



使用者指南

# Amazon Virtual Private Cloud



# Amazon Virtual Private Cloud: 使用者指南

Copyright © 2024 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 專用全球網路 .....	8
開始使用 .....	10
註冊一個 AWS 帳戶 .....	10
驗證許可 .....	10
確定您的 IP 地址範圍 .....	11
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
比較 IPv4 和 IPv6 .....	14
私有 IPv4 地址 .....	15
公有 IPv4 地址 .....	15
IPv6 地址 .....	16
使用您自己的 IP 地址 .....	17
使用 Amazon VPC IP 地址管理員 .....	17
VPC CIDR 區塊 .....	17
IPv4 VPC CIDR 區塊 .....	18
管理 VPC 的 IPv4 CIDR 區塊 .....	19
IPv4 CIDR 區塊關聯限制 .....	21
IPv6 VPC CIDR 區塊 .....	22
子網路 CIDR 區塊 .....	23

IPv4 的子網路規模調整 .....	24
IPv6 的子網規模 .....	24
受管理的字首清單 .....	25
字首清單的概念和規則 .....	26
字首清單的 Identity and Access Management .....	26
由客戶管理之前綴清單 .....	27
AWS管理的字首清單 .....	32
共用的前綴清單 .....	33
AWS 資源中的參考字首清單 .....	37
AWS IP 位址範圍 .....	39
下載 .....	40
語法 .....	40
範圍重疊 .....	43
篩選 JSON 檔案 .....	43
實作出口控制 .....	46
AWS IP 位址範圍通知 .....	47
版本備註 .....	49
進一步了解 .....	50
將 IPv6 支援新增至您的 VPC .....	50
範例：在含公有和私有子網的 VPC 中啟用 IPv6 .....	51
步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網的關聯 .....	54
步驟 2：更新路由表 .....	55
步驟 3：更新安全群組規則 .....	56
步驟 4：將 IPv6 地址指派給執行個體 .....	56
上的 IPv6 支援 AWS .....	57
支援 IPv6 的服務 .....	57
其他 IPv6 支援 .....	63
進一步了解 .....	64
Virtual Private Cloud (VPC) .....	65
VPC 基本概念 .....	65
VPC IP 地址範圍 .....	65
VPC 圖表 .....	66
VPC 資源 .....	66
預設 VPC .....	67
預設 VPC 元件 .....	67
預設子網路 .....	70

檢視您的預設 VPC 和預設子網路 .....	70
建立預設 VPC .....	71
建立預設子網路 .....	72
刪除您的預設子網路和預設 VPC .....	73
建立 VPC .....	74
VPC 組態選項 .....	74
建立 VPC 以及其他 VPC 資源 .....	76
僅建立 VPC .....	77
使用建立 VPC AWS CLI .....	78
設定您的 VPC .....	83
檢視您的 VPC 相關詳細資訊 .....	83
視覺化 VPC 中的資源 .....	83
新增 IPv4 CIDR 區塊 .....	85
新增 IPv6 CIDR 區塊 .....	86
移除 IPv4 CIDR 區塊 .....	87
移除 IPv6 CIDR 區塊 .....	87
DHCP 選項集 .....	88
什麼是 DHCP? .....	88
DHCP 選項集概念 .....	89
使用 DHCP 選項集 .....	92
DNS 屬性 .....	97
Amazon DNS 伺服器 .....	97
DNS 主機名稱 .....	98
VPC 中的 DNS 屬性 .....	99
DNS 配額 .....	100
檢視 EC2 執行個體的 DNS 主機名稱 .....	100
檢視和更新 VPC 的 DNS 屬性 .....	101
私有託管區域 .....	102
網路地址使用 .....	103
NAU 的計算方式 .....	104
NAU 範例 .....	104
共享 VPC .....	105
共用 VPC 必要條件 .....	106
共用子網路 .....	106
取消共用的子網路 .....	107
識別共用子網路的擁有者 .....	108

管理 VPC 資源 .....	108
擁有者和參與者的責任與權限 .....	109
AWS 資源和共用的 VPC 子網路 .....	111
VPC 共享配額 .....	112
共用子網路的範例 .....	112
將 VPC 擴展至另一個區域 .....	114
AWS Local Zones 中的子網路 .....	114
AWS Wavelength 中的子網路 .....	119
AWS Outposts 中的子網路 .....	121
刪除您的 VPC .....	122
使用主控台進行刪除 .....	122
使用 CLI 進行刪除 .....	123
子網 .....	125
子網基本概念 .....	125
子網路 IP 地址範圍 .....	125
子網類型 .....	126
子網圖表 .....	126
子網路路由 .....	127
子網設定 .....	127
子網安全 .....	128
建立子網 .....	128
設定您的子網路 .....	130
檢視您的子網路 .....	130
將 IPv6 CIDR 區塊新增至您的子網路 .....	131
從您的子網路中移除 IPv6 CIDR 區塊 .....	131
修改您子網路的公有 IPv4 定址屬性 .....	132
修改您子網路的公有 IPv6 定址屬性 .....	132
子網路 CIDR 保留 .....	133
透過主控台使用子網路 CIDR 保留 .....	133
使用子網路 CIDR 保留區使用 AWS CLI .....	134
路由表 .....	135
路由表概念 .....	135
子網路路由表 .....	136
閘道路由表 .....	142
路由優先順序 .....	145
路由表配額 .....	147

疑難排解可達性問題 .....	147
路由選項範例 .....	147
使用路由表 .....	160
中間設備路由精靈 .....	169
刪除子網路 .....	181
連線 VPC .....	182
網際網路閘道 .....	183
網際網路存取組態 .....	183
使用網際網路閘道 .....	186
API 和命令概觀 .....	188
定價 .....	189
輸出限定網際網路閘道 .....	189
輸出限定網際網路閘道基本概念 .....	189
使用輸出限定網際網路閘道 .....	190
API 和 CLI 概觀 .....	193
定價 .....	193
NAT 裝置 .....	193
NAT 閘道 .....	195
NAT 執行個體 .....	233
比較 NAT 裝置 .....	244
彈性 IP 地址 .....	246
彈性 IP 位址概念和規則 .....	246
使用彈性 IP 地址 .....	247
定價 .....	256
AWS 傳輸閘道 .....	256
AWS Virtual Private Network .....	257
VPC 對等連線 .....	257
監控 .....	259
VPC 流程日誌 .....	259
流量日誌基礎知識 .....	260
流量日誌記錄 .....	263
流量日誌記錄範例 .....	272
流量日誌限制 .....	279
定價 .....	281
使用流量日誌工作 .....	282
發佈至 CloudWatch 記錄 .....	285

發佈到 Amazon S3 .....	292
發佈到 Amazon 數據 Firehose 件 .....	300
使用 Athena 查詢 .....	307
疑難排解 .....	310
CloudWatch 指標 .....	314
NAU 指標與維度 .....	314
啟用或停用 NAU 監控 .....	317
NAU CloudWatch 警示範例 .....	317
安全 .....	319
資料保護 .....	319
網際網路流量隱私權 .....	320
Identity and Access Management .....	321
物件 .....	321
使用身分進行驗證 .....	321
使用政策管理存取權 .....	324
Amazon VPC 如何與 IAM 搭配運作 .....	326
政策範例 .....	330
疑難排解 .....	339
AWS 受管政策 .....	341
基礎設施安全 .....	342
網路隔離 .....	343
控制網路流量 .....	343
比較安全群組和網路 ACL .....	344
安全群組 .....	345
安全群組基礎知識 .....	346
安全群組範例 .....	348
安全群組規則 .....	349
預設安全群組 .....	358
使用安全群組 .....	360
網路 ACL .....	364
網路 ACL 基本概念 .....	365
網路 ACL 規則 .....	366
預設網路 ACL .....	366
自訂網路 ACL .....	368
自訂網路 ACL 和其他 AWS 服務 .....	374
暫時性連接埠 .....	374



路徑 MTU 探索 .....	374
使用網路 ACL .....	375
範例：控制對子網路中執行個體的存取 .....	381
疑難排解可達性問題 .....	384
恢復能力 .....	384
法規遵循驗證 .....	384
最佳實務 .....	385
搭配使用 與其他 服務 .....	387
AWS PrivateLink .....	387
AWS Network Firewall .....	388
Route 53 Resolver DNS Firewall .....	389
Reachability Analyzer .....	390
範例 .....	391
測試環境 .....	391
概要 .....	392
建立 VPC .....	393
部署您的應用程式 .....	394
測試組態 .....	395
清除 .....	395
網頁和資料庫伺服器 .....	395
概要 .....	395
建立 VPC .....	399
部署您的應用程式 .....	400
測試組態 .....	400
清除 .....	401
私有伺服器 .....	401
概要 .....	401
建立 VPC .....	404
部署您的應用程式 .....	405
測試組態 .....	405
清除 .....	405
配額 .....	406
VPC 和子網路 .....	406
DNS .....	406
彈性 IP 地址 .....	407
閘道 .....	407

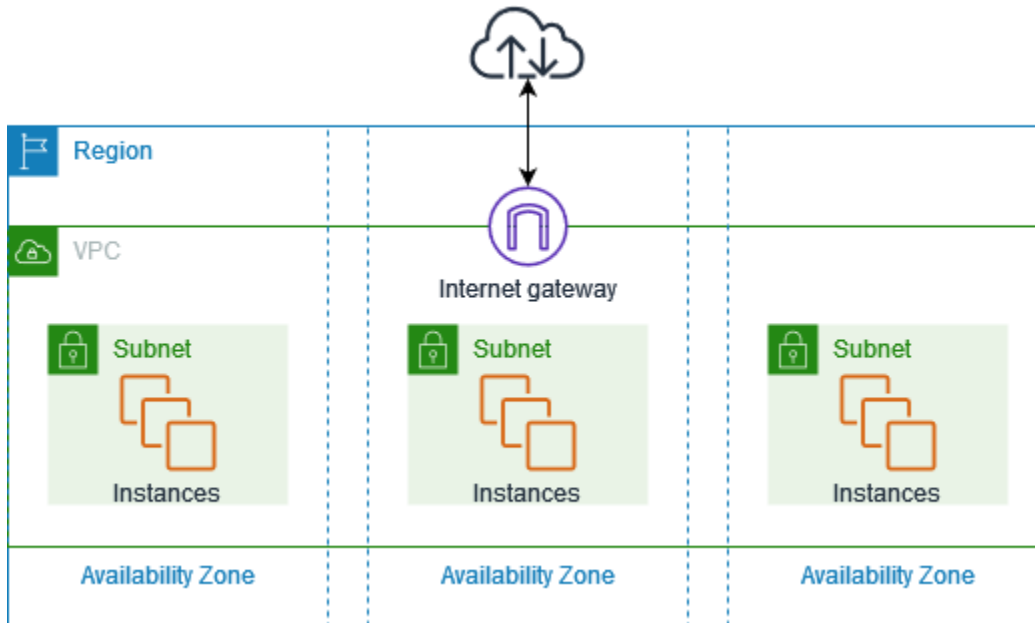
---

由客戶管理之前綴清單 .....	408
網路 ACL .....	408
網路介面 .....	409
路由表 .....	409
安全群組 .....	410
VPC 共享 .....	411
網路地址使用 .....	411
Amazon EC2 API 調節 .....	412
額外配額資源 .....	412
文件歷史記錄 .....	413
.....	cdxix

# 「什麼是 Amazon VPC？」

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。

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

[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 並將其分配到 VPC 中的資源，例如 EC2 執行個體、NAT 閘道和網路負載平衡器。

## 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](#) 連接到 AWS 服務 私有，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

使用作為中央中樞的 [傳輸閘道](#)，在 VPC、VPN 連線和 AWS 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 \(AWS VPN\)](#) 將 VPC 連線至內部部署網路。

# Amazon VPC 入門

您的每個 VPC 都 AWS 帳戶 包含一個 [AWS 區域默認 VPC](#)。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 [開始使用](#)。

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 Management Console：提供 Web 介面，您可使用此介面來存取 VPC。
- AWS Command Line Interface (AWS CLI) — 為包括 Amazon VPC 在內的一組廣泛 AWS 服務提供命令，並在視窗、Mac 和 Linux 上受到支援。如需詳細資訊，請參閱 [AWS Command Line Interface](#)。
- AWS SDK — 提供特定語言的 API，並處理許多連線詳細資料，例如計算簽章、處理要求重試和錯誤處理。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。但是，某些 VPC 元件會收取費用，例如 NAT 閘道、IP 位址管理員、流量鏡像、可 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 (VPC) 中啟動的幾乎所有資源都會為您提供連線的 IP 位址。VPC 中絕大多數資源都使用私有 IPv4 地址。但是，需要透過 IPv4 直接存取網際網路的資源，則會使用公用 IPv4 位址。

### 公有 IPv4 地址的定價

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

如果您是現有或新的 [AWS 免費方案](#) 客戶，您可以免費獲得 750 小時的公共 IPv4 地址使用時間。如果您未使用 AWS 免費方案，則會向公用 IPv4 地址收費。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。如需共用 VPC 如何收取公用 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](#)。

公用 IPv4 位址具有下列類型：

- 彈性 IP 地址 (EIP)：Amazon 提供的靜態公有 IPv4 地址，您可以與 EC2 執行個體、elastic network interface 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 位址：[您使用自帶 IP 位址 \(BYOIP\) 所帶來的 IPv4 位址範圍內的公 AWS 用 IPv4 位址](#)。

- 服務管理的 IPv4 位址：在 AWS 資源上自動佈建並由服務管理的公用 IPv4 位址。AWS 例如，Amazon ECS、Amazon RDS 或 Amazon 上的公共 IPv4 地址。WorkSpaces

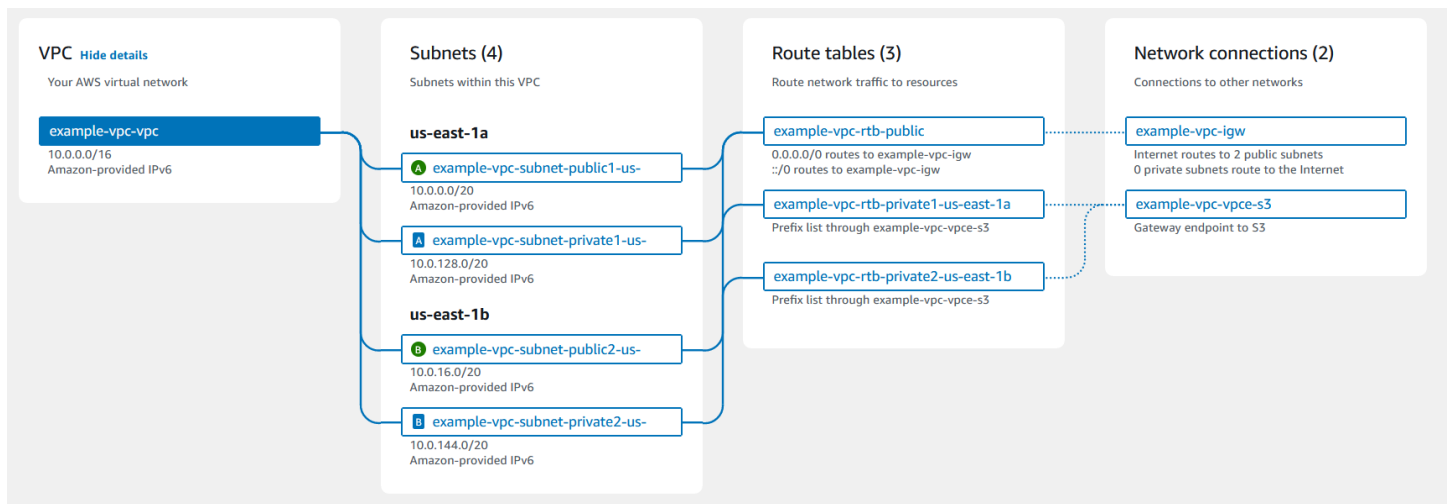
下列清單顯示可以使用公用 IPv4 位址的最常用 AWS 服務。

- Amazon AppStream 2.0
- [AWS Client VPN](#)
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift
- 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 Management Console 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 [資源映射](#) 標籤上存取此視覺效果。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 專用全球網路](#)

## 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 中的 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

- [使用網際網路閘道連線至網際網路](#)
- [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

您可以選擇性地使用 IPsec AWS Site-to-Site VPN 連接將 VPC 連接到自己的公司數據中心，從而使 AWS 雲成為數據中心的擴展。

站 Site-to-Site VPN 連線包含兩個 VPN 通道，介於 AWS 側邊的虛擬私有閘道或傳輸閘道，以及位於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 VPC、VPN 連線、AWS Direct Connect 閘道和傳輸閘道對等連線。

進一步了解

- [Amazon VPC Peering Guide](#)
- [Amazon VPC 傳輸閘道](#)

## AWS 專用全球網路

AWS 提供高效能、低延遲的私有全球網路，提供安全的雲端運算環境，以支援您的網路需求。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。

適用下列注意事項：

- 位於可用區域中或所有區域的可用區域之間的流量，會透過 AWS 私人全域網路路由傳送。
- 區域之間的流量一律會透過 AWS 私人全球網路路由，中國區域除外。

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。我們測量連接區域的全球骨幹網路中的封包損失率 (PLR)。AWS 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%。

# 開始使用 Amazon 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

- [註冊一個 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](#)

## 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建 AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 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 Identity and Access Management](#) 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

區 AWS 域是我們叢集資料中心 (稱為可用區域) 的實體位置。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，建議您至少選取兩個可用區域，並在每個作用中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 AWS Management Console 並在組態中包含公用子網路來建立 VPC，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：

- 個別 IPv4 地址為 32 位元，4 組最多 3 位數的數字。例如，10.0.1.0。
- IPv4 CIDR 區塊包含四組最多三位數的十進制數字 0-255，由句點分隔，後跟正斜線和一個 0 至 32 之間的數字。例如，10.0.0.0/16。
- 個別 IPv6 地址為 128 位元，8 組 4 位數的十六進位數字。例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334。
- IPv6 CIDR 區塊包含四組最多四位數的十六進位數字，以冒號分隔，後跟雙冒號、斜杠和 1 至 128 之間的數字。例如 2001:db8:1234:1a00::/56。

如需詳細資訊，請參閱[什麼是 CIDR？](#)

## 目錄

- [比較 IPv4 和 IPv6](#)
- [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](#)
- [使用受管前綴清單對 CIDR 區塊分組](#)
- [AWS IP 位址範圍](#)
- [將 IPv6 支援新增至您的 VPC](#)
- [AWS 支援 IPv6 的服務](#)

## 比較 IPv4 和 IPv6

下表摘要 Amazon EC2 和 Amazon VPC 中 IPv4 和 IPv6 的差異。如需支援雙堆疊設定 (IPv4 和 IPv6) 和僅限 IPv6 組態的 AWS 服務清單，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 <a href="#">配額</a> 是可調整的。	從 /44 至 /60 (增量為 /4) 最多 5 個 CIDR。此 <a href="#">配額</a> 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 <a href="#">《Amazon VPC IPAM 使用者指南》</a> 中的什麼是 IPAM？。	您可以為您的虛擬私人雲端使 AWS 用自己的 IPv6 CIDR 區塊、選擇 Amazon 提供的 IPv6 CIDR 區塊，或者您可以從 Amazon VPC IP 地址管理員 (IPAM) 配置 CIDR 區塊。如需詳細資訊，請參閱 <a href="#">《Amazon VPC IPAM 使用者指南》</a> 中的什麼是 IPAM？。
網際網路存取	需要 <a href="#">網際網路閘道</a> 。	需要網際網路閘道。支援使用 <a href="#">輸出限定網際網路閘道</a> 進行僅限傳出的通訊。
彈性 IP 地址	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	執行個體會收到 Amazon 提供的 IPBN 或 RBN 型 DNS 名稱。DNS 名



特性	IPv4	IPv6
	稱會解析為執行個體選取的 DNS 記錄。	稱會解析為執行個體選取的 DNS 記錄。

## 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，便會從子網的 IPv4 地址範圍指派一個主要私有 IP 地址給執行個體的預設網路介面 (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。如需有關網路界面的詳細資訊，請參閱 Amazon EC2 使用者指南中的[彈性網路界面](#)。

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。如需有關主要和次要 IP 地址的詳細資訊，請參閱 Amazon EC2 使用者指南中的[多個 IP 地址](#)。

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 AWS 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界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 (eth0) 指派公有 IP 地址。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 所有公用 IPv4 位址的費用，包括與執行中執行個體和彈性 IP 位址相關聯的公用 IPv4 位址。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 [修改您子網路的公有 IPv4 定址屬性](#)。
- 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。
- 啟動後，您可以管理與網路介面關聯的 IP 位址，從執行個體取消指派公用 IP 位址。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [管理 IP 地址](#)。

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。在某些情況下，我們會從您的執行個體釋出公有 IP 位址，或指派新的 IP 位址。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [公用 IP 地址](#)。

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。如需更多詳細資訊，請參閱 [VPC 的 DNS 屬性](#)。

## IPv6 地址

您可以選擇建立 IPv6 CIDR 區塊與 VPC 的關聯，並建立 IPv6 CIDR 區塊與子網的關聯。如需詳細資訊，請參閱下列主題：

- [將 IPv6 CIDR 區塊新增至您的 VPC](#)
- [將 IPv6 CIDR 區塊新增至您的子網路](#)

IPv6 地址是全域不重複的地址，可設定為維持在私有不公開的狀態，或可透過網際網路來連線。如果建立 IPv6 CIDR 區塊與 VPC 和子網的關聯，以及符合下列其中一項，則您的執行個體會收到 IPv6 地址：

- 在啟動期間，您的子網會設定為自動將 IPv6 地址指派給執行個體。如需詳細資訊，請參閱 [修改您子網路的公有 IPv6 定址屬性](#)。
- 在啟動期間，您將 IPv6 地址指派給您的執行個體。
- 在啟動之後，您將 IPv6 地址指派給執行個體的主要網路介面。
- 在啟動之後，您將 IPv6 地址指派給相同子網中的網路介面，並將網路介面連接至執行個體。

當您的執行個體在啟動期間收到 IPv6 地址時，會建立該地址與執行個體之主要網路介面 (eth0) 的關聯。您可以透過下列方式，管理執行個體主要網路介面 (eth0) 的 IPv6 位址：

- 從網路介面指派和取消指派 IPv6 位址 您可指派給網路介面的 IPv6 地址數目以及您可連接至執行個體的網路介面數目，會根據執行個體類型而不同。如需詳細資訊，請參閱 Amazon EC2 使用者指南中[每個執行個體類型的每個網路界面的 IP 地址](#)。
- 啟用主要 IPv6 位址。主要 IPv6 位址可讓您避免中斷傳送至執行個體或 ENI 的流量。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的[建立網路界面](#)和[管理 IP 地址](#)。

IPv6 地址會在您停止和啟動或休眠和啟動執行個體時持續保留，並在您終止執行個體時予以釋放。若 IPv6 地址已經指派給另一個網路介面，您無法重新指派該 IPv6 地址 (您必須先將之取消指派)。

您可以藉由控制您子網路的路由，或是使用安全群組和網路 ACL 規則，控制是否可透過執行個體的 IPv6 地址連線至執行個體。如需更多詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權](#)。

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](#)。

## 使用您自己的 IP 地址

您可以將部分或全部的公用 IPv4 位址範圍或 IPv6 位址範圍帶入您的 AWS 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。將地址範圍帶到之後 AWS，它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 使用者指南中的使用[您自己的 IP 地址 \(BYOIP\)](#)。

## 使用 Amazon VPC IP 地址管理員

Amazon VPC IP 位址管理員 (IPAM) 是一項虛擬私人 VPC 功能，可讓您更輕鬆地規劃、追蹤和監控工作負載的 IP 地址。AWS 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 [將 IPv4 CIDR 區塊新增至您的 VPC](#)。

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

### Important

某些 AWS 服務使用 172.17.0.0/16 CIDR 範圍。為避免將來發生衝突，請勿在建立 VPC 時使用此範圍。例如，如果 IP 地址範圍已在網絡中的任何地方使用，則像 AWS Cloud9 或 Amazon 這樣的服務 SageMaker 可能會遇到 172.17.0.0/16 IP 地址衝突。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。

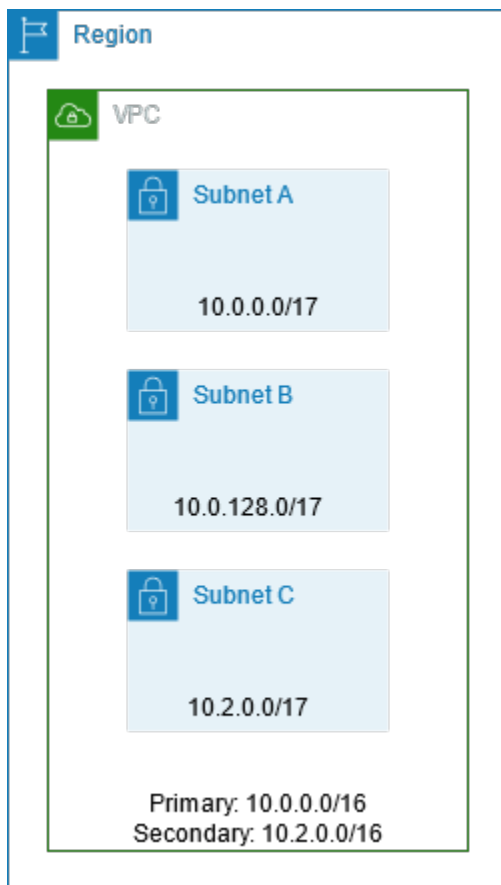
當您建立 VPC 以搭配 AWS 服務使用時，請查看服務文件以確認其組態是否有特定需求。

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。

目的地	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。
- 如果您使用透過直 AWS Direct Connect 接 Connect 閘道連線到多個 VPC，與直接連線閘道相關聯的 VPC 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《AWS 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[描述-v pcs](#) 指令，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
```

下列為範例輸出。

```
10.0.0.0/16
```

## IPv4 CIDR 區塊關聯限制

下表概述了允許和受限 VPC CIDR 區塊關聯。造成限制的原因是某些 AWS 服務會使用跨 VPC 和跨帳戶功能，這些功能需要服務端不衝突的 CIDR 區塊。AWS

IP 地址範圍	受限制的關聯	許可的關聯
10.0.0.0/8	<p>來自其他 RFC 1918* 範圍 (172.16.0.0/12 及 192.168.0.0/16) 的 CIDR 區塊。</p> <p>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。</p> <p>來自 198.19.0.0/16 範圍的 CIDR 區塊。</p>	<p>位於 /16 網路遮罩與 /28 網路遮罩之間的 10.0.0.0/8 範圍內的任何其他 CIDR 區塊，但不受限制。</p> <p>介於 /16 網路遮罩與 /28 網路遮罩之間的任何公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或介於 100.64.0.0/10 範圍之間的 /16 網路遮罩與 /28 網路遮罩之間的 CIDR 區塊。</p>
169.254.0.0/16	<p>如 <a href="#">RFC 5735</a> 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。</p>	
172.16.0.0/12	<p>來自其他 RFC 1918* 範圍 (10.0.0.0/8 及 192.168.0.0/16) 的 CIDR 區塊。</p> <p>來自 172.31.0.0/16 範圍的 CIDR 區塊。</p>	<p>172.16.0.0/12 範圍介於 /16 網路遮罩與 /28 網路遮罩之間且未受限制的任何其他 CIDR 區塊。</p> <p>介於 /16 網路遮罩與 /28 網路遮罩之間的任何公開路由 IPv4 CIDR 區塊</p>

IP 地址範圍	受限制的關聯	許可的關聯
	來自 198.19.0.0/16 範圍的 CIDR 區塊。	(非 RFC 1918)，或介於 100.64.0.0/10 範圍之間的 /16 網路遮罩與 /28 網路遮罩之間的 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。	介於 /16 網路遮罩與 /28 網路遮罩之間的任何其他 CIDR 區塊。  介於 /16 網路遮罩與 /28 網路遮罩之間的任何公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或介於 /16 網路遮罩與 /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。	介於 /16 網路遮罩與 /28 網路遮罩之間的任何公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或介於 /16 網路遮罩與 /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。	介於 /16 網路遮罩與 /28 網路遮罩之間的任何其他公開路由 IPv4 CIDR 區塊 (非 RFC 1918)，或介於 100.64.0.0/10 範圍之間的 /16 網路遮罩與 /28 網路遮罩之間的 CIDR 區塊。

\* 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 [將 IPv6 CIDR 區塊新增至您的 VPC](#)。

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”](#)。



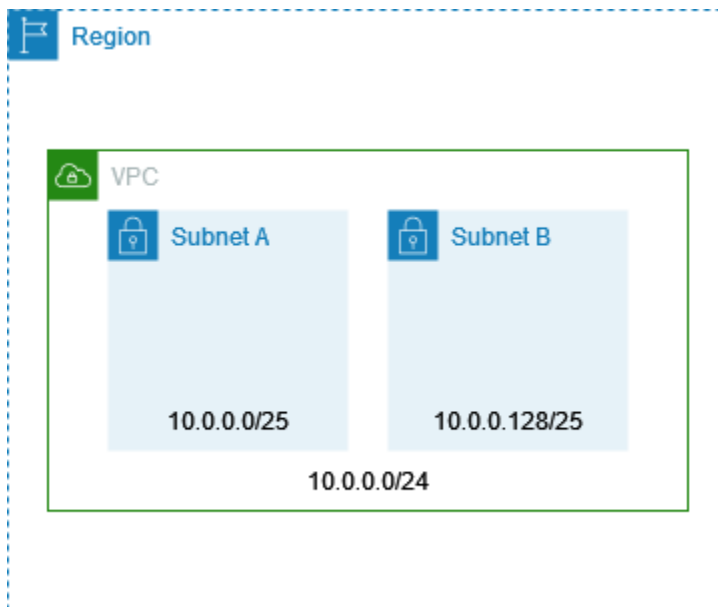
例如，您建立 VPC，並指定您希望將 Amazon 提供的 IPv6 CIDR 區塊與 VPC 建立關聯。Amazon 會指派下列 IPv6 CIDR 區塊給您的 VPC：2001:db8:1234:1a00::/56。您不能自行選擇 IP 地址的範圍。您可以建立子網，並關聯來自此範圍的 IPv6 CIDR 區塊；例如：2001:db8:1234:1a00::/64。

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 VPC 路由 AWS 器保留。
- 10.0.0.2：由保留。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：保留 AWS 供 future 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。

如果您將 IPv4 位址範圍帶到 AWS 使用 [BYOIP](#)，您可以使用範圍內的所有 IP 位址，包括第一個位址 (網路位址) 和最後一個位址 (廣播位址)。

## 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 VPC 路由器保留。
- 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 路由器保留的 IP 位址外，下列 IPv6 位址也會保留給預設 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。

## 使用受管前綴清單對 CIDR 區塊分組

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。您也可以使用 Resource Access Manager (RAM)，將受管理的前置詞清單與其他 AWS 帳號搭配使用。

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 帳號共用您的首碼清單，讓這些帳戶能夠參考其資源中的前置詞清單。
- AWS-受管理的前置詞清單 — AWS 服務的 IP 位址範圍集合。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](#)
- [使用由客戶管理之前綴清單](#)
- [使用 AWS 託管前綴列表](#)
- [使用共用字首清單](#)
- [AWS 資源中的參考字首清單](#)

## 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。如需更多詳細資訊，請參閱 [路由優先順序和字首清單](#)。
- 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。如需更多詳細資訊，請參閱 [由客戶管理之前綴清單](#)。
- 客戶管理的字首清單適用於所有商業 [AWS 區域](#) (包括 GovCloud (美國) 和中國地區)。

### AWS管理的字首清單

下列規則適用於 AWS-managed 前置詞清單：

- 您無法建立、修改、共用或刪除 AWS-managed 前置詞清單。
- 不同的 AWS-managed 前綴列表在使用它們時具有不同的權重。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-managed 前置詞清單的版本號碼。

## 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。

若要查看 Amazon VPC 動作清單以及可在 IAM 原則中使用的資源和條件金鑰，請參閱《IAM 使用者指南》中的 [Amazon EC2 的動作、資源和條件金鑰](#)。

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。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:GetManagedPrefixListAssociations",
      "ec2:GetManagedPrefixListEntries",
      "ec2:ModifyManagedPrefixList",
      "ec2:RestoreManagedPrefixListVersion"
    ],
    "Resource": "arn:aws:ec2:region:account: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 Identity and Access Management](#)。

## 使用由客戶管理之前綴清單

您可以建立及管理由客戶管理之前綴清單。您可以查看 AWS-managed 前綴列表。

### 任務

- [建立前綴清單](#)
- [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](#)

## 建立前綴清單

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)。

### 使用建立首碼清單的步驟 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」欄會顯示首碼清單擁有者的 AWS 帳號 ID。對於 AWS-managed 前綴列表，所有者 ID 是 AWS。

使用檢視字首清單的步驟 AWS CLI

使用 [describe-managed-prefix-lists](#) 命令。

## 檢視字首清單的項目

您可以檢視前置碼清單的項目、與您共用的前置碼清單，以及 AWS-managed 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。

使用檢視字首清單項目的步驟 AWS CLI

使用 [get-managed-prefix-list-entries](#) 指令。

## 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-managed 前置詞清單的相關資源。

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。

若要使用檢視前置碼清單關聯 AWS CLI

使用 [get-managed-prefix-list-關聯](#) 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 AWS-managed 前置詞清單。
- 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. 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。
6. 選擇 Save prefix list (儲存字首清單)。

### 若要使用修改字首清單 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)。

使用重新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)。

若要使用還原前置碼清單的先前版本 AWS CLI

使用 [restore-managed-prefix-list-版本](#) 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 AWS-managed 前置詞清單。

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)。

若要使用刪除字首清單 AWS CLI

使用 [delete-managed-prefix-list](#) 命令。

## 使用 AWS 託管前綴列表

AWS 管理前綴列表是 AWS 服務的 IP 地址範圍集。

目錄

- [使用 AWS-managed 前綴列表](#)
- [AWS 管理的字首清單權重](#)
- [可用的 AWS 託管前綴列表](#)

## 使用 AWS-managed 前綴列表

AWS-managed 前綴列表由 AWS 創建和維護，任何擁有 AWS 帳戶的人都可以使用。您無法建立、修改、共用或刪除 AWS-managed 前置詞清單。

與客戶管理的前置詞清單一樣，您可以將 AWS-managed 前置詞清單與 AWS 資源 (例如安全群組和路由表) 搭配使用。如需詳細資訊，請參閱 [AWS 資源中的參考字首清單](#)。

## AWS 管理的字首清單權重

AWS-managed 前綴列表的權重是指它在資源中佔用的條目數。

例如，Amazon CloudFront 託管前綴列表的權重為 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。

## 可用的 AWS 託管前綴列表

下列服務提供 AWS-managed 前置詞清單。

AWS 服務	字首清單名稱	Weight
<a href="#">Amazon CloudFront</a>	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb	1
AWS Ground Station	com.amazonaws.global.groundstation	5
<a href="#">Amazon Route 53</a>	com.amazonaws. <i>region</i> .ipv6.route53-healthchecks	25
	com.amazonaws. <i>region</i> .route53-healthchecks	25
Amazon S3	com.amazonaws. <i>region</i> .s3	1
Amazon S3 Express 單區域	com.amazonaws. <i>region</i> .s3express	6
<a href="#">Amazon VPC Lattice</a>	com.amazonaws. <i>region</i> .vpc-lattice	10
	com.amazonaws. <i>region</i> .ipv6.vpc-lattice	10

若要使用主控台檢視 AWS-managed 前置詞清單

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。

若要檢視 AWS 管理的前置詞清單，請使用 AWS CLI

使用 [describe-managed-prefix-lists](#) 命令，如下所示。

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

## 使用共用字首清單

使用 AWS Resource Access Manager (AWS RAM)，前綴列表的所有者可以與以下內容共享前綴列表：

- 其組織內部或外部的特定 AWS 帳戶 AWS Organizations
- 其組織內部的組織單位 AWS Organizations
- 中的整個組織 AWS Organizations

已共用前置碼清單的取用者可以檢視前置詞清單及其項目，而且他們可以參考其 AWS 資源中的前置詞清單。

若要取得有關的更多資訊 AWS RAM，請參閱[AWS RAM 使用者指南](#)。

## 目錄

- [共用字首清單的先決條件](#)
- [共用字首清單](#)
- [識別共用的字首清單](#)
- [識別共用字首清單的參考](#)
- [取消共享已共用的字首清單](#)
- [共用字首清單許可](#)
- [計費和計量](#)
- [的配額 AWS RAM](#)

## 共用字首清單的先決條件

- 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。您無法共享 AWS-managed 前綴列表。
- 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](#)。

## 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。

如果您是組織的一員 AWS Organizations，且已啟用組織內共用功能，則組織中的用戶會自動獲得共用前置詞清單的存取權。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。

### 使用 AWS RAM 主控台建立資源共享並共用字首清單

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的資源共享

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。

### 若要共用您使用 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](#)

## 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)。

### 若要使用識別共用首碼清單 AWS CLI

使用 [describe-managed-prefix-lists](#) 命令。該命令返回您擁有的前綴列表以及與您共享的前綴列表。OwnerId 顯示前置詞清單擁有者的 AWS 帳號 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。

若要使用識別共用字首清單的參照 AWS CLI

使用 [get-managed-prefix-list-關聯](#) 命令。

## 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前置詞清單，您必須使用將其從資源共用 AWS RAM 中移除。

若要取消共用您使用主控台擁有的 AWS RAM 共用前置詞清單

請參閱《AWS RAM 使用者指南》中的[更新資源共享](#)。

若要取消共用您所擁有的共用前置詞清單，請使用 AWS CLI

使用 [disassociate-resource-share](#) 命令。

## 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前置詞清單之 AWS 資源的 ID。但是，它們無法在取用者擁有的 AWS 資源中新增或移除前置詞清單的參照。

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

取用者可以檢視共用前置碼清單中的項目，也可以參考 AWS 資源中的共用前置詞清單。不過，消費者無法修改、還原或刪除共用的字首清單。

## 計費和計量

共用字首清單無須額外收費。

## 的配額 AWS RAM

如需詳細資訊，請參閱 [Service Quotas](#)。

## AWS 資源中的參考字首清單

您可以在以下 AWS 資源中引用前綴列表。

### 資源

- [VPC security groups \(VPC 安全群組\)](#)
- [子網路路由表](#)
- [Transit Gateway 路由表](#)
- [AWS Network Firewall 規則群組](#)
- [Amazon Managed Grafana 網路存取控制](#)
- [AWS Outposts 機架本地閘道](#)

## 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 [安全群組](#)。

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 Source (來源) (輸入規則) 或 Destination (目的地) (輸出規則)，選擇字首清單的 ID。
6. 選擇 Save rules (儲存規則)。

若要使用參照安全性群組規則中的前置碼清單 AWS CLI

使用 [authorize-security-group-ingress](#) 和 [authorize-security-group-egress](#) 指令。對於 `--ip-permissions` 參數，請使用 `PrefixListIds` 指定字首清單的 ID。

## 子網路路由表

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 Save changes (儲存變更)。

若要使用參照路由表格中的前置碼清單 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。如果您在中建立了與 Suricata 相容的可設定狀態規則群組 AWS Network Firewall，您可以參考規則群組中的前置詞



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 機架本地閘道

每個 AWS Outposts 機架都提供一個本機閘道，可讓您將 Outpost 資源與內部部署網路連線。您可以將經常在前置詞清單中使用的 CIDR 分組，並在本機閘道路由表中將此清單作為路由目標參照。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路由表路由](#)。

## AWS IP 位址範圍

AWS 以 JSON 格式發佈其目前 IP 位址範圍。有了這些信息，您可以識別來自的流量 AWS。您也可以使用此資訊來允許或拒絕往返某些 AWS 服務的流量。

### Note

- [只有部分 AWS 服務 IP 位址範圍會以 ip-ranges.json 發佈；我們會針對客戶通常想要執行輸出篩選的服務發佈 IP 位址範圍。](#)
- 服務可能會使用 IP 位址範圍與其他服務通訊，或者服務可能會使用 IP 範圍與客戶網路通訊。

若要檢視目前範圍，請下載 .json 檔案。為了保持歷史記錄，請在系統上儲存連續版本的 .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。

您 AWS 透過自攜 IP 位址 (BYOIP) 所帶來的 IP 位址範圍不會包含在檔案中 .json。

或者，某些服務會使用 AWS-managed 前置詞清單發佈其位址範圍。如需詳細資訊，請參閱 [the section called “可用的 AWS託管前綴列表”](#)。

## 目錄

- [下載](#)
- [語法](#)
- [範圍重疊](#)
- [篩選 JSON 檔案](#)
- [實作出口控制](#)
- [AWS IP 位址範圍通知](#)
- [版本備註](#)
- [進一步了解](#)

## 下載

下載 [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。

## 語法

`ip-ranges.json` 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

發佈日期和時間，以 UTC YY-MM-DD-格式表示。hh-mm-ss

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 可能會在更具體的範圍內公告前綴。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 可能會在更具體的範圍內公告前綴。

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 AWS 通告 IP 位址的唯一可用區域或本機區域集，或 GLOBAL。GLOBAL 服務的流量可能會吸引或來自多個 (最多所有) 可用區域或 Local Zones (通告 IP 位址)。

類型：字串

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

`region`

區 AWS 域或 GLOBAL。GLOBAL 服務流量可以吸引到多個 (最多所有) AWS 區域或來自多個區域。

類型：字串

有效值：`af-south-1 | ap-east-1 | 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 | ca-central-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 | 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"`

`service`

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)。

類型：字串

有效值：`AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | 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。

## 篩選 JSON 檔案

您可以下載命令列工具，協助您篩選並顯示所要尋找的資訊。

### Windows

[AWS Tools for Windows PowerShell](#) 包含的 `Get-AWSPublicIpAddressRange` 可剖析此 JSON 檔案。以下範例示範其用途。如需詳細資訊，請參閱[查詢公用 IP 位址範圍 AWS](#)和 [Get-AWSPublicIpAddressRange](#)。

#### Example 1. 取得建立日期

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

```
Wednesday, August 22, 2018 9:22:35 PM
```

#### Example 2. 取得特定區域的資訊

```
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
...			

#### Example 3. 取得所有 IP 地址

```
PS C:\> (Get-AWSPublicIpAddressRange).IpPrefix
```

```
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
2406:da00:ff00::/64
2600:1fff:6000::/40
2a01:578:3::/64
2600:9000::/28
```

#### Example 4. 取得所有 IPv4 地址

```
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
...
```

#### Example 5. 取得所有 IPv6 地址

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

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

#### Example 6. 取得適用於特定服務的所有 IP 地址

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey CODEBUILD | select IpPrefix

IpPrefix
-----
52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
```

```
...
```

## Linux

以下命令範例使用 [jq 工具](#) 來剖析 JSON 檔案的本機副本。

### Example 1. 取得建立日期

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

```
"2016-02-18-17-22-15"
```

### Example 2. 取得特定區域的資訊

```
$ 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"
},
...
```

### Example 3. 取得所有 IPv4 地址

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

```
23.20.0.0/14
27.0.0.0/22
```

```
43.250.192.0/24
...
```

#### Example 4. 取得所有 IPv6 地址

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

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

#### Example 5. 取得適用於特定服務的所有 IPv4 地址

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

52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

#### Example 6. 取得特定區域中適用於特定服務的所有 IPv4 地址

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

34.228.4.208/28
```

#### Example 7. 取得特定網路邊界群組的資訊

```
$ jq -r '.prefixes[] | select(.region=="us-west-2") |
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
...
```

## 實作出口控制

[若要允許您使用某個 AWS 服務建立的資源只能存取其他 AWS 服務，您可以使用 ip-ranges.json 檔案中的 IP 位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

部分以 EC2 為基礎建置的 AWS 服務，並使用 EC2 IP 位址空間。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。

## AWS IP 位址範圍通知

每當 AWS IP 位址範圍發生變更時，我們就會傳送通知給 AmazonIpSpaceChanged 主題的訂閱者。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。

如果您希望在 AWS IP 位址範圍發生變更時收到通知，可以按照以下方式訂閱以使用 Amazon SNS 接收通知。

## 訂閱 AWS IP 位址範圍通知

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 位址範圍通知

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 Amazon SNS 的詳細資訊，請參閱 [Amazon Simple Notification Service 開發人員指南](#)。

## 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。

描述	發行日期
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
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

描述	發行日期
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

## 進一步了解

- 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 位址範圍](#)
- 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](#)

## 將 IPv6 支援新增至您的 VPC

如果您有僅支援 IPv4 的現有 VPC，以及子網路中設定為僅使用 IPv4 的資源，則可以為您的 VPC 和資源新增 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”](#)。
- 在開始使用 IPv6 之前，請確定您已閱讀適用於 Amazon VPC 人雲端的 IPv6 定址功能：[比較 IPv4 和 IPv6](#)

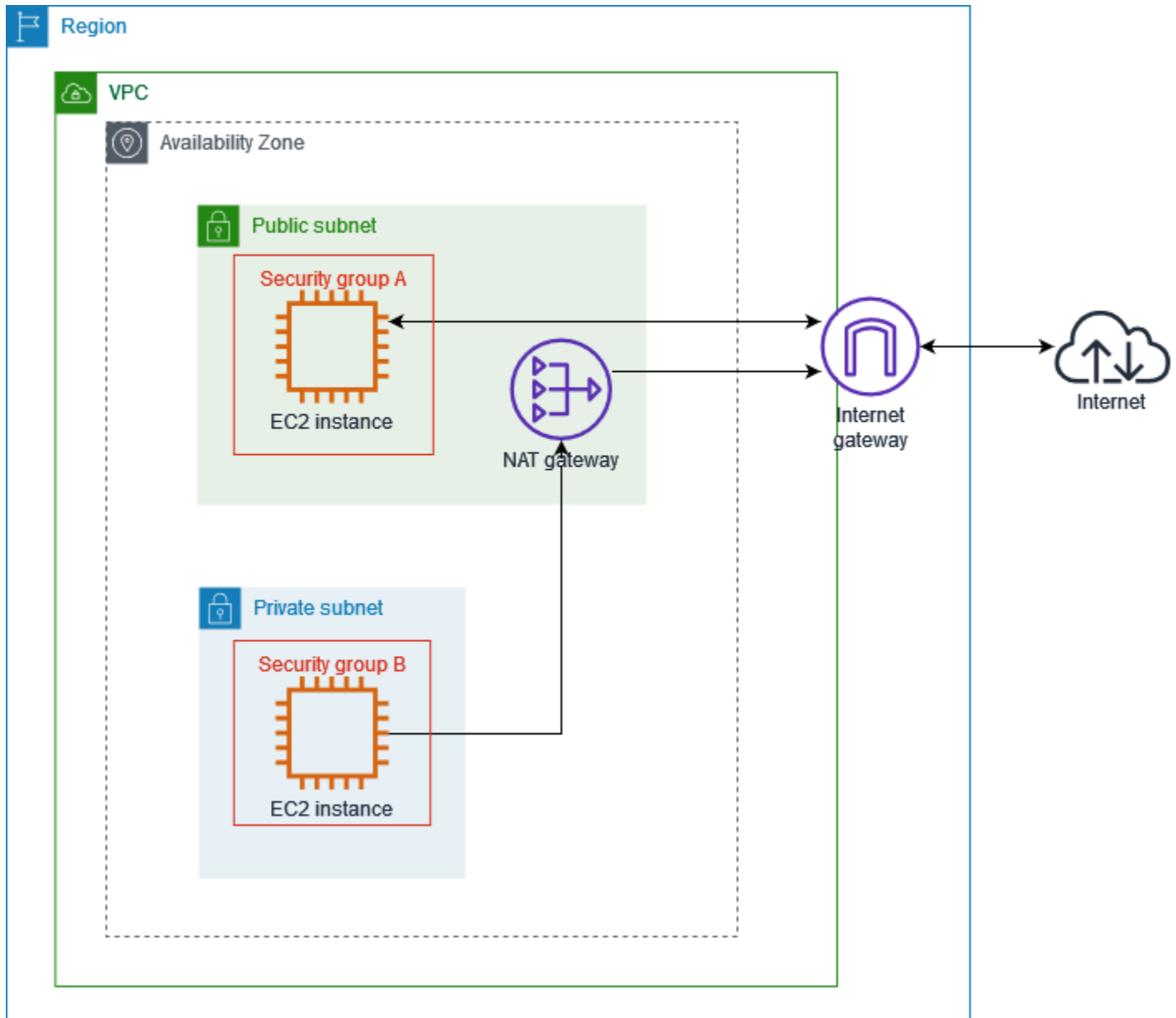
## 處理

下表概述了為您的 VPC 啟用 IPv6 的流程。

步驟	備註
<a href="#">步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網的關聯</a>	將 Amazon 提供的或 BYOIP IPv6 CIDR 區塊與 VPC 和子網建立關聯。
<a href="#">步驟 2：更新路由表</a>	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。
<a href="#">步驟 3：更新安全群組規則</a>	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。
<a href="#">步驟 4：將 IPv6 地址指派給執行個體</a>	將 IPv6 地址從子網的 IPv6 地址範圍指派給執行個體。

## 範例：在含公有和私有子網的 VPC 中啟用 IPv6

在本範例中，VPC 具有公有和私有子網。私有子網中的資料庫執行個體可在 VPC 中透過 NAT 閘道具有與網際網路的傳出通訊。公有子網中的公開 Web 伺服器透過網際網路閘道具有網際網路存取。下圖呈現 VPC 的架構。



Web 伺服器的安全群組 (例如使用安全群組 ID sg-11aa22bb11aa22bb1) 具有下列傳入規則：

類型	通訊協定	連接埠範圍	來源	註解
所有流量	全部	全部	sg-33cc44 dd33cc44dd3	允許來自與 sg-33cc44 dd33cc44dd3 (資料庫執行個體) 相關聯之執行個體

類型	通訊協定	連接埠範圍	來源	註解
				的所有流量傳入存取。
HTTP	TCP	80	0.0.0.0/0	允許來自網際網路且透過 HTTP 的傳入流量。
HTTPS	TCP	443	0.0.0.0/0	允許來自網際網路且透過 HTTPS 的傳入流量。
SSH	TCP	22	203.0.113 .123/32	允許從本機電腦執行傳入 SSH 存取；例如，當您需要連線至執行個體以執行管理任務時。

資料庫執行個體的安全群組 (例如使用安全群組 ID sg-33cc44dd33cc44dd3) 具有下列傳入規則：

類型	通訊協定	連接埠範圍	來源	註解
MySQL	TCP	3306	sg-11aa22 bb11aa22bb1	允許來自與 sg-11aa22 bb11aa22bb1 (Web 伺服器執行個體) 相關聯之執行個體的 MySQL 流量傳入存取。

兩個安全群組的預設傳出規則都允許所有傳出 IPv4 流量，而且沒有其他傳出規則。

Web 伺服器是 t2.medium 執行個體類型。資料庫伺服器是 m3.large。

您想要啟用 VPC 和資源的 IPv6 功能，而且想要它們以雙堆疊模式操作；換句話說，您想要在 VPC 中的資源與透過網際網路的資源之間同時使用 IPv6 和 IPv4 定址。

## 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。在「網路邊界群組」中，選擇通 AWS 告 IP 位址的群組。
  - 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. 前往 <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。

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 [使用網路 ACL](#)。

## 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 地址會指派給執行個體的主要網路界面 (eth0)。如需詳細資訊，請參閱 [Amazon EC2 使用者指南中的指派 IPv6 地址給執行個體](#)。

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 使用者指南中的使用安全殼層用戶端 Connect 到 Linux 執行個體](#)，或使用 Amazon EC2 [使用者指南中的 IPv6 地址 Connect 到 Windows 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。

## 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 地址的新格式為 IPv6，可提供比 IPv4 更大的地址空間。


























AWS 服務對 IPv6 的支援包括雙堆疊設定 (IPv4 和 IPv6) 或僅 IPv6 組態的支援。例如，虛擬私有雲 (VPC) 是您可以在其中啟動 AWS 資源 AWS 雲端的邏輯隔離部分。在 VPC 中，您可以建立僅限 IPv4、雙堆疊或僅限 IPv6 的子網路。


AWS 服務支持通過公共端點訪問。有些 AWS 服務還支持使用提供支持的私有端點進行訪問 AWS PrivateLink。AWS 服務可以通過其私有端點支持 IPv6，即使它們不通過其公共端點支持 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
























下表列出提供雙堆疊支援、僅 IPv6 支援，以及支援 IPv6 的端點。AWS 服務我們會在推出其他 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 <sup>1</sup>
AWS App Mesh	 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 <sup>1</sup>
Amazon AppStream 2.0	 是	 否	 否	 否
Amazon Athena	 是	 否	 是	 <u>是</u>
Amazon Aurora	 <u>是</u>	 否	 是	 否
AWS Cloud9	 <u>是</u>	 否	 是	
Amazon CloudFront	 <u>是</u>	 否	 否	
Amazon CloudWatch 日誌		 <u>是</u> 否	 是	 否
AWS Cloud Map	 <u>是</u>	 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 <sup>1</sup>
AWS 雲廣域網路	 是	 否	 是	 否
Amazon Cognito	 是	 否	 是	
AWS Database Migration Service	 <u>是</u>	 否	 否	 否
AWS Direct Connect	 是	 是	 否	
Amazon EC2	 <u>是</u>	 是	 <u>是</u>	 否
Amazon ECS	 <u>是</u>	 否	 否	 否
Amazon EKS	<u>節點：是/豆</u> <u>英：否</u>	<u>豆莢：是/節</u> <u>點：否</u>	 否	 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 <sup>1</sup>
Elastic Load Balancing	負載平衡器： 是 目標群組： 否	負載平衡器： 否 目標群組： 是	 否	 否
Amazon ElastiCache	 <u>是</u>	 是	 否	 否
AWS Fargate	 <u>是</u>	 否	 否	 否
AWS Global Accelerator	 <u>是</u>	 否	 否	
AWS Glue	 否	 否	 否	 是
AWS IoT	 是	 否	 <u>是</u>	 否
AWS Lake Formation	 否	 否	 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 <sup>1</sup>
AWS Lambda	 <u>是</u>	 否	 <u>是</u>	 否
Amazon Lightsail	 <u>是</u>	 <u>是</u>	 否	
AWS Network Firewall	 <u>是</u>	 <u>是</u>	 否	
Amazon OpenSearch 服務	 <u>是</u>	 否	 是	 否
AWS PrivateLink	 是	 是	 是	
Amazon RDS	 <u>是</u>	 否	 是	 否
Amazon Route 53	 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 <sup>1</sup>
Amazon S3	 <u>是</u>	 否	 <u>是</u>	 否
AWS Secrets Manager	 是	 否	 <u>是</u>	 否
AWS Shield	 是	 是	 否	
AWS Site-to-Site VPN	 <u>是</u>	 否	 <u>是</u>	 否
AWS Transit Gateway	 是	 否	 是	 否
Amazon VPC	 <u>是</u>	 是	 <u>是</u>	 否
AWS WAF	 <u>是</u>	 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 <sup>1</sup>
Amazon WorkSpaces	 是	 否	 否	 否

<sup>1</sup> 空白儲存格表示服務未與整合 [AWS PrivateLink](#)。

## 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。

### 聯網與內容交付

- Amazon VPC 支援建立僅限 IPv6 子網路。
- Amazon VPC 人雲端可支援您的子網路上的 DNS64 和 NAT 閘道上的 NAT64，協助 IPv6 AWS 資源與 IPv4 資源進行通訊。

### 安全性、身分與合規

- AWS Identity and Access Management (IAM) 支援身分與存取權管理政策中的 IPv6 位址。
- Amazon Macie 可在個人身分識別資訊 (PII) 中支援 IPv6 地址。

### 管理與管控

- AWS CloudTrail 記錄包括來源 IPv6 資訊。
- AWS CLI v2 支援透過 IPv6 連線進行下載，適用於僅限 IPv6 的用戶端。

## 進一步了解

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

# Virtual Private Cloud (VPC)

virtual private cloud (虛擬私有雲端，VPC) 是您的 AWS 帳戶 帳戶所專用的虛擬網路。其在邏輯上與 AWS 雲端的其他虛擬網路隔離。您可以在您的 VPC 中啟動 AWS 資源 (例如 Amazon EC2 執行個體)。

您的帳戶在每個 AWS 區域都包含一個預設 VPC。您也可以建立其他 VPC。

## 目錄

- [VPC 基本概念](#)
- [預設 VPC](#)
- [建立 VPC](#)
- [設定您的 VPC](#)
- [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](#)
- [將 VPC 擴展至本機區域、Wavelength 區域或 Outpost](#)
- [刪除您的 VPC](#)

## 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。如需更多詳細資訊，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

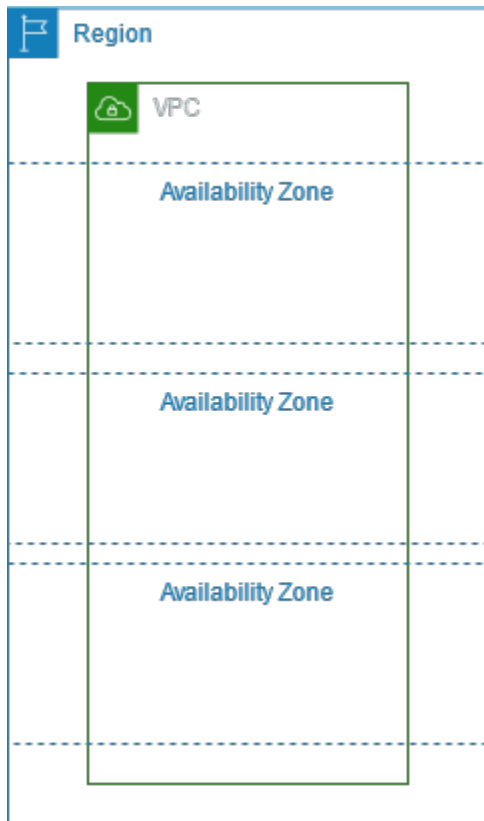
當您建立 VPC 時，您可按照下列方式指定其 IP 地址：

- 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。

如需更多詳細資訊，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](#)

## 預設 VPC

當開始使用 Amazon VPC 時，您會在每個 AWS 區域擁有預設 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。您也可以使用預設 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](#)
- [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](#)

## 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：

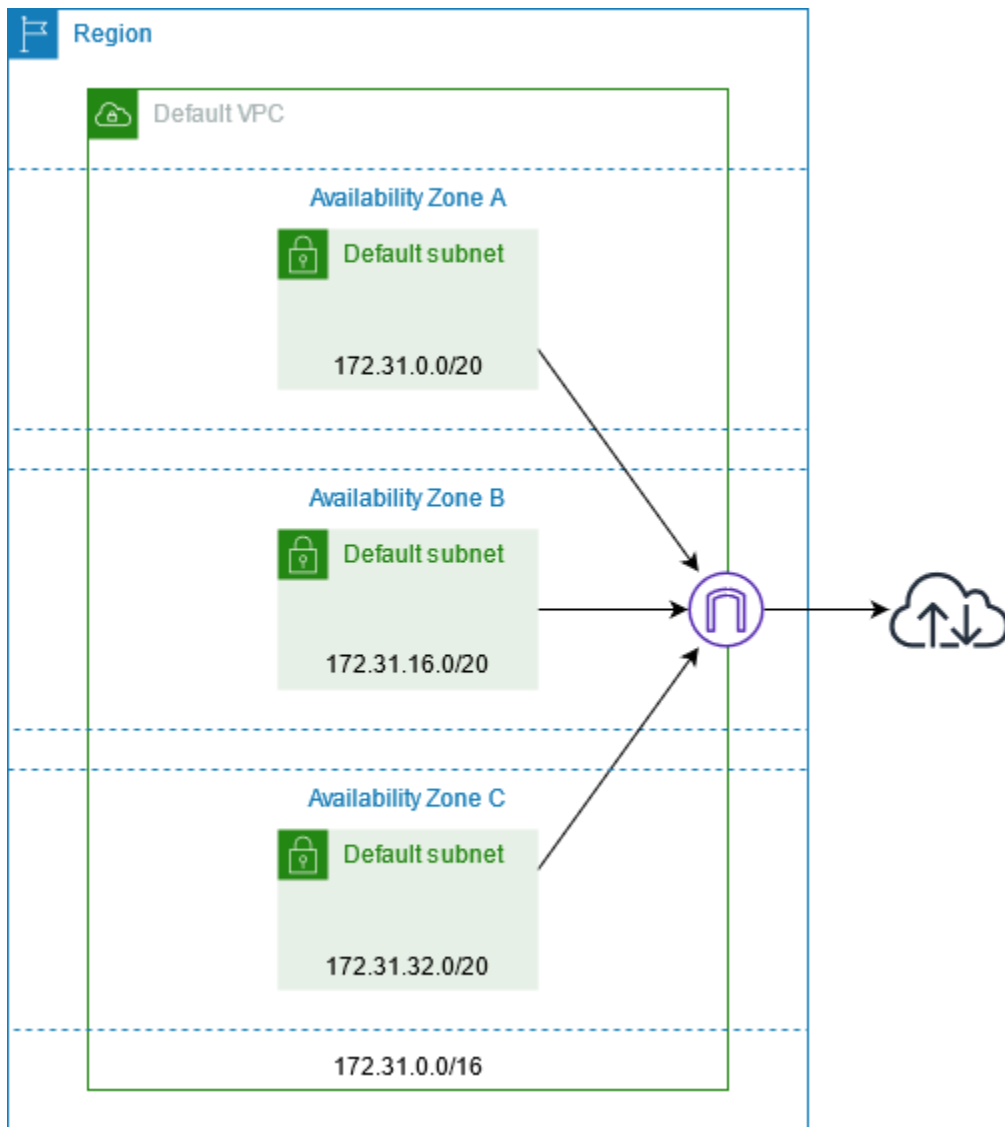
- 建立大小為 /16 IPv4 CIDR 區塊 (172.31.0.0/16) 的 VPC。這最多可提供 65,536 個私有 IPv4 地址。
- 在每個可用區域中建立大小為 /20 的預設子網路。每個子網路最多可提供 4,096 個地址，其中一些預留供我們使用。
- 建立 [網際網路閘道](#)，並將它連線到您的預設 VPC。

- 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。
- 建立您 AWS 帳戶預設 DHCP 選項集與您預設 VPC 的關聯。

 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。

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。

目的地	目標
172.31.0.0/16	區域
0.0.0.0/0	<i>internet_gateway_id</i>

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 連接。
- 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 [修改您子網路的公有 IPv4 定址屬性](#)。

有時候，AWS 會在區域中新增新的可用區域。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。但若您修改了預設的 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](#)。

## 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

您可以在沒有預設子網路的可用區域中建立預設子網路。例如，如果您已刪除預設的子網路，或如果 AWS 已新增新的可用區域，但並未在您預設 VPC 的該區域自動建立預設子網路，您可能想要建立預設子網路。

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 [將 IPv6 CIDR 區塊新增至您的子網路](#)。

您無法使用 AWS Management Console 建立預設子網路。

使用 AWS CLI 建立預設子網路

使用 [create-default-subnet](#) AWS CLI 命令，並指定建立子網路的可用區域。

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

下列為範例輸出。

```
{
  "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
  }
}
```

如需有關設定 AWS CLI 的詳細資訊，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。如需詳細資訊，請參閱 [修改您子網路的公有 IPv4 定址屬性](#)。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

- [VPC 組態選項](#)
- [建立 VPC 以及其他 VPC 資源](#)
- [僅建立 VPC](#)
- [使用建立 VPC AWS CLI](#)

如需有關檢視或修改 VPC 的資訊，請參閱 [the section called “設定您的 VPC”](#)。

## 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

您 VPC 中的 IP 地址範圍。您可以在子網路中啟動 EC2 執行個體等 AWS 資源。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。如果您選擇租用 VPCDefault，啟動到此 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已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。如果您使用的是 AWS Outposts，您的 Outpost 需要私人連接；您必須使用Default租賃。

## 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. 前往 <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，或清除它以提供您自己的名稱標籤給 VPC 資源。
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。如果您選擇要使用 VPC 的租用 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[使用已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。如果您使用的是 AWS Outposts，您的 Outpost 需要私人連接；您必須使用 Default 租賃。
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，讓我們為您 AWS 選擇它們。
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，讓我們為您 AWS 選擇它們。
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。如需詳細資訊，請參閱[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 VPC 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. 前往 <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 VPC 功能，可讓您更輕鬆地為工作負載規劃、追蹤和監控 IP 位址。AWS 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)。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。對於網路邊界群組，選取通 AWS 告 IP 位址的群組。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。如需將自己的 IP 位址範圍帶到的詳細資訊 AWS，請參閱 Amazon EC2 使用者指南中的[攜帶您自己的 IP 位址 \(BYOIP\)](#)。您可以使用下列 CIDR 區塊選項為 VPC 佈建 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。如果您選擇租用 VPCDefault，啟動到此 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已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。如果您使用的是 AWS Outposts，您的 Outpost 需要私人連接；您必須使用Default租賃。
  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。如需詳細資訊，請參閱 [建立子網](#)。

## 使用建立 VPC AWS CLI

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。配置時 AWS CLI，系統會提示您輸入身份證明。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}]
```

若要建立 VPC 加上 VPC 資源，請使用 AWS CLI

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. 使用下列建立 NAT 閘道指令，在公用子網路中建立 [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
```

# 設定您的 VPC

使用下列程序檢視和設定虛擬私有雲端 (VPC)。

## 任務

- [檢視您的 VPC 相關詳細資訊](#)
- [視覺化 VPC 中的資源](#)
- [將 IPv4 CIDR 區塊新增至您的 VPC](#)
- [將 IPv6 CIDR 區塊新增至您的 VPC](#)
- [從您的 VPC 中移除 IPv4 CIDR 區塊](#)
- [從您的 VPC 中移除 IPv6 CIDR 區塊](#)

如需有關建立或刪除 VPC 的詳細資訊，請參閱[the section called “建立 VPC”](#)或[the section called “刪除您的 VPC”](#)。

## 檢視您的 VPC 相關詳細資訊

使用下列步驟來檢視 VPC 的詳細資訊。

若要使用主控台檢視 VPC 詳細資訊

1. 前往 <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，然後選擇檢視詳細資訊，以檢視 VPC 的組態詳細資訊。

若要 VPC 用 AWS CLI

使用 [describe-vpcs](#) 命令。

如何跨所有區域檢視所有 VPC

前往 <https://console.aws.amazon.com/ec2globalview/home> 開啟 Amazon EC2 全域檢視主控台。如需詳細資訊，請參閱 [Amazon EC2 使用者指南中的使用 Amazon EC2 全域檢視列出和篩選資源](#)。

## 視覺化 VPC 中的資源

透過下列步驟，使用資源映射索引標籤查看 VPC 中資源的視覺化表示。下列資源會顯示在資源映射中：

- VPC
- 子網
  - 可用區域以字母表示。
  - 公用子網路是綠色的。
  - 私人子網路是藍色的。
- 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. 前往 <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，則會有一個閘道端點資源，其中包含您可以使用該端點連線到的 AWS 服務名稱 (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。

## 將 IPv4 CIDR 區塊新增至您的 VPC

依預設，您的 VPC 最多可以有五個 IPv4 CIDR 區塊，但此限制可調整。如需詳細資訊，請參閱 [Amazon VPC 配額](#)。如需 VPC 的 IPv4 CIDR 區塊限制的相關資訊，請參閱 [VPC CIDR 區塊](#)。

如何使用主控台將 IPv4 CIDR 區塊新增至 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 Your VPCs (您的 VPC)。
3. 選取 VPC，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 選擇 Add new IPv4 CIDR (新增新的 IPv4 CIDR)。
5. 對於 IPv4 CIDR 區塊，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。
6. 選擇 Save (儲存)，然後選擇 Close (關閉)。
7. 將 IPv4 CIDR 區塊新增至 VPC 後，您可以建立使用全新 CIDR 區塊的子網路。如需詳細資訊，請參閱 [建立子網](#)。

若要將 IPv4 CIDR 區塊與 VPC 相關聯，請使用 AWS CLI

使用 [associate-vpc-cidr-block](#) 命令。

## 將 IPv6 CIDR 區塊新增至您的 VPC

依預設，您的 VPC 最多可以有五個 IPv6 CIDR 區塊，但此限制可調整。如需詳細資訊，請參閱 [Amazon VPC 配額](#)。如需 VPC 的 IPv6 CIDR 區塊限制的相關資訊，請參閱 [VPC CIDR 區塊](#)。

如何使用主控台將 IPv6 CIDR 區塊新增至 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 Your VPCs (您的 VPC)。
3. 選取 VPC，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 選擇 Add new IPv6 CIDR (新增新的 IPv6 CIDR)。
5. 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)。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。對於網路邊界群組，選取通 AWS 告 IP 位址的群組。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。如需將自己的 IP 地址範圍帶到的詳細資訊 AWS，請參閱 [Amazon EC2 使用者指南中的在 Amazon EC2 中使用自己的 IP 地址 \(BYOIP\)](#)。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)。
6. 選擇選取 CIDR，然後選擇關閉。
  7. 將 IPv6 CIDR 區塊新增至 VPC 後，您可以建立使用全新 CIDR 區塊的子網路。如需詳細資訊，請參閱 [建立子網](#)。

使用將 IPv6 CIDR 區塊與 VPC 相關聯 AWS CLI

使用 [associate-vpc-cidr-block](#) 命令。

## 從您的 VPC 中移除 IPv4 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。

使用主控台將 CIDR 區塊從 VPC 中移除

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. 在 VPC IPv4 CIDR 下，選擇移除以移除 CIDR。
5. 選擇關閉。

若要取消 IPv4 CIDR 區塊與 VPC 的關聯，請使用 AWS CLI

使用 [disassociate-vpc-cidr-block](#) 命令。

## 從您的 VPC 中移除 IPv6 CIDR 區塊

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。

使用主控台將 IPv6 CIDR 區塊從 VPC 中移除

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)、Edit CIDRs (編輯 CIDR)。
4. 在 IPv6 CIDR 下，選擇移除以移除 IPv6 CIDR 區塊。
5. 選擇關閉。

若要取消 IPv6 CIDR 區塊與 VPC 的關聯，請使用 AWS CLI

使用 [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。
- 對於僅限 IPv4 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 伺服器將會傳回名稱伺服器做為名稱伺服器。如果選項集中缺少「AmazonProvidedDNS」，則無論選項集中是否提及其他 IPv4 名稱伺服器，IPv4 DHCP 伺服器都不會傳回位址。

亞馬遜 DHCP 伺服器也可以使用前置詞委派為 VPC 中的網路界面提供完整的 IPv4 或 IPv6 前置詞 (請參閱 Amazon EC2 使用者指南中的指派首碼給 Amazon EC2 [網路界面](#))。DHCP 回應中不提供 IPv4 前綴委派。指派給界面的 IPv4 首碼可以使用 IMDS 擷取 (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 人雲端未設定 DHCP 選項：

- 對於在 [Nitro 系統上構建的 EC2 實例](#)，AWS 將配置 169.254.169.253 為默認域名伺服器。
- 對於在 [Xen 上建置的 EC2 執行個體](#)，不會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

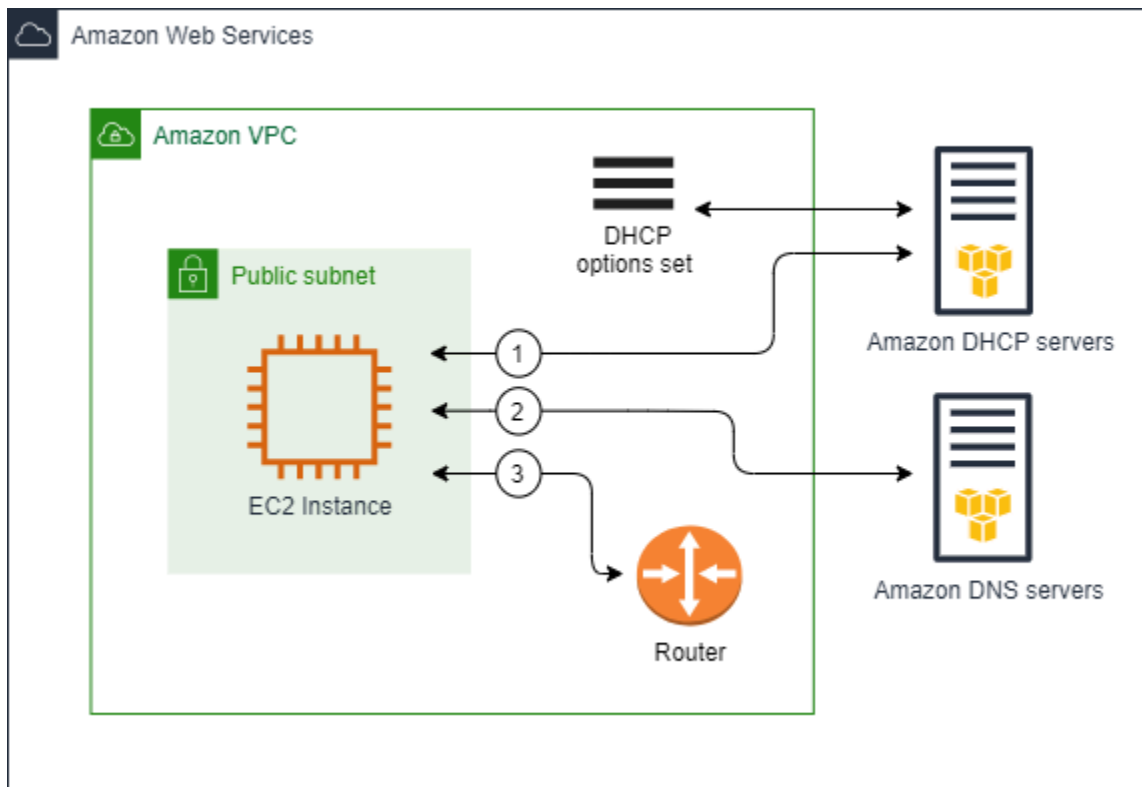
預設 DHCP 選項集包含以下設定：

- 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 偏好租用時間：指派 IPv6 的執行中執行個體經過 DHCPv6 租用續約的頻率。預設租用時間為 140 秒。租用續約通常會在一半的租用時間過去時發生。

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。

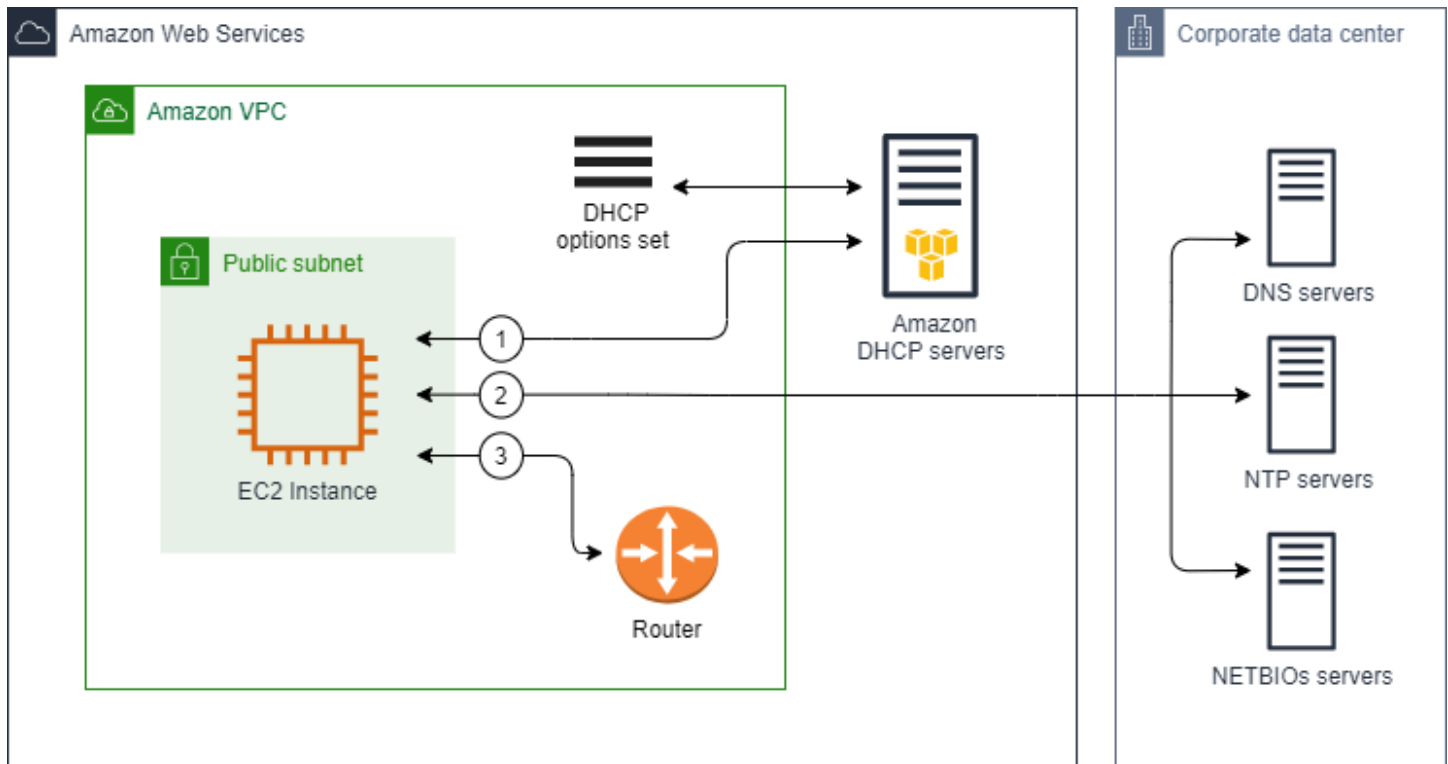


## 自訂 DHCP 選項集

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 偏好租用時間 (選擇性)**：指派 IPv6 的執行中執行個體經過 DHCPv6 租用續約的頻率值 (以秒、分鐘、小時或年為單位)。可接受的值介於 140 到 42967295 秒之間 (約 138 年)。如果未輸入任何值，則預設租用時間為 140 秒。如果您對 EC2 執行個體使用長期定址，則可以增加租用時間並避免頻繁的租用續約請求。租用續約通常會在一半的租用時間過去時發生。

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

- [檢視 DHCP 選項集](#)
- [建立 DHCP 選項集](#)
- [變更與 VPC 關聯的選項集](#)
- [刪除 DHCP 選項集](#)

## 檢視 DHCP 選項集

您可以檢視 DHCP 選項集，如下所示。對於預設 DHCP 選項集，唯一具有值的設定是網域名稱和網域名稱伺服器。

### 使用主控台檢視 DHCP 選項集

1. 前往 <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 DHCP 選項集的 ID，開啟其詳細資訊頁面。

### 使用命令列檢視您的 DHCP 選項集

如需有關這些命令列介面的詳細資訊，請參閱[使用 Amazon VPC](#)。

- [describe-dhcp-options](#) (AWS CLI)
- [Get-EC2DhcpOption](#) (AWS Tools for Windows PowerShell)

## 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. 前往 <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。

- **Domain name (網域名稱) (選用)**：輸入用戶端在透過網域名稱系統解析主機名稱時應使用的網域名稱。如果您不使用 AmazonProvided DNS，您的自訂網域名稱伺服器必須適當地解析主機名稱。如果您使用 Amazon 路線 53 私有託管區域，則可以使用 AmazonProvided DNS。如需詳細資訊，請參閱 [VPC 的 DNS 屬性](#)。

部分 Linux 作業系統接受多個網域名稱，以空格分隔。不過，Windows 和其他 Linux 作業系統會將這個值視為單一網域，這會導致非預期的行為。如果您的 DHCP 選項集與執行作業系統的執行個體的 VPC 相關聯，而 VPC 會將該值視為單一網域，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 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，請務必為網域名稱伺服器值指定您自己的 DNS 伺服器或 Amazon DNS 伺服器 (AmazonProvidedDNS)。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 Amazon 時間同步服務的詳細資訊，請參閱 Amazon EC2 使用者指南中的 [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** (point-to-point 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 偏好租用時間 (選擇性)：指派 IPv6 的執行中執行個體經過 DHCPv6 租用續約的頻率值 (以秒、分鐘、小時或年為單位)。可接受的值介於 140 到 2147483647 秒之間 (約 68 年)。如果未輸入任何值，則預設租用時間為 140 秒。如果您對 EC2 執行個體使用長期定址，則可以增加租用時間並避免頻繁的租用續約請求。租用續約通常會在一半的租用時間過去時發生。

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

如需有關這些命令列介面的詳細資訊，請參閱 [使用 Amazon VPC](#)。

- [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

如需有關這些命令列介面的詳細資訊，請參閱[使用 Amazon VPC](#)。

- [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. 前往 <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

如需有關這些命令列介面的詳細資訊，請參閱[使用 Amazon VPC](#)。

- [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

- [Amazon DNS 伺服器](#)
- [DNS 主機名稱](#)
- [VPC 中的 DNS 屬性](#)
- [DNS 配額](#)
- [檢視 EC2 執行個體的 DNS 主機名稱](#)
- [檢視和更新 VPC 的 DNS 屬性](#)
- [私有託管區域](#)

## Amazon DNS 伺服器

Route 53 解析器 (也稱為「Amazon DNS 服務器」或「AmazonProvidedDNS」) 是內置在一個區域的每個可用區域中的 DNS 解析器服務。AWS 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 fd00:ec2::253 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[連結本機位址](#)進行 DNS 查詢。這些查詢會私下傳送到 Route 53 解析器，並且在網路上看不到。在僅限 IPv4 的子網路中，只要「AmazonProvidedDNS」是 DHCP 選項集中的名稱伺服器，就可以存取 IPv4 連結本機位址 (169.254.169.253)。

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「[EC2 執行個體命名](#)」。

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。

## 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 中的 DNS 屬性](#)。

啟用 Amazon 提供的 DNS 伺服器後，會指派 DNS 主機名稱並解析如下。

### 私有 IP DNS 名稱 (僅限 IPv4)

您可以使用私有 IP DNS 名稱 (僅限 IPv4) 主機名稱，在相同 VPC 的執行個體之間進行通訊。您可以解析其他 VPC 中其他執行個體的私有 IP DNS 名稱 (僅限 IPv4) 主機名稱，只要執行個體位於相同 AWS 區域，且其他執行個體的主機名稱位於[RFC 1918](#)、和所定義的私人位址空間範圍內。10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

### 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「[EC2 執行個體主機名稱類型](#)」。

### 公有 IPv4 DNS

公有 (外部) IPv4 DNS 主機名稱會對 us-east-1 區域採用 `ec2-public-ipv4-address.compute-1.amazonaws.com` 格式，對其他區域則採用 `ec2-public-ipv4-address.region.compute.amazonaws.com` 格式。Amazon DNS 伺服器可將公有 DNS 主機名稱解析為執行個體網路外部的執行個體公有 IPv4 地址，以及執行個體網路內部的執行個體私有 IPv4 地址。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [公用 IPv4 地址和外部 DNS 主機名稱](#)。

## VPC 中的 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	描述
<code>enableDnsHostnames</code>	<p>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。</p> <p>此屬性的預設值為 <code>false</code>，除非 VPC 為預設 VPC。請注意以下此屬性的規則和考量事項。</p>
<code>enableDnsSupport</code>	<p>確定 VPC 是否支援透過 Amazon 提供的 DNS 伺服器進行 DNS 解析。</p> <p>如果此屬性為 <code>true</code>，對 Amazon 提供的 DNS 伺服器的查詢成功。如需詳細資訊，請參閱 <a href="#">Amazon DNS 伺服器</a>。</p> <p>此屬性的預設值為 <code>true</code>。請注意以下此屬性的規則和考量事項。</p>

### 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。
  - Amazon Route 53 Resolver 服務器可以解析亞馬遜提供的私有 DNS 主機名。
- 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。

- Amazon Route 53 Resolver 無法解析亞馬遜提供的私有 DNS 主機名。
- 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。如果您未使用 Amazon 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`。
- Amazon Route 53 Resolver [可以將所有位址空間的私人 DNS 主機名稱解析為私有 IPv4 位址，包括 VPC 的 IPv4 位址範圍超出 RFC 1918 指定的私有 IPv4 位址範圍的位址](#)。但是，如果您的 VPC 是在 2016 年 10 月之前建立，當 VPC 的 IPv4 地址範圍超出這些範圍時，Amazon 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 [AWS Support](#)。
- 如果您使用 VPC 對等互連，則必須為兩個 VPC 來啟用這兩個屬性，並且必須為對等互連啟用 DNS 解析。如需詳細資訊，請參閱[啟用 VPC 對等互連的 DNS 解析](#)。

## DNS 配額

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》。

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](#)。如需執行個體中繼資料擷取的相關資訊，請參閱 Amazon EC2 使用者指南中的擷取[執行個體](#)中

## 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。

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 中的 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. 在 <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

您可以使用下列其中一個命令。如需關於這些命令列介面的詳細資訊，請參閱 [使用 Amazon VPC](#)。

- [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

您可以使用下列其中一個命令。如需關於這些命令列介面的詳細資訊，請參閱 [使用 Amazon VPC](#)。

- [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。

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。

Details	CIDRs	Flow logs	Tags
<b>Details</b>			
VPC ID vpc-e03dd489	State Available	DNS hostnames Enabled	DNS resolution Enabled

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

您可以使用下列其中一個命令。如需關於這些命令列介面的詳細資訊，請參閱 [使用 Amazon VPC](#)。

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

使用命令列更新 VPC 的 DNS 支援

您可以使用下列其中一個命令。如需關於這些命令列介面的詳細資訊，請參閱 [使用 Amazon VPC](#)。

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

## 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`，您可以在 Route 53 中建立私有託管區域，而不是使用私有 IPv4 位址或 AWS 提供的私有 DNS 主機名稱。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`。

## 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。跨不同區域對等的 VPC 不計入此限制。

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 使用情況，使其不會超出 NAU 配額限制。如需詳細資訊，請參閱 [the section called “CloudWatch 指標”](#)。

## 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。某些 AWS 資源會以單一 NAU 單位表示，而某些資源則表示為多個 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 執行個體之網路界面的每個私有或公用 IPv4 和每個 IPv6 位址	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
每個 AZ 的閘道 Load Balancer	6
每個 AZ 的 VPC 端點	6
傳輸閘道連接	6
Lambda 函數	6
NAT 閘道	6
EFS 掛載目標	6

## 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

## 與其他帳戶共享 VPC

VPC 共用可讓多個 AWS 帳戶人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 叢集和功能 , 並將其 AWS Lambda 功能建立到共用的集中管理虛擬私有雲端 (VPC) 中。在此模型中 , 擁有 VPC (擁有者) 的帳戶與屬於相

同組織的其他帳戶 (參與者) 共用一或多個子網路。AWS Organizations 共用于網路後，參與者可以檢視、建立、修改及刪除與其共用于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。

您可以共享您的 VPC，讓需要高度裝置互連性，並且位於相同信任邊界內的應用程式可以利用 VPC 中的隱含路由。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。您可以使用傳輸閘道和 VPC 對等連線功能來互連共用 Amazon VPC AWS PrivateLink，以簡化網路拓撲。如需 VPC 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](#)。

## 內容

- [共用 VPC 必要條件](#)
- [共用于網路](#)
- [取消共用的子網路](#)
- [識別共用于網路的擁有者](#)
- [管理 VPC 資源](#)
- [擁有者和參與者的責任與權限](#)
- [AWS 資源和共用的 VPC 子網路](#)
- [VPC 共享配額](#)
- [共享公有子網路和私有子網路的範例](#)

## 共用 VPC 必要條件

- VPC 擁有者和參與者的帳戶必須由 AWS Organizations 管理。
- 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 使用指南》[AWS Organizations 中的「啟用資源共用」](#)。
- 您必須建立資源共用。您可以在建立資源共用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用。如需詳細資訊，請參閱 AWS RAM 使用指南中的 [建立資源共用](#)。

## 共用于網路

您可以與組織內的其他帳戶共用非預設子網路，如下所示。

### 使用主控台共用于網路

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

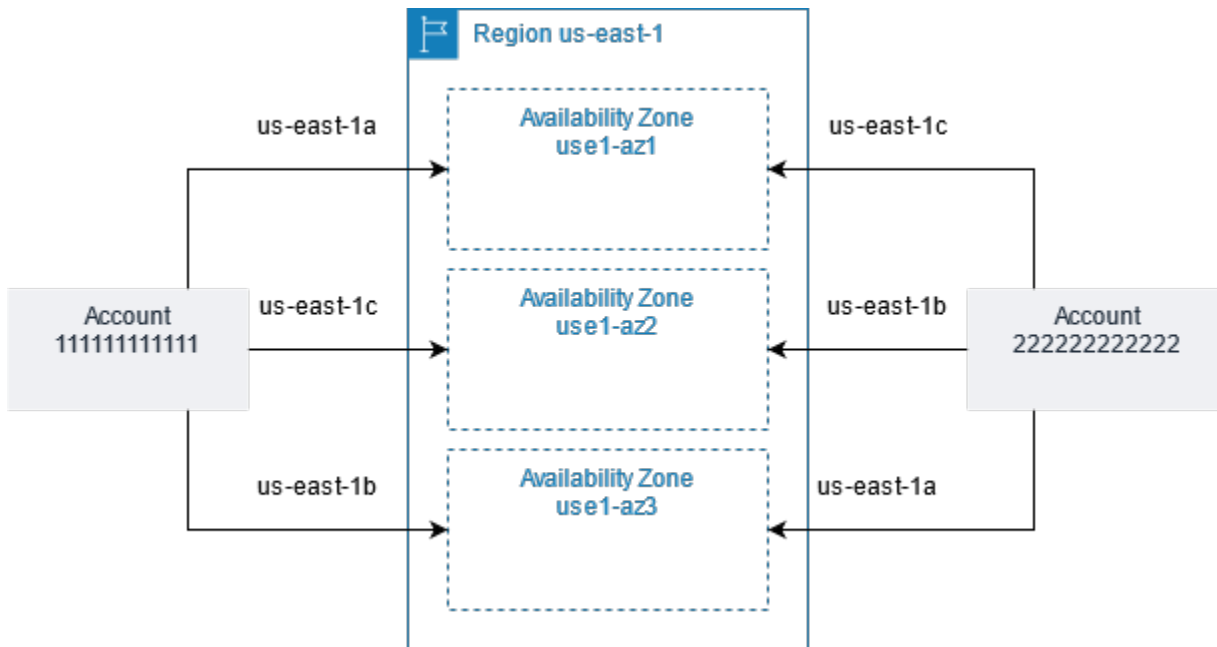
使用 [create-resource-share](#) 和 [associate-resource-share](#) 指令。

## 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，您 AWS 帳戶的可 us-east-1a 用區域可能與其他 AWS 帳戶 us-east-1a 的位置不同。

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：

- 現有參與者資源會繼續在非共用子網路中執行。AWS 具有自動/管理的工作流程 ( 例如 , Elastic Load Balancing ) 的受管理服務 ( 例如 , 彈性負載平衡 ) 可能需要對某些資源連續存取共享子網路。
- 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)。

### 若要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。

## 管理 VPC 資源

擁有者和參與者對其擁有的 VPC 資源負責。

## 擁有者資源

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、Amazon 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 共享](#)。

## 適用於擁有者及參與者的計費和計量

- 在共用 VPC 中，每位參與者支付應用程式資源的費用，包括 Amazon EC2 執行個體、Amazon 關聯式資料庫服務資料庫、Amazon Redshift 叢集和 AWS Lambda 功能。參與者還需支付與可用區間資料傳輸相關的資料傳輸費用，以及透過 VPC 對等連線、網際網路閘道和跨閘道進行資料傳輸的費用。AWS Direct Connect
- VPC 擁有者需支付 NAT 閘道、虛擬私有閘道、傳輸閘道和 VPC 端點之間的小時費用 (如適用)、資料處理和資料傳輸費用。AWS PrivateLink 此外，共用 VPC 中使用的公用 IPv4 位址會向 VPC 擁有者收費。如需有關公用 IPv4 位址定價的詳細資訊，請參閱 [Amazon VPC](#) 定價頁面上的公用 IPv4 位址索引標籤。
- 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權限

使用共用 VPC 子網路時，下列責任和權限套用至 VPC 資源：

### 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、刪除或描述流程日誌。
- VPC 擁有者無法描述或刪除參與者建立的流程記錄。

## 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。參與者可以描述共用 VPC 子網路中的網際網路閘道。參與者無法描述共用 VPC 子網路中僅限輸出的網際網路閘道。

## 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 子網路中參與者所擁有的網路介面。

## 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。

## 安全群組

- 參與者可以使用他們在共用 VPC 子網路中擁有的安全性群組 (建立、刪除、描述、修改或建立輸入和出口規則)。參與者無法以任何方式使用由 VPC 擁有者建立的安全性群組。
- 參與者可以在他們擁有的安全性群組中建立規則，該群組參照屬於其他參與者或 VPC 擁有者的安全性群組，如下所示：帳戶號碼/security-group-id



- 參與者無法使用安全群組來啟動執行個體，因為安全群組屬於 VPC 擁有者或其他參與者。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。
- 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參與者建立的安全性群組。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

- 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 擁有者只能與來自 AWS 自組織相同組織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。

## AWS 資源和共用的 VPC 子網路

共用 VPC 子網路中的下列 AWS 服務 支援資源。如需有關服務如何支援共用 VPC 子網路的詳細資訊，請依照連結查看對應服務的說明文件。

- [Amazon Aurora](#)
- [AWS CodeBuild](#)
- [AWS Database Migration Service](#)
- [Amazon EC2](#)
- [Amazon Elastic Kubernetes Service](#)
- Elastic Load Balancing
  - [Application Load Balancer](#)

- [Gateway Load Balancer](#)
- [Network Load Balancer](#)
- [Amazon EMR](#)
- [AWS Glue](#)
- [AWS Lambda](#)
- AWS Network Manager
  - [AWS 雲廣域網路](#)
  - [網路存取分析器](#)
  - [Reachability Analyzer](#)
- [AWS PrivateLink<sup>†</sup>](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Redshift](#)
- [Amazon Route 53](#)
- [AWS Transit Gateway](#)
- [AWS Verified Access](#)
- Amazon VPC
  - [對等互連](#)
  - [流量鏡射](#)
- [Amazon VPC Lattice](#)

<sup>†</sup> 您可以在共用 VPC 中 PrivateLink 使用 VPC 端點連線到支援的所有 AWS 服務。如需支援的服務清單 PrivateLink，請參閱AWS PrivateLink 指南 AWS PrivateLink中[與之整合的AWS 服務](#)。

## VPC 共享配額

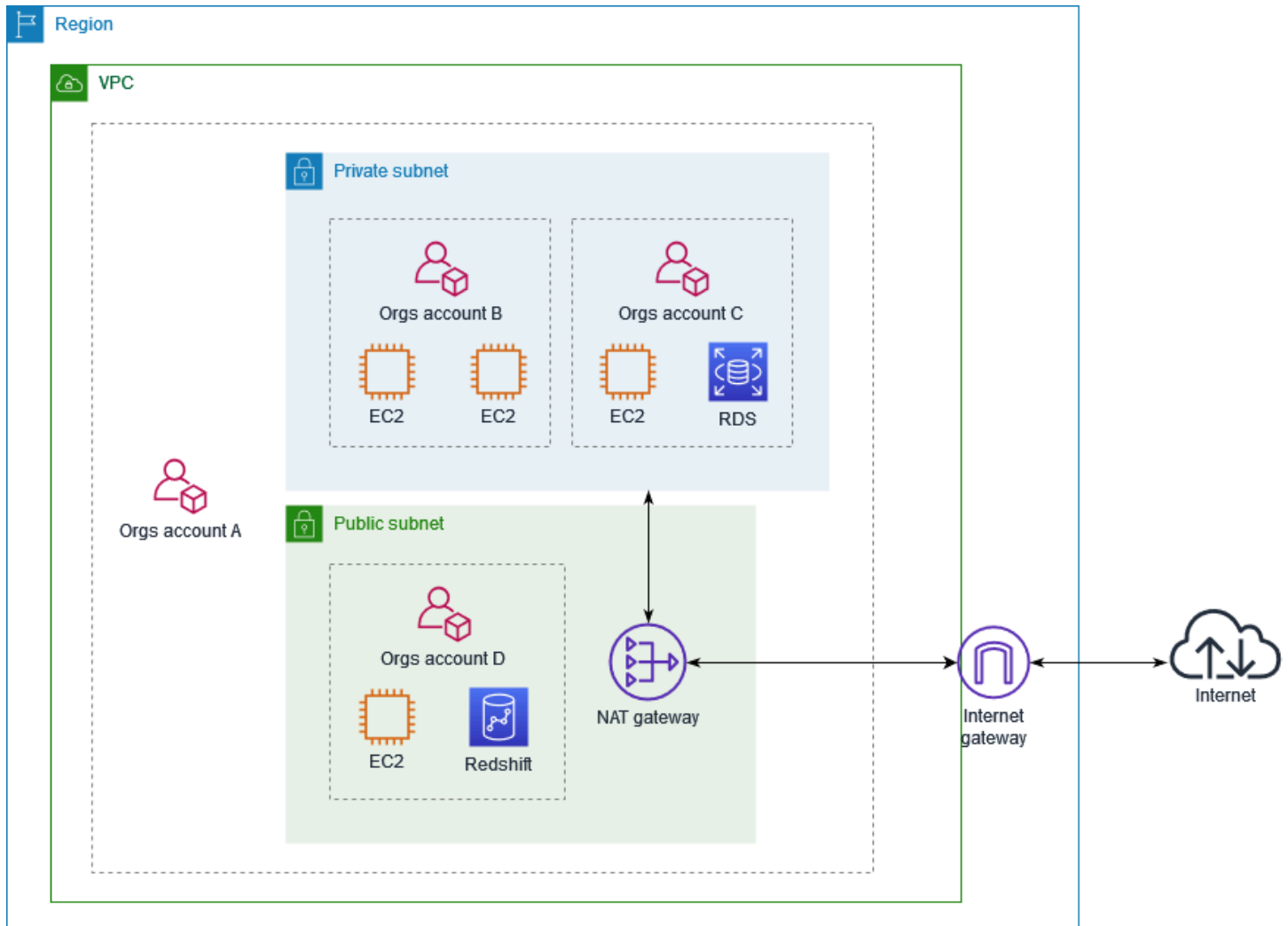
VPC 共享有相關的配額。如需更多詳細資訊，請參閱 [VPC 共享](#)。

## 共享公有子網路和私有子網路的範例

請考慮以下情況：您希望帳戶 (帳戶 A) 管理基礎設施，包括 VPC、子網路、路由表、閘道和 CIDR 範圍，以及其他將子網路用於其應用程式的成員帳戶。帳戶 D 具有需要連接到網際網路的應用程式。帳戶 B 和帳戶 C 具有不需要連接到網際網路的應用程式。

帳戶 A 用於 AWS Resource Access Manager 為子網路建立資源共享，並與帳戶 D 共用子網路，與帳戶 B 和帳戶 C 共享私有子網路。帳戶 B、帳戶 C 和帳戶 D 可以在子網路中建立資源。每個帳戶只能在與其共享的子網路中查看和建立資源。每個帳戶都可以控制它們在這些子網路中建立的資源 (例如 EC2 執行個體和安全群組)。

共享的子網路無須其他組態，因此路由表與未共享的路由表相同。



帳戶 A (111111111111) 會與帳戶 D (444444444444) 共享公有子網路。帳戶 D 會看到下列子網路，且 Owner (擁有者) 欄提供子網路共享的兩個指標。

- 擁有者的帳戶 ID 是 A (111111111111)，不是帳戶 D (444444444444)。
- 「shared」(已共享) 一字會在擁有者帳戶 ID 旁出現。

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Default subnet	Owner
<input type="checkbox"/>		subnet-0bb1c79de301436ee	available	vpc-0ee975135d74bdcfe	No	111111111111 (shared)

## 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 可將原生 AWS 服務、基礎設施和操作模型用於幾乎所有的資料中心、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 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。

AWS 營運的尖端資料中心均為高度可用。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。

為了協助您判斷哪一個部署最適合您，請參閱 [AWS Wavelength 常見問答集](#)。

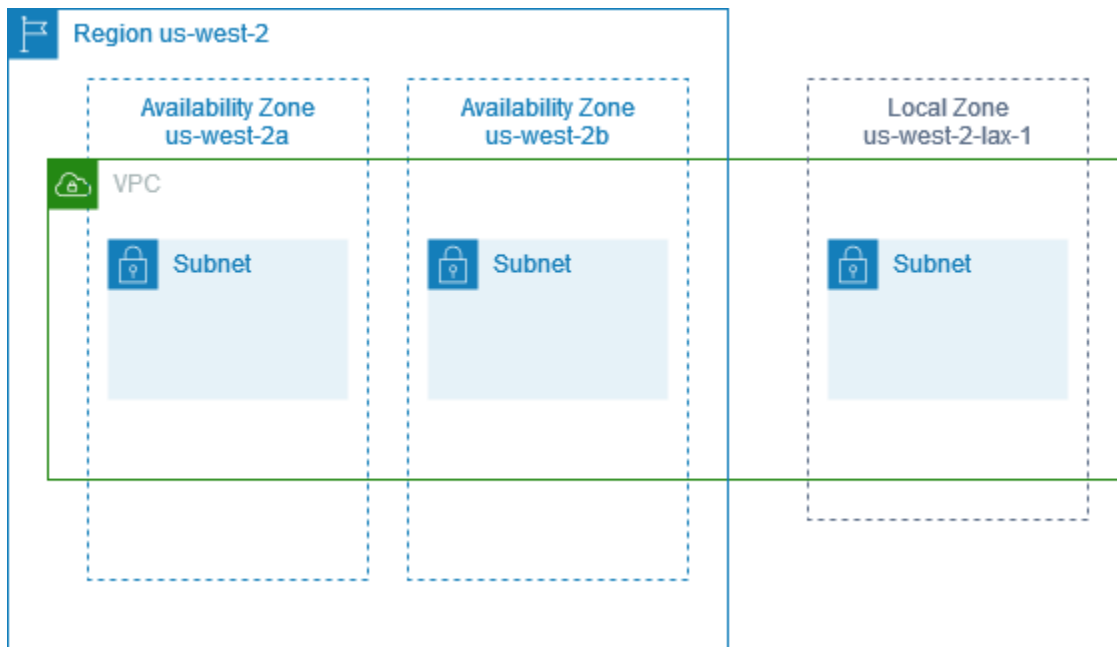
## AWS Local Zones 中的子網路

AWS Local Zones 可讓您將資源放置在更靠近使用者的位置，並使用熟悉的 API 和工具集無縫連線到 AWS 區域中的所有服務。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 地址”](#)。

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 地址”](#)。
- 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 閘道可連線至區域中的 AWS Direct Connect 位置。內部部署資料中心與該 AWS Direct Connect 位置之間有 AWS Direct Connect 連線。

### Note

美國境內使用 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 Virtual Private Cloud Console 的子網路詳細資訊頁面上檢視子網路的 VPC，或使用 [describe-subnets](#)。

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。為了取得最佳延遲效能，AWS 建議您使用最接近您子網延伸所至的目標 Local Zone 的 [Direct Connect 位置](#)。

如需如何排定連線順序的資訊，請參閱《AWS Direct Connect 使用者指南》中的 [交叉連線](#)。

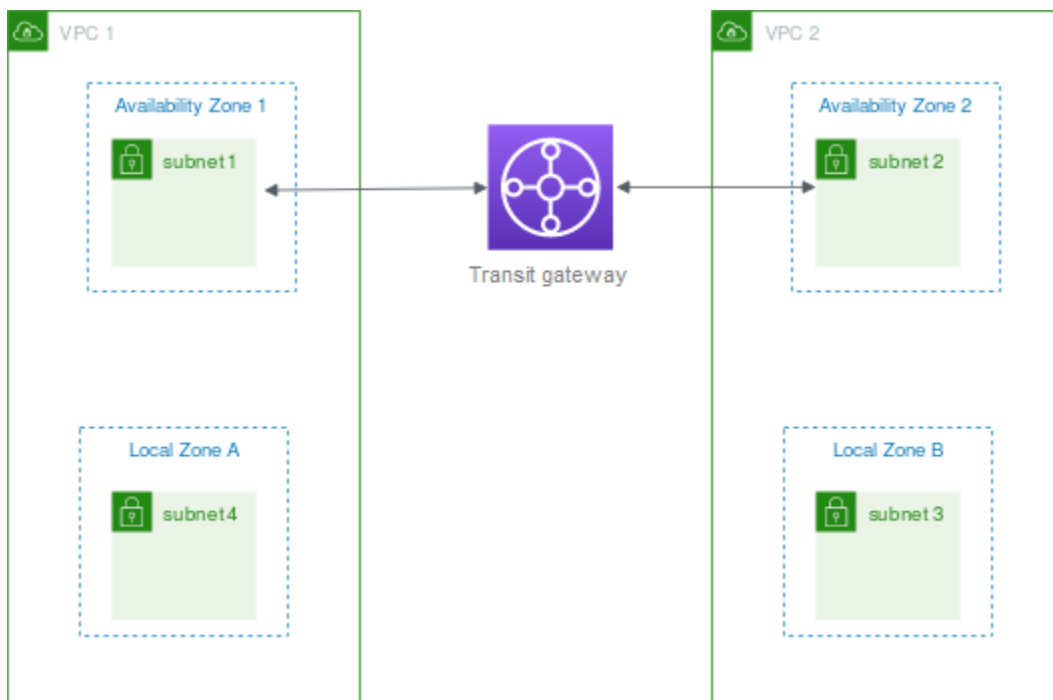
- Direct Connect 閘道。如需如何建立 Direct Connect 閘道的資訊，請參閱《AWS Direct Connect 使用者指南》中的[建立 Direct Connect 閘道](#)。
- 將 VPC 連線至 Direct Connect 閘道的虛擬私有閘道關聯。如需如何建立虛擬私有閘道關聯的資訊，請參閱《AWS Direct Connect 使用者指南》中的[建立和解除虛擬私有閘道的關聯](#)。
- 從 AWS Direct Connect 位置到內部部署資料中心的連線的私有虛擬介面。如需如何建立 Direct Connect 閘道的資訊，請參閱《AWS Direct 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。如需更多詳細資訊，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 VPC 路由表中的每個項目)，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。如需更多詳細資訊，請參閱 [the section called “傳輸閘道的路由”](#)。

以下是 VPC 1 的範例路由表。

目的地	目標
<i>VPC 1 CIDR</i>	<i>##</i>
<i>VPC 2 CIDR</i>	<i>vpc1-attachment-network-interface-id</i>

以下是 VPC 2 的範例路由表。

目的地	目標
<i>VPC 2 CIDR</i>	<i>##</i>
<i>VPC 1 CIDR</i>	<i>vpc2-attachment-network-interface-id</i>

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
<i>VPC 1 CIDR</i>	<i>VPC 1 ###</i>	已傳播
<i>VPC 2 CIDR</i>	<i>VPC 2 ###</i>	已傳播

## AWS Wavelength 中的子網路

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。開發人員可將 Virtual Private Cloud (VPC) 延伸至一或多個 Wavelength 區域，接著使用 AWS 資源 (例如 Amazon EC2 執行個體) 來執行需要極低延遲並在區域中連線至 AWS 服務的應用程式。

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。此外，您還可以使用各種服務來協調或與 EC2、EBS 和 VPC 搭配使用，例如 Amazon EC2 Auto Scaling、Amazon EKS 叢集、Amazon ECS 叢集、Amazon EC2 Systems Manager、Amazon CloudWatch、AWS CloudTrail 和 AWS CloudFormation。Wavelength 中的服務是 VPC 的一部分，透過可靠的高頻寬連線與 AWS 區域建立連線，以輕鬆存取包括 Amazon DynamoDB 和 Amazon RDS 在內的服務。

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。如果您需要進行 Wavelength 區域到 Wavelength 區域的通訊，AWS 建議您使用多個 VPC，每個 Wavelength 區域一個。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 區域流量會路由經過 AWS 區域。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：

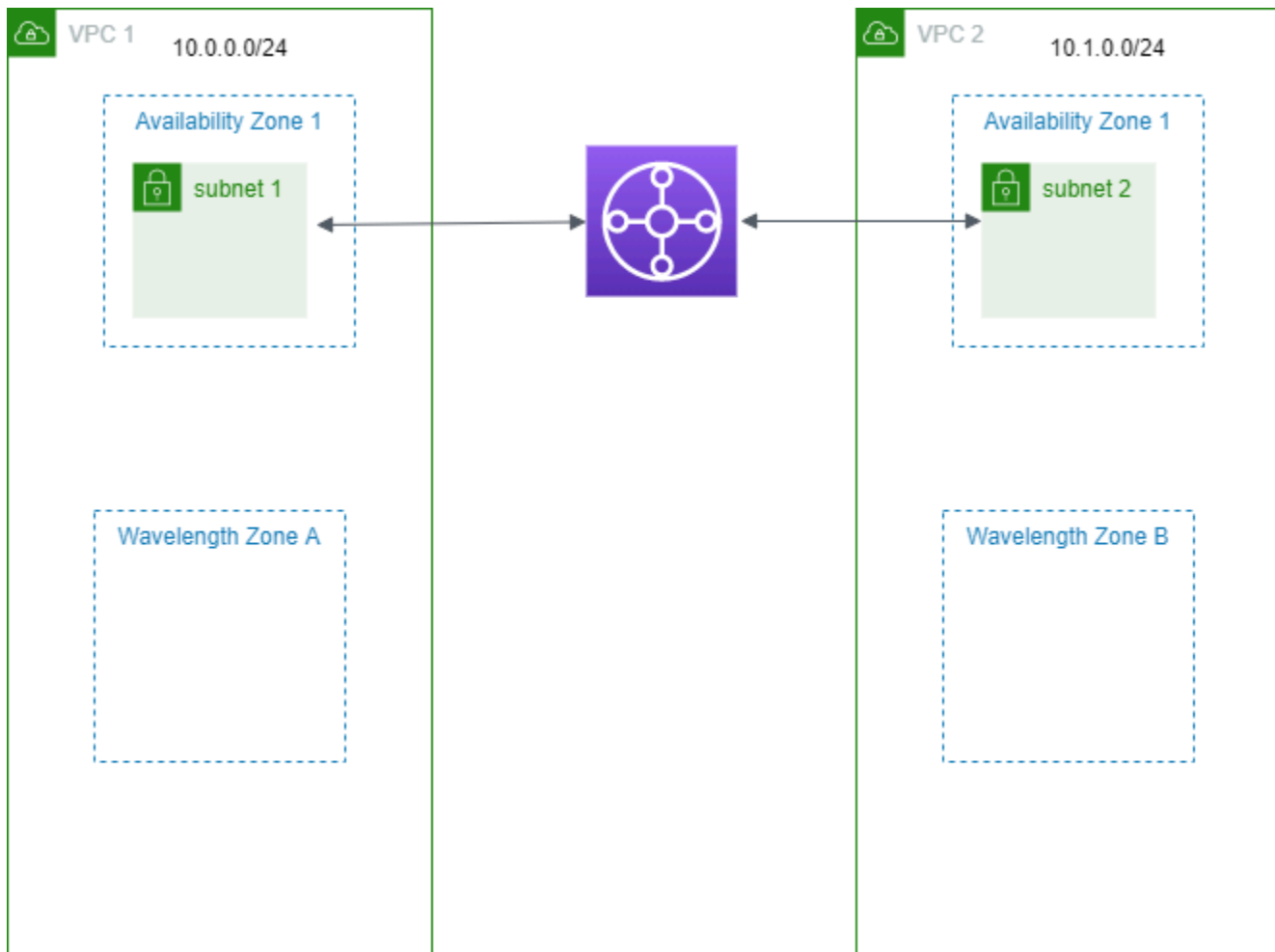
- 對於每個 Wavelength 區域，需要有可用區域中的子網路 (該可用區域屬於 Wavelength 區域的父可用區域)。在此範例中，您可以建立子網路 1 和子網路 2。如需建立子網路的相關資訊，請參閱 [the section called “建立子網”](#)。使用 [describe-availability-zones](#) 以尋找父區域。
- 傳輸閘道。傳輸閘道會連線 VPC。如需建立傳輸閘道的相關資訊，請參閱 Amazon VPC 傳輸閘道指南中的 [建立傳輸閘道](#)。
- 對於每個 VPC，與 Wavelength 區域之父可用區域中傳輸閘道的 VPC 連接。如需詳細資訊，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-222222222222222222

VPC 2 的路由表具有以下項目：

目的地	目標
10.0.0.0/24	tgw-222222222222222222



## AWS Outposts 中的子網路

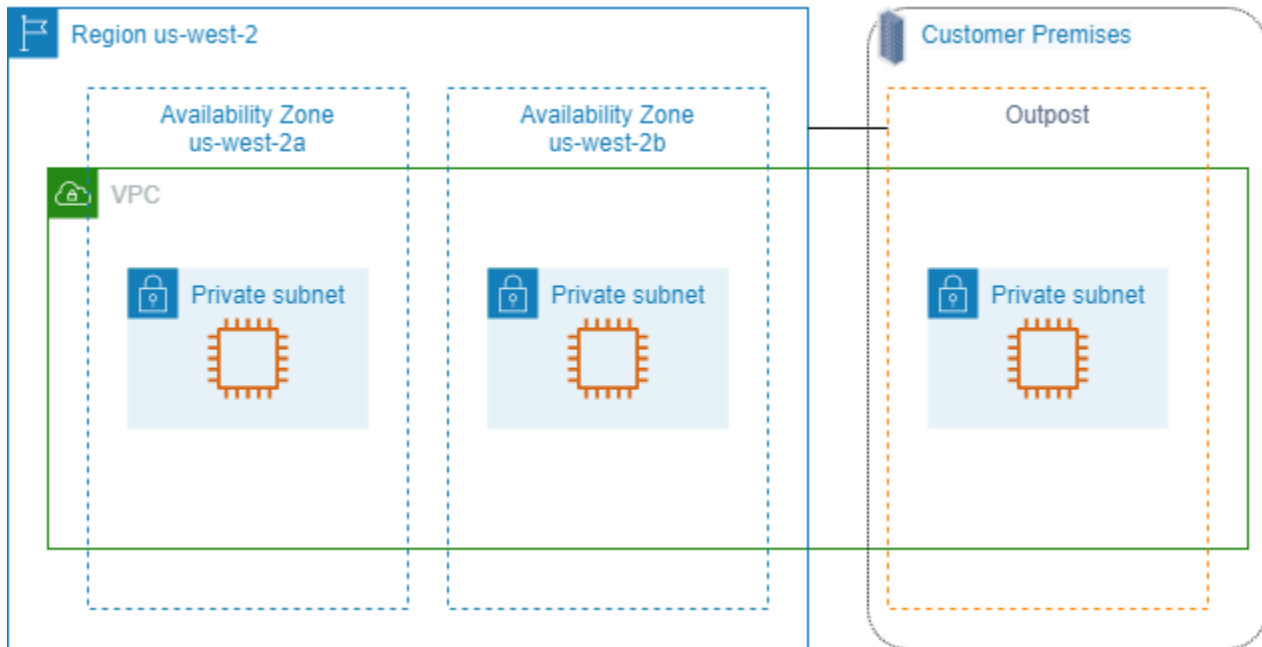
AWS Outposts 為您提供相同的 AWS 硬體基礎設施、服務、API 和工具，以在內部部署和雲端建置和執行應用程式。如果您的工作負載需要低延遲的內部部署應用程式或系統存取，以及需要在本機儲存和處理資料，AWS Outposts 是理想的選擇。如需有關 AWS Outposts 的詳細資訊，請參閱 [AWS Outposts](#)。

VPC 遍及 AWS 區域內的所有可用區域。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。

AWS Outposts 適用的規定如下：

- 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。

### 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

## 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。

## 若要使用刪除 VPC AWS CLI

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
```

# 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](#)
- [設定您的子網路](#)
- [子網路 CIDR 保留](#)
- [設定路由表](#)
- [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。透過在不同的可用區域中啟動 AWS 資源，您可以保護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](#) 地址。這些地址用於與[執行個體中繼資料服務 \(IMDS\)](#) 等 VPC 服務通訊。

如需詳細資訊，請參閱 [您 VPC 和子網路的 IP 定址](#)。

## 子網類型

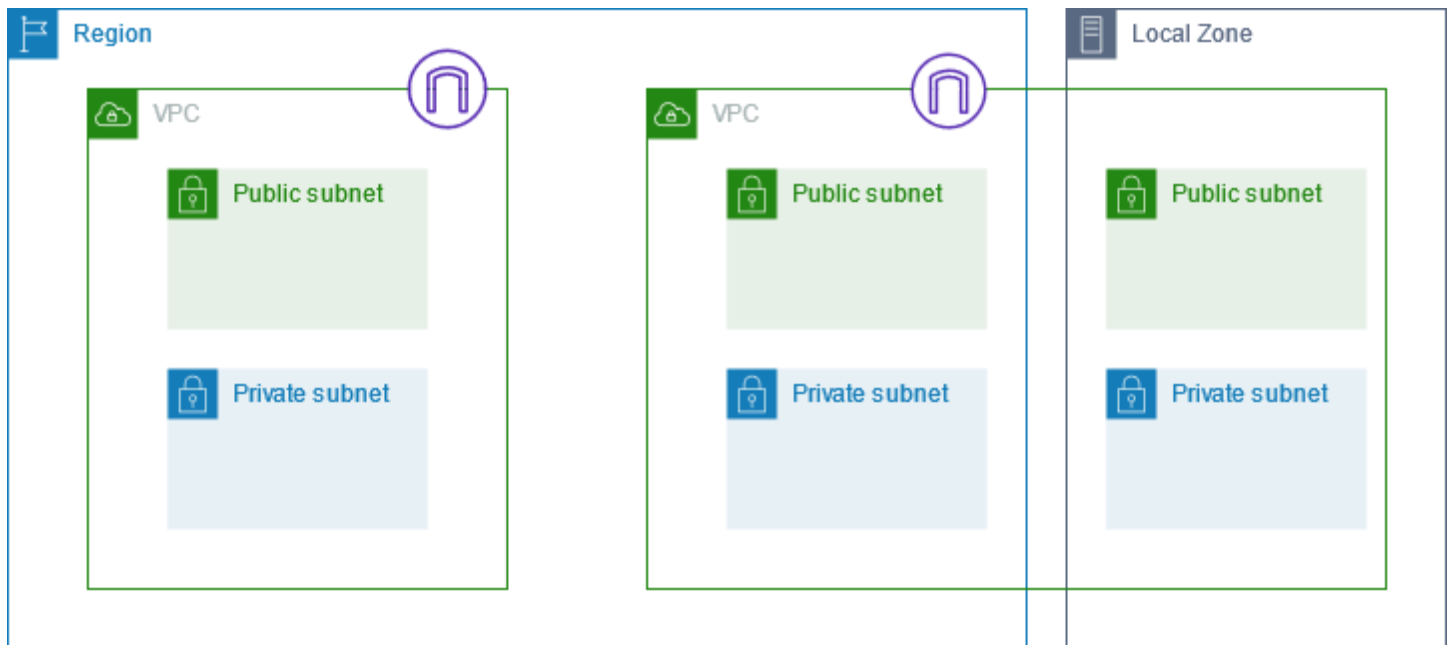
子網路類型取決於您如何設定子網路的路由。例如：

- 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。

## 子網圖表

下圖顯示了區域中的兩個 VPC。具有公有和私有子網，以及網際網路閘道的每個 VPC。如圖表所示，您可以選擇性地在本機區域中新增子網路。本機區域是一種 AWS 基礎結構部署，可將運算、儲存和資料庫服務放在更靠近使用者的位置。當您使用本機區域時，您的使用者可以執行需要個位數毫秒延遲的應用程式。如需詳細資訊，請參閱 [AWS Local Zones](#)。





## 子網路路由

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)。這包含您在該子網中啟動執行個體時，為執行個體建立的主要網路界面 (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 執行個體)。

AWS 提供可用來增加 VPC 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 ACL 控制子網路的流量](#)。

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。您也可以在各別網路界面上建立流程日誌。如需更多詳細資訊，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. 對於可用區域，您可以為子網路選擇一個區域，或保留預設的 [無偏好設定 AWS] 讓您選擇一個區域。
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)。如果您使用 Amazon VPC IP 位址管理員 (IPAM) 來規劃、追蹤和監控 AWS 工作負載的 IP 位址，則當您建立子網路時，您可以選擇從 IPAM (IPAM 分配) 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)。

使用將子網路新增至您的 VPC AWS CLI

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。如需詳細資訊，請參閱 [設定路由表](#)。
- 修改子網路 IP 位址。如需詳細資訊，請參閱 [the section called “設定您的子網路”](#)。

- 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。如需詳細資訊，請參閱 [子網設定](#)。
- 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。如需詳細資訊，請參閱 [使用網路 ACL 控制子網路的流量](#)。
- 與其他帳戶共享子網路。如需更多詳細資訊，請參閱 [???](#)。

## 設定您的子網路

使用下列步驟為您的虛擬私有雲端 (VPC) 設定子網路。

### 任務

- [檢視您的子網路](#)
- [將 IPv6 CIDR 區塊新增至您的子網路](#)
- [從您的子網路中移除 IPv6 CIDR 區塊](#)
- [修改您子網路的公有 IPv4 定址屬性](#)
- [修改您子網路的公有 IPv6 定址屬性](#)

## 檢視您的子網路

請依照本節中的下列步驟來檢視子網路的詳細資訊。

使用主控台檢視子網路詳細資訊

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. 勾選子網路的核取方塊，或選擇子網路 ID 以開啟詳細資訊頁面。

使用描述子網路 AWS CLI

使用 [describe-subnets](#) 命令。

跨所有區域檢視子網路

前往 <https://console.aws.amazon.com/ec2globalview/home> 開啟 Amazon EC2 全域檢視主控台。如需詳細資訊，請參閱 [Amazon EC2 使用者指南中的使用 Amazon EC2 全域檢視列出和篩選資源](#)。

## 將 IPv6 CIDR 區塊新增至您的子網路

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。

如何將 IPv6 CIDR 區塊新增至子網路

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)。
3. 選取您的子網路，然後選擇 Actions (動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 選擇 Add IPv6 CIDR (新增 IPv6 CIDR)。
5. 選擇 VPC CIDR block (VPC CIDR 區塊)，輸入 Subnet CIDR block (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)。
6. 選擇儲存。

使用將 IPv6 CIDR 區塊與子網路產生關聯 AWS CLI

使用 [associate-subnet-cidr-block](#) 命令。

## 從您的子網路中移除 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。

如何從子網路中移除 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. 選取子網路，然後選擇 Actions (動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 尋找 IPv6 CIDR 區塊，然後選擇 Remove (移除)。
5. 選擇儲存。

若要使用 AWS CLI

使用 [disassociate-subnet-cidr-block](#) 命令。

## 修改您子網路的公有 IPv4 定址屬性

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。

修改您子網路的公有 IPv4 定址行為

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)。

若要使用修改子網路屬性 AWS CLI

使用 [modify-subnet-attribute](#) 命令。

## 修改您子網路的公有 IPv6 定址屬性

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。

修改您子網路的公有 IPv6 定址行為

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 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)。

若要使用修改子網路屬性 AWS CLI

使用 [modify-subnet-attribute](#) 命令。

## 子網路 CIDR 保留

子網路 CIDR 保留區是您預留的 IPv4 或 IPv6 位址範圍，AWS 以便無法將它們指派給您的網路介面。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：

- 前置詞 — AWS 將保留 IP 位址範圍中的位址指派給網路介面。如需詳細資訊，請參閱 [Amazon EC2 使用者指南中的指派首碼給 Amazon EC2 網路界面](#)。
- 明確：您會手動將 IP 地址指派至網路介面。

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。當您在相同 VPC 內保留多個 CIDR 範圍時，CIDR 範圍無法重疊。
- 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。
- 刪除子網路保留區時，可以將未使用的 IP 位址指派 AWS 給您的網路介面。刪除子網保留不會取消指派任何已在使用中的 IP 地址。

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](#)。

## 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)。

## 使用子網路 CIDR 保留區使用 AWS CLI

您可以使用 AWS CLI 來建立和管理子網路 CIDR 保留區。

### 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。

### 目錄

- [路由表概念](#)
- [子網路路由表](#)
- [閘道路由表](#)
- [路由優先順序](#)
- [路由表配額](#)
- [疑難排解可達性問題](#)
- [路由選項範例](#)
- [使用路由表](#)
- [中間設備路由精靈](#)

## 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。
- 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。
- 子網路路由表 — 與子網相關聯的路由表。
- 本機路由 — VPC 內用於通訊的預設路由。
- 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](#)。

## 子網路路由表

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路由表建立關聯。

### 目錄

- [路由](#)
- [主路由表](#)
- [自訂路由表](#)
- [子網路路由表關聯](#)

## 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。

目的地	目標
0.0.0.0/0	<i>igw-id</i>

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 CIDR 區塊集，則可以建立 [客戶管理的前置詞清單](#)，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位址空間內，並保留供服務使用 AWS。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`。此範圍在唯一的本地地址 (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。

目的地	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-aabbccdde1122334

- 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 主控台內的 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。

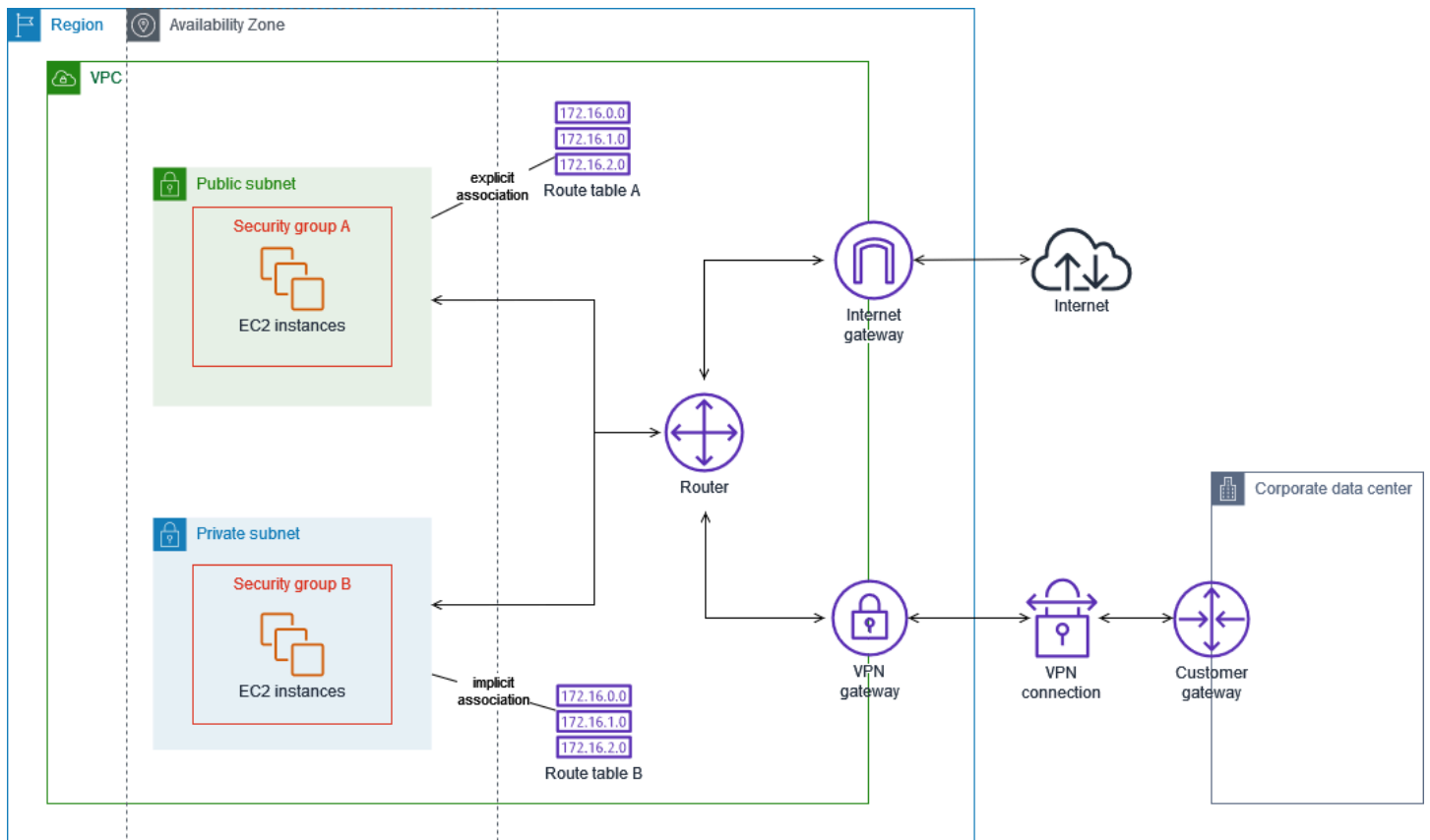
## 子網路路由表關聯

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[判斷明確相關聯的子網及 \(或\) 閘道](#)。

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。

目的地	目標
<i>VPC CIDR</i>	區域
0.0.0.0/0	<i>igw-id</i>

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。

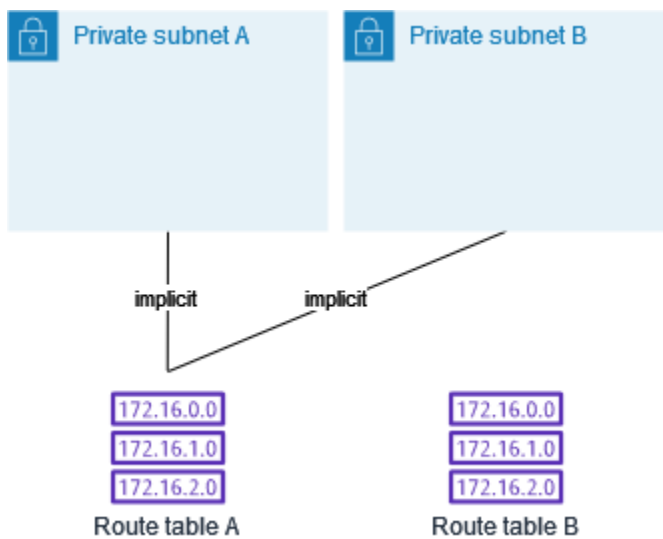
目的地	目標
<i>VPC CIDR</i>	區域

目的地	目標
0.0.0.0/0	<i>vgw-id</i>

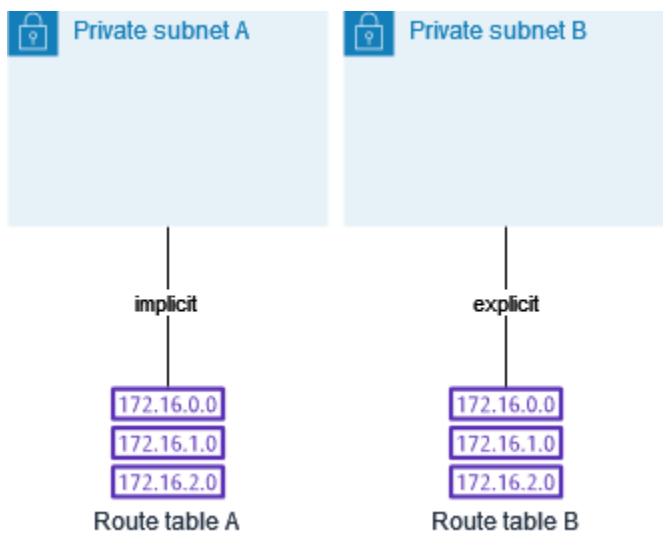
## 範例 2：取代主路由表

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。

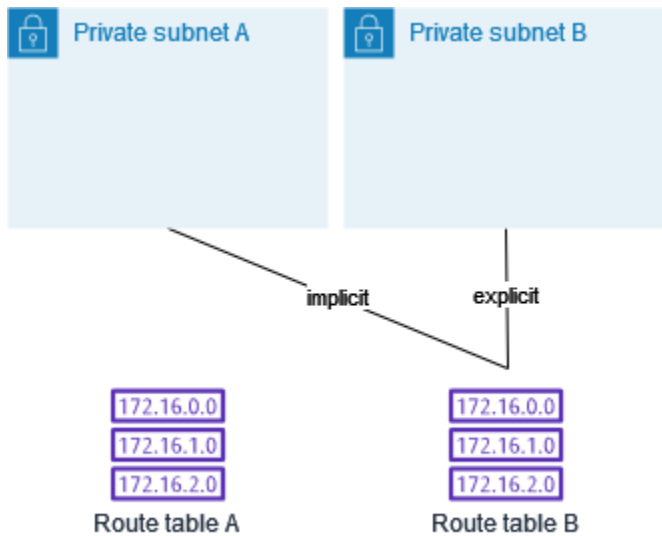
下圖顯示兩個子網路和兩個路由表。子網路 A 隱含地與路由表 A (主路由表) 相關聯。子網路 B 隱含地與路由表 A 相關聯。路由表 B (自訂路由表格) 並未與任何一個子網路相關聯。



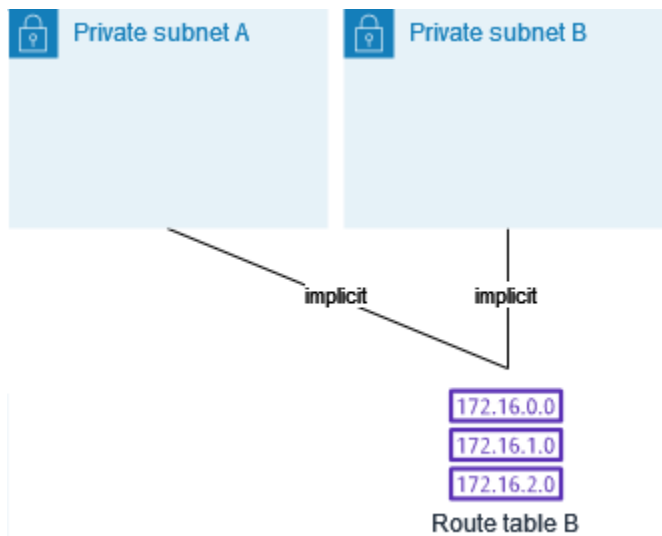
若要取代主路由表，請先在子網路 B 和路由表 B 之間建立明確關聯。然後測試路由表 B。



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	<i>eni-id</i>

## 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	<i>eni-id</i>

## 規則和考量

如果下列任一情況適用，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，目標網路界面也必須具有公有 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

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。

### 目錄

- [最長字首相符](#)
- [路由優先順序和傳播路由](#)
- [路由優先順序和字首清單](#)

## 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

## 路由優先順序和傳播路由

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重疊，則靜態路由優先。

如果傳播路由的目的地與靜態路由的目的地相同，若目標為下列其中一種，則靜態路由優先：

- 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。

目的地	目標	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

## 路由優先順序和字首清單

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具有目的地 CIDR 區塊的靜態路由 (它將靜態路由與字首清單重疊)，則具有 CIDR 區塊的靜態路由優先。
- 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。

## 路由表配額

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](#)。

## 疑難排解可達性問題

Reachability Analyzer 是一種靜態配置分析工具。使用可 Reachability Analyzer 來分析和偵錯 VPC 中兩個資源之間的網路連接性。可 Reachability Analyzer 產生這些資源之間的虛擬路徑的 hop-by-hop 詳細信息，當它們是可訪問的，並識別阻塞組件，否則。例如，它可以識別缺少或配置錯誤的路由表路由。

如需詳細資訊，請參閱 [Reachability Analyzer Guide](#) (《Reachability Analyzer 指南》)。

## 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-xxxxxxxxxxxxxxxxxxxx) 的目標。

目的地	目標
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

如需詳細資訊，請參閱 [使用網際網路閘道連線至網際網路](#)。

## 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	<i>nat-gateway-id</i>

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-xxxxxxx，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	<i>nat-gateway-id</i>
pl-xxxxxxx	<i>vpce-id</i>
10.25.0.0/16	<i>pcx-id</i>

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 連線來啟用 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-xxxxxxxxxxxxxxxxxxxxxx)。

目的地	目標
10.0.0.0/16	<i>vgw-id</i>

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 AWS Direct Connect 連線的 IPv6 流量。如需詳細資訊，請參閱《[AWS 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

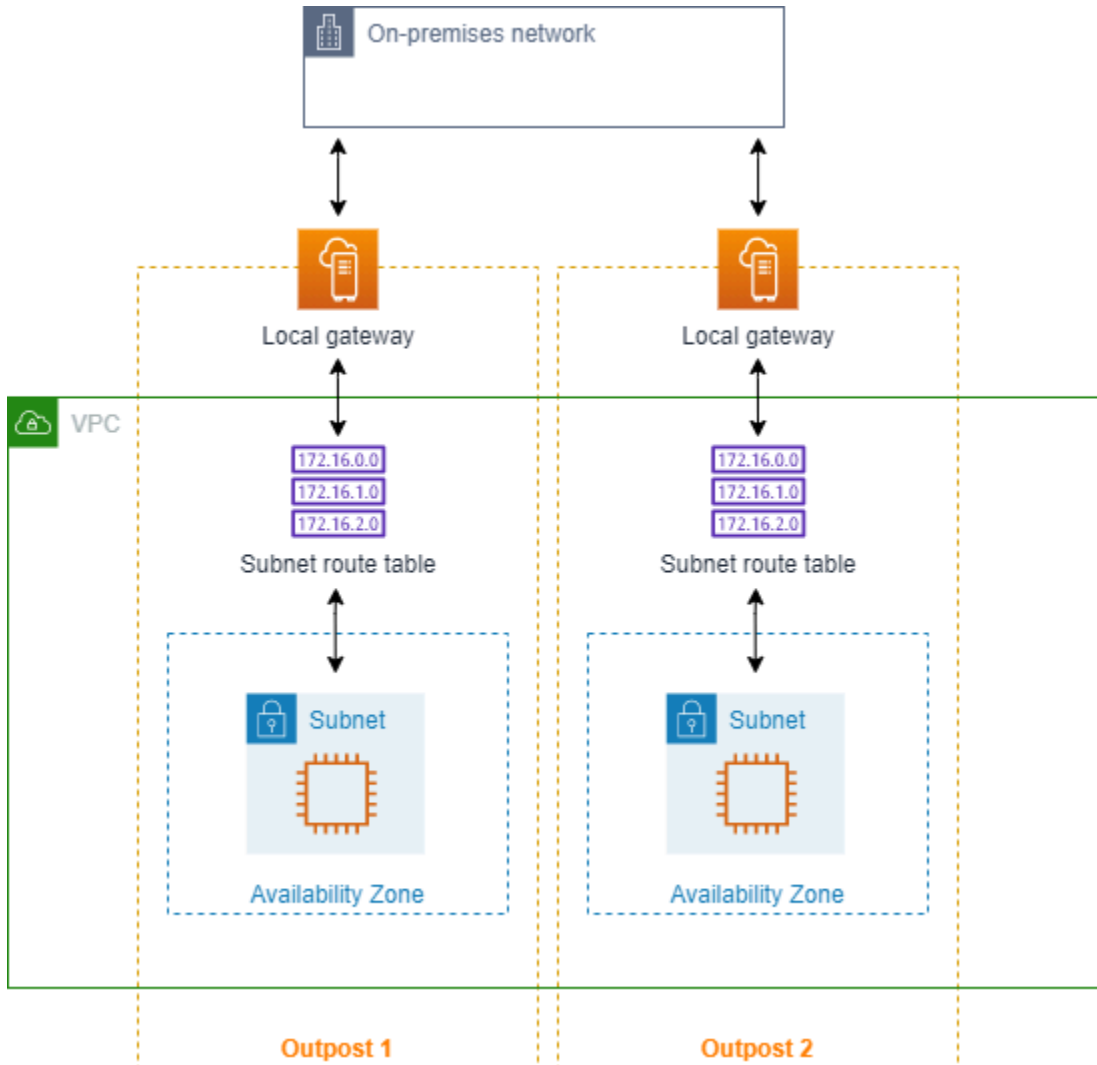
與之相關聯的 VPC 中的子網路 AWS Outposts 可以具有本機閘道的其他目標類型。請考慮您想要讓本機閘道將目的地地址為 192.168.10.0/24 的流量路由至客戶網路的情況。若要這樣做，請新增下列路由，其中具有目的地網路和本機閘道目標 (lgw-xxxx)。

目的地	目標
192.168.10.0/24	<i>lgw-id</i>

## 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 子網路的路由表項目如下所示：

目的地	目標
10.0.0.0/16	區域
10.0.2.0/24	<i>lgw-1-id</i>

Outpost 2 子網路的路由表項如下所示：

目的地	目標
10.0.0.0/16	區域
10.0.1.0/24	<i>lgw-2-id</i>

## 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 VPC 間 IPv6 流量的路由，您必須將路由新增至您的路由表，指向 VPC 對等互連連線，存取對等 VPC 之所有或部分的 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 的子網路路由表。

目的地	目標
10.0.0.0/16	區域
172.31.0.0/16	pcx-11223344556677889

目的地	目標
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 和其 AWS 他服務之間建立私人連線。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 (p1-**xxxxxxxx**) 之目標 (destination) 以及具有端點 ID 之目標 (target) (vpce-**xxxxxxxxxxxxxxxxxxxx**) 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	<i>eigw-id</i>

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-111111111111111111
- VPC B: 10.2.0.0/16, attachment ID tgw-attach-222222222222222222

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	<i>tgw-id</i>

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-111111111111111111
10.2.0.0/16	tgw-attach-222222222222222222

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。您可以使用中介方塊路由精靈，為閘道、中介盒和目的地子網路 AWS 自動設定適當的路由表。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。檢閱路由以確保流量是否正確路由，而且如果啟用或停用路由傳輸 (例如，支援 Jumbo 框架的 AWS Direct Connect 連線需要路由傳輸)，也不會產生意外後果。

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

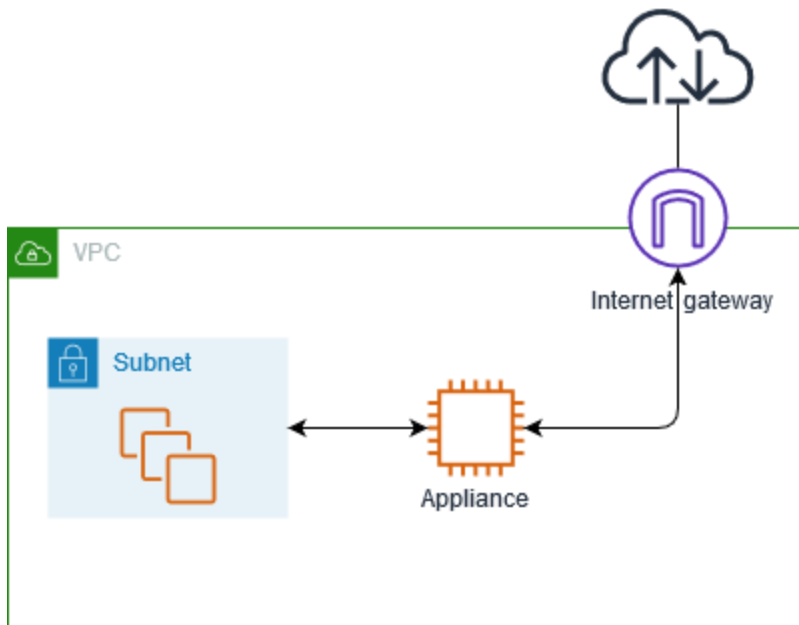
您可以從 [AWS Marketplace](#) 中選擇第三方設備，也可以設定自己的設備。建立或設定設備時，請注意下列事項：

- 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。虛擬私有閘道不支援 IPv6 流量。

### 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。

目的地	目標
<i>VPC CIDR</i>	區域
<i>## CIDR</i>	<i>##### ID</i>

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。

目的地	目標
<i>VPC CIDR</i>	<i>##### ID</i>

若要將流量從子網路路由到另一個子網中的設備，請將路由新增到子網路路由表，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)。

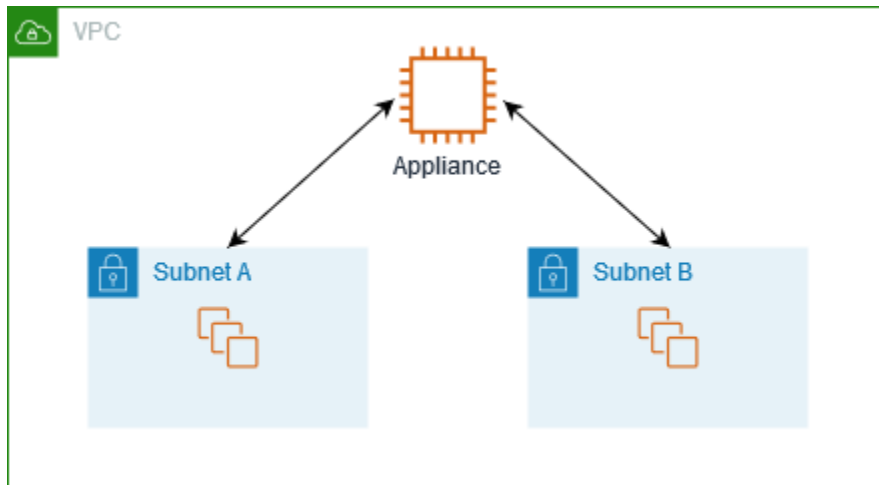
目的地	目標
<i>VPC CIDR</i>	區域
<code>0.0.0.0/0</code>	<i>##### ID</i>

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。

目的地	目標
<i>VPC CIDR</i>	區域
<code>0.0.0.0/0</code>	<i>igw-id</i>

### 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。



## 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。

目的地	目標
<i>VPC CIDR</i>	區域
<i>### B CIDR</i>	<i>##### ID</i>

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。

目的地	目標
<i>VPC CIDR</i>	區域
<i>### A CIDR</i>	<i>##### ID</i>



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。

目的地	目標
<i>VPC CIDR</i>	<i>##### ID</i>

## 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 CIDR 區塊集，則可以建立[客戶管理的前置詞清單](#)，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	<i>tgw-id</i>

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。您可以透過建立[VPC 端點服務組態](#)，將負載平衡器設定為服務。然後，您可以在 VPC 中建立[閘道負載平衡器端點](#)，以將 VPC 連線至服務。

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。

目的地	目標
10.0.1.0/24	<i>vpc-endpoint-id</i>

如需詳細資訊，請參閱[閘道負載平衡器](#)。

## 使用路由表

本節說明如何使用路由表。

### 目錄

- [判斷子網的路由表](#)
- [判斷明確相關聯的子網及 \(或\) 閘道](#)
- [建立自訂路由表](#)
- [從路由表新增和移除路由](#)
- [啟用或停用路由傳播](#)
- [建立子網與路由表之間的關聯](#)
- [變更子網的路由表](#)
- [取消子網與路由表的關聯](#)
- [取代主路由表](#)
- [建立閘道與路由表之間的關聯](#)
- [取消閘道與路由表的關聯](#)
- [取代或還原本機路由的目標](#)
- [刪除路由表](#)

## 判斷子網的路由表

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。

## 判斷子網的路由表

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 [判斷明確相關聯的子網及 \(或\) 閘道](#)。

## 判斷明確相關聯的子網及 (或) 閘道

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。

### 使用命令列描述一個或多個路由表格並檢視其關聯

- [describe-route-tables](#) (AWS CLI)

- [Get-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

## 建立自訂路由表

您可以使用 Amazon VPC 主控台建立您 VPC 的自訂路由表。

### 使用主控台建立自訂路由表

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)。

### 使用命令列建立自訂路由表

- [create-route-table](#) (AWS CLI)
- [New-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

## 從路由表新增和移除路由

您可以新增、刪除和修改路由表中的路由。您僅能修改您新增的路由。

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](#)。

### 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)。針對 Destination (目的地)，輸入目的地 CIDR 區塊、單一 IP 地址或字首清單的 ID。

- 若要修改路由，請針對 Destination (目的地)，取代目的地 CIDR 區塊或單一 IP 地址。針對 Target (目標)，選擇一個目標。
- 若要刪除路由，請選擇 Remove (移除)。
- 選擇儲存變更。

### 使用命令列更新路由表的路由

- [create-route](#) (AWS CLI)
- [replace-route](#) (AWS CLI)
- [delete-route](#) (AWS CLI)
- [New-EC2Route](#) (AWS Tools for Windows PowerShell)
- [Set-EC2Route](#) (AWS Tools for Windows PowerShell)
- [Remove-EC2Route](#) (AWS Tools for Windows PowerShell)

#### Note

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。

### 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](#)。

### 使用主控台啟用路由傳播

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. 選取位於虛擬私有閘道旁邊的 Enable (啟用) 核取方塊，然後選擇 Save (儲存)。

## 使用命令列或 API 啟用路由傳播

- [enable-vgw-route-propagation](#) (AWS CLI)
- [Enable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

## 使用主控台停用路由傳播

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. 清除位於虛擬私有閘道旁邊的 Enable (啟用) 核取方塊，然後選擇 Save (儲存)。

## 使用命令列或 API 停用路由傳播

- [disable-vgw-route-propagation](#) (AWS CLI)
- [Disable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

## 建立子網與路由表之間的關聯

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。

## 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)。

## 使用命令列將子網與路由表建立關聯

- [associate-route-table](#) (AWS CLI)
- [Register-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

## 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。

使用命令列變更與子網關聯的路由表

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (AWS Tools for Windows PowerShell)

## 取消子網與路由表的關聯

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。

使用主控台取消子網與路由表的關聯

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 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)。

使用命令列取消子網與路由表的關聯

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

## 取代主路由表

您可以變更在您的 VPC 中，哪個路由表是主路由表。

### 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)。

### 使用命令列取代主路由表

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (AWS Tools for Windows PowerShell)

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)。

## 建立閘道與路由表之間的關聯

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。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. 選取閘道的核取方塊。
5. 選擇儲存變更。

### 使用將閘道與路由表相關聯 AWS CLI

使用 [associate-route-table](#) 命令。以下範例會將網際網路閘道 `igw-11aa22bb33cc44dd1` 與路由表 `rtb-01234567890123456` 建立關聯。

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id igw-11aa22bb33cc44dd1
```

### 取消閘道與路由表的關聯

您可以取消網際網路閘道或虛擬私有閘道與路由表的關聯。

#### 使用主控台將閘道與路由表建立關聯

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. 從 Edge associations (邊緣關聯) 標籤，選擇 Edit edge associations (編輯邊緣關聯)。
4. 清除閘道的核取方塊。
5. 選擇儲存變更。

#### 使用命令列取消閘道與路由表的關聯

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

### 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。

#### 使用主控台更新本機路由

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。

#### 若要使用取代本機路由的目標 AWS CLI

使用 [replace-route](#) 命令。下列範例會將本機路由的目標取代為 eni-11223344556677889。

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block 10.0.0.0/16 --network-interface-id eni-11223344556677889
```

#### 若要使用還原本機路由的目標 AWS CLI

以下範例還原路由表 rtb-01234567890123456 的本機目標。

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block 10.0.0.0/16 --local-target
```

## 刪除路由表

只有在路由表未與任何子網相關聯時，您才可以刪除路由表。但無法刪除主路由表。

#### 使用主控台刪除路由表

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)、Delete route table (刪除路由表)。

4. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

使用主控台刪除路由表

- [delete-route-table](#) (AWS CLI)
- [Remove-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

## 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](#)
- [管理中間設備路由](#)
- [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。

## 管理中間設備路由

可在 Amazon Virtual Private Cloud Console 中使用中間設備路由精靈。

### 目錄

- [使用中間設備路由精靈建立路由](#)
- [修改中間設備路由](#)
- [檢視中間設備路由精靈路由表](#)
- [刪除中間設備路由精靈組態](#)

### 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)。

### 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)。

## 檢視中間設備路由精靈路由表

### 若要檢視中間設備路由精靈路由表

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 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. 在 Middlebox route tables (中間設備路由表) 下方，該數字表示中間設備路由精靈建立的路由數目。選擇編號以檢視路由。

我們會在單獨的路由表頁面上顯示中間設備路由精靈的路由。

### 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。如需詳細資訊，請參閱[the section called “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。如需詳細資訊，請參閱[the section called “刪除路由表”](#)。

## 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。

## 中間設備案例

下列範例介紹中間設備路由精靈的案例。

### 內容

- [檢查目的地為子網的流量](#)
- [使用安全 VPC 中的設備檢查流量](#)
- [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。

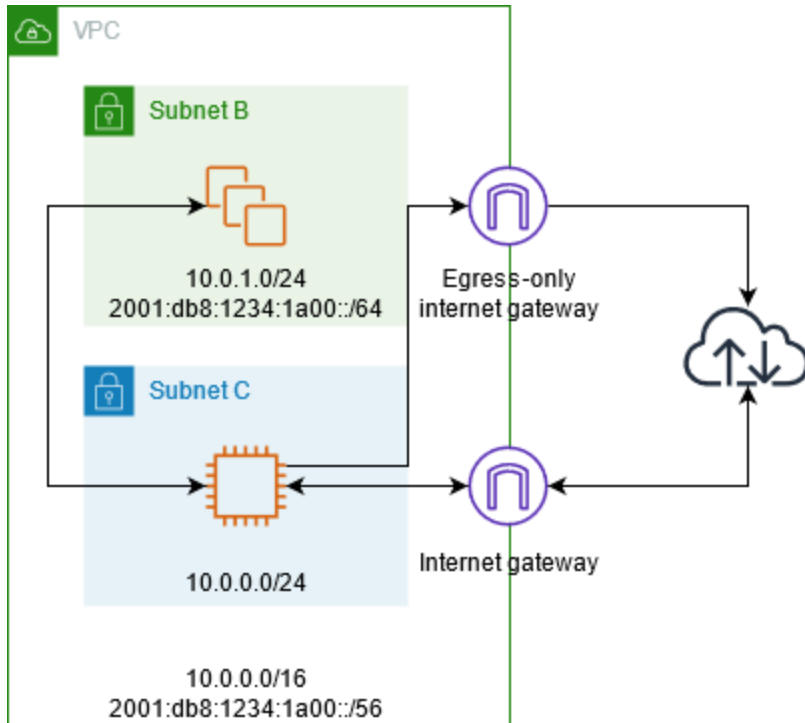
中間設備路由精靈會自動執行下列操作：

- 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	目標	用途
10.0.0.0/16	區域	IPv4 的本機路由
10.0.1.0/24	<i>appliance-eni</i>	將目的地為子網 B 的 IPv4 流量路由到中間設備
<i>2001:db8:1234:1a00::/56</i>	區域	IPv6 的本機路由



目標	目標	用途
<code>2001:db8:1234:1a00::/64</code>	<code>appliance-eni</code>	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	目標	用途
10.0.0.0/16	區域	IPv4 的本機路由
0.0.0.0/0	<code>appliance-eni</code>	將目的地為網際網路的 IPv4 流量路由至中間設備
<code>2001:db8:1234:1a00::/56</code>	區域	IPv6 的本機路由
::/0	<code>appliance-eni</code>	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	目標	用途
10.0.0.0/16	區域	IPv4 的本機路由
0.0.0.0/0	<i>igw-id</i>	將 IPv4 流量路由至網際網路閘道
<i>2001:db8:1234:1a00::/56</i>	區域	IPv6 的本機路由
::/0	<i>eigw-id</i>	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")

### 使用安全 VPC 中的設備檢查流量

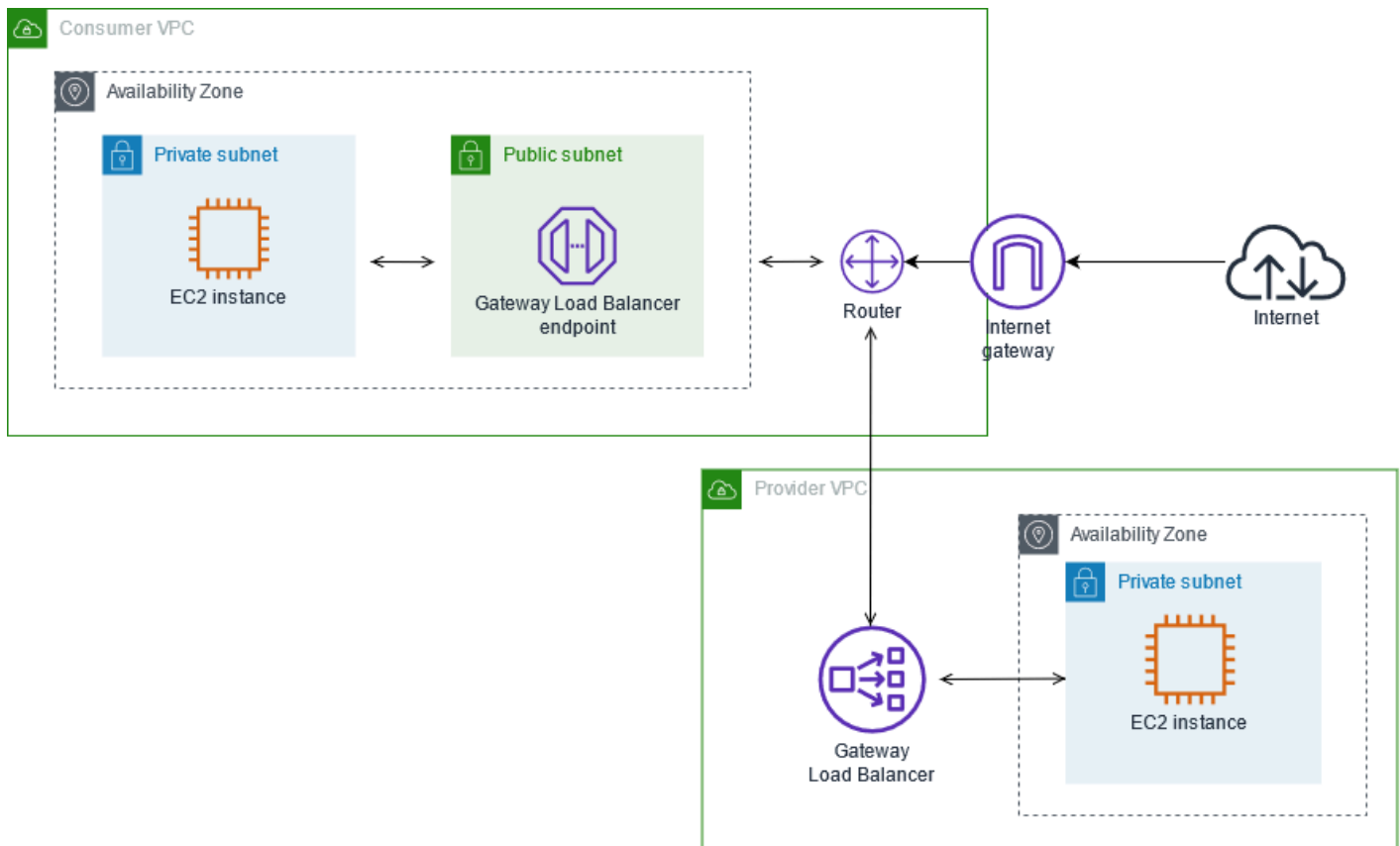
試想這樣一個案例：您需要使用在 Gateway Load Balancer 後方設定的安全設備機群，檢查從網際網路閘道進入 VPC 且目的地為子網的流量。服務消費者 VPC 的擁有者會在其 VPC (由端點網路介面表示) 的子網中建立 Gateway Load Balancer 端點。所有透過網際網路閘道進入 VPC 的流量會先路由至 Gateway Load Balancer 端點，以便進行檢查，然後再路由至應用程式子網。同樣地，離開應用程式子網的所有流量會先路由至 Gateway Load Balancer 端點，以便進行檢查，然後再路由至網際網路。

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	目標	用途
<code>### VPC CIDR</code>	區域	本機路由
<code>##### CIDR</code>	<code>endpoint-id</code>	將目的地為應用程式子網的流量路由至 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	目標	用途
<i>### VPC CIDR</i>	區域	本機路由
0.0.0.0/0	<i>endpoint-id</i>	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	目標	用途
<i>### VPC CIDR</i>	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	<i>igw-id</i>	將所有流量路由至網際網路閘道

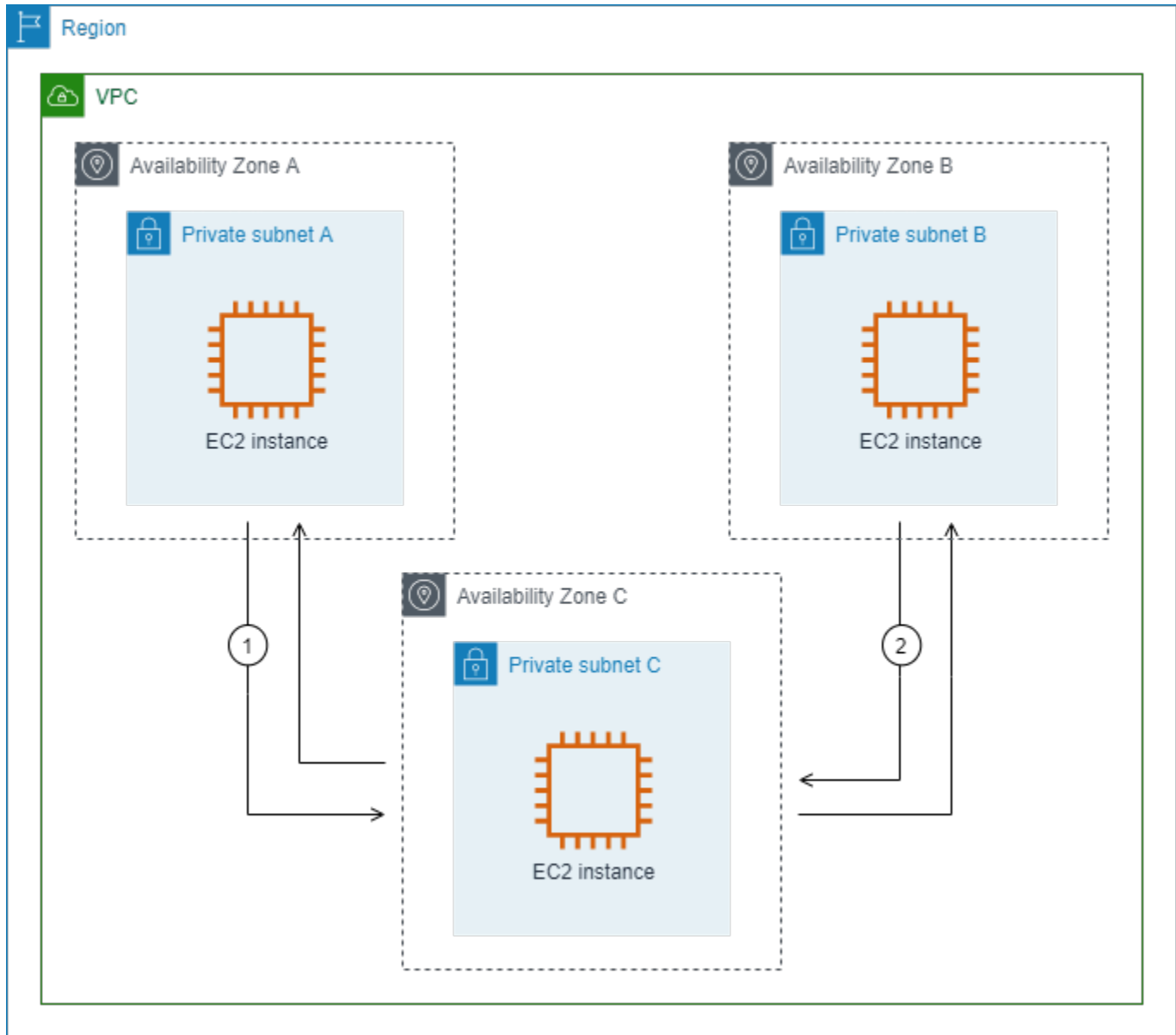
當您使用中間設備路由精靈時，其可將下列標籤與路由表相關聯：

- 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	目標	用途
<i>VPC CIDR</i>	區域	本機路由
<i>## B CIDR</i>	<i>appliance-eni</i>	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	目標	用途
<i>VPC CIDR</i>	區域	本機路由
<i>## A CIDR</i>	<i>appliance-eni</i>	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	目標	用途
<i>VPC CIDR</i>	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。

### 如何使用主控台刪除子網路

1. 在 <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)。

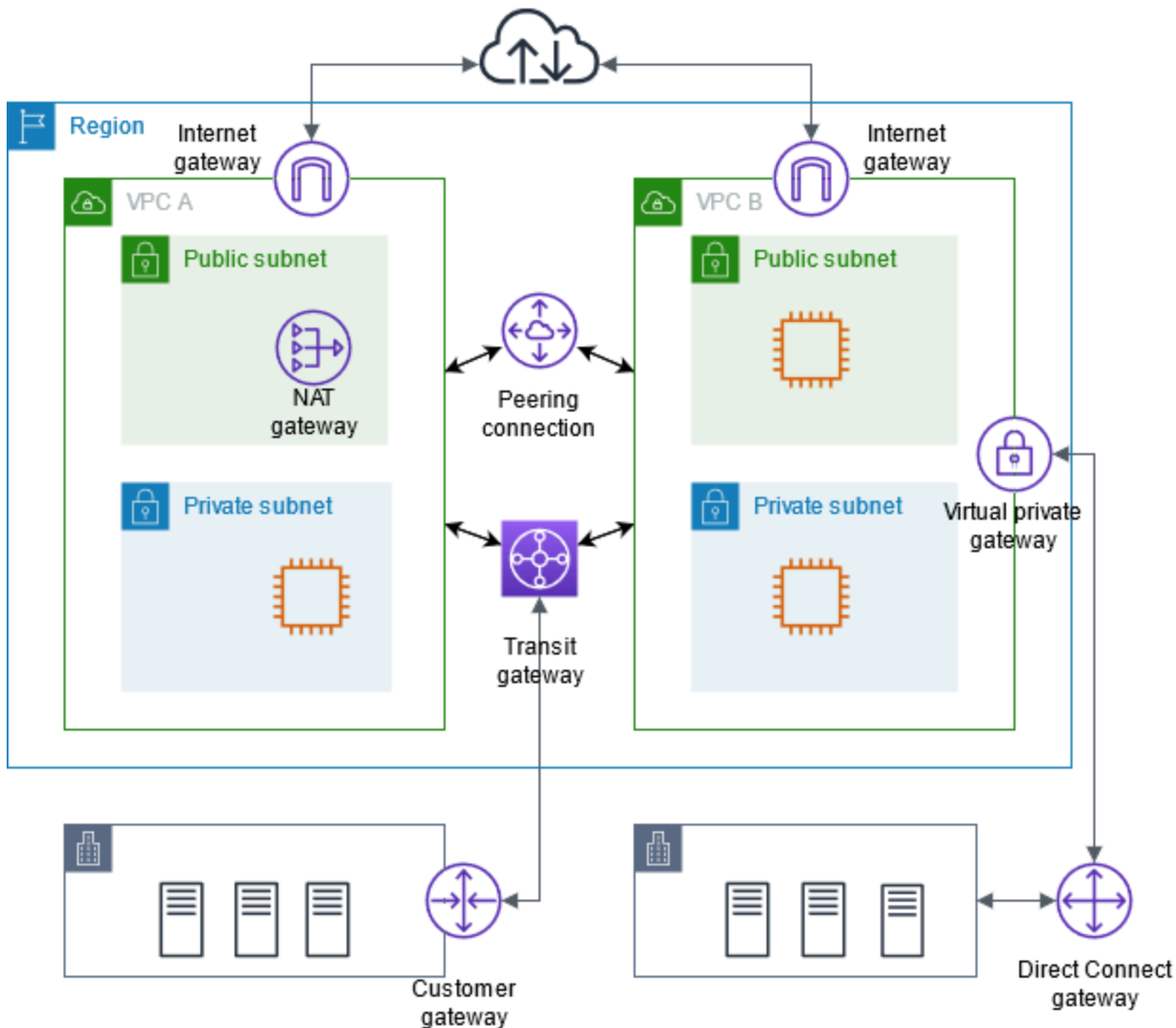
### 如何使用 AWS CLI 刪除子網路

使用 [delete-subnet](#) 命令。

## 將 VPC 連線至其他網路

您可以將 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。

下圖示範了其中一些連線選項。VPC A 透過網際網路閘道連線至網際網路。VPC A 私有子網中的 EC2 執行個體可以使用 VPC A 公有子網中的 NAT 閘道連線至網際網路。VPC B 透過網際網路閘道連線至網際網路。VPC B 公有子網中的 EC2 執行個體可以使用網際網路閘道連線至網際網路。VPC A 和 VPC B 透過 VPC 對等互連和傳輸閘道互連。傳輸閘道具有到資料中心的 VPN 連接。VPC B 具有與資料中心的 AWS Direct Connect 連線。



如需詳細資訊，請參閱 [Amazon Virtual Private Cloud 連線選項](#)。

### 目錄

- [使用網際網路閘道連線至網際網路](#)



- [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](#)

## 使用網際網路閘道連線至網際網路

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 使用本機電腦連線至 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)。針對使用 IPv6 的通訊，不需要 NAT，因為 IPv6 地址是公有的。如需詳細資訊，請參閱 [IP 地址和 NAT](#)。

## 網際網路存取組態

若要讓執行個體從網際網路接收或傳送流量，請執行以下動作：

- [建立網際網路閘道](#)，並將其連接至您的 VPC。
- [新增路由](#)至子網路的路由表，網際網路綁定型流量導向至網際網路閘道。
- 確保子網中的執行個體具有公有 IPv4 地址或 IPv6 地址。[如需詳細資訊，請參閱 Amazon EC2 使用者指南中的執行個體 IP 定址](#)。
- 確保[安全群組](#)和[網路存取控制清單](#)允許所需網際網路流量流向和流出執行個體。

如要為執行個體提供網際網路存取，但不為其指派公有 IP 地址，可以改用 NAT 裝置。NAT 裝置可讓私有子網中的執行個體連線至網際網路，但會阻止網際網路上的主機啟動與執行個體的連線。如需詳細資訊，請參閱 [NAT 裝置](#)。

### 公有和私有子網

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。

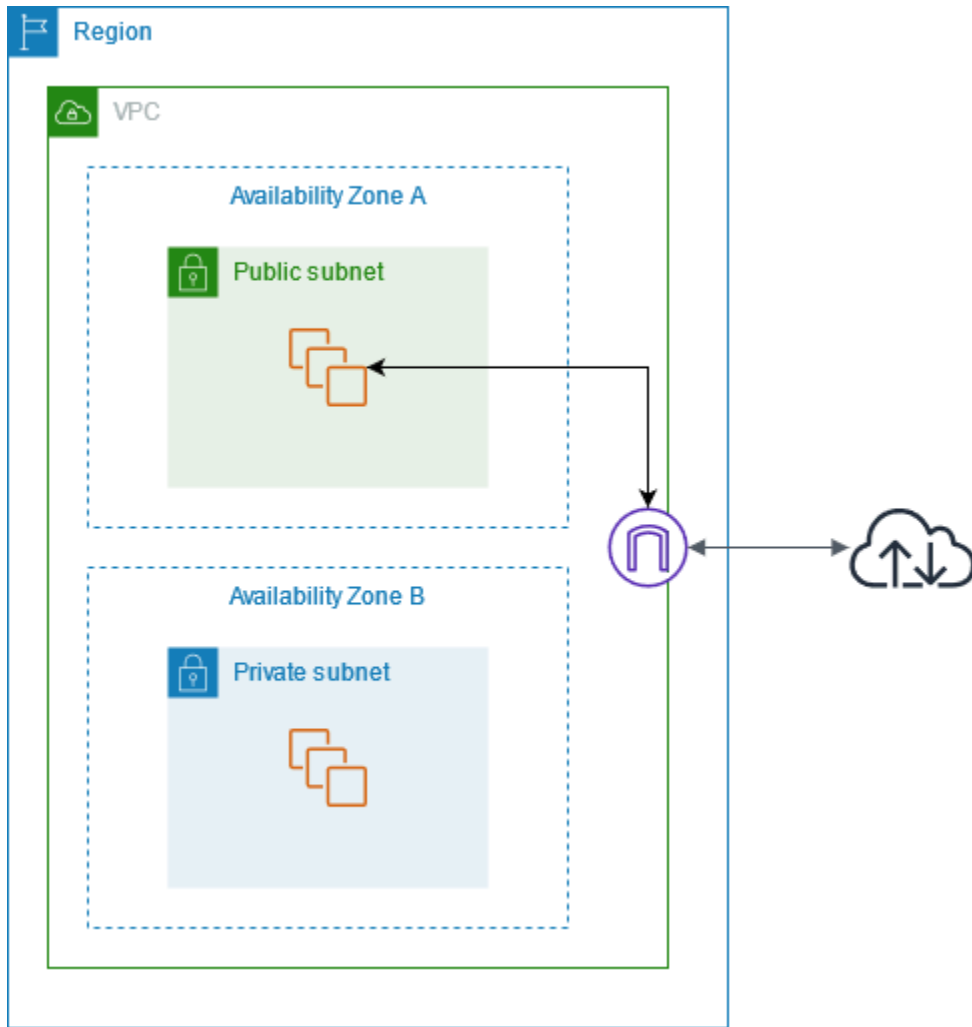
在公有子網路由表中，您可為網際網路閘道指定路由至路由表無法明確辨識的所有目的地 (用於 IPv4 的  $0.0.0.0/0$ ，或用於 IPv6 的  $::/0$ )。或者，您可以將路由範圍設定到較窄範圍的 IP 地址；例如，您公司外部公有端點的公有 IPv4 地址 AWS，或 VPC 外部其他 Amazon EC2 執行個體的彈性 IP 地址。

## 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表您的執行個體提供 one-to-one NAT，因此當流量離開您的 VPC 子網路並前往網際網路時，回覆位址欄位會設定為執行個體的公用 IPv4 位址或彈性 IP 位址，而非其私有 IP 位址。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。

在以下圖表中，可用區域 A 中的子網是公有子網。此子網的路由表具有可將所有網際網路綁定 IPv4 流量發送至網際網路閘道的路由。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，所以私有子網路中的執行個體即使擁有公用 IP 位址，也無法與網際網路通訊。



## 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

元件	預設 VPC	非預設 VPC
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)

如需預設 VPC 的詳細資訊，請參閱[預設 VPC](#)。如需有關建立 VPC 的詳細資訊，請參閱[建立 VPC](#)。

## 使用網際網路閘道

以下說明如何使用網際網路閘道，從 VPC 中的子網存取網際網路。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。

### 任務

- [建立網際網路閘道](#)
- [將網際網路閘道連接至 VPC](#)
- [將網際網路閘道自 VPC 分開](#)
- [刪除網際網路閘道](#)

## 建立網際網路閘道

使用下列程序建立網際網路閘道。

### 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。

## 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。

### 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. 依次選擇 Actions (動作)、Attach to VPC (連接至 VPC)。
5. 選取可用的 VPC。
6. 選擇 Attach internet gateway (連接網際網路閘道)。

### 將網際網路閘道自 VPC 分開

如果您不再需要透過網際網路存取在 VPC 中啟動的執行個體，則可以將網際網路閘道自 VPC 分離。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。

### 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. 選擇 Actions, Detach from VPC (動作、自 VPC 分離)。
5. 出現確認提示時，選擇 Detach internet gateway (分離網際網路閘道)。

### 刪除網際網路閘道

如果您不再需要網際網路閘道，可以予以刪除。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。

### 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)。

## API 和命令概觀

您可以使用命令列或 API 執行此頁面所述的任務。如需命令列界面的詳細資訊與可用的 API 動作清單，請參閱[使用 Amazon VPC](#)。

### 建立網際網路閘道

- [create-internet-gateway](#) (AWS CLI)
- [New-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

### 將網際網路閘道連接至 VPC

- [attach-internet-gateway](#) (AWS CLI)
- [Add-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

### 說明網際網路閘道

- [describe-internet-gateways](#) (AWS CLI)
- [Get-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

### 將網際網路閘道自 VPC 分離

- [detach-internet-gateway](#) (AWS CLI)
- [Dismount-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

### 刪除網際網路閘道

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

## 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](#)。

## 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。

### Note

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](#)。

### 內容

- [輸出限定網際網路閘道基本概念](#)
- [使用輸出限定網際網路閘道](#)
- [API 和 CLI 概觀](#)
- [定價](#)

## 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。

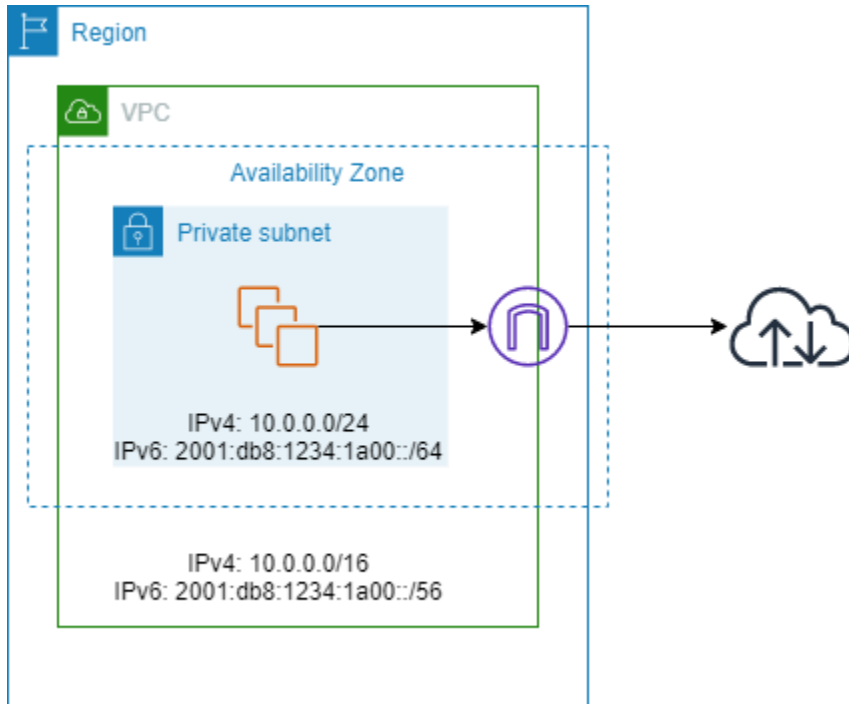
僅限輸出的網際網路閘道是可設定狀態的：它會將流量從子網路中的執行個體轉送至網際網路或其他 AWS 服務，然後將回應傳送回執行個體。

輸出限定網際網路閘道具有下列特性：

- 您無法建立安全群組與輸出限定網際網路閘道的關聯。您可以使用私有子網路中執行個體的安全群組，來控制進出這些執行個體的流量。

- 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。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00:/64	區域
::/0	<i>eigw-id</i>

## 使用輸出限定網際網路閘道

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

- [建立輸出限定網際網路閘道](#)



- [檢視您的輸出限定網際網路閘道](#)
- [建立自訂路由表](#)
- [刪除輸出限定網際網路閘道](#)

## 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。
- 對於 Value (值)，進入金鑰值。

[移除標籤] 選擇標籤「金鑰」和「值」右側移除。

5. 選取要在其中建立輸出限定網際網路閘道的 VPC。
6. 選擇 Create (建立)。

## 檢視您的輸出限定網際網路閘道

您可以在 Amazon VPC 主控台中檢視輸出限定網際網路閘道的相關資訊。

### 檢視輸出限定網際網路閘道的相關資訊

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. 選取要在詳細資訊窗格中檢視資訊的輸出限定網際網路閘道。

## 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](#)。

## 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)。

## API 和 CLI 概觀

您可以使用命令列或 API 執行此頁面所述的任務。如需命令列界面的詳細資訊與可用的 API 動作清單，請參閱[使用 Amazon VPC](#)。

### 建立輸出限定網際網路閘道

- [create-egress-only-internet-網關](#) ( ) 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-閘道](#) ( ) 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-網關](#) ( ) AWS CLI
- [Remove-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

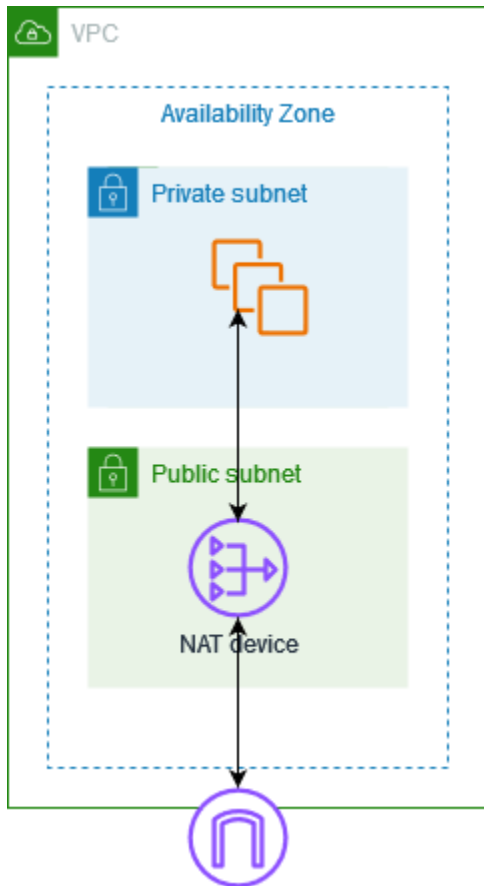
## 定價

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](#)。

## 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，該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到網際網路。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)。
- 您可以使用由 AWS NAT 閘道提供的受管 NAT 裝置，也可以在 EC2 執行個體 (稱為 NAT 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，使私有子網中的執行個體可以連線到 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) 私有子網中的執行個體可以透過公有 NAT 閘道連線到網際網路，但無法從網際網路接收來路不明的輸入連線。您可以在公有子網中建立公有 NAT 閘道，並且必須在建立時讓彈性 IP 地址與 NAT 閘道產生關聯。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 – 私有子網中的執行個體可以透過私有 NAT 閘道連線到其他 VPC 或您的內部部署網路。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 地址與私有 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。

私有和公有 NAT 閘道都會將執行個體的來源私有 IPv4 地址對應至 NAT 閘道的私有 IPv4 地址，但如果是公有 NAT 閘道，網際網路閘道則會將公有 NAT 閘道的私有 IPv4 地址對應至與 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。

### Important

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 地址 (除非您使用網際網路閘道)。公用 NAT 閘道僅會在與網際網路閘道搭配使用時，才會使用其 EIP 作為來源 IP 地址。

## 目錄

- [NAT 閘道基本概念](#)
- [控制 NAT 閘道的使用](#)
- [使用 NAT 閘道](#)
- [API 和 CLI 概觀](#)

- [API 閘道使用案例](#)
- [DNS64 和 NAT64](#)
- [使用 Amazon 監控 NAT 閘道 CloudWatch](#)
- [疑難排解 NAT 閘道](#)
- [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 [Amazon VPC 配額](#)。

若您在多個可用區域中皆有資源，且他們都共享同一個 NAT 閘道，則若 NAT 閘道的可用區域未運作時，其他可用區域中的資源都會喪失網際網路存取權。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 100 萬個封包，並自動擴展至每秒 1000 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 地址與 NAT 閘道關聯 (1 個主要 IPv4 地址和 7 個次要 IPv4 地址) 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 地址](#)。
- 您可以挑選要指派給 NAT 閘道的私有 IPv4 地址，或者使其從子網路的 IPv4 地址範圍自動指派。指派的私有 IPv4 地址會一直保留，直到您刪除私有 NAT 閘道。您無法將此私有 IPv4 地址分開，也無法連接其他私有 IPv4 地址。

- 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。
- 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 [使用網路 ACL 控制子網路的流量](#)。
- NAT 閘道會接收網路介面。您可以挑選要指派給介面的私有 IPv4 地址，或者使其從子網路的 IPv4 地址範圍自動指派。您可以使用 Amazon EC2 主控台檢視 NAT 閘道的網路介面。如需詳細資訊，請參閱 [檢視網路介面的詳細資訊](#)。您無法修改此網路介面的屬性。
- 您無法透過 VPC 對等連線將流量路由至 NAT 閘道。當流量透過虛擬私有閘道透過混合式連線 (網站對站台 VPN 或直 Connect 連線) 抵達時，您無法透過 NAT 閘道路由流量。當流量透過傳輸閘道透過混合式連線 (站台對站台 VPN 或直 Connect 連線) 抵達時，您可以透過 NAT 閘道路由流量。
- NAT 閘道支援最大傳輸單元 (MTU) 為 8500 的流量，但請務必注意下列事項：
  - 為了避免在使用公有 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。如需有關在執行個體上檢查和設定 MTU 的詳細資訊，請參閱 [Amazon EC2 使用者指南中的在 Linux 執行個體上檢查並設定 MTU](#)。
  - NAT 閘道支援透過需要的 ICMPv4 封包和封包過大 (PTB) 的路徑 MTU 探索 (PMTUD)。
  - NAT 閘道會對所有封包強制執行「最大區段大小 (MSS)」限制。如需詳細資訊，請參閱 [RFC879](#)。

## 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 Identity and Access Management](#)。

## 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

- [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](#)

## 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 EIP 數量，您將無法建立公有 NAT 閘道。如需 EIP 配額以及如何對其進行調整的詳細資訊，請參閱 [彈性 IP 地址](#)。
- 您可以將最多 8 個私有 IPv4 地址指派給私有 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 地址](#)。

### 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 EIP 指派給 NAT 閘道；或選擇配置彈性 IP，為公有 NAT 閘道自動配置 EIP。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 地址](#)。


#### Important

將 EIP 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。如需網路邊界群組和 EIP 的詳細資訊，請參閱 [配置彈性 IP 地址](#)。

2. (選用) 選擇其他設定，並在私有 IP 地址 - 選取下，輸入 NAT 閘道的私有 IPv4 地址。如果您沒有輸入位址，AWS 將會從 NAT 閘道所在的子網路隨機自動指派私人 IPv4 位址給 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 閘道的主要私人 IPv4 位址。對於自動指派的私人 IPv4 位址數目，您可以選擇性地指定 NAT 閘道的次要私人 IPv4 位址數目。AWS 從 NAT 閘道的子網路中隨機選擇這些 IP 位址。
  - 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」，請在自動指派的私人 IP 位址數目下，選擇要指 AWS 派給此私人 NAT 閘道的次要 IPv4 位址數目。您最多可以選擇 7 個 IPv4 地址。

 Note

次要 IPv4 地址是選用的，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 地址與 NAT

閘道關聯 (1 個主要 IPv4 地址和 7 個次要 IPv4 地址) 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 地址](#)。

您可以使用 [NAT 閘道 CloudWatch 度量 ErrorPort](#) 配置和 PacketsDrop 計數來判斷 NAT 閘道是否產生連接埠配置錯誤或丟棄封包。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，您才可以將次要 EIP 地址新增至公有 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 地址指派給私有 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 地址](#)。

### 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 自動選擇主要私人 IPv4 位址，您可以選擇是否 AWS 要指派最多 7 個次要私人 IPv4 位址以指派給 NAT 閘道。AWS 自動從 NAT 閘道所在的子網路中隨機選擇並指派這些資訊。
      - 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 地址的 EIP。此步驟為必要。您必須選取 EIP 以及私有 IPv4 地址。如果將私有 IP 地址指派方法選為自訂，則您也必須為新增的每個 EIP 輸入私有 IPv4 地址。

**⚠ 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。如需網路邊界群組和 EIP 的詳細資訊，請參閱 [配置彈性 IP 地址](#)。

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 EIP 都有預設配額限制。如需詳細資訊，請參閱 [彈性 IP 地址](#)。

- 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。如需使用標籤的相關資訊，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組織帳 AWS 單並反映自己的成本結構。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](#)。如需有關使用標籤設定成本分配報表的詳細資訊，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 Gateways (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 Gateways (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 [釋出彈性 IP 地址](#)。

## API 和 CLI 概觀

您可以使用命令列或 API 執行此頁面所述的任務。如需命令列介面的詳細資訊與可用的 API 操作清單，請參閱 [使用 Amazon VPC](#)。

### 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)
- [AssignPrivateNatGateway地址](#) (Amazon EC2 查詢 API)

### 將彈性 IP 地址 (EIP) 和私有 IPv4 地址與公有 NAT 閘道建立關聯

- [associate-nat-gateway-address](#) (AWS CLI)
- [Register-EC2NatGatewayAddress](#) (AWS Tools for Windows PowerShell)
- [AssociateNatGatewayAddress](#)(Amazon EC2 查詢 API)

## 建立 NAT 閘道

- [create-nat-gateway](#) (AWS CLI)

- [New-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [CreateNat閘道](#) (Amazon EC2 查詢 API)

### 刪除 NAT 閘道

- [delete-nat-gateway](#) (AWS CLI)
- [Remove-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [DeleteNat閘道](#) (Amazon EC2 查詢 API)

### 描述 NAT 閘道

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [DescribeNat閘道器](#) (Amazon EC2 查詢 API)

### 取消次要彈性 IP 地址 (EIP) 與公有 NAT 閘道的關聯

- [disassociate-nat-gateway-address](#) (AWS CLI)
- [Unregister-EC2NatGatewayAddress](#) (AWS Tools for Windows PowerShell)
- [DisassociateNatGatewayAddress](#)(Amazon EC2 查詢 API)

### 為 NAT 閘道新增標籤

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)
- [CreateTags](#)(Amazon EC2 查詢 API)

### 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)
- [UnassignPrivateNatGateway地址](#) (Amazon EC2 查詢 API)

## 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

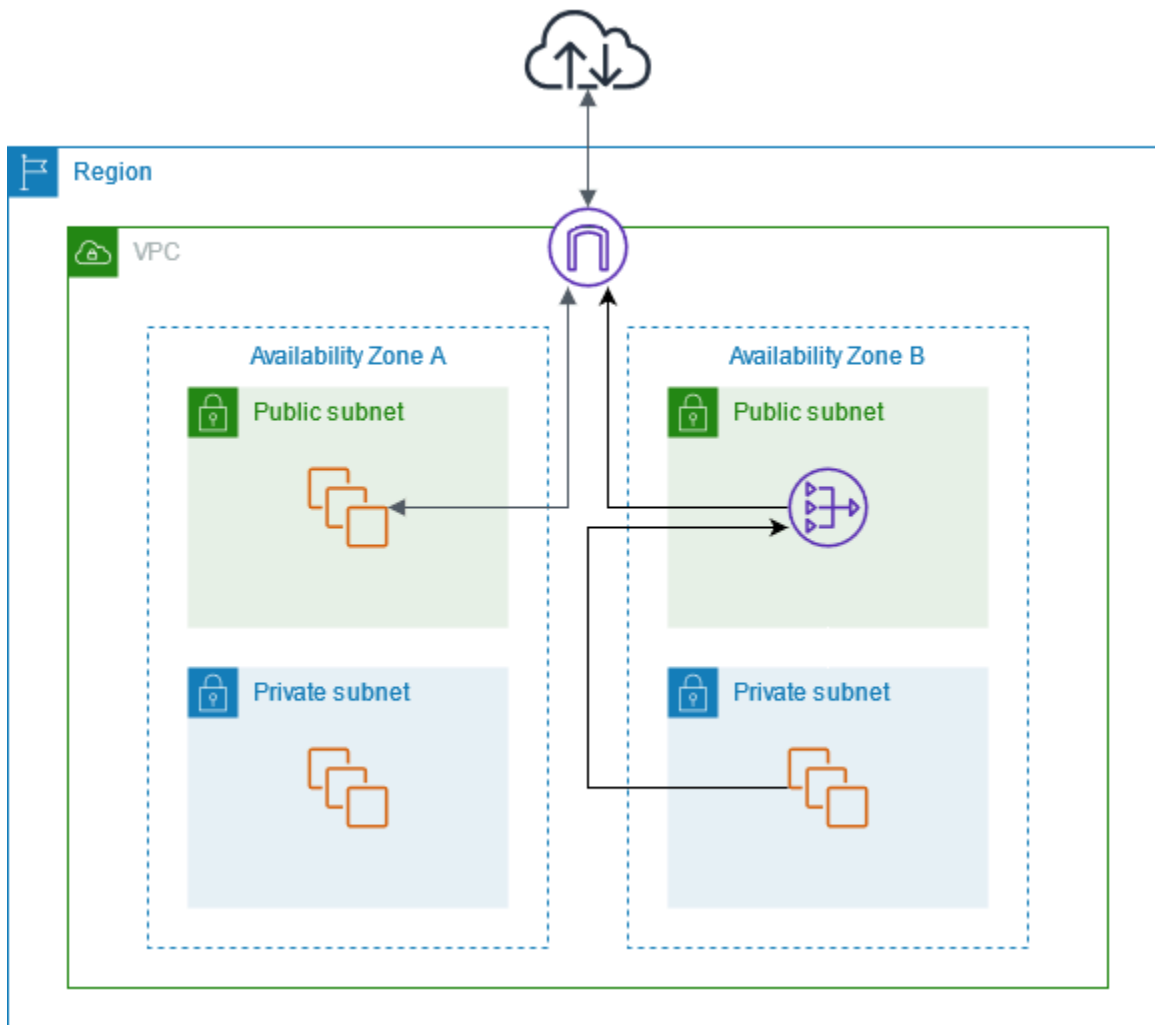
您可以使用公有 NAT 閘道讓私有子網中的執行個體能將傳出流量傳送到網際網路，同時阻止網際網路建立與執行個體的連線。

### 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。私有和公有 NAT 閘道都會將執行個體的來源私有 IPv4 地址對應至私有 NAT 閘道的私有 IPv4 地址，但在公有 NAT 閘道的情況下，網際網路閘道會將公有 NAT 閘道的私有 IPv4 地址對應至與 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。



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，您也可以在每个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。

目的地	目標
<i>VPC CIDR</i>	區域
0.0.0.0/0	<i>internet-gateway-id</i>

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。

目的地	目標
<i>VPC CIDR</i>	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。

目的地	目標
<i>VPC CIDR</i>	區域
0.0.0.0/0	<i>internet-gateway-id</i>

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。

目的地	目標
<i>VPC CIDR</i>	區域
0.0.0.0/0	<i>nat-gateway-id</i>

如需詳細資訊，請參閱 [the section called “使用路由表”](#)。

### 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 地址應為 NAT 閘道的彈性 IP 地址。

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。確認您的安全群組規則允許來自您本機網路 IP 地址範圍的傳入 SSH 流量，以及目標為您私有子網 IP 地址範圍的傳出 SSH 流量 (您也可以針對此測試對傳入和傳出 SSH 流量使用 `0.0.0.0/0`)。
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 轉換私密金鑰](#)。
3. 啟動 Pageant，在任務列的 Pageant 圖示 (可能隱藏) 上按一下滑鼠右鍵，然後選擇 Add Key (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 [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

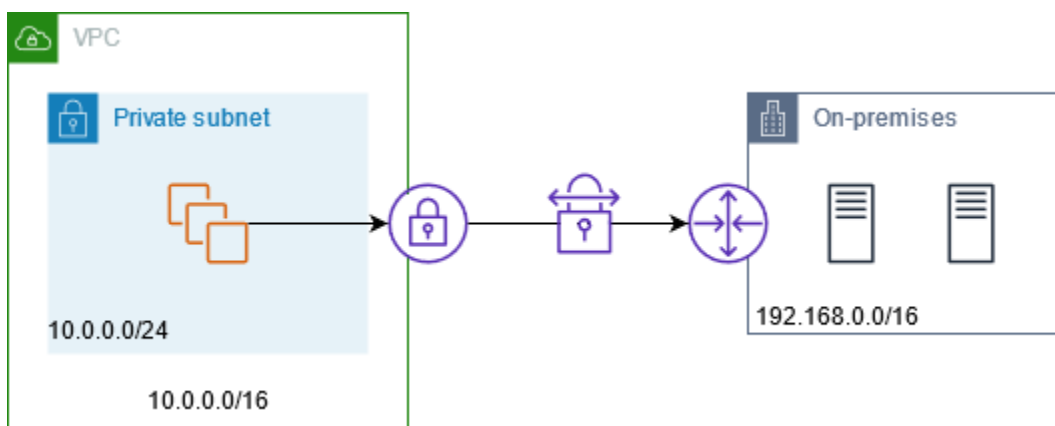
您可以使用私有 NAT 閘道，利用允許清單中的地址集區，實現從 VPC 對內部部署網路的通訊。您可以經由具有允許清單 IP 地址範圍內 IP 地址的私有 NAT 閘道，路由來自以內部部署網路為目的地的子網的流量，而不用從允許清單 IP 地址範圍中為每個執行個體指派單獨的 IP 地址。

### 目錄

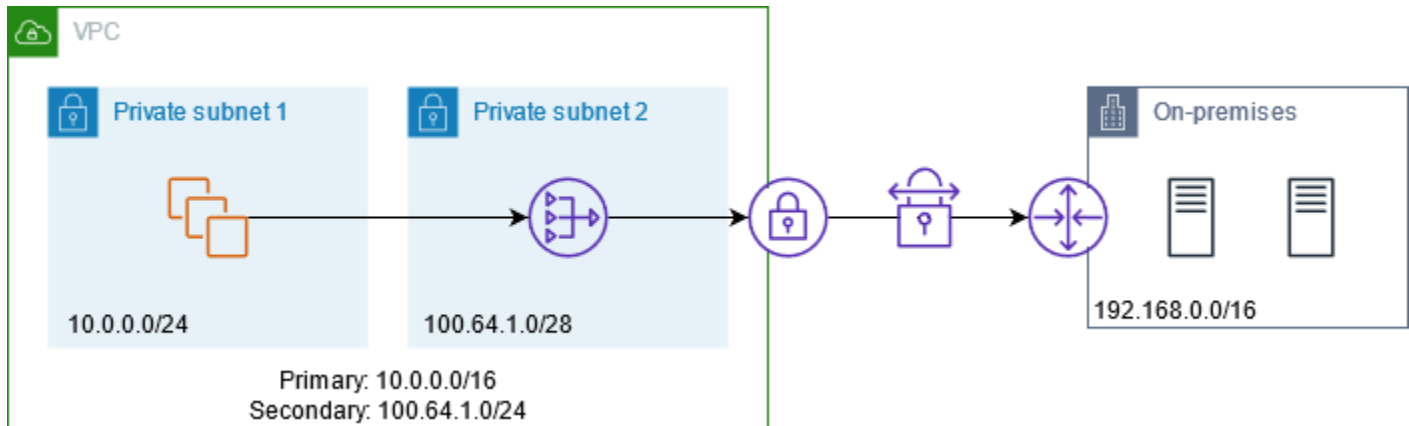
- [概要](#)
- [資源](#)
- [路由](#)

### 概要

下圖顯示執行個體如何透過存取內部部署資源 AWS 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。



## 資源

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。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.1.0/24</i>	本機

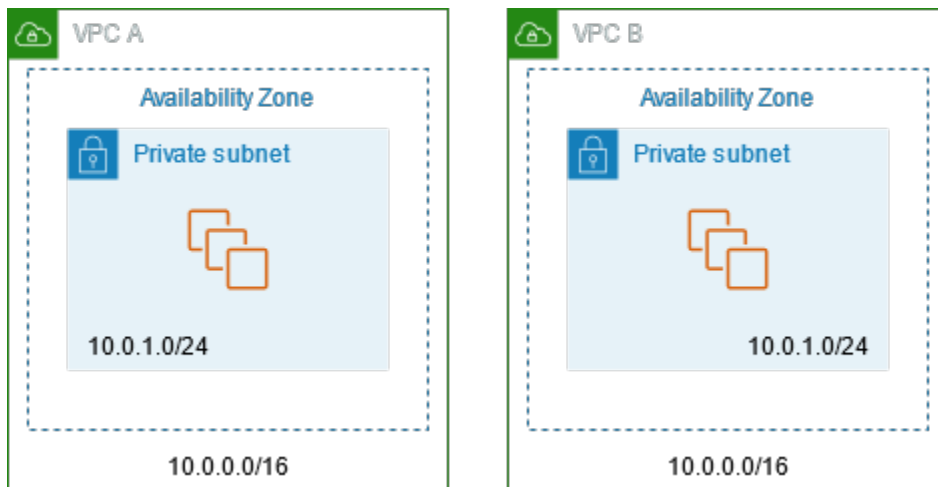
目的地	目標
<i>192.168.0.0/16</i>	<i>nat-gateway-id</i>

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。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.1.0/24</i>	本機
<i>192.168.0.0/16</i>	<i>vgw-id</i>

### 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

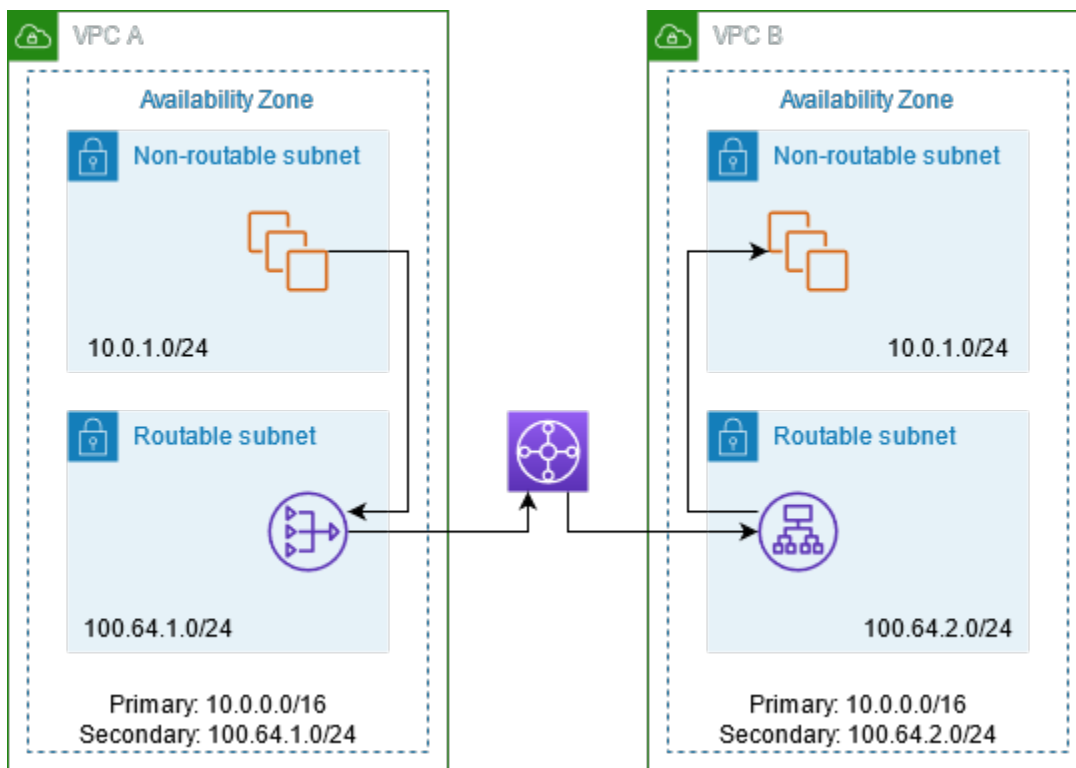
- [概要](#)
- [資源](#)
- [路由](#)

## 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地址範圍可以重疊 (不可路由地址範圍)，而哪些範圍不能重疊 (可路由地址範圍)。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。

以 VPC B 不可路由子網中的執行個體為目的地之來自 VPC A 不可路由子網中的執行個體的流量經由私有 NAT 閘道發送，然後路由至傳輸閘道。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。



## 資源

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。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.1.0/24</i>	本機
<i>100.64.2.0/24</i>	<i>nat-gateway-id</i>

以下為 VPC A 中可路由子網的路由表。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.1.0/24</i>	本機
<i>100.64.2.0/24</i>	<i>transit-gateway-id</i>

以下為 VPC B 中不可路由子網的路由表。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.2.0/24</i>	本機

以下為 VPC B 中可路由子網的路由表。

目的地	目標
<i>10.0.0.0/16</i>	本機
<i>100.64.2.0/24</i>	本機
<i>100.64.1.0/24</i>	<i>transit-gateway-id</i>

以下為傳輸閘道路由表。

CIDR	連接	路由類型
<i>100.64.1.0/24</i>	<i>VPC A ###</i>	靜態
<i>100.64.2.0/24</i>	<i>VPC B ###</i>	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 或不同虛擬私人雲端、內部部署網路或網際網路中的 IPv4 資源進行通訊。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，僅限 IPv4 服務的 DNS 查詢將產生 IPv4 目的地地址作為回應，而且您的僅限 IPv6 服務無法與其通訊。若要彌補此通訊差距，您可以為子網路啟用 DNS64，並將其套用至該子網路內的所有 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，您需要透過 NAT 閘道路由此流量，該閘道會對流量執行必要的轉譯，以允許子網中的 IPv6 服務存取該子網外的 IPv4 服務。

您可以使用 AWS CLI 或使用 VPC 主控台使用[修改子網路屬性，在子網路上啟用或停用 DNS64](#)，方法是選取子網路，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 封包的目的地是 NAT 閘道，閘道會接收封包並透過以主機的 IPv6 地址來取代其 IP (目的地 IP) 並將 64:ff9b::/96 預先加回來源 IPv4 地址的方式來取消其 NAT。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

- [透過 AWS CLI 來啟用與網際網路上僅限 IPv4 的服務之通訊](#)
- [在您的內部部署環境啟用中啟用與僅限 IPv4 的服務之通訊](#)

## 透過 AWS CLI 來啟用與網際網路上僅限 IPv4 的服務之通訊

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 閘道的子網路應具有指向網際網路閘道路 0.0.0.0/0 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。
- 既然您已經設定 Route 53 Resolver 輸出端點，您必須在包含僅限 IPv6 的工作負載之子網上啟用 DNS64，並透過 NAT 閘道路由目的地為內部部署網路的任何資料。

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，則記錄會保持內容原貌，但如果僅包含 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。

## 使用 Amazon 監控 NAT 閘道 CloudWatch

您可以使用來監控 NAT 閘道 CloudWatch，該閘道會從 NAT 閘道收集資訊，並建立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。NAT 閘道指標資料會以每分鐘一次的間隔提供，統計資訊的記錄會保留 15 個月。

有關 Amazon 的更多信息 CloudWatch，請參閱 [Amazon CloudWatch 用戶指南](#)。如需有關定價的詳細資訊，請參閱 [Amazon CloudWatch 定價](#)。

### 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	<p>通過 NAT 閘道的並行作用中 TCP 連線的總數。</p> <p>0 值表示沒有作用中連線通過 NAT 閘道。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Max。</p>
BytesInFromDestination	<p>NAT 閘道接收到來自目的地的位元組數量。</p> <p>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。</p> <p>單位：位元組</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
BytesInFromSource	<p>NAT 閘道接收到來自您的 VPC 中的用戶端的位元組數量。</p>

指標	描述
	<p>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。</p> <p>單位：位元組</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
BytesOutToDestination	<p>透過 NAT 閘道送出至目的地的位元組數量。</p> <p>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。</p> <p>單位：位元組</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
BytesOutToSource	<p>透過 NAT 閘道送出至您的 VPC 中的用戶端的位元組數量。</p> <p>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。</p> <p>單位：位元組</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>

指標	描述
ConnectionAttemptCount	<p>透過 NAT 閘道嘗試連線的數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
ConnectionEstablishedCount	<p>透過 NAT 閘道建立的連線數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
ErrorPortAllocation	<p>NAT 閘道無法配置來源連接埠的次數。</p> <p>大於 0 的值表示，有過多的並行連線透過 NAT 閘道開啟。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>

指標	描述
IdleTimeoutCount	<p>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。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
PacketsDropCount	<p>NAT 閘道捨棄的封包數量。</p> <p>若要以整體封包流量的百分比計算捨棄的封包數目，請使用以下公式：<math>PacketsDropCount / (PacketsInFromSource + PacketsInFromDestination) * 100</math>。如果此值超過 NAT 閘道上總流量的 0.01%，則可能是 Amazon VPC 服務發生問題。使用<a href="#">AWS 服務健全狀況儀表板</a>來識別可能導致 NAT 閘道丟棄封包的服務問題。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
PacketsInFromDestination	<p>NAT 閘道接收到來自目的地的封包數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>

指標	描述
PacketsInFromSource	<p>NAT 閘道接收到來自您的 VPC 中的用戶端的封包數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
PacketsOutToDestination	<p>透過 NAT 閘道送出至目的地的封包數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>
PacketsOutToSource	<p>透過 NAT 閘道送出至您的 VPC 中的用戶端的封包數量。</p> <p>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。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Sum。</p>



指標	描述
PeakBytesPerSecond	<p>此指標報告一分鐘內每秒最高 10 秒位元組的平均值。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Maximum。</p>
PeakPacketsPerSecond	<p>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)。</p> <p>單位：計數</p> <p>統計資訊：最實用的統計資訊是 Maximum。</p>

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。

### 檢視 NAT 閘道 CloudWatch 指標

NAT 閘度量度會以 1 分鐘的間隔傳送到 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. [請在以下位置開啟 CloudWatch 主控台。](https://console.aws.amazon.com/cloudwatch/) <https://console.aws.amazon.com/cloudwatch/>
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。

#### 若要使用 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 警示以監控 NAT 閘道

您可以建立 CloudWatch 警示，在警示狀態變更時傳送 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. [請在以下位置開啟 CloudWatch 主控台。](https://console.aws.amazon.com/cloudwatch/) <https://console.aws.amazon.com/cloudwatch/>
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。取得指標後，請選取 NAT 閘道 BytesOutToDestination 量度旁的核取方塊，然後選擇 [選取量度]。
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. [請在以下位置開啟 CloudWatch 主控台。](https://console.aws.amazon.com/cloudwatch/) <https://console.aws.amazon.com/cloudwatch/>
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。取得指標後，請選取 NAT 閘道ErrorPortAllocation量度旁的核取方塊，然後選擇 [選取量度]。
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 使用 CloudWatch 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 IP 地址。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-xxxxxxx 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。如需更多詳細資訊，請參閱 <a href="#">使用網際網路閘道</a> 。

顯示的錯誤	原因	解決方案
彈性 IP 地址 eipalloc-xxxxxxx 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。如需更多詳細資訊，請參閱 <a href="#">使用彈性 IP 地址</a> 。

## 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。

如果您無法存取遠端伺服器，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

執行下列任意一項：

- 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 地址的 NAT 閘道，或將次要 IP 地址新增至現有的 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](#)。

## 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，您也可以在各個可用區域中建立包含資源的 NAT 閘道。
- 如果通過 NAT 閘道的大多數流量都是傳輸到支援介面端點或閘道端點的 AWS 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 上，該版本於 2020 年 12 月 31 日終止標準支援，維護支援於 2023 年 12 月 31 日終止。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[移轉至 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 NAT 執行個體比 NAT 閘道更符合您的使用案例，您可以從目前版本的 Amazon Linux 建立自己的 NAT AMI，如中所述[the section called “建立 NAT AMI”](#)。

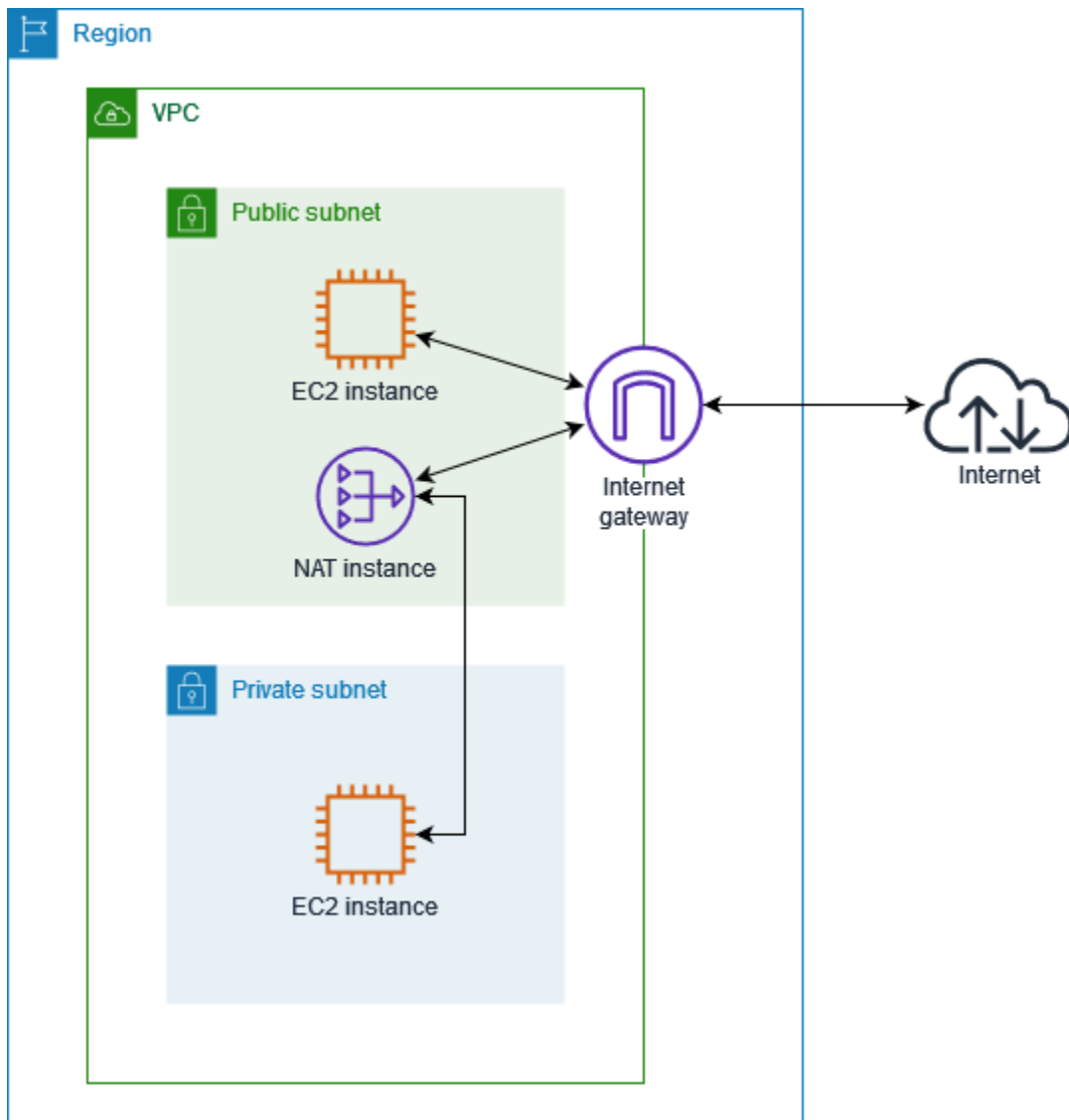
## 目錄

- [NAT 執行個體基本概念](#)
- [為 NAT 執行個體建立 VPC](#)
- [為 NAT 執行個體建立安全群組](#)
- [建立 NAT AMI](#)
- [啟動 NAT 執行個體](#)
- [停用來源/目標檢查](#)
- [更新路由表](#)
- [測試 NAT 執行個體](#)

## 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](#)。

## 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. 前往 <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。

## 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。

下列是建議的規則。

### 傳入

來源	通訊協定	連接埠範圍	評論
<i>##### CIDR</i>	TCP	80	允許來自私有子網路伺服器的傳入 HTTP 流量
<i>##### CIDR</i>	TCP	443	允許來自私有子網路伺服器的傳入 HTTPS 流量
<i>##### IP #####</i>	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)

### 傳出

目的地	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 [安全群組](#)。

## 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 建立的網路介面，`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](#)。

## 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. 在 <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 [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 [更新路由表](#))。

## 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. 在 <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)。

## 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](#)。

## 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. 在 <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 [將私有金鑰轉換為 .ppk 格式](#)。

啟動 Pageant，在任務列的 Pageant 圖示 (可能隱藏) 上按一下滑鼠右鍵，然後選擇 Add Key (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  
...
```

## 故障診斷

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 [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 [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。
維護	由管理 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。

屬性	NAT 閘道	NAT 執行個體
類型和大小	統一提供；您不需要選擇類型或大小。	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。
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 <a href="#">NAT 閘道的 CloudWatch 指標</a> 。	檢視執行處理的 CloudWatch 測量結果。
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。

屬性	NAT 閘道	NAT 執行個體
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 地址是針對動態雲端運算設計的靜態公有 IPv4 地址。您可以將彈性 IP 位址與您帳戶之任意 VPC 的執行個體或網路介面建立關聯。透過彈性 IP 地址，您可以快速地將地址重新映射至您 VPC 中的另一個執行個體，藉以遮罩執行個體的故障。

## 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 地址將保持分配給您的 AWS 帳戶，直到您明確釋放它。

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，即可將網路界面的所有屬性從一個執行個體移至另一個執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的[彈性網路界面](#)。

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 地址與您執行個體的 eth0 網路界面建立關聯，即會向 EC2-VPC 公有 IP 地址集區釋出其目前的公有 IPv4 地址 (如果有的話)。如果您取消彈性 IP 地址的關聯，則會在幾分鐘內自動將新的公有 IPv4 地址指派給 eth0 網路界面。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。如需更多詳細資訊，請參閱 [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。如需使用自己 IP 位址的相關資訊，請參閱 Amazon EC2 使用者指南中的使用 [自己的 IP 位址 \(BYOIP\)](#)。

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](#)。

## 使用彈性 IP 地址

下列各節說明如何使用彈性 IP 地址。

### 任務

- [配置彈性 IP 地址](#)
- [建立彈性 IP 地址的關聯](#)
- [檢視您的彈性 IP 地址](#)
- [為彈性 IP 地址套用標籤](#)
- [取消彈性 IP 地址的關聯](#)
- [轉移彈性 IP 地址](#)
- [釋出彈性 IP 地址](#)

- [復原彈性 IP 地址](#)
- [API 和命令概觀](#)

## 配置彈性 IP 地址

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 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. 選擇 Allocate Elastic IP address (配置彈性 IP 地址)。
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 (AZ)、Local Zones 或 Wavelength 區域的集合，用於通 AWS 告公用 IP 位址。Local Zones 和 Wavelength 區域可能具有與區域中的 AZ 不同的網路邊界組，以確保 AWS 網絡與訪問這些區域中資源的客戶之間的最小延遲或物理距離。

#### Important

您必須在與 EIP 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。請謹慎選擇網路邊界群組，因為 EIP 及其關聯的 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。

- 我的公用 IPv4 位址集區 — 如果您想要從您帶入帳戶的 IP 位址集區配置 IPv4 位址。AWS 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。
- 對於 Value (值)，進入金鑰值。

[移除標籤] 選擇標籤「金鑰」和「值」右側移除。

7. 選擇 Allocate (配置)。

## 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 (網路介面)，然後選取執行個體或網路介面 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)。

## 檢視您的彈性 IP 地址

您可以檢視分配給您帳戶的彈性 IP 位址。

檢視您的彈性 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. 若要篩選顯示的清單，請開始在搜尋方塊中輸入彈性 IP 位址的一部分或其屬性之一。

## 為彈性 IP 地址套用標籤

您可將標籤套用到您的彈性 IP 地址，以利您依據組織需求加以識別或分類。

### 為彈性 IP 地址套用標籤

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 地址，然後選擇 Tags (標籤)。
4. 選擇 Manage tags (管理標籤)，輸入需要的標籤金鑰和值，然後選擇 Save (儲存)。

## 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)。

## 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 位址傳輸，快速將工作負載從一個移 AWS 帳戶 至另一個。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。
- 集中式安全性管理 — 使用集中式 AWS 安全性帳戶來追蹤和傳輸已針對安全性合規審查的彈性 IP 位址。

- 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 地址無需付費。

## 任務

- [啟用彈性 IP 地址轉移](#)
- [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 地址轉移

本節旨在說明如何接受轉移後的彈性 IP 地址。請注意下列與啟用彈性 IP 地址轉移的相關限制：

- 您可以將彈性 IP 地址從任何 AWS 帳戶（源帳戶）轉移到同一 AWS 區域中的任何其他 AWS 帳戶（轉移帳戶）。
- 當您轉移彈性 IP 地址時，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 地址轉移。在這七天內，來源帳戶可以檢視擱置中的傳輸（例如，在 AWS 主控台中或使用[描述-位址-傳輸命](#) AWS CLI 令）。七天後轉移將到期，屆時彈性 IP 地址的擁有權會回到來源帳戶。
- 在接受傳輸後的三天內，來源帳戶可以看到接受的傳輸（例如在 AWS 主控台中或使用[描述位址-傳輸](#) AWS CLI 命令）。
- AWS 不會通知轉移帳戶有關待處理的彈性 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 地址轉移的請求。
- 轉移完成時，會重設與要轉移之彈性 IP 地址相關的所有標籤。
- 您無法轉移從您 AWS 帳戶帶入的公用 IPv4 位址集區配置的彈性 IP 位址，通常稱為自攜 IP (BYOIP) 位址集區。
- 如果您嘗試轉移的彈性 IP 地址，具有與其相關聯的反向 DNS 記錄，您可以開始轉移程序，但轉移帳戶無法接受轉移，除非移除相關聯的 DNS 記錄。
- 如果您已啟用並設定 AWS Outposts，則可能已從客戶擁有的 IP 位址集區 (CoIP) 配置彈性 IP 位址。您無法轉移從 CoIP 配置的彈性 IP 地址。但是，您可以使 AWS RAM 用與另一個帳戶共享 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 地址](#)。
- 您可使用 Amazon VPC IPAM 來追蹤彈性 IP 地址在 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 地址歷程記錄)。如果將彈性 IP 地址轉移至組織外部的 AWS 帳戶，就會失去彈性 IP 地址的 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 地址轉移

1. 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 地址，然後選擇 Actions (動作)、Enable transfer (啟用轉移)。
5. 如果要轉移多個彈性 IP 地址，您會看到 Transfer type (轉移類型) 選項。請選擇下列其中一個選項：
  - 如果要將彈性 IP 地址傳輸到單個帳戶，請選擇單個 AWS 帳戶。
  - 如果要將彈性 IP 地址傳輸到多個帳戶，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 地址轉移至哪個 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 地址轉移

1. 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 地址，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 地址。

當您轉移彈性 IP 地址時，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 地址轉移。在這七天內，來源帳戶可以檢視擱置中的傳輸 (例如，在 AWS 主控台中或使用[描述-位址-傳輸命 AWS CLI 令](#))。七天後轉移將到期，屆時彈性 IP 地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：

- AddressLimit已超過：如果您的移轉帳戶已超過彈性 IP 位址配額，則來源帳戶可以啟用彈性 IP 位址傳輸，但是當移轉帳戶嘗試接受移轉時，就會發生此例外狀況。根據預設，每個區域的所有 AWS 帳戶限制為 5 個彈性 IP 位址。如需提高[限制的指示](#)，請參閱 [Amazon EC2 使用者指南中的彈性 IP 地址限制](#)。
- InvalidTransfer。AddressCustomPtrSet: 如果您或組織中的某人已設定您嘗試轉移的彈性 IP 位址以使用反向 DNS 查閱，則來源帳戶可以啟用彈性 IP 位址的傳輸，但是當移轉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 地址的 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 地址與 ENI 或 EC2 執行個體相關聯，則來源帳戶可以為彈性 IP 地址啟用傳輸，但是當轉移帳戶嘗試接受傳輸時，會發生此例外狀況。若要解決這個問題，來源帳戶必須取消與該彈性 IP 地址的關聯。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的[取消彈性 IP 地址的關聯](#)。

如有任何其他異常情況，[請聯絡 AWS Support](#)。

這些步驟必須由轉移帳戶完成。

### 接受彈性 IP 地址轉移

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 地址有關的所有標籤都不會隨著該彈性 IP 地址轉移。如果您要為接受的彈性 IP 地址定義 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 地址。
7. 如果您要接受多個轉移的彈性 IP 地址，請選擇 Add address (新增位址)，以輸入其他彈性 IP 地址。
8. 選擇提交。

## 釋出彈性 IP 地址

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 地址都會產生費用。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)。

## 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 地址已分配給其他 AWS 帳戶，或者如果恢復它導致您超出彈性 IP 地址配額，則無法恢復該地址。

您可以使用 Amazon EC2 API 或命令列工具來復原彈性 IP 地址。

若要使用復原彈性 IP 位址 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
```

## API 和命令概觀

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 地址

- [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 地址的關聯

- [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 地址

- [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)

## 定價

為了確保有效使用彈性 IP 地址，我們會收取少量的計時費用。如需詳細資訊，請參閱 [《Amazon VPC 定價》](#) 中的公有 IPv4 地址。

## 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 AWS Direct Connect 連接之間路由流量。如需詳細資訊，請參閱 [AWS 傳輸閘道](#)。

下表說明了傳輸閘道的一些常見使用案例，並提供 Amazon VPC 傳輸閘道的詳細資訊連結。

範例	用量
集中式路由器	將傳輸閘道設定為集中式路由器，用以連接所有的 VPC、AWS Direct Connect 和 AWS Site-to-Site VPN 連接。如需詳細資訊，請參閱 <a href="#">範例：集中式路由器</a> 。
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。如需詳細資訊，請參閱 <a href="#">範例：隔離式 VPC</a> 。
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 <a href="#">範例：隔離式 VPC 與共享服務</a> 。

## 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。

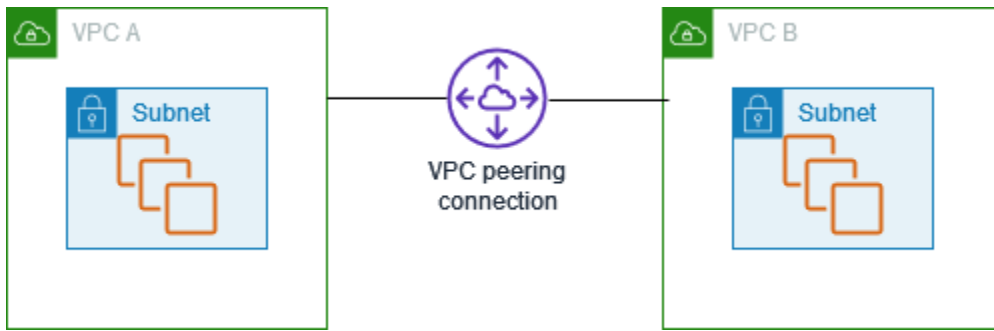
VPN 連線選項	描述
AWS Site-to-Site VPN	您可在您的 VPC 與您的遠端網路之間建立 IPsec VPN 連接。在 Site-to-Site VPN 連接的 AWS 端上，虛擬私有閘道或傳輸閘道會提供兩個 VPN 端點 (通道) 用於自動容錯移轉。您在 Site-to-Site VPN 連線的遠端配置您的客戶閘道裝置。如需詳細資訊，請參閱 <a href="#">《AWS Site-to-Site VPN 使用者指南》</a> 。
AWS Client VPN	AWS Client VPN 是以用戶端為基礎的受管 VPN 服務，能讓您安全地存取您的 AWS 資源或您的內部部署網路。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 <a href="#">AWS Client VPN 管理員指南</a> 。
AWS VPN CloudHub	如有多個遠端網路 (例如多個分公司)，您可透過您的虛擬私有閘道建立多個 AWS Site-to-Site VPN 連接，讓這些網路能彼此通訊。如需詳細資訊，請參閱 <a href="#">《AWS Site-to-Site VPN 使用者指南》</a> 中的 <a href="#">使用 VPN CloudHub 提供網站間的安全通訊</a> 。
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 <a href="#">AWS Marketplace</a> 中尋找第三方軟體 VPN 應用裝置。

您也可以使用 AWS 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 [《AWS Direct Connect 使用者指南》](#) 中的 [什麼是 AWS Direct Connect?](#)。

## 使用 VPC 對等互連來連線 VPC

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。您可以為其他 AWS 帳戶中的 VPC，或是不同

AWS 區域中的 VPC，與您的不同 VPC 之間建立 VPC 對等連線。對等 VPC 之間的流量不會周遊公用網際網路。



AWS 會使用現有的 VPC 基礎設施建立 VPC 對等互連。VPC 對等互連不是閘道，也不是 AWS Site-to-Site VPN 連線，且不倚賴另一個實體硬體。因此不會有通訊的單一故障點或頻寬瓶頸問題。

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 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

您可以使用 AWS CloudTrail 來擷取有關對 Amazon VPC API 進行呼叫的詳細資訊。您可以使用產生的 CloudTrail 日誌來判斷提出了哪些呼叫、提出呼叫的來源 IP 地址、提出呼叫的人員及時間等。如需詳細資訊，請參閱 Amazon EC2 API 參考中的 [使用 AWS CloudTrail 記錄 Amazon EC2、Amazon EBS 及 Amazon VPC API 呼叫的日誌](#)。

# 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。流程日誌資料可以發佈到下列位置：Amazon CloudWatch 日誌、Amazon S3 或亞馬遜資料 Firehose。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 的流程記錄。如需第 6 版中引入的傳輸閘道流程日誌的相關資訊，請參閱 Amazon VPC Transit Gateway 道使用者指南中的使用傳輸閘道[流量記錄網路](#)流量記錄。

## 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](#)
- [將流程記錄發佈到 CloudWatch 記錄](#)
- [將流量日誌發佈到 Amazon S3](#)
- [將流程日誌發佈到 Amazon 資料 Firehose](#)
- [使用 Amazon Athena 查詢流量日誌](#)
- [疑難排解 VPC 流量日誌](#)

## 流量日誌基礎知識

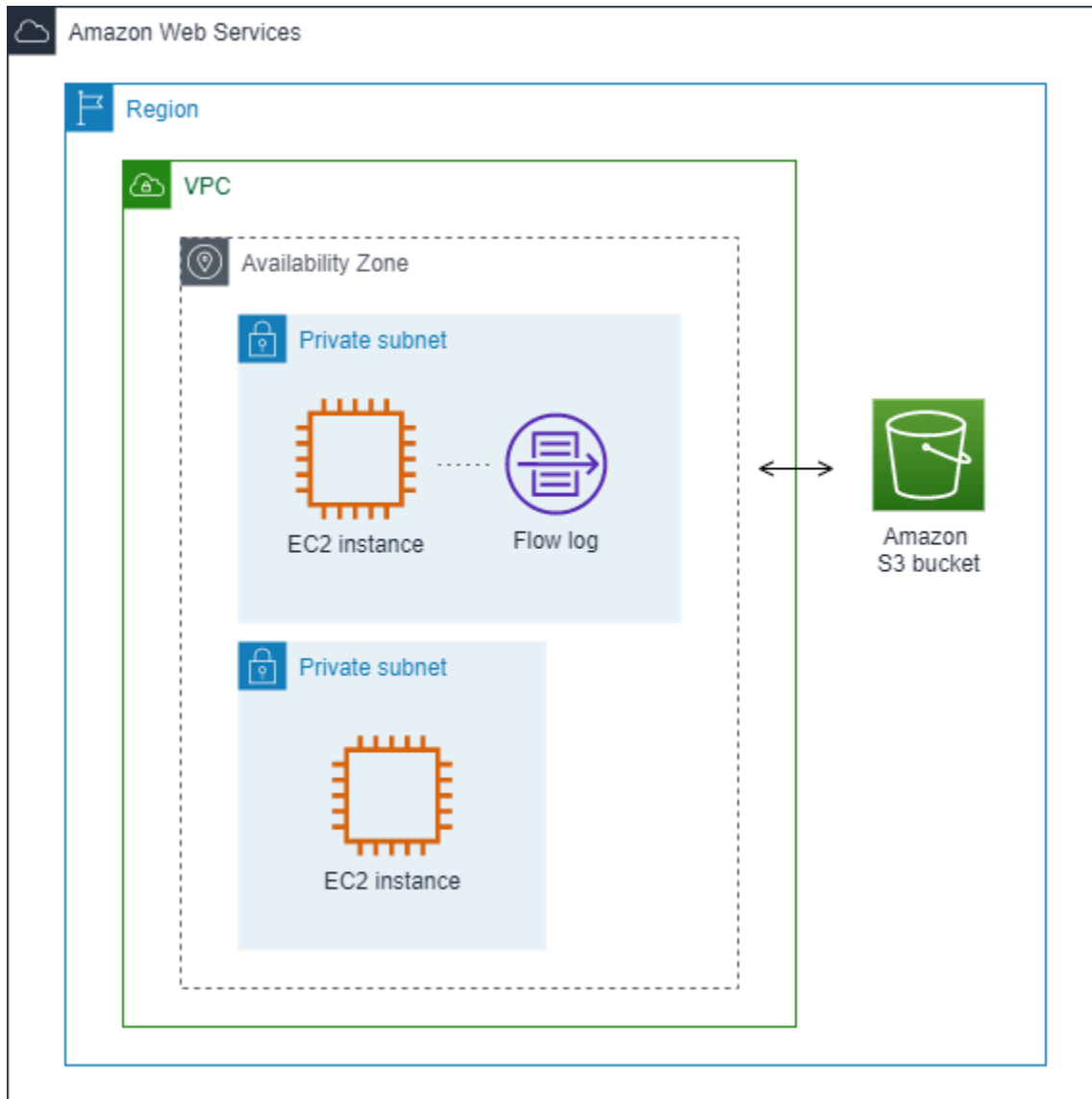
您可以建立 VPC、子網或網路介面的流量日誌。如果建立子網或 VPC 的流量日誌，則會監控該子網或 VPC 中的每個網路介面。

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](#)。

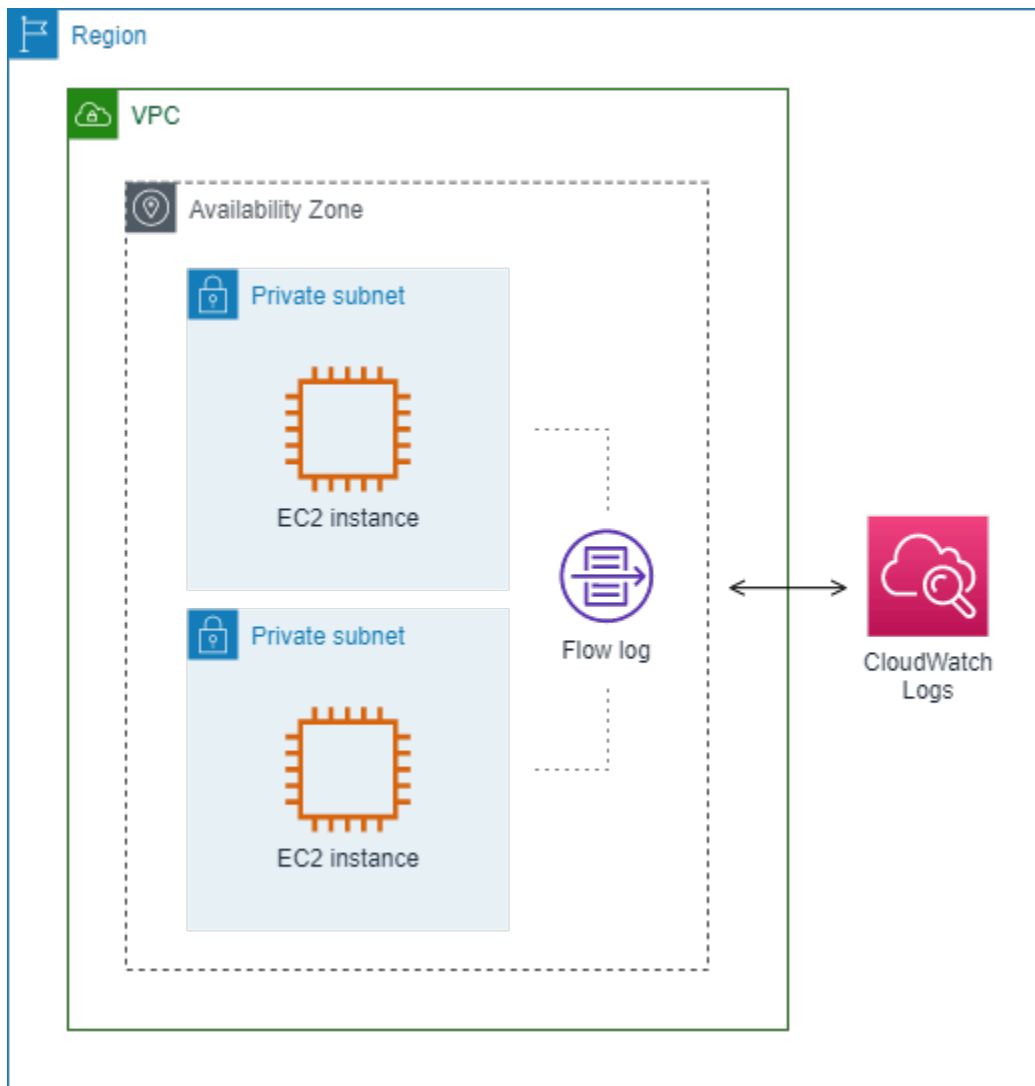
若要建立流量日誌，您要指定：

- 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，流程記錄會擷取子網路的所有流量，並將流程日誌記錄發佈到 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 [建立流量日誌](#)。

如果您在為子網路或 VPC 建立流程日誌後將執行個體啟動到子網路，我們會在網路介面有網路流量後立即為新網路介面建立 CloudWatch 日誌串流 (針對日誌) 或日誌檔物件 (適用於 Amazon S3)。

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 [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。

在彙總間隔內擷取資料後，處理資料並將其發佈到 CloudWatch 日誌或 Amazon S3 需要額外的時間。流程日誌服務通常在 5 分鐘內將 CloudWatch 日誌交付到日誌，並在大約 10 分鐘內將日誌交付到 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之擁有者的 AWS 帳戶 ID。如果網路介面是由 AWS 服務建立的，例如建立 VPC 端點或 Network Load Balancer 時，可能會顯示此欄位 unknown 的記錄。  Parquet 資料類型：STRING	2

欄位	描述	版本
interface-id	要記錄流量的網路介面 ID。  Parquet 資料類型：STRING	2
srcaddr	網路介面上傳入流量的來源地址，或傳出流量網路介面的 IPv4 或 IPv6 地址。網路介面的 IPv4 地址永遠都是其私有 IPv4 地址。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。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 <a href="#">指派的網際網路通訊協定號碼</a> 。  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
bytes	在流量期間傳輸的位元組數。  Parquet 資料類型：INT_64	2

欄位	描述	版本
start	<p>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。</p> <p>Parquet 資料類型：INT_64</p>	2
end	<p>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。</p> <p>Parquet 資料類型：INT_64</p>	2
action	<p>與流量相關聯的動作：</p> <ul style="list-style-type: none"> <li>• ACCEPT – 已接受流量。</li> <li>• 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。</li> </ul> <p>Parquet 資料類型：STRING</p>	2
log-status	<p>流量日誌的記錄狀態：</p> <ul style="list-style-type: none"> <li>• OK – 資料正常記錄至選擇的目的地。</li> <li>• 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。</li> <li>• 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。</li> </ul> <p>Parquet 資料類型：STRING</p>	2
vpc-id	<p>包含要記錄流量之網路介面的 VPC ID。</p> <p>Parquet 資料類型：STRING</p>	3
subnet-id	<p>包含要記錄流量之網路介面的子網 ID。</p> <p>Parquet 資料類型：STRING</p>	3

欄位	描述	版本
instance-id	<p>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<a href="#">請求者管理網路介面</a>的 '-' 符號，例如 NAT 閘道的網路介面。</p> <p>Parquet 資料類型：STRING</p>	3
tcp-flags	<p>下列 TCP 標記的位元遮罩值：</p> <ul style="list-style-type: none"> <li>• FIN – 1</li> <li>• SYN – 2</li> <li>• RST – 4</li> <li>• SYN-ACK – 18</li> </ul> <p>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，標誌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。</p> <p>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<a href="#">TCP 標記序列</a>。</p> <p>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 <a href="#">TCP segment structure</a> (TCP 區段結構)。</p> <p>Parquet 資料類型：INT_32</p>	3
type	<p>流量類型。可能的值為：IPv4   IPv6   EFA。如需詳細資訊，請參閱<a href="#">Elastic Fabric Adapter</a>。</p> <p>Parquet 資料類型：STRING</p>	3

欄位	描述	版本
pkt-srcaddr	<p>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，當流量流經 <a href="#">NAT 閘道的網路介面</a> 時，或 Amazon EKS 的 Pod IP 地址和 Pod 執行 (用於 VPC 內部通訊) 所在執行個體節點的網路介面 IP 地址不同時。</p> <p>Parquet 資料類型：STRING</p>	3
pkt-dstaddr	<p>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，當流量流經 <a href="#">NAT 閘道的網路介面</a> 時，或 Amazon EKS 的 Pod IP 地址和 Pod 執行 (用於 VPC 內部通訊) 所在執行個體節點的網路介面 IP 地址不同時。</p> <p>Parquet 資料類型：STRING</p>	3
region	<p>包含記錄流量之網路介面的區域。</p> <p>Parquet 資料類型：STRING</p>	4
az-id	<p>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。</p> <p>Parquet 資料類型：STRING</p>	4
sublocation-type	<p>在 sublocation-id 欄位中傳回的子位置類型。可能的值為：<a href="#">波長</a>   <a href="#">outpost</a>   <a href="#">本機區域</a>。如果流量不是來自子位置，則記錄會在此欄位顯示 '-' 符號。</p> <p>Parquet 資料類型：STRING</p>	4
sublocation-id	<p>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。</p> <p>Parquet 資料類型：STRING</p>	4

欄位	描述	版本
pkt-src-aws-service	<p>如果來源 <a href="#">IP 位址適用於 AWS 服務</a>，則 <code>pkt-srcaddr</code> 欄位的 <a href="#">IP 位址範圍</a> 子集名稱。如果 <code>pkt-srcaddr</code> 屬於 <a href="#">重疊的範圍</a>，則只 <code>pkt-src-aws-service</code> 會顯示其中一個服務代碼。AWS 可能的值為：AMAZON   AMAZON_APPFLOW   AMAZON_CONNECT   API_GATEWAY   CHIME_MEETINGS   CHIME_VOICECONNECTOR   CLOUD9   CLOUDFRONT   CODEBUILD   DYNAMODB   EBS   EC2   EC2_INSTANCE_CONNECT   GLOBALACCELERATOR   KINESIS_VIDEO_STREAMS   ROUTE53   ROUTE53_HEALTHCHECKS   ROUTE53_HEALTHCHECKS_PUBLISHING   ROUTE53_RESOLVER   S3   WORKSPACES_GATEWAYS。</p> <p>Parquet 資料類型：STRING</p>	5
pkt-dst-aws-service	<p><code>pkt-dstaddr</code> 欄位之 IP 位址範圍子集的名稱 (如果目的地 IP 位址適用於 AWS 服務)。如需可能值的清單，請參閱 <code>pkt-src-aws-service</code> 欄位。</p> <p>Parquet 資料類型：STRING</p>	5
flow-direction	<p>關於擷取流量的介面的流程方向。可能的值為：ingress   egress。</p> <p>Parquet 資料類型：STRING</p>	5

欄位	描述	版本
traffic-path	<p>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 -。</p> <ul style="list-style-type: none"> <li>• 1 — 透過相同 VPC 中的另一個資源，包括在 VPC 中建立網路介面的資源</li> <li>• 2 – 透過網際網路閘道或閘道 VPC 端點</li> <li>• 3 – 透過虛擬私有閘道</li> <li>• 4 – 透過區域內 VPC 對等連線</li> <li>• 5 – 透過區域間 VPC 對等連線</li> <li>• 6 – 透過本機閘道</li> <li>• 7 – 透過閘道 VPC 端點 (僅限 Nitro 型執行個體)</li> <li>• 8 – 透過網際網路閘道 (僅限 Nitro 執行個體)</li> </ul> <p>Parquet 資料類型：INT_32</p>	5
ECS-聚類集群	<p>AWS ECS 叢集的資源名稱 (ARN) (如果流量來自執行中的 ECS 工作)。若要在訂閱中包含此欄位，您需要呼叫 ecs: ListClusters 的權限。</p> <p>Parquet 資料類型：STRING</p>	7
ECS-叢集名稱	<p>ECS 叢集的名稱 (如果流量來自執行中的 ECS 工作)。若要在訂閱中包含此欄位，您需要呼叫 ecs: ListClusters 的權限。</p> <p>Parquet 資料類型：STRING</p>	7
EC 容器執行個體 arn	<p>如果流量來自 EC2 執行個體上執行中的 ECS 任務，則為 ECS 容器執行個體的 ARN。如果容量提供者是 AWS Fargate，此欄位將是 '-'。若要在訂閱中包含此欄位，您需要呼叫 ecs: ListClusters 和 ecs: ListContainer 執行個體的權限。</p> <p>Parquet 資料類型：STRING</p>	7



欄位	描述	版本
EC 容器實例 ID	如果流量來自 EC2 執行個體上執行中的 ECS 任務，則為 ECS 容器執行個體的識別碼。如果容量提供者是 AWS Fargate，此欄位將是 '-'。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 和 <code>ecs: ListContainer</code> 執行個體的權限。 Parquet 資料類型：STRING	7
ECS 容器識別碼	容器的 Docker 執行階段識別碼 (如果流量來自執行中的 ECS 工作)。如果 ECS 工作中有一或多個容器，這將是第一個容器的碼 <code>docker</code> 執行階段識別碼。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 的權限。 Parquet 資料類型：STRING	7
ECS 第二容器 ID	容器的 Docker 執行階段識別碼 (如果流量來自執行中的 ECS 工作)。如果 ECS 工作中有多個容器，這將是第二個容器的 Docker 執行階段識別碼。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 的權限。 Parquet 資料類型：STRING	7
EC-服務名稱	如果流量來自執行中的 ECS 工作，且 ECS 工作是由 ECS 服務啟動，則為 ECS 服務的名稱。如果 ECS 任務不是由 ECS 服務啟動，則此欄位將為 '-'。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 和 <code>ecs: ListServices</code> 的權限。 Parquet 資料類型：STRING	7
ECS-任務定義 arn	如果流量來自執行中的 ECS 工作，則為 ECS 工作定義的 ARN。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 和 <code>ecs: ListTaskDefinitions</code> 的權限。 Parquet 資料類型：STRING	7
Ec-任務處理器	如果流量來自執行中的 ECS 工作，則為 ECS 工作的 ARN。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 和 <code>ecs: ListTasks</code> 的權限。 Parquet 資料類型：STRING	7

欄位	描述	版本
ECS-任務標識	ECS 工作的識別碼 (如果流量來自執行中的 ECS 工作)。若要在訂閱中包含此欄位，您需要呼叫 <code>ecs: ListClusters</code> 和 <code>ecs:</code> 的權限。ListTasks Parquet 資料類型：STRING	7

## 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](#)
- [通過 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 到具有私有 IP 位址的網路介面的 SSH 流量 (目的地連接埠 22、TCP 通訊協定) 為 123456710 帳戶中的識別碼。

```
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
```

在此範例中，彙總時間間隔內會跳過記錄。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-111111111aaaaaaaa - - - - - 1431280876 1431280934 - SKIPDATA
```

## 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 欄位由流程記錄中的 second-to-last 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。用戶端將 FIN 標記 (1) 傳送到伺服器，供連接埠 43418 的連線使用。伺服器將 FIN 傳送至連接埠 43418 的用戶端。

```

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

```

針對在單一彙總時間間隔內開啟關閉的短暫連線 (例如數秒)，標記可能設在同方向流量之流量日誌記錄的同一行中。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。

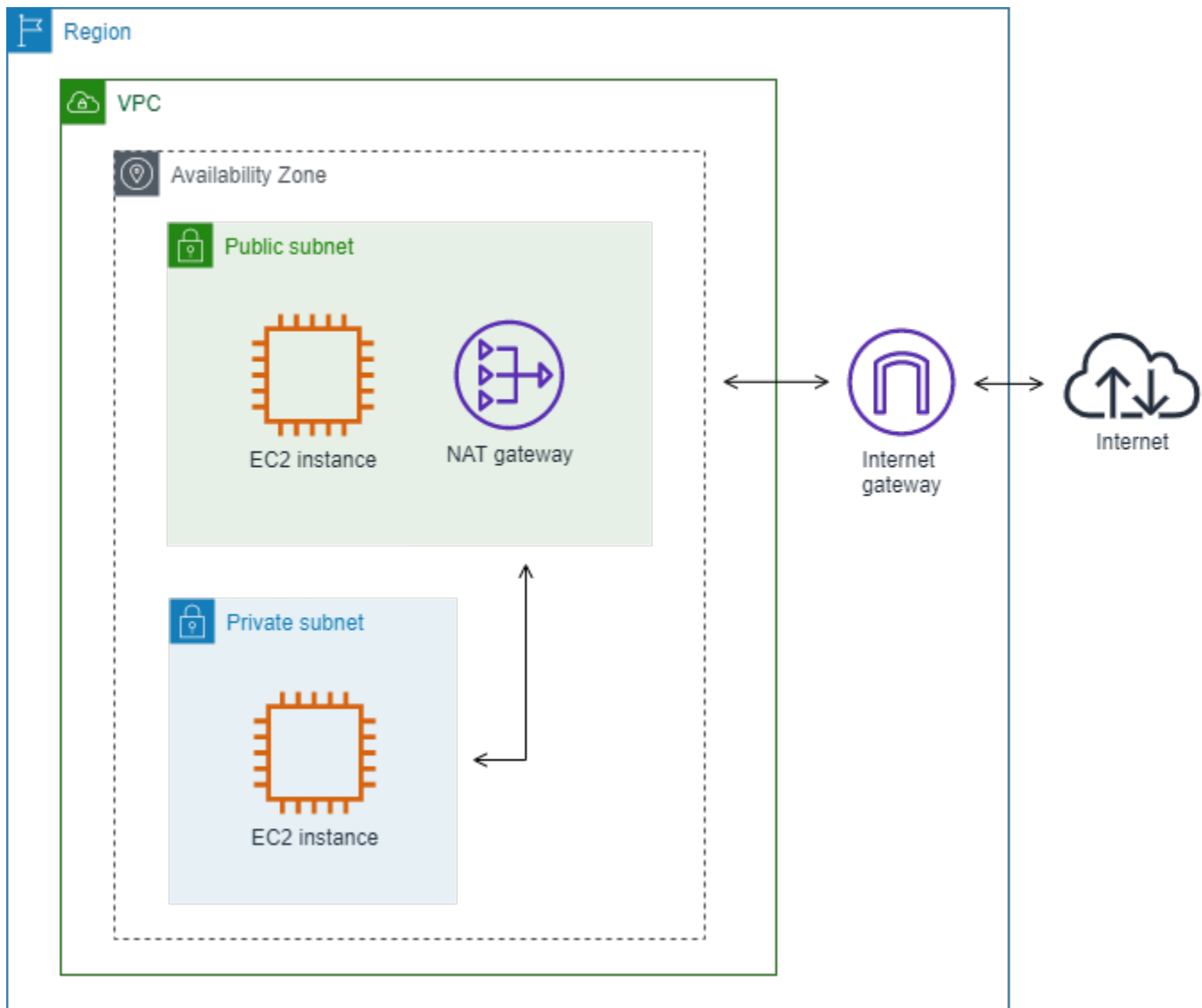
```

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

```

## 通過 NAT 閘道的流量

在本範例中，私有子網中的執行個體透過位在公有子網中的 NAT 閘道存取網際網路。



以下 NAT 閘道網路介面的自訂流量日誌會依以下順序擷取下列欄位。

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

流量日誌顯示流量從執行個體 IP 地址 (10.0.1.5) 經由 NAT 閘道網路介面流向網際網路的主機 (203.0.113.5)。NAT 閘道網路介面是申請者管理的網路介面，因此流量日誌記錄會在 instance-id 欄位顯示 '-' 符號。下行顯示從來源執行個體流向 NAT 閘道網路介面的流量。dstaddr 和 pkt-dstaddr 欄位的值不一樣。dstaddr 欄位顯示 NAT 閘道網路介面的私有 IP 地址，而 pkt-dstaddr 欄位則顯示網際網路主機的最終目標 IP 地址。

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

接下來兩行會顯示從 NAT 閘道網路介面流向網際網路目標主機的流量，以及從主機到 NAT 閘道網路介面的回應流量。

```
- 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 NAT 閘道網路介面流向來源執行個體的回應流量。srcaddr 和 pkt-srcaddr 欄位的值不一樣。srcaddr 欄位顯示 NAT 閘道網路介面的私有 IP 地址，而 pkt-srcaddr 欄位則顯示網際網路主機的 IP 地址。

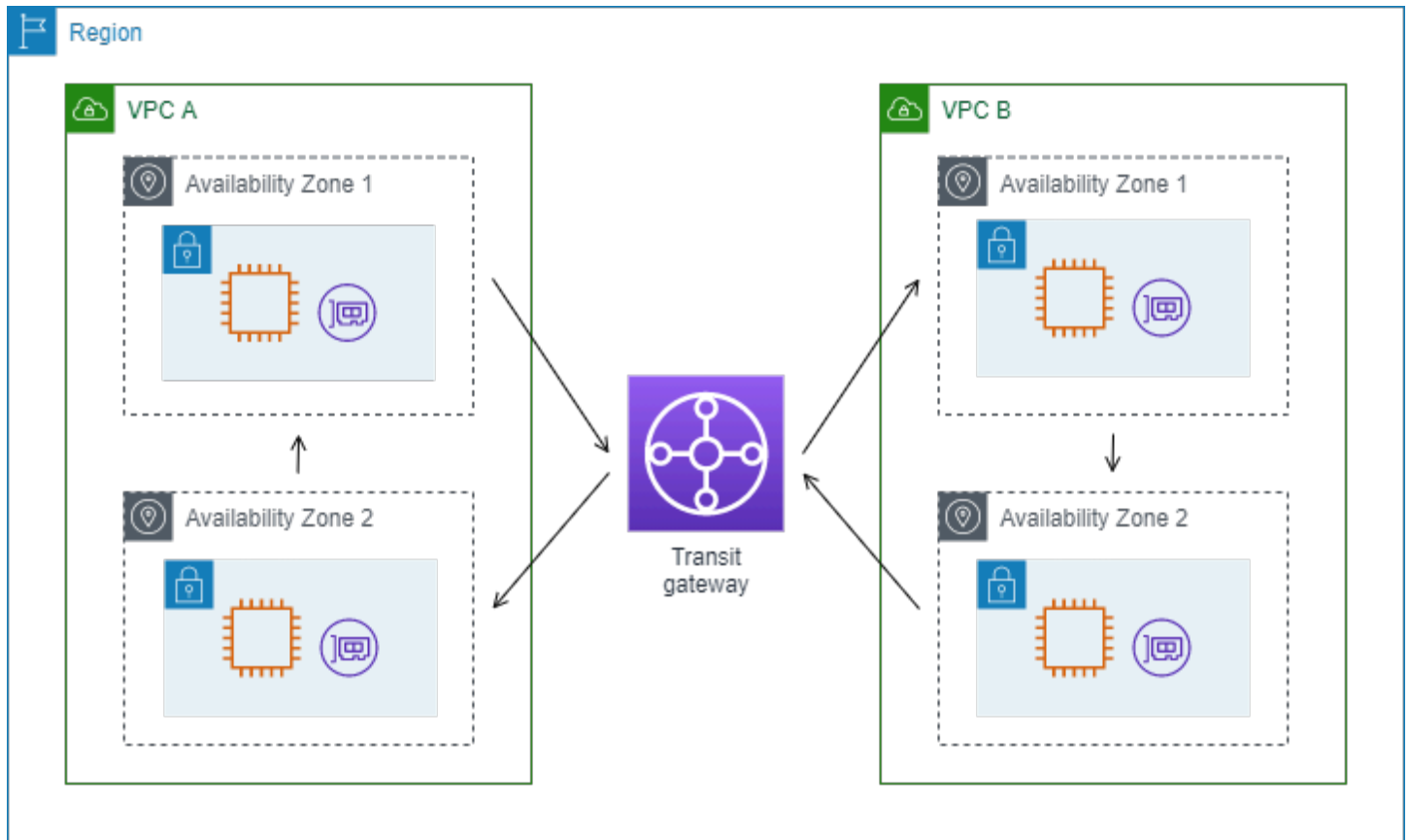
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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。在本案例中，instance-id 欄位會傳回與網路介面相關聯的執行個體 ID，而 dstaddr 和 pkt-dstaddr 欄位以及 srcaddr 和 pkt-srcaddr 欄位之間沒有任何差異。與 NAT 閘道的網路介面不同，此網路介面不是流量的中繼網路介面。

```
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
```

## 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-3333333333333333 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-3333333333333333 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-11111111aaaaaaaa 中，傳輸閘道申請者管理網路介面在 eni-1111111111111111 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-111111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaa -
  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-22222222bbbbbbbbbb 中，傳輸閘道申請者管理網路介面在 eni-2222222222222222 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-2222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb -
  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：

- 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。
- 如果流量來自網路介面，但來源不是任一網路介面的 IP 地址，則流量日誌會在 `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。
- 若流量會傳送到或來自網路介面，則流量日誌的 `srcaddr` 和 `dstaddr` 欄位一律會顯示主要私有 IPv4 地址，無論封包來源或目標為何。若要擷取封包來源或目標，請建立具有 `pkt-srcaddr` 和 `pkt-dstaddr` 欄位的流量日誌。
- 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。

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。
- 鏡像流量。
- 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。

第 7 版中 ECS 欄位的特定限制：

- 若要使用 ECS 欄位建立流程記錄訂閱，您的帳戶必須至少包含一個 ECS 叢集。

- 如果基礎 ECS 任務不是由流程記錄訂閱的擁有者所擁有，則不會計算 ECS 欄位。例如，如果您與另一個帳戶 (SubnetA) 共用于網路 (AccountB)，然後建立流程記錄訂閱SubnetA，如果在共用于網路中AccountB啟動 ECS 工作，您的訂閱將會接收來自由啟動之 ECS 工作的流量記錄，AccountB但是基於安全性考量，不會計算這些記錄的 ECS 欄位。
- 如果您在 VPC /子網路資源層級使用ECS 欄位建立流程記錄訂閱，則針對非 ECS 網路介面產生的任何流量也會針對您的訂閱傳送。對於非 ECS IP 流量，ECS 欄位的值將為「-」。例如，您有一個子網路 (subnet-000000)，而且您使用 ECS 欄位 (f1-00000000) 為此子網路建立流程記錄訂閱。在中subnet-000000，您可以啟動連接到網際網路並主動產生 IP 流量的 EC2 執行個體 (i-00000000)。您也可以相同的子網路中啟動執行中的 ECS 工作 (ECS-Task-1)。由於i-00000000和ECS-Task-1正在產生 IP 流量，因此您的流量日誌訂閱f1-00000000將為兩個實體提供流量日誌。但是，只有ECS-Task-1您包含在日誌格式中的 ECS 字段的實際 ECS 元數據。對於i-00000000相關流量，這些欄位的值為 '-'。
- ecs-container-id並ecs-second-container-id在 VPC 流程記錄服務從 ECS 事件串流接收這些記錄時進行排序。無法保證它們的順序與您在 ECS 主控台或 DescribeTask API 呼叫中看到的順序相同。如果容器在工作仍在執行時進入「已停止」狀態，它可能會繼續出現在記錄檔中。
- ECS 中繼資料和 IP 流量記錄來自兩個不同的來源。一旦我們從上游依賴項中獲得所有必需的信息，我們就會開始計算您的 ECS 流量。開始新任務後，我們開始計算您的 ECS 字段 1) 當我們收到基礎網路接口的 IP 流量時，2) 當我們收到包含 ECS 任務的元數據的 ECS 事件時，表明任務正在運行。當您停止任務後，當我們收到 ECS 任務中繼資料的 ECS 事件時，我們會停止計算您的 ECS 欄位 1) 當我們不再收到基礎網路介面的 IP 流量時，我們會停止計算您的 ECS 欄位 1)，以表示您的工作不再執行。
- 僅支援在aws vpc [網路模式下](#) 啟動的 ECS 工作。

## 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。如需發佈付費日誌時定價的詳細資訊，請開啟 [Amazon CloudWatch 定價](#)，選取日誌並尋找付費日誌。

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 成本分配報告會納入這些標籤彙總的使用量和成本。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 使用者指南》中的 [使用成本分配標籤](#)
- [在 Amazon CloudWatch 日誌使用者指南中標 CloudWatch 記日誌群組](#)
- 《Amazon Simple Storage Service 使用者指南》中的 [使用成本分配 S3 儲存貯體標籤](#)

- 在 Amazon 資料 Firehose 開發人員指南中 [標記您的交付串流](#)

## 使用流量日誌工作

您可以使用 Amazon EC2 和 Amazon VPC 的主控制台來處理流程日誌。

### 任務

- [控制流量日誌的使用方式](#)
- [建立流量日誌](#)
- [檢視流程日誌](#)
- [標記流程日誌](#)
- [刪除流量日誌](#)
- [API 和 CLI 概觀](#)

### 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。

```
{
  "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”](#)。

## 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 記錄的流程記錄”](#)
- [the section called “建立發佈到 Amazon S3 的流量日誌”](#)
- [the section called “建立發佈至 Amazon 資料 Firehose 的流程日誌”](#)

## 檢視流程日誌

您可以檢視資源流程日誌的相關資訊，例如網路介面。顯示的資訊包含流量日誌的 ID、流量日誌組態，以及流量日誌狀態的相關資訊。

### 檢視有關流程日誌的資訊

1. 執行以下任意一項：
  - 在 <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. (選用) 若要檢視流程日誌資料，請開啟日誌目的地。

## 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：
  - 在 <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)。

## 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：
  - 在 <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)。

## API 和 CLI 概觀

您可以使用命令列或 API 執行此頁面所述的任務。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](#)。

### 建立流量日誌

- [create-flow-logs](#) (AWS CLI)

- [New-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [CreateFlow 日誌](#) (Amazon EC2 查詢 API)

### 描述流程日誌

- [describe-flow-logs](#) (AWS CLI)
- [Get-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DescribeFlow 日誌](#) (Amazon EC2 查詢 API)

### 標記流程日誌

- [create-tags](#) 和 [delete-tags](#) (AWS CLI)
- [New-EC2Tag](#)和 [Remove-EC2Tag](#) ( AWS Tools for Windows PowerShell )
- [CreateTags](#)和 [DeleteTags](#) ( Amazon EC2 查詢 API )

### 刪除流量日誌

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DeleteFlow 日誌](#) (Amazon EC2 查詢 API)

## 將流程記錄發佈到 CloudWatch 記錄

流程日誌可以將流程日誌資料直接發佈到 Amazon CloudWatch。

發佈至 CloudWatch 記錄檔時，流程記錄資料會發佈至記錄群組，且每個網路介面在記錄群組中都有唯一的記錄資料流。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。

在記 CloudWatch 錄中，時間戳記欄位對應於流程記錄中擷取的開始時間。ingestionTime 欄位會指出日誌收到流程記錄的日期和時間。CloudWatch 這個時間戳記晚於流量日誌記錄中擷取的結束時間。

如需有關 CloudWatch 日誌的詳細資訊，請參閱 Amazon [日誌 CloudWatch 誌使用者指南中的傳送至 CloudWatch 日誌的日誌](#)。

## 定價

當您將流程記錄發佈至記錄檔時，付費記錄的資料擷取和封存費用將適用。CloudWatch 如需詳細資訊，請開啟 [Amazon CloudWatch 定價](#)，選取日誌並尋找付費日誌。

## 目錄

- [將流程日誌發佈到日 CloudWatch 誌的 IAM 角色](#)
- [將流程日誌發佈到 CloudWatch 日誌的 IAM 主體的許可](#)
- [建立發佈至 CloudWatch 記錄的流程記錄](#)
- [檢視流量日誌記錄](#)
- [搜尋流量日誌記錄](#)
- [CloudWatch 日誌中的處理流程日誌記錄](#)

## 將流程日誌發佈到日 CloudWatch 誌的 IAM 角色

與流程日誌關聯的 IAM 角色必須具有足夠的許可，才能將流程日誌發佈到日誌中指定的 CloudWatch 日誌群組。IAM 角色必須屬於您的 AWS 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：

```
{
  "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。



```
{
  "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. 輸入原則的名稱以及選擇性的說明和標記，然後選擇 [建立原則]。
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心取方塊，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)。

## 將流程日誌發佈到 CloudWatch 日誌的 IAM 主體的許可

確認您用來發出請求的 IAM 主體具有呼叫 iam:PassRole 動作的權限。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": ["iam:PassRole"],  
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"  
    }  
  ]  
}
```

## 建立發佈至 CloudWatch 記錄的流程記錄

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。如需詳細資訊，請參閱 [將流程日誌發佈到 CloudWatch 日誌的 IAM 主體的許可](#)。

## 先決條件

- 如 [the section called “將流程日誌發佈到日 CloudWatch 誌的 IAM 角色”](#) 所述，建立 IAM 角色。

## 使用主控台建立流程日誌

1. 執行以下任意一項：
  - 在 <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「目的地」，選擇「傳送至 CloudWatch 記錄檔」。
6. 對於目的地日誌群組，請選擇現有日誌群組的名稱，或輸入建立此流程日誌時將建立的新日誌群組名稱。
7. 對於 IAM 角色，請指定具有將日誌發佈到日誌的權限的角色名稱。 CloudWatch
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. 對於其他中繼資料，請選取是否要以日誌格式包含來自 Amazon ECS 的中繼資料。
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)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立流程記錄，以擷取指定子網路的所有可接受流量。流程日誌會交付至指定的日誌群組。該 `--deliver-logs-permission-arn` 參數指定發佈到 CloudWatch 日誌所需的 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
```

## 檢視流量日誌記錄

您可以使用記錄主控台檢視流程 CloudWatch 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 記錄的流程記錄

1. [請在以下位置開啟 CloudWatch 主控台。](https://console.aws.amazon.com/cloudwatch/) <https://console.aws.amazon.com/cloudwatch/>
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 記錄的流程記錄

- [get-log-events](#) (AWS CLI)
- [取得 CWL \(\) LogEvent](#) AWS Tools for Windows PowerShell

## 搜尋流量日誌記錄

您可以使用記錄主控台搜尋發佈至 CloudWatch Logs 的流程 CloudWatch 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。

使用記錄主控台搜尋流程 CloudWatch 記錄

1. [請在以下位置開啟 CloudWatch 主控台。](https://console.aws.amazon.com/cloudwatch/) <https://console.aws.amazon.com/cloudwatch/>
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，輸入以下字串。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]
```

## CloudWatch 日誌中的處理流程日誌記錄

您可以像處理任何其他記錄事件一樣處理流程記錄檔記 CloudWatch 錄。如需監控日誌資料和指標篩選器的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的[搜尋和篩選日誌資料](#)。

範例：建立流程記錄的 CloudWatch 指標篩選器和警示

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. [請在以下位置開啟 CloudWatch 主控台](https://console.aws.amazon.com/cloudwatch/)。 <https://console.aws.amazon.com/cloudwatch/>
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)。

- 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]
```

- 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)。
- 就緒後，請選擇 Next (下一步)。
- 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)。
- 在導覽窗格中，選擇 Alarms (警示)、All alarms (所有警示)。
- 選擇 Create alarm (建立警示)。
- 選取您建立的測量結果名稱，然後選擇選取測量結果。
- 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)。
  - 對於每 TimeSinceLastActive 當...，選擇「大於/等於」，然後輸入 10 做為臨界值。
  - 對於 Additional configuration (其他組態)、Datapoints to alarm (要警示的資料點)，保留預設值 1。
- 選擇下一步。
- 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。
- 輸入警示的名稱和說明，然後選擇 Next (下一步)。
- 當您完成預覽鬧鐘時，請選擇 [建立鬧鐘]。

## 將流量日誌發佈到 Amazon S3

現在流量日誌可將流量日誌資料發佈至 Amazon S3。

當發佈至 Amazon S3 時，流量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 Simple Storage Service 使用者指南》中的[建立儲存貯體](#)。

如需有關多個帳戶記錄的詳細資訊，請參閱 AWS 解決方案程式庫中的 [中央記錄](#)。

如需有關 CloudWatch 日誌的詳細資訊，請參閱 [Amazon 日誌使用者指南中的傳送到 Amazon S3 的 CloudWatch 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](#)，選取日誌並尋找付費日誌。

## 目錄

- [流量日誌檔](#)
- [將流程日誌發佈至 Amazon S3 的 IAM 主體的許可](#)
- [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](#)
- [檢視流量日誌記錄](#)
- [Amazon S3 中的處理流量日誌記錄](#)

## 流量日誌檔

VPC 流程日誌會將進出 VPC 的 IP 流量相關資料收集到日誌記錄中，將這些記錄彙總到日誌檔中，然後每隔 5 分鐘將日誌檔發佈到 Amazon S3 儲存貯體。可能會發佈多個檔案，且每個記錄檔可能包含前 5 分鐘記錄之 IP 流量的部分或全部流程記錄。

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
```

## 將流程日誌發佈至 Amazon S3 的 IAM 主體的許可

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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

## 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](#)」。

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

```
    }  
  }  
]  
}
```

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/*
```

最佳作法是將這些權限授與記錄傳遞服務主體，而非個別的 AWS 帳戶 ARN。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。

## 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 無法交付](#) 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。如需與 SSE-KMS 搭配使用所需金鑰政策的詳細資訊，請參閱 [Amazon CloudWatch 日誌使用者指南中的 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 Simple Storage Service 使用者指南》中的[存取控制清單 \(ACL\) 概觀](#)。

## 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。

### 使用主控台建立流程日誌

- 執行以下任意一項：
  - 在 <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。
- 選擇 Actions (動作)、Create flow log (建立流量日誌)。
- 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。
- 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。
- 針對目的地，選擇傳送至 Amazon S3 儲存貯體。
- 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](#)。
- 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. 對於其他中繼資料，請選取是否要以日誌格式包含來自 Amazon ECS 的中繼資料。
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)。

使用命令列工具建立可發佈至 Amazon S3 的流量日誌

請使用以下其中一個命令：

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立一個流程日誌，以擷取指定 VPC 的所有流量，並將流程日誌傳送到指定的 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}'
```

## 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。

檢視發佈至 Amazon S3 的流量日誌記錄

1. 在以下網址開啟 Amazon S3 主控台：<https://console.aws.amazon.com/s3/>。

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。`#####//## ID /vpcflow ##AWSLogs/##/##/##/##`
4. 選取檔案名稱旁邊的核取方塊，然後選擇 Download (下載)。

## Amazon S3 中的處理流量日誌記錄

日誌檔案已壓縮。如果您使用 Amazon S3 主控台開啟日誌檔案，這些檔案將會解壓縮，並顯示流量日誌記錄。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。

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](#)。

## 將流程日誌發佈到 Amazon 資料 Firehose

流程日誌可以將流程日誌資料直接發佈到 Amazon 資料 Firehose。

發佈到 Amazon 資料 Firehose 時，流程日誌資料會以純文字格式發佈到 Amazon 資料 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](#)，選取日誌並尋找付費日誌。

### 目錄

- [跨帳戶交付的 IAM 角色](#)
- [建立發佈至 Amazon 資料 Firehose 的流程日誌](#)
- [在 Amazon 數據 Firehose 件中處理流程日誌記錄](#)

## 跨帳戶交付的 IAM 角色

當您發佈到 Amazon Data Firehose 時，您可以選擇與要監控資源 (來源帳戶) 位於相同帳戶的交付串流 (來源帳戶)，或在不同的帳戶 (目標帳戶) 中。若要啟用跨帳戶將流程日誌交付到 Amazon Data Firehose，您必須在來源帳戶中建立 IAM 角色，並在目標帳戶中建立 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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "delivery.logs.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries",
        "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account: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。

```
{  
  "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. 輸入原則的名稱以及選擇性的說明和標記，然後選擇 [建立原則]。
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心方塊，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，建立名稱開頭為的角色AWSLogDeliveryFirehoseCrossAccountRole。此角色必須授予下列許可。

```
{
  "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。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account: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. 輸入原則開頭為的名稱 `AWSLogDeliveryFirehoseCrossAccountRole`，然後選擇 [建立原則]。
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)。

### 建立發佈至 Amazon 資料 Firehose 的流程日誌

您可以建立 VPC、子網或網路介面的流量日誌。

## 必要條件

- 建立目的地 Amazon 資料 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 資料 Firehose 交付串流](#)。
- 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。

## 若要建立發佈至 Amazon 資料 Firehose 的流程日誌

1. 執行以下任意一項：
  - 在 <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位於同一個帳戶中。
  - 使用不同的帳戶傳送至 Amazon Data Firehose — 交付串流和要監控的資源位於不同的帳戶中。
6. 對於 Amazon 資料 Firehose 串流名稱，請選擇您建立的交付串流。
7. [僅限跨帳戶交付] 對於 IAM 角色，指定所需的角色 (請參閱 [the section called “跨帳戶交付的 IAM 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. 對於其他中繼資料，請選取是否要以日誌格式包含來自 Amazon ECS 的中繼資料。
  10. (可選) 選擇「新增標籤」，將標籤套用至流程記錄。
  11. 選擇 Create flow log (建立流量日誌)。

若要使用命令列工具建立發佈到 Amazon 資料 Firehose 的流程記錄

請使用以下其中一個命令：

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)

下列 AWS CLI 範例會建立一個流程記錄，以擷取指定 VPC 的所有流量，並將流程日誌傳送到同一帳戶中的指定 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 範例會建立一個流程記錄，以擷取指定 VPC 的所有流量，並將流程日誌傳送到不同帳戶中的指定 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
```

## 在 Amazon 數據 Firehose 件中處理流程日誌記錄

您可以從為交付串流設定的目的地取得流程日誌資料。

## 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

- 您可以透過產生 CloudFormation 範本建立必要的 AWS 資源和預先定義的查詢，從而簡化並自動化 VPC 流程記錄與 Athena 的整合，以取得有關流經 VPC 流量的深入解析。
- 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

- [使用控制台生成 CloudFormation 模板](#)
- [使用產生 CloudFormation 範本 AWS CLI](#)
- [執行預先定義的查詢](#)

## 使用控制台生成 CloudFormation 模板

將第一個流程日誌傳遞到 S3 儲存貯體之後，您可以產生 CloudFormation 範本並使用範本建立堆疊來與 Athena 進行整合。

### 要求

- 所選區域必須支持 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。如果您未指定開始和結束日期，CloudFormation 範本會建立 Lambda 函數，以便按照週期性排程載入新的分區。
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，選擇連結以導覽至您為 CloudFormation 範本指定的值區，然後自訂範本。
7. 在成功訊息中，選擇 [建立 CloudFormation 堆疊]，在 AWS CloudFormation 主控台中開啟 [建立堆疊] 精靈。所產生 CloudFormation 範本的 URL 會在「範本」區段中指定。完成精靈以建立範本中指定的資源。

### 由 CloudFormation 模板創建的資源

- 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 函數的權限的 IAM 角色。

## 使用產生 CloudFormation 範本 AWS CLI

將第一個流程日誌傳遞到 S3 儲存貯體之後，您可以產生並使用 CloudFormation 範本與 Athena 整合。

使用下面的[獲取流程日誌集成模板命令](#)來生成模板。 CloudFormation

```
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"
      }
    ]
  }
}
```

使用下面的[創建堆棧命令](#)，[使用生成](#)的模板創建一個堆棧。 CloudFormation

```
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，以便快速取得有關 AWS 網路中流量的有意義見解。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「工作群組」下，選取由 CloudFormation 樣板建立的工作群組。
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。

- VpcFlowLogsAccepted流量 — 根據您的安全群組和網路 ACL 允許的 TCP 連線。
- VpcFlowLogsAdminPortTraffic— 流量最多的前 10 個 IP 位址，由在管理連接埠上提供要求的應用程式所記錄。
- VpcFlow記錄檔 4 流量 — 記錄的 IPv4 流量的總位元組。
- VpcFlow記錄 6 流量 — 記錄的 IPv6 流量的總位元組。
- VpcFlowLogsRejectedTCP 流量 — 根據您的安全群組或網路 ACL 拒絕的 TCP 連線。
- VpcFlowLogsRejected流量 — 根據您的安全群組或網路 ACL 拒絕的流量。
- VpcFlowLogsSshRdpTraffic— 安全殼層和 RDP 流量。
- VpcFlowLogsTop發言者 — 記錄流量最多的 50 個 IP 地址。
- VpcFlowLogsTopTalkersPacket層級 — 記錄最多流量的 50 個封包層級 IP 位址。
- VpcFlowLogsTopTalkingInstances— 記錄最多流量的 50 個執行個體的 ID。
- VpcFlowLogsTopTalkingSubnets— 記錄最多流量的 50 個子網路的 ID。
- VpcFlowLogsTopTCP 流量 — 針對來源 IP 位址記錄的所有 TCP 流量。
- VpcFlowLogsTotalBytesTransferred— 記錄最多位元組的 50 對來源和目標 IP 位址。
- VpcFlowLogsTotalBytesTransferredPacketLevel— 記錄最多位元組的 50 對封包層級來源和目標 IP 位址。
- VpcFlowLogsTrafficFrmSrcAddr — 針對特定來源 IP 位址記錄的流量。
- VpcFlowLogsTrafficToDstAddr — 針對特定目標 IP 位址記錄的流量。

## 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](#)
- ['LogDestinationNotFound異常' 或 '訪問被拒絕' 錯誤 LogDestination](#)
- [超過 Amazon S3 儲存貯體原則限制](#)
- [LogDestination 無法交付](#)

## 不完整的流量日誌記錄

### 問題

您的流量日誌記錄不完整，或已不再發佈。

### 原因

將流程記錄傳送至記錄檔記 CloudWatch 錄群組時可能發生問題。

### 解決方案

在 Amazon EC2 主控台或 Amazon VPC 主控台中，選擇相關資源的流量日誌索引標籤。如需更多詳細資訊，請參閱 [檢視流程日誌](#)。流量日誌表會在 Status (狀態) 欄中顯示所有錯誤。或者，使用 [describe-flow-logs](#) 命令，然後檢查在 DeliverLogsErrorMessage 欄位中傳回的值。可能會顯示下列任一項錯誤：

- **Rate limited**：如果已套用記 CloudWatch 錄節流，則會發生此錯誤 — 當網路介面的流程記錄數目大於特定時間範圍內可發佈的記錄數目上限時，就會發生此錯誤。如果您已達到可建立之 CloudWatch 記錄檔群組數目的配額，也會發生這個錯誤。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的 Ser CloudWatch [vice Quotas](#)。
- **Access error**：此錯誤可能的發生原因如下：
  - 流程日誌的 IAM 角色沒有足夠的許可將流程日誌記錄發佈到 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 [將流程日誌發佈到日 CloudWatch 誌的 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 儲存貯體的 CloudWatch 日誌或日誌檔中看到任何日誌串流。

### 可能原因

- 系統仍在建立流量日誌。在某些情況下，在您建立流量日誌之後，可能需要十分鐘以上，才會建立日誌群組及顯示資料。
- 尚未記錄到任何網路介面的流量。記錄 CloudWatch 檔中的記錄群組只會在記錄流量時建立。

### 解決方案

等待幾分鐘建立日誌群組或記錄流量。

## 'LogDestinationNotFound異常' 或 '訪問被拒絕' 錯誤 LogDestination

### 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

- 建立可將資料發佈至 Amazon S3 儲存貯體的流量記錄檔時若出現此錯誤，表示找不到指定的 S3 儲存貯體，或儲存貯體政策不允許將記錄檔傳送至該儲存貯體。
- 建立將資料發佈到 Amazon CloudWatch Logs 的流程日誌時，此錯誤表示 IAM 角色不允許將日誌傳送到日誌群組。

### 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](#)具有所需的許可權限，並在 ARN 中使用正確的帳戶 ID 和儲存貯體名稱。
- 發佈到 CloudWatch 記錄檔時，請確認 [IAM 角色](#)具有必要的許可。

## 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 無法交付

### 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

目標 Amazon S3 儲存貯體使用具有 AWS KMS (SSE-KMS) 的伺服器端加密進行加密，而儲存貯體的預設加密是 KMS 金鑰識別碼。

### 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](#)。

## 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](#)。

### 內容

- [NAU 指標與維度](#)
- [啟用或停用 NAU 監控](#)
- [NAU CloudWatch 警示范例](#)

## 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	描述
NetworkAddressUsage	每個 VPC 的 NAU 計數。  報告準則 <ul style="list-style-type: none"><li>• 每 24 小時。</li></ul> Dimensions (尺寸) <ul style="list-style-type: none"><li>• 名稱：Per-VPC Metrics，值：VPC ID。</li></ul>

指標	描述
NetworkAddressUsagePeered	<p>VPC 和與之對等的所有 VPC 的 NAU 計數。</p> <p>報告準則</p> <ul style="list-style-type: none"> <li>每 24 小時。</li> </ul> <p>Dimensions (尺寸)</p> <ul style="list-style-type: none"> <li>名稱：Per-VPC Metrics，值：VPC ID。</li> </ul>

AWS/Usage 命名空間包含下列用於監控 NAU 的指標。

指標	描述
ResourceCount	<p>每個 VPC 的 NAU 計數。</p> <p>報告準則</p> <ul style="list-style-type: none"> <li>每 24 小時。</li> </ul> <p>Dimensions (尺寸)</p> <ul style="list-style-type: none"> <li>名稱：Service，值：EC2</li> <li>名稱：Type，值：Resource</li> <li>名稱：Resource，值：VPC ID。</li> <li>名稱：Class，值：NetworkAddressUsage</li> </ul>
ResourceCount	<p>VPC 和與之對等的所有 VPC 的 NAU 計數。</p> <p>報告準則</p> <ul style="list-style-type: none"> <li>每 24 小時。</li> </ul> <p>Dimensions (尺寸)</p>

指標	描述
	<ul style="list-style-type: none"> <li>名稱：Service，值：EC2</li> <li>名稱：Type，值：Resource</li> <li>名稱：Resource，值：VPC ID。</li> <li>名稱：Class，值：NetworkAddressUsagePeered</li> </ul>
ResourceCount	<p>VPC 之間 NAU 使用的組合視圖。</p> <p>報告準則</p> <ul style="list-style-type: none"> <li>每 24 小時。</li> </ul> <p>Dimensions (尺寸)</p> <ul style="list-style-type: none"> <li>名稱：Service，值：EC2</li> <li>名稱：Type，值：Resource</li> <li>名稱：Resource，值：VPC</li> <li>名稱：Class，值：NetworkAddressUsage</li> </ul>
ResourceCount	<p>對等 VPC 之間 NAU 使用的組合視圖。</p> <p>報告準則</p> <ul style="list-style-type: none"> <li>每 24 小時。</li> </ul> <p>Dimensions (尺寸)</p> <ul style="list-style-type: none"> <li>名稱：Service，值：EC2</li> <li>名稱：Type，值：Resource</li> <li>名稱：Resource，值：VPC</li> <li>名稱：Class，值：NetworkAddressUsagePeered</li> </ul>

## 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. 執行下列任意一項：
  - 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"  
}
```



# Amazon Virtual Private Cloud 中的安全性

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同的責任。[共同責任模型](#)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 雲端中執行 AWS 服務的基礎架構。AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon 虛擬私有雲端的合規計劃，請參閱[AWS 合規計劃合規計劃範圍](#)的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您的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。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon VPC 資源的服務。

## 目錄

- [Amazon Virtual Private Cloud 中的資料保護](#)
- [Amazon VPC 的 Identity and Access Management](#)
- [Amazon VPC 的基礎設施安全性](#)
- [使用安全性群組控制 AWS 資源的流量](#)
- [使用網路 ACL 控制子網路的流量](#)
- [Amazon Virtual Private Cloud 的恢復能力](#)
- [Amazon Virtual Private Cloud 的合規驗證](#)
- [VPC 的安全最佳實務](#)

## Amazon Virtual Private Cloud 中的資料保護

AWS [共同責任模型](#)適用於 Amazon Virtual Private Cloud 中的資料保護。如此模型中所述，AWS 負責保護執行所有 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](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。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 資源進行通訊。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。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 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。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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 \(FIPS\) 140-2 概觀](#)。

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。這包括當您使用主控台、API 或 AWS 開發套件 AWS 服務使用 Amazon VPC 或其他軟體時。AWS CLI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。

## 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 [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 ACL 控制子網路的流量](#)。
- **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到 CloudWatch 日誌或 Amazon S3，可協助您診斷過度限制或過於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，您可以將流量傳送到 out-of-band 安全性和監控設備。如需詳細資訊，請參閱 [流量鏡射指南](#)。

# Amazon VPC 的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 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。您可以使用 IAM AWS 服務，無需額外付費。

## 目錄

- [物件](#)
- [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](#)

## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會因您在 Amazon VPC 中所做的工作而有所不同。

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

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》AWS 帳戶中的[如何登入](#)您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的[簽署 AWS API 請求](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的[多重要素驗證](#)和 IAM 使用者指南中的[在 AWS 中使用多重要素驗證 \(MFA\)](#)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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](#)是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的[建立 IAM 使用者 \(而非角色\) 的時機](#)。

## IAM 角色

[IAM 角色](#)是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以[切換角色，在中暫時擔任 IAM 角色](#)。AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的[使用 IAM 角色](#)。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 [IAM 使用者指南](#) 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 [IAM 角色與資源類型政策的差異](#)。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的[建立角色以委派許可給 AWS 服務](#)。
- 服務連結角色 — 服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體

的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的[利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的[建立 IAM 角色 \(而非使用者\) 的時機](#)。

## 使用政策管理存取權

您可以透過 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS，當與身分識別或資源相關聯時，會定義其權限。AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的[JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

## 身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的[建立 IAM 政策](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶。受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的[在受管政策和內嵌政策間選擇](#)。

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 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。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 和 Amazon VPC 是支援 ACL 的服務範例。AWS WAF 若要進一步了解 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 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的[IAM 實體許可範圍](#)。
- 服務控制策略 (SCP) — SCP 是 JSON 策略，用於指定中組織或組織單位 (OU) 的最大權限。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶。若您啟用組織中的所有功能，您可以將服務控制策略 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的[SCP 運作方式](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，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。若要深入瞭解 Amazon VPC 和其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的可與 IAM 搭配使用的[AWS 服務](#)。

### 目錄

- [動作](#)
- [資源](#)
- [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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

原則會使用動作來授予執行相關聯操作的許可。

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](#)。

## 資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示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哪些內容。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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。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。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯 OR 運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容金鑰](#)。

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。當主參與者和資源位於不同的 AWS 帳號中時，您也必須授與主參與者實體存取資源的權限。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 角色與資源型政策有何差異](#)。

## 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[在建立期間標記資源和使用資源標籤控制對 EC2 資源的存取](#)。

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](#)是您 AWS 帳戶 內部具有特定許可的實體。

### 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[GetFederation權杖](#)等 AWS STS API 作業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。建立流程記錄檔時，您必須選擇允許流程記錄服務存取記錄 CloudWatch 檔的角色。如需詳細資訊，請參閱 [the section called “將流程日誌發佈到日 CloudWatch 誌的 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 Management Console、AWS CLI、或 AWS API 執行工作。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](#)
- [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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的 AWS 受管理原則。它們在您的 AWS 帳戶。建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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](#)。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM Access Analyzer 政策驗證](#)。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的設定 MFA 保護的 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。

```
{
  "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": "*"
}
]
}

```

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的角色允許最低主控台權限。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。

```
{
  "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。

```
{
  "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 服務無法使用此原則來建立具有必要標記的安全性群組。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。

```

{
  "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"
        },
        "ForAllValues: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` 條件金鑰將權限範圍設定為特定 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。

```

{
  "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:region:account-id:security-group/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
      }
    }
  }],
}

```

```

{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeTags"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:ModifySecurityGroupRules"
  ],
  "Resource": "arn:aws:ec2:region:account-id: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。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/subnet-id",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/sg-id"
    ]
  }]
}

```

```

    }
  ]
}

```

## 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。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:region:account-id:subnet/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
      }
    }
  }],
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:region::image/ami-*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/department": "dev"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group*"
    ]
  }
}

```

```
    }  
  ]  
}
```

## 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 端點和 VPC 端點服務](#)
- [VPC 端點政策](#)
- [VPC 對等互連](#)
- [AWS Wavelength](#)

## 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](#)
- [我沒有授權執行 iam : PassRole](#)
- [我想允許我 AWS 帳戶以外的人員存取我的 Amazon VPC 資源](#)

### 我未獲授權，不得在 Amazon VPC 中執行動作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。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。

## 我沒有授權執行 iam : PassRole

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 允許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 沒有將角色傳遞至該服務的許可。

```
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。

## 我想允許我 AWS 帳戶以外的人員存取我的 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](#)。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 [《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限](#)。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的 [提供第三方 AWS 帳戶 擁有的存取權](#)。
- 若要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 \(聯合身分\)](#)。
- 若要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 角色 與資源型政策的差異](#)。

## AWS Amazon Virtual Private Cloud 的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住，AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。AWS 當新的啟動或新 AWS 服務的 API 操作可供現有服務使用時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 受管政策](#)。

### AWS 管理策略：亞馬遜 VPC FullAccess

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。

若要檢視此原則的權限，請參閱AWS 受管原則參考FullAccess中的[AmazonVPC](#)。

### AWS 管理策略：亞馬遜 VPC 訪ReadOnly問

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。

若要檢視此原則的權限，請參閱AWS 受管原則參考中的[AmazonVPC ReadOnly 存取](#)。

### AWS 管理策略：亞馬遜 VPC 操CrossAccountNetworkInterface作

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。

若要檢視此原則的權限，請參閱AWS 受管政策參考中的[AmazonVPC CrossAccount NetworkInterface 操作](#)。

### Amazon VPC 更新 AWS 受管政策

檢視有關 Amazon VPC AWS 受管政策更新的詳細資訊，因為此服務於 2021 年 3 月開始追蹤這些變更。

變更	描述	日期
<a href="#">the section called “亞馬遜 VPC FullAccess”</a> – 更新現有政策	已新增 GetSecurityGroupsForVpc 動作，可讓您取得可在 VPC 中使用的安全性群組。	2024年2月8日
<a href="#">the section called “亞馬遜 VPC 訪ReadOnly問”</a> – 更新現有政策	已新增 GetSecurityGroupsForVpc 動作，可讓您取得可在 VPC 中使用的安全性群組。	2024年2月8日
<a href="#">the section called “亞馬遜 VPC 操作 CrossAccount NetworkInterface”</a> – 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
<a href="#">the section called “亞馬遜 VPC 訪ReadOnly問”</a> – 更新現有政策	新增了 DescribeSecurityGroupRules 動作，可讓您檢視 <a href="#">安全群組規則</a> 。	2021年8月2日
<a href="#">the section called “亞馬遜 VPC FullAccess”</a> – 更新現有政策	新增了 DescribeSecurityGroupRules 和 ModifySecurityGroupRules 動作，可讓您檢視和修改 <a href="#">安全群組規則</a> 。	2021年8月2日
<a href="#">the section called “亞馬遜 VPC FullAccess”</a> – 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
<a href="#">the section called “亞馬遜 VPC 訪ReadOnly問”</a> – 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

## Amazon VPC 的基礎設施安全性

作為受管服務，Amazon Virtual Private Cloud 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱[AWS 雲端安全](#)。若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱[安全性支柱架構](#)。良 AWS 好的架構中的基礎結構保護。



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。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 [AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

## 網路隔離

虛擬私有雲 (VPC) 是您自己在 AWS 雲中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 位址連線，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 裝置即可存取 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，由於網路 ACL 適用於整個子網路，因此可以像 defense-in-depth 在沒有正確安全性群組的情況下啟動執行個體一樣使用。
- 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。多個網路界面也提供其他控制網路流量的選項，包括能夠建立以主機為基礎的路由政策，或能夠根據網路界面指派的子網路運用不同的 VPC 子網路路由規則。

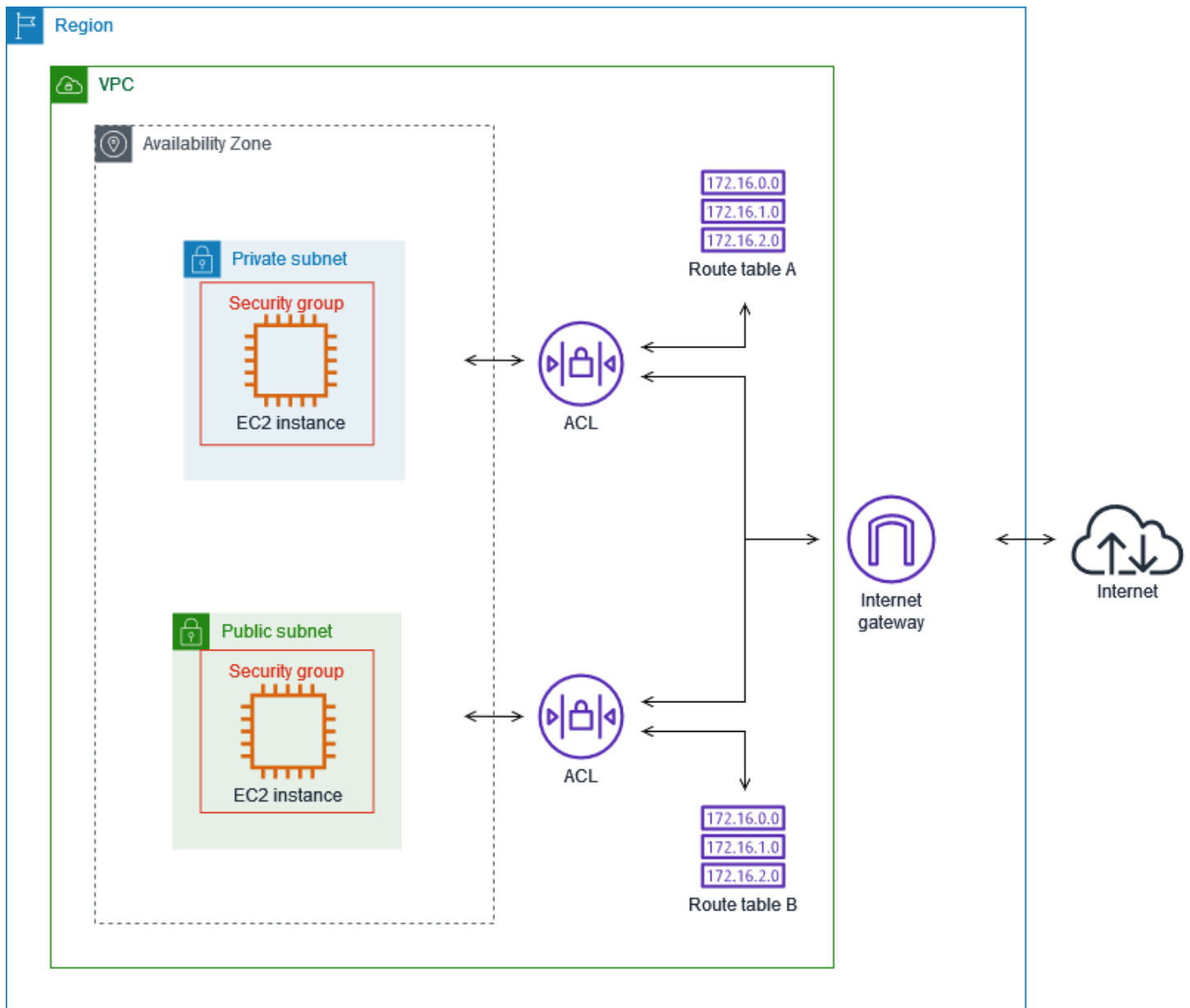
- 使用 AWS Virtual Private Network 或 AWS Direct Connect 建立從遠端網路到 VPC 的私人連線。如需詳細資訊，請參閱 [Network-to-Amazon VPC 連線選項](#)。
- 使用 [VPC 流程日誌](#) 監控到達您執行個體的流量。
- 使用 [AWS Security Hub](#) 檢查來自您執行個體的意外網路存取性。
- 使用 [AWS Network Firewall](#) 保護 VPC 中的子網路，以免遭受常見網路威脅的侵害。

## 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。

安全群組	網路 ACL
在執行個體層級運作	在子網路層級運作
僅當其與執行個體相關聯時才套用至執行個體	套用至部署在相關子網中的所有執行個體 (如果安全群組規則太過寬鬆，則提供額外一層防禦)
僅支援允許規則	支援允許規則和拒絕規則
在決定是否允許流量前，先評估所有規則	在決定是否允許流量時，從編號最低的規則開始依序評估規則
具狀態：允許傳回流量，不受任何規則影響	無狀態：傳回流量必須經該規則明確允許

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。



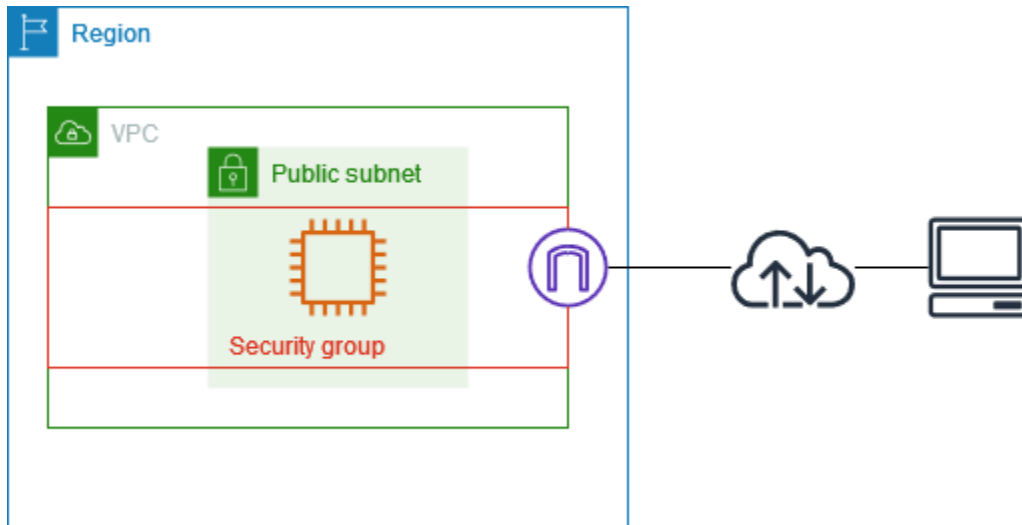
您只能使用安全群組來保護執行個體。不過，您可以新增網路 ACL 做為額外的防禦層。如需詳細資訊，請參閱 [範例：控制對子網路中執行個體的存取](#)。

## 使用安全性群組控制 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](#)
- [使用安全群組](#)

## 定價

使用安全群組無需額外收費。

## 安全群組基礎知識

- 您只能將安全群組指派給與安全群組在相同 VPC 中建立的資源。您可以將多個安全群組指派資源。
- 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。

- 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](#)。

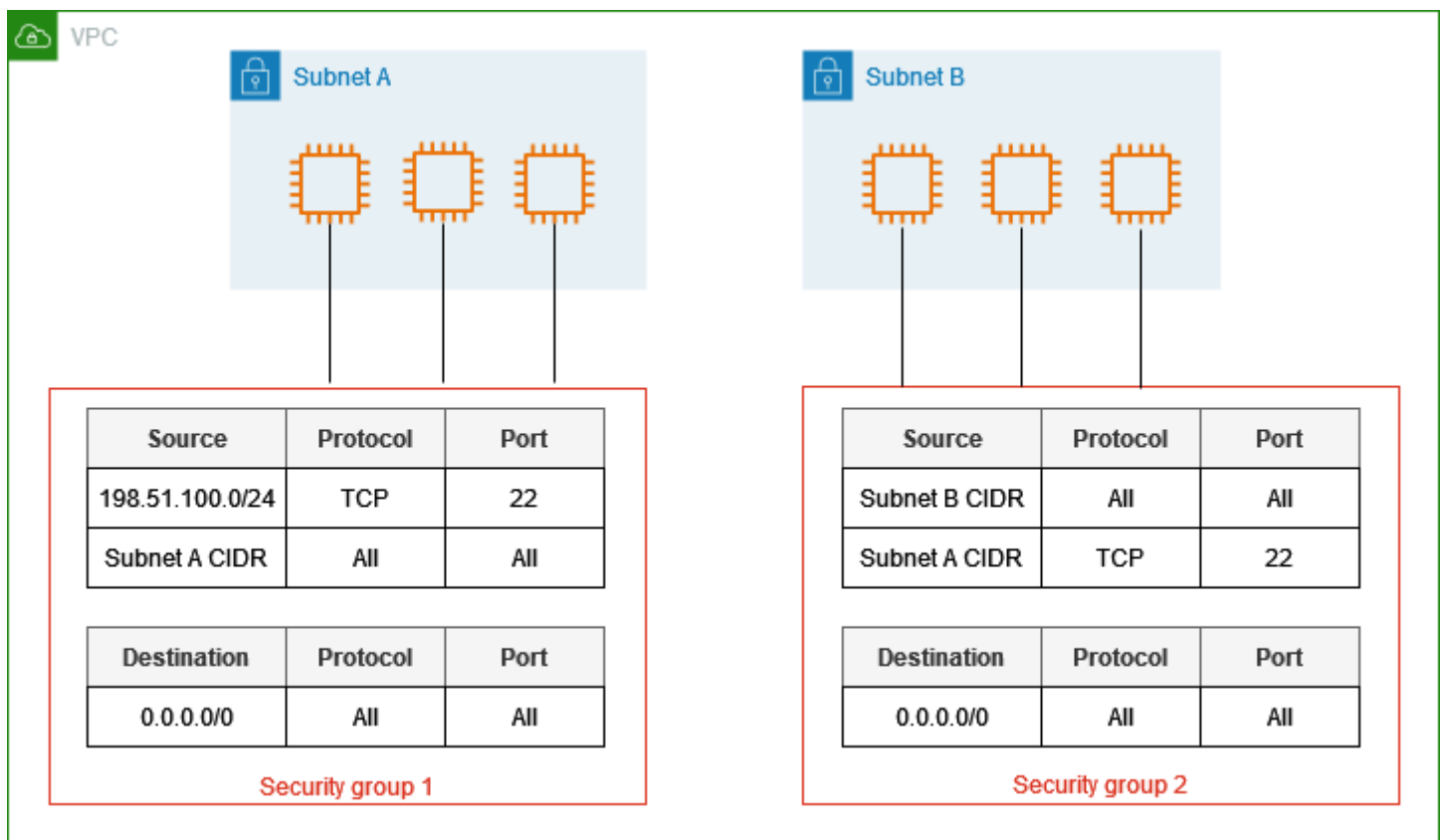
## 最佳實務

- 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](#)
- [使用安全群組規則](#)
- [範例規則](#)
- [疑難排解可達性問題](#)

### 安全群組規則基礎知識

- 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。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](#)。
- 當您建立安全性群組規則時，AWS 會為規則指派唯一 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

安全群組無法封鎖傳送至 Route 53 解析程式的 DNS 要求，有時也稱為「VPC+2 IP 位址」（請參閱 [Amazon Route 53 開發人員指南](#) Amazon Route 53 Resolver 中的，或做為 DNS）。AmazonProvided 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

- 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」。
- 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：p1-1234abc1234abc123。如需詳細資訊，請參閱 [the section called “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 `._-:/()#,@[]+=;{}!$*`。

## 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
<i>sg-0abcdef1234567890</i>	TCP	22



在安全群組規則中參考安全群組時，請注意下列事項：

- 兩個安全群組必須屬於相同的 VPC 或對等 VPC。
- 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的安全群組相關聯之 EC2 執行個體的私有 IP 地址中接收傳入流量。
- 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的安全群組相關聯之 EC2 執行個體的私有 IP 地址。

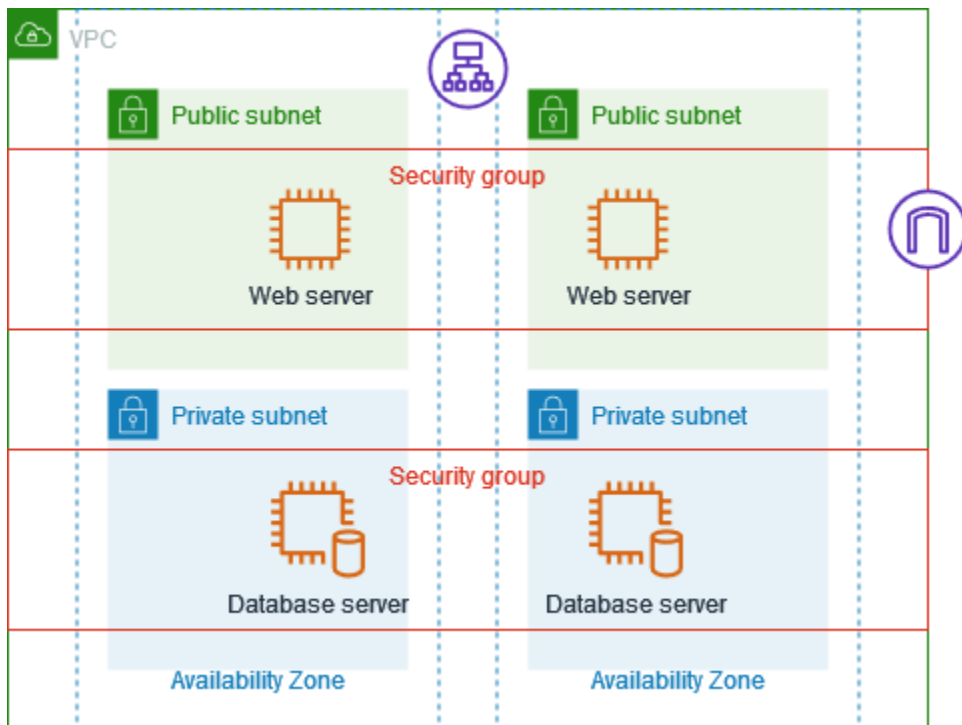
## 限制

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-managed 前置詞清單的規則會計為首碼清單的權重。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 託管前綴列表”](#)。

## 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。

如果共用 VPC 中的安全群組遭到刪除，或是 VPC 對等互連連線遭到刪除，則安全群組規則會標示為過時。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。如需詳細資訊，請參閱 [Amazon VPC 對等指南中的使用過時安全群組規則](#)。

## 使用安全群組規則

下列任務會示範如何使用安全群組規則。

所需的許可

- [管理安全群組規則](#)

任務

- [將規則新增至安全群組](#)
- [更新安全群組規則](#)
- [將安全群組規則加上標籤](#)
- [刪除安全群組規則](#)

將規則新增至安全群組

當您為安全群組新增規則時，新規則會自動套用到所有與安全群組相關聯的任何資源。

若您有 VPC 對等互連連線，您可以參考對等 VPC 的安全群組做為您安全群組規則中的來源或目標。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 VPC 安全群組](#)。

如需有關管理安全群組規則所需之許可的詳細資訊，請參閱 [管理安全群組規則](#)。

### 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。在您為連接埠 22 (SSH) 或 3,389 (RDP) 新增規則時，請僅授權特定 IP 地址範圍以存取您的執行個體。

使用主控台新增規則

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. 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. 針對每個規則，選擇 Add rule (新增規則) 並執行下列動作。
  - a. 在 Type (類型) 中，選擇要允許的通訊協定類型。
    - 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，則系統會自動設定通訊協定和連接埠範圍。
  - b. 針對 Source type (來源類型) (傳入規則) 或 Destination type (目的地類型) (傳出規則)，請執行下列其中一項操作以允許流量：
    - 選擇 Custom (自訂)，然後以 CIDR 標記法、CIDR 區塊、其他安全群組或字首清單輸入 IP 地址。
    - 選擇 Anywhere-IPv4 (任何位置-IPv4) 可允許來自任何 IPv4 地址的流量 (傳入規則) 或允許流量到達所有 IPv4 地址 (傳出規則)。此會自動為 0.0.0.0/0 IPv4 CIDR 區塊新增規則。
    - 選擇 Anywhere-IPv6 (任何位置-IPv6) 可允許來自任何 IPv6 地址的流量 (傳入規則) 或允許流量到達所有 IPv6 地址 (傳出規則)。此會自動為 ::/0 IPv6 區塊新增規則。
    - 選擇 My IP (我的 IP) 可僅允許來自 (傳入規則) 或傳送到 (傳出規則) 本機電腦的公有 IPv4 地址的流量。
  - c. (選用) 針對 Description (描述)，指定規則的簡短描述。
6. 選擇 Save rules (儲存規則)。

若要使用將規則新增至安全群組 AWS CLI

使用 [authorize-security-group-ingress](#) 和 [authorize-security-group-egress](#) 命令。

更新安全群組規則

當您更新規則時，更新的規則會自動套用至與安全群組相關聯的任何資源。

如需有關管理安全群組規則所需之許可的詳細資訊，請參閱[管理安全群組規則](#)。

使用主控台更新規則

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. 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. 視需求更新規則。
6. 選擇 Save rules (儲存規則)。

若要使用更新安全群組規則 AWS CLI

使用 [modify-security-group-rules](#)、[update-security-group-rule-descriptions-ingress](#) 和 [update-security-group-rule-descriptions-egress](#) 命令。

將安全群組規則加上標籤

將標籤新增至您的資源，以利您依據用途、擁有者或環境來整理並辨識資源。您可以為安全群組規則新增標籤。每個安全群組規則的標籤索引鍵必須是唯一的。如果新增的標籤有已經和安全群組規則建立關聯的索引鍵，則此動作會更新該標籤的值。

使用主控台將規則加上標籤

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. 在 Inbound rules (傳入規則) 或 Outbound rules (傳出規則) 索引標籤上，選取規則的核取方塊，然後選取 Manage tags (管理標籤)。
5. Manage tags (管理標籤) 頁面會顯示指派給規則的任何標籤。若要新增標籤，請選擇 Add tag (新增標籤)，然後輸入標籤金鑰和值。若要移除標籤，請在您要移除的標籤旁邊選擇 Remove (移除)。
6. 選擇 Save changes (儲存變更)。

若要使用標記規則 AWS CLI

使用 [create-tags](#) 命令。

刪除安全群組規則

當您從安全群組刪除規則時，變更會自動套用到所有與安全群組相關聯的所有執行個體。

## 使用主控台刪除安全群組規則

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。
3. 選取安全群組。
4. 選擇 Actions (動作)，然後選擇 Edit inbound rules (編輯傳入規則) 以移除傳入規則，或選擇 Edit outbound rules (編輯傳出規則) 以移除傳出規則。
5. 選擇規則右側的 Delete (刪除) 按鈕以進行刪除。
6. 選擇 Save rules (儲存規則)。或者，選擇預覽變更，檢閱變更，然後選擇確認。

## 若要使用刪除安全群組規則 AWS CLI

使用 [revoke-security-group-ingress](#) 和 [revoke-security-group-egress](#) 命令。

## 範例規則

### Web 伺服器

以下是 Web 伺服器安全群組的範例規則。Web 伺服器可接收來自所有 IPv4 和 IPv6 地址的 HTTP 和 HTTPS 流量，並將 SQL 或 MySQL 流量傳送至您的資料庫伺服器。

#### Warning

在您為連接埠 22 (SSH) 或 3389 (RDP) 新增規則以便可以存取 EC2 執行個體時，我們建議您僅授權特定 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。

### 傳入

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

來源	通訊協定	連接埠範圍	描述
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
<i>##### IPv4 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 SSH 存取
<i>##### IPv6 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 SSH 存取
<i>##### IPv4 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 RDP 存取
<i>##### IPv6 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 RDP 存取
<i>##### ID</i>	全部	全部	(選用) 允許來自與此安全群組相關聯之其他伺服器的傳入流量。

## 傳出

目的地	通訊協定	連接埠範圍	描述
<i>## Microsoft SQL Server ##### ID</i>	TCP	1433	允許傳出 Microsoft SQL 伺服器存取

目的地	通訊協定	連接埠範圍	描述
## MySQL ##### ID	TCP	3306	允許傳出 MySQL 存取

## 資料庫伺服器

資料庫伺服器需要允許傳入特定通訊協定的規則，例如 MySQL 或 Microsoft SQL Server。如需範例，請參閱《Amazon EC2 使用者指南》中的[資料庫伺服器規則](#)。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](#)。

## 疑難排解可達性問題

Reachability Analyzer 是一種靜態配置分析工具。使用可 Reachability Analyzer 來分析和偵錯 VPC 中兩個資源之間的網路連接性。可 Reachability Analyzer 產生這些資源之間的虛擬路徑的 hop-by-hop 詳細信息，當它們是可訪問的，並識別阻塞組件，否則。例如，它可以識別遺漏或設定錯誤的安全群組規則。

如需詳細資訊，請參閱 [Reachability Analyzer Guide](#) (《Reachability Analyzer 指南》)。

## 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規則。



## 傳入

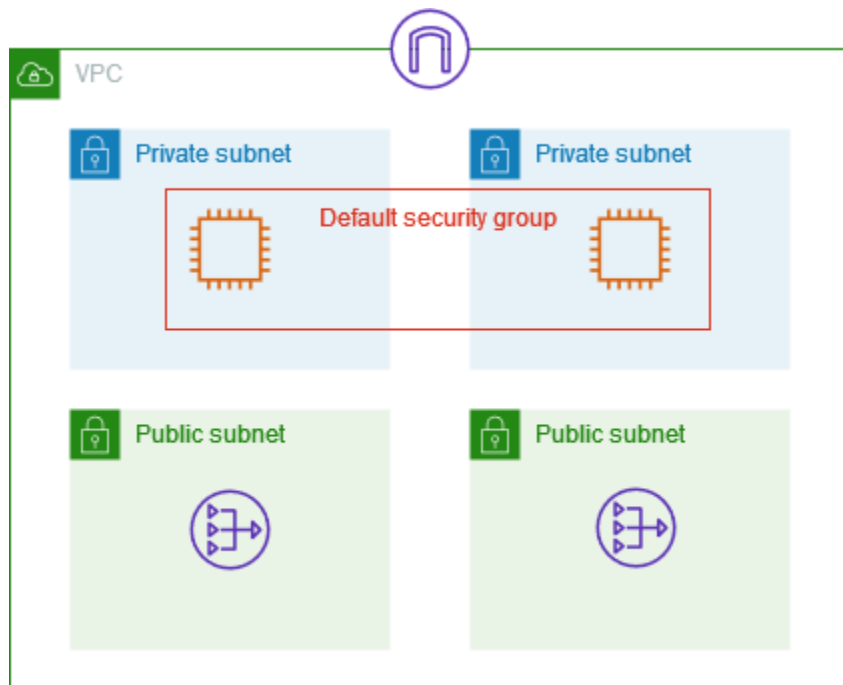
來源	通訊協定	連接埠範圍	描述
<i>sg-1234567890abcdef0</i>	全部	全部	允許來自指派給此安全群組的所有資源的傳入流量。來源為此安全群組的 ID。

## 傳出

目的地	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。



## 使用安全群組

下列任務會示範如何使用安全群組。

### 任務

- [建立安全群組](#)
- [檢視您的安全群組](#)
- [將您的安全群組加上標籤](#)
- [刪除安全群組](#)
- [使用 Firewall Manager 管理安全群組](#)

### 所需的許可

開始之前，請務必備妥必要的許可。

- [管理安全群組](#)
- [管理安全群組規則](#)

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。如需安全群組規則的詳細資訊，請參閱 [安全群組規則](#)。

## 建立安全群組

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。

### 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. 從 VPC 中選擇 VPC。安全群組只能在建立該群組的 VPC 中使用。
6. 您可以立即新增安全群組規則，也可以稍後再新增。如需詳細資訊，請參閱 [將規則新增至安全群組](#)。
7. 您可以立即新增標籤，也可以稍後再新增。若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的索引鍵和值。
8. 選擇 Create Security Group (建立安全群組)。

建立安全群組之後，您可能想要執行以下其中一項：

- 在啟動執行個體時或變更目前指派給執行個體的安全群組時，將安全群組指派給 EC2 執行個體。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [啟動執行個體](#) 或 [變更安全群組](#)。
- 新增安全群組規則。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。如需安全群組規則的詳細資訊，請參閱 [使用安全群組規則](#)。

### 若要使用建立安全性群組 AWS CLI

使用 [create-security-group](#) 命令。

## 檢視您的安全群組

您可以按照以下方式檢視安全群組的相關資訊。

### 使用主控台檢視您的安全群組

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. 系統會列出您的安全群組。若要檢視包括其輸入和輸出規則等特定安全群組詳細資訊，請選取安全群組。如需更新安全群組規則的詳細資訊，請參閱 [更新安全群組規則](#)。

### 若要跨區域檢視所有安全群組

前往 <https://console.aws.amazon.com/ec2globalview/home> 開啟 Amazon EC2 全域檢視主控台。如需詳細資訊，請參閱 [Amazon EC2 使用者指南中的使用 Amazon EC2 全域檢視列出和篩選資源](#)。

### 使用檢視您的安全性群組 AWS CLI

使用 [describe-security-groups](#) 和 [describe-security-group-rules](#) 命令。

### 將您的安全群組加上標籤

將標籤新增至您的資源，以利您依據用途、擁有者或環境來整理並辨識資源。您可以為安全群組新增標籤。每個安全群組的標籤索引鍵必須是唯一的。如果新增的標籤有已經和規則建立關聯的索引鍵，則此動作會更新該標籤的值。

### 使用主控台將安全群組加上標籤

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. 選取安全群組的核取方塊。
4. 選擇 Actions (動作)、Manage tags (管理標籤)。Manage tags(管理標籤) 頁面會顯示指派給安全群組的所有標籤。
5. 若要新增標籤，請選擇新增標籤，然後輸入標籤金鑰和標籤值。若要移除標籤，請選擇標籤旁的 Remove (移除) 以移除。
6. 選擇 Save Changes (儲存變更)。

### 若要使用標記安全群組 AWS CLI

使用 [create-tags](#) 命令。

### 刪除安全群組

只有在未與資源相關聯的情況下，才能刪除安全群組。您無法刪除預設安全群組。

若您使用主控台，您可以一次刪除超過一個安全群組。若您使用命令列或 API，您一次只能刪除一個安全群組。

## 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. 出現確認提示時，請選擇刪除。

## 若要使用刪除安全群組 AWS CLI

使用 [delete-security-group](#) 命令。

## 使用 Firewall Manager 管理安全群組

AWS Firewall Manager 簡化您跨多個帳戶和資源的安全性群組管理和維護工作。使用 Firewall Manager，您可以從單一中央系統管理員帳戶設定及稽核組織的安全群組。Firewall Manager 會自動在帳號和資源中套用規則和防護，甚至在您新增資源時也可套用。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保護的新資源時，Firewall Manager 特別有用。

您可以使用 Firewall Manager 以下列方式集中管理安全群組：

- 設定全組織適用的通用基準安全群組：您可以使用通用安全群組政策，為組織中的帳戶和資源提供安全群組的集中控制關聯。您可以指定要在您組織中要套用政策的項目與如何套用。
- 稽核組織中現有的安全群組：您可以使用稽核安全群組政策來檢查組織安全群組中正在使用的現有規則。您可以將策略範圍限制為稽核組織內標記的所有帳號、特定帳號或資源。Firewall Manager 會自動偵測新帳號和資源並進行稽核。您可以建立稽核規則來設定在組織中允許或不允許的安全群組規則護欄，以及檢查是否有未使用或多餘的安全群組。
- 取得不合規資源的報告並加以修復：您可以針對基準和稽核政策取得不合規資源的報告和警示。您也可以設定自動修復工作流程，以修復 Firewall Manager 偵測到的任何不合規的資源。

若要深入瞭解如何使用 Firewall Manager 員來管理安全性群組，請參閱AWS Firewall Manager 開發人員指南中的下列資源：

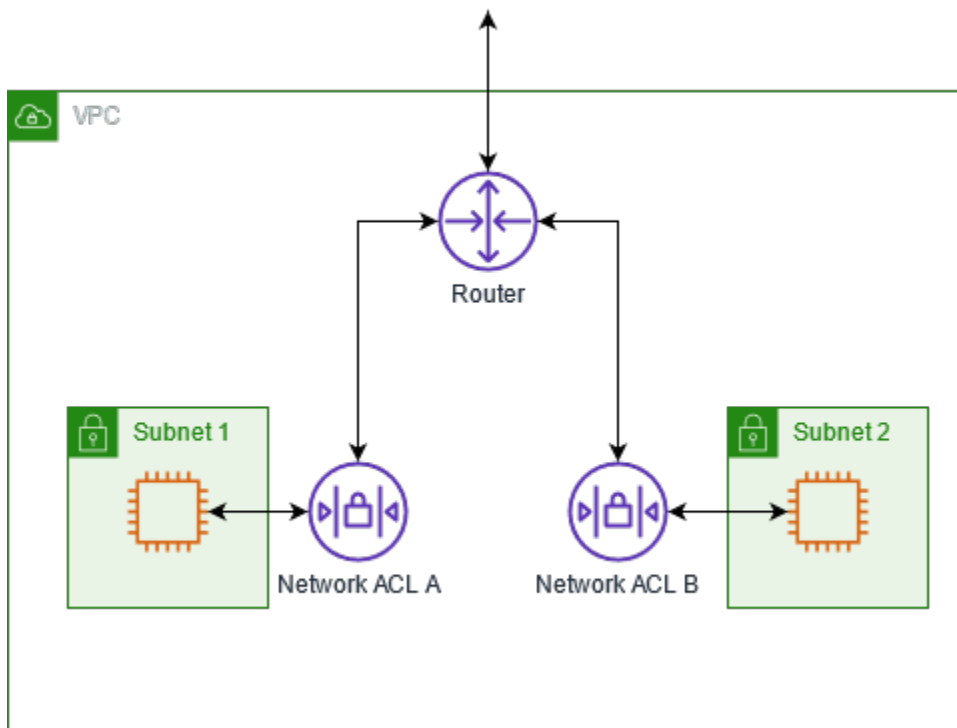
- [AWS Firewall Manager 前提](#)
- [開始使用 AWS Firewall Manager Amazon VPC 安全群組政策](#)
- [安全性群組原則的運作方式 AWS Firewall Manager](#)
- [安全群組政策使用案例](#)

## 使用網路 ACL 控制子網路的流量

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或傳出流量。您可使用 VPC 的預設網路 ACL，亦可使用與安全群組規則類似的規則來為 VPC 建立自訂網路 ACL，為 VPC 提供多一層的安全性。

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](#)
- [預設網路 ACL](#)
- [自訂網路 ACL](#)
- [自訂網路 ACL 和其他 AWS 服務](#)

- [暫時性連接埠](#)
- [路徑 MTU 探索](#)
- [使用網路 ACL](#)
- [範例：控制對子網路中執行個體的存取](#)
- [疑難排解可達性問題](#)

## 網路 ACL 基本概念

下列是您需要了解的網路 ACL 基本事項：

- 您的 VPC 已自動隨附可修改的預設網路 ACL。根據預設，它會允許所有傳入和傳出 IPv4 流量與 IPv6 流量 (如適用)。
- 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。
- 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 具有傳入規則和傳出規則。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。
- 網路 ACL 無法封鎖傳送至或傳出路由 53 解析程式的 DNS 要求 (也稱為 VPC+2 IP 位址或 DNS)。AmazonProvided 若要透過 Route 53 Resolver 篩選 DNS 請求，則可以如《Amazon Route 53 開發人員指南》所述，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
- 每個 VPC 的網路 ACL 數目和每個網路 ACL 的規則數目有配額 (亦稱為限制)。如需詳細資訊，請參閱 [Amazon VPC 配額](#)。

## 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。

## 預設網路 ACL

系統會將網路 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 也包括一個規則編號為星號 (\*) 的規則。此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。您無法修改或移除這項規則。

下列為 VPC 的範例預設網路 ACL，其僅支援 IPv4。




## 傳入

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
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒絕

## 傳出

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕
100	所有 IPv4 流量	全部	全部	0.0.0.0/0	允許
*	所有 IPv4 流量	全部	全部	0.0.0.0/0	拒絕

如果您使用 IPv6 CIDR 區塊建立 VPC；或者，如果您將 IPv6 CIDR 區塊與現有 VPC 建立關聯，我們會自動建立規則以允許所有 IPv6 流量流進和流出您的子網路。我們也會新增規則編號為星號的規則，以確保拒絕未符合任何其他編號規則的封包。您無法修改或移除這些規則。下列為 VPC 的範例預設網路 ACL，其支援 IPv4 和 IPv6。

 Note

若您已修改預設網路 ACL 的傳入規則，我們就不會在您將 IPv6 區塊與 VPC 建立關聯時自動新增傳入 IPv6 流量的 ALLOW 規則。同樣地，若您已修改傳出規則，我們就不會自動新增傳出 IPv6 流量的 ALLOW 規則。

## 傳入

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

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕
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

## 傳出

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

## 自訂網路 ACL

下列範例顯示 VPC 的自訂網路 ACL，其僅支援 IPv4。其中包括可允許 HTTP 和 HTTPS 流量 (100 和 110) 的傳入規則。也有對應的傳出規則，可啟用對上述傳入流量的回應 (140)，其涵蓋暫時性連接埠 32768-65535。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](#)。

網路 ACL 也包括傳入規則，其允許 SSH 和 RDP 流量進入子網路。傳出規則 120 可讓回應離開子網路。

網路 ACL 具有傳出規則 (100 和 110)，其允許傳出 HTTP 和 HTTPS 流量流出子網路。也有對應的傳入規則，可啟用對上述傳出流量的回應 (140)，其涵蓋暫時性連接埠 32768-65535。

每個網路 ACL 都包括一個規則編號為星號的預設規則。此規則可確保在封包未符合任何其他規則時拒絕該封包。您無法修改或移除這項規則。

## 傳入

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。
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。
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)。
130	RDP	TCP	3389	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 RDP 流量流向 Web 伺服器 (透過網際網路閘道)。
140	自訂 TCP	TCP	32768-65535	0.0.0.0/0	允許	允許來自網際網路的回傳傳入 IPv4 流量 (亦即出自子網路的請求)。  此範圍僅為範例。
*	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。

## 傳出

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。
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。
120	SSH	TCP	1024-65535	192.0.2.0/24	允許	允許輸出將 SSH 流量傳回至您家用網路的公用 IPv4 位址範圍 (透過網際網路閘道)。
140	自訂 TCP	TCP	32768-65535	0.0.0.0/0	允許	允許傳出 IPv4 回應網際網路上的用戶端 (例如, 將網頁提供給瀏覽子網路中 Web 伺服器的使用者)。  此範圍僅為範例。
*	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) 尚未處理的所有傳出 IPv4 流量。

在封包前往子網路時，我們會依據子網路的相關聯 ACL 傳入規則再次評估該封包 (從規則清單頂端開始，由上至下)。下列為評估 HTTPS 連接埠 (443) 是否要拒絕封包的進行方式。封包不符合第一個評估規則 (規則 100)。它符合第二個規則 (110)，其允許封包進入子網路。如果連接埠 139 (NetBIOS) 已拒絕封包，它就不符合任何規則，而 \* 規則最終也會拒絕封包。

如果您需要開放範圍很廣的連接埠，但該範圍內有您要拒絕的特定連接埠，則您可能想要新增拒絕規則。您只要比允許廣泛連接埠流量的規則更早在資料表中放入拒絕規則即可。

您可以新增允許規則，視您的使用案例而定。例如，您可以新增一個原則，允許 DNS 解析所用連接埠 53 的傳出 TCP 和 UDP 存取權。對於每個新增的規則，請確定其中設有允許回應流量的傳入或傳出規則。

下列範例顯示 VPC 自訂網路 ACL 範例，其具備相關聯的 IPv6 CIDR 區塊。這個網路 ACL 包括的規則適用於所有 IPv6 HTTP 和 HTTPS 流量。在此情況下，已在 IPv4 流量的現有規則之間插入新規則。您也可以將這些規則新增為編號更高的規則。IPv4 和 IPv6 流量是分開的，因此，IPv4 流量的規則都不會套用至 IPv6 流量。

## 傳入

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)。
130	RDP	TCP	3389	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 RDP 流量流向

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕	說明
						Web 伺服器 (透過網際網路開道)。
140	自訂 TCP	TCP	32768-65535	0.0.0.0/0	允許	允許來自網際網路的回傳傳入 IPv4 流量 (亦即出自子網路的請求)。  此範圍僅為範例。
145	自訂 TCP	TCP	32768-65535	::/0	允許	允許來自網際網路的回傳傳入 IPv6 流量 (亦即出自子網路的請求)。  此範圍僅為範例。
*	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。
*	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 #	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。

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕	說明
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。
140	自訂 TCP	TCP	32768-65535	0.0.0.0/0	允許	<p>允許傳出 IPv4 回應網際網路上的用戶端 (例如，將網頁提供給瀏覽子網路中 Web 伺服器的使用者)。</p> <p>此範圍僅為範例。</p>
145	自訂 TCP	TCP	32768-65535	::/0	允許	<p>允許傳出 IPv6 回應網際網路上的用戶端 (例如，將網頁提供給瀏覽子網路中 Web 伺服器的使用者)。</p> <p>此範圍僅為範例。</p>
*	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) 尚未處理的所有傳出 IPv4 流量。
*	所有流量	全部	全部	::/0	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

## 自訂網路 ACL 和其他 AWS 服務

如果您建立自訂網路 ACL，請注意它可能會對您使用其他 AWS 服務建立的資源造成的影響。

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。如需負載平衡器和後端執行個體之建議網路 ACL 規則的詳細資訊，請參閱《Classic Load Balancer 的使用者指南》中的 [VPC 中負載平衡器的網路 ACL](#)。

## 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 功能使用連接埠

例如，如果送達 VPC 之 Web 伺服器的請求來自網際網路的 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類型 (Amazon Linux、Windows Server 2008 等) 的暫時性連線埠。

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。

## 路徑 MTU 探索

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。



針對 IPv4，若主機傳送的封包大小大於接收主機的 MTU，或是大於路徑上裝置的 MTU，則接收主機或裝置便會丟棄封包，然後傳回下列 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。若主機傳送的封包大小大於接收主機的 MTU，或是大於路徑上裝置的 MTU，則接收主機或裝置便會丟棄封包，然後傳回下列 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 [EC2 執行個體的網路最大傳輸單位 \(MTU\)](#)。

## 使用網路 ACL

下列任務會示範如何搭配 Amazon VPC 主控台使用網路 ACL。

### 任務

- [判斷網路 ACL 關聯](#)
- [建立網路 ACL](#)
- [新增和刪除規則](#)
- [將子網路與網路 ACL 建立關聯](#)
- [取消子網路與網路 ACL 的關聯](#)
- [變更子網路的網路 ACL](#)
- [刪除網路 ACL](#)
- [API 和命令概觀](#)
- [使用 Firewall Manager 員管理網路 ACL](#)

### 判斷網路 ACL 關聯

您可以使用 Amazon VPC 主控台，來判斷與子網路相關聯的網路 ACL：網路 ACL 可以與多個子網路建立關聯，因此您也可以判斷哪些子網路與網路 ACL 相關聯。

## 判斷哪個網路 ACL 與子網路有所關聯

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 (子網路)，然後選取子網路。

Network ACL (網路 ACL) 標籤中包含與子網路相關聯的網路 ACL 以及網路 ACL 的規則。

## 判斷哪些子網路與網路 ACL 相關聯

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)。Associated With (關聯對象) 欄會指出每個網路 ACL 的相關聯子網路數目。
3. 選取網路 ACL。
4. 在詳細資訊窗格中，選擇 Subnet Associations (子網路關聯) 以顯示與網路 ACL 相關聯的子網路。

## 建立網路 ACL

您可以為 VPC 建立自訂網路 ACL。根據預設，在您新增規則之前，您建立的網路 ACL 會封鎖所有傳入和傳出流量，且除非您明確將某個網路 ACL 與子網路建立關聯，否則其不會與子網路建立關聯。

### 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 Create Network ACL (建立網路 ACL)。
4. 在 Create Network ACL (建立網路 ACL) 對話方塊中，選擇性命名您的網路 ACL，並從 VPC 清單選取您 VPC 的 ID。然後，選擇 Yes, Create (是，建立)。

## 新增和刪除規則

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。您不必終止並重新啟動子網路中的執行個體。這些變更在很短時間後便會生效。

### ⚠ Important

如果您同時新增和刪除規則，請格外謹慎。網路 ACL 規則會定義哪些類型的網路流量可以傳入或傳出您的 VPC。如果您刪除傳入或傳出規則，然後新增的項目數量超過 [Amazon VPC 配額](#) 中允許的上限，那麼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，並且意外阻止流量傳入和傳出您的 VPC。

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。

### 新增規則至網路 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. 在詳細資訊窗格中，依據您要新增的規則類型，選擇 Inbound Rules (傳入規則) 或 Outbound Rules (傳出規則) 標籤，然後選擇 Edit (編輯)。
4. 在 Rule # (規則 #) 中，輸入規則的編號 (例如 100)。規則編號不得與網路 ACL 中已使用的編號重複。我們會從最低的編號開始，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。

5. 從 Type (類型) 清單選取一個規則。例如，若要新增 HTTP 的規則，請選擇 HTTP。若要新增規則以允許所有 TCP 流量，請選擇 All TCP (所有 TCP)。針對其中部分選項 (例如 HTTP)，我們會為您填入連接埠。若要使用未列出的通訊協定，請選擇 Custom Protocol Rule (自訂通訊協定規則)。
6. (選用) 如果您要建立自訂通訊協定規則，請從 Protocol (通訊協定) 清單選取通訊協定編號和名稱。如需詳細資訊，請參閱 [IANA List of Protocol Numbers](#)。
7. (選用) 如果您所選取的通訊協定需要連接埠號碼，請輸入連接埠號碼或連接埠範圍，中間以連字號分隔 (例如 49152-65535)。
8. 在 Source (來源) 或 Destination (目標) 欄位中 (視此為傳入或傳出規則而定)，輸入要套用規則的 CIDR 範圍。
9. 從 Allow/Deny (允許/拒絕) 清單，選取 ALLOW (允許) 允許指定的流量，或 DENY (拒絕) 拒絕指定的流量。
10. (選用) 若要新增其他規則，請選擇 Add another rule (新增其他規則) 並視需要重複步驟 4 到 9。

11. 完成後，選擇 Save (儲存)。

### 刪除網路 ACL 中的規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)，然後選取網路 ACL。
3. 在詳細資訊窗格中，選取 Inbound Rules (傳入規則) 或 Outbound Rules (傳出規則) 標籤，然後選擇 Edit (編輯)。針對您要刪除的規則，選擇 Remove (移除)，然後選擇 Save (儲存)。

### 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)。

### 取消子網路與網路 ACL 的關聯

您可以取消自訂網路 ACL 與子網路的關聯。當子網路已取消與自訂網路 ACL 的關聯時，它會自動與預設網路 ACL 相關聯。

#### 取消子網路與網路 ACL 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 Network ACLs (網路 ACL)，然後選取網路 ACL。
3. 在詳細資訊窗格中，選擇 Subnet Associations (子網路關聯) 標籤。
4. 選擇 Edit (編輯)，然後取消選取子網路的 Associate (關聯) 核取方塊。選擇 Save (儲存)。

## 變更子網路的網路 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，它一開始就會與預設網路 ACL 建立關聯。建議您改將子網路與您建立的自訂網路 ACL 建立關聯。

變更子網路的網路 ACL 之後，您不需要終止和重新啟動子網路中的執行個體。這些變更在很短時間後便會生效。

### 變更子網路的網路 ACL 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 (子網路)，然後選取子網路。
3. 選擇 Network ACL (網路 ACL) 標籤，然後選擇 Edit (編輯)。
4. 從 Change to (變更為) 清單中，選取要與子網路建立關聯的網路 ACL，然後選擇 Save (儲存)。

## 刪除網路 ACL

僅有當網路 ACL 未與任何子網路相關聯時，您才可以刪除該網路 ACL。您無法刪除預設網路 ACL。

### 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. 選取網路 ACL，然後選擇 Delete (刪除)。
4. 在確認對話方塊中，選擇 Yes, Delete (刪除)。

## API 和命令概觀

您可以使用命令列或 API 執行此頁面所述的任務。如需命令列介面與可用 API 清單的詳細資訊，請參閱 [使用 Amazon VPC](#)。

### 為您的 VPC 建立網路 ACL

- [create-network-acl](#) (AWS CLI)
- [New-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

## 說明一或多個網路 ACL

- [describe-network-acls](#) (AWS CLI)
- [Get-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

## 新增規則至網路 ACL

- [create-network-acl-entry](#) (AWS CLI)
- [New-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

## 刪除網路 ACL 中的規則

- [delete-network-acl-entry](#) (AWS CLI)
- [Remove-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

## 取代網路 ACL 中的現有規則

- [replace-network-acl-entry](#) (AWS CLI)
- [Set-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

## 取代網路 ACL 關聯

- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (AWS Tools for Windows PowerShell)

## 刪除網路 ACL

- [delete-network-acl](#) (AWS CLI)
- [Remove-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

## 使用 Firewall Manager 員管理網路 ACL

AWS Firewall Manager 簡化您跨多個帳戶和子網路的網路 ACL 管理和維護工作。您可以使用 Firewall Manager 員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，或經常新增要自動防止中央系統管理員帳戶防護的新子網路時，Firewall Manager 特別有用。

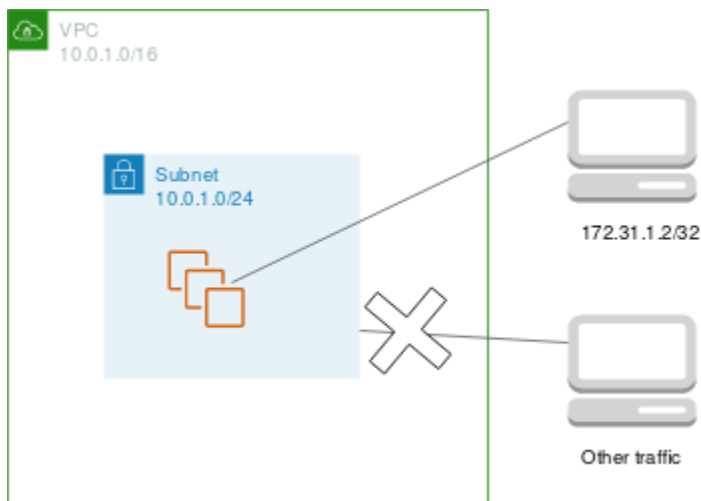
使用 Firewall Manager 網路 ACL 策略時，您可以使用單一系統管理員帳戶來設定、監視和管理您想要在整個組織中使用的網路 ACL 中定義的最低規則集。您可以指定組織中的哪些帳戶和子網路位於 Firewall Manager 員策略範圍內。Firewall Manager 會報告範圍內子網路之網路 ACL 的符合性狀態，而且您可以將 Firewall Manager 員設定為自動修復不符合標準的網路 ACL，使其符合規範。

若要進一步了解如何使用 Firewall Manager 員來管理網路 ACL，請參閱AWS Firewall Manager 開發人員指南中的下列資源：

- [AWS Firewall Manager 前提](#)
- [開始使用 AWS Firewall Manager Amazon VPC 網路 ACL 政策](#)
- [Amazon Virtual Private Cloud 網路存取控制清單 \(ACL\) 政策](#)

## 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，並可從信任的遠端電腦存取。遠端電腦可能是區域網路中的電腦，或是位於不同子網路或 VPC 中的執行個體。您可以使用它來連線到執行個體，以執行管理工作。您的安全群組規則和網路 ACL 規則可允許從遠端電腦的 IP 地址 (172.31.1.2/32) 進行存取。其他所有來自網際網路或其他網路的流量都會遭拒。此案例可讓您以彈性的方式變更執行個體的安全群組或安全群組規則，並將網路 ACL 做為備份防禦 layer。



以下是與執行個體產生關聯的安全群組範例。安全群組有狀態。因此，您不需要允許回應傳入流量的規則。

## 傳入

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-123456 7890abcdef0	與此安全群組相關聯的所有執行個體都可以彼此通訊。
SSH	TCP	22	172.31.1.2/32	允許來自遠端電腦的傳入 SSH 存取。

## 傳出

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-123456 7890abcdef0	與此安全群組相關聯的所有執行個體都可以彼此通訊。

以下是與執行個體的子網路產生關聯的網路 ACL 範例。網路 ACL 規則會套用至子網路中的所有執行個體。網路 ACL 無狀態。因此，您需要允許回應傳入流量的規則。

## 傳入

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。



## 傳出

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	1024-6553 5	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。

如果您不小心將安全群組規則設得太寬鬆，此範例中的網路 ACL 會持續只允許來自指定 IP 地址的存取。例如，下列安全群組包含允許來自任何 IP 地址的傳入 SSH 存取的規則。不過，如果您將此安全群組與使用網路 ACL 的子網路中的執行個體建立關聯，則只有子網路 and 遠端電腦內的其他執行個體可以存取執行個體，因為網路 ACL 規則拒絕其他傳入子網路的流量。

## 傳入

Type	通訊協定	連接埠範圍	來源	評論
所有流量	全部	全部	sg-123456 7890abcdef0	與此安全群組相關聯的所有執行個體都可以彼此通訊。
SSH	TCP	22	0.0.0.0/0	允許來自任何 IP 地址的 SSH 存取。

## 傳出

Type	通訊協定	連接埠範圍	目的地	評論
所有流量	全部	全部	0.0.0.0/0	允許所有對外流量。

## 疑難排解可達性問題

Reachability Analyzer 是一種靜態配置分析工具。使用可 Reachability Analyzer 來分析和偵錯 VPC 中兩個資源之間的網路連接性。可 Reachability Analyzer 產生這些資源之間的虛擬路徑的 hop-by-hop 詳細信息，當它們是可訪問的，並識別阻塞組件，否則。例如，它可以識別遺漏或設定錯誤的網路 ACL 規則。

如需詳細資訊，請參閱 [Reachability Analyzer Guide](#) (《Reachability Analyzer 指南》)。

## Amazon Virtual Private Cloud 的恢復能力

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。AWS 區域 提供多個實體分離和隔離的可用區域，這些可用區域使用低延遲、高輸送量和高冗餘網路進行連線。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。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全域基礎結構](#)。

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：

- [了解恢復模式和權衡 \(架構部落格\)AWS](#)
- [規劃您的網路拓撲 \(AWS Well-Architected 的架構\)](#)
- [Amazon Virtual Private Cloud 連線選項 \(AWS 白皮書\)](#)

## Amazon Virtual Private Cloud 的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱 [AWS 服務 遵循規範計劃](#) 方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱 [AWS 規範計劃AWS](#)。

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 [下載中的報告中的 AWS Artifact](#)。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- [安全性與合規性快速入門指南](#) — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- [在 Amazon Web Services 上架構 HIPAA 安全性與合規性](#) — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 應用程式。

**Note**

並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 [HIPAA 資格服務參照](#)。

- [AWS 合規資源AWS](#) — 此工作簿和指南集合可能適用於您的產業和所在地。
- [AWS 客戶合規指南](#) — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- [使用AWS Config 開發人員指南中的規則評估資源](#) — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#)— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。
- [Amazon GuardDuty](#) — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- [AWS Audit Manager](#)— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化管理風險以及遵守法規和業界標準的方式。

## 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。可用區域是一或多個獨立資料中心，在一個區 AWS 域中具有備援電源、網路和連線能力。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。如需詳細資訊，請參閱 [AWS 上的 Amazon VPC](#)。
- 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 [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 ACL 控制子網路的流量](#)。
- 使用 AWS Identity and Access Management (IAM) 身分聯盟、使用者和角色來管理 VPC 中 AWS 資源的存取。如需詳細資訊，請參閱 [Amazon VPC 的 Identity and Access Management](#)。
- 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》)。
- 用 AWS Network Firewall 於透過篩選入站和出站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 GuardDuty 用 Amazon 偵測 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 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

您可以將 Amazon VPC 與其他 VPC 搭配使用，AWS 服務 建立符合您需求的解決方案。

## 目錄

- [使用 AWS PrivateLink 將 VPC 連線至服務](#)
- [使用 AWS Network Firewall 篩選網路流量](#)
- [使用 Route 53 Resolver DNS Firewall 來篩選 DNS 流量](#)
- [使用可達性分析器疑難排解可達性問題](#)

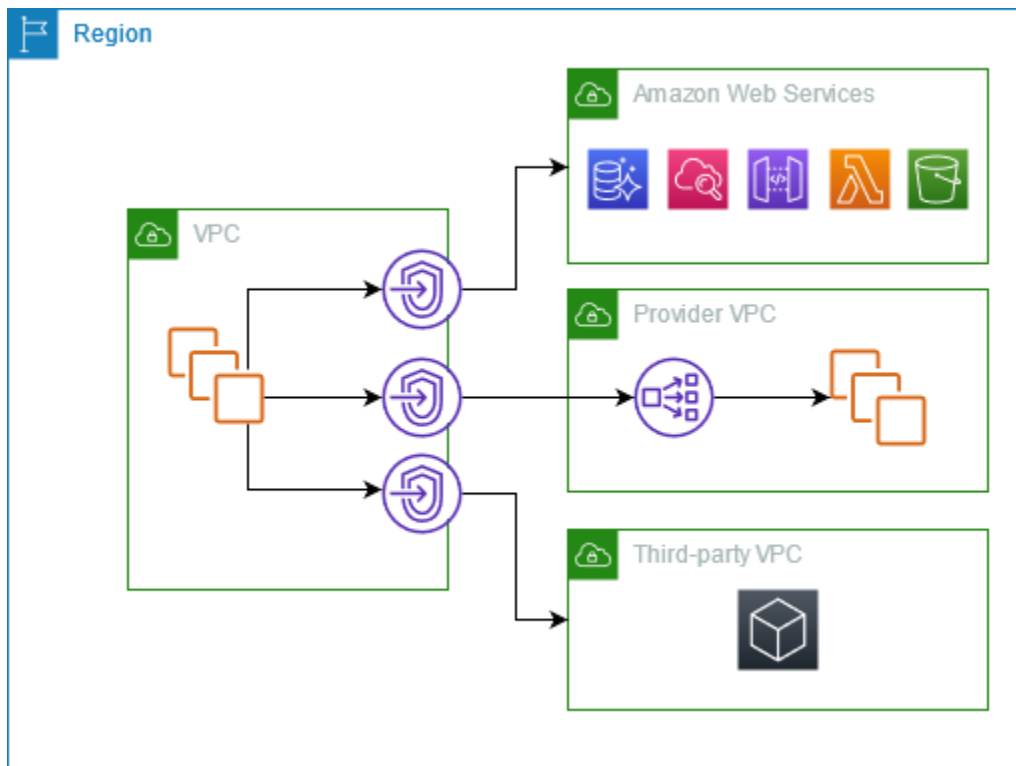
## 使用 AWS PrivateLink 將 VPC 連線至服務

AWS PrivateLink 在 Virtual Private Cloud (VPC) 與支援的 AWS 服務、由其他 AWS 帳戶 託管的服務和支援的 AWS Marketplace 服務之間建立私有連線。您不需要使用網際網路閘道、NAT 裝置、AWS Direct Connect 連線或 AWS Site-to-Site VPN 連線來與服務通訊。

若要使用 AWS PrivateLink，請在 VPC 中建立 VPC 端點，指定服務和子網路的名稱。這會在子網路中建立彈性網路介面，用於指定於服務的流量進入點。

您可以建立自有 AWS PrivateLink 提供的服務 (VPC 端點服務)，並讓其他 AWS 客戶能夠存取您的服務。

下圖顯示了 AWS PrivateLink 常見的使用案例。左側的 VPC 在私有子網路中有多個 EC2 執行個體和三個介面 VPC 端點。最頂層 VPC 端點連線至 AWS 服務。中間層 VPC 端點連線至另一個 AWS 帳戶 託管的服務 (VPC 端點服務)。最底層 VPC 端點連線至 AWS Marketplace 合作夥伴服務。



如需更多詳細資訊，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	<p>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。</p> <p>如需詳細資訊，請參閱 <a href="#">AWS Network Firewall 中的防火牆</a>。</p>
防火牆政策	<p>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。</p>

Network Firewall 資源	描述
	如需詳細資訊，請參閱 <a href="#">AWS Network Firewall 中的防火牆政策</a> 。

### 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	<p>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。</p> <p>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。</p>

DNS Firewall 資源	描述
	如需詳細資訊，請參閱 <a href="#">Route 53 Resolver DNS Firewall 中的規則群組和規則</a> 。
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 <a href="#">Route 53 Resolver DNS Firewall 中的網域清單</a> 。

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](#)。

## 使用可達性分析器疑難排解可達性問題

Reachability Analyzer 是一種靜態配置分析工具。使用可 Reachability Analyzer 來分析和偵錯 VPC 中兩個資源之間的網路連接性。可 Reachability Analyzer 產生這些資源之間的虛擬路徑的 hop-by-hop 詳細信息，當它們是可訪問的，並識別阻塞組件，否則。

您可以使用「可 Reachability Analyzer」來分析下列資源之間的可達性：

- 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 閘道器

如需詳細資訊，請參閱 [Reachability Analyzer Guide](#) (《Reachability Analyzer 指南》)。



# VPC 範例

以下是虛擬私有雲端 (VPC) 的範例組態。

## 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 連線至您自己的網路，請參閱《AWS Site-to-Site VPN 使用者指南》中的 [站台對站台 VPN 架構](#)。
- 若要讓 VPC 彼此連線並連線至您自己的網路，請參閱 Amazon VPC 傳輸閘道中的 [傳輸閘道範例](#)。

## 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

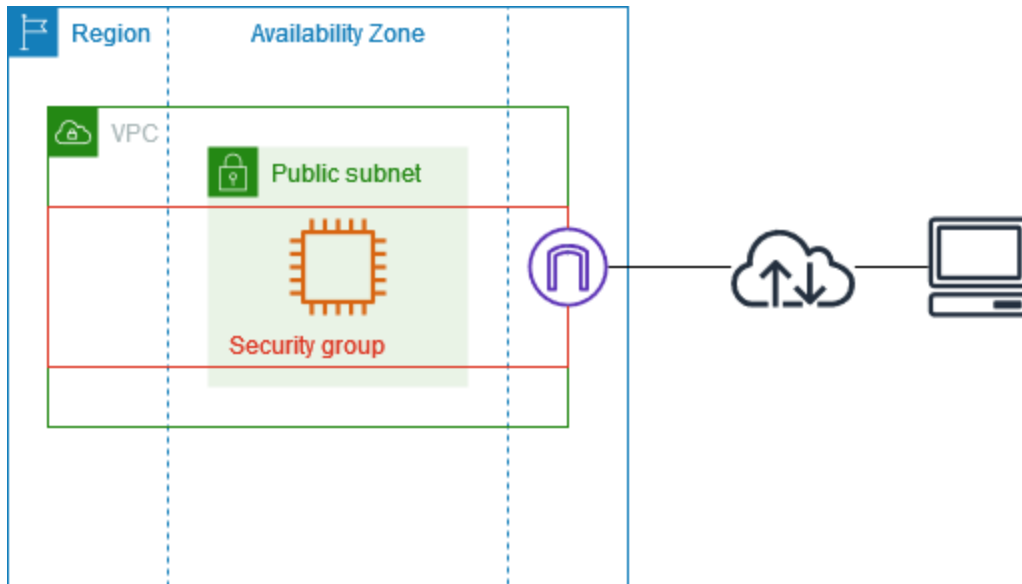
此範例示範如何建立可用作開發或測試環境的 VPC。由於此 VPC 並非用於生產，因此不需要在多個可用區域中部署伺服器。若要維持低成本和複雜性，您可以在單一可用區域中部署伺服器。

## 目錄

- [概要](#)
- [建立 VPC](#)
- [部署您的應用程式](#)
- [測試組態](#)
- [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。

目的地	目標
<i>10.0.0.0/16</i>	區域
<i>2001:db8:1234:1a00::/56</i>	區域
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

## 安全性

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。

### 傳入

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
<i>##### IPv4 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 SSH 存取
<i>##### IPv6 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 SSH 存取
<i>##### IPv4 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 RDP 存取
<i>##### IPv6 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 RDP 存取

## 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. 對於 Name tag auto-generation (自動產生名稱標籤)，請輸入 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。如需更多詳細資訊，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。如需更多詳細資訊，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 Create VPC (建立 VPC)。

## 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 文件中的[建立 Linux AMI](#) 或[建立 Windows AMI](#)。或者，您也可以使用 [EC2 Image Builder](#) 來建立和管理您的 Amazon Machine Image (AMI)。

## 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》)。

## 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。如需更多詳細資訊，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。

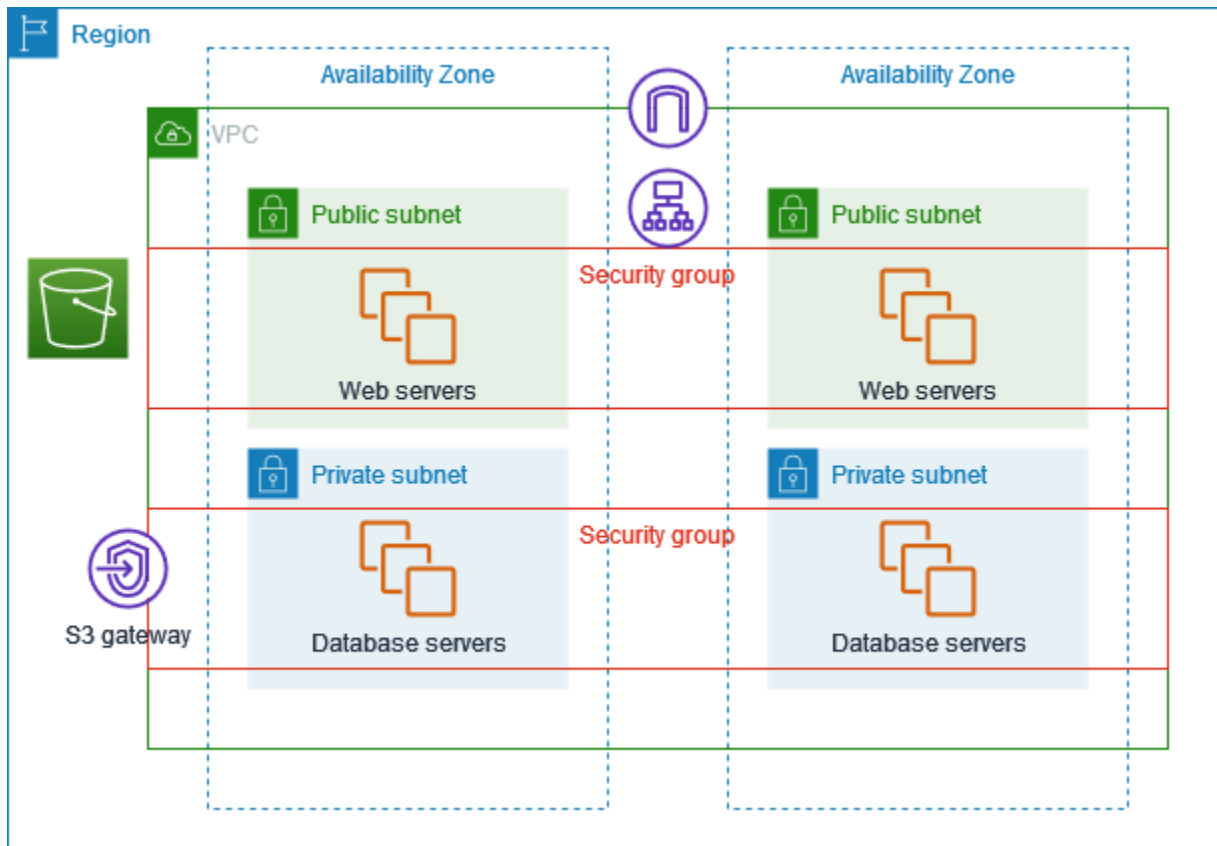
### 目錄

- [概要](#)
- [建立 VPC](#)
- [部署您的應用程式](#)
- [測試組態](#)
- [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

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。

目的地	目標
<i>10.0.0.0/16</i>	區域
<i>2001:db8:1234:1a00::/56</i>	區域
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

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。

目的地	目標
<i>10.0.0.0/16</i>	區域
<i>2001:db8:1234:1a00::/56</i>	本機
<i>s3- ##### ID</i>	<i>S3 #####</i>

## 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。

### 傳入

來源	通訊協定	連接埠範圍	描述
<i>##### ID</i>	TCP	80	允許來自負載平衡器的傳入 HTTP 存取
<i>##### ID</i>	TCP	443	允許來自負載平衡器的傳入 HTTPS 存取

來源	通訊協定	連接埠範圍	描述
<i>##### IPv4 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 SSH 存取
<i>##### IPv6 #####</i>	TCP	22	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 SSH 存取
<i>##### IPv4 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv4 IP 地址的傳入 RDP 存取
<i>##### IPv6 #####</i>	TCP	3389	(選用) 允許來自您網路中 IPv6 IP 地址的傳入 RDP 存取

## 傳出

目的地	通訊協定	連接埠範圍	描述
<i>## Microsoft SQL Server ##### ID</i>	TCP	1433	允許傳出 Microsoft SQL Server 存取資料庫伺服器。
<i>## MySQL ##### # ID</i>	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。

## 傳入

來源	通訊協定	連接埠範圍	評論
<i>Web ##### ID</i>	TCP	1433	允許來自 Web 伺服器的傳入 Microsoft SQL Server 存取
<i>Web ##### ID</i>	TCP	3306	允許來自 Web 伺服器的傳入 MySQL Server 存取



## 傳出

目的地	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](#)。

## 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. 前往 <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，或清除它以提供您自己的名稱標籤給 VPC 資源。
  - 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。如果您選擇要使用 VPC 的租用 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[使用已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，然後輸入 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。

## 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 [AWS 列資料庫：如何選擇](#)。

## 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》)。

## 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。如需更多詳細資訊，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

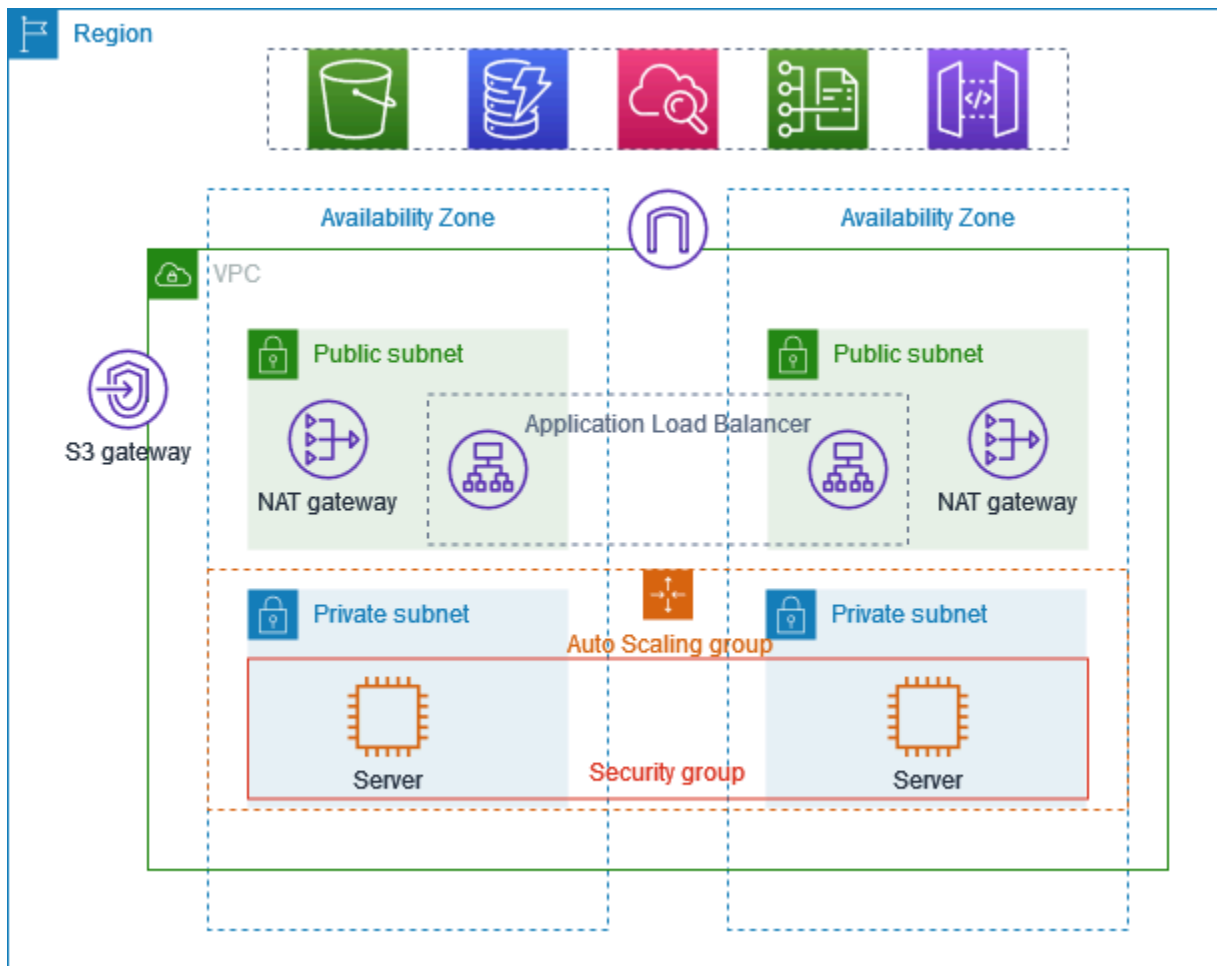
此範例示範如何建立 VPC，以便用於生產環境中的伺服器。若要提升彈性，您可以使用 Auto Scaling 群組和 Application Load Balancer，在兩個可用區域中部署伺服器。若要提高安全性，您可以在私有子網路中部署伺服器。伺服器會透過負載平衡器接收要求。伺服器可以使用 NAT 閘道連線至網際網路。若要提升彈性，您可以在兩個可用區域中部署 NAT 閘道。

### 目錄

- [概要](#)
- [建立 VPC](#)
- [部署您的應用程式](#)
- [測試組態](#)
- [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
<i>10.0.0.0/16</i>	區域
<i>2001:db8:1234:1a00::/56</i>	區域
0.0.0.0/0	<i>igw-id</i>

目的地	目標
::/0	<i>igw-id</i>

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。

目的地	目標
<i>10.0.0.0/16</i>	區域
<i>2001:db8:1234:1a00::/56</i>	區域
0.0.0.0/0	<i>nat-gateway-id</i>
::/0	<i>eigw-id</i>
<i>s3- #### ID</i>	<i>S3 #####</i>

## 安全性

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。

### 傳入

來源	通訊協定	連接埠範圍	評論
<i>##### ID</i>	<i>#####</i>	<i>#####</i>	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
<i>##### ID</i>	<i>#####</i>	<i>#####</i>	允許來自負載平衡器的傳入運作狀態檢查流量

## 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. 對於 Name tag auto-generation (自動產生名稱標籤)，請輸入 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. 在 Number of public subnet (公有子網路數量) 中，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。如需更多詳細資訊，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 Create VPC (建立 VPC)。

## 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](#)。

## 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》)。

## 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。如需更多詳細資訊，請參閱 [the section called “刪除您的 VPC”](#)。

## Amazon VPC 配額

下表列出您 AWS 帳戶之 Amazon VPC 資源的配額 (以前稱為限制)。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	<a href="#">是</a>	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	<a href="#">是</a>	
每個 VPC 的 IPv4 CIDR 區塊數	5	<a href="#">是</a> (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	<a href="#">是</a> (最多 50 個)	您可以配置到單一 VPC 的 CIDR 數目。

### 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 地址

名稱	預設	可調整	說明
每個區域的彈性 IP 地址數	5	<a href="#">是</a>	此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。
每個公有 NAT 閘道的彈性 IP 地址	2	<a href="#">是</a>	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	<a href="#">是</a>	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	<a href="#">是</a>	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	<a href="#">是</a>	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	否	
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。您必須使用 AWS Support Center Console 來[開啟服務限制提高案例](#)。

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 <a href="#">調整字首清單大小</a> 。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	5,000	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擁有 5,000 個字首清單的參照，以及在所有子網路路由表中對字首清單的 5,000 個參照。如果您與其他帳號共用前置碼清單，其他 AWS 帳戶對您前置碼清單的參照會計入此配額。

## 網路 ACL

名稱	預設	可調整	說明
每個 VPC 的網路 ACL 數	200	<a href="#">是</a>	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	<a href="#">是</a>	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 <a href="#">每個執行個體類型的網路介面</a> 。
每個區域的網路介面	5,000	<a href="#">是</a>	此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。此限制是針對每個可用區域 (AZ) 強制執行。例如，如果網路介面位於三個 AZ 中，則每個 AZ 的限制為 5,000，而且該區域的上限為 15,000。

## 路由表

名稱	預設	可調整	說明
每個 VPC 的路由表	200	<a href="#">是</a>	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)	50	<a href="#">是</a>	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。

## 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	<a href="#">是</a>	<p>此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。</p> <p>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。</p>
每個安全群組的傳入或傳出規則	60	<a href="#">是</a>	<p>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 <a href="#">the section called “安全群組大小”</a>。</p> <p>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。</p>
每個網路介面的安全群組數	5	<a href="#">是</a>	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。

名稱	預設	可調整	說明
		(最多 16 個)	

## VPC 共享

所有標準 VPC 配額均適用於共享 VPC。

名稱	預設	可調整	說明
每個 VPC 的參與者帳戶	100	<a href="#">是</a>	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	<a href="#">是</a>	這是可與 AWS 帳戶共用的子網路數目上限。

## 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	<a href="#">是</a> (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	<a href="#">是</a> (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 Amazon EC2 節流的詳細資訊，請參閱 Amazon EC2 API 參考中的 [API 請求節流](#) 設定。

### 額外配額資源

如需詳細資訊，請參閱下列內容：

- AWS Client VPN 《AWS Client VPN 管理員指南》中的 [配額](#)
- 《AWS Direct Connect 使用者指南》中的 [AWS Direct Connect 配額](#)
- 《Amazon VPC 對等互連指南》中的 [對等互連配額](#)
- PrivateLink AWS PrivateLink 指南中的 [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
<a href="#">首選租賃時間</a>	您現在可以選擇指派 IPv6 的執行中執行個體經過 DHCPv6 租用續約的頻率。	2024年2月20日
<a href="#">AWS 受管理策略更新</a>	Amazon VPC 更新了 Amazon VPCFullAccess 和受 AmazonVPCReadOnlyAccess 管政策。	2024年2月8日
<a href="#">AWS 受管理策略更新</a>	Amazon VPC 更新了受 AmazonVPCCrossAccountNetworkInterfaceOperations 管政策。	2023 年 9 月 25 日
<a href="#">已取代 EC2-Classic</a>	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
<a href="#">將次要 IPv4 地址新增至 NAT 閘道</a>	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

<a href="#">符合 IAM 最佳實務</a>	更新了指南以符合 IAM 最佳實務。如需詳細資訊，請參閱 <a href="#">IAM 中的安全最佳實務</a> 。	2023 年 1 月 4 日
<a href="#">挑選 NAT 閘道的私有 IP 地址</a>	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
<a href="#">IPv6 預設的閘道路由器組態</a>	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
<a href="#">轉移彈性 IP 地址</a>	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
<a href="#">網路地址使用指標</a>	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
<a href="#">將流程日誌發佈到 Amazon 資料 Firehose</a>	您可以指定 Amazon 資料 Firehose 交付串流作為流程日誌資料的目的地。	2022 年 9 月 8 日
<a href="#">NAT 閘道頻寬</a>	NAT 閘道現在支援高達 100 Gbps 的頻寬 (之前為 45 Gbps)，並且每秒最多可處理 1,000 萬個封包 (之前為 400 萬個封包)。	2022 年 6 月 15 日
<a href="#">多個 IPv6 CIDR 區塊</a>	您可以將最多五個 IPv6 CIDR 區塊與 VPC 建立關聯。	2022 年 5 月 12 日
<a href="#">重組</a>	本《Amazon Virtual Private Cloud 使用者指南》的一般重組。	2022 年 1 月 2 日



<a href="#">NAT 閘道 IPv6 至 IPv4</a>	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
<a href="#">VPC 中僅限 IPv6 的子網</a>	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
<a href="#">Amazon S3 的 VPC Flow Logs 交付選項</a>	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
<a href="#">Amazon EC2 全域檢視</a>	Amazon EC2 全球視圖可讓您在單一主控台中檢視跨多個區域的 VPC、子網路、執行個體、安全群組和磁碟 AWS 區。	2021 年 9 月 1 日
<a href="#">更具體的路由</a>	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
<a href="#">支援安全群組規則的資源 ID 和標記</a>	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
<a href="#">私有 NAT 閘道</a>	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

<a href="#">建立時的標籤</a>	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
<a href="#">受管理的字首清單</a>	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
<a href="#">流程日誌增強功能</a>	新的流程記錄欄位可用，您可以為發佈到 CloudWatch 記錄的流程記錄指定自訂格式。	2020 年 5 月 4 日
<a href="#">流量日誌的標記支援</a>	您可以將標籤新增至流量日誌。	2020 年 3 月 16 日
<a href="#">在建立 NAT 閘道時套用標籤</a>	您可以在建立 NAT 閘道時新增標籤。	2020 年 3 月 9 日
<a href="#">流程日誌的最大彙總時間間隔</a>	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
<a href="#">網路邊界群組組態</a>	您可以從 Amazon Virtual Private Cloud Console 為您的 VPC 設定網路邊界群組。	2020 年 1 月 22 日
<a href="#">私有 DNS 名稱</a>	您可 AWS PrivateLink 以使用私人 DNS 名稱，從 VPC 中私下存取基於服務。	2020 年 1 月 6 日
<a href="#">閘道路由表</a>	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
<a href="#">流程日誌增強功能</a>	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

<a href="#">VPC 共享</a>	您可以與同一組織中的多個帳戶共用位於相同 VPC 中的子網路。AWS	2018 年 11 月 27 日
<a href="#">建立預設子網</a>	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
<a href="#">NAT 閘道的標籤支援</a>	您可以標記 NAT 閘道。	2017 年 9 月 7 日
<a href="#">NAT 閘道的 Amazon CloudWatch 指標</a>	您可以檢視 NAT 閘道的 CloudWatch 指標。	2017 年 9 月 7 日
<a href="#">安全群組規則說明</a>	您可以為安全群組規則新增說明。	2017 年 8 月 31 日
<a href="#">您 VPC 的輔助 IPv4 CIDR 區塊</a>	您可在您的 VPC 中新增多個 IPv4 CIDR 區塊。	2017 年 8 月 29 日
<a href="#">復原彈性 IP 地址</a>	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
<a href="#">建立預設 VPC</a>	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
<a href="#">IPv6 支援</a>	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
<a href="#">非 RFC 1918 IP 地址範圍的 DNS 解析支援</a>	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
<a href="#">NAT 閘道</a>	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

<a href="#">VPC 流程日誌</a>	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
<a href="#">ClassicLink</a>	您可以使用 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
<a href="#">使用私有託管區域</a>	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
<a href="#">修改子網的公有 IP 定址屬性</a>	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
<a href="#">指派公有 IP 地址</a>	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
<a href="#">啟用 DNS 主機名稱和停用 DNS 解析</a>	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
<a href="#">VPC 無所不在</a>	新增對五 AWS 個區域中的 VPC、多個可用區域中的 VPC、每個 AWS 帳戶多個 VPC 以及每個 VPC 多個 VPN 連線的支援。	2011 年 8 月 3 日
<a href="#">專用執行個體</a>	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。