTTPS 流量傳送至您的 Web 伺服器。

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 80 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 443 --cidr 0.0.0.0/0
```

注意：若用於生產環境，應將傳入流量限制於特定 IP 範圍，而不是允許來自 0.0.0.0/0 (任何 IP 位址) 的流量。

建立資料庫伺服器的安全群組

```
aws ec2 create-security-group \
  --group-name DBServerSG \
  --description "Security group for database servers" \
  --vpc-id vpc-0123456789abcdef0
```

記錄輸出中的安全群組 ID。在本教學課程中，我們會將 "sg-0123456789abcdef1" 用作資料庫伺服器安全群組的範例 ID。

僅允許來自 Web 伺服器的 MySQL/Aurora 流量。

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef1 --protocol tcp
 --port 3306 --source-group sg-0123456789abcdef0
```

這項設定遵循最低權限原則，確保僅 Web 伺服器安全群組中的執行個體，能透過 3306 連接埠存取您的資料庫伺服器。

驗證 VPC 組態

建立所有必要元件之後，請驗證 VPC 組態，確保所有設定均正確完成。

檢查 VPC

```
aws ec2 describe-vpcs --vpc-id vpc-0123456789abcdef0
```

檢查子網路

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

檢查路由表

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

檢查網際網路閘道

```
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-
id,Values=vpc-0123456789abcdef0"
```

檢 NAT 閘道

```
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

檢查安全群組

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

這些命令提供有關 VPC 每個元件的詳細資訊，便於您驗證所有設定是否均正確完成。

部署 EC2 執行個體

此時您已建立 VPC 基礎結構，接著可以部署 EC2 執行個體來示範架構的運作方式。您需在公有子網路中啟動 Web 伺服器，並在私有子網路中啟動資料庫伺服器。

建立用於 SSH 存取的金鑰對

首先，建立金鑰對，用於安全地連線至執行個體：

```
aws ec2 create-key-pair --key-name vpc-tutorial-key --query 'KeyMaterial' --output text
 > vpc-tutorial-key.pem
chmod 400 vpc-tutorial-key.pem
```

此命令會建立新的金鑰對，並將私有金鑰儲存至具備受限許可的檔案。

尋找最新的 Amazon Linux 2 AMI

尋找要用於執行個體的最新 Amazon Linux 2 AMI：

```
aws ec2 describe-images --owners amazon \
  --filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2" "Name=state,Values=available"
 \
  --query "sort_by(Images, &CreationDate)[-1].ImageId" --output text
```

記錄輸出中的 AMI ID。在本教學課程中，我們會將 "ami-0123456789abcdef0" 用作範例 ID。

在公有子網路中啟動 Web 伺服器

現在，在公有子網路中啟動 EC2 執行個體作為 Web 伺服器：

```
aws ec2 run-instances \
```

```
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef0 \
  --subnet-id subnet-0123456789abcdef0 \
  --associate-public-ip-address \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y httpd
               systemctl start httpd
               systemctl enable httpd
               echo "<h1>Hello from $(hostname -f)</h1>" > /var/www/html/index.html' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]'
```

記錄輸出中的執行個體 ID。在本教學課程中，我們會將 "i-0123456789abcdef0" 用作 Web 伺服器執行個體的範例 ID。

在私有子網路中啟動資料庫伺服器

接著，在私有子網路中啟動 EC2 執行個體作為資料庫伺服器：

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef1 \
  --subnet-id subnet-0123456789abcdef2 \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y mariadb-server
               systemctl start mariadb
               systemctl enable mariadb' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]'
```

記錄輸出中的執行個體 ID。在本教學課程中，我們會將 "i-0123456789abcdef1" 用作資料庫伺服器執行個體的範例 ID。

存取 Web 伺服器

Web 伺服器執行個體執行後，您可透過其公有 IP 位址對其進行存取：

```
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef0 \
  --query 'Reservations[0].Instances[0].PublicIpAddress' \
  --output text
```

此命令會輸出 Web 伺服器的公有 IP 位址。在本教學課程中，我們會將 "203.0.113.10" 用作範例 ID。

您現在可於 Web 瀏覽器中開啟此 URL：http://203.0.113.10

透過 SSH 連線至執行個體

若要連線至 Web 伺服器：

```
ssh -i vpc-tutorial-key.pem ec2-user@203.0.113.10
```

若要連線至資料庫伺服器，必須透過 SSH 連線至 Web 伺服器，再轉接至資料庫伺服器：

```
# Get the private IP of the database server
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef1 \
  --query 'Reservations[0].Instances[0].PrivateIpAddress' \
  --output text
```

此命令會輸出資料庫伺服器的私有 IP 位址。在本教學課程中，我們會將 "10.0.2.10" 用作範例 ID。

```
# First SSH to web server, then to database server
ssh -i vpc-tutorial-key.pem -A ec2-user@203.0.113.10
ssh ec2-user@10.0.2.10
```

這會示範您建立的網路架構：Web 伺服器可從公網存取，而資料庫伺服器僅能透過 VPC 內部網路連線。

疑難排解

以下是在建立 VPC 時可能遇到的部分常見問題，以及解決這些問題的實用方法：

CIDR 區塊重疊

若收到有關 CIDR 區塊重疊的錯誤，確認 VPC 及子網路的 CIDR 區塊未與帳戶中現有的 VPC 或子網路重疊。

許可錯誤

如遇許可錯誤，確認 IAM 使用者或角色具有建立與管理 VPC 資源所需的許可。您可能需要連接 AmazonVPCFullAccess 政策或建立具備必要許可的自訂政策。

資源限制

AWS 帳戶對您可以建立VPCs、子網路和其他資源數量有預設限制。如果您達到這些限制，您可以透過 AWS 支援中心請求提高。

清理期間相依性失敗

清理資源時，若以錯誤順序刪除資源，可能遭遇相依性錯誤。一律依照與建立過程相反的順序刪除資源，從依賴性最高的項目開始刪除。

清除資源

使用完 VPC 後，即可清理資源，避免產生費用。為正確處理相依性關係，依照與建立過程相反的順序刪除資源。

終止 EC2 執行個體

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
aws ec2 wait instance-terminated --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

刪除金鑰對

```
aws ec2 delete-key-pair --key-name vpc-tutorial-key
rm vpc-tutorial-key.pem
```

刪除 NAT 閘道

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-0123456789abcdef0
aws ec2 wait nat-gateway-deleted --nat-gateway-ids nat-0123456789abcdef0
```

釋放彈性 IP

```
aws ec2 release-address --allocation-id eipalloc-0123456789abcdef0
```

刪除安全群組

```
aws ec2 delete-security-group --group-id sg-0123456789abcdef1
aws ec2 delete-security-group --group-id sg-0123456789abcdef0
```

刪除路由表

首先，查詢路由表關聯 ID：

```
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef0
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef1
```

接著，取消路由表與子網路的關聯 (將關聯 ID 取代為輸出中的關聯 ID)：

```
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef0
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef1
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef2
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef3
```

然後，刪除路由表：

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef1
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef0
```

分離與刪除網際網路閘道

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0
```

刪除子網路

```
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef0
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef1
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef2
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef3
```

刪除 VPC

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0
```

生產環境部署須知

本教學課程旨在協助您了解如何透過 AWS CLI建立 VPC。若用於生產環境，建議遵循下列安全與架構最佳實務：

1. 安全群組規則：將傳入流量限制於特定 IP 範圍，而不是允許來自 0.0.0.0/0 的流量。
2. 高可用性：在具備私有子網路的每個可用區域中部署 NAT 閘道，用以消除單點故障。
3. 網路 ACL：實作網路 ACL，作為安全群組之外的額外安全層。
4. VPC 流量日誌：啟用 VPC 流量日誌功能，用以監控與分析網路流量模式。
5. 資源標記：實作完善的標記策略，提升資源管理效率。

如需有關建置生產就緒架構的詳細資訊，請參閱《AWS Well-Architected Framework》與《AWS 安全最佳實務》。

後續步驟

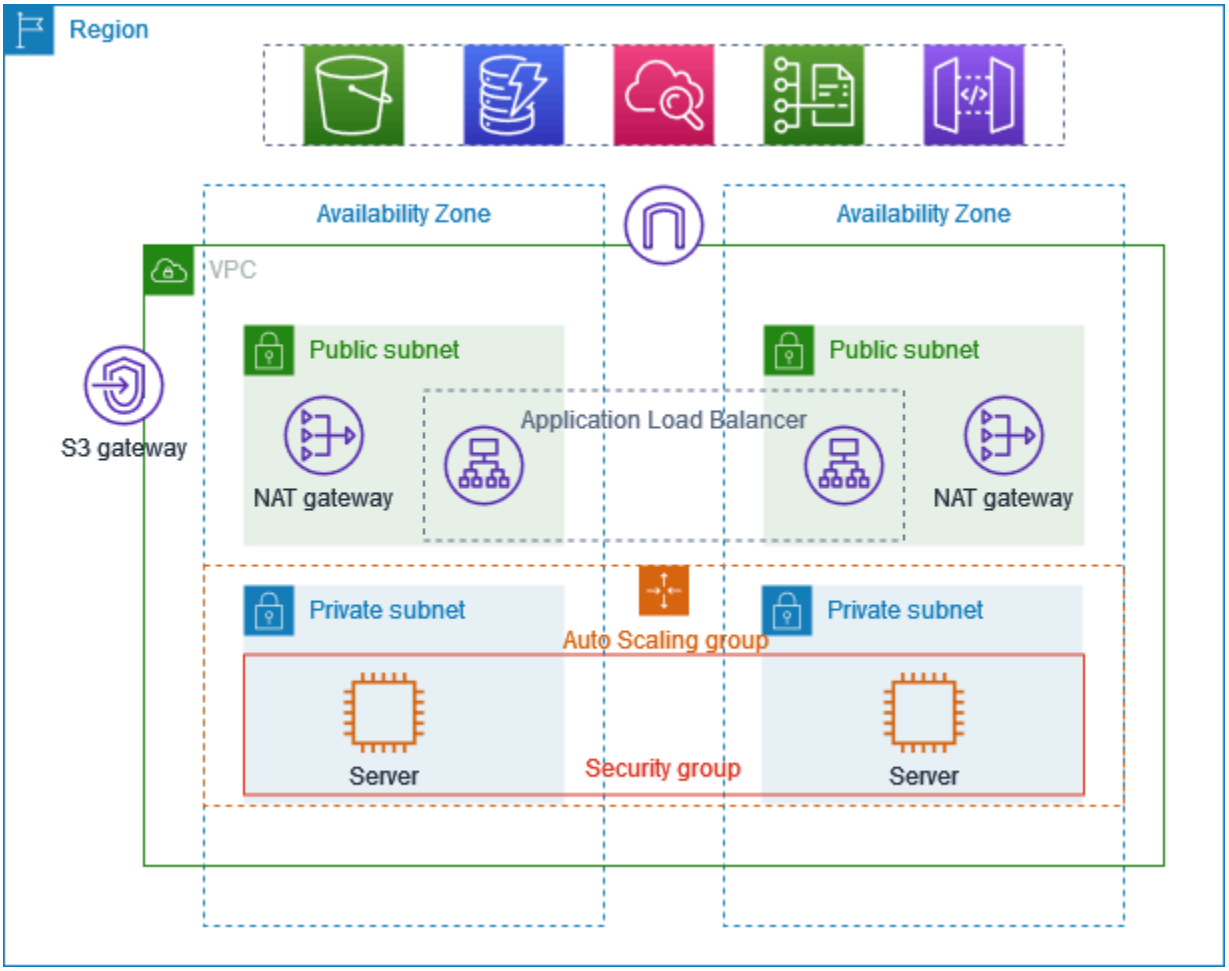
此時已建立具備公有與私有子網路的 VPC，接下來可以執行以下操作：

1. 在公有或私有子網路中啟動 EC2 執行個體。
2. 部署負載平衡器，將流量分散至多個執行個體。
3. 設定 Auto Scaling 群組，實現高可用性與可擴展性。
4. 在私有子網路中設定 RDS 資料庫。
5. 實作 VPC 對等互連，實現與其他 VPC 的連線。
6. 設定 VPN 連線，將 VPC 連線至內部部署網路。

透過 AWS CLI 建立包含私有子網路與 NAT 閘道的 VPC

此教學課程會示範如何透過 AWS CLI 建立專為生產環境伺服器設計的 VPC。為了提高彈性，您將使用 Auto Scaling 群組與 Application Load Balancer，在兩個可用區域中部署伺服器。為了提高安全性，您將在私有子網路中部署伺服器。伺服器會透過負載平衡器接收請求，並可藉由 NAT 閘道連線至網際網路。為了提高彈性，您將在每個可用區域中部署 NAT 閘道。

下圖提供此教學課程所包含的資源概觀。VPC 具有兩個可用區域中的公有子網路和私有子網路。每個公有子網路都包含一個 NAT 閘道和一個負載平衡器節點。在私有子網路中執行的伺服器會使用 Auto Scaling 群組啟動和終止，並從負載平衡器接收流量。伺服器可以使用 NAT 閘道連線至網際網路。伺服器可以使用閘道 VPC 端點連線至 Amazon S3。



必要條件

在開始本教學課程之前，需要滿足以下條件：

- 已安裝並設定 AWS CLI，且其具備建立 VPC 資源、EC2 執行個體、負載平衡器與 Auto Scaling 群組的許可。如需安裝 AWS CLI 的相關資訊，請參閱安裝或更新 AWS CLI 的最新版本。
- 掌握 VPC 概念的基本知識，包括子網路、路由表與網際網路閘道。
- 已安裝 `jq` 命令列 JSON 處理器。此工具用於剖析 AWS CLI 命令的輸出結果。如需有關安裝 jq 的資訊，請參閱 Download jq。
- 所建立資源需具備足夠的服務配額，包括：
- 至少 2 個可用的彈性 IP 位址
- 至少 2 個 NAT 閘道
- 至少 1 個 VPC
- 至少 4 個子網路

- 至少 1 個 Application Load Balancer

預估成本：在本教學課程中建立的資源會在您的 AWS 帳戶中產生費用：NAT 閘道：每小時約 0.045 USD，外加資料處理費用 彈性 IP 位址：與執行中的執行個體相關聯時免費，無關聯時每小時約 0.005 USD EC2 執行個體：因執行個體類型而異 (本教學課程中使用的是 t3.micro) Application Load Balancer：每小時約 0.0225 USD，外加資料處理費用

建立 VPC 與子網路

首先，您將建立 CIDR 區塊為 10.0.0.0/16 的 VPC，最多可提供 65,536 個私有 IP 位址。

```
# Create a VPC with CIDR block 10.0.0.0/16
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC}]'
```

此命令會傳回類似以下的輸出：

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-abcd1234",
        "State": "pending",
        "VpcId": "vpc-abcd1234",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-abcd1234",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "ProductionVPC"
            }
        ]
```

```
    }
}
```

記錄輸出中的 VPC ID (例如 vpc-abcd1234)。後續命令中會用到此 ID。

接下來，您需在所在區域中選定兩個可用區域，用以建立具韌性的架構。

```
# Get available Availability Zones
aws ec2 describe-availability-zones --query 'AvailabilityZones[0:2].ZoneName' --output
 text
```

此命令會傳回類似以下的輸出：

```
us-east-1a us-east-1b
```

現在，建立四個子網路：兩個公有子網路分別用於負載平衡器與 NAT 閘道，兩個私有子網路用於應用程式伺服器。將vpc-abcd1234 取代為實際的 VPC ID，將 us-east-1a 與 us-east-1b 取代為實際的可用區域。

```
# Create public subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1}]'

# Create private subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1}]'

# Create public subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2}]'

# Create private subnet in second AZ
aws ec2 create-subnet \
```

```
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2}]'
```

每個命令皆會傳回包含子網路 ID 的輸出結果。記錄這些 ID，供後續命令使用：

- 公有子網路 1：subnet-abcd1234
- 私有子網路 1：subnet-abcd5678
- 公有子網路 2：subnet-efgh1234
- 私有子網路 2：subnet-efgh5678

建立與設定網際網路連線

在本節中，您將建立網際網路閘道 (用於實現 VPC 與網際網路的通訊)，並將其連接至 VPC。

```
# Create an Internet Gateway
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=ProductionIGW}]'
```

命令會傳回包含網際網路閘道 ID 的輸出結果。記錄此 ID (例如 igw-abcd1234)。

將網際網路閘道連接至 VPC。將 igw-abcd1234 取代為實際的網際網路閘道 ID，將 vpc-abcd1234 取代為實際的 VPC ID。

```
# Attach the Internet Gateway to the VPC
aws ec2 attach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234
```

接著，為公有與私有子網路建立路由表。將 vpc-abcd1234 取代為實際的 VPC ID。

```
# Create a route table for public subnets
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable}]'

# Create route table for private subnet in first AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1}]'

# Create route table for private subnet in second AZ
```

```
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2}]'
```

每個命令皆會傳回包含路由表 ID 的輸出結果。記錄這些 ID：

- 公有路由表：rtb-abcd1234
- 私有路由表 1：rtb-efgh1234
- 私有路由表 2：rtb-ijkl1234

在公有路由表中新增通往網際網路閘道的路由，用以啟用網際網路存取功能。將 rtb-abcd1234 取代為實際的公有路由表 ID，將 igw-abcd1234 取代為實際的網際網路閘道 ID。

```
# Add a route to the Internet Gateway
aws ec2 create-route --route-table-id rtb-abcd1234 --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-abcd1234
```

將子網路與對應的路由表建立關聯。將路由表 ID 與子網路 ID 取代為實際的 ID。

```
# Associate public subnets with the public route table
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-abcd1234
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-efgh1234

# Associate private subnets with their respective route tables
aws ec2 associate-route-table --route-table-id rtb-efgh1234 --subnet-id subnet-abcd5678
aws ec2 associate-route-table --route-table-id rtb-ijkl1234 --subnet-id subnet-efgh5678
```

建立 NAT 閘道

NAT 閘道允許私有子網路中的執行個體連線至網際網路或其他 AWS 服務，但會阻止網際網路啟動與這些執行個體的連線。首先，為 NAT 閘道配置彈性 IP 位址。

```
# Allocate Elastic IP for NAT Gateway in first AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT1-EIP}]'

# Allocate Elastic IP for NAT Gateway in second AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT2-EIP}]'
```

每個命令皆會傳回包含配置 ID 的輸出結果。記錄這些 ID：

- EIP 1 配置 ID：eipalloc-abcd1234
- EIP 2 配置 ID：eipalloc-efgh1234

在每個公有子網路中建立 NAT 閘道。將子網路 ID 與配置 ID 取代為實際的 ID。

```
# Create NAT Gateway in public subnet of first AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-abcd1234 \
  --allocation-id eipalloc-abcd1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1}]'

# Create NAT Gateway in public subnet of second AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-efgh1234 \
  --allocation-id eipalloc-efgh1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2}]'
```

每個命令皆會傳回包含 NAT 閘道 ID 的輸出結果。記錄這些 ID：

- NAT 閘道 1：nat-abcd1234
- NAT 閘道 2：nat-efgh1234

NAT 閘道需要幾分鐘的時間完成佈建。等待這些閘道可用後再繼續操作。將 NAT 閘道 ID 取代為實際的 ID。

```
# Wait for NAT Gateways to be available
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-abcd1234
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-efgh1234
```

在私有路由表中新增通往 NAT 閘道的路由，用以啟用私有子網路中執行個體的網際網路存取功能。將路由表 ID 與 NAT 閘道 ID 取代為實際的 ID。

```
# Add route to NAT Gateway 1 in private route table 1
aws ec2 create-route \
  --route-table-id rtb-efgh1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-abcd1234

# Add route to NAT Gateway 2 in private route table 2
aws ec2 create-route \
```

```
  --route-table-id rtb-ijkl1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-efgh1234
```

建立 Amazon S3 的 VPC 端點

Amazon S3 的 VPC 端點能讓私有子網路中的執行個體無需經過 NAT 閘道即可存取 S3，既可降低資料傳輸成本，又能提升網路效能。將 vpc-abcd1234 取代為實際的 VPC ID，將路由表 ID 取代為實際的 ID。

```
# Get the prefix list ID for S3 in your region
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.$(aws configure get region).s3" --query
 'PrefixLists[0].PrefixListId' --output text)

# Create the VPC endpoint for S3
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-abcd1234 \
  --service-name com.amazonaws.$(aws configure get region).s3 \
  --route-table-ids rtb-efgh1234 rtb-ijkl1234 \
  --tag-specifications 'ResourceType=vpc-endpoint,Tags=[{Key=Name,Value=S3-Endpoint}]'
```

命令會傳回包含 VPC 端點 ID 的輸出結果。記錄此 ID (例如 vpce-abcd1234)。

設定安全群組

安全群組會作為執行個體的虛擬防火牆，控管傳入及傳出流量。為負載平衡器建立安全群組，允許任意來源的 HTTP 傳入流量。將 vpc-abcd1234 取代為實際的 VPC ID。

```
# Create security group for the load balancer
aws ec2 create-security-group \
  --group-name LoadBalancerSG \
  --description "Security group for the load balancer" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=LoadBalancerSG}]'
```

命令會傳回包含安全群組 ID 的輸出結果。記錄此 ID (例如 sg-abcd1234)。

允許傳送至負載平衡器的 HTTP 傳入流量。將 sg-abcd1234 取代為實際的負載平衡器安全群組 ID。

```
# Allow inbound HTTP traffic from anywhere
```

```
aws ec2 authorize-security-group-ingress \
  --group-id sg-abcd1234 \
  --protocol tcp \
  --port 80 \
  --cidr 0.0.0.0/0
```

為應用程式伺服器建立安全群組，僅允許來自負載平衡器的傳入流量。將 vpc-abcd1234 取代為實際的 VPC ID。

```
# Create security group for the application servers
aws ec2 create-security-group \
  --group-name AppServerSG \
  --description "Security group for the application servers" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=AppServerSG}]'
```

命令會傳回包含安全群組 ID 的輸出結果。記錄此 ID (例如 sg-efgh1234)。

允許來自負載平衡器安全群組的 HTTP 傳入流量傳送至應用程式伺服器。將 sg-efgh1234 取代為實際的應用程式伺服器安全群組 ID，將 sg-abcd1234 取代為實際的負載平衡器安全群組 ID。

```
# Allow inbound HTTP traffic from the load balancer security group
aws ec2 authorize-security-group-ingress \
  --group-id sg-efgh1234 \
  --protocol tcp \
  --port 80 \
  --source-group sg-abcd1234
```

建立 EC2 執行個體的啟動範本

啟動範本包含用於啟動執行個體的組態資訊，例如 AMI ID、執行個體類型與安全群組。首先，建立一個將在執行個體啟動時執行的使用者資料指令碼。

```
cat > user-data.sh << 'EOF'
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello from $(hostname -f) in $(curl -s http://169.254.169.254/latest/meta-
data/placement/availability-zone)</h1>" > /var/www/html/index.html
```

```
EOF
```

將使用者資料指令碼編碼為 base64 格式。

```
USER_DATA=$(base64 -w 0 user-data.sh)
```

取得最新的 Amazon Linux 2 AMI ID。

```
# Get the latest Amazon Linux 2 AMI ID
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-
*-x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images, &CreationDate)
[-1].ImageId' --output text
```

建立包含 AMI ID、執行個體類型、安全群組與使用者資料的啟動範本。將 sg-efgh1234 取代為實際的應用程式伺服器安全群組 ID，將 $AMI_ID 和 $USER_DATA 取代為從先前命令取得的值。

```
# Create a launch template
aws ec2 create-launch-template \
  --launch-template-name AppServerTemplate \
  --version-description "Initial version" \
  --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=Name,Value=AppServerTemplate}]' \
  --launch-template-data '{
    "NetworkInterfaces": [{
      "DeviceIndex": 0,
      "Groups": ["sg-efgh1234"],
      "DeleteOnTermination": true
    }],
    "ImageId": "ami-abcd1234",
    "InstanceType": "t3.micro",
    "UserData":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQp5dW0gaW5zdGFsbCAteSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
+SGVsbG8gZnJvbSAkKGhvc3RuYW1lIC1mKSBpbiAkKGN1cmwgLXMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXRlc3QvbW
    "TagSpecifications": [{
      "ResourceType": "instance",
      "Tags": [{
        "Key": "Name",
        "Value": "AppServer"
      }]
    }]
  }'
```

建立負載平衡器與目標群組

目標群組會依據您指定的通訊協定與連接埠號碼，將請求路由至一或多個已註冊的目標，例如 EC2 執行個體。為應用程式伺服器建立目標群組。將 vpc-abcd1234 取代為實際的 VPC ID。

```
# Create a target group
aws elbv2 create-target-group \
  --name AppTargetGroup \
  --protocol HTTP \
  --port 80 \
  --vpc-id vpc-abcd1234 \
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path / \
  --health-check-port traffic-port
```

命令會傳回包含目標群組 ARN 的輸出結果。記錄此 ARN (例如 arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/AppTargetGroup/abcd1234)。

在公有子網路中建立 Application Load Balancer。將子網路 ID 與安全群組 ID 取代為實際值。

```
# Create a load balancer
aws elbv2 create-load-balancer \
  --name AppLoadBalancer \
  --subnets subnet-abcd1234 subnet-efgh1234 \
  --security-groups sg-abcd1234 \
  --tags Key=Name,Value=AppLoadBalancer
```

命令會傳回包含負載平衡器 ARN 的輸出結果。記錄此 ARN (例如 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234)。

等待負載平衡器處於作用中狀態後再繼續操作。將 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 取代為負載平衡器 ARN。

```
# Wait for load balancer to be active
aws elbv2 wait load-balancer-available \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234
```

為負載平衡器建立接聽程式，其可將 HTTP 流量轉送至目標群組。將負載平衡器 ARN 與目標群組 ARN 取代為實際的 ARN。

```
# Create a listener
aws elbv2 create-listener \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234 \
  --protocol HTTP \
  --port 80 \
  --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/AppTargetGroup/abcd1234
```

建立 Auto Scaling 群組

Auto Scaling 群組包含一群 EC2 執行個體，該群就自動擴展和管理目的而言被視為一個邏輯分組。建立 Auto Scaling 群組，其可使用啟動範本並將執行個體部署於私有子網路。將子網路 ID 與目標群組 ARN 取代為實際的 ID 與 ARN。

```
# Create an Auto Scaling group
aws autoscaling create-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --launch-template LaunchTemplateName=AppServerTemplate,Version='$Latest' \
  --min-size 2 \
  --max-size 4 \
  --desired-capacity 2 \
  --vpc-zone-identifier "subnet-abcd5678,subnet-efgh5678" \
  --target-group-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234 \
  --health-check-type ELB \
  --health-check-grace-period 300 \
  --tags Key=Name,Value=AppServer,PropagateAtLaunch=true
```

測試組態

Auto Scaling 群組啟動執行個體且這些執行個體通過運作狀態檢查後，即可測試負載平衡器。取得負載平衡器的 DNS 名稱。將負載平衡器 ARN 取代為實際的 ARN。

```
# Get the DNS name of the load balancer
aws elbv2 describe-load-balancers \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 \
```

```
  --query "LoadBalancers[0].DNSName" \
  --output text
```

使用 curl 透過負載平衡器名稱來測試應用程式。

```
curl http://LoadBalancerName
```

如果多次重新整理頁面，您應該會看到不同可用區域中不同執行個體的回應。

清除資源

完成本教學課程後，您應刪除所有資源，避免產生費用。將所有 ID 取代為實際的資源 ID。

```
# Delete the Auto Scaling group
aws autoscaling delete-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --force-delete

# Wait for the Auto Scaling group to be deleted
sleep 60

# Delete the load balancer
aws elbv2 delete-load-balancer \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234

# Wait for the load balancer to be deleted
sleep 30

# Delete the target group
aws elbv2 delete-target-group \
  --target-group-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234

# Delete the launch template
aws ec2 delete-launch-template \
  --launch-template-name AppServerTemplate

# Delete the NAT Gateways
aws ec2 delete-nat-gateway --nat-gateway-id nat-abcd1234
aws ec2 delete-nat-gateway --nat-gateway-id nat-efgh1234

# Wait for the NAT Gateways to be deleted
```

```
sleep 90

# Release the Elastic IPs
aws ec2 release-address --allocation-id eipalloc-abcd1234
aws ec2 release-address --allocation-id eipalloc-efgh1234

# Delete the VPC endpoint
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-abcd1234

# Wait for security group dependencies to clear
sleep 30

# Delete the security groups
aws ec2 delete-security-group --group-id sg-efgh1234
aws ec2 delete-security-group --group-id sg-abcd1234

# Detach the Internet Gateway
aws ec2 detach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234

# Delete the Internet Gateway
aws ec2 delete-internet-gateway --internet-gateway-id igw-abcd1234

# Delete the route tables
aws ec2 delete-route-table --route-table-id rtb-efgh1234
aws ec2 delete-route-table --route-table-id rtb-ijkl1234
aws ec2 delete-route-table --route-table-id rtb-abcd1234

# Delete the subnets
aws ec2 delete-subnet --subnet-id subnet-abcd1234
aws ec2 delete-subnet --subnet-id subnet-efgh1234
aws ec2 delete-subnet --subnet-id subnet-abcd5678
aws ec2 delete-subnet --subnet-id subnet-efgh5678

# Delete the VPC
aws ec2 delete-vpc --vpc-id vpc-abcd1234
```

後續步驟

現在您已建立包含私有子網路與 NAT 閘道的 VPC，接下來可以參閱下列相關主題：

- VPC 的安全最佳實務
- 使用 VPC 流量日誌來記錄 IP 流量

- Auto Scaling 群組擴缩政策
- 負載平衡器目標群組運作狀態檢查

Amazon VPC 配額

下表列出您 AWS 帳戶的 Amazon VPC 資源配額，先前稱為限制。除非另有指示，否則以每一區域指定這些配額。

如果您請求提高每項資源適用的配額，我們會增加該區域中所有資源的配額。

VPC 和子網路

名稱	預設	可調整	說明
每個區域的 VPC 數	5	是	提高此配額會以相同的數量提高每個區域的網際網路閘道配額。 您可增加此限制，讓每個區域擁有數百個 VPC。
每個 VPC 的子網路數	200	是	
每個 VPC 的 IPv4 CIDR 區塊數	5	是 (最多 50 個)	此主要 CIDR 區塊及所有輔助 CIDR 區塊合計趨近此配額。
每個 VPC 的 IPv6 CIDR 區塊數	5	是 (最多 50 個)	您可以配置到單一 VPC 的 CIDR 數量。
每個區域每個帳戶的 VPC 封鎖公開存取排除	50	是。若要請求提高配額，請參閱《AWS Support 使用者指南》中的請求提高服務配額。	您可以在帳戶中建立的 VPC BPA 排除數量。

DNS

每個 EC2 執行個體會將每個網路介面每秒 1024 個封包傳送至 Route 53 Resolver (亦即 .2 地址，例如 10.0.0.2 和 169.254.169.253)。此配額無法增加。依據查詢類型、回應大小以及使用的通訊協定而

異，Route 53 Resolver 支援的每秒 DNS 查詢數目也不同。如需詳細資訊和可擴展的 DNS 架構建議，請參閱《AWS 混合 DNS 與 Active Directory 技術指南》。

彈性 IP 位址

名稱	預設	可調整	說明
每個區域的彈性 IP 地址數	5	是	此配額適用於個別 AWS 帳戶 VPCs和共用 VPCs。
每個公有 NAT 閘道的彈性 IP 地址	2	是	您可以請求增加最多 8 個配額。

閘道

名稱	預設	可調整	說明
每個區域的輸出限定網際網路閘道數	5	是	若要增加此配額，請增加每個區域的 VPC 配額。 您一次只能連接一個輸出限定網際網路閘道至 VPC。
每個區域的網際網路閘道數	5	是	若要增加此配額，請增加每個區域的 VPC 配額。 您一次只能連接一個網際網路閘道至 VPC。
每個可用區域的 NAT 閘道數	5	是	`pending`、`active` 和 `deleting` 狀態中的 NAT 閘道只會計入您的配額。
每個 NAT 閘道的私有 IP 地址配額	8	是	
每個 VPC 的電信業者閘道	1	否	

由客戶管理之前綴清單

雖然由客戶管理之前綴清單的預設配額可調整，但您無法使用 Service Quotas 主控台來請求提高。您必須提交支援請求。請參閱《AWS Support 使用者指南》中的請求提高服務配額。

名稱	預設	可調整	說明
每個區域的字首清單	100	是	
每個字首清單的版本數目	1,000	是	如果字首清單有 1,000 個儲存版本而且您要新增新版本，會移除最舊的版本，以便新增新版本。
每個前綴清單的項目數目上限	1,000	是	您可以將客戶管理的字首清單調整大小，最多可調整 1000 個。如需詳細資訊，請參閱調整字首清單大小。當您在資源中參考字首清單時，字首清單的項目數上限會計入資源項目數的配額。例如，如果您建立最多包含 20 個項目的字首清單，而您在安全群組規則中參考該字首清單，這就會計為該安全群組的 20 個規則。
每個資源類型的字首清單的參照	10,000	是	此配額適用於每個可參考字首清單的資源類型。例如，您可以在所有安全群組中有 10，000 個字首清單的參考，以及在所有子網路路由表中有 10，000 個字首清單的參考。如果您與其他 AWS 帳戶共用字首清單，其他帳戶的字首清單參考會計入您的配額。

網路 ACL

名稱	預設	可調整	說明
每個 VPC 的網路 ACL 數	200	是	您可以將一個網路 ACL 關聯至 VPC 中的一或多個子網路。

名稱	預設	可調整	說明
每個網路 ACL 的規則數	20	是	此配額可決定傳入規則數目上限和傳出規則數目上限。此配額最多可以增加到 40 個傳入規則和 40 個傳出規則 (總共 80 個規則)，但網路效能可能會受到影響。

網路介面

名稱	預設	可調整	說明
每個執行個體的網路介面	依執行個體類型而異	否	如需詳細資訊，請參閱每個執行個體類型的網路介面。
每個區域的網路介面	5,000	是	此配額適用於個別 AWS 帳戶 VPCs和共用 VPCs。每個可用區域 (AZ) 都會強制執行此限制。例如，如果網路介面位於三個 AZ 中，則每個 AZ 的限制為 5000 個，區域的限制為 15000 個。

路由表

名稱	預設	可調整	說明
每個 VPC 的路由表	200	是	主要路由表計數趨近此配額。請注意，如果您要求增加路由表的配額，您可能也會想要求增加子網的配額。路由表可以與多個子網共用，但一個子網只能與一個路由表建立關聯。
每個路由表的路由數 (非傳播路由)	500	是	您可以最多可將此配額提高到 1000 個；不過，網路效能可能會受到影響。此配額由 IPv4 和 IPv6 路由分別強制執行。

名稱	預設	可調整	說明
			如果您有超過 125 個路由，我們建議您對呼叫進行分頁來說明您的路由表，以便提升效能。
每個路由表的傳播路由數	100	否	如果您需要額外的字首，請公告預設路由。

路由伺服器

名稱	預設	可調整	說明
每個 VPC 的路由伺服器數量	5	是。若要請求提高配額，請參閱《AWS Support 使用者指南》中的請求提高服務配額。	
每個路由伺服器的路由伺服器端點數量	10	是。若要請求提高配額，請參閱《AWS Support 使用者指南》中的請求提高服務配額。	

名稱	預設	可調整	說明
每個網路介面的對等工作階段數量	20	是。若要請求提高配額，請參閱《AWS Support 使用者指南》中的請求提高服務配額。	
每個路由伺服器與子網路的路由伺服器端點數量	2	否	為實現備援，同一路由伺服器在同一子網路中最多只能有兩個端點。
每個路由伺服器對等的路由數量	100	否	這是可透過路由伺服器對等動態公告的路由數量
每個路由伺服器的路由數量	100	否	這是可安裝至路由伺服器的轉送資訊庫 (FIB) 中的路由數量。

Security groups (安全群組)

名稱	預設	可調整	說明
每個區域的 VPC 安全群組	2,500	是	此配額適用於個別 AWS 帳戶 VPCs和共用 VPCs。 如果您將此配額增加到區域中 5,000 個安全群組以上，我們建議您對呼叫進行分頁來說明您的安全群組，以便提升效能。
每個安全群組的傳入或傳出規則	60	是	此配額會分別針對傳入和傳出規則強制執行。因此，對於預設配額為 60 個規則的帳戶，一個安全群組可擁有 60 個傳入規

名稱	預設	可調整	說明
			則和 60 個傳出規則。此外，此配額會分別針對 IPv4 和 IPv6 規則強制執行。對於預設配額為 60 個規則的帳戶，一個安全群組可擁有 60 個 IPv4 流量傳入規則和 60 個 IPv6 流量傳入規則。如需詳細資訊，請參閱the section called “安全群組大小”。 配額變更會同時套用至傳入和傳出規則。此配額與每個網路介面的安全群組數量配額的乘積不得超過 1,000。
每個網路介面的安全群組數	5	是 (最多 16 個)	此配額與每個安全群組之規則數量配額的乘積不得超過 1,000。若要將每個網路介面的安全群組數量的配額降低至預設值 5 以下，請參閱《AWS Support 使用者指南》中的請求提高服務配額。請求降低配額的程序與請求提高配額的程序相同。

VPC 子網路共用

所有標準 VPC 配額均適用於共用 VPC 子網路。

名稱	預設	可調整	說明
每個 VPC 的參與者帳戶	100	是	可以共享 VPC 中子網路的不同參與者帳戶數量上限。這是每個 VPC 的配額，並且會套用至 VPC 中共享的所有子網路。 VPC 擁有者可以檢視連接到參與者資源的網路介面和安全群組。
可與帳戶共享的子網路	100	是	這是可與 AWS 帳戶共用的子網路數量上限。

網路地址使用

網路地址使用 (NAU) 是由受管前綴清單中的 IP 地址、網路介面和 CIDR 組成。NAU 是套用至 VPC 中資源的指標，可協助您規劃和監控 VPC 大小。如需詳細資訊，請參閱網路地址使用。

構成 NAU 計數的資源擁有自己的個別服務配額。即使 VPC 具有可用的 NAU 容量，如果資源超過其服務配額，您也無法在 VPC 中啟動資源。

名稱	預設	可調整	說明
網路地址使用	64，000	是 (最多 256,000)	每個 VPC 的 NAU 單位數量上限。
對等網路地址使用	128，000	是 (最多 512,000)	VPC 及其區域內所有對等 VPC 的 NAU 單位數量上限。跨不同區域對等的 VPC 不計入此數字。

Amazon EC2 API 調節

如需有關 Amazon EC2 限流的資訊，請參閱《Amazon EC2 開發人員指南》中的請求限流。

額外配額資源

如需詳細資訊，請參閱下列內容：

- 《 AWS Client VPN 管理員指南》中的AWS Client VPN 配額
- 《AWS Direct Connect 使用者指南》中的 Direct Connect 配額
- 《Amazon VPC 對等互連指南》中的對等互連配額
- 《AWS PrivateLink 指南》中的 PrivateLink 配額
- 《AWS Site-to-Site VPN 使用者指南》中的 Site-to-Site VPN 配額
- 《Amazon VPC Traffic Mirroring 指南》中的 Traffic Mirroring 配額
- 《Amazon VPC 傳輸閘道指南》中的傳輸閘道配額

文件歷史記錄

下表說明 Amazon VPC 使用者指南每個版本的重要變更。

變更	描述	日期
VPC 加密控制	您現在可以使用 VPC 加密控制，對 VPC 內的網路流量強制執行傳輸中加密。此功能提供集中式加密政策強制執行和監控功能。	2025 年 11 月 21 日
用於自動多可用區域擴展的區域 NAT 閘道	您現在可以使用區域 NAT 閘道，根據您的工作負載使用量自動跨可用區域擴展。區域 NAT 閘道提供簡化的設定、增強的安全性和自動高可用性，無需手動介入。	2025 年 11 月 19 日
將傳入 VPC 流量路由至公有 IP 位址	您現在可以設定進階路由規則，將傳入流量從網際網路導向 VPC 中的特定公有 IP 位址，從而對輸入流量的傳輸與路由決策進行更精細地控制。	2025 年 8 月 13 日
使用 Amazon VPC 路由伺服器在 VPC 中進行動態路由	Amazon VPC 路由伺服器可簡化 VPC 及其網際網路閘道內部署的工作負載之間的流量路由。透過此功能，VPC 路由伺服器可使用您偏好的 IPv4 或 IPv6 路由動態更新 VPC 與閘道路由表，為這些工作負載實現路由容錯能力。這讓您能夠自動重新路由 VPC 內的流量，進而提高 VPC 路由的可管理性，以及與第三方工作負載的互通性。	2025 年 3 月 31 日

AWS 受管政策更新	Amazon VPC 已更新 AmazonVPCFullAccess 和 AmazonVPCReadOnlyAccess 受管政策。	2024 年 12 月 9 日
VPC BPA 的宣告政策支援	如果您使用 AWS Organizations 來管理組織中的帳戶，則可以使用宣告政策在組織中的帳戶強制執行 VPC BPA。	2024 年 12 月 1 日
VPC 封鎖公開存取 (BPA)	VPC 封鎖公開存取 (BPA) 可讓您封鎖您在區域中擁有 VPC 和子網路中的資源，透過網際網路閘道和僅輸出網際網路閘道來到達或接觸網際網路。	2024 年 11 月 19 日
共用安全群組	此功能可讓您與其他 AWS Organizations 帳戶共用安全群組。	2024 年 10 月 30 日
安全群組 VPC 關聯	此功能可讓您將安全群組與相同區域中 VPC 建立關聯。	2024 年 10 月 30 日
NAT 閘道 MTU 支援	NAT 閘道支援最大傳輸單位 (MTU) 為 8500 的流量。	2024 年 9 月 10 日
私有 IPv6 定址	已新增私有 IPv6 定址的相關資訊。私有 IPv6 地址僅適用於 Amazon VPC IP Address Manager。	2024 年 8 月 8 日
IPv6 偏好的租賃時間	您現在可以選擇指派 IPv6 的執行中執行個體經過 DHCPv6 租賃續約的頻率。	2024 年 2 月 20 日
指南結構檢閱和改善	已檢閱本指南的結構，並改進了改善與尋找特定案例資訊相關的客戶體驗。	2024 年 2 月 20 日

AWS 受管政策更新	Amazon VPC 已更新 AmazonVPCFullAccess 和 AmazonVPCReadOnlyAccess 受管政策。	2024 年 2 月 8 日
AWS 受管政策更新	Amazon VPC 已更新 AmazonVPCCrossAccountNetworkInterfaceOperations 受管政策。	2023 年 9 月 25 日
已取代 EC2-Classic	搭配 EC2-Classic，EC2 執行個體可在與其他客戶共用的單一平面網路中執行。Amazon VPC 取代 EC2-Classic。使用 Amazon VPC，您的執行個體可在邏輯上與 AWS 帳戶帳戶隔離的虛擬私有雲端 (VPC) 中執行。	2023 年 7 月 31 日
將次要 IPv4 地址新增至 NAT 閘道	您可以將次要私有 IPv4 地址新增至公有和私有 NAT 閘道。次要 IPv4 地址會增加可用連接埠的數目，因此會增加工作負載可使用 NAT 閘道建立之並行連線數目的限制。	2023 年 1 月 31 日
符合 IAM 最佳實務	更新了指南以符合 IAM 最佳實務。如需詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 1 月 4 日
挑選 NAT 閘道的私有 IP 地址	當您建立 NAT 閘道時，您現在就能選擇以挑選指派給 NAT 閘道的私有 IP 地址。之前，會從子網路的私有 IP 地址範圍中自動指派私有 IP 地址。	2022 年 11 月 17 日
IPv6 預設的閘道路由器組態	現在會保留三個 IPv6 地址供預設的 VPC 路由器使用。	2022 年 11 月 11 日

轉移彈性 IP 地址	您現在可以將彈性 IP 地址從一個 AWS 帳戶轉移到另一個帳戶。	2022 年 10 月 31 日
網路地址使用指標	您可以為 VPC 啟用網路地址使用指標，以協助您規劃和監控 VPC 的大小。	2022 年 10 月 4 日
將流量日誌發布至 Amazon Data Firehose	您可以將 Amazon Data Firehose 交付串流指定為流量日誌資料的目的地。	2022 年 9 月 8 日
NAT 閘道頻寬	NAT 閘道現在支援高達 100 Gbps（從 45 Gbps 增加）的頻寬，每秒最多可處理 1000 萬個封包（從 400 萬個封包增加）。	2022 年 6 月 15 日
多個 IPv6 CIDR 區塊	您可以將最多五個 IPv6 CIDR 區塊與 VPC 建立關聯。	2022 年 5 月 12 日
重組	本《Amazon Virtual Private Cloud 使用者指南》的一般重組。	2022 年 1 月 2 日
NAT 閘道 IPv6 至 IPv4	NAT 閘道支援從 IPv6 到 IPv4 的網路地址轉譯，通常稱為 NAT64。	2021 年 11 月 24 日
VPC 中僅限 IPv6 的子網	您可以建立僅限 IPv6 的子網，以便在其中啟動僅限 IPv6 的 EC2 執行個體。	2021 年 11 月 23 日
Amazon S3 的 VPC Flow Logs 交付選項	您可以指定 Apache Parquet 日誌檔案格式、每小時分割和 Hive 相容的 S3 字首。	2021 年 10 月 13 日

Amazon EC2 全域檢視	Amazon EC2 Global View 可讓您在單一主控台中檢視跨多個 AWS 區域的 VPCs、子網路、執行個體、安全群組和磁碟區。	2021 年 9 月 1 日
更具體的路由	您可以新增路由至比本機路由更具體的路由表。您可以使用更具體的路由，將 VPC (東西流量) 內子網之間的流量重新引導至中間設備。您可以設定路由的目的地，以符合 VPC 中子網的整個 IPv4 或 IPv6 CIDR 區塊。	2021 年 8 月 30 日
支援安全群組規則的資源 ID 和標記	您可以依資源 ID 參考安全群組規則。您也可以為安全群組規則新增標籤。	2021 年 7 月 7 日
私有 NAT 閘道	您可以使用私有 NAT 閘道在 VPC 之間或 VPC 與內部部署網路之間進行傳出限定私有通訊。	2021 年 6 月 10 日
建立時的標籤	您可以在建立 VPC、DHCP 選項、網際網路閘道、僅輸出閘道、網路 ACL 和安全群組時新增標籤。	2020 年 6 月 30 日
受管理的字首清單	您可以在字首清單中建立和管理一組 CIDR 區塊。	2020 年 6 月 29 日
流程日誌增強功能	新的流程記錄欄位可用，您可以為發佈至 CloudWatch Logs 的流程記錄指定自訂格式。	2020 年 5 月 4 日
流量日誌的標記支援	您可以將標籤新增至流量日誌。	2020 年 3 月 16 日

在建立 NAT 閘道時套用標籤	您可以在建立 NAT 閘道時新增標籤。	2020 年 3 月 9 日
流程日誌的最大彙總時間間隔	您可以指定擷取流程並彙總至流程日誌記錄的最長期間。	2020 年 2 月 4 日
網路邊界群組組態	您可以透過 Amazon VPC 主控台為 VPC 設定網路邊界群組。	2020 年 1 月 22 日
閘道路由表	您可以將路由表與閘道建立關聯，並將傳入 VPC 流量路由至 VPC 中的特定網路界面。	2019 年 12 月 3 日
流程日誌增強功能	您可指定流程日誌的自訂格式，並選擇在流程日誌記錄中傳回的欄位。	2019 年 9 月 11 日
VPC 共享	您可以與相同 AWS 組織中的多個帳戶共用位於相同 VPC 中的子網路。	2018 年 11 月 27 日
建立預設子網	您可以在沒有預設子網的可用區域中建立預設子網。	2017 年 11 月 9 日
NAT 閘道的標籤支援	您可以標記 NAT 閘道。	2017 年 9 月 7 日
適用於 NAT 閘道的 Amazon CloudWatch 指標	您可以檢視 NAT 閘道的 CloudWatch 指標。	2017 年 9 月 7 日
安全群組規則說明	您可以為安全群組規則新增說明。	2017 年 8 月 31 日
您 VPC 的輔助 IPv4 CIDR 區塊	您可在您的 VPC 中新增多個 IPv4 CIDR 區塊。	2017 年 8 月 29 日
復原彈性 IP 地址	如果您釋放彈性 IP 地址，您也許能夠予以復原。	2017 年 8 月 11 日
建立預設 VPC	如果您刪除現有的預設 VPC，您就可以建立新的預設 VPC。	2017 年 7 月 27 日

IPv6 支援	您可以建立 IPv6 CIDR 區塊與您 VPC 的關聯，然後將 IPv6 地址指派給 VPC 中的資源。	2016 年 12 月 1 日
非 RFC 1918 IP 地址範圍的 DNS 解析支援	Amazon DNS 伺服器現可將私有 DNS 主機名稱解析為所有地址空間的私有 IP 地址。	2016 年 10 月 24 日
NAT 閘道	您可在公有子網中建立 NAT 閘道，讓私有子網中的執行個體初始化通往網際網路或其他 AWS 服務的傳出流量。	2015 年 12 月 17 日
VPC 流程日誌	您可建立流程日誌，以擷取出入您 VPC 網路界面之 IP 流量的相關資訊。	2015 年 6 月 10 日
ClassicLink	您可使用 ClassicLink 將 EC2-Classic 執行個體連結至帳戶中的 VPC。您可以將 VPC 安全群組與 EC2-Classic 執行個體建立關聯，讓 EC2-Classic 執行個體可以使用私有 IP 地址與您 VPC 中的執行個體通訊。	2015 年 1 月 7 日
使用私有託管區域	您可使用您在 Route 53 私有託管區域中定義的自訂 DNS 網域名稱，存取您 VPC 中的資源。	2014 年 11 月 5 日
修改子網的公有 IP 定址屬性	您可以修改您子網的公有 IP 定址屬性，指出在該子網中啟動的執行個體是否應該接收公有 IP 地址。	2014 年 6 月 21 日
指派公有 IP 地址	您可以在啟動期間將公有 IP 地址指派給執行個體。	2013 年 8 月 20 日

啟用 DNS 主機名稱和停用 DNS 解析	您可以修改 VPC 預設值，並停用 DNS 解析，以及啟用 DNS 主機名稱。	2013 年 3 月 11 日
VPC 無所不在	新增五個 AWS 區域中的 VPC 支援、多個可用區域中VPCs、每個 AWS 帳戶多個 VPCs，以及每個 VPC 的多個 VPN 連線。	2011 年 8 月 3 日
專用執行個體	專用執行個體是在您 VPC 內啟動的 Amazon EC2 執行個體，會執行單一客戶專用的硬體。	2011 年 3 月 27 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。