

---

# Amazon Virtual Private Cloud

## 使用者指南



## Amazon Virtual Private Cloud: 使用者指南

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

# Table of Contents

什麼是 Amazon VPC ? .....	1
Amazon VPC 概念 .....	1
存取 Amazon VPC .....	1
Amazon VPC 的定價 .....	1
Amazon VPC 配額 .....	1
PCI DSS 合規 .....	2
Amazon VPC 的運作方式 .....	3
VPC 和子網路 .....	3
預設和非預設 VPC .....	3
路由表 .....	4
存取網際網路 .....	4
存取公司或家用網路 .....	6
透過 AWS PrivateLink 存取服務 .....	7
連接 VPC 和網路 .....	8
AWS 私有全球網路注意事項 .....	8
支援的平台 .....	9
Amazon VPC 資源 .....	9
入門 .....	10
概觀 .....	10
步驟 1：建立 VPC .....	10
檢視您的 VPC 相關資訊 .....	11
步驟 2：在您的 VPC 中啟動執行個體 .....	11
步驟 3：將彈性 IP 地址指派給執行個體 .....	12
步驟 4：清理 .....	13
後續步驟 .....	13
IPv6 入門 .....	13
步驟 1：建立 VPC .....	14
步驟 2：建立安全群組 .....	16
步驟 3：啟動執行個體 .....	16
Amazon VPC 主控台精靈組態 .....	17
具有單一公有子網路的 VPC .....	18
具有公有和私有子網路 (NAT) 的 VPC .....	24
具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC .....	37
僅具有私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC .....	50
VPC 的範例 .....	55
範例：共享公有子網路和私有子網路 .....	55
範例：使用的服務 AWS PrivateLink 和 VPC 對等 .....	56
範例：服務供應商設定服務 .....	57
範例：服務消費者設定存取 .....	57
範例：服務供應商設定橫跨區域的服務 .....	58
範例：服務消費者設定跨區域存取 .....	59
範例：使用 AWS CLI 建立 IPv4 VPC 及子網路 .....	60
步驟 1：建立 VPC 和子網路 .....	60
步驟 2：將您的子網路設為公有 .....	60
步驟 3：在子網路中啟動執行個體 .....	62
步驟 4：清理 .....	64
範例：使用 AWS CLI 建立 IPv6 VPC 及子網路 .....	64
步驟 1：建立 VPC 和子網路 .....	65
步驟 2：設定公有子網路 .....	65
步驟 3：設定輸出限定私有子網路 .....	67
步驟 4：修改子網路的 IPv6 定址行為 .....	68
步驟 5：在公有子網路中啟動執行個體 .....	68
步驟 6：在私有子網路中啟動執行個體 .....	70
步驟 7：清理 .....	71

VPC 和子網路 .....	73
VPC 和子網路基本概念 .....	73
VPC 和子網路大小調整 .....	76
IPv4 的 VPC 和子網路規模 .....	76
將 IPv4 CIDR 區塊新增至 VPC .....	77
IPv6 的 VPC 和子網路規模 .....	80
子網路路由 .....	81
子網路安全 .....	81
使用 VPC 和子網路 .....	81
建立 VPC .....	82
在您的 VPC 中建立子網路 .....	83
將輔助 IPv4 CIDR 區塊與您的 VPC 建立關聯 .....	84
建立 IPv6 CIDR 區塊與 VPC 的關聯 .....	84
建立 IPv6 CIDR 區塊與子網路的關聯 .....	85
在您的子網路中啟動執行個體 .....	85
刪除您的子網路 .....	86
取消 IPv4 CIDR 區塊與您 VPC 的關聯 .....	86
取消 IPv6 CIDR 區塊與您 VPC 或子網路的關聯 .....	87
刪除您的 VPC .....	88
使用共用 VPC .....	89
共用 VPC 必要條件 .....	89
共用子網路 .....	89
取消共享已共用的子網路 .....	90
識別共用的子網路的擁有者 .....	90
共用子網路許可 .....	90
適用於擁有者及參與者的計費和計量 .....	91
不受共用子網路支援的服務 .....	91
限制 .....	91
擴充您的 VPC .....	91
將您的 VPC 資源擴展到本機區域 .....	92
將您的 VPC 資源擴展到 Wavelength 區域 .....	92
AWS Outposts 中的子網路 .....	94
預設 VPC 和預設子網路 .....	95
預設 VPC 元件 .....	95
預設子網路 .....	97
可用性與支援的平台 .....	97
偵測支援的平台 .....	97
檢視您的預設 VPC 和預設子網路 .....	98
在您的預設 VPC 中啟動 EC2 執行個體 .....	98
使用主控台來啟動 EC2 執行個體 .....	99
使用命令列啟動 EC2 執行個體 .....	99
刪除您的預設子網路和預設 VPC .....	99
建立預設的 VPC .....	99
建立預設子網路 .....	100
IP 定址 .....	102
私有 IPv4 地址 .....	103
公有 IPv4 地址 .....	103
IPv6 地址 .....	104
您子網路的 IP 定址行為 .....	104
使用 IP 地址 .....	104
修改您子網路的公有 IPv4 定址屬性 .....	105
修改您子網路的公有 IPv6 定址屬性 .....	105
在啟動執行個體期間指派公有 IPv4 地址 .....	105
在啟動執行個體期間指派公有 IPv6 地址 .....	106
將 IPv6 地址指派給執行個體 .....	107
從執行個體取消指派 IPv6 地址 .....	107
API 和命令概觀 .....	108

遷移至 IPv6 .....	108
範例：在含公有和私有子網路的 VPC 中啟用 IPv6 .....	109
步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網路的關聯 .....	112
步驟 2：更新路由表 .....	113
步驟 3：更新安全群組規則 .....	113
步驟 4：變更執行個體類型 .....	114
步驟 5：將 IPv6 地址指派給執行個體 .....	114
步驟 6：(選用) 在執行個體上設定 IPv6 .....	115
安全性 .....	121
資料保護 .....	121
網際網路流量隱私權 .....	122
傳輸中加密 .....	123
Identity and Access Management .....	123
對象 .....	124
使用身分來驗證 .....	124
使用政策管理存取權 .....	125
Amazon VPC 如何搭配 IAM 運作 .....	127
政策範例 .....	129
疑難排解 .....	135
記錄和監控 .....	137
彈性 .....	137
合規驗證 .....	137
安全群組 .....	138
安全群組基礎知識 .....	138
VPC 的預設安全群組 .....	139
安全群組規則 .....	140
EC2-Classic 和 EC2-VPC 間安全群組的差異 .....	141
使用安全群組 .....	141
使用 AWS Firewall Manager 集中管理 VPC 安全群組 .....	145
網路 ACL .....	146
網路 ACL 基本概念 .....	146
網路 ACL 規則 .....	147
預設網路 ACL .....	147
自訂網路 ACL .....	148
自訂網路 ACL 和其他 AWS 服務 .....	151
暫時性連接埠 .....	152
路徑 MTU 探索 .....	152
使用網路 ACL .....	152
範例：控制對子網路中執行個體的存取 .....	156
VPC 精靈案例的建議規則 .....	158
VPC 流程日誌 .....	158
流程日誌基礎知識 .....	159
流程日誌記錄 .....	160
流程日誌記錄範例 .....	163
流程日誌限制 .....	167
流程日誌定價 .....	168
發佈至 CloudWatch Logs .....	168
發佈至 Amazon S3 .....	172
使用流程日誌 .....	176
疑難排解 .....	180
最佳實務 .....	182
其他資源 .....	182
VPC 聯網元件 .....	183
網路界面 .....	183
路由表 .....	184
路由表概念 .....	184
路由表的運作方式 .....	184

路由優先順序 .....	189
路由選項範例 .....	191
使用路由表 .....	197
字首清單 .....	204
字首清單的概念和規則 .....	205
使用字首清單 .....	205
字首清單的識別與存取管理 .....	209
使用共用字首清單 .....	210
網際網路閘道 .....	212
啟用網際網路存取 .....	212
將網際網路閘道新增至 VPC。 .....	214
輸出限定網際網路閘道 .....	218
輸出限定網際網路閘道基本概念 .....	218
使用輸出限定網際網路閘道 .....	219
API 和 CLI 概觀 .....	220
電信業者閘道 .....	221
啟用 電信運營商 網路存取 .....	221
使用電信業者閘道 .....	221
管理區域 .....	226
NAT .....	226
NAT 閘道 .....	226
NAT 執行個體 .....	243
NAT 執行個體和 NAT 閘道的比較 .....	250
DHCP 選項集 .....	251
DHCP 選項集概觀 .....	251
Amazon DNS 伺服器 .....	253
變更 DHCP 選項 .....	253
使用 DHCP 選項集 .....	253
API 和命令概觀 .....	256
DNS .....	256
DNS 主機名稱 .....	256
VPC 中的 DNS 支援 .....	257
DNS 配額 .....	258
檢視 EC2 執行個體的 DNS 主機名稱 .....	258
檢視並更新 VPC 的 DNS 支援 .....	259
使用私有託管區域 .....	259
VPC 互連 .....	260
彈性 IP 地址 .....	260
彈性 IP 位址概念和規則 .....	260
使用彈性 IP 地址 .....	261
ClassicLink .....	264
VPC 端點 和 VPC 端點服務 (AWS PrivateLink) .....	265
VPC 端點概念 .....	265
使用 VPC 端點 .....	265
VPC 端點 .....	266
界面端點 .....	266
閘道端點 .....	279
使用 VPC 端點 控制服務的存取 .....	292
刪除 VPC 端點 .....	293
VPC 端點服務 (AWS PrivateLink) .....	294
概觀 .....	294
端點服務可用區域的考量 .....	296
端點服務 DNS 名稱 .....	296
連線至內部部署的資料中心 .....	270
透過 VPC 對等連線存取服務 .....	296
使用 Proxy Protocol (代理通訊協定) 取得連線資訊 .....	296
端點服務限制 .....	297

建立 VPC 端點服務組態 .....	297
為您的端點服務新增和移除許可 .....	298
變更 網路負載平衡器 和接受設定 .....	300
接受與拒絕界面端點連線請求 .....	300
建立與管理端點服務的通知 .....	301
新增或移除 VPC 端點服務標籤 .....	303
刪除端點服務組態 .....	304
Identity and Access Management .....	305
端點服務的私有 DNS 名稱 .....	306
網域名稱驗證考量 .....	307
VPC 端點服務私有 DNS 名稱驗證 .....	308
修改現有的端點服務私有 DNS 名稱 .....	309
檢視端點服務私有 DNS 名稱組態 .....	309
手動啟動端點服務私有 DNS 名稱網域驗證 .....	310
移除端點服務私有 DNS 名稱 .....	310
私有 DNS 名稱網域驗證 TXT 記錄 .....	311
針對常見的網域驗證問題進行疑難排解 .....	312
可與 AWS PrivateLink 搭配使用的 AWS 服務 .....	314
VPN 連接 .....	319
配額 .....	320
VPC 和子網路 .....	320
DNS .....	320
彈性 IP 地址 (IPv4) .....	320
閘道 .....	321
客戶管理的字首清單 .....	321
網路 ACL .....	321
網路界面 .....	322
路由表 .....	322
安全群組 .....	322
VPC 對等連線 .....	323
VPC 端點 .....	323
AWS Site-to-Site VPN 連線 .....	324
VPC 共享 .....	324
Amazon EC2 API 調節 .....	324
文件歷史記錄 .....	325

# 什麼是 Amazon VPC ?

Amazon Virtual Private Cloud (Amazon VPC) 可讓您將 AWS 資源啟動至已定義的虛擬網路。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。

## Amazon VPC 概念

Amazon VPC 是 Amazon EC2 的聯網 layer。如果您是 Amazon EC2 的新手，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [什麼是 Amazon EC2 ?](#) 來取得簡要概觀。

以下是 VPC 的重要概念：

- Virtual private cloud (VPC)：是您 AWS 帳戶專用的虛擬網路。
- 子網路：是您的 VPC 中的 IP 地址範圍。
- 路由表：一組名為路由的規則，用來判斷網路流量的方向。
- 網際網路閘道：您連接至 VPC 的閘道，可在 VPC 中的資源與網際網路之間進行通訊。
- VPC 端點：可讓您將 VPC 私下連線至支援的 AWS 服務以及具有 PrivateLink 功能的 VPC 端點服務，而不需要網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，即可與服務中的資源通訊。VPC 與另一個服務之間的流量都會保持在 Amazon 網路的範圍內。如需詳細資訊，請參閱 [VPC 端點](#) 和 [VPC 端點服務 \(AWS PrivateLink\)](#) (p. 265)。

## 存取 Amazon VPC

您可以使用下列任一界面來建立、存取和管理您的 VPC：

- AWS 管理主控台：提供 Web 界面，您可使用此界面來存取 VPC。
- AWS 命令列界面 (AWS CLI) — 提供許多 AWS 服務 (包括 Amazon VPC) 的命令，且支援在 Windows、Mac 和 Linux 上使用。如需詳細資訊，請參閱 [AWS Command Line Interface](#)。
- AWS SDK — 提供語言特定 API，並處理許多連線詳細資訊，例如計算簽章、處理請求重試和錯誤處理。如需詳細資訊，請參閱 [AWS SDK](#)。
- 查詢 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 Reference](#)。

## Amazon VPC 的定價

使用 VPC；無需負擔額外費用。下列 VPC 元件需支付費用：Site-to-Site VPN 連線、PrivateLink、流量鏡射，和 NAT 閘道。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。

## Amazon VPC 配額

您可以佈建的 Amazon VPC 元件數具有配額。您可以對一部分配額請求提高限制。如需詳細資訊，請參閱「[Amazon VPC 配額](#) (p. 320)」。



## PCI DSS 合規

Amazon VPC 支援處理、儲存、傳輸商家或服務供應商的信用卡資料，並且已驗證符合支付卡產業 (PCI) 資料安全標準 (DSS)。如需 PCI DSS 的詳細資訊，包括如何索取 &AWS; PCI 合規套裝服務的複本，請參閱 [PCI DSS 第 1 級](#)。

# Amazon VPC 的運作方式

Amazon Virtual Private Cloud (Amazon VPC) 可讓您將 AWS 資源啟動至已定義的虛擬網路。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。

Amazon VPC 是 Amazon EC2 的聯網 layer。如果您是 Amazon EC2 的新手，請參閱 [Linux 執行個體的 Amazon EC2 使用者指南](#) 中的 [什麼是 Amazon EC2？](#) 來取得簡要概觀。

## 內容

- [VPC 和子網路 \(p. 3\)](#)
- [預設和非預設 VPC \(p. 3\)](#)
- [路由表 \(p. 4\)](#)
- [存取網際網路 \(p. 4\)](#)
- [存取公司或家用網路 \(p. 6\)](#)
- [透過 AWS PrivateLink 存取服務 \(p. 7\)](#)
- [連接 VPC 和網路 \(p. 8\)](#)
- [AWS 私有全球網路注意事項 \(p. 8\)](#)
- [支援的平台 \(p. 9\)](#)
- [Amazon VPC 資源 \(p. 9\)](#)

## VPC 和子網路

虛擬私有雲端 (VPC) 是您 AWS 帳戶專用的虛擬網路。此虛擬網路在邏輯上與 AWS 雲端中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)。您可以為 VPC 指定 IP 地址範圍、新增子網路、與安全群組建立關聯，以及設定路由表。

子網路是您的 VPC 中的 IP 地址範圍。您可以在指定的子網路中啟動 AWS 資源。針對必須連線至網際網路的資源使用公有子網路，並針對不會連線至網際網路的資源使用私有子網路。

若要保護各子網路的 AWS 資源，您可使用多個安全 layer，包括安全群組及網路存取控制清單 (ACL)。

您可以選擇將 IPv6 CIDR 區塊與 VPC 建立關聯，並指派 IPv6 地址給 VPC 中的執行個體。

## 其他資訊

- [VPC 和子網路基本概念 \(p. 73\)](#)
- [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)
- [您 VPC 中的 IP 定址 \(p. 102\)](#)

## 預設和非預設 VPC

如果您的帳戶是在 2013 年 12 月 4 日之後建立，則會隨附預設 VPC，該 VPC 在每個可用區域中都具有預設子網路。預設 VPC 具有 EC2-VPC 提供的進階功能優勢，並已準備就緒供您使用。如果您有預設 VPC，且在啟動執行個體時未指定子網路，則執行個體會於您的預設 VPC 啟動。您無須任何 Amazon VPC 的知識，就可以在預設 VPC 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 中建立的子網路，以及您在預設 VPC 中建立的額外子網路，稱為非預設子網路。

## 其他資訊

- [預設 VPC 和預設子網路 \(p. 95\)](#)

- [Amazon VPC 入門 \(p. 10\)](#)

## 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路與特定路由表建立關聯。否則，子網路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 位址範圍 (目的地)，以及傳送流量 (目標) 的閘道、網路界面或連線。

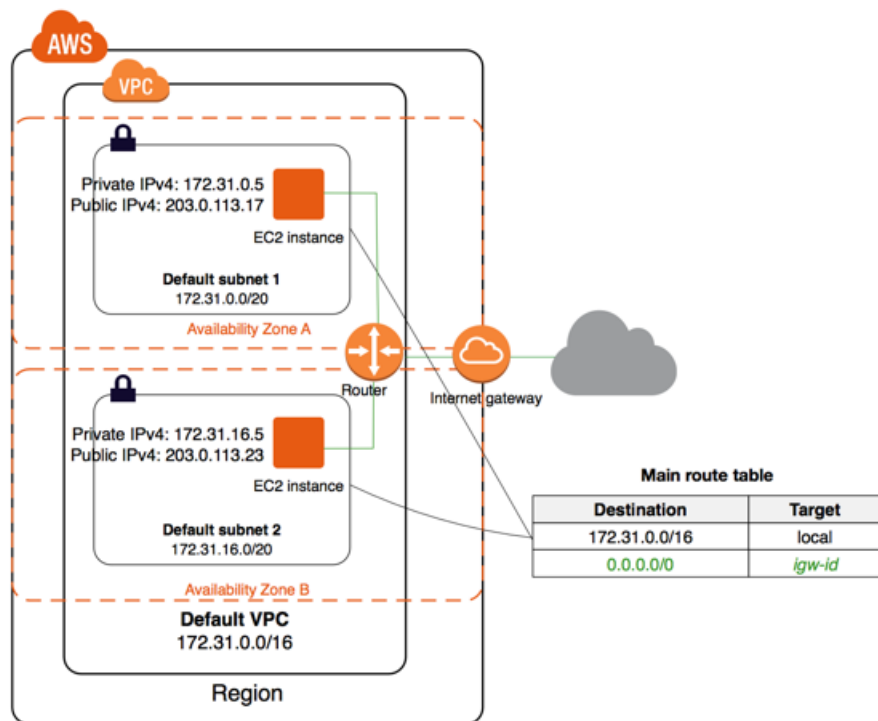
其他資訊

- [路由表 \(p. 184\)](#)

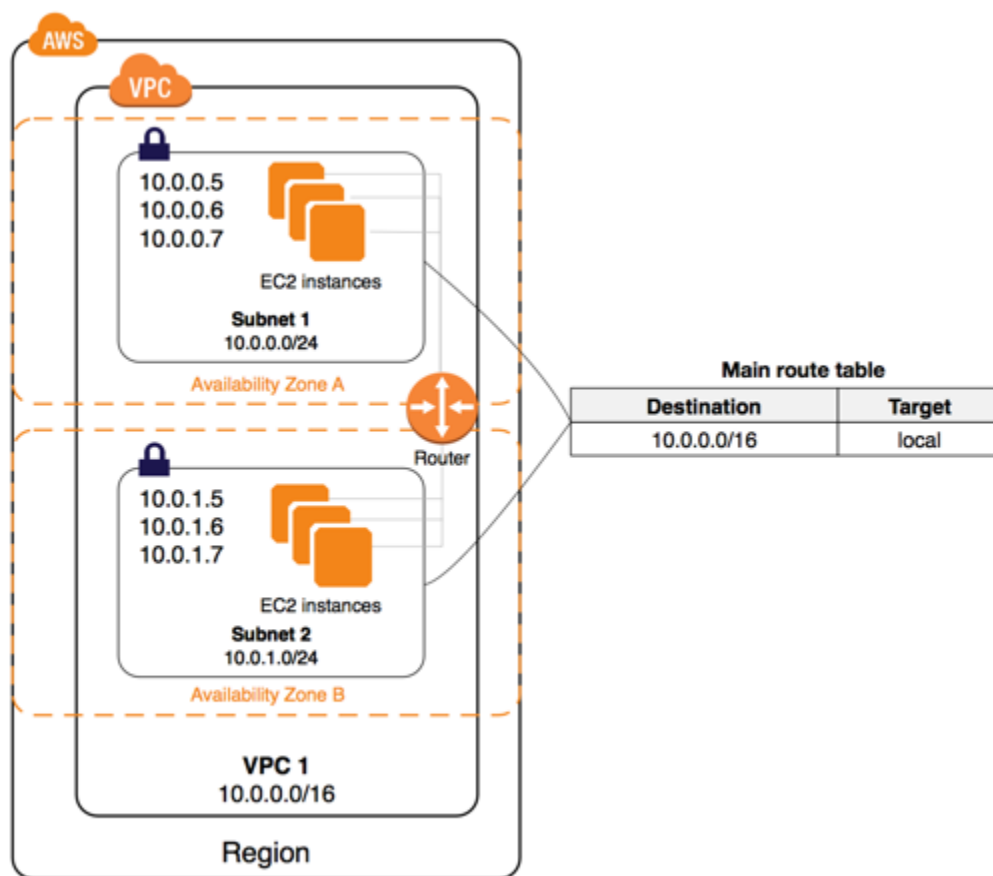
## 存取網際網路

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。

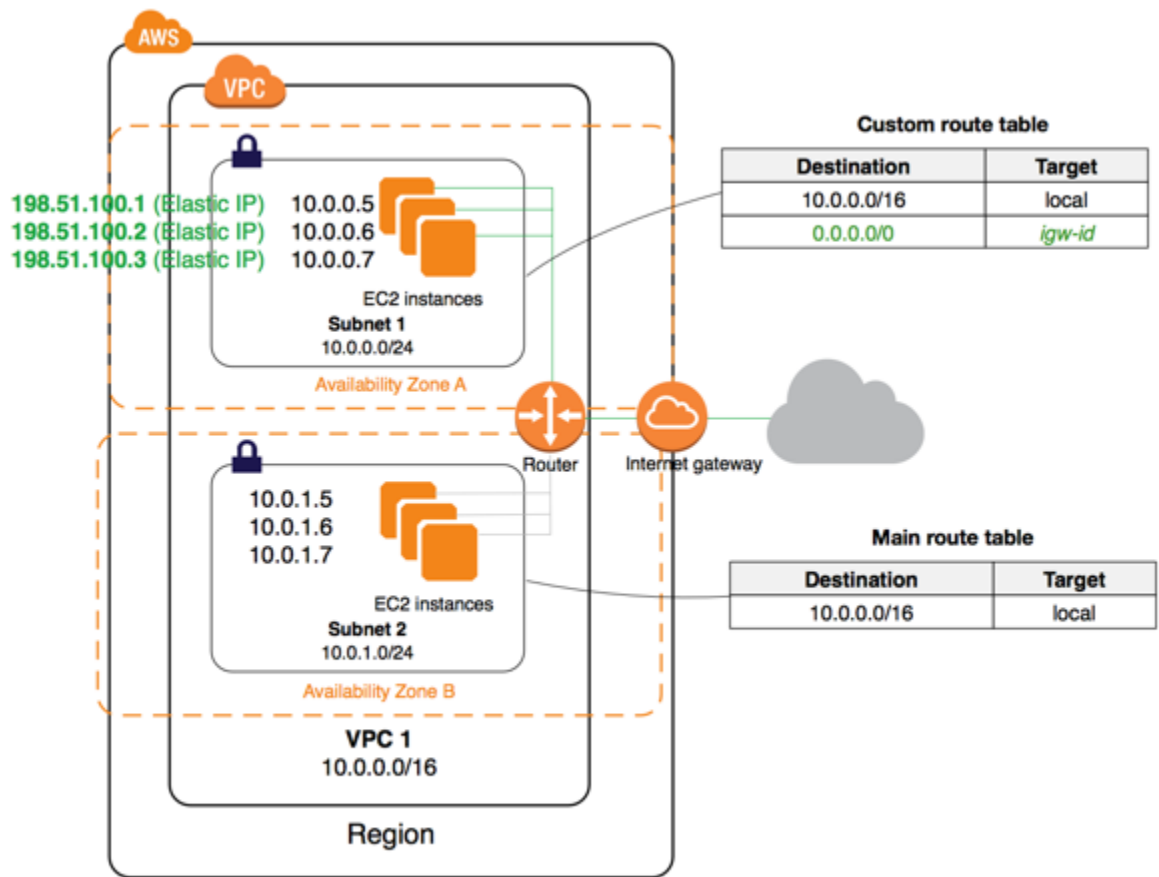
您的預設 VPC 包含網際網路閘道，且每個預設子網路皆為公有子網路。您在預設子網路中啟動的每個執行個體都具有私有 IPv4 地址和公有 IPv4 地址。這些執行個體可以透過網際網路閘道與網際網路通訊。網際網路閘道可讓您的執行個體透過 Amazon EC2 網路邊緣連線至網際網路。



根據預設，您在非預設子網路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，或修改子網路的公有 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，來為在非預設子網路上啟動的執行個體啟用網路存取。



或者，您也可以為 IPv4 流量使用網路位址轉譯 (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。NAT 裝置具有彈性 IP 地址，並透過網際網路閘道連線至網際網路。您可以透過 NAT 裝置將私有子網路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 位址指派給執行個體，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。

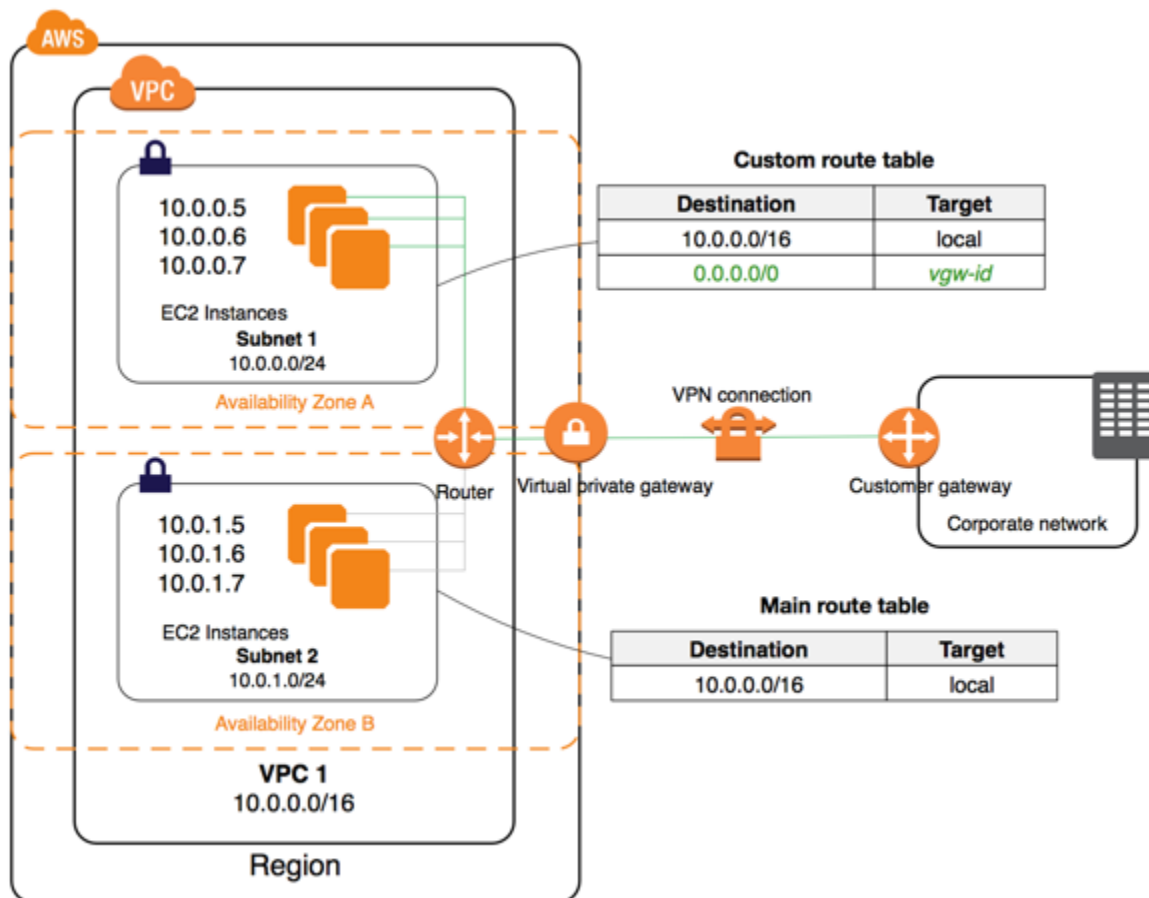
#### 其他資訊

- [網際網路閘道 \(p. 212\)](#)
- [輸出限定網際網路閘道 \(p. 218\)](#)
- [NAT \(p. 226\)](#)

## 存取公司或家用網路

您可以選擇使用 IPsec AWS Site-to-Site VPN 連接，將 VPC 連線至您自己的企業資料中心，讓 AWS 雲端成為資料中心的延伸。

Site-to-Site VPN 連線是由 AWS 端虛擬私有閘道或交通閘道之間的兩個 VPN 通道，以及位於資料中心的客戶閘道裝置之間的兩個 VPN 通道組成。客戶閘道裝置是在您這端的 Site-to-Site VPN 連線中設定的實體裝置或軟體裝置。



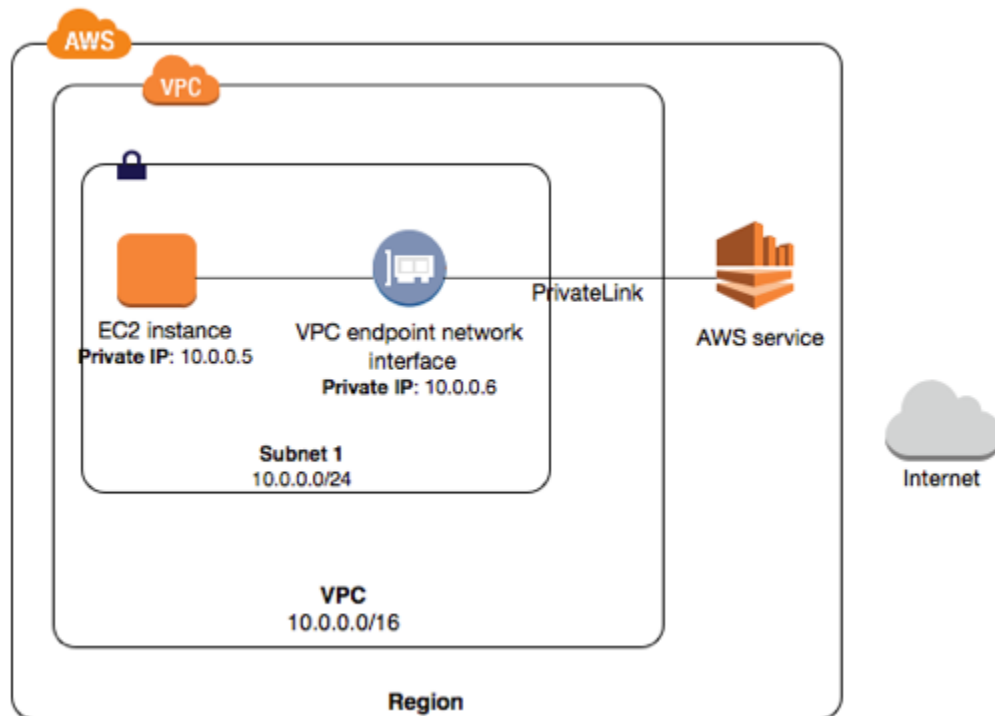
#### 其他資訊

- [AWS Site-to-Site VPN 使用者指南](#)
- [傳輸閘道](#)

## 透過 AWS PrivateLink 存取服務

AWS PrivateLink 是一項具有高可用性和可擴展性的技術，讓您能夠將您的 VPC 私下連線到支援的 AWS 服務、由其他 AWS 帳戶託管的服務 (VPC 端點服務)，以及支援的 AWS Marketplace 合作夥伴服務。您不需要網際網路閘道、NAT 裝置、公有 IP 地址、AWS Direct Connect 連線或 AWS Site-to-Site VPN 連接來與服務通訊。您 VPC 與服務之間的流量都會保持在 Amazon 網路的範圍內。

若要用 AWS PrivateLink，您需要在 VPC 中為服務建立介面 VPC 端點。這會在您的子網路中建立包含私有 IP 地址的彈性網路介面，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 (端點服務)，並讓其他 AWS 客戶能夠存取您的服務。

其他資訊

- [VPC 端點](#) (p. 266)
- [VPC 端點服務 \(AWS PrivateLink\)](#) (p. 294)

## 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。傳輸閘道做為區域虛擬路由器，適用於在其附件之間流動的流量，其中可能包括 VPC、VPN 連線、AWS Direct Connect 閘道和傳輸閘道對等連線。

其他資訊

- [VPC 對等指南](#)
- [傳輸閘道](#)

## AWS 私有全球網路注意事項

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

- 在可用區域中或在所有區域之可用區域間的流量，透過 AWS 私有全球網路進行路由。
- 區域之間的流量一律透過 AWS 私有全球網路進行路由，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。我們會測量連接 AWS 區域之全球骨幹的封包遺失率 (PLR)。我們骨幹網路的運作目標是每小時 PLR 的 p99，也就是少於 0.0001%。

## 支援的平台

Amazon EC2 的原始版本支援與其他客戶共享的單一平面網路，此網路稱為 EC2-Classic 平台。早期的 AWS 帳戶仍支援此平台，並且可在 EC2-Classic 或 VPC 中啟動執行個體。在 2013 年 12 月 4 日之後建立的帳戶則僅支援 EC2-VPC。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [EC2-Classic](#)。

## Amazon VPC 資源

下表列出在使用 Amazon VPC 時可能有用的其他資源。

資源	描述
<a href="#">Amazon Virtual Private Cloud 連線選項</a>	提供網路連線的選項概觀。
<a href="#">VPC 對等指南</a>	說明 VPC 互連案例和支援的互連組態。
<a href="#">流量鏡射</a>	說明流量鏡像目標、篩選條件和工作階段，並協助管理員進行設定。
<a href="#">傳輸閘道</a>	說明傳輸閘道並協助網路管理員進行設定。
<a href="#">傳輸閘道網路管理工具指南</a>	說明傳輸閘道網路管理工具，並協助您設定和監控全域網路。
<a href="#">AWS Direct Connect 使用者指南</a>	說明如何使用 AWS Direct Connect 建立遠端網路到您 VPC 的專用私有連線。
<a href="#">AWS Client VPN 管理員指南</a>	說明如何建立和設定 用戶端 VPN 端點，讓遠端使用者能夠存取 VPC 的資源。
<a href="#">Amazon VPC forum</a>	社群形式的論壇，供予討論 Amazon VPC 相關技術問題。
<a href="#">資源中心入門</a>	可協助您在 AWS 上開始建置的資訊。
<a href="#">AWS Support 中心</a>	AWS Support 的首頁
<a href="#">聯絡我們</a>	詢問有關 AWS 帳單、帳戶、活動等問題的聯絡中心。



# Amazon VPC 入門

若要開始使用 Amazon VPC，您可以建立非預設 VPC。下列步驟說明如何使用 Amazon VPC 精靈來建立具有公用子網路的非預設 VPC，其是可透過網際網路閘道存取網際網路的子網路。之後，您可以在子網路中啟動執行個體，然後與其連線。

或者，若要在現有預設 VPC 中啟動執行個體，請參閱[在預設 VPC 中啟動 EC2 執行個體](#)。

您必須先註冊 Amazon Web Services (AWS)，才能開始使用 Amazon VPC。註冊時，您的 AWS 帳戶會自動註冊所有 AWS 中的服務，包括 Amazon VPC。如果您尚未建立 AWS 帳戶，請前往 <https://aws.amazon.com/>，然後選擇 Create a Free Account (建立免費帳戶)。

如果您想要為 VPC 使用本機區域，請建立 VPC，然後在本機區域中建立子網路。如需更多詳細資訊，請參閱 [the section called “建立 VPC” \(p. 82\)](#) 及 [the section called “在您的 VPC 中建立子網路” \(p. 83\)](#)。

## 主題

- [概觀 \(p. 10\)](#)
- [步驟 1：建立 VPC \(p. 10\)](#)
- [步驟 2：在您的 VPC 中啟動執行個體 \(p. 11\)](#)
- [步驟 3：將彈性 IP 地址指派給執行個體 \(p. 12\)](#)
- [步驟 4：清理 \(p. 13\)](#)
- [後續步驟 \(p. 13\)](#)
- [適用於 Amazon VPC 的 IPv6 入門 \(p. 13\)](#)
- [Amazon VPC 主控台精靈組態 \(p. 17\)](#)

## 概觀

若要完成本練習，請執行下列作業：

- 建立具有單一公有子網路的非預設 VPC。
- 在子網路中啟動 Amazon EC2 執行個體。
- 將彈性 IP 地址與您的執行個體建立關聯。這允許您的執行個體存取網際網路。

如需授與 IAM 使用者使用 Amazon VPC 之許可的詳細資訊，請參閱[Amazon VPC 的 Identity and Access Management \(p. 123\)](#)和[Amazon VPC 政策範例 \(p. 129\)](#)。

## 步驟 1：建立 VPC

在此步驟中，您將在 Amazon VPC 主控台中使用 Amazon VPC 精靈，以建立 VPC。精靈會為您執行下列步驟：

- 建立包含 /16 IPv4 CIDR 區塊的 VPC (包含 65,536 個私有 IP 地址的網路)。
- 將網際網路閘道連接至 VPC。
- 在 VPC 中建立大小 /24 IPv4 子網路 (256 個私有 IP 地址的範圍)。
- 建立自訂路由表，並建立它與您子網路的關聯，以便流量可在子網路和網際網路閘道間往來。

## 使用 Amazon VPC 精靈建立 VPC

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 記下導覽列右上角您要建立 VPC 的 **AWS 區域**。確保此練習的剩餘部分都繼續在同一區域中工作，因為您不能從其他區域啟動您 VPC 中的執行個體。
3. 在導覽窗格中，選擇 VPC dashboard (VPC 儀表板)。從儀表板選擇 Launch VPC Wizard (啟動 VPC 精靈)。

### Note

請不要選擇導覽窗格中的 Your VPCs (VPC)；您無法使用該頁面上的 Create VPC (建立 VPC) 按鈕來存取 VPC 精靈。

4. 選擇 VPC with a Single Public Subnet (具有單一公有子網路的 VPC)，然後選擇 Select (選取)。
5. 在組態頁面上，於 VPC name (VPC 名稱) 欄位中輸入 VPC 名稱 (例如 my-vpc)，然後在 Subnet name (子網路名稱) 欄位中輸入子網路名稱。這可協助您在建立 VPC 和子網路之後，於 Amazon VPC 主控台中識別 VPC 和子網路。在本練習中，保留此頁面上的其餘組態設定，然後選擇 Create VPC (建立 VPC)。
6. 狀態視窗會顯示進行中的工作。工作完成時，請選擇 OK (確定) 關閉狀態視窗。
7. Your VPCs (VPC) 頁面會顯示預設 VPC 以及您剛建立的 VPC。您建立的 VPC 是非預設 VPC，因此 Default VPC (預設 VPC) 欄會顯示 No (否)。

## 檢視您的 VPC 相關資訊

在您建立 VPC 之後，即可檢視子網路、網際網路閘道和路由表的相關資訊。您建立的 VPC 有兩份路由表：主路由表是所有 VPC 預設有的項目，自訂路由表則由精靈建立。自訂路由表與您的子網路相關聯，這表示該表格中的路由可決定子網路流量的流向。如果您在 VPC 中新增新的子網路，它預設會使用主路由表。

### 檢視您的 VPC 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 Your VPCs (您的 VPC)。請記下您已建立之 VPC 的名稱和 ID (請查看 Name (名稱) 和 VPC ID 欄)。您將使用此資訊來識別與 VPC 建立關聯的元件。
3. 在導覽窗格中，選擇 Subnets (子網路)。主控台會顯示您建立 VPC 時所建立的子網路。您可以在 Name (名稱) 欄位中依子網路的名稱來識別子網路，也可以使用您在上一步中取得的 VPC 資訊，並查看 VPC 欄位。
4. 在導覽窗格中，選擇 Internet Gateways (網際網路閘道)。您可以查看 VPC 欄找出連接至 VPC 的網際網路閘道，該欄會顯示 VPC 的 ID 和名稱 (若適用)。
5. 在導覽窗格中，選擇 Route Tables (路由表)。有兩個路由表與 VPC 相關聯。選取自訂路由表 (Main (主要) 欄顯示 No (否))，然後選擇 Routes (路由) 標籤以顯示詳細資訊窗格中的路由資訊：
  - 資料表中的第一列就是本機路由，可讓 VPC 內的執行個體通訊。根據預設，此路由存在於每個路由表中，而且您無法予以移除。
  - 第二列顯示 Amazon VPC 精靈所新增的路由，以讓目標為在網際網路 (0.0.0.0/0) 的流量可從子網路流向網際網路閘道。
6. 選取主路由表。主路由表有本機路由，但沒有其他路由。

## 步驟 2：在您的 VPC 中啟動執行個體

當您在 VPC 中啟動 EC2 執行個體時，您必須指定執行個體啟動所在的子網路。在本例中，您會在您所建立之 VPC 的公有子網路中啟動執行個體。您將在 Amazon EC2 主控台中使用 Amazon EC2 啟動精靈來啟動您的執行個體。

### 在您的 VPC 中啟動 EC2 執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽列的右上角，確定選取您 VPC 建立所在的相同區域。
3. 在儀表中，選擇 Launch Instance (啟動執行個體)。
4. 在精靈的第一頁上，選擇您要使用的 AMI。在本練習中，請選擇 Amazon Linux AMI 或 Windows AMI。
5. 在 Choose an Instance Type (選擇執行個體類型) 頁面上，您可以選取要啟動之執行個體的硬體組態和大小。根據預設，精靈會根據您選取的 AMI 來選取第一個可用的執行個體類型。您可以保留預設選項，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
6. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 清單選取您建立的 VPC，然後從 Subnet (子網路) 清單選取子網路。保留其餘預設設定，然後繼續前往精靈的後續頁面，一直到 Add Tags (新增標籤) 頁面為止。
7. 在 Add Tags (新增標籤) 頁面上，您可以使用 Name 標籤建立執行個體的標籤，例如 Name=MyWebServer。這可協助您在啟動執行個體之後，於 Amazon EC2 主控台中識別您的執行個體。當完成時，請選擇 Next: Configure Security Group (下一步：設定安全群組)。
8. 在 Configure Security Group (設定安全群組) 頁面上，精靈會自動定義 launch-wizard-x 安全群組，允許您連線至您的執行個體。選擇 Review and Launch (檢閱和啟動)。

#### Important

精靈會建立安全性群組規則，這可讓所有 IP 位址 (0.0.0.0/0) 使用 SSH 或 RDP 存取您的執行個體。此操作用於短暫練習沒有問題，但用在生產環境則不安全。在生產環境中，您應只授權特定 IP 地址或特定範圍的地址存取您的執行個體。

9. 在 Review Instance Launch (檢閱執行個體啟動) 頁面，選擇 Launch (啟動)。
10. 在 Select an existing key pair or create a new key pair (選取現有的金鑰對或建立新的金鑰對) 對話方塊中，您可以選擇現有的金鑰對或建立新的金鑰對。如果您建立新的金鑰對，請確定您下載檔案並存放在安全的位置。啟動執行個體之後，您需要有私有金鑰的內容才能連線至執行個體。

若要啟動您的執行個體，請選取確認核取方塊，然後選擇 Launch Instances (啟動執行個體)。

11. 在確認頁面上，選擇 View Instances (檢視執行個體)，以在 Instances (執行個體) 頁面上檢視執行個體。選取執行個體，然後在 Description (描述) 標籤中檢視其詳細資訊。Private IPs (私有 IP) 欄位會顯示從子網路 IP 地址範圍指派給您執行個體的私有 IP 地址。

如需 Amazon EC2 啟動精靈中可用選項的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [啟動執行個體](#)。

## 步驟 3：將彈性 IP 地址指派給執行個體

在上一步中，您已於公有子網路啟動執行個體，而公有子網路是具有網際網路閘道路由的子網路。不過，子網路中的執行個體也需要公有 IPv4 地址才能與網際網路通訊。根據預設，公有 IPv4 地址不會指派給非預設 VPC 中的執行個體。在此步驟中，您會將彈性 IP 地址配置給您的帳戶，然後建立地址與您執行個體的關聯。

### 配置並指派彈性 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 new address (配置新地址)，然後選擇 Allocate (配置)。
4. 從清單選取彈性 IP 地址，並選擇 Actions (動作)，然後選擇 Associate Address (與地址建立關聯)。
5. 針對 Resource type (資源類型)，確定已選取 Instance (執行個體)。從 Instance (執行個體) 清單選擇執行個體。完成後，請選擇 Associate (關聯)。

現在可以從網際網路存取您的執行個體。您可以從家用網路，使用 SSH 或遠端桌面透過彈性 IP 地址連線至執行個體。如需如何連線至 Linux 執行個體的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的[連線至 Linux 執行個體](#)。如需如何連線至 Windows 執行個體的詳細資訊，請參閱 Windows 執行個體的 Amazon EC2 使用者指南中的[連線至 Windows 執行個體](#)。

## 步驟 4：清理

您可以選擇在 VPC 中繼續使用執行個體；如果您不需要執行個體，可以予以終止，並釋出其彈性 IP 地址，避免它們產生費用。您也可以刪除 VPC。請注意，不會向您收取 VPC 以及本練習中所建立 VPC 元件 (例如子網路和路由表) 的費用。

您必須先終止 VPC 中執行的所有執行個體，才能刪除 VPC。然後，您可以使用 VPC 主控台刪除 VPC 及其元件。

若要終止執行個體，請釋出彈性 IP 地址，然後刪除 VPC。

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)。
3. 選取執行個體，選擇 Actions (動作) 和 Instance State (執行個體狀態)，然後選取 Terminate (終止)。
4. 在此對話方塊中，展開 Release attached Elastic IPs (釋出已連接的彈性 IP) 區段，然後選取彈性 IP 地址旁的核取方塊。選擇 Yes, Terminate (是，終止)。
5. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
6. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
7. 選取 VPC，並選擇 Actions (動作)，然後選擇 Delete VPC (刪除 VPC)。
8. 出現確認提示時，請選擇 Delete VPC (刪除 VPC)。

## 後續步驟

建立非預設 VPC 之後，您可能想要執行下列操作：

- 將更多子網路新增至 VPC。如需更多詳細資訊，請參閱 [在您的 VPC 中建立子網路](#) (p. 83)。
- 為您的 VPC 和子網路啟用 IPv6 支援。如需更多詳細資訊，請參閱 [建立 IPv6 CIDR 區塊與 VPC 的關聯](#) (p. 84) 及 [建立 IPv6 CIDR 區塊與子網路的關聯](#) (p. 85)。
- 啟用私有子網路中的執行個體以存取網際網路。如需更多詳細資訊，請參閱 [NAT](#) (p. 226)。

## 適用於 Amazon VPC 的 IPv6 入門

下列步驟說明如何建立支援 IPv6 定址的非預設 VPC。

若要完成本練習，請執行下列作業：

- 建立具有 IPv6 CIDR 區塊和單一公有子網路的非預設 VPC。子網路可讓您根據安全性和操作需求分組執行個體。公有子網路是可透過網際網路閘道存取網際網路的子網路。
- 為您的執行個體建立只允許特定連接埠流量的安全群組。
- 在啟動期間，在您的子網路中啟動 Amazon EC2 執行個體，並建立 IPv6 地址與您執行個體的關聯。IPv6 地址為全域唯一，可讓您的執行個體與網際網路通訊。
- 您可以請求適用於 VPC 的 IPv6 CIDR 區塊。選取此選項時，您可以設定網路邊界群組，這是我們公告 IPv6 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。

如需 IPv4 和 IPv6 定址的詳細資訊，請參閱 [VPC 的 IP 定址](#)。

如果您想要為 VPC 使用本機區域，請建立 VPC，然後在本機區域中建立子網路。如需更多詳細資訊，請參閱 [the section called “建立 VPC” \(p. 82\)](#) 及 [the section called “在您的 VPC 中建立子網路” \(p. 83\)](#)。

#### 任務

- [步驟 1：建立 VPC \(p. 14\)](#)
- [步驟 2：建立安全群組 \(p. 16\)](#)
- [步驟 3：啟動執行個體 \(p. 16\)](#)

## 步驟 1：建立 VPC

在此步驟中，您要在 Amazon VPC 主控台中使用 Amazon VPC 精靈建立 VPC。根據預設，精靈會為您執行下列步驟：

- 建立包含 /16 IPv4 CIDR 區塊的 VPC，並建立 /56 IPv6 CIDR 區塊與 VPC 的關聯。如需詳細資訊，請參閱 [您的 VPC](#)。IPv6 CIDR 區塊的大小是固定的 (/56)，而且 IPv6 地址的範圍會自動從 IPv6 地址的 Amazon 集區配置 (您無法自行選取範圍)。
- 將網際網路閘道連接至 VPC。如需網際網路閘道的詳細資訊，請參閱 [網際網路閘道](#)。
- 在 VPC 中建立包含 /24 IPv4 CIDR 區塊和 /64 IPv6 CIDR 區塊的子網路。IPv6 CIDR 區塊的大小是固定的 (/64)。
- 建立自訂路由表，並建立它與您子網路的關聯，以便流量可在子網路和網際網路閘道間往來。如需路由表的詳細資訊，請參閱 [路由表](#)。
- 將 IPv6 Amazon 提供的 CIDR 區塊與網路邊界群組建立關聯。如需更多詳細資訊，請參閱 [the section called “將您的 VPC 資源擴展到本機區域” \(p. 92\)](#)。

#### Note

此練習涵蓋 VPC 精靈的第一個案例。如需其他案例的詳細資訊，請參閱 [Amazon VPC 案例](#)。

若要在預設可用區域中建立 VPC

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 記下導覽列右上角您要建立 VPC 的區域。確保此練習的剩餘部分都繼續在同一區域中工作，因為您不能從其他區域啟動您 VPC 中的執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [區域和可用區域](#)。
3. 在導覽窗格中，選擇 VPC dashboard (VPC 儀表板)，然後選擇 Launch VPC Wizard (啟動 VPC 精靈)。

#### Note

請不要選擇導覽窗格中的 Your VPCs (VPC)；您無法使用該頁面上的 Create VPC (建立 VPC) 按鈕來存取 VPC 精靈。

4. 針對您要實作的組態選擇選項，例如 VPC with a Single Public Subnet (具有單一公用子網路的 VPC)，然後選擇 Select (選取)。
5. 在 configuration (組態) 頁面上，針對 VPC name (VPC 名稱) 輸入您的 VPC 名稱 (例如 my-vpc)，然後在 Subnet name (子網路名稱) 中輸入您的子網路名稱。這可協助您在建立 VPC 和子網路之後，於 Amazon VPC 主控台中識別 VPC 和子網路。
6. (對於 IPv4 CIDR block (IPv4 CIDR 區塊)，可保留預設設定 (10.0.0.0/16)，或指定您自己的設定。如需詳細資訊，請參閱 [調整 VPC 大小](#)。

針對 IPv6 CIDR block (IPv6 CIDR 區塊)，選擇 Amazon-provided IPv6 CIDR block (Amazon 提供的 IPv6 CIDR 區塊)。

7. 針對 Public subnet's IPv4 CIDR (公有子網路的 IPv4 CIDR)，保留預設設定或指定您自己的設定。針對 Public subnet's IPv6 CIDR (公有子網路的 IPv6 CIDR)，選擇 Specify a custom IPv6 CIDR (指定自訂 IPv6 CIDR)。您可在 IPv6 子網路保留預設的十六進位對值 (00)。



8. 在頁面中保留其他預設的組態，然後選擇 **Create VPC** (建立 VPC)。
9. 狀態視窗會顯示進行中的工作。工作完成時，請選擇 **OK** (確定) 關閉狀態視窗。
10. **Your VPCs** (VPC) 頁面會顯示預設 VPC 以及您剛建立的 VPC。

若要在本機區域中建立 VPC

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 記下導覽列右上角您要建立 VPC 的區域。確保此練習的剩餘部分都繼續在同一區域中工作，因為您不能從其他區域啟動您 VPC 中的執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [區域和可用區域](#)。
3. 在導覽窗格中，選擇 **VPC dashboard** (VPC 儀表板)，然後選擇 **Launch VPC Wizard** (啟動 VPC 精靈)。

#### Note

請不要選擇導覽窗格中的 **Your VPCs** (VPC)；您無法使用該頁面上的 **Create VPC** (建立 VPC) 按鈕來存取 VPC 精靈。

4. 針對您要實作的組態選擇選項，例如 **VPC with a Single Public Subnet** (具有單一公用子網路的 VPC)，然後選擇 **Select** (選取)。
5. 在 **configuration** (組態) 頁面上，針對 **VPC name** (VPC 名稱) 輸入您的 VPC 名稱 (例如 `my-vpc`)，然後在 **Subnet name** (子網路名稱) 中輸入您的子網路名稱。這可協助您在建立 VPC 和子網路之後，於 Amazon VPC 主控台中識別 VPC 和子網路。
6. (對於 IPv4 CIDR block (IPv4 CIDR 區塊)，指定 CIDR 區塊。如需詳細資訊，請參閱 [調整 VPC 大小](#)。
7. 針對 IPv6 CIDR block (IPv6 CIDR 區塊)，選擇 **Amazon-provided IPv6 CIDR block** (Amazon 提供的 IPv6 CIDR 區塊)。
8. 對於 **Network Border Group** (網路邊界群組)，選擇 AWS 公告 IP 地址的來源群組。
9. 在頁面中保留其他預設的組態，然後選擇 **Create VPC** (建立 VPC)。
10. 狀態視窗會顯示進行中的工作。工作完成時，請選擇 **OK** (確定) 關閉狀態視窗。
11. **Your VPCs** (VPC) 頁面會顯示預設 VPC 以及您剛建立的 VPC。

## 檢視您的 VPC 資訊

在您建立 VPC 之後，即可檢視子網路、網際網路閘道和路由表的相關資訊。您建立的 VPC 有兩份路由表：主路由表是所有 VPC 預設有的項目，自訂路由表則由精靈建立。自訂路由表與您的子網路相關聯，這表示該表格中的路由可決定子網路流量的流向。如果您在 VPC 中新增新的子網路，它預設會使用主路由表。

檢視您的 VPC 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 **Your VPCs** (您的 VPC)。請記下您已建立之 VPC 的名稱和 ID (請查看 **Name** (名稱) 和 **VPC ID** 欄)。您會使用此資訊來識別與 VPC 相關聯的元件。  
  
當您使用本機區域時，**IPv6** (網路邊界群組) 項目會指出 VPC 網路邊界群組 (例如，`us-west-2-lax-1`)。
3. 在導覽窗格中，選擇 **Subnets** (子網路)。主控台會顯示您建立 VPC 時所建立的子網路。您可以在 **Name** (名稱) 欄位中依子網路的名稱來識別子網路，也可以使用您在上一步中取得的 VPC 資訊，並查看 **VPC** 欄位。
4. 在導覽窗格中，選擇 **Internet Gateways** (網際網路閘道)。您可以查看 **VPC** 欄找出連接至 VPC 的網際網路閘道，該欄會顯示 VPC 的 ID 和名稱 (若適用)。
5. 在導覽窗格中，選擇 **Route Tables** (路由表)。有兩個路由表與 VPC 相關聯。選取自訂路由表 (**Main** (主要) 欄顯示 **No** (否))，然後選擇 **Routes** (路由) 標籤以顯示詳細資訊窗格中的路由資訊：
  - 資料表中前兩列是本機路由，可讓 VPC 內的執行個體透過 IPv4 和 IPv6 通訊。您無法移除這些路由。

- 下一列顯示 Amazon VPC 精靈所新增的路由，以啟用目標設為 VPC 外部之 IPv4 地址 (0.0.0.0/0) 的流量從子網路流向網際網路閘道。
  - 下一列顯示的路由，以啟用目標設為 VPC 外部之 IPv6 地址 (:::/0) 的流量從子網路流向網際網路閘道。
6. 選取主路由表。主路由表有本機路由，但沒有其他路由。

## 步驟 2：建立安全群組

安全群組可做為一種虛擬防火牆，控制相關聯之執行個體的流量。若要使用安全群組，請新增傳入規則來控制傳入至執行個體的流量，以及新增傳出規則來控制從執行個體傳出的流量。若要建立安全群組與執行個體的關聯，請在啟動執行個體時指定安全群組。

您的 VPC 隨附預設安全群組。在啟動期間，任何未與其他安全群組建立關聯的執行個體，都與預設安全群組相關聯。在本練習中，您要建立新的安全群組 WebServerSG，並在 VPC 中啟動執行個體時指定此安全群組。

### 建立您的 WebServerSG 安全群組

您可以使用 Amazon VPC 主控台建立您的安全群組。

建立 WebServerSG 安全群組並新增規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
  2. 在導覽窗格中，選擇 Security Groups (安全群組)、Create Security Group (建立安全群組)。
  3. 針對 Group name (群組名稱)，輸入 WebServerSG 做為安全群組名稱，並提供描述。您可以選擇性地使用 Name tag (名稱標籤) 欄位來建立索引鍵為 Name 並具有您指定值之安全群組的標籤。
  4. 從 VPC 選單選取您 VPC 的 ID，然後選擇 Yes, Create (是，建立)。
  5. 選取您剛建立的 WebServerSG 安全群組 (您可以在 Group Name (群組名稱) 欄中檢視其名稱)。
  6. 在 Inbound Rules (傳入規則) 標籤上，選擇 Edit (編輯)，然後新增傳入流量的規則，如下所示：
    - a. 針對 Type (類型)，選擇 HTTP，然後在 Source (來源) 欄位中輸入 ::/0。
    - b. 選擇 Add another rule (新增其他規則)，針對 Type (類型)，選擇 HTTPS，然後在 Source (來源) 欄位中輸入 ::/0。
    - c. 選擇 Add another rule (新增其他規則)。如果您要啟動 Linux 執行個體，請針對 Type (類型) 選取 SSH；或者，如果您要啟動 Windows 執行個體，則請選擇 RDP。在 Source (來源) 欄位中，輸入您網路的公有 IPv6 地址範圍。如果您不知道此地址類型，則可以針對此練習使用 ::/0。
- Important**
- 如果您使用 ::/0，則可讓所有 IPv6 地址使用 SSH 或 RDP 存取您的執行個體。此操作用於短暫練習沒有問題，但用在生產環境則不安全。在生產環境中，建議您只授權特定 IP 地址或特定範圍的地址存取您的執行個體。
- d. 選擇 Save (儲存)。

## 步驟 3：啟動執行個體

當您在 VPC 中啟動 EC2 執行個體時，您必須指定執行個體啟動所在的子網路。在本例中，您會在您所建立之 VPC 的公有子網路中啟動執行個體。在 Amazon EC2 主控台中使用 Amazon EC2 啟動精靈來啟動您的執行個體。

為確保可從網際網路存取您的執行個體，請在啟動期間將子網路範圍中的 IPv6 地址指派給執行個體。這可確保您的執行個體能透過 IPv6 與網際網路通訊。

## 在您的 VPC 中啟動 EC2 執行個體

在 VPC 中啟動 EC2 執行個體之前，請將 VPC 的子網路設定為自動指派 IPv6 地址。如需更多詳細資訊，請參閱 [the section called “修改您子網路的公有 IPv6 定址屬性” \(p. 105\)](#)。

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
  2. 在導覽列的右上角，確定選取您 VPC 和安全群組建立所在的相同區域。
  3. 在儀表板中，選擇 Launch Instance (啟動執行個體)。
  4. 在精靈的第一頁上，選擇要使用的 AMI。我們建議您在此練習中選擇 Amazon Linux AMI 或 Windows AMI。
  5. 在 Choose an Instance Type (選擇執行個體類型) 頁面上，您可以選取要啟動之執行個體的硬體組態和大小。根據預設，精靈會根據您選取的 AMI 來選取第一個可用的執行個體類型。您可以保留預設選項，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
  6. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 清單選取您建立的 VPC，然後從 Subnet (子網路) 清單選取子網路。
  7. 針對 Auto-assign IPv6 IP (自動指派 IPv6 IP)，選擇 Enable (啟用)。
  8. 保留其餘預設設定，然後繼續前往精靈的後續頁面，一直到 Add Tags (新增標籤) 頁面為止。
  9. 在 Add Tags (新增標籤) 頁面上，您可以使用 Name 標籤建立執行個體的標籤，例如 Name=MyWebServer。這可協助您在啟動執行個體之後，於 Amazon EC2 主控台中識別您的執行個體。當完成時，請選擇 Next: Configure Security Group (下一步：設定安全群組)。
  10. 在 Configure Security Group (設定安全群組) 頁面上，精靈會自動定義 launch-wizard-x 安全群組，允許您連線至您的執行個體。相反地，選擇 Select an existing security group (選取現有安全群組) 選項，並選取您先前建立的 WebServerSG 群組，然後選擇 Review and Launch (檢閱和啟動)。
  11. 在 Review Instance Launch (檢閱執行個體啟動) 頁面上，檢查執行個體的詳細資訊，然後選擇 Launch (啟動)。
  12. 在 Select an existing key pair or create a new key pair (選取現有金鑰對或建立新的金鑰對) 對話方塊中，您可以選擇現有的金鑰對或建立新的金鑰對。如果您建立新的金鑰對，請確定您下載檔案並存放在安全的位置。啟動執行個體之後，您需要有私有金鑰的內容才能連線至執行個體。
- 若要啟動您的執行個體，請選取確認核取方塊，然後選擇 Launch Instances (啟動執行個體)。
13. 在確認頁面上，選擇 View Instances (檢視執行個體)，以在 Instances (執行個體) 頁面上檢視執行個體。選取執行個體，然後在 Description (描述) 標籤中檢視其詳細資訊。Private IPs (私有 IP) 欄位會顯示從子網路 IPv4 地址範圍中指派給您執行個體的私有 IPv4 地址。IPv6 IPs 欄位會顯示從子網路 IPv6 地址範圍中指派給您執行個體的 IPv6 地址。

如需 Amazon EC2 啟動精靈中可用選項的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [啟動執行個體](#)。

您可以從家用網路，使用 SSH 或遠端桌面以透過 IPv6 地址連線至執行個體。您的本機電腦必須擁有 IPv6 地址，且必須設定以使用 IPv6。如需如何連線至 Linux 執行個體的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [連線至 Linux 執行個體](#)。如需如何連線至 Windows 執行個體的詳細資訊，請參閱 Windows 執行個體的 Amazon EC2 使用者指南 中的 [使用 RDP 連線至 Windows 執行個體](#)。

### Note

如果您也希望能透過網際網路、SSH 或 RDP 上的 IPv4 地址存取您的執行個體，您必須建立彈性 IP 地址 (靜態公有 IPv4 地址) 與您執行個體的關聯，而且您也必須調整您的安全群組規則允許透過 IPv4 存取。如需更多詳細資訊，請參閱 [Amazon VPC 入門 \(p. 10\)](#)。

## Amazon VPC 主控台精靈組態

您可以使用 Amazon VPC 主控台精靈，建立下列其中一個非預設 VPC 組態。



## 主題

- [具有單一公有子網路的 VPC \(p. 18\)](#)
- [具公有和私有子網路 \(NAT\) 的 VPC \(p. 24\)](#)
- [具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC \(p. 37\)](#)
- [僅具有私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC \(p. 50\)](#)

# 具有單一公有子網路的 VPC

此案例的組態，包含一個具有單一公有子網路的虛擬私有雲端 (VPC)，以及用於啟用網際網路通訊的網際網路閘道。如果您需要執行單層且公開的 Web 應用程式 (例如部落格或簡單網站)，建議您使用此組態。

也可以選擇為 IPv6 設定此案例 – 您可以使用 VPC 精靈來建立與 IPv6 CIDR 區塊相關聯的 VPC 和子網路。在公有子網路上啟動的執行個體可接收 IPv6 地址，並使用 IPv6 通訊。如需 IPv4 和 IPv6 定址的詳細資訊，請參閱[您 VPC 中的 IP 定址 \(p. 102\)](#)。

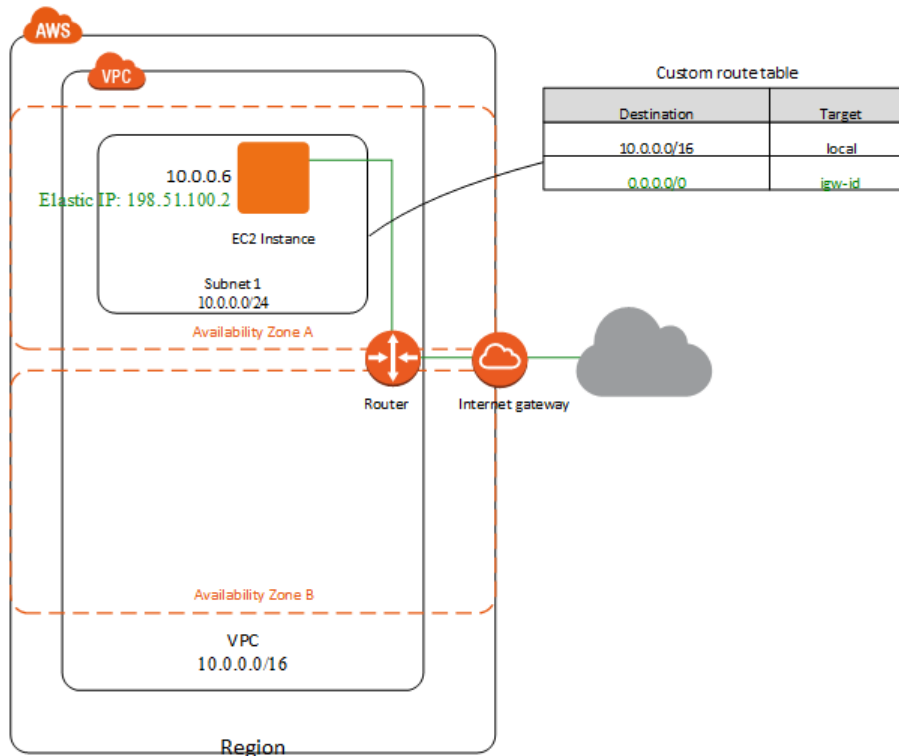
如需管理 EC2 執行個體軟體的相關資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[在您的 Linux 執行個體上管理軟體](#)。

## 內容

- [概觀 \(p. 18\)](#)
- [路由 \(p. 20\)](#)
- [安全性 \(p. 21\)](#)

## 概觀

下圖顯示此案例組態的重要元件。



## Note

如果您已完成 [Amazon VPC 入門 \(p. 10\)](#)，則您已使用過 Amazon VPC 主控台內的 VPC 精靈來實作此案例。

此案例的組態設定包括下列項目：

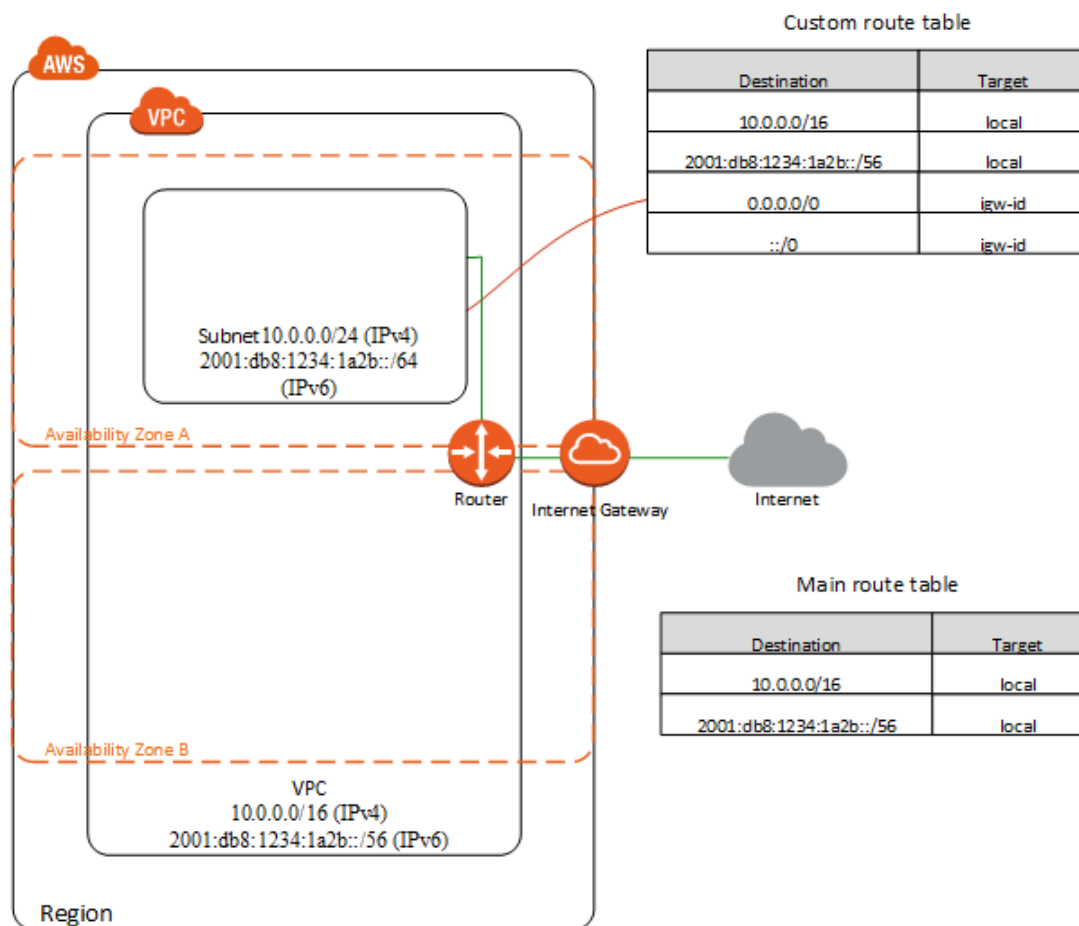
- 具有 /16 大小 IPv4 CIDR 區塊的虛擬私有雲端 (VPC) (範例：10.0.0.0/16)。可提供 65,536 個私有 IPv4 地址。
- 具有 /24 大小 IPv4 CIDR 區塊的子網路 (範例：10.0.0.0/24)。可提供 256 個私有 IPv4 地址。
- 網際網路閘道。這會將 VPC 連線至網際網路和其他 AWS 服務。
- 具有子網路範圍內 (範例：10.0.0.6) 私有 IPv4 地址的執行個體，此執行個體可以與 VPC 中的其他執行個體通訊；以及一個彈性 IPv4 地址 (範例：198.51.100.2)，這是使執行個體能夠連線至網際網路並透過網際網路觸及的公有 IPv4 地址。
- 與子網路相關聯的自訂路由表。此路由表項目可讓子網路中的執行個體使用 IPv4 與 VPC 中其他執行個體進行通訊，並在網際網路上直接通訊。與路由至網際網路閘道之路由表相關聯的子網路，稱為公有子網路。

如需子網路的詳細資訊，請參閱 [VPC 和子網路 \(p. 73\)](#)。如需網際網路閘道的詳細資訊，請參閱 [網際網路閘道 \(p. 212\)](#)。

## IPv6 概觀

您可以選擇為此案例啟用 IPv6。除了以上列出的元件，此組態也包含下列項目：

- 與 VPC 相關聯的 /56 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/56)。Amazon 會自動指派 CIDR；您無法自行選擇範圍。
- 與公有子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇子網路 IPv6 CIDR 區塊的大小。
- 從子網路範圍內指派給執行個體的 IPv6 地址 (範例：2001:db8:1234:1a00::123)。
- 自訂路由表中的路由表項目，可讓 VPC 中的執行個體使用 IPv6 互相通訊，並在網際網路上直接通訊。



## 路由

您的 VPC 具有隱含路由器 (顯示於上面的組態圖表中)。在此案例中，VPC 精靈會建立自訂路由表，將目標為 VPC 外部地址的所有流量路由至網際網路閘道，並將此路由表與子網路建立關聯。

下表顯示在上方組態圖表中用於示範的路由表。第一個項目是 VPC 中本機 IPv4 路由的預設項目；該項目能讓此 VPC 中的執行個體互相通訊。第二個項目會將所有其他 IPv4 子網路流量路由至網際網路閘道 (例如，igw-1a2b3c4d)。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	igw-id

## IPv6 路由

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則您的路由表必須包含 IPv6 流量的個別路由。下表顯示如果您選擇在 VPC 中啟用 IPv6 通訊，此案例會具有的自訂路由表。第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。第四個項目會將所有其他 IPv6 子網路流量路由至網際網路閘道。

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

## 安全性

AWS 提供兩項功能，可用於提升 VPC 中的安全性：安全群組和網路 ACL。安全群組控制執行個體的傳入與傳出流量，網路 ACL 則是控制子網路的傳入與傳出流量。在大部分情況下，安全群組可以符合您的需求；然而，如果您想讓 VPC 多一層安全，也可以使用網路 ACL。如需詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)。

針對此案例，您可以使用安全群組 (而不是網路 ACL)。如果您希望使用網路 ACL，請參閱 [針對具有單一公有子網路之 VPC 建議的網路 ACL 規則 \(p. 22\)](#)。

您的 VPC 隨附 [預設安全群組 \(p. 139\)](#)。如果您在執行個體啟動期間未指定不同的安全群組，則在 VPC 中啟動的執行個體會自動與預設安全群組建立關聯。您可以將特定規則新增至預設安全群組，但這些規則可能不適用於您在該 VPC 中啟動的其他執行個體。建議您為 Web 伺服器建立自訂安全群組。

針對此案例，請建立名為 `WebServerSG` 的安全群組。當您建立安全群組時，該安全群組具有允許所有流量離開執行個體的單一傳出規則。您必須修改規則以啟用傳入流量，並根據需要限制傳出流量。當您在 VPC 中啟動執行個體時，您可以指定此安全群組。

下列是 `WebServerSG` 安全群組的 IPv4 流量傳入和傳出規則。

傳入			
來源	通訊協定	連接埠範圍	評論
0.0.0.0/0	TCP	80	允許來自任何 IPv4 地址的 Web 伺服器進行傳入 HTTP 存取。
0.0.0.0/0	TCP	443	允許從任何 IPv4 地址傳入 Web 伺服器的 HTTPS 存取。
您網路的公有 IPv4 地址範圍	TCP	22	(Linux 執行個體) 允許透過 IPv4 從您的網路進行傳入 SSH 存取。您可以使用 <a href="http://checkip.amazonaws.com">http://checkip.amazonaws.com</a> 或 <a href="https://checkip.amazonaws.com">https://checkip.amazonaws.com</a> 等服務來取得本機電腦的公有 IPv4 地址。如果您透過 ISP 或是從防火牆後方進行連線，不具備靜態 IP 地址，則需要找到用戶端電腦使用的 IP 地址範圍。
您網路的公有 IPv4 地址範圍	TCP	3389	(Windows 執行個體) 允許透過 IPv4 從您的網路進行傳入 RDP 存取。
安全群組 ID (sg-xxxxxxx)	全部	全部	(選用) 允許來自與此安全群組相關聯之其他執行個體的傳入流量。此規則會自動新增至 VPC 的預設安全群組；針對您建立的任何自訂安全組，您必須手動新增規則來允許此類型的通訊。

傳出 (選用)			
目的地	通訊協定	連接埠範圍	評論
0.0.0.0/0	全部	全部	允許前往任何 IPv4 地址之傳出存取的預設規則。如果您希望將您的 Web 伺服器初始化傳出流量 (例如取得軟體更新)，您可以保留預設傳出規則。否則，您可以移除這項規則。

#### IPv6 的安全性群組規則

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則必須將單個別規則新增至安全群組，以控制 Web 伺服器執行個體的傳入和傳出 IPv6 流量。在此案例中，Web 伺服器能夠接收透過 IPv6 的所有網際網路流量，以及來自您本地網路透過 IPv6 的 SSH 或 RDP 流量。

下列是 WebServerSG 安全群組的 IPv6 特定規則 (上面所列規則的補充)。

傳入			
來源	通訊協定	連接埠範圍	評論
::/0	TCP	80	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTP 存取。
::/0	TCP	443	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTPS 存取。
您網路的公有 IPv6 地址範圍	TCP	22	(Linux 執行個體) 允許從您的網路透過 IPv6 進行傳入 SSH 存取。
您網路的公有 IPv6 地址範圍	TCP	3389	(Windows 執行個體) 允許從您的網路透過 IPv6 進行傳入 RDP 存取。
傳出 (選用)			
目的地	通訊協定	連接埠範圍	評論
::/0	全部	全部	允許前往任何 IPv6 地址之傳出存取的預設規則。如果您希望將您的 Web 伺服器初始化傳出流量 (例如取得軟體更新)，您可以保留預設傳出規則。否則，您可以移除這項規則。

### 針對具有單一公有子網路之 VPC 建議的網路 ACL 規則

下表顯示我們建議的規則。它們會封鎖除了明確需要的流量之外的所有流量。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許來自任何 IPv4 地址的傳入 HTTP 流量。
110	0.0.0.0/0	TCP	443	允許	允許來自任何 IPv4 地址的傳入 HTTPS 流量。

120	您家用網路的公有 IPv4 地址範圍	TCP	22	允許	允許來自您家用網路的傳入 SSH 流量 (透過網際網路閘道)。
130	您家用網路的公有 IPv4 地址範圍	TCP	3389	允許	允許來自您家用網路的傳入 RDP 流量 (透過網際網路閘道)。
140	0.0.0.0/0	TCP	32768-65535	允許	允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
110	0.0.0.0/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
120	0.0.0.0/0	TCP	32768-65535	允許	允許傳出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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv4 流量。

#### 適用於您 VPC 的建議網路 IPv6 規則

如果您已實作 IPv6 支援，並已建立 VPC 和子網路，其中具有相關聯的 IPv6 CIDR 區塊，則您必須將個別規則新增至您的網路 ACL，以控制傳入及傳出 IPv6 流量。

下列是您網路 ACL 的 IPv6 特定規則 (上述規則的補充)。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允許	允許來自任何 IPv6 地址的傳入 HTTP 流量。

160	::/0	TCP	443	允許	允許來自任何 IPv6 地址的傳入 HTTPS 流量。
170	您家用網路的 IPv6 地址範圍	TCP	22	允許	允許來自您家用網路的傳入 SSH 流量 (透過網際網路閘道)。
180	您家用網路的 IPv6 地址範圍	TCP	3389	允許	允許來自您家用網路的傳入 RDP 流量 (透過網際網路閘道)。
190	::/0	TCP	32768-65535	允許	允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
140	::/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
150	::/0	TCP	32768-65535	允許	允許傳出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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

## 具公有和私有子網路 (NAT) 的 VPC

此案例的組態，包含一個具有公有子網路和私有子網路的虛擬私有雲端 (VPC)。若您希望執行公開 Web 應用程式，同時維護不可公開存取的後端伺服器，我們建議使用此案例。其中一個常見的範例便是多層網站，其中 Web 伺服器位於公有子網路中，資料庫伺服器則位於私有子網路中。您可以設定安全和路由，讓 Web 伺服器與資料庫伺服器通訊。

公有子網路中的執行個體可將傳出流量直接傳送至網際網路，私有子網路中的執行個體則無法。私有子網路中的執行個體可改為透過使用位在公有子網路中的網路位址轉譯 (NAT) 閘道來存取網際網路。資料庫伺服器可使用 NAT 閘道連線到網際網路以取得軟體更新，但網際網路則無法建立與資料庫伺服器的連線。

## Note

您也可以使用 VPC 精靈設定具有 NAT 執行個體的 VPC；但是，我們建議您使用 NAT 閘道。如需更多詳細資訊，請參閱 [NAT 閘道 \(p. 226\)](#)。

您也可以選擇為 IPv6 設定此案例 – 您可以使用 VPC 精靈與相關聯的 IPv6 CIDR 區塊來建立 VPC 及子網路。在子網路上啟動的執行個體可接收 IPv6 地址並使用 IPv6 通訊。在私有子網路中的執行個體可使用僅輸出網際網路閘道，透過 IPv6 連線到網際網路，但網際網路無法透過 IPv6 與私有執行個體建立連線。如需 IPv4 和 IPv6 定址的詳細資訊，請參閱 [您 VPC 中的 IP 定址 \(p. 102\)](#)。

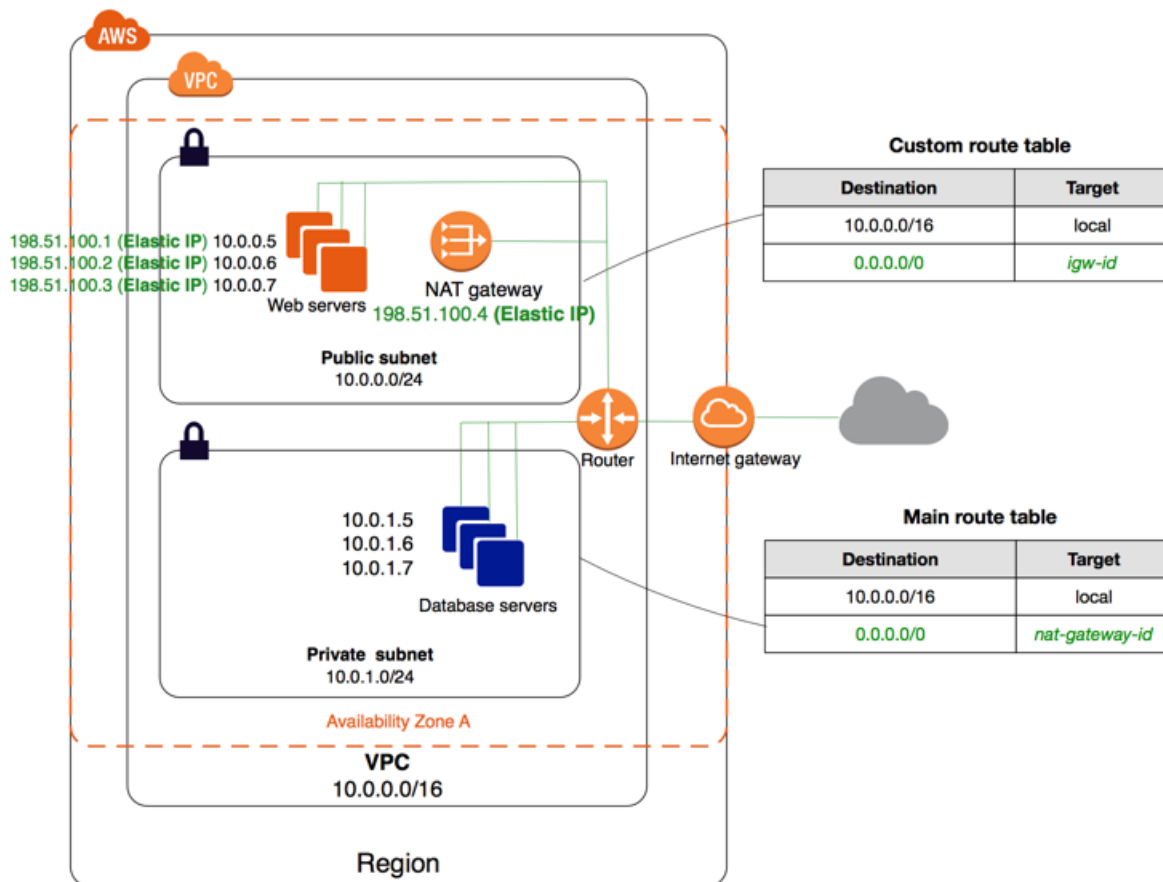
如需管理 EC2 執行個體軟體的相關資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [在您的 Linux 執行個體上管理軟體](#)。

## 內容

- [概觀 \(p. 25\)](#)
- [路由 \(p. 27\)](#)
- [安全性 \(p. 28\)](#)
- [實作案例 2 \(p. 31\)](#)
- [使用 NAT 執行個體實作案例 2 \(p. 31\)](#)
- [針對具有公有和私有子網路 \(NAT\) 之 VPC 建議的網路 ACL 規則 \(p. 32\)](#)

## 概觀

下圖顯示此案例組態的重要元件。





此案例的組態設定包括下列項目：

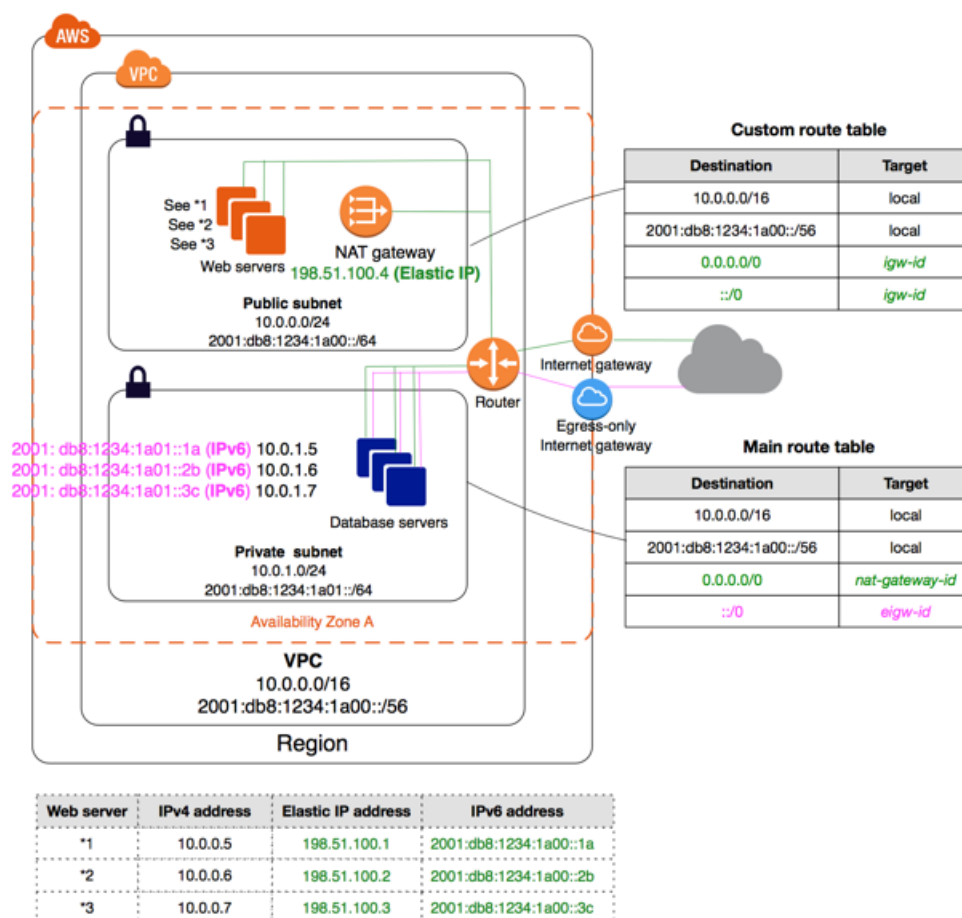
- 具有 /16 大小 IPv4 CIDR 區塊的 VPC (範例：10.0.0.0/16)。可提供 65,536 個私有 IPv4 地址。
- 具有 /24 大小 IPv4 CIDR 區塊的公有子網路 (範例：10.0.0.0/24)。可提供 256 個私有 IPv4 地址。公有子網路是一種子網路，其與具有網際網路閘道路由的路由表相關聯。
- 具有 /24 大小 IPv4 CIDR 區塊的私有子網路 (範例：10.0.1.0/24)。可提供 256 個私有 IPv4 地址。
- 網際網路閘道。這會將 VPC 連線至網際網路和其他 AWS 服務。
- 具子網路範圍內私有 IPv4 地址的執行個體 (範例：10.0.0.5、10.0.1.5)。這可讓它們與彼此以及 VPC 中的其他執行個體通訊。
- 公有子網路中具彈性 IPv4 地址 (例如：198.51.100.1) 的執行個體；這些地址是公有 IPv4 地址，其可讓執行個體透過網際網路受到存取。您可以在啟動時將公有 IP 地址 (而不是彈性 IP 地址) 指派給執行個體。私有子網路中的執行個體是後端伺服器，其不需要接收來自網際網路的傳入流量，因此不具有公有 IP 地址；但是，它們可以使用 NAT 閘道將請求傳送到網際網路 (請參閱下一個項目符號)。
- 具有自有彈性 IPv4 地址的 NAT 閘道。私有子網路中的執行個體可利用 IPv4，透過 NAT 閘道傳送請求至網際網路 (例如取得軟體更新)。
- 與公有子網路相關聯的自訂路由表。此路由表包含的項目可讓子網路中的執行個體透過 IPv4 與 VPC 中其他執行個體通訊，也可讓子網路中的執行個體透過 IPv4 直接與網際網路通訊。
- 與私有子網路相關聯的主路由表。路由表包含的項目可讓子網路中的執行個體透過 IPv4 與 VPC 中其他執行個體通訊，也可讓子網路中的執行個體利用 IPv4，透過 NAT 閘道直接與網際網路通訊。

如需子網路的詳細資訊，請參閱 [VPC 和子網路 \(p. 73\)](#)。如需網際網路閘道的詳細資訊，請參閱 [網際網路閘道 \(p. 212\)](#)。如需 NAT 閘道的詳細資訊，請參閱 [NAT 閘道 \(p. 226\)](#)。

## IPv6 概觀

您可以選擇為此案例啟用 IPv6。除了以上列出的元件，此組態也包含下列項目：

- 與 VPC 相關聯的 /56 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/56)。Amazon 會自動指派 CIDR；您無法自行選擇範圍。
- 與公有子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇 VPC IPv6 CIDR 區塊的大小。
- 與私有子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a01::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇子網路 IPv6 CIDR 區塊的大小。
- 從子網路範圍內指派給執行個體的 IPv6 地址 (範例：2001:db8:1234:1a00::1a)。
- 僅輸出網際網路閘道。這可讓私有子網路中的執行個體透過 IPv6 傳送請求至網際網路 (以進行軟體更新等作業)。若您希望私有子網路中的執行個體能夠初始化透過 IPv6 的網際網路通訊，便需要僅輸出網際網路閘道。如需更多詳細資訊，請參閱 [輸出限定網際網路閘道 \(p. 218\)](#)。
- 自訂路由表中的路由表項目，可讓公有子網路中的執行個體使用 IPv6 互相通訊，並在網際網路上直接通訊。
- 主路由表中的路由表項目，可讓私有子網路中的執行個體使用 IPv6 互相通訊，並透過僅輸出網際網路閘道與網際網路通訊。



## 路由

在此案例中，VPC 精靈會更新私有子網路使用的主路由表，並建立自訂路由表，然後將此路由表與公有子網路建立關聯。

在此案例中，所有來自每個子網路且目標為 AWS 的流量 (例如前往 Amazon EC2 或 Amazon S3 端點的流量) 都會通過網際網路閘道。私有子網路中的資料庫伺服器無法直接接收來自網際網路的流量，因為它們沒有彈性 IP 地址。但是，資料庫伺服器可透過公有子網路中的 NAT 裝置傳送及接收網際網路流量。

任何您建立的其他子網路預設都會使用主路由表，這表示根據預設，它們都是私有子網路。若您希望公開子網路，您一律可以變更與其關聯的路由表。

下表說明適用於此案例的路由表。

### 主路由表

第一個項目是 VPC 中本機路由的預設項目；該項目能讓 VPC 中的執行個體互相通訊。第二個項目會將所有其他子網路的流量傳送到 NAT 閘道 (例如 nat-12345678901234567)。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	nat-gateway-id

## 自訂路由表

第一個項目是 VPC 中本機路由的預設項目；該項目能讓此 VPC 中的執行個體互相通訊。第二個項目會將所有其他子網路流量，透過網際網路閘道路由至網際網路 (例如 `igw-1a2b3d4d`)。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	igw-id

## IPv6 路由

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則您的路由表必須包含 IPv6 流量的個別路由。下表顯示如果您選擇在 VPC 中啟用 IPv6 通訊，此案例會用的路由表。

### 主路由表

第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。第四個項目會將所有其他 IPv6 子網路流量路由至僅輸出網際網路閘道。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	nat-gateway-id
::/0	egress-only-igw-id

### 自訂路由表

第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。第四個項目會將所有其他 IPv6 子網路流量路由至網際網路閘道。

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

## 安全性

AWS 提供兩項功能，可用於提升 VPC 中的安全性：安全群組和網路 ACL。安全群組控制執行個體的傳入與傳出流量，網路 ACL 則是控制子網路的傳入與傳出流量。在大部分情況下，安全群組可以符合您的需求；然而，如果您想讓 VPC 多一層安全，也可以使用網路 ACL。如需詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)。

針對案例 2，您可以使用安全群組 (而不是網路 ACL)。如果您希望使用網路 ACL，請參閱 [針對具有公有和私有子網路 \(NAT\) 之 VPC 建議的網路 ACL 規則 \(p. 32\)](#)。

您的 VPC 隨附**預設安全群組** (p. 139)。如果您在執行個體啟動期間未指定不同的安全群組，則在 VPC 中啟動的執行個體會自動與預設安全群組建立關聯。在這個案例中，我們建議您建立下列安全群組，而非使用預設安全群組：

- WebServerSG：當您在公有子網路中啟動 Web 伺服器時，請指定此安全群組。
- DBServerSG：當您在私有子網路中啟動資料庫伺服器時，請指定此安全群組。

指派給安全群組的執行個體可位於不同的子網路中。不過，此案例的每個安全群組都會與執行個體扮演的角色類型相對應，且每個角色都要求執行個體位於特定子網路中。因此，此案例中所有指派給安全群組的執行個體均位於相同子網路中。

下表說明建議的 WebServerSG 安全群組規則，其可讓 Web 伺服器接收網際網路流量，以及來自您網路的 SSH 和 RDP 流量。Web 伺服器也可初始化對私有子網路中資料庫伺服器的讀取和寫入請求，並傳送流量至網際網路 (以取得軟體更新等等)。由於 Web 伺服器不會初始化其他傳出通訊，因此會移除預設的傳出規則。

#### Note

這些建議項目包含 SSH 和 RDP 存取，以及 Microsoft SQL Server 和 MySQL 兩種存取。針對您的情況，您可能只需要 Linux (SSH 和 MySQL) 或 Windows (RDP 和 Microsoft SQL Server) 規則。

#### WebServerSG：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
0.0.0.0/0	TCP	80	允許來自任何 IPv4 地址的 Web 伺服器進行傳入 HTTP 存取。
0.0.0.0/0	TCP	443	允許從任何 IPv4 地址傳入 Web 伺服器的 HTTPS 存取。
您家用網路的公有 IPv4 地址範圍	TCP	22	允許傳入 SSH 由您的家用網路存取 Linux 執行個體 (透過網際網路開道)。您可以使用 <a href="http://checkip.amazonaws.com">http://checkip.amazonaws.com</a> 或 <a href="https://checkip.amazonaws.com">https://checkip.amazonaws.com</a> 等服務來取得本機電腦的公有 IPv4 地址。如果您透過 ISP 或是從防火牆後方進行連線，不具備靜態 IP 地址，則需要找到用戶端電腦使用的 IP 地址範圍。
您家用網路的公有 IPv4 地址範圍	TCP	3389	允許傳入 RDP 由您的家用網路存取 Windows 執行個體 (透過網際網路開道)。
傳出			
目的地	通訊協定	連接埠範圍	評論
DBServerSG 安全群組的 ID	TCP	1433	允許傳出 Microsoft SQL Server 存取指派給 DBServerSG 安全群組的資料庫伺服器。
DBServerSG 安全群組的 ID	TCP	3306	允許傳出 MySQL 存取指派給 DBServerSG 安全群組的資料庫伺服器。
0.0.0.0/0	TCP	80	允許傳出 HTTP 存取任何 IPv4 地址。

0.0.0.0/0	TCP	443	允許傳出 HTTPS 存取任何 IPv4 地址。
-----------	-----	-----	--------------------------

下表說明建議的 DBServerSG 安全群組規則，其允許來自 Web 伺服器的讀取或寫入資料庫請求。資料庫伺服器也可初始化目標為網際網路的流量 (路由表會將該流量傳送到 NAT 閘道，NAT 閘道會再將該流量透過網際網路閘道轉送到網際網路)。

#### DBServerSG：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
WebServerSG 安全群組的 ID	TCP	1433	允許來自 Web 伺服器 (與 WebServerSG 安全群組相關聯) 的傳入 Microsoft SQL Server 存取。
WebServerSG 安全群組的 ID	TCP	3306	允許來自 Web 伺服器 (與 WebServerSG 安全群組相關聯) 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 (以進行軟體更新等作業)。
0.0.0.0/0	TCP	443	允許傳出 HTTPS 透過 IPv4 存取網際網路 (以進行軟體更新等作業)。

(選用) VPC 的預設安全群組具有的規則可自動允許指派的執行個體互相通訊。若要允許自訂安全群組的該類型通訊，您必須新增下列規則：

傳入			
來源	通訊協定	連接埠範圍	評論
安全群組的 ID	全部	全部	允許來自指派給此安全群組之其他執行個體的傳入流量。
傳出			
目的地	通訊協定	連接埠範圍	評論
安全群組的 ID	全部	全部	允許前往指派給此安全群組之其他執行個體的傳出流量。

(選用) 若您在您的公有子網路中啟動堡壘主機，做為來自您的家用網路，前往您私有子網路之 SSH 或 RDP 流量的代理，請新增規則至 DBServerSG 安全群組，允許來自堡壘執行個體或其關聯安全群組的傳入 SSH 或 RDP 流量。

### IPv6 的安全性群組規則

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則必須將個別規則新增至 WebServerSG 和 DBServerSG 安全群組，以控制執行個體的傳入和傳出 IPv6 流量。在此案例中，Web 伺服器能夠接收透過

IPv6 的所有網際網路流量，以及來自您本機網路透過 IPv6 的 SSH 或 RDP 流量。伺服器也可以初始化前往網際網路的傳出 IPv6 流量。資料庫伺服器也可以初始化前往網際網路的傳出 IPv6 流量。

下列是 WebServerSG 安全群組的 IPv6 特定規則 (上面所列規則的補充)。

傳入			
來源	通訊協定	連接埠範圍	評論
::/0	TCP	80	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTP 存取。
::/0	TCP	443	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTPS 存取。
您網路的公有 IPv6 地址範圍	TCP	22	(Linux 執行個體) 允許從您的網路透過 IPv6 進行傳入 SSH 存取。
您網路的公有 IPv6 地址範圍	TCP	3389	(Windows 執行個體) 允許從您的網路透過 IPv6 進行傳入 RDP 存取。
傳出			
目的地	通訊協定	連接埠範圍	評論
::/0	TCP	HTTP	允許傳出 HTTP 存取任何 IPv6 地址。
::/0	TCP	HTTPS	允許傳出 HTTPS 存取任何 IPv6 地址。

下列是 DBServerSG 安全群組的 IPv6 特定規則 (上面所列規則的補充)。

傳出			
目的地	通訊協定	連接埠範圍	評論
::/0	TCP	80	允許傳出 HTTP 存取任何 IPv6 地址。
::/0	TCP	443	允許傳出 HTTPS 存取任何 IPv6 地址。

## 實作案例 2

您可以使用 VPC 精靈建立 VPC、子網路、NAT 閘道，以及選擇性建立僅輸出網際網路閘道。您必須為您的 NAT 閘道指定彈性 IP 地址；若您沒有彈性 IP 地址，您必須先配置一個到您的帳戶。若您希望使用現有的彈性 IP 地址，請確認它目前並未與其他執行個體或網路界面建立關聯。NAT 閘道會自動在您 VPC 的公有子網路中建立。

## 使用 NAT 執行個體實作案例 2

您可以使用 NAT 執行個體 (而非 NAT 閘道) 實作案例 2。如需 NAT 執行個體的詳細資訊，請參閱 [NAT 執行個體 \(p. 243\)](#)。

您可以遵循與以上內容相同的程序；但是，在 VPC 精靈的 NAT 區段中，請選擇 Use a NAT instance instead (改為使用 NAT 執行個體)，然後指定您 NAT 執行個體的詳細資訊。您也需要您 NAT 執行個體

(NATSG) 的安全群組，允許 NAT 執行個體接收來自私有子網路中的執行個體，前往網際網路的流量，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。

在您使用 NAT 執行個體建立 VPC 之後，您必須將與 NAT 執行個體關聯的安全群組變更為新的 NATSG 安全群組 (根據預設，NAT 執行個體會使用預設安全群組啟動)。

#### NATSG：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
10.0.1.0/24	TCP	80	允許來自私有子網路中資料庫伺服器的傳入 HTTP 流量
10.0.1.0/24	TCP	443	允許來自私有子網路中資料庫伺服器的傳入 HTTPS 流量
您網路的公有 IP 地址範圍	TCP	22	允許傳入 SSH 由您的網路存取 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 (透過網際網路閘道)
0.0.0.0/0	TCP	443	允許傳出 HTTPS 存取網際網路 (透過網際網路閘道)

## 針對具有公有和私有子網路 (NAT) 之 VPC 建議的網路 ACL 規則

針對此案例，您會具有公有子網路的網路 ACL，以及私有子網路的個別網路 ACL。下表顯示我們針對每一個 ACL 建議的規則。它們會封鎖除了明確需要的流量之外的所有流量。它們大部分都模仿了案例的安全群組規則。

#### 公有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許來自任何 IPv4 地址的傳入 HTTP 流量。
110	0.0.0.0/0	TCP	443	允許	允許來自任何 IPv4 地址的傳入 HTTPS 流量。
120	您家用網路的公有 IP 地址範圍	TCP	22	允許	允許來自您家用網路的傳入 SSH 流量 (透過網際網路閘道)。
130	您家用網路的公有 IP 地址範圍	TCP	3389	允許	允許來自您家用網路的傳入 RDP 流量 (透過網際網路閘道)。



140	0.0.0.0/0	TCP	1024-65535	允許	<p>允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。</p> <p>此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
110	0.0.0.0/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
120	10.0.1.0/24	TCP	1433	允許	<p>允許傳出 MS SQL 存取私有子網路中的資料庫伺服器。</p> <p>此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。</p>
140	0.0.0.0/0	TCP	32768-65535	允許	<p>允許傳出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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>
150	10.0.1.0/24	TCP	22	允許	允許傳出 SSH 存取您私有子網路中的執行個體 (來自 SSH 堡壘 (若您有的話))。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv4 流量。

#### 私有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments



100	10.0.0.0/24	TCP	1433	允許	<p>允許公有子網路中的 Web 伺服器讀取及寫入私有子網路中的 MS SQL 伺服器。</p> <p>此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。</p>
120	10.0.0.0/24	TCP	22	允許	允許來自公有子網路中 SSH 堡壘的傳入 SSH 流量 (若您有的話)。
130	10.0.0.0/24	TCP	3389	允許	允許來自公有子網路中 Microsoft Terminal Services 閘道的傳入 RDP 流量。
140	0.0.0.0/0	TCP	1024-65535	允許	<p>允許來自公有子網路中的 NAT 裝置，針對出自私有子網路請求的傳入回傳流量。</p> <p>如需指定正確暫時性連接埠的資訊，請參閱本主題開頭的重要注意事項。</p>
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
110	0.0.0.0/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
120	10.0.0.0/24	TCP	32768-65535	允許	<p>允許目標為公有子網路的傳出回應 (例如，針對公有子網路中正在與私有子網路內 DB 伺服器通訊之 Web 伺服器的回應)。</p> <p>此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv4 流量。

## 適用於您 VPC 的建議網路 IPv6 規則

如果您已實作 IPv6 支援，並已建立 VPC 和子網路，其中具有關聯的 IPv6 CIDR 區塊，則必須將個別的規則新增到您的網路 ACL，以控制傳入及傳出 IPv6 流量。

下列是您網路 ACL 的 IPv6 特定規則 (上述規則的補充)。

### 公有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允許	允許來自任何 IPv6 地址的傳入 HTTP 流量。
160	::/0	TCP	443	允許	允許來自任何 IPv6 地址的傳入 HTTPS 流量。
170	您家用網路的 IPv6 地址範圍	TCP	22	允許	允許來自您家用網路，透過 IPv6 的傳入 SSH 流量 (透過網際網路閘道)。
180	您家用網路的 IPv6 地址範圍	TCP	3389	允許	允許來自您家用網路，透過 IPv6 的傳入 RDP 流量 (透過網際網路閘道)。
190	::/0	TCP	1024-65535	允許	允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
160	::/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
170	::/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
180	2001:db8:1234::/64	TCP	1433	允許	允許傳出 MS SQL 存取私有子網路中的資料庫伺服器。  此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以

					及適用於 Oracle 存取的 1521。
200	::/0	TCP	32768-65535	允許	<p>允許傳出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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>
210	2001:db8:1234::/64	TCP	22	允許	允許傳出 SSH 存取您私有子網路中的執行個體 (來自 SSH 堡壘 (若您有的話))。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

#### 私有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234::/64	TCP	1433	允許	<p>允許公有子網路中的 Web 伺服器讀取及寫入私有子網路中的 MS SQL 伺服器。</p> <p>此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。</p>
170	2001:db8:1234::/64	TCP	22	允許	允許來自公有子網路中 SSH 堡壘的傳入 SSH 流量 (若適用)。
180	2001:db8:1234::/64	TCP	3389	允許	允許來自公有子網路中 Microsoft Terminal Services 開道的傳入 RDP 流量 (若適用)。
190	::/0	TCP	1024-65535	允許	<p>允許來自僅輸出網際網路開道，針對出自私有子網路請求的傳入回傳流量。</p> <p>此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>

*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
130	::/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
140	::/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
150	2001:db8:1234::/64	TCP	32768-65535	允許	允許目標為公有子網路的傳出回應 (例如, 針對公有子網路中正在與私有子網路內 DB 伺服器通訊之 Web 伺服器的回應)。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊, 請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

## 具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC

此案例的組態包括一個含公有子網路與私有子網路的虛擬私有雲端 (VPC), 以及可經由 IPsec VPN 通道與您自己的網路通訊的虛擬私有閘道。若您想要將您的網路擴展至雲端, 並直接從 VPC 存取網際網路, 則建議您使用此案例。此案例可讓您在公有子網路中使用可擴展的 Web 前端來執行多層應用程式, 並將資料存放在私有子網路中, 而該子網路會透過 IPsec AWS Site-to-Site VPN 連接連線至您的網路。

您也可以選擇為 IPv6 設定此案例 – 您可以使用 VPC 精靈與相關聯的 IPv6 CIDR 區塊來建立 VPC 及子網路。在子網路中啟動的執行個體都可以收到 IPv6 地址。我們不支援透過虛擬私有閘道上 Site-to-Site VPN 連線的 IPv6 通訊; 不過, VPC 中的執行個體可以透過 IPv6 互相通訊, 而公有子網路中的執行個體也可以在網際網路中透過 IPv6 來通訊。如需 IPv4 和 IPv6 定址的詳細資訊, 請參閱[您 VPC 中的 IP 定址 \(p. 102\)](#)。

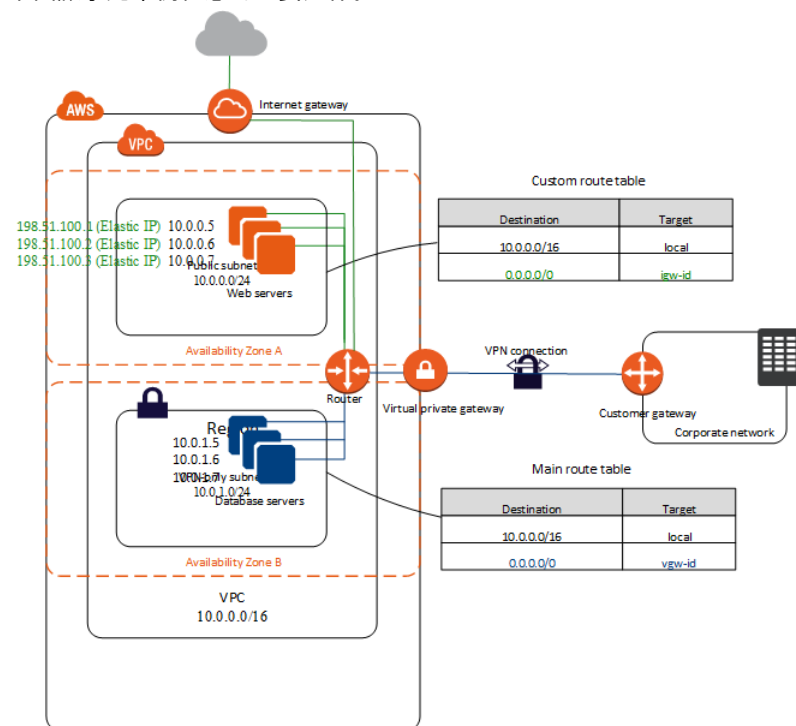
如需管理 EC2 執行個體軟體的相關資訊, 請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[在您的 Linux 執行個體上管理軟體](#)。

### 內容

- [概觀 \(p. 38\)](#)
- [路由 \(p. 40\)](#)
- [安全性 \(p. 42\)](#)
- [實作案例 3 \(p. 45\)](#)
- [針對具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 之 VPC 建議的網路 ACL 規則 \(p. 45\)](#)

## 概觀

下圖顯示此案例組態的重要元件。



### Important

對於此案例，如需在 Site-to-Site VPN 連線端設定客戶閘道裝置的詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的[您的客戶閘道裝置](#)。

此案例的組態設定包括下列項目：

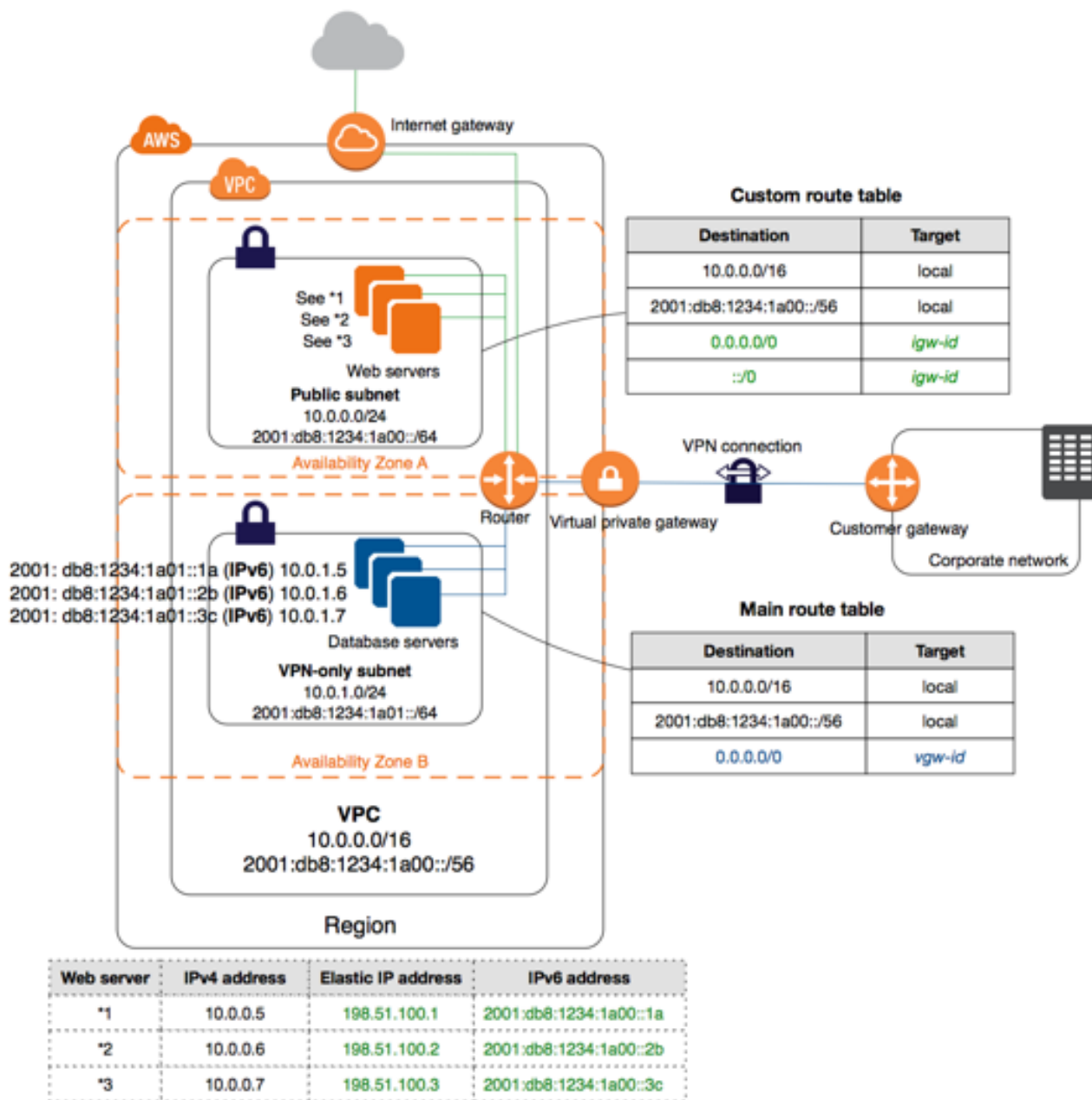
- 具有 /16 大小 IPv4 CIDR 的虛擬私有雲端 (VPC) (範例：10.0.0.0/16)。可提供 65,536 個私有 IPv4 地址。
- 具有 /24 大小 IPv4 CIDR 的公有子網路 (範例：10.0.0.0/24)。可提供 256 個私有 IPv4 地址。公有子網路是一種子網路，其與具有網際網路閘道路由的路由表相關聯。
- 具有 /24 大小 IPv4 CIDR 的僅 VPN 子網路 (範例：10.0.1.0/24)。可提供 256 個私有 IPv4 地址。
- 網際網路閘道。這會將 VPC 連線至網際網路和其他 AWS 產品。
- 您 VPC 與網路之間的 Site-to-Site VPN 連接。Site-to-Site VPN 連接由位於 Site-to-Site VPN 連接 Amazon 端的虛擬私有閘道，以及位於 Site-to-Site VPN 連接您這一端的客戶閘道組成。
- 私有 IPv4 地址在子網路範圍內 (例如：10.0.0.5 與 10.0.1.5) 的執行個體；該範圍可讓執行個體互相通訊，並與 VPC 中的其他執行個體通訊。
- 公有子網路中含彈性 IP 地址 (例如：198.51.100.1) 的執行個體；這些地址是公有 IPv4 地址，其可讓執行個體透過網際網路受到存取。您可以在啟動時將公有 IPv4 地址 (而不是彈性 IP 地址) 指派給執行個體。僅 VPN 子網路中的執行個體是後端伺服器，其不需要接收來自網際網路的傳入流量，但可以傳送並接收您的網路流量。
- 與公有子網路相關聯的自訂路由表。此路由表包含的項目可讓子網路中的執行個體與 VPC 中其他執行個體通訊，也可讓子網路中的執行個體直接與網際網路通訊。
- 與僅 VPN 子網路相關聯的主路由表。路由表包含的項目可讓子網路中的執行個體與 VPC 中其他執行個體通訊，也可讓子網路中的執行個體直接與您的網路通訊。

如需子網路的詳細資訊，請參閱 [VPC 和子網路 \(p. 73\)](#) 和 [您 VPC 中的 IP 定址 \(p. 102\)](#)。如需網際網路閘道的詳細資訊，請參閱 [網際網路閘道 \(p. 212\)](#)。如需有關 AWS Site-to-Site VPN 連接的詳細資訊，請參閱 [AWS Site-to-Site VPN 使用者指南中的什麼是 AWS Site-to-Site VPN ?](#)。

## IPv6 概觀

您可以選擇為此案例啟用 IPv6。除了以上列出的元件，此組態也包含下列項目：

- 與 VPC 相關聯的 /56 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/56)。AWS 會自動指派 CIDR；您無法自行選擇範圍。
- 與公有子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇 IPv6 CIDR 的大小。
- 與僅 VPN 子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a01::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇 IPv6 CIDR 的大小。
- 從子網路範圍內指派給執行個體的 IPv6 地址 (範例：2001:db8:1234:1a00::1a)。
- 自訂路由表中的路由表項目，可讓公有子網路中的執行個體使用 IPv6 互相通訊，並在網際網路上直接通訊。
- 主路由表中的路由表項目，可讓僅 VPN 子網路中的執行個體使用 IPv6 互相通訊。



## 路由

您的 VPC 具有隱含路由器 (顯示於此案例的組態圖表中)。在此案例中，VPC 精靈會更新僅 VPN 子網路使用的主路由表，並建立自訂路由表，然後將此路由表與公有子網路建立關聯。

位於僅 VPN 子網路中的執行個體無法直接連接網際網路；任何進出網際網路的流量都必須先周遊至您網路的虛擬私有閘道，以受您的防火牆和企業安全政策的規範。如果執行個體要傳送任何進出 AWS 的流量 (例如，對 Amazon S3 或 Amazon EC2 API 的請求)，請求必須透過虛擬私有閘道通往您的網路，然後傳出到網際網路之後再抵達 AWS。



## Tip

任何從您的網路前往公有子網路執行個體之彈性 IP 地址的流量，皆會通過網際網路，而不是虛擬私有閘道。您可以改為設定路由和安全群組規則，讓流量透過虛擬私有閘道從您的網路前往公有子網路。

您可將 Site-to-Site VPN 連接設為靜態路由 Site-to-Site VPN 連接或動態路由 Site-to-Site VPN 連接 (使用 BGP)。若您選取靜態路由，則當您建立 Site-to-Site VPN 連接時，您會接到提示要求您手動輸入您網路的 IP 前綴。如果您選取動態路由，系統會自動使用 BGP 為您的 VPC 向虛擬私有閘道公告 IP 字首。

下表說明適用於此案例的路由表。

## 主路由表

第一個項目是 VPC 中本機路由的預設項目；該項目能讓 VPC 中的執行個體透過 IPv4 互相通訊。第二個項目會透過虛擬私有閘道 (例如 vgw-1a2b3c4d)，將所有其他 IPv4 子網路流量從私有子網路路由至您的網路。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	vgw-id

## 自訂路由表

第一個項目是 VPC 中本機路由的預設項目；該項目能讓 VPC 中的執行個體互相通訊。第二個項目會透過網際網路閘道 (例如 igw-1a2b3c4d)，將所有其他 IPv4 子網路流量從公有子網路路由至網際網路。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	igw-id

## 其他路由

或者，如果您想讓私有子網路中的執行個體存取網際網路，您可以建立網路地址轉譯 (NAT) 閘道或公有子網路中的執行個體，並設定路由以讓子網路進出網際網路的流量前往 NAT 裝置。這可讓僅 VPN 子網路中的執行個體透過網際網路閘道傳送請求 (以進行軟體更新等作業)。

如需手動設定 NAT 裝置的詳細資訊，請參閱 [NAT \(p. 226\)](#)。如需如何使用 VPC 精靈設定 NAT 裝置的資訊，請參閱 [具有公有和私有子網路 \(NAT\) 的 VPC \(p. 24\)](#)。

若要讓私有子網路進出網際網路的流量前往 NAT 裝置，您必須更新主路由表，如下所示。

第一個項目是用來在 VPC 中本機路由的預設項目。第二個項目會將繫結至您自己本機 (客戶) 網路的子網路流量路由至虛擬私有閘道。在此範例中，假設您的區域網路的 IP 地址範圍為 172.16.0.0/12。第三個項目會將所有其他子網路流量傳送至 NAT 閘道。

目的地	目標
10.0.0.0/16	區域
172.16.0.0/12	vgw-id
0.0.0.0/0	nat-gateway-id



## IPv6 路由

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則您的路由表必須包含 IPv6 流量的個別路由。下表顯示如果您選擇在 VPC 中啟用 IPv6 通訊，此案例會用的路由表。

### 主路由表

第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	vgw-id

### 自訂路由表

第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。第四個項目會將所有其他 IPv6 子網路流量路由至網際網路閘道。

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

## 安全性

AWS 提供兩項功能，可用於提升 VPC 中的安全性：安全群組和網路 ACL。安全群組控制執行個體的傳入與傳出流量，網路 ACL 則是控制子網路的傳入與傳出流量。在大部分情況下，安全群組可以符合您的需求；然而，如果您想讓 VPC 多一層安全，也可以使用網路 ACL。如需詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)。

針對案例 3，您可以使用安全群組 (而不是網路 ACL)。如果您希望使用網路 ACL，請參閱 [針對具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 之 VPC 建議的網路 ACL 規則 \(p. 45\)](#)。

您的 VPC 隨附 [預設安全群組 \(p. 139\)](#)。如果您在執行個體啟動期間未指定不同的安全群組，則在 VPC 中啟動的執行個體會自動與預設安全群組建立關聯。在這個案例中，我們建議您建立下列安全群組，而非使用預設安全群組：

- WebServerSG：當您在公有子網路中啟動 Web 伺服器時，請指定此安全群組。
- DBServerSG：當您在僅 VPN 子網路中啟動資料庫伺服器時，請指定此安全群組。

指派給安全群組的執行個體可位於不同的子網路中。不過，此案例的每個安全群組都會與執行個體扮演的角色類型相對應，且每個角色都要求執行個體位於特定子網路中。因此，此案例中所有指派給安全群組的執行個體均位於相同子網路中。

下表說明建議的 WebServerSG 安全群組規則，其可讓 Web 伺服器接收網際網路流量，以及來自您網路的 SSH 和 RDP 流量。Web 伺服器也可初始化對僅 VPN 子網路中資料庫伺服器的讀取和寫入請求，並傳送流

量至網際網路 (以取得軟體更新等)。由於 Web 伺服器不會初始化其他傳出通訊，因此會移除預設的傳出規則。

#### Note

此群組包括 SSH 和 RDP 存取，以及 Microsoft SQL Server 和 MySQL 兩種存取。針對您的情況，您可能只需要 Linux (SSH 和 MySQL) 或 Windows (RDP 和 Microsoft SQL Server) 規則。

#### WebServerSG：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
0.0.0.0/0	TCP	80	允許來自任何 IPv4 地址的 Web 伺服器進行傳入 HTTP 存取。
0.0.0.0/0	TCP	443	允許從任何 IPv4 地址傳入 Web 伺服器的 HTTPS 存取。
您網路的公有 IP 地址範圍	TCP	22	允許傳入 SSH 由您的網路存取 Linux 執行個體 (透過網際網路閘道)。
您網路的公有 IP 地址範圍	TCP	3389	允許傳入 RDP 由您的網路存取 Windows 執行個體 (透過網際網路閘道)。
傳出			
DBServerSG 安全群組的 ID	TCP	1433	允許傳出 Microsoft SQL Server 存取指派給 DBServerSG 的資料庫伺服器。
DBServerSG 安全群組的 ID	TCP	3306	允許傳出 MySQL 存取指派給 DBServerSG 的資料庫伺服器。
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。

下表說明建議的 DBServerSG 安全群組規則，其可讓 Microsoft SQL Server 和 MySQL 讀取和寫入 Web 伺服器的請求，以及來自您網路的 SSH 和 RDP 流量。資料庫伺服器也會初始化進出網際網路的流量 (您的路由表會透過虛擬私有閘道傳送該流量)。

#### DBServerSG：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
WebServerSG 安全群組的 ID	TCP	1433	允許來自 Web 伺服器 (與 WebServerSG 安全群組相關聯) 的傳入 Microsoft SQL Server 存取。
WebServerSG 安全群組的 ID	TCP	3306	允許來自 Web 伺服器 (與 WebServerSG 安全群組相關聯) 的傳入 MySQL Server 存取。
您網路的 IPv4 地址範圍	TCP	22	允許從您的網路到 Linux 執行個體的傳入 SSH 流量 (透過虛擬私有閘道)。

您網路的 IPv4 地址範圍	TCP	3389	允許從您的網路到 Windows 執行個體的傳入 RDP 流量 (透過虛擬私有閘道)。
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 IPv4 HTTP 透過虛擬私有閘道存取網際網路 (以進行軟體更新等作業)。
0.0.0.0/0	TCP	443	允許傳出 IPv4 HTTPS 透過虛擬私有閘道存取網際網路 (以進行軟體更新等作業)。

(選用) VPC 的預設安全群組具有的規則可自動允許指派的執行個體互相通訊。若要允許自訂安全群組的該類型通訊，您必須新增下列規則：

傳入			
來源	通訊協定	連接埠範圍	評論
安全群組的 ID	全部	全部	允許來自指派給此安全群組之其他執行個體的傳入流量。
傳出			
目的地	通訊協定	連接埠範圍	評論
安全群組的 ID	全部	全部	允許前往指派給此安全群組之其他執行個體的傳出流量。

## IPv6 的安全性群組規則

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則必須將個別規則新增至 WebServerSG 和 DBServerSG 安全群組，以控制執行個體的傳入和傳出 IPv6 流量。在此案例中，Web 伺服器能夠接收透過 IPv6 的所有網際網路流量，以及來自您本機網路透過 IPv6 的 SSH 或 RDP 流量。伺服器也可以初始化前往網際網路的傳出 IPv6 流量。資料庫伺服器無法初始化前往網際網路的傳出 IPv6 流量，因此不需要任何額外的安全群組規則。

下列是 WebServerSG 安全群組的 IPv6 特定規則 (上面所列規則的補充)。

傳入			
來源	通訊協定	連接埠範圍	評論
::/0	TCP	80	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTP 存取。
::/0	TCP	443	允許來自任何 IPv6 地址的 Web 伺服器進行傳入 HTTPS 存取。
您網路的公有 IPv6 地址範圍	TCP	22	(Linux 執行個體) 允許從您的網路透過 IPv6 進行傳入 SSH 存取。

您網路的公有 IPv6 地址範圍	TCP	3389	(Windows 執行個體) 允許從您的網路透過 IPv6 進行傳入 RDP 存取。
傳出			
目的地	通訊協定	連接埠範圍	評論
::/0	TCP	HTTP	允許傳出 HTTP 存取任何 IPv6 地址。
::/0	TCP	HTTPS	允許傳出 HTTPS 存取任何 IPv6 地址。

### 實作案例 3

若要實作案例 3，請取得客戶閘道的資訊，並使用 VPC 精靈建立 VPC。VPC 精靈會使用客戶閘道和虛擬私有閘道為您建立 Site-to-Site VPN 連接。

這些程序包括用於為 VPC 啟用和設定 IPv6 通訊的選用步驟。如果您不希望在 VPC 上使用 IPv6，則不需執行這些步驟。

#### 準備您的客戶閘道

1. 判斷您會用來做為客戶閘道裝置的裝置。如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的[您的客戶閘道裝置](#)。
2. 獲取客戶閘道裝置外部界面的網際網路可路由傳送 IP 地址。此地址必須為靜態，而且能在裝置後端執行網路位址轉譯 (NAT)。
3. 若您希望建立可靜態路由的 Site-to-Site VPN 連接，請取得應在前往虛擬私有閘道的 Site-to-Site VPN 連接內公告的內部 IP 範圍清單 (以 CIDR 表示法表示)。如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的[路由表與 VPN 路由優先順序](#)。

如需如何搭配 IPv4 使用 VPC 精靈的相關資訊，請參閱[入門 \(p. 10\)](#)。

如需如何將 VPC 精靈搭配 IPv6 使用的詳細資訊，請參閱[the section called “IPv6 入門” \(p. 13\)](#)。

### 針對具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 之 VPC 建議的網路 ACL 規則

針對此案例，您會具有公有子網路的網路 ACL，以及僅 VPN 子網路的個別網路 ACL。下表顯示我們針對每一個 ACL 建議的規則。它們會封鎖除了明確需要的流量之外的所有流量。

#### 公有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許來自任何 IPv4 地址，目標為 Web 伺服器的傳入 HTTP 流量。
110	0.0.0.0/0	TCP	443	允許	允許來自任何 IPv4 地址，目標為 Web 伺服器的傳入 HTTPS 流量。

Amazon Virtual Private Cloud 使用者指南  
具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC

120	您家用網路的公有 IPv4 地址範圍	TCP	22	允許	允許來自您家用網路，目標為 Web 伺服器的傳入 SSH 流量 (透過網際網路閘道)。
130	您家用網路的公有 IPv4 地址範圍	TCP	3389	允許	允許來自您家用網路，目標為 Web 伺服器的傳入 RDP 流量 (透過網際網路閘道)。
140	0.0.0.0/0	TCP	32768-65535	允許	允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv4 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	0.0.0.0/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
110	0.0.0.0/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
120	10.0.1.0/24	TCP	1433	允許	允許傳出 MS SQL 存取僅 VPN 子網路中的資料庫伺服器。  此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。
140	0.0.0.0/0	TCP	32768-65535	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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出流量。

適用於僅 VPN 子網路的 ACL 設定

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	10.0.0.0/24	TCP	1433	允許	<p>允許公有子網路中的 Web 伺服器讀取及寫入僅 VPN 子網路中的 MS SQL 伺服器。</p> <p>此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。</p>
120	您家用網路的私有 IPv4 地址範圍	TCP	22	允許	允許來自家用網路的傳入 SSH 流量 (透過虛擬私有閘道)。
130	您家用網路的私有 IPv4 地址範圍	TCP	3389	允許	允許來自家用網路的傳入 RDP 流量 (透過虛擬私有閘道)。
140	您家用網路的私有 IP 地址範圍	TCP	32768-65535	允許	<p>允許來自家用網路中用戶端的傳入回傳流量 (透過虛擬私有閘道)</p> <p>此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱<a href="#">暫時性連接埠 (p. 152)</a>。</p>
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	您家用網路的私有 IP 地址範圍	全部	全部	允許	<p>允許所有來自子網路，目標為您家用網路的傳出流量 (透過虛擬私有閘道)。此規則也涵蓋規則 120。不過，您可以透過使用特定的通訊協定類型及連接埠號碼，來提高此規則的限制性。若您提高此規則的限制性，您必須在您的網路 ACL 中包含規則 120，確保不會封鎖傳出回應。</p>
110	10.0.0.0/24	TCP	32768-65535	允許	<p>允許傳出回應公有子網路中的 Web 伺服器。</p> <p>此範圍僅為範例。如需選擇適用於您組態之正確暫時性</p>

					連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
120	您家用網路的私有 IP 地址範圍	TCP	32768-65535	允許	允許傳出回應家用網路中的用戶端 (透過虛擬私有閘道)。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出流量。

## 適用於您 VPC 的建議網路 IPv6 規則

如果您已實作 IPv6 支援，並已建立 VPC 和子網路，其中具有關聯的 IPv6 CIDR 區塊，則必須將個別的規則新增到您的網路 ACL，以控制傳入及傳出 IPv6 流量。

下列是您網路 ACL 的 IPv6 特定規則 (上述規則的補充)。

### 公有子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	::/0	TCP	80	允許	允許來自任何 IPv6 地址的傳入 HTTP 流量。
160	::/0	TCP	443	允許	允許來自任何 IPv6 地址的傳入 HTTPS 流量。
170	您家用網路的 IPv6 地址範圍	TCP	22	允許	允許來自您家用網路，透過 IPv6 的傳入 SSH 流量 (透過網際網路閘道)。
180	您家用網路的 IPv6 地址範圍	TCP	3389	允許	允許來自您家用網路，透過 IPv6 的傳入 RDP 流量 (透過網際網路閘道)。
190	::/0	TCP	1024-65535	允許	允許來自網際網路，正在回應出自子網路之請求主機的傳入回傳流量。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments

Amazon Virtual Private Cloud 使用者指南  
具有公有和私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC

150	::/0	TCP	80	允許	允許傳出 HTTP 流量從子網路流向網際網路。
160	::/0	TCP	443	允許	允許傳出 HTTPS 流量從子網路流向網際網路。
170	2001:db8:1234::/64	TCP	1433	允許	允許傳出 MS SQL 存取私有子網路中的資料庫伺服器。  此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。
190	::/0	TCP	32768-65535	允許	允許傳出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。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

適用於僅 VPN 子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
150	2001:db8:1234::/64	TCP	1433	允許	允許公有子網路中的 Web 伺服器讀取及寫入私有子網路中的 MS SQL 伺服器。  此連接埠號碼僅為範例。其他範例包含適用於 MySQL/Aurora 存取的 3306、適用於 PostgreSQL 存取的 5432、適用於 Amazon Redshift 存取的 5439，以及適用於 Oracle 存取的 1521。
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments



130	2001:db8:1234:1600::/64	32768-65535	允許	允許目標為公有子網路的傳出回應 (例如, 針對公有子網路中正在與私有子網路內 DB 伺服器通訊之 Web 伺服器的回應)。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊, 請參閱 <a href="#">暫時性連接埠</a> (p. 152)。	
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

## 僅具有私有子網路以及可存取 AWS Site-to-Site VPN 的 VPC

此案例的組態包括一個具有單一私有子網路的虛擬私有雲端 (VPC), 以及可經由 IPsec VPN 通道與您自己的網路通訊的虛擬私有閘道。其中沒有可啟用網際網路通訊的網際網路閘道。若您希望使用 Amazon 的基礎設施將您的網路擴展至雲端, 而無須將您的網路向網際網路公開, 則建議使用此案例。

也可以選擇為 IPv6 設定此案例 – 您可以使用 VPC 精靈來建立與 IPv6 CIDR 區塊相關聯的 VPC 和子網路。在子網路中啟動的執行個體都可以收到 IPv6 地址。目前, 我們不支援透過虛擬私有閘道上 AWS Site-to-Site VPN 連線的 IPv6 通訊; 不過, VPC 中的執行個體可以透過 IPv6 彼此互相通訊。如需 IPv4 和 IPv6 定址的詳細資訊, 請參閱[您 VPC 中的 IP 定址](#) (p. 102)。

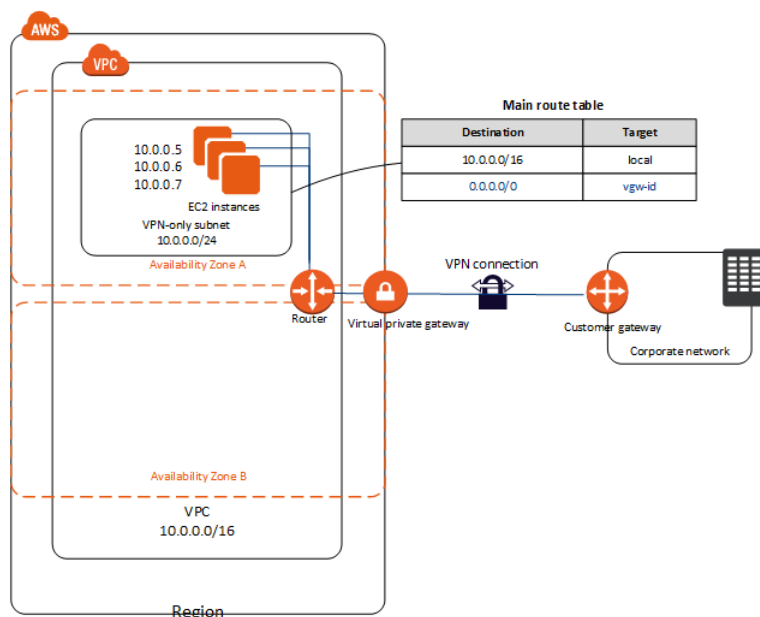
如需管理 EC2 執行個體軟體的相關資訊, 請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[在您的 Linux 執行個體上管理軟體](#)。

### 內容

- [概觀](#) (p. 50)
- [路由](#) (p. 52)
- [安全性](#) (p. 53)

## 概觀

下圖顯示此案例組態的重要元件。



### Important

對於此案例，請參閱您的[客戶閘道裝置](#)，以便在您的 Site-to-Site VPN 連線端設定客戶閘道裝置。

此案例的組態設定包括下列項目：

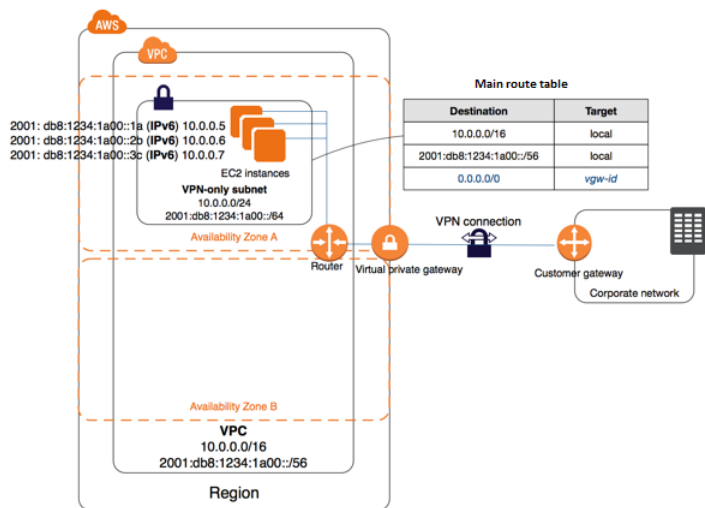
- 具有 /16 大小 CIDR 的虛擬私有雲端 (VPC) (範例：10.0.0.0/16)。可提供 65,536 個私有 IP 地址。
- 具有 /24 大小 CIDR 的僅 VPN 子網路 (範例：10.0.0.0/24)。可提供 256 個私有 IP 地址。
- 您 VPC 與網路之間的 Site-to-Site VPN 連接。Site-to-Site VPN 連接由位於 Site-to-Site VPN 連接 Amazon 端的虛擬私有閘道，以及位於 Site-to-Site VPN 連接您這一端的客戶閘道組成。
- 私有 IP 地址在子網路範圍內 (例如：10.0.0.5、10.0.0.6，以及 10.0.0.7) 的執行個體；該範圍可讓執行個體互相通訊，並與 VPC 中的其他執行個體通訊。
- 主路由表包含一個路由，可讓子網路中的執行個體與 VPC 中的其他執行個體通訊。由於路由傳播已啟用，因此可讓子網路中的執行個體直接與您網路通訊的路由在主路由表中顯示為傳播路由。

如需子網路的詳細資訊，請參閱 [VPC 和子網路 \(p. 73\)](#) 和 [您 VPC 中的 IP 定址 \(p. 102\)](#)。如需有關 Site-to-Site VPN 連接的詳細資訊，請參閱 AWS Site-to-Site VPN 使用者指南中的 [什麼是 AWS Site-to-Site VPN？](#)。如需有關設定客戶閘道裝置的詳細資訊，請參閱您的[客戶閘道裝置](#)。

## IPv6 概觀

您可以選擇為此案例啟用 IPv6。除了以上列出的元件，此組態也包含下列項目：

- 與 VPC 相關聯的 /56 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/56)。AWS 會自動指派 CIDR；您無法自行選擇範圍。
- 與僅 VPN 子網路相關聯的 /64 大小 IPv6 CIDR 區塊 (範例：2001:db8:1234:1a00::/64)。您可以從配置給 VPC 的範圍內選擇子網路範圍。您無法選擇 IPv6 CIDR 的大小。
- 從子網路範圍內指派給執行個體的 IPv6 地址 (範例：2001:db8:1234:1a00::1a)。
- 主路由表中的路由表項目，可讓私有子網路中的執行個體使用 IPv6 互相通訊。



## 路由

您的 VPC 具有隱含路由器 (顯示於此案例的組態圖表中)。在此案例中，VPC 精靈會建立路由表，將目的地為 VPC 外部地址的所有流量路由至 AWS Site-to-Site VPN 連接，並將路由表與子網路建立關聯。

下列說明適用於此案例的路由表。第一個項目是 VPC 中本機路由的預設項目；該項目能讓此 VPC 中的執行個體互相通訊。第二個項目會將所有其他子網路流量路由至虛擬私有閘道 (例如 `vgw-1a2b3c4d`)。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	vgw-id

您可將 AWS Site-to-Site VPN 連接設為靜態路由 Site-to-Site VPN 連接或動態路由 Site-to-Site VPN 連接 (使用 BGP)。若您選取靜態路由，則當您建立 Site-to-Site VPN 連接時，您會接到提示要求您手動輸入您網路的 IP 前綴。若您選取動態路由，系統會自動透過 BGP 向您的 VPC 公告 IP 前綴。

位於您 VPC 中的執行個體無法直接連接網際網路；任何進出網際網路的流量都必須先周遊至您網路的虛擬私有閘道，以受您的防火牆和企業安全政策的規範。如果執行個體要傳送任何進出 AWS 的流量 (例如，對 Amazon S3 或 Amazon EC2 的請求)，請求必須透過虛擬私有閘道通往您的網路，然後通往網際網路之後再抵達 AWS。

## IPv6 路由

如果您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，則您的路由表會包含 IPv6 流量的個別路由。下列說明適用於此案例的自訂路由表。第二個項目是自動為在 VPC 中透過 IPv6 之本機路由新增的預設路由。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域
0.0.0.0/0	vgw-id

## 安全性

AWS 提供兩項功能，可用於提升 VPC 中的安全性：安全群組和網路 ACL。安全群組控制執行個體的傳入與傳出流量，網路 ACL 則是控制子網路的傳入與傳出流量。在大部分情況下，安全群組可以符合您的需求；然而，如果您想讓 VPC 多一層安全，也可以使用網路 ACL。如需詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)。

針對案例 4，您會使用您 VPC 的預設安全群組，而非網路 ACL。如果您希望使用網路 ACL，請參閱 [僅具有私有子網路的 VPC 和 AWS Site-to-Site VPN 存取的建議網路 ACL 規則 \(p. 53\)](#)。

您的 VPC 隨附一個預設安全群組，其初始設定為拒絕所有傳入流量、允許所有傳出流量，以及允許所有指派給安全群組的執行個體間的流量。針對此案例，我們建議您將傳入規則新增至預設安全群組，允許來自您網路的 SSH 流量 (Linux) 及遠端桌面流量 (Windows)。

### Important

預設安全群組會自動允許指派的執行個體互相通訊，因此您不需要新增規則來允許它。若您使用不同的安全群組，您必須新增規則以允許它。

下表說明您應新增到您 VPC 預設安全群組的傳入規則。

### 預設安全群組：建議的規則

傳入			
來源	通訊協定	連接埠範圍	評論
您網路的私有 IPv4 地址範圍	TCP	22	(Linux 執行個體) 允許來自您網路的傳入 SSH 流量。
您網路的私有 IPv4 地址範圍	TCP	3389	(Windows 執行個體) 允許來自您網路的傳入 RDP 流量。

### IPv6 的安全性群組規則

若您將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，您必須新增個別的規則至您的安全群組，以控制您執行個體的傳入及傳出 IPv6 流量。在此案例中，資料庫伺服器無法透過 Site-to-Site VPN 連接使用 IPv6 觸達，因此不需要額外的安全群組規則。

## 僅具有私有子網路的 VPC 和 AWS Site-to-Site VPN 存取的建議網路 ACL 規則

下表顯示我們建議的規則。它們會封鎖除了明確需要的流量之外的所有流量。

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
100	您家用網路的私有 IP 地址範圍	TCP	22	允許	允許來自您的家用網路，目標為子網路的傳入 SSH 流量 (透過網際網路閘道)。
110	您家用網路的私有 IP 地址範圍	TCP	3389	允許	允許來自您的家用網路，目標為子網路的傳入 RDP 流量 (透過網際網路閘道)。
120	您家用網路的私有 IP 地址範圍	TCP	32768-65535	允許	允許來自子網路之請求的傳入回傳流量。

					此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
100	您家用網路的私有 IP 地址範圍	全部	全部	允許	允許來自子網路，目標為您家用網路的所有傳出流量。此規則也涵蓋規則 120。不過，您可以透過使用特定的通訊協定類型及連接埠號碼，來提高此規則的限制性。若您提高此規則的限制性，您必須在您的網路 ACL 中包含規則 120，確保不會封鎖傳出回應。
120	您家用網路的私有 IP 地址範圍	TCP	32768-65535	允許	允許傳出回應家用網路中的用戶端。  此範圍僅為範例。如需選擇適用於您組態之正確暫時性連接埠的資訊，請參閱 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	0.0.0.0/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出流量。

### 適用於您 VPC 的建議網路 IPv6 規則

若您使用 IPv6 支援實作案例 4 並使用關聯的 IPv6 CIDR 區塊建立 VPC 和子網路，您必須將個別的規則新增到您的網路 ACL，以控制傳入及傳出 IPv6 流量。

在此案例中，資料庫伺服器無法透過 VPN 連線使用 IPv6 觸達，因此不需要額外的網路 ACL。下列是拒絕前往及來自子網路之 IPv6 流量的預設規則。

### 適用於僅 VPN 子網路的 ACL 規則

Inbound					
Rule #	Source IP	Protocol	Port	Allow/Deny	Comments
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳入 IPv6 流量。
Outbound					
Rule #	Dest IP	Protocol	Port	Allow/Deny	Comments
*	::/0	全部	全部	拒絕	拒絕上述規則 (無法修改) 尚未處理的所有傳出 IPv6 流量。

# VPC 的範例

本節具有建立和設定 VPC 的範例。

範例	用量
<a href="#">範例：使用 AWS CLI 建立 IPv4 VPC 及子網路 (p. 60)</a>	使用 AWS CLI 來建立包含公有子網路和私有子網路的 VPC。
<a href="#">範例：使用 AWS CLI 建立 IPv6 VPC 及子網路 (p. 64)</a>	使用 AWS CLI 來建立 VPC，其具有相關聯的 IPv6 CIDR 區塊以及公有子網路和私有子網路，各有相關聯的 IPv6 CIDR 區塊。
<a href="#">the section called “範例：共享公有子網路和私有子網路” (p. 55)</a>	與帳戶共享私有和公有子網路。
<a href="#">the section called “範例：使用的服務 AWS PrivateLink 和 VPC 對等” (p. 56)</a>	了解如何使用 VPC 互連和 AWS PrivateLink 的組合，擴展消費者私有服務存取。

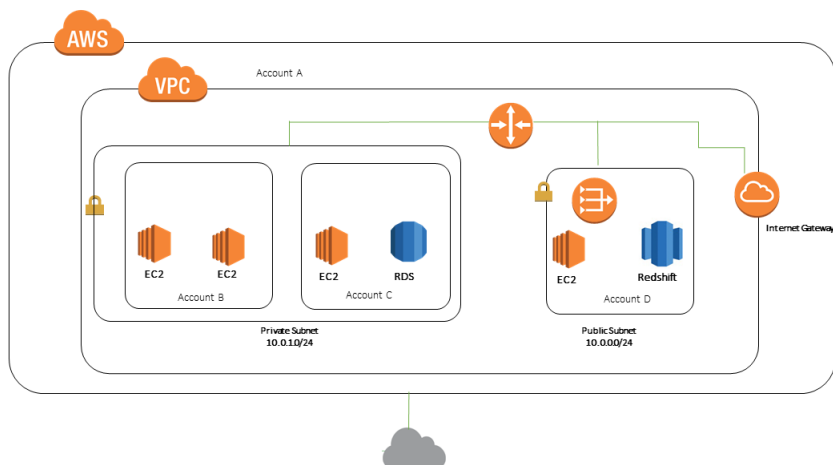
您也可以使用transit gateway來連接您的 VPC。

範例	用量
集中式路由器	您可將 transit gateway 設為集中式路由器，用以連接所有的 VPC、AWS Direct Connect 和 AWS Site-to-Site VPN 連接。  如需將您的transit gateway設定為集中式路由器的詳細資訊，請參閱《Amazon VPC 傳輸閘道》中的 <a href="#">傳輸閘道範例：集中式路由器</a> 。
隔離的 VPC	您可將transit gateway設為多個隔離路由器，這就類似於使用多個 transit gateways，但更具彈性，可讓路由和附件變更。  如需設定transit gateway以隔離 VPC 的詳細資訊，請參閱《Amazon VPC 傳輸閘道》中的 <a href="#">傳輸閘道範例：隔離的 VPC</a> 。
隔離 VPC 與共享服務	您可以將transit gateway設定為使用共享服務的多個隔離路由器。這就類似於使用多個transit gateways，但更具彈性，可讓路由和附件變更。  如需設定transit gateway以隔離 VPC 的詳細資訊，請參閱《Amazon VPC 傳輸閘道》中的 <a href="#">傳輸閘道範例：隔離 VPC 與共享服務</a> 。

## 範例：共享公有子網路和私有子網路

請考慮此案例，其中您想要讓一個帳戶負責基礎設施 (包括子網路、路由表、閘道和 CIDR 範圍)，並讓在同一 AWS 組織內的其他帳戶使用子網路。VPC 擁有者 (帳戶 A) 建立路由基礎設施，包括 VPC、子網路、路由表、閘道和網路 ACL。帳戶 D 想要建立面對大眾的應用程式。帳戶 B 和帳戶 C 想要建立的私有應用程式，不需要連線到網際網路，且位於私有子網路內。帳戶 A 可以使用 AWS Resource Access Manager 建立子網路的資源共享，然後共享子網路。帳戶 A 與帳戶 D 共享公有子網路，並與帳戶 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。各帳戶僅可看到與其共享的子網路，例如，帳戶 D 僅可看到公有子網路。各帳戶都可以控制其資源，包括執行個體和安全群組。

帳戶 A 管理 IP 基礎設施，包括公有子網路和私有子網路的路由表。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 (帳戶 ID 111111111111) 會與帳戶 D (444444444444) 共用公有子網路。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。

- 帳戶 ID 是 VPC 擁有者 (111111111111)，不同於帳戶 D 的 ID (444444444444)。
- 「shared」(已共享) 一字會在擁有者帳戶 ID 旁出現。

Create subnet

Actions

Filter by tags and attributes or search by keyword

<div><input type="checkbox"/></div>	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Route table	Default subnet	Owner
<div><input type="checkbox"/></div>		subnet-0bb1c79de301436ee	available	vpc-0ee975135d74bdcfe	10.0.0.0/24	251	rtb-0825a8caf09467ea8	No	111111111111 (S)

## 範例：使用的服務 AWS PrivateLink 和 VPC 對等

AWS PrivateLink 服務供應商會設定在其 VPC 中執行服務的執行個體，以網路負載平衡器做為前端。使用區域內 VPC 對等 (VPC 位於同一區域) 和區域間 VPC 對等 (VPC 位於不同區域) 結合 AWS PrivateLink，就能私有存取在所有 VPC 對等連線上的消費者。

遠端 VPC 中的消費者無法跨越對等連線使用 [私有 DNS \(p. 306\)](#) 名稱。然而，他們可以在 Route 53 上建立自己的私有託管區域，並將其連接到 VPC 以使用相同的私有 DNS 名稱。如需有關使用 transit gateway 結合 Amazon Route 53 Resolver，以在多重連接 VPC 與內部部署環境之間共用 PrivateLink 界面端點的資訊，請參閱 [將 AWS Transit Gateway 與 AWS PrivateLink 和 Amazon Route 53 Resolver 整合](#)。

以下是使用 AWS PrivateLink 和 VPC 對等的設定範例。

### 範例

- [範例：服務供應商設定服務 \(p. 57\)](#)
- [範例：服務消費者設定存取 \(p. 57\)](#)
- [範例：服務供應商設定橫跨區域的服務 \(p. 58\)](#)
- [範例：服務消費者設定跨區域存取 \(p. 59\)](#)

### 其他資源



下列主題可協助您設定範例所需的元件：

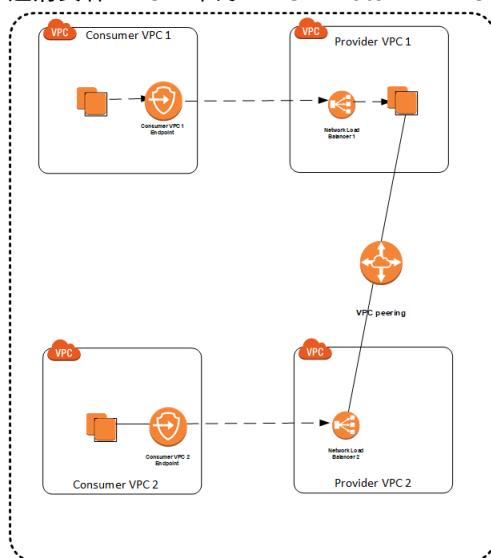
- [VPC 端點服務 \(AWS PrivateLink\) \(p. 294\)](#)
- [開始使用網路負載平衡器](#)
- [使用 VPC 互連連線](#)
- [建立界面端點 \(p. 272\)](#)

如需更多 VPC 互連範例，請參閱 Amazon VPC Peering Guide 中的下列主題：

- [VPC 互連組態](#)
- [不支援的 VPC 互連組態](#)

## 範例：服務供應商設定服務

請考量下列範例。在範例中，一項服務在供應商 VPC 1 的執行個體上執行。消費者 VPC 1 中的資源可以透過消費者 VPC 1 中的 AWS PrivateLink VPC 端點直接存取服務。

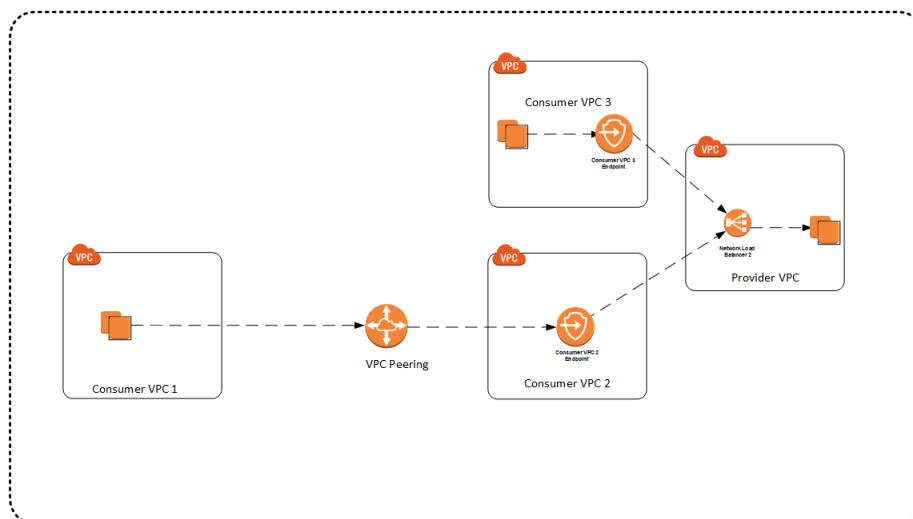


若要允許消費者 VPC 2 的資源私下存取此服務，服務供應者必須完成下列步驟：

1. 建立供應商 VPC 2。
2. 設定供應商 VPC 1 與供應商 VPC 2 之間的 VPC 互連，以便在兩個 VPC 之間路由流量。
3. 在供應商 VPC 2 中建立網路負載平衡器 2。
4. 設定網路負載平衡器 2 上的目標群組。這些目標群組指向在 VPC 1 中服務執行個體的 IP 地址。
5. 調整與供應商 VPC 1 中服務執行個體關聯的安全群組，讓這些安全群組允許來自於網路負載平衡器 2 的流量。
6. 在供應商 VPC 2 中建立 VPC 端點服務組態，並將此服務組態與網路負載平衡器 2 關聯。然後，服務取用者可以在 Consumer VPC 2 中建立介面端點，以連線 Provider VPC 2 中的服務。

## 範例：服務消費者設定存取

請考量下列範例。在範例中，一項服務在供應商 VPC 的執行個體上執行。在消費者 VPC 3 中的資源可以透過消費者 VPC 3 中的 AWS PrivateLink VPC 界面端點服務，直接存取此服務。

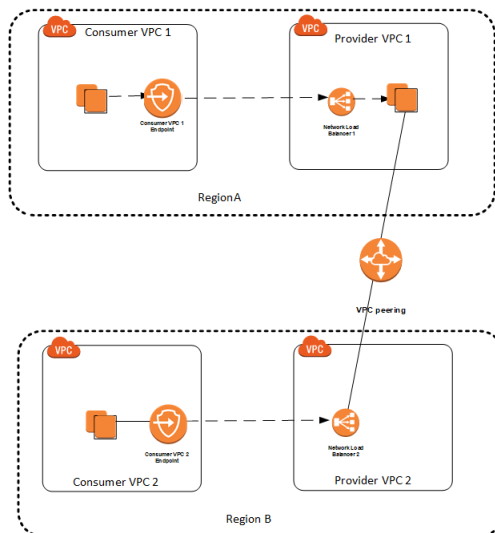


若要允許 Consumer VPC 1 中的資源私下存取服務 (不直接在 Consumer VPC 1 中建立介面端點)，服務使用者可以執行下列動作：

1. 建立消費者 VPC 2。
2. 建立遍及消費者 VPC 2 中一個或多個子網路的 VPC 介面端點。
3. 調整消費者 VPC 2 中與 VPC 端點服務關聯的安全群組，以允許來自於消費者 VPC 1 中執行個體的流量。調整與消費者 VPC 1 中執行個體關聯的安全群組，以允許流量前往消費者 VPC 2 中的 VPC 端點服務。
4. 設定消費者 VPC 1 與消費者 VPC 2 之間的 VPC 互連，以便在兩個 VPC 之間路由流量。

## 範例：服務供應商設定橫跨區域的服務

請考量下列範例。在範例中，一項服務在區域 A 中供應商 VPC 1 的執行個體上執行，例如 us-east-1 區域。在同一區域內，消費者 VPC 1 中的資源可以透過消費者 VPC 1 中的 AWS PrivateLink VPC 端點服務，直接存取此服務。



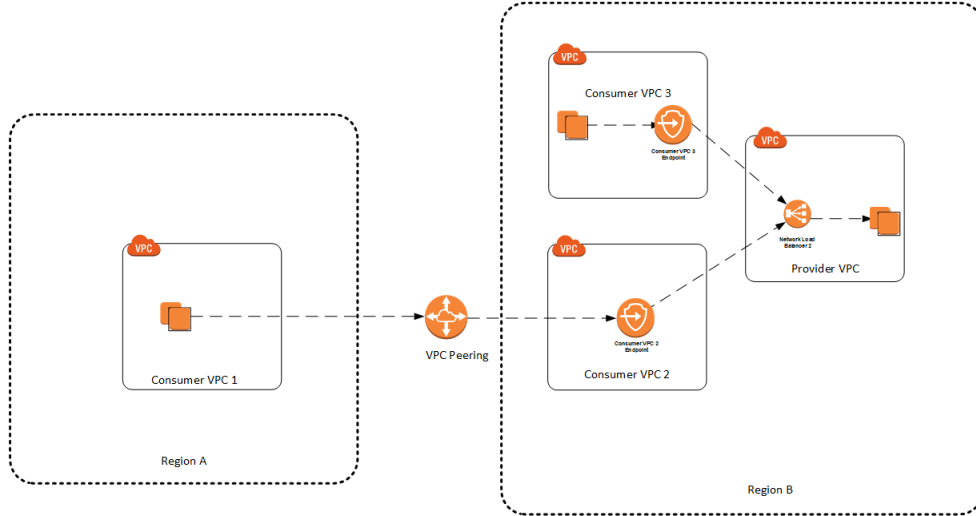
若要允許在區域 B (如 eu-west-2 區域) 中消費者 VPC 1 的資源私下存取此服務，服務供應商必須完成下列步驟：

1. 在區域 B 中建立供應商 VPC 2。
2. 設定供應商 VPC 1 與供應商 VPC 2 之間的 VPC 區域間互連，以便在兩個 VPC 之間路由流量。
3. 在供應商 VPC 2 中建立網路負載平衡器 2。
4. 設定 Network Load Balancer 2 上的目標群組。這些目標群組指向在 Provider VPC 1 中服務執行個體的 IP 地址。
5. 調整與供應商 VPC 1 中服務執行個體關聯的安全群組，讓這些安全群組允許來自於網路負載平衡器 2 的流量。
6. 在供應商 VPC 2 中建立 VPC 端點服務組態，並將此服務組態與網路負載平衡器 2 關聯。然後，服務取用者可以在 Consumer VPC 2 中建立介面端點，以連線 Provider VPC 2 中的服務。

供應商 2 的帳戶會產生區域間互連的數據傳輸費、網路負載平衡器費用。供應商 1 的帳戶則會產生服務執行個體費用。

## 範例：服務消費者設定跨區域存取

請考量下列範例。在範例中，一項服務在區域 B 中供應商 VPC 的執行個體上執行，例如 us-east-1 區域。在消費者 VPC 3 中的資源可以透過消費者 VPC 3 中的 AWS PrivateLink VPC 介面端點，直接存取此服務。



若要允許消費者 VPC 1 的資源私下存取此服務，服務消費者必須完成下列步驟：

1. 在區域 B 中建立消費者 VPC 2。
2. 建立遍及消費者 VPC 2 中一個或多個子網路的 VPC 介面端點。
3. 調整消費者 VPC 2 中與 VPC 端點服務關聯的安全群組，以允許來自於消費者 VPC 1 中執行個體的流量。調整與消費者 VPC 1 中執行個體關聯的安全群組，以允許流量前往消費者 VPC 2 中的 VPC 端點服務。
4. 設定消費者 VPC 1 與消費者 VPC 2 之間的 VPC 區域間互連，以便在兩個 VPC 之間路由流量。

設定完成後，消費者 VPC 1 可以私下存取服務。

消費者帳戶會產生區域間互連的數據傳輸費、VPC 端點的資料處理費用，以及 VPC 端點的按時計費。供應商則會產生網路負載平衡器費用，以及服務執行個體費用。

## 範例：使用 AWS CLI 建立 IPv4 VPC 及子網路

以下範例使用 AWS CLI 命令以 IPv4 CIDR 區塊建立非預設 VPC，以及在 VPC 中的公有及私有子網路。在您建立 VPC 和子網路後，您可以在公有子網路中啟動執行個體並連線到它。若要開始，您必須先安裝和設定 AWS CLI。如需詳細資訊，請參閱[安裝 AWS CLI](#)。

### 任務

- [步驟 1：建立 VPC 和子網路 \(p. 60\)](#)
- [步驟 2：將您的子網路設為公有 \(p. 60\)](#)
- [步驟 3：在子網路中啟動執行個體 \(p. 62\)](#)
- [步驟 4：清理 \(p. 64\)](#)

## 步驟 1：建立 VPC 和子網路

第一步是建立 VPC 和兩個子網路。此範例針對 VPC 使用 CIDR 區塊 10.0.0.0/16，但您可以選擇不同的 CIDR 區塊。如需詳細資訊，請參閱「[VPC 和子網路大小調整 \(p. 76\)](#)」。

使用 AWS CLI 建立 VPC 和子網路

1. 使用 10.0.0.0/16 CIDR 區塊建立 VPC。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

記下所傳回之輸出中的 VPC ID。

```
{
  "Vpc": {
    "VpcId": "vpc-2f09a348",
    ...
  }
}
```

2. 使用上一步的 VPC ID，使用 10.0.1.0/24 CIDR 區塊建立子網路。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24
```

3. 使用 10.0.0.0/24 CIDR 區塊在您的 VPC 中建立第二個子網路。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24
```

## 步驟 2：將您的子網路設為公有

在您建立 VPC 和子網路後，您可以透過將網際網路閘道連接到您的 VPC、建立自訂路由表，以及設定子網路導向網際網路閘道的路由，來將其中一個子網路設為公有子網路。

將您的子網路設為公有子網路

1. 建立網際網路閘道。

```
aws ec2 create-internet-gateway
```

記下所傳回之輸出中的網際網路閘道 ID。

```
{
  "InternetGateway": {
    ...
    "InternetGatewayId": "igw-1ff7a07b",
    ...
  }
}
```

2. 使用上一步的 ID，將網際網路閘道連接到您的 VPC。

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-id igw-1ff7a07b
```

3. 建立您 VPC 的自訂路由表。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

記下所傳回之輸出中的路由表 ID。

```
{
  "RouteTable": {
    ...
    "RouteTableId": "rtb-c1c8faa6",
    ...
  }
}
```

4. 在路由表中建立路由，將所有流量 (0.0.0.0/0) 指向網際網路閘道。

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0 --gateway-id igw-1ff7a07b
```

5. 若要確認路由已建立並在作用中，您可以描述路由表並檢視結果。

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{
  "RouteTables": [
    {
      "Associations": [],
      "RouteTableId": "rtb-c1c8faa6",
      "VpcId": "vpc-2f09a348",
      "PropagatingVgws": [],
      "Tags": [],
      "Routes": [
        {
          "GatewayId": "local",
          "DestinationCidrBlock": "10.0.0.0/16",
          "State": "active",
          "Origin": "CreateRouteTable"
        },
        {
          "GatewayId": "igw-1ff7a07b",
          "DestinationCidrBlock": "0.0.0.0/0",
          "State": "active",
          "Origin": "CreateRoute"
        }
      ]
    }
  ]
}
```

```
]
}
```

6. 路由表目前未與任何子網路建立關聯。您需要將路由表與您 VPC 中的子網路建立關聯，使來自該子網路的流量能路由到網際網路。首先，請使用 `describe-subnets` 命令取得您的子網路 ID。您可以使用 `--filter` 選項單獨傳回新 VPC 的子網路，以及使用 `--query` 選項單獨傳回子網路 ID 和其 CIDR 區塊。

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query
'Subnets[*].{ID:SubnetId,CIDR:CidrBlock}'
```

```
[
  {
    "CIDR": "10.0.1.0/24",
    "ID": "subnet-b46032ec"
  },
  {
    "CIDR": "10.0.0.0/24",
    "ID": "subnet-a46032fc"
  }
]
```

7. 您可以選擇哪些子網路要與自訂路由表建立關聯，例如 `subnet-b46032ec`。此子網路將會是您的公有子網路。

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-
c1c8faa6
```

8. 您可以選擇性地修改您子網路的公有 IP 定址行為，使在該子網路中啟動的執行個體都會自動接收到公有 IP 地址。否則，您應在啟動之後將彈性 IP 地址與您的執行個體建立關聯，使其可透過網際網路連接。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --map-public-ip-on-launch
```

## 步驟 3：在子網路中啟動執行個體

若要測試您的子網路已為公有，且子網路中的執行個體都可透過網際網路存取，請在您的公有子網路中啟動執行個體並與其連線。首先，您必須建立安全群組，與您的執行個體建立關聯，以及您用來連線到您執行個體的金鑰對。如需安全群組的詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。如需索引鍵組的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [Amazon EC2 索引鍵組](#)。

在您的公有子網路中啟動執行個體並與其連線

1. 建立金鑰對，然後使用 `--query` 選項和 `--output` 文字選項，將您的私有金鑰直接輸送到具有 `.pem` 副檔名的檔案。

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text
> MyKeyPair.pem
```

在此範例中，您會啟動一個 Amazon Linux 執行個體。如果您要在 Linux 或 Mac OS X 作業系統上使用 SSH 用戶端連線至您的執行個體，請使用下列命令設定私有金鑰檔案的許可，以便只有您能夠讀取該檔案。

```
chmod 400 MyKeyPair.pem
```

2. 在您的 VPC 中建立安全群組，然後新增規則以允許來自任何地方的 SSH 存取。

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{
  "GroupId": "sg-e1fb8c9a"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --protocol tcp --port 22 --cidr 0.0.0.0/0
```

#### Note

如果您使用 `0.0.0.0/0`，則可讓所有 IPv4 地址使用 SSH 存取您的執行個體。在這個簡短的練習中，此為可接受的做法。但在生產環境中，建議您只授權特定 IP 地址或特定範圍的地址。

3. 使用安全群組和您建立的金鑰對，在您的公有子網路中啟動執行個體。在輸出中，請記下您執行個體的執行個體 ID。

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-b46032ec
```

#### Note

在此範例中，AMI 為位於 US East (N. Virginia) 區域中的 Amazon Linux AMI。若您在不同的區域，您將需要您區域內合適 AMI 的 AMI ID。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [尋找 Linux AMI](#)。

4. 您的執行個體必須處於 `running` 狀態，才能進行連線。描述您的執行個體並確認其狀態，然後記下其公有 IP 地址。

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{
  "Reservations": [
    {
      ...
      "Instances": [
        {
          ...
          "State": {
            "Code": 16,
            "Name": "running"
          },
          ...
          "PublicIpAddress": "52.87.168.235",
          ...
        }
      ]
    }
  ]
}
```

5. 當您的執行個體處於執行中狀態時，您可以使用下列命令，於 Linux 或 Mac OS X 電腦上使用 SSH 用戶端與其連線：

```
ssh -i "MyKeyPair.pem" ec2-user@52.87.168.235
```



若您要從 Windows 電腦連線，請使用下列指示：[使用 PuTTY 從 Windows 連線到您的 Linux 執行個體](#)。

## 步驟 4：清理

在您確認您已連線到執行個體之後，若您不再需要執行個體，您可以加以終止。若要執行此作業，請使用 [terminate-instances](#) 命令。若要刪除其他您在此範例中建立的資源，請依照其列出的順序，使用下列命令：

1. 刪除您的安全群組：

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

2. 刪除您的子網路：

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. 刪除您的自訂路由表：

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

4. 將您的網際網路閘道與您的 VPC 分離：

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. 刪除您的網際網路閘道：

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. 刪除您的 VPC：

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

## 範例：使用 AWS CLI 建立 IPv6 VPC 及子網路

下列範例使用 AWS CLI 命令來建立具有 IPv6 CIDR 區塊、公有子網路和私有子網路的 VPC，並僅具有傳出網際網路存取。在您建立 VPC 和子網路後，您可以在公有子網路中啟動執行個體並連線到它。您可以啟動私有子網路中的執行個體，並確認它可以連線到網際網路。若要開始，您必須先安裝和設定 AWS CLI。如需詳細資訊，請參閱[安裝 AWS CLI](#)。

### 任務

- [步驟 1：建立 VPC 和子網路 \(p. 65\)](#)
- [步驟 2：設定公有子網路 \(p. 65\)](#)
- [步驟 3：設定輸出限定私有子網路 \(p. 67\)](#)
- [步驟 4：修改子網路的 IPv6 定址行為 \(p. 68\)](#)
- [步驟 5：在公有子網路中啟動執行個體 \(p. 68\)](#)
- [步驟 6：在私有子網路中啟動執行個體 \(p. 70\)](#)
- [步驟 7：清理 \(p. 71\)](#)

## 步驟 1：建立 VPC 和子網路

第一步是建立 VPC 和兩個子網路。此範例針對 VPC 使用 IPv4 CIDR 區塊 10.0.0.0/16，但您可以選擇不同的 CIDR 區塊。如需詳細資訊，請參閱「[VPC 和子網路大小調整 \(p. 76\)](#)」。

使用 AWS CLI 建立 VPC 和子網路

1. 建立包含 10.0.0.0/16 CIDR 區塊的 VPC，並將 IPv6 CIDR 區塊與此 VPC 建立關聯。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
```

記下所傳回之輸出中的 VPC ID。

```
{
  "Vpc": {
    "VpcId": "vpc-2f09a348",
    ...
  }
}
```

2. 說明您的 VPC 以取得與 VPC 相關聯的 IPv6 CIDR 區塊。

```
aws ec2 describe-vpcs --vpc-id vpc-2f09a348
```

```
{
  "Vpcs": [
    {
      ...
      "Ipv6CidrBlockAssociationSet": [
        {
          "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
          "AssociationId": "vpc-cidr-assoc-17a5407e",
          "Ipv6CidrBlockState": {
            "State": "ASSOCIATED"
          }
        }
      ],
      ...
    }
  ]
}
```

3. 建立具有 10.0.0.0/24 IPv4 CIDR 區塊和 2001:db8:1234:1a00::/64 IPv6 CIDR 區塊的子網路 (依據先前步驟傳回的範圍)。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24 --ipv6-cidr-block 2001:db8:1234:1a00::/64
```

4. 在 VPC 中建立具有 10.0.1.0/24 IPv4 CIDR 區塊和 2001:db8:1234:1a01::/64 IPv6 CIDR 區塊的第二個子網路。

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24 --ipv6-cidr-block 2001:db8:1234:1a01::/64
```

## 步驟 2：設定公有子網路

在您建立 VPC 和子網路後，您可以透過將網際網路閘道連接到您的 VPC、建立自訂路由表，以及設定子網路導向網際網路閘道的路由，來將其中一個子網路設為公有子網路。在此範例中，會建立一個路由表將所有 IPv4 流量和 IPv6 流量路由至網際網路閘道。

將您的子網路設為公有子網路

1. 建立網際網路閘道。

```
aws ec2 create-internet-gateway
```

記下所傳回之輸出中的網際網路閘道 ID。

```
{
  "InternetGateway": {
    ...
    "InternetGatewayId": "igw-1ff7a07b",
    ...
  }
}
```

2. 使用上一步的 ID，將網際網路閘道連接到您的 VPC。

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-id igw-1ff7a07b
```

3. 建立您 VPC 的自訂路由表。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

記下所傳回之輸出中的路由表 ID。

```
{
  "RouteTable": {
    ...
    "RouteTableId": "rtb-c1c8faa6",
    ...
  }
}
```

4. 在路由表中建立路由，將所有 IPv6 流量 (:::/0) 指向網際網路閘道。

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-ipv6-cidr-block ::/0 --gateway-id igw-1ff7a07b
```

#### Note

如果您也想要將公有子網路用於 IPv4 流量，則需要新增另一個用於 0.0.0.0/0 流量的路由，來指向網際網路閘道。

5. 若要確認路由已建立並在作用中，您可以描述路由表並檢視結果。

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{
  "RouteTables": [
    {
      "Associations": [],
      "RouteTableId": "rtb-c1c8faa6",
      "VpcId": "vpc-2f09a348",
      "PropagatingVgws": [],
      "Tags": [],
      "Routes": [
```

```
{
  "GatewayId": "local",
  "DestinationCidrBlock": "10.0.0.0/16",
  "State": "active",
  "Origin": "CreateRouteTable"
},
{
  "GatewayId": "local",
  "Origin": "CreateRouteTable",
  "State": "active",
  "DestinationIpv6CidrBlock": "2001:db8:1234:1a00::/56"
},
{
  "GatewayId": "igw-1ff7a07b",
  "Origin": "CreateRoute",
  "State": "active",
  "DestinationIpv6CidrBlock": "::/0"
}
]
}
]
```

6. 路由表目前未與任何子網路建立關聯。請將它與您 VPC 中的子網路建立關聯，使來自該子網路的流量能路由到網際網路閘道。首先，請說明您的子網路以取得其 ID。您可以使用 `--filter` 選項以僅傳回新 VPC 的子網路；使用 `--query` 選項以僅傳回子網路 ID 和其 IPv4 和 IPv6 CIDR 區塊。

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query
'Subnets[*].
{ID:SubnetId,IPv4CIDR:CidrBlock,IPv6CIDR:Ipv6CidrBlockAssociationSet[*].Ipv6CidrBlock}'
```

```
[
  {
    "IPv6CIDR": [
      "2001:db8:1234:1a00::/64"
    ],
    "ID": "subnet-b46032ec",
    "IPv4CIDR": "10.0.0.0/24"
  },
  {
    "IPv6CIDR": [
      "2001:db8:1234:1a01::/64"
    ],
    "ID": "subnet-a46032fc",
    "IPv4CIDR": "10.0.1.0/24"
  }
]
```

7. 您可以選擇哪些子網路要與自訂路由表建立關聯，例如 `subnet-b46032ec`。此子網路將會是您的公有子網路。

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-
c1c8faa6
```

## 步驟 3：設定輸出限定私有子網路

您可以將 VPC 中的第二個子網路設定為 IPv6 輸出限定私有子網路。此子網路中啟動的執行個體可使用輸出限定網際網路閘道，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連接您的執行個體。

將子網路設定為輸出限定私有子網路

1. 為您的 VPC 建立輸出限定網際網路閘道。記下傳回輸出中的閘道 ID。

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-2f09a348
```

```
{
  "EgressOnlyInternetGateway": {
    "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
    "Attachments": [
      {
        "State": "attached",
        "VpcId": "vpc-2f09a348"
      }
    ]
  }
}
```

2. 建立您 VPC 的自訂路由表。記下所傳回之輸出中的路由表 ID。

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

3. 在路由表中建立路由，將所有 IPv6 流量 (:::/0) 指向輸出限定網際網路閘道。

```
aws ec2 create-route --route-table-id rtb-abc123ab --destination-ipv6-cidr-block ::/0
--egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

4. 將路由表與 VPC 中的第二個子網路建立關聯 (您於上一節中描述的子網路)。這個子網路即為您的私有子網路，並具有輸出限定的 IPv6 網際網路存取權。

```
aws ec2 associate-route-table --subnet-id subnet-a46032fc --route-table-id rtb-abc123ab
```

## 步驟 4：修改子網路的 IPv6 定址行為

您可以修改子網路的 IP 定址行為，以讓於子網路中啟動的執行個體可以自動接收 IPv6 地址。當您在子網路中啟動執行個體時，便會從子網路的範圍指派單一 IPv6 地址給執行個體的主要網路界面 (eth0)。

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --assign-ipv6-address-on-creation
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-a46032fc --assign-ipv6-address-on-creation
```

## 步驟 5：在公有子網路中啟動執行個體

若要測試您的公有子網路是否已為公有且子網路中的執行個體都可透過網際網路存取，請在您的公有子網路中啟動執行個體並與其連線。首先，您必須建立安全群組，與您的執行個體建立關聯，以及您用來連線到您執行個體的金鑰對。如需安全群組的詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。如需金鑰對的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [Amazon EC2 金鑰對](#)。

在您的公有子網路中啟動執行個體並與其連線

1. 建立金鑰對，然後使用 --query 選項和 --output 文字選項，將您的私有金鑰直接輸送到具有 .pem 副檔名的檔案。

```
aws ec2 create-key-pair --key-name MyKeyPair --query 'KeyMaterial' --output text  
> MyKeyPair.pem
```

在此範例中，會啟動一個 Amazon Linux 執行個體。如果您要在 Linux 或 OS X 作業系統上使用 SSH 用戶端連線至您的執行個體，請使用下列命令設定私有金鑰檔案的許可，以便只有您能夠讀取該檔案。

```
chmod 400 MyKeyPair.pem
```

2. 為您的 VPC 建立安全群組，然後新增規則以允許來自任何 IPv6 地址的 SSH 存取。

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
  "GroupId": "sg-e1fb8c9a"  
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --ip-permissions  
'[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":  
  ":::/0"}]}]'
```

#### Note

如果您使用 `:::/0`，則可讓所有 IPv6 地址使用 SSH 存取您的執行個體。此作業用於簡短練習沒有問題，但在生產環境中，建議您只授權特定 IP 地址或特定範圍的地址來存取您的執行個體。

3. 使用安全群組和您建立的金鑰對，在您的公有子網路中啟動執行個體。在輸出中，請記下您執行個體的執行個體 ID。

```
aws ec2 run-instances --image-id ami-0de53d8956e8dcf80 --count 1 --instance-  
type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-  
b46032ec
```

#### Note

在此範例中，AMI 為位於 US East (N. Virginia) 區域中的 Amazon Linux AMI。若您在不同的區域，則需要區域內合適 AMI 的 AMI ID。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [尋找 Linux AMI](#)。

4. 您的執行個體必須處於 `running` 狀態，才能進行連線。說明您的執行個體並確認其狀態，然後記下其 IPv6 地址。

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

```
{  
  "Reservations": [  
    {  
      ...  
      "Instances": [  
        {  
          ...  
          "State": {  
            "Code": 16,  
            "Name": "running"  
          },  
          ...  
        }  
      ]  
    }  
  ]  
}
```

```
...
    "NetworkInterfaces": {
      "Ipv6Addresses": {
        "Ipv6Address": "2001:db8:1234:1a00::123"
      }
    }
  }
}
]
```

5. 當您的執行個體處於執行中狀態時，您可以在 Linux 上使用 SSH 用戶端，或在 OS X 電腦上使用下列命令與其連線。您的本機電腦必須已設定 IPv6 地址。

```
ssh -i "MyKeyPair.pem" ec2-user@2001:db8:1234:1a00::123
```

若您要從 Windows 電腦連線，請使用下列指示：[使用 PuTTY 從 Windows 連線到您的 Linux 執行個體](#)。

## 步驟 6：在私有子網路中啟動執行個體

若要測試輸出限定私有子網路中的執行個體是否可以存取網際網路，請在您的私有子網路中啟動執行個體，並使用公有子網路中的堡壘執行個體與其連線（您可以使用上一節啟動的執行個體）。首先，您必須為執行個體建立安全群組。安全群組必須具備兩個規則，一個允許堡壘執行個體使用 SSH 連線，另一個允許 ping6 命令 (ICMPv6 流量) 驗證確實無法從網際網路存取執行個體。

1. 在您的 VPC 中建立安全群組，然後新增兩個規則，一個允許從公有子網路中執行個體 IPv6 地址傳入的 SSH 存取，另一個允許所有 ICMPv6 流量：

```
aws ec2 create-security-group --group-name SSHAccessRestricted --description "Security group for SSH access from bastion" --vpc-id vpc-2f09a348
```

```
{
  "GroupId": "sg-aabb1122"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions '[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6": "2001:db8:1234:1a00::123/128"}]}]
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions '[{"IpProtocol": "58", "FromPort": -1, "ToPort": -1, "Ipv6Ranges": [{"CidrIpv6": "::/0"}]}]
```

2. 使用您建立的安全群組和您用來在公有子網路中啟動執行個體的相同金鑰對，在私有子網路中啟動執行個體。

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-aabb1122 --subnet-id subnet-a46032fc
```

使用 describe-instances 命令驗證執行個體正在執行，並取得其 IPv6 地址。

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路中的執行個體。針對 Linux，請使用下列命令：

```
ssh-add MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

針對 OS X，請使用下列命令：

```
ssh-add -K MyKeyPair.pem
```

```
ssh -A ec2-user@2001:db8:1234:1a00::123
```

針對 Windows，請使用下列指示：[設定 Windows \(PuTTY\) 的 SSH 代理程式轉送 \(p. 231\)](#)。使用公有子網路執行個體的 IPv6 地址連線到該執行個體。

4. 從公有子網路中的執行個體 (堡壘執行個體)，使用私有子網路的 IPv6 地址連線到該私有子網路中的執行個體：

```
ssh ec2-user@2001:db8:1234:1a01::456
```

5. 從私有執行個體中，針對已啟用 ICMP 的網站執行 ping6 命令，以測試您是否能連線至網際網路，例如：

```
ping6 -n ietf.org
```

```
PING ietf.org(2001:1900:3001:11::2c) 56 data bytes
64 bytes from 2001:1900:3001:11::2c: icmp_seq=1 ttl=46 time=73.9 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=2 ttl=46 time=73.8 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=3 ttl=46 time=73.9 ms
...
```

6. 若要測試網際網路上的主機是否無法連接您私有子網路中的執行個體，請從已啟用 IPv6 的電腦執行 ping6 命令。您應該會取得逾時回應。如果您取得有效的回應，就表示您的執行個體可透過網際網路存取；請檢查您私有子網路的相關聯路由表，並確認其中不含將 IPv6 流量傳到網際網路閘道的路由。

```
ping6 2001:db8:1234:1a01::456
```

## 步驟 7：清理

在您確認可以連線到公有子網路中的執行個體，且私有子網路中的執行個體可以存取網際網路之後，若您不再需要執行個體即可將其終止。若要執行此作業，請使用 [terminate-instances](#) 命令。若要刪除其他您在此範例中建立的資源，請依照其列出的順序，使用下列命令：

1. 刪除您的安全群組：

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

```
aws ec2 delete-security-group --group-id sg-aabb1122
```

2. 刪除您的子網路：

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```



```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. 刪除您的自訂路由表：

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

```
aws ec2 delete-route-table --route-table-id rtb-abc123ab
```

4. 將您的網際網路閘道與您的 VPC 分離：

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. 刪除您的網際網路閘道：

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. 刪除您的輸出限定網際網路閘道：

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

7. 刪除您的 VPC：

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

# VPC 和子網路

若要開始使用 Amazon Virtual Private Cloud (Amazon VPC)，您可以建立 VPC 和子網路。如需 Amazon VPC 的一般概觀，請參閱 [什麼是 Amazon VPC？](#) (p. 1)。

## 內容

- [VPC 和子網路基本概念](#) (p. 73)
- [VPC 和子網路大小調整](#) (p. 76)
- [子網路路由](#) (p. 81)
- [子網路安全](#) (p. 81)
- [使用 VPC 和子網路](#) (p. 81)
- [使用共用 VPC](#) (p. 89)
- [擴充您的 VPC](#) (p. 91)

## VPC 和子網路基本概念

虛擬私有雲端 (VPC) 是您 AWS 帳戶專用的虛擬網路。此虛擬網路在邏輯上與 AWS 雲端中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)。

當您建立 VPC 時，您必須以無類別網域間路由選擇 (CIDR) 區塊的格式，為 VPC 指定 IPv4 地址的範圍。例如：10.0.0.0/16。這是您 VPC 的主要 CIDR 區塊。如需 CIDR 表示法的詳細資訊，請參閱 [RFC 4632](#)。

下圖顯示使用 IPv4 CIDR 區塊的新 VPC。



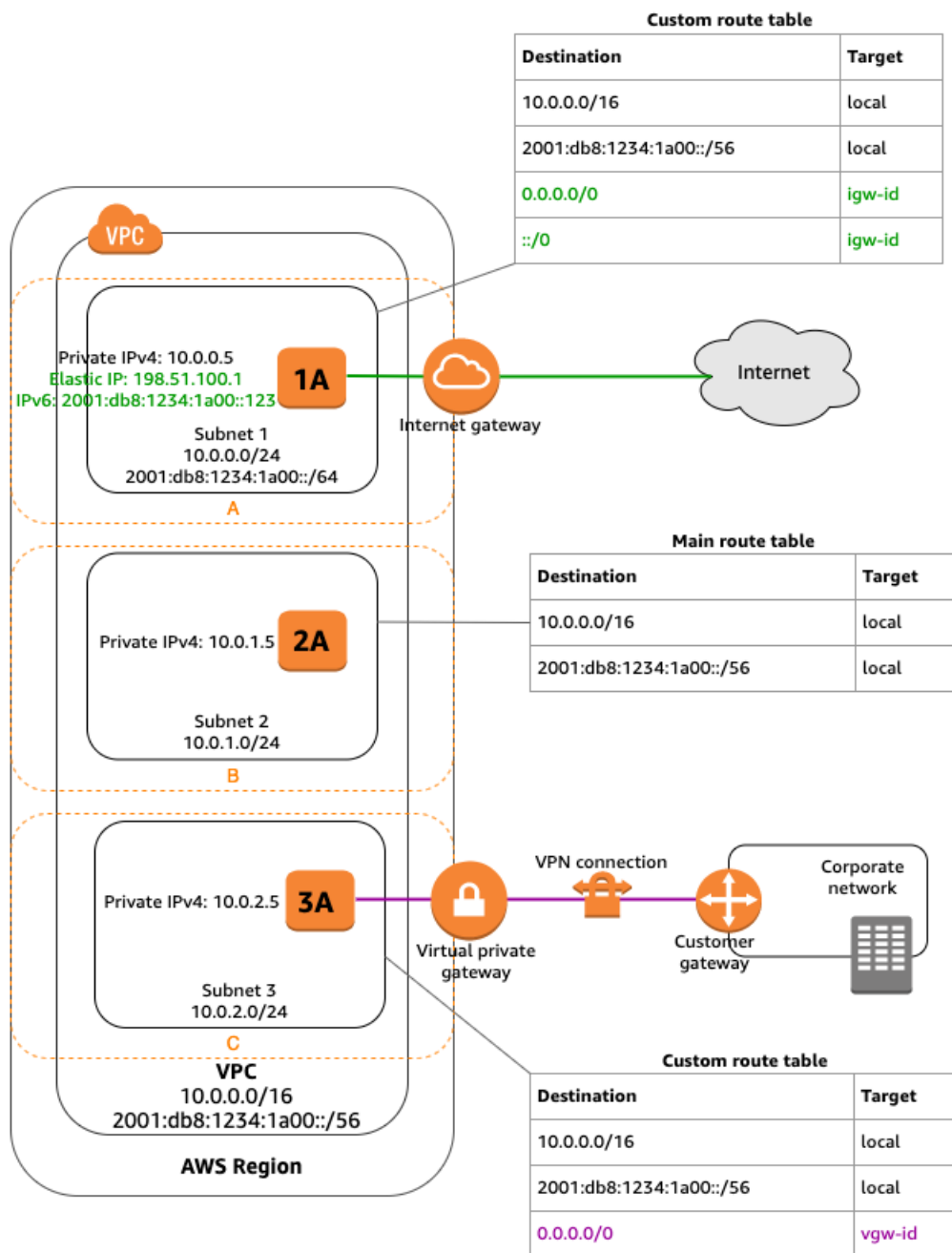
主路由表具有以下路由。

目的地	目標
10.0.0.0/16	區域

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或多個子網路。您可以選擇性地在本地區域中新增子網路，該區域是 AWS 基礎設施部署，可將運算、儲存體、資料庫和其他選取服務放在更接近使用者的位置。本地區域可讓您的使用者執行需要個位數毫秒延遲的應用程式。如需哪些區域支援本地區域的相關資訊，請參閱《Linux 執行個體的 Amazon EC2 使用者指南》中的[可用區域](#)。建立子網路時，您要為該子網路指定 CIDR 區塊，其即是 VPC CIDR 區塊的子網路。各個子網路必須完全位於某一可用區域內，不得跨越多個區域。可用區域是代表不同的位置，旨在隔離其他可用區域的故障。藉由在個別的可用區域中啟動執行個體，您就可以保護應用程式免於發生單點故障。我們會為每個子網路指派一個唯一 ID。

您也可以選擇將 IPv6 CIDR 區塊指派給您的 VPC，以及將 IPv6 CIDR 區塊指派給您的子網路。

下表顯示已在多個可用區域內使用子網路設定的 VPC。1A、2A 和 3A 是您 VPC 中的執行個體。IPv6 CIDR 區塊與 VPC 相關聯，另一個 IPv6 CIDR 區塊則與子網路 1 相關聯。網際網路閘道會啟用網際網路通訊，而虛擬私有網路 (VPN) 連線則會啟用與您企業網路的通訊。



若子網路的流量路由至網際網路閘道，則該子網路便稱為公有子網路。在此圖中，子網路 1 即是公有子網路。若您希望您在公有子網路中的執行個體透過 IPv4 與網際網路通訊，它必須具備公有 IPv4 地址或彈性 IP 地址 (IPv4)。如需公有 IPv4 地址的詳細資訊，請參閱[公有 IPv4 地址 \(p. 103\)](#)。若您希望您在公有子網路中的執行個體透過 IPv6 與網際網路通訊，它必須具備 IPv6 地址。

若子網路沒有導向網際網路閘道的路由，則該子網路便稱為私有子網路。在此圖中，子網路 2 即是私有子網路。

若子網路沒有導向網際網路閘道的路由，但其流量會路由至 Site-to-Site VPN 連接的虛擬私有閘道，則該子網路便稱為僅 VPN 子網路。在此圖中，子網路 3 即是僅 VPN 子網路。目前，我們不支援透過 Site-to-Site VPN 連接的 IPv6 流量。

如需詳細資訊，請參閱 AWS Site-to-Site VPN 使用者指南中的 [VPC 的範例 \(p. 55\)](#)、[網際網路閘道 \(p. 212\)](#) 和 [什麼是 AWS Site-to-Site VPN ?](#)。

#### Note

無論子網路的類型為何，子網路的內部 IPv4 地址範圍一律為私有，我們不會向網際網路公告地址區塊。

您能夠在您帳戶中建立的 VPC 和子網路數目具有配額。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。

## VPC 和子網路大小調整

Amazon VPC 支援 IPv4 和 IPv6 定址，其分別具有不同的 CIDR 區塊大小配額。根據預設，所有 VPC 和子網路都必須具有 IPv4 CIDR 區塊 — 您無法變更此行為。您可以選擇性地建立 IPv6 CIDR 區塊與您 VPC 的關聯。

如需 IP 定址的詳細資訊，請參閱 [您 VPC 中的 IP 定址 \(p. 102\)](#)。

#### 內容

- [IPv4 的 VPC 和子網路規模 \(p. 76\)](#)
- [將 IPv4 CIDR 區塊新增至 VPC \(p. 77\)](#)
- [IPv6 的 VPC 和子網路規模 \(p. 80\)](#)

## IPv4 的 VPC 和子網路規模

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，您可以將輔助 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 VPC \(p. 77\)](#)。

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 前綴)	您的 VPC 必須是 /16 或更小，例如 10.0.0.0/16。
172.16.0.0 – 172.31.255.255 (172.16/12 前綴)	您的 VPC 必須是 /16 或更小，例如 172.31.0.0/16。
192.168.0.0 – 192.168.255.255 (192.168/16 前綴)	您的 VPC 可以更小，例如 192.168.0.0/20。

您可以使用位在 RFC 1918 指定之私有 IPv4 地址範圍之外的可公開路由 CIDR 區塊建立 VPC。但是，基於本文件的用途，我們在此提到的私有 IP 地址都是指位在您 VPC 的 CIDR 範圍內的 IPv4 地址。

#### Note

若您要建立 VPC 搭配其他 AWS 服務使用，請檢查服務的文件，確認 IP 地址範圍或聯網元件是否有特定需求。

子網路的 CIDR 區塊可以和 VPC 的 CIDR 區塊相同 (適用於 VPC 中的單子網路)，或是與 VPC 的 CIDR 區塊子集相同 (適用於多個子網路)。允許的區塊大小介於 /28 網路遮罩和 /16 網路遮罩之間。若您在 VPC 中建立超過一個子網路，子網路的 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 區塊拆成兩個子網路，每個子網路都支援 128 個 IP 地址。其中一個子網路使用 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)。

網際網路上有可用的工具可協助您計算和建立 IPv4 子網路 CIDR 區塊；例如 [IPv4 位址規劃工具](#)。您可以搜尋符合需求的其他工具，例如「子網路計算器」或「CIDR 計算器」。您的網路工程群組可協助您判斷要為您的子網路指定的 CIDR 區塊。

您無法使用每個子網路 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 地址指派給執行個體。例如，在使用 CIDR 區塊 10.0.0.0/24 的子網路中，會預留下述五個 IP 地址：

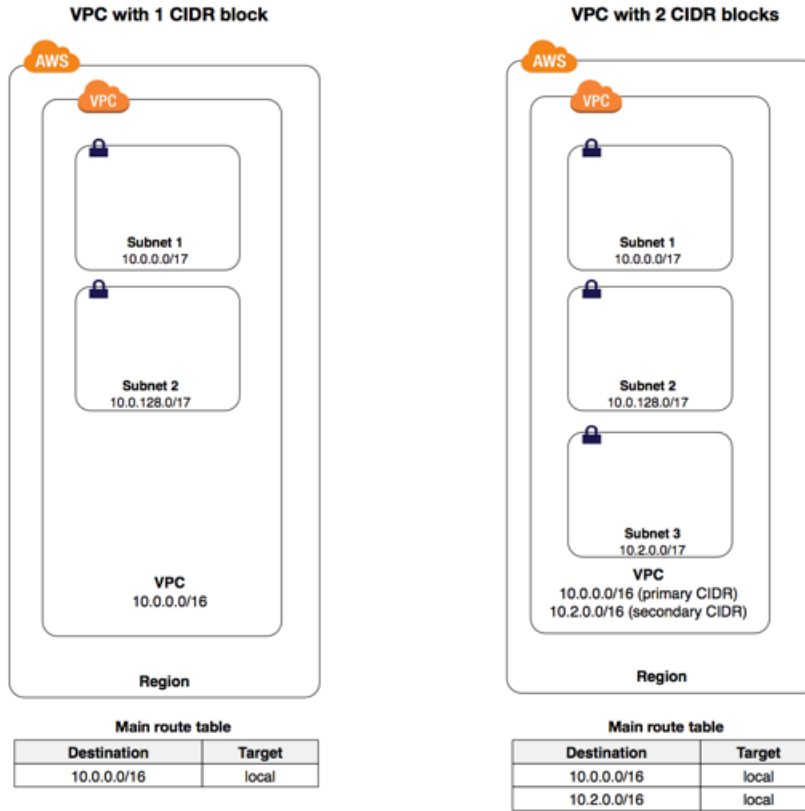
- 10.0.0.0：網路地址。
- 10.0.0.1：由 AWS 為 VPC 路由器預留。
- 10.0.0.2：由 AWS 預留。DNS 伺服器的 IP 地址是 VPC 網路範圍的基礎加 2。針對使用多個 CIDR 區塊的 VPC，DNS 伺服器的 IP 地址會位於主要 CIDR。我們也會為 VPC 中的所有 CIDR 區塊保留每個子網路範圍的基礎加 2。如需詳細資訊，請參閱[Amazon DNS 伺服器 \(p. 253\)](#)。
- 10.0.0.3：由 AWS 預留，供日後使用。
- 10.0.0.255：網路廣播地址。我們不支援在 VPC 中廣播，因此我們會預留此地址。

如果您使用命令列工具或 Amazon EC2 API 建立 VPC 或子網路，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 100.68.0.0/18 的 CIDR 區塊。

## 將 IPv4 CIDR 區塊新增至 VPC

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，位於左側的 VPC 具有單一 CIDR 區塊 (10.0.0.0/16) 及兩個子網路。位於右側的 VPC 則代表您新增第二個 CIDR 區塊 (10.2.0.0/16) 並從第二個 CIDR 的範圍建立新的子網路後，相同 VPC 的架構。



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 \(p. 79\)](#)。
- 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。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。
- 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。
- 若您為 ClassicLink 啟用 VPC，您可以與介於 10.0.0.0/16 和 10.1.0.0/16 範圍之間的 CIDR 區塊建立關聯，但您無法與任何來自 10.0.0.0/8 範圍的其他 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 互連連線一部分的 VPC 時套用：
  - 若 VPC 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 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 的擁有者必須接受互連連線，否則申請者 VPC 的擁有者必須刪除 VPC 互連連線請求、新增 CIDR 區塊，然後請求新的 VPC 互連連線。
  - 若 VPC 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 互連連線會失敗，無法獲得接受。
- 若您使用 AWS Direct Connect 透過直接連線閘道連線到多個 VPC，則與直接連線閘道相關聯的 VPC 不可擁有重疊的 CIDR 區塊。若您將 CIDR 區塊新增到其中一個與直接連線閘道建立關聯的 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[直接連線閘道](#)。

- 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。

下表提供允許及限制的 CIDR 區塊關聯概觀，其會根據您 VPC 主要 CIDR 區塊存在的 IPv4 地址範圍。

#### IPv4 CIDR 區塊關聯限制

您主要 VPC CIDR 區塊存在的 IP 地址範圍	限制的 CIDR 區塊關聯	允許的 CIDR 區塊關聯
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>若您的主要 CIDR 區塊位於 10.0.0.0/15 範圍內，您便無法新增來自 10.0.0.0/16 範圍的 CIDR 區塊。</p> <p>來自 198.19.0.0/16 範圍的 CIDR 區塊。</p>	<p>任何其他來自 10.0.0.0/8 範圍，未受限制的 CIDR。</p> <p>任何可公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊。</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>來自 198.19.0.0/16 範圍的 CIDR 區塊。</p>	<p>任何其他來自 172.16.0.0/12 範圍，未受限制的 CIDR。</p> <p>任何可公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊。</p>
192.168.0.0/16	<p>來自其他 RFC 1918* 範圍 (172.16.0.0/12 及 10.0.0.0/8) 的 CIDR 區塊。</p> <p>來自 198.19.0.0/16 範圍的 CIDR 區塊。</p>	<p>任何其他來自 192.168.0.0/16 範圍的 CIDR 區塊。</p> <p>任何可公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊。</p>
198.19.0.0/16	<p>來自 RFC 1918* 範圍的 CIDR 區塊。</p>	<p>任何可公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊。</p>
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。	<p>來自 RFC 1918* 範圍的 CIDR 區塊。</p> <p>來自 198.19.0.0/16 範圍的 CIDR 區塊。</p>	<p>任何其他可公開路由的 IPv4 CIDR 區塊 (非 RFC 1918)，或是來自 100.64.0.0/10 範圍的 CIDR 區塊。</p>

\*RFC 1918 範圍是 [RFC 1918](#) 中指定的私有 IPv4 地址範圍。

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 主控台中檢視您 VPC 的主要 CIDR，請選擇 Your VPCs



(您的 VPC)、選取您的 VPC，然後記下 CIDR blocks (CIDR 區塊) 下的第一個項目。或者，您可以使用 [describe-vpcs](#) 命令：

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d
```

在傳回的輸出中，主要 CIDR 會在最上層 CidrBlock 元素中傳回 (下方範例輸出中的倒數第二個元素)。

```
{
  "Vpcs": [
    {
      "VpcId": "vpc-1a2b3c4d",
      "InstanceTenancy": "default",
      "Tags": [
        {
          "Value": "MyVPC",
          "Key": "Name"
        }
      ],
      "CidrBlockAssociations": [
        {
          "AssociationId": "vpc-cidr-assoc-3781aa5e",
          "CidrBlock": "10.0.0.0/16",
          "CidrBlockState": {
            "State": "associated"
          }
        },
        {
          "AssociationId": "vpc-cidr-assoc-0280ab6b",
          "CidrBlock": "10.2.0.0/16",
          "CidrBlockState": {
            "State": "associated"
          }
        }
      ],
      "State": "available",
      "DhcpOptionsId": "dopt-e0fe0e88",
      "CidrBlock": "10.0.0.0/16",
      "IsDefault": false
    }
  ]
}
```

## IPv6 的 VPC 和子網路規模

您可以將單一 IPv6 CIDR 區塊與您帳戶中的現有 VPC，或是在您建立新的 VPC 時建立關聯。CIDR 區塊是 /56 的固定前綴長度。您可以從 Amazon 的 IPv6 地址集區中申請 IPv6 CIDR 區塊。

若您已將 IPv6 CIDR 區塊與您的 VPC 建立關聯，您可以將 IPv6 CIDR 區塊與您 VPC 中的現有子網路，或是在您建立新的子網路時建立關聯。子網路的 IPv6 CIDR 區塊是 /64 的固定前綴長度。

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。您可以建立子網路，並關聯來自此範圍的 IPv6 CIDR 區塊；例如：2001:db8:1234:1a00::/64。

網際網路上有可用的工具可協助您計算和建立 IPv6 子網路 CIDR 區塊；例如 [IPv6 位址規劃工具](#)。您可以搜尋符合您需求的其他工具，例如「IPv6 子網路計算器」或「IPv6 CIDR 計算器」。此外，您的網路工程群組可協助您判斷要為您的子網路指定的 IPv6 CIDR 區塊。

您可以取消 IPv6 CIDR 區塊與子網路的關聯，也可以取消 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。

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

- 2001:db8:1234:1a00::
- 2001:db8:1234:1a00::1
- 2001:db8:1234:1a00::2
- 2001:db8:1234:1a00::3
- 2001:db8:1234:1a00:ffff:ffff:ffff:ffff

## 子網路路由

每個子網路都必須具有關聯的路由表，指定離開子網路之傳出流量的允許路由。每個您建立的子網路都會自動與 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[路由表](#) (p. 184)。

在先前的圖中，與子網路 1 相關聯的路由表會將所有 IPv4 流量 (0.0.0.0/0) 和 IPv6 流量 (:::/0) 路由至網際網路閘道 (例如，igw-1a2b3c4d)。由於執行個體 1A 具有 IPv4 彈性 IP 位址和 IPv6 位址，因此可以透過 IPv4 和 IPv6 從網際網路連線。

### Note

(僅限 IPv4) 與您執行個體相關聯的彈性 IPv4 地址或公有 IPv4 地址可透過您 VPC 的網際網路閘道存取。通過您執行個體和另一個網路之間 AWS Site-to-Site VPN 連接的流量會周遊虛擬私有閘道，而非網際網路閘道，因此不會存取彈性 IPv4 地址或公有 IPv4 地址。

執行個體 2A 無法觸達網際網路，但可觸達 VPC 中的其他執行個體。您可以使用網路位址轉譯 (NAT) 閘道或執行個體，允許您 VPC 中的執行個體初始化透過 IPv4 的網際網路傳出連線，但防止來自網際網路未經要求的傳入連線。因為您只能配置有限數目的彈性 IP 地址，若您擁有更多需要靜態公有 IP 地址的執行個體，我們建議您使用 NAT 裝置。如需詳細資訊，請參閱[NAT](#) (p. 226)。若要初始化透過 IPv6 僅傳出至網際網路的通訊，您可以使用僅限輸出網際網路閘道。如需詳細資訊，請參閱[輸出限定網際網路閘道](#) (p. 218)。

與子網路 3 相關聯的路由表會將所有 IPv4 流量 (0.0.0.0/0) 路由至虛擬私有閘道 (例如，vgw-1a2b3c4d)。執行個體 3A 可透過 Site-to-Site VPN 連接觸達企業網路中的電腦。

## 子網路安全

AWS 提供兩項功能，可用於提升 VPC 中的安全性：安全群組和網路 ACL。安全群組控制執行個體的傳入與傳出流量，網路 ACL 則是控制子網路的傳入與傳出流量。在大部分情況下，安全群組可以符合您的需求；然而，如果您想讓 VPC 多一層安全，也可以使用網路 ACL。如需詳細資訊，請參閱[Amazon VPC 中的網際網路流量隱私權](#) (p. 122)。

根據設計，每個子網路都必須與一個網路 ACL 相關聯。每個您建立的子網路都會自動與 VPC 的預設網路 ACL 建立關聯。您可以變更關聯，也可以變更預設網路 ACL 的內容。如需詳細資訊，請參閱[網路 ACL](#) (p. 146)。

您可以在您的 VPC 或子網路上建立流程日誌，以擷取流入或流出您 VPC 或子網路中網路界面的流量。您也可以在各別網路界面上建立流程日誌。流程日誌會發佈至 CloudWatch Logs 或 Amazon S3。如需詳細資訊，請參閱[VPC 流程日誌](#) (p. 158)。

## 使用 VPC 和子網路

下列程序適用於手動建立 VPC 和子網路。您也必須手動新增閘道和路由表。或者，您可以使用 Amazon VPC 精靈，僅使用一個步驟來建立 VPC 和其子網路、閘道及路由表。如需詳細資訊，請參閱「[VPC 的範例](#) (p. 55)」。

#### 工作

- [建立 VPC \(p. 82\)](#)
- [在您的 VPC 中建立子網路 \(p. 83\)](#)
- [將輔助 IPv4 CIDR 區塊與您的 VPC 建立關聯 \(p. 84\)](#)
- [建立 IPv6 CIDR 區塊與 VPC 的關聯 \(p. 84\)](#)
- [建立 IPv6 CIDR 區塊與子網路的關聯 \(p. 85\)](#)
- [在您的子網路中啟動執行個體 \(p. 85\)](#)
- [刪除您的子網路 \(p. 86\)](#)
- [取消 IPv4 CIDR 區塊與您 VPC 的關聯 \(p. 86\)](#)
- [取消 IPv6 CIDR 區塊與您 VPC 或子網路的關聯 \(p. 87\)](#)
- [刪除您的 VPC \(p. 88\)](#)

## 建立 VPC

您可以使用 Amazon VPC 主控台來建立空白 VPC。

#### 使用主控台建立 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)、Create VPC (建立 VPC)。
3. 視需要指定下列 VPC 詳細資料。
  - Name tag (名稱標籤)：選擇性提供您 VPC 的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
  - IPv4 CIDR block (IPv4 CIDR 區塊)：指定 VPC 的 IPv4 CIDR 區塊。您可以指定的最小 CIDR 區塊是 /28，而最大的是 /16。我們建議您從 [RFC 1918](#) 中指定的私有 (非可公開路由) IP 地址範圍指定 CIDR 區塊；例如，10.0.0.0/16 或 192.168.0.0/16。

#### Note

您可以指定公開可路由傳送的 IPv4 位址範圍。但是，我們目前不支援從 VPC 中公開可路由傳送的 CIDR 區塊直接存取網際網路。若使用介於 224.0.0.0 和 255.255.255.255 之間 (類別 D 和類別 E IP 地址範圍) 的範圍在 VPC 中啟動，則 Windows 執行個體將無法正常開機。

- IPv6 CIDR 區塊：您可以選擇性地建立 IPv6 CIDR 區塊與您 VPC 的關聯。選擇下列其中一個選項，然後選擇選取 CIDR：
  - Amazon-provided IPv6 CIDR block (Amazon 提供的 IPv6 CIDR 區塊)：向 Amazon 的 IPv6 地址集區申請 IPv6 CIDR 區塊。對於網路邊界群組，請選取 AWS 公告 IP 位址的群組。
  - 我擁有的 IPv6 CIDR：([BYOIP](#)) 從您的 IPv6 地址集區配置 1 個 IPv6 CIDR 區塊。在 Pool (集區) 中，選擇要從中配置 IPv6 CIDR 區塊的 IPv6 地址集區。
- Tenancy (租用)：選取租用選項。專用租用可確保您的執行個體執行於單一租用用戶的硬體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [專用執行個體](#)。
- (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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。

4. 選擇 Create (建立)。

或者，您可以使用命令列工具。

使用命令列工具建立 VPC

- [create-vpc](#) (AWS CLI)
- [New-EC2Vpc](#) (適用於 Windows PowerShell 的 AWS 工具)

使用命令列工具說明 VPC

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (適用於 Windows PowerShell 的 AWS 工具)

若需 IP 地址的詳細資訊，請參閱[您 VPC 中的 IP 定址 \(p. 102\)](#)。

建立 VPC 後，您可以建立子網路。如需更多詳細資訊，請參閱 [在您的 VPC 中建立子網路 \(p. 83\)](#)。

## 在您的 VPC 中建立子網路

若要將新的子網路新增到您的 VPC，您必須從您 VPC 的範圍中，指定子網路的 IPv4 CIDR 區塊。您可以指定您希望子網路存在的可用區域。您可以在相同的可用區域內擁有多個子網路。

若您的 VPC 有和 IPv6 CIDR 區塊相關聯，您可以選擇性的為您的子網路指定 IPv6 CIDR 區塊。

若要在本機區域或 Wavelength 區域中建立子網路，您必須啟用「區域」。如需如何啟用 Wavelength 區域的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的[啟用區域](#)。

使用主控台來將子網路新增到您的 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 (子網路)、Create subnet (建立子網路)。
3. 視需要指定子網路詳細資訊，然後選擇 Create (建立)。
  - 名稱標籤：選擇性提供您子網路的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
  - VPC：選擇您希望為其建立子網路的 VPC。
  - 可用區域：選擇性的選擇您子網路存在的可用區域，或是使用預設的無偏好設定，讓 AWS 為您選擇可用區域。

如需有關「區域」和「區域」的資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的[區域和區域](#)。

  - IPv4 CIDR 區塊：指定您子網路的 IPv4 CIDR 區塊，例如：10.0.1.0/24。如需詳細資訊，請參閱[IPv4 的 VPC 和子網路規模 \(p. 76\)](#)。
  - IPv6 CIDR 區塊：(選用) 若您已將 IPv6 CIDR 區塊與您的 VPC 建立關聯，請選擇 Specify a custom IPv6 CIDR (指定自訂 IPv6 CIDR)。指定子網路的十六進位對值，或是使用預設值。
4. (選用) 若需要的話，重複以上步驟來在您的 VPC 中建立更多子網路。

或者，您可以使用命令列工具。

使用命令列工具新增子網路

- [create-subnet](#) (AWS CLI)
- [New-EC2Subnet](#) (適用於 Windows PowerShell 的 AWS 工具)

### 使用命令列工具說明子網路

- [describe-subnets](#) (AWS CLI)
- [Get-EC2Subnet](#) (適用於 Windows PowerShell 的 AWS 工具)

建立子網路後，您可以執行下列作業：

- 設定您的路由。若要將您的子網路設為公有子網路，您必須將網際網路閘道連接到您的 VPC。如需詳細資訊，請參閱[建立並連接網際網路閘道](#) (p. 215)。您接著可以建立自訂路由表，將路由新增到網際網路閘道。如需詳細資訊，請參閱「[建立自訂路由表](#) (p. 215)」。
- 修改子網路設定，以指定所有在該子網路啟動的執行個體接收公有 IPv4 地址或 IPv6 地址，或是兩者。如需詳細資訊，請參閱[您子網路的 IP 定址行為](#) (p. 104)。
- 依需要建立或修改您的安全群組。如需詳細資訊，請參閱[VPC 的安全群組](#) (p. 138)。
- 依需要建立或修改您的網路 ACL。如需詳細資訊，請參閱[網路 ACL](#) (p. 146)。
- 與其他帳戶共享子網路。如需詳細資訊，請參閱[???](#) (p. 89)。

## 將輔助 IPv4 CIDR 區塊與您的 VPC 建立關聯

您可以將另一個 IPv4 CIDR 區塊新增至您的 VPC。請確認您已詳閱適用的[限制](#) (p. 77)。

在您建立與 CIDR 區塊的關聯後，狀態會成為 associating。當其處於 associated 狀態時，表示 CIDR 區塊已準備好可供使用。

使用主控台來將 CIDR 區塊新增到您的 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 IPv4 CIDR (新增 IPv4 CIDR)，然後輸入要新增的 CIDR 區塊，例如 10.2.0.0/16。選擇核取圖示。
5. 選擇 Close (關閉)。

或者，您可以使用命令列工具。

使用命令列工具新增 CIDR 區塊

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)

在依需要新增 IPv4 CIDR 區塊之後，您可以建立子網路。如需更多詳細資訊，請參閱[在您的 VPC 中建立子網路](#) (p. 83)。

## 建立 IPv6 CIDR 區塊與 VPC 的關聯

您可以建立 IPv6 CIDR 區塊與任何現有 VPC 的關聯。VPC 不可擁有任何已和其建立關聯的現有 IPv6 CIDR 區塊。

使用主控台建立 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，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 選擇 Add IPv6 CIDR (新增 IPv6 CIDR)。
5. 選擇 Add IPv6 CIDR (新增 IPv6 CIDR)。
6. 對於 IPv6 CIDR block (IPv6 CIDR 區塊)，請選擇下列其中一項，然後選擇 Select CIDR (選取 CIDR)：
  - Amazon-provided IPv6 CIDR block (Amazon 提供的 IPv6 CIDR 區塊：向 Amazon 的 IPv6 地址集區申請 IPv6 CIDR 區塊。
  - IPv6 CIDR owned by me (我擁有的 IPv6 CIDR)：(BYOIP) 從您的 IPv6 地址集區配置個 IPv6 CIDR 區塊。在 Pool (集區) 中，選擇要從中配置 IPv6 CIDR 區塊的 IPv6 地址集區。
7. 如果您已選取 Amazon-provided IPv6 CIDR block (Amazon 提供的 IPv6 CIDR 區塊)，請從 Network Border Group (網路邊界群組)，選取 AWS 公告 IP 地址的來源群組。
8. 選擇 Select CIDR (選取 CIDR)。
9. 選擇 Close (關閉)。

或者，您可以使用命令列工具。

使用命令列工具建立 IPv6 CIDR 區塊與 VPC 的關聯

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)

## 建立 IPv6 CIDR 區塊與子網路的關聯

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。

使用主控台建立 IPv6 CIDR 區塊與子網路的關聯

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 (子網路)。
3. 選取您的子網路，然後選擇 Subnet Actions (子網路動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 選擇 Add IPv6 CIDR (新增 IPv6 CIDR)。指定子網路的十六進位對 (例如，00)，然後透過選擇核取圖示來確認項目。
5. 選擇 Close (關閉)。

或者，您可以使用命令列工具。

使用命令列工具建立 IPv6 CIDR 區塊與子網路的關聯

- [associate-subnet-cidr-block](#) (AWS CLI)
- [Register-EC2SubnetCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)

## 在您的子網路中啟動執行個體

建立您的子網路並設定您的路由之後，您可以使用 Amazon EC2 主控台在您的子網路中啟動執行個體。

使用主控台在您的子網路中啟動執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。



2. 在儀表板上，選擇 Launch Instance (啟動執行個體)。
3. 請遵循精靈的指示進行。選取 AMI 和執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體的詳細資訊)。

#### Note

如果您希望您的執行個體透過 IPv6 通訊，您必須選取支援的執行個體類型。所有目前世代的執行個體類型皆支援 IPv6 地址。

4. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，確認您已在 Network (網路) 清單中選取需要的 VPC，然後選取要在其中啟動執行個體的字網路。維持其他在此頁面上的預設設定，然後選擇 Next: Add Storage (下一步：新增儲存體)。
5. 在精靈的下一頁上，您可以為您的執行個體設定儲存體並新增標籤。在 Configure Security Group (設定安全群組) 頁面上，您可以從您擁有的任何現有安全群組中選擇，或是遵循精靈的指示建立新的安全群組。完成時，選擇 Review and Launch (檢閱及啟動)。
6. 檢閱您的設定，然後選擇 Launch (啟動)。
7. 選取您擁有的現有金鑰對，或是建立新的金鑰對，然後在完成時選擇 Launch Instances (啟動執行個體)。

或者，您可以使用命令列工具。

使用命令列工具在您的子網路中啟動執行個體

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (適用於 Windows PowerShell 的 AWS 工具)

## 刪除您的子網路

若您不再需要您的子網路，您可以刪除它。您必須先終止子網路中的任何執行個體。

使用主控台來刪除您的子網路

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 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 (子網路)。
5. 選取要刪除的子網路，然後選擇 Actions (動作)、Delete subnet (刪除子網路)。
6. 在 Delete Subnet (刪除子網路) 對話方塊中，選擇 Delete subnet (刪除子網路)。

或者，您可以使用命令列工具。

使用命令列工具刪除子網路

- [delete-subnet](#) (AWS CLI)
- [Remove-EC2Subnet](#) (適用於 Windows PowerShell 的 AWS 工具)

## 取消 IPv4 CIDR 區塊與您 VPC 的關聯

若您的 VPC 有超過一個相關聯的 IPv4 CIDR 區塊，您可以取消 IPv4 CIDR 區塊與 VPC 的關聯。您無法取消與主要 IPv4 CIDR 區塊的關聯。您只能取消關聯整個 CIDR 區塊；您無法取消關聯一部分的 CIDR 區塊，或是合併的 CIDR 區塊範圍。您必須先刪除 CIDR 區塊中的所有子網路。

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 CIDRs (VPC IPv4 CIDR) 下，選擇要移除之 CIDR 區塊的刪除按鈕 (十字)。
5. 選擇 Close (關閉)。

或者，您可以使用命令列工具。

使用命令列工具從 VPC 移除 IPv4 CIDR 區塊

- [disassociate-vpc-cidr-block](#) (AWS CLI)
- [Unregister-EC2VpcCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)

## 取消 IPv6 CIDR 區塊與您 VPC 或子網路的關聯

若您不再希望您的 VPC 或子網路支援 IPv6，但您希望繼續使用您的 VPC 或子網路建立及和 IPv4 資源通訊，您可以取消關聯 IPv6 CIDR 區塊。

若要取消關聯 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。如需詳細資訊，請參閱[從執行個體取消指派 IPv6 地址](#) (p. 107)。

使用主控台取消 IPv6 CIDR 區塊與子網路的關聯

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 (子網路)。
3. 選取您的子網路，然後選擇 Actions (動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 選擇十字圖示來移除子網路的 IPv6 CIDR 區塊。
5. 選擇 Close (關閉)。

使用主控台取消 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，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 選擇十字圖示來移除 IPv6 CIDR 區塊。
5. 選擇 Close (關閉)。

### Note

取消與 IPv6 CIDR 區塊的關聯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。

或者，您可以使用命令列工具。

使用命令列工具取消 IPv6 CIDR 區塊與子網路的關聯

- [disassociate-subnet-cidr-block](#) (AWS CLI)
- [Unregister-EC2SubnetCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)



使用命令列工具取消 IPv6 CIDR 區塊與 VPC 的關聯

- [disassociate-vpc-cidr-block](#) (AWS CLI)
- [Unregister-EC2VpcCidrBlock](#) (適用於 Windows PowerShell 的 AWS 工具)

## 刪除您的 VPC

若要使用 VPC 主控台刪除 VPC，您必須先終止或刪除下列元件：

- VPC 中的所有執行個體 - 如需如何終止執行個體的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [終止您的執行個體](#)。
- VPC 對等連線
- 界面端點
- NAT 閘道

當您使用 VPC 主控台刪除 VPC 時，我們也會為您刪除下列 VPC 元件：

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

若您擁有 AWS Site-to-Site VPN 連接，您不需要刪除它或其他與 VPN 相關的元件 (例如客戶閘道和虛擬私有閘道)。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 連接和閘道。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。

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 Linux 執行個體的 Amazon EC2 使用者指南中的 [終止您的執行個體](#)。
3. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
4. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
5. 選取要刪除的 VPC，然後選擇 Actions (動作)、Delete VPC (刪除 VPC)。
6. 如果您有 Site-to-Site VPN 連線，請選取刪除該連線的選項；否則，請不要選取該連線。選擇 Delete VPC (刪除 VPC)。

或者，您可以使用命令列工具。使用命令列刪除 VPC 時，必須先終止所有執行個體，並刪除或中斷所有相關聯的資源，包括子網路、自訂安全群組、自訂網路 ACL、自訂路由表、VPC 對等連線、端點、NAT 閘道、網際網路閘道和僅輸出網際網路閘道。

使用命令列工具刪除 VPC

- [delete-vpc](#) (AWS CLI)
- [Remove-EC2Vpc](#) (適用於 Windows PowerShell 的 AWS 工具)

## 使用共用 VPC

VPC 共用允許多個 AWS 帳戶在共用、集中管理的 Amazon Virtual Private Clouds (VPCs) 中建立其應用程式資源，例如 Amazon EC2 執行個體、Amazon Relational Database Service (RDS) 資料庫、Amazon Redshift 叢集和 AWS Lambda 函數。在此模型中，擁有 VPC (擁有的) 的帳戶會和屬於 AWS Organizations 中相同組織的其他帳戶 (參與者) 共用一個或多個子網路。共用子網路後，參與者可以檢視、建立、修改及刪除與其共用之子網路中的應用程式資源。參與者無法檢視、修改或刪除屬於其他參與者或 VPC 擁有者的資源。

您可以共享 Amazon 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。您可以透過使用 AWS PrivateLink、AWS Transit Gateway 和 Amazon VPC 對等這類連線功能來與共享 Amazon VPC 互連，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](#) (p. 89)
- [共用子網路](#) (p. 89)
- [取消共享已共用的子網路](#) (p. 90)
- [識別共用的子網路的擁有者](#) (p. 90)
- [共用子網路許可](#) (p. 90)
- [適用於擁有者及參與者的計費和計量](#) (p. 91)
- [不受共用子網路支援的服務](#) (p. 91)
- [限制](#) (p. 91)

## 共用 VPC 必要條件

您必須從您組織的 management account 啟用資源共享。如需啟用資源共享的資訊，請參閱 AWS RAM 使用者指南 中的 [啟用與 AWS Organizations 共享](#)。

## 共用子網路

您可以與組織中的其他帳戶共用非預設的資料夾。若要共用子網路，您必須先建立要共用之子網路和 AWS 帳戶、組織單位，或您想要共用子網路之整個組織的資源共享。如需建立資源共享的資訊，請參閱 AWS RAM 使用者指南 中的 [建立資源共享](#)。

### 使用主控台共用子網路

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

### 使用 AWS CLI 共用子網路

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

## 跨可用區域對應子網路

為確保資源分配至區域中的所有可用區域，可用區域會獨立對應至各個帳戶的名稱。例如，您 AWS 帳戶的可用區域 us-east-1a 與其他 AWS 帳戶的 us-east-1a 可能不在同一位置。

為協調各 VPC 共享之帳戶的可用區域，您必須使用 AZ ID，這是可用區域唯一且一致的識別符。例如，`us-east-1-az1` 是 `us-east-1` 區域中的其中一個可用區域。可用區域 ID 能讓您判斷某個帳戶資源在另一個帳戶中的相對位置。如需詳細資訊，請參閱 AWS RAM 使用者指南 中的 [您的資源的 AZ ID](#)。

## 取消共享已共用的子網路

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。當擁有者取消共享子網路後，便會套用以下規則：

- 現有的參與者資源繼續在取消共用的子網路中執行。
- 參與者再也不能在已取消共用的子網路中建立新資源。
- 參與者可以修改、描述及刪除其在子網路中的資源。
- 如果參與者在已取消共用的子網路中仍擁有資源，該擁有者便無法刪除共用的子網路或共用的子網路 VPC。在參與者刪除已取消共用的子網路中的所有資源後，參與者只能刪除共用的子網路或共用的子網路 VPC。

### 使用主控台取消共用子網路

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

### 使用 AWS CLI 取消共用子網路

使用 `disassociate-resource-share` 命令。

## 識別共用的子網路的擁有者

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用的子網路。

### 識別子網路擁有者 (主控台)

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

### 使用 AWS CLI 識別子網路擁有者

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

## 共用子網路許可

### Owner permissions (擁有者許可)

VPC 擁有者負責建立、管理及刪除所有 VPC 層級的資源，包括子網路、路由表、網路 ACL、對等連線、閘道端點、界面端點、Amazon Route 53 Resolver 端點、網際網路閘道、NAT 閘道、虛擬私有閘道及 transit gateway 附件。

VPC 擁有者無法修改或刪除參與者資源，包括參與者所建立的安全群組。VPC 擁有者可以檢視所有網路介面及連接到參與者資源的安全群組的詳細資訊，這樣才能加速實行疑難排解與稽核。VPC 擁有者可以在 VPC、子網路或適用於流量監控或疑難排解的 ENI 層級建立流程日誌訂閱。

## 參與者許可

在共用 VPC 中的參與者負責建立、管理和刪除其資源，包括 Amazon EC2 執行個體、Amazon RDS 資料庫和負載平衡器。參與者無法檢視或修改屬於其他參與者帳戶的資源。參與者可以檢視路由表的詳細資訊，以及連接與其共用子網路的網路 ACL。不過，他們並不能修改 VPC 層級資源，包括路由表、網路 ACL 或子網路。參與者可以參照屬於其他參與者或使用安全群組 ID 之擁有者的安全群組。參與者只能建立其擁有之界面的流程日誌訂閱。

## 適用於擁有者及參與者的計費和計量

在共用的 VPC 中，每個參與者支付其應用程式資源，包括 Amazon EC2 的執行個體、Amazon Relational Database Service 資料庫、Amazon Redshift 叢集和 AWS Lambda 函數。參與者也會支付與可用區域間資料傳輸、透過 VPC 對等連線的資料傳輸，以及透過 AWS Direct Connect 閘道的資料傳輸相關聯的資料傳輸費。VPC 擁有者跨 NAT 閘道、虛擬私有閘道、傳輸閘道、AWS PrivateLink 和 VPC 端點依時數支付費用（如適用）、資料處理和資料傳輸費。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。

## 不受共用子網路支援的服務

參與者無法為下列共用子網路內服務建立資源：

- AWS CloudHSM Classic

子網路擁有者可以將 transit gateway 附加到子網路。參與者（擁有者組織內共用子網路的其他帳戶）無法連線 transit gateway 到子網路。

## 限制

使用 VPC 共享時適用下列限制：

- 擁有者只能與其他帳戶，或位於 AWS Organizations 的相同組織中的組織單位共用子網路。
- 擁有者不能共享在預設 VPC 中的子網路。
- 參與者無法啟動使用安全群組的資源，該安全群組的擁有者為其他共用 VPC 的參與者或 VPC 擁有者。
- 參與者無法啟動使用 VPC 預設安全群組的資源，因為該資源屬於擁有者。
- 擁有者無法使用由其他參與者所擁有的安全群組啟動資源。
- 服務配額適用於個別帳戶。如需服務配額的詳細資訊，請參閱 Amazon Web Services 一般參考 中的 [AWS 服務配額](#)。
- VPC 標籤以及共享 VPC 內資源的標籤不會與參與者共享。
- 當參與者在共享子網路中啟用資源時，他們應該確定將安全群組附加至資源，並且不依賴預設的安全群組。參與者無法使用預設安全群組，因為它屬於 VPC 擁有者。

## 擴充您的 VPC

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、本機區域和 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。
- 本機區域可讓您將資源（例如運算和儲存）放置在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](#)。

## 將您的 VPC 資源擴展到本機區域

AWS 本機區域可讓您透過相同的 API 和工具集，無縫地連接到 AWS 區域內的全系列服務，例如 Amazon Simple Storage Service 和 Amazon DynamoDB。您可以藉由建立具有本機區域指派的新子網路來擴展 VPC 區域。當您在本機區域中建立子網路時，VPC 也會擴展到該本機區域。

若要使用區域，您必須先選擇加入區域。在本機區域中建立子網路。最後，在本機區域子網路中啟動下列任一資源，讓您的應用程式更接近最終使用者：

- Amazon EC2 執行個體
- Amazon EBS 磁碟區
- Amazon FSx 檔案伺服器
- Application Load Balancer
- 專用主機

網路邊界群組是一組唯一的可用區域或本機區域，AWS 可從中公告公用 IP 地址。

當您建立具有 IPv6 地址的 VPC 時，您可以選擇將一組 Amazon 提供的公用 IP 地址指派給 VPC，也可以針對將地址限制為群組的地址，設定網路邊界群組。當您設定網路邊界群組時，IP 地址無法在網路邊界群組之間移動。us-west-2 網路邊界群組包含四個美國西部 (奧勒岡) 可用區域。us-west-2-lax-1 網路邊界群組包含洛杉磯本機區域。

下列規則適用於本機區域：

- 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。
- 您可以使用 Amazon VPC 主控台、AWS CLI 或 API，將本機區域指派給子網路。
- 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)。
- 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。

## 將您的 VPC 資源擴展到 Wavelength 區域

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 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 Amazon Virtual Private Cloud (VPC) 延伸至一或多個 Wavelength 區域，接著使用如 Amazon Elastic Compute Cloud (EC2) 等 AWS 資源來執行需要極低延遲並在區域中有連線 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 區域中建立 Amazon EC2 執行個體、Amazon EBS 磁碟區、Amazon VPC 子網路和電信業者閘道。您也可以使用協調或使用 EC2、EBS 和 VPC 的服務例如 Amazon EC2 Auto Scaling、Amazon EKS 叢集、Amazon ECS 叢集 Amazon EC2 Systems Manager、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 位址。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位址。電信業者閘道會使用 NAT 來轉譯位址，然後將流量傳送到目的地。透過電信業者閘道從電信電信業者網路路由傳送的流量。
- 您可以將 VPC 路由表的目標或 Wavelength 區域的子網路路由表設定為電信業者閘道，允許從特定位置的電信業者網路的傳入流量，以及向電信業者網路和網際網路的傳出流量。如需 Wavelength 區域中路由選項的詳細資訊，請參閱 AWS Wavelength Developer Guide 中的 [Routing](#)。
- 您可以使用 Amazon VPC 主控台、AWS CLI 或 API 將 Wavelength 區域指派給子網路。
- 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 位址、DHCP 選項組和網路 ACL。

## 多個 Wavelength 區域的考量

### Note

位於相同 VPC 中兩個不同 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 Transit Gateway](#)。

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：

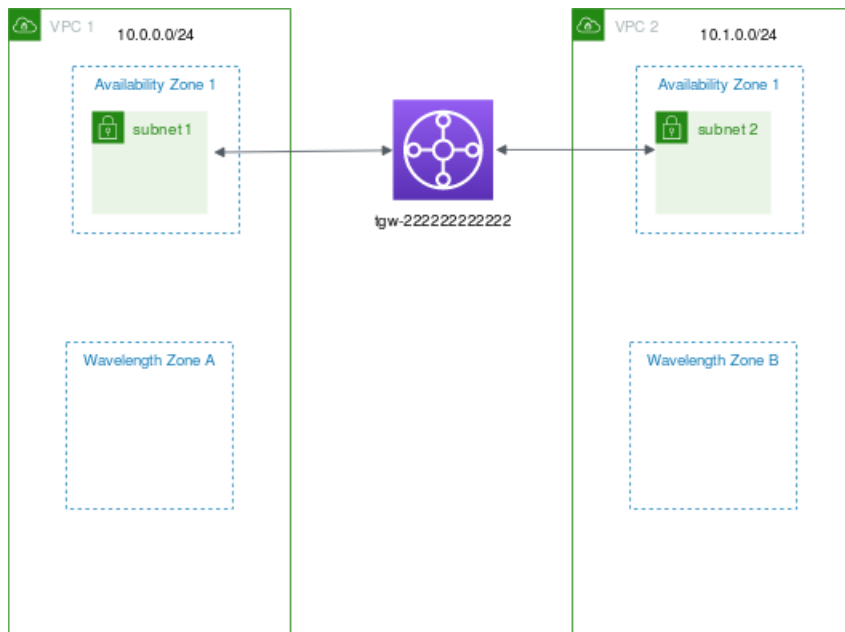
- 對於每個 Wavelength 區域，需要有可用區域中的子網路 (該可用區域屬於 Wavelength 區域的父可用區域)。在此範例中，您可以建立子網路 1 和子網路 2。如需建立子網路的相關資訊，請參閱 [the section called “在您的 VPC 中建立子網路” \(p. 83\)](#)。使用 [describe-availability-zones](#) 以尋找父區域。
- transit gateway。transit gateway 連線 VPC。如需如何建立 transit gateway 的相關資訊，請參閱《AWS Transit Gateway 指南》中的 [建立傳輸閘道](#)。
- 對於每個 VPC，需要有連接到 transit gateway 的 VPC。如需如何建立連接至 VPC 的 transit gateway 相關資訊，請參閱《AWS Transit Gateway 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。如需如何建立 transit gateway 路由的相關資訊，請參閱《AWS Transit Gateway 指南》中的 [傳輸閘道路由表](#)。
- 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 transit gateway ID 做為目標。如需詳細資訊，請參閱 [the section called “傳輸閘道的路由” \(p. 195\)](#)。

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-2222222222222222

VPC 2 的路由表具有以下項目：

目的地	目標
10.1.0.0/24	tgw-2222222222222222



## AWS Outposts 中的子網路

AWS Outposts 可讓您使用相同的 AWS 硬體基礎設施、服務、API 和工具，以在內部部署和雲端建置並執行應用程式。AWS Outposts 適用於需要以低延遲存取應用程式或系統的工作負載，以及需要在本機儲存和處理資料的工作負載。如需 AWS Outposts 的詳細資訊，請參閱 [AWS Outposts](#)。

Amazon VPC 遍及整個 AWS 區域內的所有可用區域。當您將 Outpost 連線到父區域時，您帳戶中所有現有和新建立的 VPC 會遍及整個區域內的所有可用區域和任何相關聯的 Outpost 位置。

下列規則適用於 AWS Outposts：

- 子網路必須位於某個 Outpost 位置。
- 本機閘道會處理 VPC 與內部部署網路之間的網路連線能力。如需本機閘道的相關資訊，請參閱《AWS Outposts 使用者指南》中的 [本機閘道](#)。
- 如果您的帳戶與 AWS Outposts 相關聯，您可以在建立子網路時指定 Outpost ARN，將子網路指派給 Outpost。
- 根據預設，您在與 Outpost 相關聯的 VPC 中建立的每個子網路都會繼承主 VPC 路由表，包括本機閘道路由。您也可以明確地將自訂路由表與 VPC 中的子網路建立關聯，並將本機閘道做為需要路由至內部部署網路之所有流量的下一個躍點目標。

# 預設 VPC 和預設子網路

如果您的 AWS 帳戶是在 2013 年 12 月 4 日之後建立，則僅支援 EC2-VPC。在此案例中，您在每個 AWS 區域中都有預設的 VPC。預設的 VPC 已就緒可供使用，所以您不必建立與設定您自己的 VPC。您可以在您的預設 VPC 中立即開始啟動 Amazon EC2 執行個體。您也可以使用 Elastic Load Balancing、Amazon RDS 與 Amazon EMR 等服務。

預設的 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。如果您偏好建立適合您特定需求的非預設 VPC；例如，使用您慣用的 CIDR 區塊範圍和子網路大小，請參閱[範例藍本](#) (p. 55)。

## 內容

- [預設 VPC 元件](#) (p. 95)
- [可用性與支援的平台](#) (p. 97)
- [檢視您的預設 VPC 和預設子網路](#) (p. 98)
- [在您的預設 VPC 中啟動 EC2 執行個體](#) (p. 98)
- [刪除您的預設子網路和預設 VPC](#) (p. 99)
- [建立預設的 VPC](#) (p. 99)
- [建立預設子網路](#) (p. 100)

## 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：

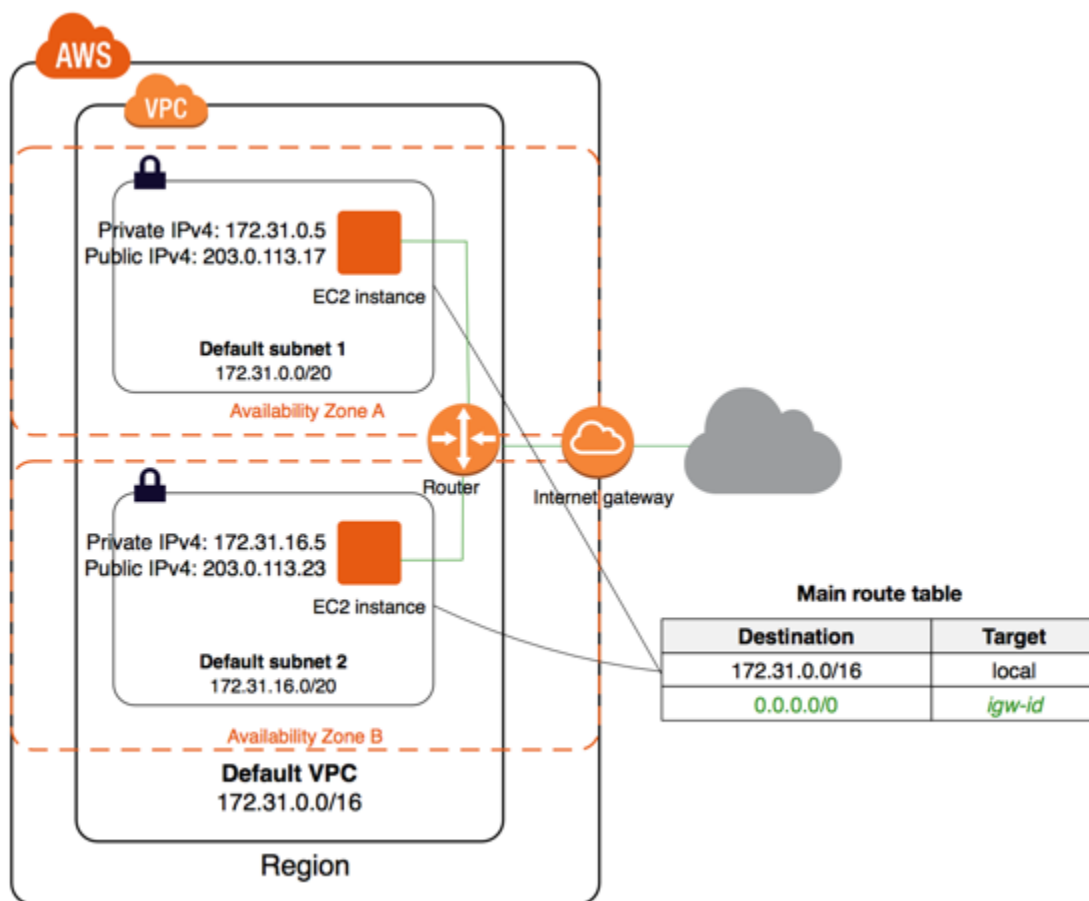
- 建立大小為 /16 IPv4 CIDR 區塊 (172.31.0.0/16) 的 VPC。這最多可提供 65,536 個私有 IPv4 地址。
- 在每個可用區域中建立大小為 /20 的預設子網路。每個子網路最多可提供 4,096 個地址，其中一些預留供我們使用。
- 建立[網際網路閘道](#) (p. 212)，並將它連線到您的預設 VPC。
- 建立預設的安全群組，並與您預設的 VPC 建立關聯。
- 建立預設的網路存取控制清單 (ACL)，並與您預設的 VPC 建立關聯。
- 建立您 AWS 帳戶預設 DHCP 選項集與您預設 VPC 的關聯。

### 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。





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[使用 Direct Connect 閘道](#)。

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

您可以選擇性建立 IPv6 CIDR 區塊與您預設 VPC 的關聯。如需詳細資訊，請參閱「[使用 VPC 和子網路 \(p. 81\)](#)」。

## 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。如需更多詳細資訊，請參閱 [修改您子網路的公有 IPv4 定址屬性 \(p. 105\)](#)。

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 \(p. 100\)](#)。

## 可用性與支援的平台

如果您是在 2013 年 12 月 4 日之後建立 AWS 帳戶，則僅會支援 EC2-VPC，而且您在每個 AWS 區域中都會有預設的 VPC。因此，除非您建立非預設的 VPC 並在您啟動執行個體時指定它，否則我們會在您的預設 VPC 中啟動您的執行個體。

您的 AWS 帳戶若是在 2013 年 3 月 18 日前建立，使用過的區域中會支援 [EC2-Classic](#) 和 EC2-VPC，但未用過的區域只支援 EC2-VPC。在此案例中，我們會在您未建立過任何 AWS 資源的每個區域中建立預設的 VPC。除非您建立非預設的 VPC，並在新區域中啟動執行個體時指定它，否則我們會在該區域您預設的 VPC 中啟動執行個體。但您若在曾用過的區域中啟動執行個體，我們會在 EC2-Classic 中啟動該執行個體。

如果您的 AWS 帳戶是在 2013 年 3 月 18 日到 2013 年 12 月 4 日之間所建立，它可能只支援 EC2-VPC。它在您曾用過的某些區域中也可能支援 EC2-Classic 和 EC2-VPC。如需偵測您 AWS 帳戶在每個區域中支援之平台的資訊，請參閱 [偵測支援的平台 \(p. 97\)](#)。如需何時為預設 VPC 啟用每個區域的資訊，請參閱 Amazon VPC AWS 論壇中的 [公告：啟用適用於預設 VPC 功能集的區域](#)。

如果某個 AWS 帳戶只支援 EC2-VPC，任何與此 AWS 帳戶相關聯的 IAM 帳戶也只支援 EC2-VPC，並和 AWS 帳戶使用相同的預設 VPC。

如果您的 AWS 帳戶支援 EC2-Classic 和 EC2-VPC，您可建立新的 AWS 帳戶，或在您未用過的區域中啟動您的執行個體。您可以如此做，利用在 EC2-Classic 中啟動執行個體的簡易性取得使用 EC2-VPC 的利益。如果您還是想要在沒有預設 VPC 且支援 EC2-Classic 的區域中新增預設 VPC，請參閱 [「我真的希望現有的 EC2 帳戶中能有預設的 VPC。是否能達成？」](#)，位於 [預設 VPC 常見問答集中](#)。

## 偵測支援的平台

您可以使用 Amazon EC2 主控台或命令列判斷您的 AWS 帳戶是否支援這兩個平台，或您是否擁有預設 VPC。

使用 Amazon EC2 主控台偵測平台支援

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽列中，使用在右上角的區域選取器選取您的區域。
3. 在 Amazon EC2 主控台儀表板上，於 Account Attributes (帳戶屬性) 下尋找 Supported Platforms (支援的平台)。如果有 EC2 和 VPC 兩個值，則您可以在任一平台啟動執行個體。如果有一個值 VPC，則您只能在 EC2-VPC 啟動執行個體。

例如，下列內容指出此帳戶僅支援 EC2-VPC 平台，且具有識別符為 vpc-1a2b3c4d 的預設 VPC。

```
Supported Platforms
VPC

Default VPC
vpc-1a2b3c4d
```

如果您刪除您的預設 VPC，則 Default VPC (預設 VPC) 值會顯示 None。

使用命令列偵測平台支援

- `describe-account-attributes` (AWS CLI)
- `Get-EC2AccountAttribute` (適用於 Windows PowerShell 的 AWS 工具)

輸出中的 `supported-platforms` 屬性指出您可在哪個平台中啟動 EC2 執行個體。

## 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 Amazon VPC 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` (適用於 Windows PowerShell 的 AWS 工具)

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` (適用於 Windows PowerShell 的 AWS 工具)

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`。

## 在您的預設 VPC 中啟動 EC2 執行個體

當您在未指定子網路的情況下啟動 EC2 執行個體時，它會自動在您預設 VPC 的預設子網路中啟動。根據預設，我們會為您選取可用區域，並在該可用區域的對應子網路中啟動執行個體。或者，您可在主控台中選取其對應的預設子網路，或在 AWS CLI 中指定子網路或可用區域，為您的執行個體選取可用區域。

## 使用主控台來啟動 EC2 執行個體

在您的預設 VPC 中啟動 EC2 執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在 EC2 儀表板中，選擇 Launch Instance (啟動執行個體)。
3. 請遵循精靈的指示進行。選取一個 AMI，然後選擇執行個體類型。您可以選擇 Review and Launch (檢閱和啟動)，接受精靈其餘的預設設定。這會直接帶您前往 Review Instance Launch (檢閱執行個體啟動) 頁面。
4. 檢閱您的設定。在 Instance Details (執行個體詳細資訊) 區段中，Subnet (子網路) 的預設值是 No preference (default subnet in any Availability Zone) (無偏好設定 (任何可用區域中的預設子網路))。這表示執行個體會我們在選取的可用區域預設子網路中啟動。或者，選擇 Edit instance details (編輯執行個體詳細資訊)，然後選取特定可用區域的預設子網路。
5. 選擇 Launch (啟動) 以選擇金鑰對並啟動執行個體。

## 使用命令列啟動 EC2 執行個體

您可以使用下列其中一項命令來啟動 EC2 執行個體：

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (適用於 Windows PowerShell 的 AWS 工具)

若要在您的預設 VPC 中啟動 EC2 執行個體，請使用這些命令，但不指定子網路或可用區域。

若要在您預設 VPC 的特定預設子網路中啟動 EC2 執行個體，請指定其子網路 ID 或可用區域。

## 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。如需更多詳細資訊，請參閱 [使用 VPC 和子網路 \(p. 81\)](#)。但若您刪除預設的子網路或預設的 VPC，您即必須在啟動您執行個體的另一個 VPC 中明確指定子網路，因為您無法在 EC2-Classic 中啟動執行個體。如果您沒有另一個 VPC，您即必須建立非預設 VPC 和非預設子網路。如需更多詳細資訊，請參閱 [建立 VPC \(p. 82\)](#)。

如果您刪除預設的 VPC，您可以再建立一個新的。如需更多詳細資訊，請參閱 [建立預設的 VPC \(p. 99\)](#)。

如果您刪除預設的子網路，您可以再建立一個新的。如需更多詳細資訊，請參閱 [建立預設子網路 \(p. 100\)](#)。或者，您可以在您預設的 VPC 中建立非預設子網路，然後聯絡 AWS Support 將此子網路標記為預設子網路。您必須提供下列詳細資訊：您的 AWS 帳戶 ID、區域和子網路 ID。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 \(p. 105\)](#)」。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。

## 建立預設的 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。如果您的帳戶支援 EC2-Classic，您即無法使用這些程序在支援 EC2-Classic 的區域中建立預設 VPC。

當您建立預設的 VPC 時，它是使用預設 VPC 的標準元件 ([p. 95](#)) 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 Amazon VPC 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
```

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

或者，您可以使用 `New-EC2DefaultVpc` 適用於 Windows PowerShell 的工具命令或 `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，您可以在您的 VPC 中新增 IPv4 CIDR 區塊 (p. 77)。

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 [建立 IPv6 CIDR 區塊與子網路的關聯 \(p. 85\)](#)。

目前，您只能使用 AWS CLI、AWS 開發套件或 Amazon EC2 API 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
```

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

如需設定 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](#) 適用於 Windows PowerShell 的工具命令或 [CreateDefaultSubnet](#) Amazon EC2 API 動作。



# 您 VPC 中的 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。Amazon EC2 與 Amazon VPC 支援 IPv4 和 IPv6 定址通訊協定。

根據預設，Amazon EC2 和 Amazon VPC 使用 IPv4 定址通訊協定。當您建立 VPC 時，您必須為它指定一個 IPv4 CIDR 區塊 (私有 IPv4 地址範圍)。私有 IPv4 地址無法透過網際網路存取。若要透過網際網路連線到您的執行個體，或是在您的執行個體和其他具有公有端點的 AWS 服務間啟用通訊，您可以指派全域唯一的公有 IPv4 地址給您的執行個體。

您可以選擇性的將 IPv6 CIDR 區塊與您的 VPC 和子網路建立關聯，並指派該區塊的 IPv6 地址給您 VPC 中的資源。IPv6 地址為公有且可以透過網際網路存取。

## Note

為了確保您的執行個體可和網際網路通訊，您也必須將網際網路閘道連接到您的 VPC。如需更多詳細資訊，請參閱 [網際網路閘道 \(p. 212\)](#)。

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 地址彼此互相獨立。您必須在您的 VPC 中分別為 IPv4 和 IPv6 設定路由和安全。

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

## IPv4 和 IPv6 特性及限制

IPv4	IPv6
格式為 32 位元，4 組最多 3 位數的數字。	格式為 128 位元，8 組 4 位數的十六進位數。
為所有 VPC 的預設和必要項目；無法移除。	僅限加入。
VPC CIDR 區塊大小可介於 /16 至 /28 間。	VPC CIDR 區塊大小固定為 /56。
子網路 CIDR 區塊大小可介於 /16 至 /28 間。	子網路 CIDR 區塊大小固定為 /64。
您可以為您的 VPC 選擇私有 IPv4 CIDR 區塊。	我們會為您的 VPC 從 Amazon 的 IPv6 地址集區中選擇 IPv6 CIDR 區塊。您無法選取您自己的範圍。
私有和公有 IP 地址有所差異。為啟用使用網際網路的通訊，公有 IPv4 地址會透過網路位址轉譯 (NAT) 映射至主要私有 IPv4 地址。	公有和私有 IP 地址沒有差異。IPv6 地址為公有。
支援所有執行個體類型。	支援所有目前世代的執行個體類型和 C3、R3 和 I2 先前世代的執行個體類型。如需詳細資訊，請參閱 <a href="#">執行個體類型</a> 。
支援 EC2-Classic 和透過 ClassicLink 使用 VPC 的 EC2-Classic 連線。	不支援 EC2-Classic，也不支援透過 ClassicLink 使用 VPC 的 EC2-Classic 連線。
支援所有 AMI。	自動支援針對 DHCPv6 設定的 AMI。Amazon Linux 2016.09.0 版本及更新版本，以及 Windows Server 2008 R2 及更新版本都會針對 DHCPv6 進行設定。針對其他 AMI，您必須 <a href="#">手動設定您的執行個體 (p. 115)</a> 以識別任何指派的 IPv6 地址。
執行個體會收到由 Amazon 提供的私有 DNS 主機名稱，該名稱會對應到其私有 IPv4 地址，並且在適用的情況下，也會收到對應至其公有 IPv4 或彈性 IP 地址的公有 DNS 主機名稱。	不支援由 Amazon 提供的 DNS 主機名稱。



IPv4	IPv6
支援彈性 IPv4 地址。	不支援彈性 IPv6 地址。
支援客戶閘道、虛擬私有閘道、NAT 裝置和 VPC 端點。	不支援客戶閘道、虛擬私有閘道、NAT 裝置和 VPC 端點。

我們支援透過虛擬私有閘道連線到 AWS Direct Connect 的 IPv6 流量。如需詳細資訊，請參閱 [AWS Direct Connect 使用者指南](#)。

## 私有 IPv4 地址

私有 IPv4 地址 (本主題中又稱為私有 IP 地址) 無法透過網際網路存取，僅能用於您 VPC 中執行個體間的通訊。當您在 VPC 中啟動執行個體時，便會從子網路的 IPv4 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界面 (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。若您沒有指定主要私有 IP 地址，我們會為您子網路範圍中選取可用的 IP 地址。如需網路界面的詳細資訊，請參閱 Linux 執行個體的 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，您可以將網路界面中的輔助私有 IP 地址重新指派給另一個網路界面。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界面的關聯，而會在執行個體終止時予以釋出。如需主要和輔助 IP 地址的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [多個 IP 地址](#)。

### Note

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 連接或 AWS Direct Connect。

## 公有 IPv4 地址

所有子網路都具有可判斷在子網路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路中啟動執行個體時，便會為針對執行個體建立的主要網路界面 (eth0) 指派公有 IP 地址。公有 IP 地址會透過網路位址轉譯 (NAT) 映射至主要私有 IP 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：

- 修改子網路的公有 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 \(p. 105\)](#)。
- 在執行個體啟動期間啟用或停用公有 IP 定址功能，其可覆寫子網路的公有 IP 定址屬性。如需更多詳細資訊，請參閱 [在啟動執行個體期間指派公有 IPv4 地址 \(p. 105\)](#)。

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。您無法手動建立或取消公有 IP 地址的關聯。相反的，在特定情況下，我們會從您的執行個體釋出公有 IP 地址，或將新的公有 IP 地址指派給執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [公有 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 [彈性 IP 地址 \(p. 260\)](#)。

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 [搭配使用 DNS 與 VPC \(p. 256\)](#)。

## IPv6 地址

您可以選擇性的建立 IPv6 CIDR 區塊與您 VPC 和子網路的關聯。如需詳細資訊，請參閱下列主題：

- [建立 IPv6 CIDR 區塊與 VPC 的關聯 \(p. 84\)](#)
- [建立 IPv6 CIDR 區塊與子網路的關聯 \(p. 85\)](#)

若建立 IPv6 CIDR 區塊與您 VPC 和子網路的關聯，並且符合下列其中一項，則 VPC 中的執行個體會收到 IPv6 地址：

- 您的子網路已設定為在啟動時自動指派 IPv6 地址給執行個體的主要網路界面。
- 在啟動期間，您手動將 IPv6 地址指派給您的執行個體。
- 您在啟動之後將 IPv6 地址指派給執行個體。
- 在啟動之後，您將 IPv6 地址指派給相同子網路中的網路界面，並將網路界面連接至執行個體。

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界面 (eth0) 的關聯。您可以取消 IPv6 地址與主要網路界面的關聯。我們不支援執行個體的 IPv6 DNS 主機名稱。

IPv6 地址會在您停止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界面，您無法重新指派該 IPv6 地址 (您必須先將之取消指派)。—

您可以將其他 IPv6 地址指派給執行個體，方法是將其他地址指派給連接至執行個體的網路界面。您可指派給網路界面的 IPv6 地址數目以及您可連接至執行個體的網路界面數目，會根據執行個體類型而不同。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [每個執行個體類型每個網路界面的 IP 地址](#)。

IPv6 地址是全域唯一的，因此可透過網際網路存取。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，來控制是否可透過其 IPv6 地址存取執行個體。如需詳細資訊，請參閱 [Amazon VPC 中的網際網路流量隱私權 \(p. 122\)](#)。

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](#)。

## 您子網路的 IP 定址行為

所有子網路都有可修改的屬性，決定在該子網路中建立的網路界面是否獲派公有 IPv4 地址及 IPv6 地址 (若適用的話)。這包含您在該子網路中啟動執行個體時，為執行個體建立的主要網路界面 (eth0)。

無論子網路的屬性為何，您仍然可以在啟動時覆寫特定執行個體的此設定。如需更多詳細資訊，請參閱 [在啟動執行個體期間指派公有 IPv4 地址 \(p. 105\)](#) 及 [在啟動執行個體期間指派公有 IPv6 地址 \(p. 106\)](#)。

## 使用 IP 地址

您可以修改您子網路的 IP 定址行為、在啟動時指派公有 IPv4 地址給您的執行個體，以及指派或取消指派 IPv6 地址給您的執行個體。

工作

- [修改您子網路的公有 IPv4 定址屬性 \(p. 105\)](#)
- [修改您子網路的公有 IPv6 定址屬性 \(p. 105\)](#)
- [在啟動執行個體期間指派公有 IPv4 地址 \(p. 105\)](#)

- 在啟動執行個體期間指派公有 IPv6 地址 (p. 106)
- 將 IPv6 地址指派給執行個體 (p. 107)
- 從執行個體取消指派 IPv6 地址 (p. 107)
- API 和命令概觀 (p. 108)

## 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 (子網路)。
3. 選取您的子網路，然後選擇 Subnet Actions (子網路動作)、Modify auto-assign IP settings (修改自動指派 IP 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)。

## 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，您的網路界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 (子網路)。
3. 選取您的子網路，然後選擇 Subnet Actions (子網路動作)、Modify auto-assign IP settings (修改自動指派 IP 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)。

## 在啟動執行個體期間指派公有 IPv4 地址

您可以控制您在預設或非預設子網路中的執行個體是否會在啟動時獲得指派公有 IPv4 地址。

### Important

在啟動之後，您無法手動取消公有 IPv4 地址與執行個體的關聯。在特定情況下反而會自動予以釋出，之後您即無法重複使用之。如果需要可讓您自由建立關聯或取消關聯的持久性公有 IP 地址，請改為在啟動之後將彈性 IP 地址與執行個體建立關聯。如需更多詳細資訊，請參閱 [彈性 IP 地址](#) (p. 260)。

### 在啟動期間將公有 IPv4 地址指派給執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 選擇 Launch Instance (啟動執行個體)。
3. 選擇 AMI 和執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
4. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 清單選取 VPC。即會顯示 Auto-assign Public IP (自動指派公有 IP) 清單。選取 Enable (啟用) 或 Disable (停用) 覆寫子網路的預設設定。

#### Important

如果您指定多個網路界面，則無法自動指派公有 IPv4 地址。此外，如果您為 eth0 指定現有網路界面，則無法使用自動指派公有 IPv4 功能覆寫子網路設定。

5. 遵循精靈中的其餘步驟，以啟動執行個體。
6. 在 Instances (執行個體) 畫面上，選取您的執行個體。在 Description (描述) 標籤上，於 IPv4 Public IP (IPv4 公有 IP) 欄位中，您可以檢視您執行個體的公有 IP 地址。或者，在導覽窗格中，選擇 Network Interfaces (網路界面)，然後選取您執行個體的 eth0 網路界面。您可以在 IPv4 Public IP (IPv4 公有 IP) 欄位中檢視公有 IP 地址。

#### Note

公有 IPv4 地址會顯示為主控台中網路界面的屬性，但會透過 NAT 映射至主要私有 IPv4 地址。因此，若您檢查您執行個體上網路界面的屬性 (例如在 Windows 執行個體上透過 `ipconfig`，或是在 Linux 執行個體上透過 `ifconfig`)，則不會顯示公有 IP 地址。若要從執行個體內判定執行個體的公有 IP 地址，您可以使用執行個體中繼資料。如需詳細資訊，請參閱[執行個體中繼資料和使用者資料](#)。

這項功能只在啟動時可供使用。不過，不論您是否在啟動期間將公有 IPv4 地址指派給執行個體，在啟動執行個體之後，都可以建立彈性 IP 地址與執行個體的關聯。如需更多詳細資訊，請參閱[彈性 IP 地址 \(p. 260\)](#)。

## 在啟動執行個體期間指派公有 IPv6 地址

在啟動期間，您可以將 IPv6 地址自動指派給您的執行個體。若要執行此作業，您必須在具有[相關聯 IPv6 CIDR 區塊 \(p. 84\)](#)的 VPC 和子網路中啟動您的執行個體。IPv6 地址會從子網路的範圍指派，並會指派給主要網路界面 (eth0)。

### 在啟動期間將 IPv6 地址自動指派給執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 選擇 Launch Instance (啟動執行個體)。
3. 選取 AMI 和執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體的詳細資訊)。

#### Note

選取可支援 IPv6 地址的執行個體類型。

4. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 選取 VPC，並從 Subnet (子網路) 選取子網路。針對 Auto-assign IPv6 IP (自動指派 IPv6 IP)，選擇 Enable (啟用)。
5. 遵循精靈中的其餘步驟，以啟動執行個體。

或者，若您希望在啟動時從子網路範圍指派特定 IPv6 地址給您的執行個體，您可以將地址指派給您執行個體的主要網路界面。

### 在啟動期間將特定 IPv6 地址指派給執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 選擇 Launch Instance (啟動執行個體)。
3. 選取 AMI 和執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體的詳細資訊)。

#### Note

選取可支援 IPv6 地址的執行個體類型。

4. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 選取 VPC，並從 Subnet (子網路) 選取子網路。
5. 前往 Network interfaces (網路界面) 區段。針對 eth0 網路界面，在 IPv6 IPs (IPv6 IP) 下，選擇 Add IP (新增 IP)。
6. 輸入子網路範圍中的 IPv6 地址。
7. 遵循精靈中的其餘步驟，以啟動執行個體。

如需在啟動時指派多個 IPv6 地址給您的執行個體的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [使用多個 IPv6 地址](#)

## 將 IPv6 地址指派給執行個體

若您的執行個體位於 VPC 及 [具有相關聯 IPv6 CIDR 區塊 \(p. 84\)](#) 的子網路中，您可以使用 Amazon EC2 主控台從子網路範圍指派 IPv6 地址給您的執行個體。

### 將 IPv6 地址與您的執行個體建立關聯

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)，然後選取您的執行個體。
3. 選擇 Actions (動作)、Networking (聯網)、Manage IP Addresses (管理 IP 地址)。
4. 在 IPv6 Addresses (IPv6 地址) 下選擇 Assign new IP (指派新 IP)。您可以指定子網路範圍中的 IPv6 地址，或保留 Auto-assign (自動指派) 值，讓 Amazon 為您選擇 IPv6 地址。
5. 選擇 Save (儲存)。

或者，您可以將 IPv6 地址指派給網路界面。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中彈性網路界面主題內的 [指派 IPv6 地址](#)。

## 從執行個體取消指派 IPv6 地址

若您的執行個體不再需要 IPv6 地址，您可以使用 Amazon EC2 主控台從執行個體取消關聯它。

### 將 IPv6 地址與您的執行個體取消關聯

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)，然後選取您的執行個體。
3. 選擇 Actions (動作)、Networking (聯網)、Manage IP Addresses (管理 IP 地址)。
4. 在 IPv6 Addresses (IPv6 地址) 下，為 IPv6 地址選擇 Unassign (取消指派)。
5. 選擇 Save (儲存)。

或者，您可以將 IPv6 地址與網路界面取消關聯。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中彈性網路界面主題內的 [取消指派 IPv6 地址](#)。



## 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。如需命令列界面與可用 API 清單的詳細資訊，請參閱[存取 Amazon VPC \(p. 1\)](#)。

在啟動期間指派公有 IPv4 地址

- 使用 `--associate-public-ip-address` 或 `--no-associate-public-ip-address` 選項並搭配 [run-instances](#) 命令 (AWS CLI)
- 使用 `-AssociatePublicIp` 參數與 [New-EC2Instance](#) 命令 (適用於 Windows PowerShell 的 AWS 工具) 搭配

在啟動期間指派 IPv6 地址

- 使用 `--ipv6-addresses` 選項並搭配 [run-instances](#) 命令 (AWS CLI)
- 使用 `-Ipv6Addresses` 參數與 [New-EC2Instance](#) 命令 (適用於 Windows PowerShell 的 AWS 工具) 搭配

修改子網路的 IP 定址行為

- [modify-subnet-attribute](#) (AWS CLI)
- [Edit-EC2SubnetAttribute](#) (適用於 Windows PowerShell 的 AWS 工具)

將 IPv6 地址指派給網路界面

- [assign-ipv6-addresses](#) (AWS CLI)
- [Register-EC2Ipv6AddressList](#) (適用於 Windows PowerShell 的 AWS 工具)

從網路界面取消指派 IPv6 地址

- [unassign-ipv6-addresses](#) (AWS CLI)
- [Unregister-EC2Ipv6AddressList](#) (適用於 Windows PowerShell 的 AWS 工具)。

## 遷移至 IPv6

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

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

### Note

本資訊您的現有 VPC 包含公有和私有子網路。如需設定新 VPC 以搭配使用 IPv6 的資訊，請參閱[the section called "IPv6 概觀" \(p. 19\)](#)。

下表概述讓 VPC 和子網路使用 IPv6 的步驟。

步驟	備註
<a href="#">步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網路的關聯 (p. 112)</a>	建立 Amazon 提供的 IPv6 CIDR 區塊與 VPC 和子網路的關聯。

步驟	備註
<a href="#">步驟 2：更新路由表 (p. 113)</a>	更新路由表以遞送 IPv6 流量。針對公有子網路，建立路由，以將所有 IPv6 流量從子網路遞送至網際網路閘道。針對私有子網路，建立路由，以將所有網際網路綁定型 IPv6 流量從子網路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 (p. 113)</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路的流量流程，則必須包含 IPv6 流量的規則。
<a href="#">步驟 4：變更執行個體類型 (p. 114)</a>	如果您的執行個體類型不支援 IPv6，請變更執行個體類型。
<a href="#">步驟 5：將 IPv6 地址指派給執行個體 (p. 114)</a>	將 IPv6 地址從子網路的 IPv6 地址範圍指派給執行個體。
<a href="#">步驟 6：(選用) 在執行個體上設定 IPv6 (p. 115)</a>	如果從未設定成使用 DHCPv6 的 AMI 啟動執行個體，您必須手動設定執行個體辨識指派給執行個體的 IPv6 地址。

遷移至使用 IPv6 之前，請確定您已閱讀 Amazon VPC 的 IPv6 定址功能：[IPv4 和 IPv6 特性及限制 \(p. 102\)](#)。

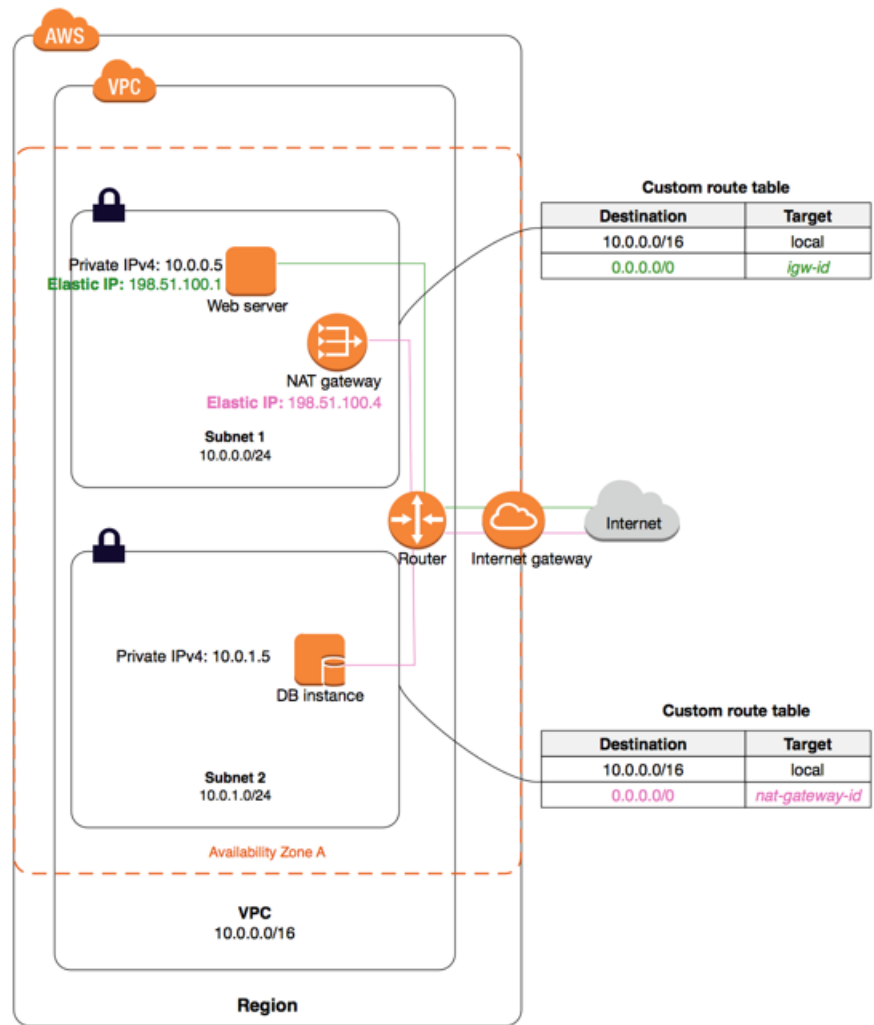
#### 內容

- [範例：在含公有和私有子網路的 VPC 中啟用 IPv6 \(p. 109\)](#)
- [步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網路的關聯 \(p. 112\)](#)
- [步驟 2：更新路由表 \(p. 113\)](#)
- [步驟 3：更新安全群組規則 \(p. 113\)](#)
- [步驟 4：變更執行個體類型 \(p. 114\)](#)
- [步驟 5：將 IPv6 地址指派給執行個體 \(p. 114\)](#)
- [步驟 6：\(選用\) 在執行個體上設定 IPv6 \(p. 115\)](#)

## 範例：在含公有和私有子網路的 VPC 中啟用 IPv6

在本範例中，VPC 具有公有和私有子網路。私有子網路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。公有子網路中的公開 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 (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-33cc44dd33cc44dd3	允許來自與 sg-33cc44dd33cc44dd3 (資料庫執行個體) 相關聯之執行個體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；

類型	通訊協定	連接埠範圍	來源	註解
				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 (sg-33cc44dd33cc44dd3) 具有下列傳入規則：

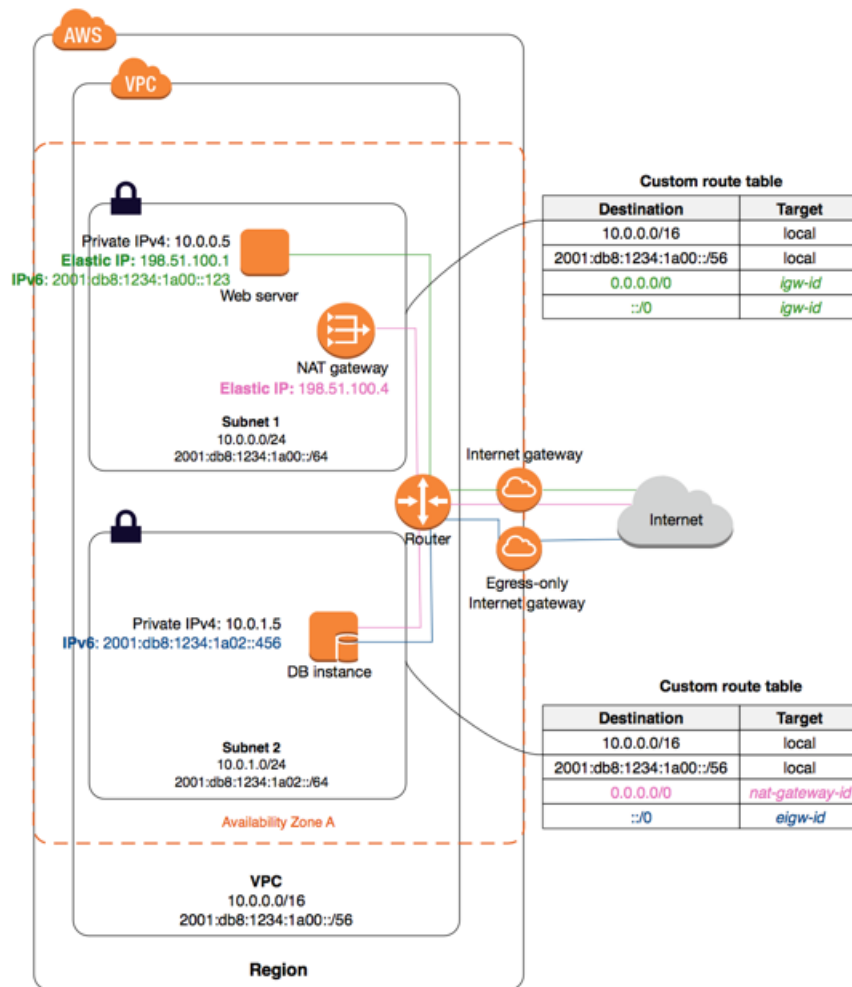
類型	通訊協定	連接埠範圍	來源	註解
MySQL	TCP	3306	sg-11aa22bb11aa22bb1	允許來自與 sg-11aa22bb11aa22bb1 (Web 伺服器執行個體) 相關聯之執行個體的 MySQL 流量傳入存取。

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。

完成這些步驟之後，VPC 將具有下列組態。



## 步驟 1：建立 IPv6 CIDR 區塊與 VPC 和子網路的關聯

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 區塊與每個子網路的關聯。

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，然後選擇 Actions (動作)、Edit CIDRs (編輯 CIDR)。
4. 選擇新增 IPv6 CIDR，選擇下列其中一個選項，然後選擇選取 CIDR：
  - Amazon-provided IPv6 CIDR block (Amazon 提供的 IPv6 CIDR 區塊：向 Amazon 的 IPv6 地址集區申請 IPv6 CIDR 區塊。對於網路邊界群組，請選取 AWS 公告 IP 位址的群組。
  - 我擁有的 IPv6 CIDR：(BYOIP) 從您的 IPv6 地址集區配置 1 個 IPv6 CIDR 區塊。在 Pool (集區) 中，選擇要從中配置 IPv6 CIDR 區塊的 IPv6 地址集區。

建立 IPv6 CIDR 區塊與子網路的關聯

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 (子網路)。

3. 選取您的子網路，然後選擇 Subnet Actions (子網路動作)、Edit IPv6 CIDRs (編輯 IPv6 CIDR)。
4. 選擇 Add IPv6 CIDR (新增 IPv6 CIDR)。指定子網路的十六進位對 (例如，00)，然後透過選擇核取圖示來確認項目。
5. 選擇 Close (關閉)。為 VPC 中的其他子網路重複這些步驟。

如需更多詳細資訊，請參閱 [IPv6 的 VPC 和子網路規模 \(p. 80\)](#)。

## 步驟 2：更新路由表

針對公有子網路，您必須更新路由表，讓執行個體 (例如 Web 伺服器) 將網際網路閘道用於 IPv6 流量。

針對私有子網路，您必須更新路由表，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。

### 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 Route Tables (路由表)，然後選取與公有子網路建立關聯的路由表。
3. 在 Routes (路由) 標籤上，選擇 Edit (編輯)。
4. 選擇 Add another route (新增其他路由)。針對 Destination (目的地) 指定 `::/0`，並針對 Target (目標) 選取網際網路閘道 ID，然後選擇 Save (儲存)。

### 更新私有子網路的路由表

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 如果您在私有子網路中使用 NAT 裝置，則不支援 IPv6 流量。相反地，請建立私有子網路的輸出限定網際網路閘道，以啟用透過 IPv6 與網際網路的傳出通訊，並防止傳入通訊。輸出限定網際網路閘道僅支援 IPv6 流量。如需詳細資訊，請參閱 [輸出限定網際網路閘道 \(p. 218\)](#)。
3. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取與私有子網路建立關聯的路由表。
4. 在 Routes (路由) 標籤上，選擇 Edit (編輯)。
5. 選擇 Add another route (新增其他路由)。針對 Destination (目標)，指定 `::/0`。針對 Target (目標) 選取輸出限定網際網路閘道 ID，然後選擇 Save (儲存)。

如需更多詳細資訊，請參閱 [路由選項範例 \(p. 191\)](#)。

## 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；根據預設，允許來自 `sg-11aa22bb11aa22bb1` 之所有通訊的規則包含 IPv6 通訊。

### 更新安全群組規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)，然後選取 Web 伺服器安全群組。
3. 在 Inbound Rules (傳入規則) 標籤中，選擇 Edit (編輯)。
4. 針對每個規則，選擇 Add another rule (新增其他規則)，然後在完成時選擇 Save (儲存)。例如，若要新增規則以允許透過 IPv6 的所有 HTTP 流量，請針對 Type (類型) 選取 HTTP，然後針對 Source (來源) 輸入 `::/0`。

根據預設，在您建立 IPv6 CIDR 區塊與 VPC 的關聯時，會針對安全群組自動新增可允許所有 IPv6 流量的傳出規則。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。如需更多詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。

## 更新網路 ACL 規則

如果您建立 IPv6 CIDR 區塊與 VPC 的關聯，則會自動將規則新增至預設網路 ACL 來允許 IPv6 流量，但前提是您尚未修改其預設規則。如果您已修改預設網路 ACL，或已建立具有規則可控制進出子網路之流量流程的自訂網路 ACL，則必須手動新增 IPv6 流量的規則。如需更多詳細資訊，請參閱 [網路 ACL \(p. 146\)](#)。

## 步驟 4：變更執行個體類型

所有目前世代的執行個體類型都支援 IPv6。如需詳細資訊，請參閱 [執行個體類型](#)。

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。在上述範例中，資料庫執行個體是不支援 IPv6 的 `m3.large` 執行個體類型。您必須將執行個體的大小調整為支援的執行個體類型 (例如，`m4.large`)。

若要調整執行個體的大小，請注意相容性限制。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [重新調整執行個體大小的相容性](#)。在本藍本中，如果已從使用 HVM 虛擬化的 AMI 啟動您的資料庫執行個體，則可以使用下列程序將其大小調整為 `m4.large` 執行個體類型。

### Important

若要調整執行個體的大小，您必須停止執行個體。停止和啟動執行個體時，會變更執行個體的公有 IPv4 地址 (若有的話)。如果您有任何資料存放在執行個體存放區磁碟區上，則會清除資料。

### 調整執行個體的大小

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)，然後選取資料庫執行個體。
3. 選擇 Actions (動作)、Instance State (執行個體狀態)、Stop (停止)。
4. 在確認對話方塊中，選擇 Yes, Stop (是，停止)。
5. 在仍然選取執行個體的情況下，選擇 Actions (動作)、Instance Settings (執行個體設定)、Change Instance Type (變更執行個體類型)。
6. 針對 Instance Type (執行個體類型)，選擇新的執行個體類型，然後選擇 Apply (套用)。
7. 若要重新啟動已停止的執行個體，請選取執行個體，然後選擇 Actions (動作)、Instance State (執行個體狀態)、Start (啟動)。在確認對話方塊中，選擇 Yes, Start (是，啟動)。

如果您的執行個體是執行個體後端 AMI，則您無法使用較舊的程序來調整執行個體的大小。相反地，您可以從執行個體建立執行個體後端 AMI，並使用新的執行個體類型從 AMI 啟動新的執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [建立執行個體存放區後端 Linux AMI](#) 以及 Windows 執行個體的 Amazon EC2 使用者指南中的 [建立執行個體存放區後端 Windows AMI](#)。

如果有相容性限制，則您可能無法遷移至新的執行個體類型。例如，如果已從使用 PV 虛擬化的 AMI 啟動您的執行個體，則唯一同時支援 PV 虛擬化和 IPv6 的執行個體類型為 C3。此執行個體類型可能不適合您的需求。在此情況下，您可能需要在基本 HVM AMI 上重新安裝軟體，並啟動新的執行個體。

如果您從新的 AMI 啟動執行個體，則可以在啟動期間將 IPv6 地址指派給執行個體。

## 步驟 5：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)。

### 將 IPv6 地址指派給執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)。
3. 選取執行個體，然後選擇 Actions (動作)、Networking (聯網)、Manage IP Addresses (管理 IP 地址)。
4. 在 IPv6 Addresses (IPv6 地址) 下選擇 Assign new IP (指派新 IP)。您可以輸入子網路範圍中的 IPv6 地址，也可以保留預設 Auto-Assign 值，讓 Amazon 為您選擇地址。
5. 選擇 Yes, Update (是，更新)。

或者，如果您啟動新的執行個體 (例如，如果無法變更執行個體類型，並改為建立新的 AMI)，則可以在啟動期間指派 IPv6 地址。

### 在啟動期間將 IPv6 地址指派給執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 選取 AMI 和 IPv6 相容執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
3. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，針對 Network (網路) 選取 VPC，然後針對 Subnet (子網路) 選取子網路。針對 Auto-assign IPv6 IP (自動指派 IPv6 IP)，選取 Enable (啟用)。
4. 遵循精靈中的其餘步驟，以啟動執行個體。

您可以使用執行個體的 IPv6 地址連線到執行個體。如果您是從本機電腦連線，請確定您的本機電腦具有 IPv6 地址，並設定為使用 IPv6。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [連線至 Linux 執行個體](#) 以及 Windows 執行個體的 Amazon EC2 使用者指南 中的 [連線至 Windows 執行個體](#)。

## 步驟 6：(選用) 在執行個體上設定 IPv6

如果您已使用 Amazon Linux 2016.09.0 或更新版本、Windows Server 2008 R2 或更新版本，或 Ubuntu Server 2018 或更新版本來啟動執行個體，即會設定執行個體的 IPv6 功能，而且不需要其他步驟。

如果您已從不同的 AMI 啟動執行個體，則可能無法設定其 DHCPv6 功能，這表示主要網路界面上不會自動辨識您指派給執行個體的任何 IPv6 地址。若要確認網路界面上是否設定 IPv6 地址，請在 Linux 上使用 `ifconfig` 命令，或在 Windows 上使用 `ipconfig` 命令。

您可以使用下列步驟來設定執行個體。您需要使用執行個體的公有 IPv4 地址連線至執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [連線至 Linux 執行個體](#) 以及 Windows 執行個體的 Amazon EC2 使用者指南 中的 [連線至 Windows 執行個體](#)。

#### 作業系統

- [Amazon Linux \(p. 115\)](#)
- [Ubuntu \(p. 116\)](#)
- [RHEL/CentOS \(p. 118\)](#)
- [Windows \(p. 119\)](#)

## Amazon Linux

### 在 Amazon Linux 上設定 DHCPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 取得執行個體的最新軟體套件：

```
sudo yum update -y
```

3. 使用您選擇的文字編輯器，開啟 `/etc/sysconfig/network-scripts/ifcfg-eth0`，並找到下行：

```
IPV6INIT=no
```

將該行取代為下列內容：

```
IPV6INIT=yes
```

新增下列兩行，然後儲存您的變更：

```
DHCPV6C=yes  
DHCPV6C_OPTIONS=--nw
```

4. 開啟 `/etc/sysconfig/network`，並移除下列各行，然後儲存您的變更：

```
NETWORKING_IPV6=no  
IPV6INIT=no  
IPV6_ROUTER=no  
IPV6_AUTOCONF=no  
IPV6FORWARDING=no  
IPV6TO4INIT=no  
IPV6_CONTROL_RADVD=no
```

5. 開啟 `/etc/hosts`，並將該內容取代為下列內容，然後儲存您的變更：

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4  
::1         localhost6 localhost6.localdomain6
```

6. 將執行個體重新開機。重新連線至執行個體，然後使用 `ifconfig` 命令確認主要網路界面上可辨識 IPv6 地址。

## Ubuntu

您可以設定 Ubuntu 執行個體，動態辨識任何指派給網路界面的 IPv6 地址。如果您的執行個體沒有 IPv6 地址，則此組態可能會將執行個體的開機時間延長為高達 5 分鐘。

必須以 root 使用者身分執行這些步驟。

## Ubuntu Server 16

在執行中 Ubuntu Server 16 執行個體上設定 IPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 檢視 `/etc/network/interfaces.d/50-cloud-init.cfg` 檔案的內容：

```
cat /etc/network/interfaces.d/50-cloud-init.cfg
```

```
# This file is generated from information provided by  
# the datasource. Changes to it will not persist across an instance.  
# To disable cloud-init's network configuration capabilities, write a file  
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
```



```
# network: {config: disabled}
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

確認已設定迴路網路裝置 (lo)，並記下網路界面的名稱。在本範例中，網路界面名稱是 eth0；根據執行個體類型，名稱可能會不同。

3. 建立 /etc/network/interfaces.d/60-default-with-ipv6.cfg 檔案，並新增下行。必要時，請將 eth0 取代為您上面的步驟中所擷取的網路界面名稱。

```
iface eth0 inet6 dhcp
```

4. 將執行個體重新開機，或執行下列命令重新啟動網路界面。必要時，請將 eth0 取代為您網路界面的名稱。

```
sudo ifdown eth0 ; sudo ifup eth0
```

5. 重新連線至執行個體，然後使用 ifconfig 命令確認網路界面上已設定 IPv6 地址。

### 利用使用者資料設定 IPv6

- 您可以啟動新的 Ubuntu 執行個體，並確定已在啟動期間指定下列使用者資料，以在網路界面上自動設定指派給執行個體的任何 IPv6 地址：

```
#!/bin/bash
echo "iface eth0 inet6 dhcp" >> /etc/network/interfaces.d/60-default-with-ipv6.cfg
dhclient -6
```

在此情況下，您不需要連線至執行個體即可設定 IPv6 地址。

如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [於啟動時在 Linux 執行個體上執行命令](#)。

## Ubuntu Server 14

如果您使用 Ubuntu Server 14，則必須包含重新啟動雙堆疊網路界面時所發生之 [已知問題](#) 的解決方法 (重新啟動會導致延長逾時，在此期間無法連線執行個體)。

必須以 root 使用者身分執行這些步驟。

### 在執行中 Ubuntu Server 14 執行個體上設定 IPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 編輯 /etc/network/interfaces.d/eth0.cfg 檔案，使其包含下列內容：

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
    up dhclient -6 $IFACE
```

3. 將執行個體重新開機：

```
sudo reboot
```

4. 重新連線至執行個體，然後使用 `ifconfig` 命令確認網路界面上已設定 IPv6 地址。

## 啟動 DHCPv6 用戶端

或者，若要立即啟動網路界面的 IPv6 地址，而不提示任何額外組態，您可以啟動執行個體的 DHCPv6 用戶端。不過，在重新開機之後，IPv6 地址就不會持續保存在網路界面上。

在 Ubuntu 上啟動 DHCPv6 用戶端

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 啟動 DHCPv6 用戶端：

```
sudo dhclient -6
```

3. 使用 `ifconfig` 命令確認主要網路界面上可辨識 IPv6 地址。

## RHEL/CentOS

RHEL 7.4 以及 CentOS 7 和更新版本使用 `cloud-init` 設定網路界面，並產生 `/etc/sysconfig/network-scripts/ifcfg-eth0` 檔案。您可以建立自訂 `cloud-init` 組態檔案來啟用 DHCPv6，這會在每次重新開機之後產生具有可啟用 DHCPv6 之設定的 `ifcfg-eth0` 檔案。

### Note

基於已知問題，如果您搭配使用 RHEL/CentOS 7.4 與最新 `cloud-init-0.7.9` 版本，則這些步驟可能會在重新開機之後導致您中斷與執行個體的連線。若要解決這項問題，您可以手動編輯 `/etc/sysconfig/network-scripts/ifcfg-eth0` 檔案。

在 RHEL 7.4 或 CentOS 7 上設定 DHCPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 使用您選擇的文字編輯器，建立自訂檔案，例如：

```
/etc/cloud/cloud.cfg.d/99-custom-networking.cfg
```

3. 在檔案中新增下列各行，然後儲存您的變更：

```
network:
  version: 1
  config:
    - type: physical
      name: eth0
      subnets:
        - type: dhcp
        - type: dhcp6
```

4. 使用您選擇的文字編輯器，將以下行新增到 `/etc/sysctl.d` 底下的介面特有檔案。如果停用「穩定一致的網路裝置命名方式」，則網路介面名稱為 `ethX`，或次要介面。

```
net.ipv6.conf.network-interface-name.accept_ra=1
```

在下列範例中，網路介面為 `en5`。

```
net.ipv6.conf.en5.accept_ra=1
```

5. 將執行個體重新開機。

6. 重新連線至執行個體，然後使用 `ifconfig` 命令確認網路界面上已設定 IPv6 地址。

針對 RHEL 7.3 版和更早版本，您可以直接使用下列程序修改 `/etc/sysconfig/network-scripts/ifcfg-eth0` 檔案。

在 RHEL 7.3 和更早版本上設定 DHCPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 使用您選擇的文字編輯器，開啟 `/etc/sysconfig/network-scripts/ifcfg-eth0`，並找到下行：

```
IPV6INIT="no"
```

將該行取代為下列內容：

```
IPV6INIT="yes"
```

新增下列兩行，然後儲存您的變更：

```
DHCPV6C=yes  
NM_CONTROLLED=no
```

3. 開啟 `/etc/sysconfig/network`，並如下新增或附加下行，然後儲存您的變更：

```
NETWORKING_IPV6=yes
```

4. 執行下列命令，在執行個體上重新啟動聯網：

```
sudo service network restart
```

您可以使用 `ifconfig` 命令確認主要網路界面上可辨識 IPv6 地址。

在 RHEL 6 或 CentOS 6 上設定 DHCPv6

1. 使用執行個體的公有 IPv4 地址連線至執行個體。
2. 遵循上述程序中的步驟 2 - 4，以設定 RHEL 7/CentOS 7。
3. 如果您重新啟動聯網，並收到無法取得 IPv6 地址的錯誤，請開啟 `/etc/sysconfig/network-scripts/ifup-eth`，並找到下行 (根據預設，為第 327 行)：

```
if /sbin/dhclient "$DHCLIENTARGS"; then
```

移除括住 `$DHCLIENTARGS` 的引號，然後儲存您的變更。在執行個體上重新啟動聯網：

```
sudo service network restart
```

## Windows

使用下列程序，在 Windows Server 2003 和 Windows Server 2008 SP2 上設定 IPv6。

若要確定 IPv6 優於 IPv4，請從下列 Microsoft 支援頁面下載名為在字首政策中偏好 IPv6 而非 IPv4 的修正：<https://support.microsoft.com/en-us/help/929852/how-to-disable-ipv6-or-its-components-in-windows>。

### 在 Windows Server 2003 上啟用和設定 IPv6

1. 使用 [describe-instances](#) AWS CLI 命令，或在 Amazon EC2 主控台中檢查執行個體的 IPv6 IPs (IPv6 IPs) 欄位，以取得執行個體的 IPv6 地址。
2. 使用執行個體的公有 IPv4 地址連線至執行個體。
3. 從執行個體內，選擇開始、控制台、網路連線、區域連線。
4. 選擇屬性，然後選擇安裝。
5. 選擇通訊協定，然後選擇新增。在網路通訊協定清單中，選擇 Microsoft TCP/IP 第 6 版，然後選擇確定。
6. 開啟命令提示，然後開啟網路 Shell。

```
netsh
```

7. 切換至界面 IPv6 內容。

```
interface ipv6
```

8. 使用下列命令，將 IPv6 地址新增至區域連線。將 IPv6 地址的值取代為執行個體的 IPv6 地址。

```
add address "Local Area Connection" "ipv6-address"
```

例如：

```
add address "Local Area Connection" "2001:db8:1234:1a00:1a01:2b:12:d08b"
```

9. 結束網路 Shell。

```
exit
```

10. 使用 ipconfig 命令確認可辨識區域連線的 IPv6 地址。

### 在 Windows Server 2008 SP2 上啟用和設定 IPv6

1. 使用 [describe-instances](#) AWS CLI 命令，或在 Amazon EC2 主控台中檢查執行個體的 IPv6 IPs (IPv6 IPs) 欄位，以取得執行個體的 IPv6 地址。
2. 使用執行個體的公有 IPv4 地址連線至 Windows 執行個體。
3. 選擇開始、控制台。
4. 開啟網路和共用中心，然後開啟網路連線。
5. 以滑鼠右鍵按一下區域連線 (適用於網路界面)，然後選擇屬性。
6. 選擇網際網路通訊協定第 6 版 (TCP/IPv6) 核取方塊，然後選擇確定。
7. 再次開啟 [區域網路] 的屬性對話方塊。選擇網際網路通訊協定第 6 版 (TCP/IPv6)，然後選擇屬性。
8. 選擇使用下列 IPv6 位址，並執行下列作業：
  - 針對 IPv6 位址，輸入您在步驟 1 取得的 IPv6 地址。
  - 針對子網路前置詞長度，輸入 64。
9. 選擇確定，然後關閉屬性對話方塊。
10. 開啟命令提示。使用 ipconfig 命令確認可辨識區域連線的 IPv6 地址。

# Amazon Virtual Private Cloud 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

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

- 雲端本身的安全 – AWS 負責保護執行 AWS 雲端內 AWS 服務的基礎設施。AWS 提供的服務，也可讓您安全使用。第三方稽核人員會定期測試和驗證我們安全性的有效性，做為 [AWS 合規計劃](#) 的一部分。若要了解適用於 Amazon Virtual Private Cloud 的合規計畫，請參閱 [合規計畫的 AWS 服務範圍](#)。
- 雲端內部的安全 – 您的責任取決於所使用的 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。下列主題將顯示如何設定 Amazon VPC 以達到您的安全和合規目標。您也將了解如何使用其他 AWS 服務，幫助您監控並保護 Amazon VPC 資源。

## 主題

- [Amazon Virtual Private Cloud 中的資料保護](#) (p. 121)
- [Amazon VPC 的 Identity and Access Management](#) (p. 123)
- [Amazon VPC 的記錄和監控](#) (p. 137)
- [Amazon Virtual Private Cloud 中的彈性](#) (p. 137)
- [Amazon Virtual Private Cloud 的合規驗證](#) (p. 137)
- [VPC 的安全群組](#) (p. 138)
- [網路 ACL](#) (p. 146)
- [VPC 流程日誌](#) (p. 158)
- [VPC 的安全最佳實務](#) (p. 182)

## Amazon Virtual Private Cloud 中的資料保護

Amazon Virtual Private Cloud 會遵循 AWS [共同責任模型](#)，此模型包含資料保護的法規和指導。AWS 會負責保護執行所有 AWS 服務的全球基礎設施。AWS 會維持對此基礎設施上託管資料的控制，包含處理客戶內容和個人資料的安全性組態控制。身為資料控制者或資料處理者的 AWS 客戶和 APN 合作夥伴都需負責保護在 AWS 雲端中放置的任何個人資料。

基於資料保護目的，我們建議您保護 AWS 帳戶登入資料，並使用 AWS Identity and Access Management (IAM) 設定個別使用者帳戶，以便每個使用者都只獲得完成其任務所需的許可。我們也建議您以下列方式保護資料：

- 每個帳戶都使用多重驗證 (MFA)。如需有關 MFA 的資訊，請參閱 [AWS Multi-Factor Authentication \(MFA\)](#)。
- 使用 TLS 與 AWS 資源進行通訊。建議使用 TLS 1.2 或更新版本。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。如需有關使用 AWS CloudTrail 的資訊，請參閱 [AWS CloudTrail 使用指南中的使用 CloudTrail](#)。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制。
- 使用進階的受管安全服務，例如 Amazon Macie，協助探索和保護存放在 Amazon S3 的個人資料。如需 Amazon Macie 的詳細資訊，請參閱 [Amazon Macie 使用者指南](#)。

我們強烈建議您絕對不要將客戶帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，如 Name (名稱) 欄位。這包括當您使用 Amazon VPC 或使用主控台、API、AWS CLI 或 AWS 開發套件的其他 AWS 服務。您在 Amazon VPC 或其他服務中輸入的任何資料都可能被選入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在 URL 中包含登入資料資訊，以驗證您對該伺服器的請求。

如需資料保護的詳細資訊，請參閱「AWS 安全部落格」上的 [AWS 共同責任模型](#) 和 [GDPR](#) 部落格文章。

## 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虛擬私有雲端 (VPC) 安全的功能：

- **安全群組**：安全群組就像是防火牆，用於關聯的 Amazon EC2 執行個體，可在執行個體層級控制傳入及傳出流量。當執行個體啟動後，其可與您已建立的一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 VPC 的預設安全群組相關聯。如需詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。
- **網路存取控制清單 (ACL)**：網路 ACL 就像是防火牆，用於關聯的子網路，可在子網路層級控制傳入及傳出流量。如需詳細資訊，請參閱 [網路 ACL \(p. 146\)](#)。
- **流量日誌**：流量日誌可擷取您 VPC 中傳入和傳出網路界面之 IP 流量資訊。您可以建立 VPC、子網路或個別網路界面的流程日誌。流量日誌資料會發佈至 CloudWatch Logs 或 Amazon S3，並可協助您診斷過度限制或過度寬鬆的安全群組和網路 ACL 規則。如需詳細資訊，請參閱 [VPC 流程日誌 \(p. 158\)](#)。
- **流量鏡射**：您可以從 Amazon EC2 執行個體的彈性網路界面複製網路流量。然後，您可以將流量傳送至頻外安全性和監控設備。如需詳細資訊，請參閱 [流量鏡射指南](#)。

您可使用 AWS Identity and Access Management (IAM) 控制組織中具有安全群組、網路 ACL 和流量日誌之建立和管理許可的人員。例如，您可以向網路管理員授與該許可，但不將許可授與僅需啟動執行個體的人員。如需詳細資訊，請參閱 [Amazon VPC 的 Identity and Access Management \(p. 123\)](#)。

Amazon 安全群組和網路 ACL 不會篩選進出連結本機地址 (169.254.0.0/16) 或 AWS 預留 IPv4 地址的流量 (這些是子網路的前四個 IPv4 地址，包括 VPC 的 Amazon DNS 伺服器地址)。同樣地，流量日誌不會擷取進出這些地址的 IP 流量。這些地址支援下列項目：

- 網域名稱服務 (DNS)
- 動態主機組態通訊協定 (DHCP)
- Amazon EC2 執行個體中繼資料
- 金鑰管理伺服器 (KMS) — 適用於 Windows 執行個體的授權管理
- 子網路中的路由

您可在執行個體中實作額外的防火牆解決方案，以封鎖與連結本機地址的網路通訊。

## 安全群組和網路 ACL 的比較

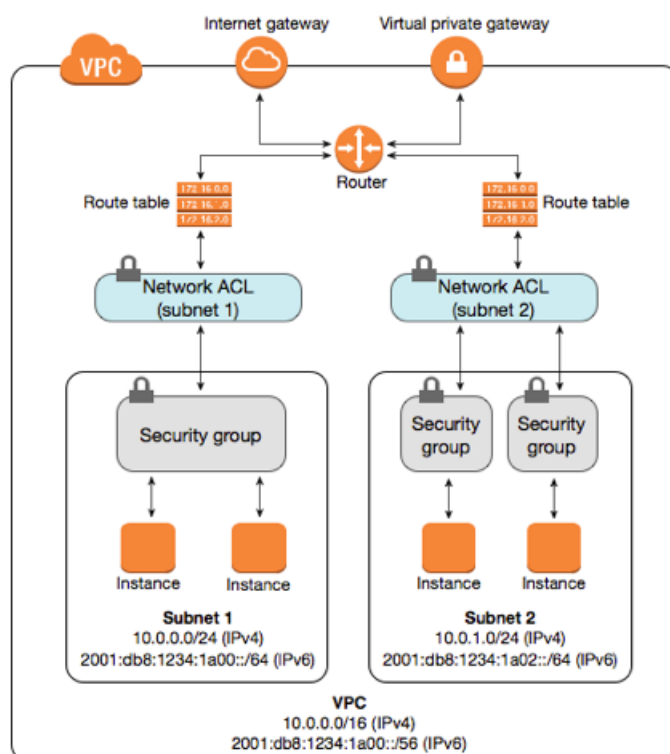
下表總結了安全群組與網路 ACL 之間的基本差異。

安全群組	網路 ACL
在執行個體層級運作	在子網路層級運作
僅支援允許規則	支援允許規則和拒絕規則
具狀態：自動允許傳回流量，不受任何規則影響	無狀態：傳回流量必須經規則明確允許
我們會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，我們會依序處理規則，從編號最低的規則開始



安全群組	網路 ACL
若某人於啟動執行個體時指定安全群組，或在啟動後將安全群組與執行個體建立關聯，才會套用至執行個體。	自動套用至子網路與其相關聯的所有執行個體 (因此，如果安全群組規則太過寬鬆，則它會提供額外一層防禦)

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。如需範例，請參閱範例：控制對子網路中執行個體的存取 (p. 156)。

## 傳輸中加密

AWS 在所有類型的 EC2 執行個體之間提供安全和私有連線。此外，某些執行個體類型使用基礎硬體的卸載功能，將 AEAD 演算法與 256 位元加密搭配使用，以自動加密執行個體之間的傳輸中流量。這對網路效能沒有影響。如需執行個體加密的詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [傳輸中加密](#)。

## Amazon VPC 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制 AWS 資源的存取。IAM 管理員可以控制能進行身份驗證 (登入) 及獲得授權 (具備許可) 以使用 Amazon VPC 資源的人員。IAM 是一種 AWS 服務，無須支付任何額外的費用即可使用。



## 主題

- [對象 \(p. 124\)](#)
- [使用身分來驗證 \(p. 124\)](#)
- [使用政策管理存取權 \(p. 125\)](#)
- [Amazon VPC 如何搭配 IAM 運作 \(p. 127\)](#)
- [Amazon VPC 政策範例 \(p. 129\)](#)
- [對 Amazon VPC 身分與存取進行疑難排解 \(p. 135\)](#)

## 對象

根據您在 Amazon VPC 中所進行的工作而定，AWS Identity and Access Management (IAM) 的使用方式會不同。

**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。若您無法存取 Amazon VPC 中的某項功能，請參閱[對 Amazon VPC 身分與存取進行疑難排解 \(p. 135\)](#)。

**服務管理員** – 如果您是負責管理您公司的 Amazon VPC 資源，您應該會具備 Amazon VPC 的完整存取權限。您的任務是判斷您員工應存取的 Amazon VPC 功能及資源。您可將請求提交給您的 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。若要進一步了解您公司可搭配 Amazon VPC 使用 IAM 的方式，請參閱[Amazon VPC 如何搭配 IAM 運作 \(p. 127\)](#)。

**IAM 管理員** – 如果您是 IAM 管理員，請了解如何撰寫政策來管理 Amazon VPC 存取的詳細資訊。若要檢視範例政策，請參閱[Amazon VPC 政策範例 \(p. 129\)](#)。

## 使用身分來驗證

身份驗證是使用身分登入資料登入 AWS 的方式。如需使用 AWS 管理主控台 登入的詳細資訊，請參閱 IAM 使用者指南中的 [IAM 主控台及登入頁面](#)。

您必須以 AWS 帳戶根使用者、IAM 使用者，或取得 IAM 角色身分的方式進行身份驗證 (登入 AWS)。您也可以使用貴公司的單一登入身分驗證，甚至使用 Google 或 Facebook 進行登入。在上述案例中，您的管理員會使用 IAM 角色預先設定聯合身分。當您使用來自其他公司的身份驗證來存取 AWS 時，您是間接地擔任角色。

若要直接登入 [AWS 管理主控台](#)，請使用您的密碼及您的 根使用者 電子郵件或您的 IAM 使用者名稱。您可以使用您的 根使用者 或 IAM 使用者存取金鑰，透過編寫程式的方式存取 AWS。AWS 提供軟體開發套件和命令行工具，以加密的方式使用您的登入資料簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。請使用 Signature 第 4 版來執行此作業，它是針對傳入 API 請求進行身份驗證的通訊協定。如需驗證請求的詳細資訊，請參閱 AWS General Reference 中的 [Signature 第 4 版簽署程序](#)。

無論您使用何種身份驗證方法，您可能還需要提供額外的安全性資訊。例如，AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全。若要進一步了解，請參閱 IAM 使用者指南 中的 [在 AWS 中使用多重驗證 \(MFA\)](#)。

## AWS 帳戶根使用者

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

## IAM 使用者和群組

[IAM 使用者](#)是您 AWS 帳戶中的一種實體，具備單一人員或應用程式的特定許可。IAM 使用者可有長期登入資料 (例如，使用者名稱和密碼或一組存取金鑰)。若要了解如何產生存取金鑰，請參閱 IAM 使用者指南中

的[管理 IAM 使用者的存取金鑰](#)。當您產生 IAM 使用者的存取金鑰時，請確認您已檢視且安全地儲存金鑰對。您在這之後便無法復原私密存取金鑰。屆時您必須改為產生新的存取金鑰對。

[IAM 群組](#)是一種指定 IAM 使用者集合的實體。您無法以群組身分登入。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過程變得更為容易。例如，您可以擁有一個名為 IAMAdmin 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登入資料，但角色僅提供暫時登入資料。若要進一步了解，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 帳戶中的一種實體，具備特定許可。它與 IAM 使用者相似，但是不會與特定人員建立關聯。您可以在 AWS 管理主控台中透過[切換角色](#)來暫時取得 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的[使用 IAM 角色](#)。

使用臨時登入資料的 IAM 角色在下列情況中非常有用：

- 暫時 IAM 使用者許可 – IAM 使用者可以取得 IAM 角色來暫時針對特定任務具備不同的許可。
- 聯合身分使用者存取 – 您可以使用 AWS Directory Service、您企業使用者目錄或 Web 身分供應商現有的使用者身分，而不需要建立 IAM 使用者。這些稱為聯合身分使用者。透過[身分供應商](#)來請求存取時，AWS 會指派角色給聯合身分使用者。如需聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的[聯合身分使用者與角色](#)。
- 跨帳戶存取 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶的資源。角色是授予跨帳戶存取的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色做為代理)。若要了解跨帳戶存取角色和資源類型政策間的差異，請參閱 IAM 使用者指南中的[IAM 角色與資源類型政策的差異](#)。
- AWS 服務存取 – 服務角色是服務擔任的 IAM 角色，以代表您在您的帳戶中執行動作。當您設定部分 AWS 服務環境時，您必須定義讓服務擔任的角色。此服務角色必須包含服務存取 AWS 資源所需的所有許可。各個服務的服務角色不同，但許多都可讓您選擇許可，只要您符合該服務所記錄的需求。服務角色提供的存取權僅限在您的帳戶內，不能用來授予存取其他帳戶中的服務。您可以從 IAM 內建立、修改和刪除服務角色。例如，您可以建立一個角色允許 Amazon Redshift 代表您存取 Amazon S3 儲存貯體，然後將儲存貯體中的資料載入 Amazon Redshift 叢集。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。
- 在 Amazon EC2 上執行的應用程式 – 針對在 EC2 執行個體上執行並提出 AWS CLI 或 AWS API 請求的應用程式，您可以使用 IAM 角色來管理臨時登入資料。這是在 EC2 執行個體內存放存取金鑰的較好方式。若要指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個體的執行個體描述檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時登入資料。如需詳細資訊，請參閱 IAM 使用者指南中的[使用 IAM 角色授與許可給 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，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

您可以透過建立政策並將其連接到 IAM 身分或 AWS 資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和實體或資源建立關聯時，便可定義其許可。AWS 會在實體 (根使用者、IAM 使用者或 IAM 角色) 發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式存放在 AWS 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的[JSON 政策概觀](#)。

IAM 管理員可以使用政策指定能存取 AWS 資源的人員，以及他們能在這些資源上執行的動作。每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。換句話說，根據預設，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策連接到使用者。或者，管理員可

以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

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。具備該政策的使用者便可以從 AWS 管理主控台、AWS CLI 或 AWS API 取得使用者資訊。

## 以身分為基礎的政策

身分類型政策是您可以連接到身分 (例如 IAM 使用者、角色或群組) 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](#)。

身分類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。受管政策則是獨立的政策，您可以將這些政策連接到 AWS 帳戶中的多個使用者、群組和角色。受管政策包含 AWS 受管政策和客戶受管政策。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](#)。

## 以資源為基礎的政策

以資源為基礎的政策是附加到資源 (如 Amazon S3 儲存貯體) 的 JSON 政策文件。服務管理員可使用這些政策來定義指定委託人 (帳戶成員、使用者或角色) 可以在什麼情況下對該資源執行什麼動作。以資源為基礎的政策是內嵌政策。不存在受管的以資源為基礎的政策。

## 存取控制清單 (ACL)

存取控制政策 (ACL) 是一種準則，可用來控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類型的政策與以資源為基礎的政策類似，不過其並不使用 JSON 政策文件格式。Amazon S3、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。如需進一步了解 ACL 的相關資訊，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 支援其他較少見的政策類型。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 – 許可界限是一種進階功能，可供您設定身分類型政策能授予 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類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類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。如需許可界限的詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 實體的許可界限](#)。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位的最大許可。AWS Organizations 是一種用來群組和集中管理您商業所擁有多個 AWS 的一項服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需組織和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [SCP 的運作方式](#)。
- 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身分使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分類型政策和工作階段政策的交集。許可也可以來自資源類型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，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。若要了解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

## Amazon VPC 如何搭配 IAM 運作

在您使用 IAM 管理對 Amazon VPC 的存取之前，您應該先了解可搭配 Amazon VPC 使用的 IAM 功能有哪些。若要取得 Amazon VPC 和其他 AWS 服務如何使用 IAM 的高階檢視，請參閱《IAM 使用者指南》中的[使用 IAM 的 AWS 服務](#)。

### 主題

- [動作 \(p. 127\)](#)
- [資源 \(p. 127\)](#)
- [條件鍵 \(p. 128\)](#)
- [Amazon VPC 資源型政策 \(p. 128\)](#)
- [以標籤為基礎的授權 \(p. 129\)](#)
- [IAM 角色 \(p. 129\)](#)

使用 IAM 身分型政策，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

IAM 身分類型政策的 Action 元素會描述政策將允許或拒絕的特定動作。政策動作的名稱通常會和相關聯的 AWS API 操作相同。政策會使用動作來授予執行相關聯操作的許可。

Amazon VPC 與 Amazon EC2 共用其 API 命名空間。Amazon VPC 中的政策動作會在動作之前使用以下字首：ec2:。例如，若要授予某人使用 Amazon EC2 CreateVpc API 操作建立 VPC 的許可，請在其政策中包含 ec2:CreateVpc 動作。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，若要指定開頭是 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《IAM 使用者指南》中的[Amazon EC2 的動作、資源和條件金鑰](#)。

## 資源

Resource 元素可指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。您可以使用 ARN 來指定資源，或是使用萬用字元 (\*) 來指定陳述式套用到所有資源。

### Important

目前，並非所有 Amazon EC2 API 動作都支援資源層級許可。若 Amazon EC2 API 動作不支援資源層級許可，您仍然可以授予使用者使用此動作的許可，但您必須針對政策陳述式中的資源元素指定 \* (萬用字元)。若要檢視您可以為資源元素指定 ARN 的動作，請參閱[Amazon EC2 定義的動作](#)。



VPC 資源具有下列範例所示的 ARN。

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

如需 ARN 格式的詳細資訊，請參閱 [Amazon Resource Name \(ARN\)](#)。

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"
```

若要指定所有屬於特定帳戶的 VPC，請使用萬用字元 (\*)。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

有些 Amazon VPC 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在那些情況下，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 資源類型的清單及其 ARN，請參閱《IAM 使用者指南》中的 [Amazon EC2 定義的資源](#)。

## 條件鍵

Condition 元素 (或 Condition 「區塊」) 可讓您指定使陳述式生效的條件。Condition 元素是選用的。您可以建置使用 [條件運算子](#) 的條件表達式 (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 元素中指定多個金鑰，AWS 會使用邏輯 AND 操作評估他們。若您為單一條件金鑰指定多個值，AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才會授予陳述式的許可。

您也可以在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。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

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 動作均支援 aws:RequestedRegion 和 ec2:Region 條件金鑰。如需詳細資訊，請參閱 [範例：將存取限制在特定區域](#)。

若要查看 Amazon VPC 條件金鑰清單，請參閱 IAM 使用者指南中的 [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](#)。

## Amazon VPC 資源型政策

資源型政策是 JSON 政策文件，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，做為以資源為基礎政策的委託人。新增跨帳戶委託人至資源型政策，只是建立信任關係的一半。當委託人和資源分屬不同的 AWS 帳戶時，您也必須授與委託人實體資源的存取權。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與存取，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](#) 有何不同。

## 以標籤為基礎的授權

您可以將標籤連接到 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 `ec2:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 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[用於標記的資源層級許可](#)。

若要檢視身分型政策範例，了解如何根據資源上的標籤來限制該資源的存取權，請參閱[在特定 VPC 中啟動執行個體](#) (p. 134)。

## IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具備特定許可的實體。

### 使用暫時登入資料

您可以使用暫時登入資料登入聯合、取得 IAM 角色，或是取得跨帳戶角色。您取得暫時安全登入資料的方式是透過呼叫 AWS STS API 操作 (例如，[AssumeRole](#) 或 [GetFederationToken](#))。

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，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Amazon VPC 支援流程日誌的服務角色。建立流程日誌時，您必須選擇允許流程日誌服務存取 CloudWatch Logs 的角色。如需詳細資訊，請參閱[用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色](#) (p. 168)。

## Amazon VPC 政策範例

根據預設，IAM 使用者和角色不具備建立或修改 VPC 資源的許可。他們也無法使用 AWS 管理主控台、AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 操作的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

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[在 JSON 標籤上建立政策](#)。

#### 主題

- [政策最佳實務](#) (p. 130)
- [檢視 Amazon VPC 主控台](#) (p. 130)

- [允許使用者檢視他們自己的許可 \(p. 131\)](#)
- [建立包含公有子網路的 VPC \(p. 132\)](#)
- [修改和刪除 VPC 資源 \(p. 132\)](#)
- [管理安全群組 \(p. 133\)](#)
- [在特定子網路中啟動執行個體 \(p. 134\)](#)
- [在特定 VPC 中啟動執行個體 \(p. 134\)](#)
- [其他 Amazon VPC 政策範例 \(p. 135\)](#)

## 政策最佳實務

身分類型政策相當強大。他們可以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 帳戶產生成本。當您建立或編輯身分類型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策 – 若要快速地開始使用 Amazon VPC，請使用 AWS 受管政策來給予您的員工他們需要的許可。這些政策已在您的帳戶中提供，並由 AWS 維護和更新。如需詳細資訊，請參閱《IAM 使用者指南》中的[開始搭配 AWS 受管政策使用許可](#)。
- 授予最低權限 – 當您建立自訂政策時，請只授予執行任務所需要的許可。以最小一組許可開始，然後依需要授予額外的許可。這比一開始使用太寬鬆的許可，稍後再嘗試將他們限縮更為安全。如需詳細資訊，請參閱《IAM 使用者指南》中的[授予最低權限](#)。
- 為敏感操作啟用 MFA – 為了增加安全，請要求 IAM 使用者使用多重驗證 (MFA) 存取敏感資源或 API 操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[在 AWS 中使用多重驗證 \(MFA\)](#)。
- 使用政策條件以增加安全 – 在切實可行的範圍中，請定義您身分類型政策允許存取資源的條件。例如，您可以撰寫條件，指定請求必須來自一定的允許 IP 地址範圍。您也可以撰寫條件，只在指定的日期或時間範圍內允許請求，或是要求使用 SSL 或 MFA。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素：條件](#)。

## 檢視 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您 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 使用者或角色) 而言，主控台就無法如預期運作。

下列政策會授與使用者在 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: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": "*"
  }
}
]
}

```

您不需要針對只呼叫 AWS CLI 或 AWS API 的使用者允許最基本的主控制台許可。反之，對於這些使用者，只允許存取符合他們需要執行之 API 操作的動作。

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台上，或是使用 AWS CLI 或 AWS API 透過編寫程式的方式完成此動作的許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",

```

```
        "Action": [
            "iam:GetGroupPolicy",
            "iam:GetPolicyVersion",
            "iam:GetPolicy",
            "iam:ListAttachedGroupPolicies",
            "iam:ListGroupPolicies",
            "iam:ListPolicyVersions",
            "iam:ListPolicies",
            "iam:ListUsers"
        ],
        "Resource": "*"
    }
}
```

## 建立包含公有子網路的 VPC

下列範例可讓使用者建立 VPC、子網路、路由表和網際網路閘道。使用者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` 動作可讓使用者啟用 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": "*"
  }]
}
```

上述政策也可讓使用者在 Amazon VPC 主控台中使用第一個 VPC 精靈組態選項來建立 VPC。若要檢視 VPC 精靈，使用者也須具有使用 `ec2:DescribeVpcEndpointServices` 的許可。這可確保 VPC 精靈的 VPC 端點區段正確載入。

## 修改和刪除 VPC 資源

您可能想要控制使用者可以修改或刪除哪些 VPC 資源。例如，下列政策允許使用者使用和刪除具有標籤 `Purpose=Test` 的路由表。此政策也會指定使用者只能刪除具有標籤 `Purpose=Test` 的網際網路閘道。使用者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

下列政策會授予使用者許可來針對特定 VPC 的任何安全群組建立和刪除傳入和傳出規則。此政策執行這項作業的方式是將條件金鑰 (ec2:Vpc) 套用至 Authorize 和 Revoke 動作的安全群組資源。

第二個陳述式會授予使用者許可來說明所有安全群組。這可讓使用者檢視安全群組規則，以便修改它們。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress"],
    "Resource": "arn:aws:ec2:region:account:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeSecurityGroups",
    "Resource": "*"
  }
]
```

若要在 Amazon VPC 主控台的 Security Groups (安全群組) 頁面上檢視安全群組，使用者必須具備使用 ec2:DescribeSecurityGroups 動作的許可。若要使用 Create security group (建立安全群組) 頁面，使用者必須具有使用 ec2:DescribeVpcs 和 ec2:CreateSecurityGroup 動作的許可。

下列政策可讓使用者檢視和建立安全群組。它也可讓他們將傳入和傳出規則新增至與 vpc-11223344556677889 相關聯的任何安全群組，以及從中移除它們。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroups", "ec2:DescribeVpcs", "ec2:CreateSecurityGroup"
    ],
    "Resource": "*"
  }
]
```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup", "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress", "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:*:*:vpc/vpc-11223344556677889"
        }
      }
    }
  ]
}

```

若要允許使用者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。或者，若要讓使用者變更網路界面的安全群組，請將 `ec2:ModifyNetworkInterfaceAttribute` 動作新增至您的政策。

## 在特定子網路中啟動執行個體

下列政策會授予使用者許可以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 `subnet-11223344556677889` 的 ARN 以及 `sg-11223344551122334` 的 ARN。如果使用者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使用者許可來執行該作業)。

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界面，因此使用者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-11223344556677889",
      "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-11223344551122334"
    ]
  }]
}

```

## 在特定 VPC 中啟動執行個體

下列政策會授予使用者許可以在特定 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。

此政策也會授予使用者許可可以僅使用標籤為 `"department=dev"` 的 AMI 啟動執行個體。

```

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

```

```
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:region:account:subnet/*",
    "Condition": {
      "StringEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
      }
    }
  },
  {
    "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 政策範例

您可以在下列主題中找到與 Amazon VPC 相關的其他範例 IAM 政策：

- [ClassicLink](#)
- [受管理的字首清單 \(p. 209\)](#)
- [流量鏡射](#)
- [傳輸閘道](#)
- [VPC 端點 和 VPC 端點 服務](#)
- [VPC 端點政策 \(p. 292\)](#)
- [VPC Peering](#)
- [AWS Wavelength](#)

## 對 Amazon VPC 身分與存取進行疑難排解

請使用以下資訊來協助您診斷和修復使用 Amazon VPC 和 IAM 時發生的常見問題。

### 主題

- [我未獲授權，不得在 Amazon VPC 中執行動作 \(p. 136\)](#)
- [我未獲得執行 iam: PassRole 的授權 \(p. 136\)](#)
- [我想要檢視我的存取金鑰 \(p. 136\)](#)
- [我是管理員，並且想要允許其他人存取 Amazon VPC \(p. 136\)](#)
- [我想要允許 AWS 帳戶以外的人員存取我的 Amazon VPC 資源 \(p. 137\)](#)

## 我未獲授權，不得在 Amazon VPC 中執行動作

若 AWS 管理主控台告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。

以下範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台檢視子網路的詳細資訊，但卻沒有 ec2:DescribeSubnets 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:DescribeSubnets on resource: subnet-id
```

在此情況下，Mateo 會請求管理員更新他的政策，以允許他存取子網路。

## 我未獲得執行 iam: PassRole 的授權

若您收到錯誤，告知您並未獲得執行 iam:PassRole 動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。請求該人員更新您的政策，允許您將角色傳遞給 Amazon VPC。

有些 AWS 服務允許您傳遞現有的角色至該服務，而無須建立新的服務角色或服務連結角色。若要執行此作業，您必須擁有將角色傳遞至該服務的許可。

以下範例錯誤會在名為 marymajor 的 IAM 使用者嘗試使用主控台在 Amazon VPC 中執行動作時發生。但是，動作要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 會請求管理員更新她的政策，允許她執行 iam:PassRole 動作。

## 我想要檢視我的存取金鑰

在您建立 IAM 使用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了秘密金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 AKIAIOSFODNN7EXAMPLE) 和私密存取金鑰 (例如 wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

### Important

請不要將您的存取金鑰提供給第三方，甚至是協助 [尋找您的標準使用者 ID](#)。執行此作業，可能會讓他人能夠永久存取您的帳戶。

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。若您遺失了私密存取金鑰，您必須將新的存取金鑰新增到您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的 [管理存取金鑰](#)。

## 我是管理員，並且想要允許其他人存取 Amazon VPC

若要允許其他人存取 Amazon VPC，您必須針對需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的登入資料來存取 AWS。您接著必須將政策連接到實體，在 Amazon VPC 中授予正確的許可。

若要立即開始使用，請參閱《IAM 使用者指南》中的 [建立您的第一個 IAM 委派使用者及群組](#)。

## 我想要允許 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對象取得該角色。針對支援資源類型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資源的權限。

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 如何搭配 IAM 運作 \(p. 127\)](#)。
- 若要了解如何對您擁有的所有 AWS 帳戶提供資源的存取，請參閱《IAM 使用者指南》中的[對您所擁有的另一個 AWS 帳戶中的 IAM 使用者提供存取](#)。
- 若要了解如何將資源的存取權限提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的[將存取權限提供給第三方擁有的 AWS 帳戶](#)。
- 若要了解如何透過聯合身分提供存取權限，請參閱《IAM 使用者指南》中的[將存取權限提供給在外部進行身份驗證的使用者 \(聯合身分\)](#)。
- 若要了解針對跨帳戶存取使用角色及資源類型政策的差異，請參閱《IAM 使用者指南》中的[IAM 角色與資源類型政策的差異](#)。

## Amazon VPC 的記錄和監控

您可以使用下列自動化監控工具來監看 VPC 中的元件，並在發生錯誤時進行回報：

- **流量日誌：**流量日誌可擷取您 VPC 中傳入和傳出網路界面之 IP 流量資訊。您可以建立 VPC、子網路或個別網路界面的流程日誌。流量日誌資料會發佈至 CloudWatch Logs 或 Amazon S3，並可協助您診斷過度限制或過度寬鬆的安全群組和網路 ACL 規則。如需詳細資訊，請參閱[VPC 流程日誌 \(p. 158\)](#)。
- **監控 NAT 閘道：**您可以使用 CloudWatch 監控 NAT 閘道以收集來自 NAT 閘道的原始資料，並處理為可讀且近乎即時的指標。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控 NAT 閘道 \(p. 233\)](#)。

## Amazon Virtual Private Cloud 中的彈性

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您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、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域與可用區域的詳細資訊，請參閱[AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施外，Amazon VPC 還提供數種支援資料復原和備份需求的功能。

- [Amazon VPC 對 Amazon VPC 連線選項](#)
- [網路對 Amazon VPC 連線選項](#)

## Amazon Virtual Private Cloud 的合規驗證

在多個 AWS 合規計畫中，第三方稽核人員會評估 Amazon Virtual Private Cloud 的安全性與合規。其中包括 SOC、PCI、FedRAMP、DoD CCSP、HIPAA BAA、IRAP、MTCS、C5、K-ISMS、ENS-High、OSPAR 和 HITRUST-CSF。

如需特定合規計畫範圍內的 AWS 服務清單，請參閱[合規計畫範圍內的 AWS 服務](#)。如需一般資訊，請參閱[AWS 合規計畫](#)。



您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱在 [AWS Artifact](#) 中下載報告。

您使用 Amazon VPC 時的合規責任，取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 會提供以下資源協助您處理合規事宜：

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

## VPC 的安全群組

安全群組會做為您執行個體的虛擬防火牆，控制傳入及傳出流量。當您在 VPC 中啟動執行個體時，您可以為執行個體指派最多五個安全群組。安全群組會在執行個體層級執行，而非子網路層級。因此，在您 VPC 中子網路內的每個執行個體都可指派給一組不同的安全群組。

如果您使用 Amazon EC2 API 或命令列工具啟動執行個體，但未指定安全群組，則會自動將執行個體指派給 VPC 的預設安全群組。如果您使用 Amazon EC2 主控台啟動執行個體，您可以選擇為執行個體建立新的安全群組。

針對每個安全群組，您可新增規則，用以控制傳入執行個體的流量，以及另一組規則，用以控制傳出的流量。本節說明 VPC 安全群組及其規則的基本需知事項。

您可以使用與您的安全群組相似的規則來設定網路 ACL，以為您的 VPC 新增額外的安全 layer。如需安全群組與網路 ACL 間差異的詳細資訊，請參閱 [安全群組和網路 ACL 的比較 \(p. 122\)](#)。

### 內容

- [安全群組基礎知識 \(p. 138\)](#)
- [VPC 的預設安全群組 \(p. 139\)](#)
- [安全群組規則 \(p. 140\)](#)
- [EC2-Classic 和 EC2-VPC 間安全群組的差異 \(p. 141\)](#)
- [使用安全群組 \(p. 141\)](#)
- [使用 AWS Firewall Manager 集中管理 VPC 安全群組 \(p. 145\)](#)

## 安全群組基礎知識

下列是您 VPC 安全群組的基礎特性：

- 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，以及您可以與網路界面建立關聯的安全群組數都具有配額。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。
- 您可以指定允許規則，但無法指定拒絕規則。
- 您可以為傳入和傳出規則分別指定規則。
- 當您建立安全群組時，它沒有傳入規則。因此，直到您將傳入規則新增到安全群組之前，來自其他主機的流量都無法傳入您的執行個體。
- 根據預設，安全群組會包含允許所有傳出流量的規則。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，將不會允許來自您執行個體的傳出流量。

- 安全群組是具狀態 — 的，若您從執行個體傳送請求，該請求的回應流量將允許流入，與對內安全群組規則無關。無論傳出規則為何，針對允許傳入流量的回應都會允許傳出。

#### Note

有些類型流量的追蹤方式與其他類型不同。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[連線追蹤](#)。

- 與安全群組相關聯的執行個體無法與彼此交談，除非您新增允許流量的規則 (例外：預設安全群組預設具有這些規則)。
- 安全群組與網路界面關聯。在您啟動執行個體之後，您可以變更與執行個體相關聯的安全群組，以變更與主要網路界面 (eth0) 相關聯的安全群組。您也可以指定或變更與任何其他網路界面相關聯的安全群組。根據預設，當您建立網路界面時，它會與 VPC 的預設安全群組相關聯，除非您指定不同的安全群組。如需網路界面的詳細資訊，請參閱[彈性網路界面](#)。
- 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：
  - 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 . \_ - / ( ) # , @ [ ] + = & ; { } ! \$ \* 。
  - 當名稱尾隨空格時，我們會裁切空格並儲存名稱。例如，如果您輸入「測試安全群組」作為名稱，我們會將其儲存為「測試安全群組」。
  - 安全群組名稱不能以 sg- 為開頭，因為這些表示預設安全群組。
  - 安全群組名稱在 VPC 中必須是唯一的。
- 安全群組只能在您建立安全群組時指定的 VPC 中使用。

## VPC 的預設安全群組

您的 VPC 會自動具有預設安全群組。如果您並未在啟動執行個體時指定不同的安全群組，則與您的執行個體預設安全群組建立關聯。

#### Note

如果您在 Amazon EC2 主控台啟動執行個體，啟動執行個體精靈則自動定義「啟動精靈 **xx**」安全群組，在此您可以與執行個體建立關聯而非預設的安全群組。

下表說明預設安全群組的預設規則。

Inbound			
Source	Protocol	Port range	Description
安全群組 ID (sg-xxxxxxx)	全部	全部	允許來自網路界面 (及其關聯執行個體) 的傳入流量，而這些網路界面會指派給相同的安全群組。
Outbound			
Destination	Protocol	Port range	Description
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。若您使用 IPv6 CIDR 區塊建立 VPC，或是您將 IPv6 CIDR 區塊與您現有的 VPC 建立關聯，根據預設會新增此規則。

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。如果您嘗試刪除預設安全群組，則會收到下列錯誤：`Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user。`

#### Note

若您已修改您安全群組的傳出規則，我們不會在您將 IPv6 區塊與您的 VPC 建立關聯時自動新增 IPv6 流量的傳出規則。

## 安全群組規則

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）。您可以將存取授予特定 CIDR 範圍，或是您 VPC 或對等 VPC（需要 VPC 互連連線）中的另一個安全群組。

下列是 VPC 中安全群組規則的基礎部分：

- （僅限傳入規則）流量的來源以及目標連接埠或連接埠範圍。來源可以是另一個安全群組、IPv4 或 IPv6 CIDR 區塊，或是單一 IPv4 或 IPv6 地址，或字首清單 ID。
- （僅限傳出規則）流量的目標以及目標連接埠或連接埠範圍。目的地可以是另一個安全群組、IPv4 或 IPv6 CIDR 區塊，或是單一 IPv4 或 IPv6 地址，或字首清單 ID。
- 任何具有標準通訊協定號碼的通訊協定（如需清單，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。
- 安全群組規則的選擇性描述，可協助您在稍後進行識別。描述的長度最高可達 255 個字元。允許的字元為 a-z、A-Z、0-9、空格鍵和 `._-:/()#,@[]+=;{}!$*`。
- 如果您使用 AWS CLI 新增安全群組規則，我們會自動將來源或目的地 CIDR 區塊設定為正式格式。例如，如果您為 CIDR 區塊指定 100.68.0.18/18，我們會建立一個 CIDR 區塊為 100.68.0.0/18 的規則。

當您指定 CIDR 區塊做為規則的來源時，將會針對指定的通訊協定和連接埠允許來自指定地址的流量。

當您指定安全群組做為規則的來源時，將會針對指定的通訊協定和連接埠允許來自與來源安全群組相關聯之網路界面的流量。傳入流量會根據與來源安全群組相關聯之網路界面的私有 IP 地址允許（而非公有 IP 或彈性 IP 地址）。新增安全群組做為來源不會新增來源安全群組的規則。如需範例，請參閱「[VPC 的預設安全群組 \(p. 139\)](#)」。

若您指定單一 IPv4 地址，請使用 /32 前綴長度指定地址。若您指定單一 IPv6 地址，請使用 /128 前綴長度指定它。

有些設定防火牆的系統可讓您篩選來源連接埠。安全群組只能讓您篩選目標連接埠。

當您新增或移除規則時，它們會自動套用至與安全群組建立關聯的所有執行個體。

您新增的規則種類可以視安全群組的用途而定。下表描述與 Web 伺服器相關聯之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，並可將 SQL 或 MySQL 流量傳送至資料庫伺服器。

Inbound			
Source	Protocol	Port range	Description
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
您網路的公有 IPv4 地址範圍	TCP	22	允許來自您網路中 IPv4 IP 地址 (透過網際網路閘道) 的傳入 SSH 存取 Linux 執行個體
您網路的公有 IPv4 地址範圍	TCP	3389	允許來自您網路中 IPv4 IP 地址 (透過網際網路閘道) 的傳入 RDP 存取 Windows 執行個體
Outbound			
Destination	Protocol	Port range	Description
您 Microsoft SQL Server 資料庫伺服器安全群組的 ID	TCP	1433	允許傳出 Microsoft SQL Server 存取指定安全群組中的執行個體
您 MySQL 資料庫伺服器安全群組的 ID	TCP	3306	允許傳出 MySQL 存取指定安全群組中的執行個體

資料庫伺服器需要不同的一組規則。例如，相較於傳入 HTTP 和 HTTPS 流量，您可以改為新增一條規則，允許傳入 MySQL 或 Microsoft SQL Server 存取。如需 Web 伺服器 and 資料庫伺服器的安全群組規則範例，請參閱[安全性 \(p. 42\)](#)。如需 Amazon RDS 資料庫執行個體之安全群組的詳細資訊，請參閱 Amazon RDS 使用者指南中的[運用安全群組控制存取](#)。

如需特定類型存取的安全群組規則範例，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[安全群組規則參考](#)。

## 過時的安全群組規則

若您的 VPC 具有和另一個 VPC 的 VPC 互連連線，則安全群組規則可參考對等 VPC 中的另一個安全群組。這可讓與被參考安全群組相關聯的執行個體，以及與參考安全群組相關聯的執行個體彼此通訊。

若對等 VPC 的擁有者刪除參考的安全群組，或是您或對等 VPC 的擁有者刪除 VPC 互連連線，則安全群組規則會標記為 `stale`。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 Peering Guide 中的[使用過時安全群組](#)。

## EC2-Classic 和 EC2-VPC 間安全群組的差異

您無法使用您已建立的安全群組來搭配您 VPC 中的執行個體使用 EC2-Classic。您必須為使用您 VPC 中的執行個體建立特別的安全群組。您為使用 VPC 安全群組而建立的規則無法參考 EC2-Classic 的安全群組，反之亦然。如需關於使用 EC2-Classic 和使用 VPC 時安全群組的差異詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的[EC2-Classic 與 VPC 之間的差異](#)。

## 使用安全群組

下列任務會示範如何搭配 Amazon VPC 主控台使用安全群組。

如需使用安全群組的範例 IAM 政策，請參閱[管理安全群組 \(p. 133\)](#)。

工作

- [修改預設安全群組 \(p. 142\)](#)

- [建立安全群組](#) (p. 142)
- [新增、移除和更新規則](#) (p. 142)
- [變更執行個體的安全群組](#) (p. 144)
- [刪除安全群組](#) (p. 144)
- [刪除 2009-07-15-default 安全群組](#) (p. 145)

## 修改預設安全群組

您的 VPC 包括[預設安全群組](#) (p. 139)。您無法刪除此群組；但是，您可以變更群組的規則。程序與修改任何其他的安全群組相同。如需詳細資訊，請參閱[新增、移除和更新規則](#) (p. 142)。

## 建立安全群組

雖然您可以針對您的執行個體使用預設安全群組，但您可能會希望建立您自己的群組，以反映執行個體在您系統上所扮演的不同角色。

### 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 Security Groups (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 (例如，my-security-group)，並提供描述。
5. 在 VPC 中，選取 VPC 的 ID。
6. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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 Create (建立)。

### 使用命令列建立安全群組

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (適用於 Windows PowerShell 的 AWS 工具)

### 使用命令列描述一或多個安全群組

- [describe-security-groups](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (適用於 Windows PowerShell 的 AWS 工具)

根據預設，新的安全群組一開始只有允許流量離開執行個體的傳出規則。您必須新增規則啟用任何傳入流量，或是限制傳出流量。

## 新增、移除和更新規則

當您新增或移除規則時，任何已指派給安全群組的執行個體都會套用變更。

若您有 VPC 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 Peering Guide 中的[更新您的安全群組以參考對等連接的 VPC 安全群組](#)。

#### 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 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)。在 Type (類型) 中，選取流量類型，然後指定來源 (輸入規則) 或目的地 (輸出規則)。例如，針對公有 Web 伺服器，請選擇 HTTP 或 HTTPS，然後指定 Source (來源) 的值為 0.0.0.0/0。

若您使用 0.0.0.0/0，您會啟用所有使用 HTTP 或 HTTPS 來存取您執行個體的 IPv4 地址。若要限制存取，請輸入特定的 IP 地址或地址範圍。

6. 您也可以允許所有和此安全群組相關聯之執行個體間的通訊。使用下列選項建立傳入規則：

- Type (類型)：All Traffic (所有流量)
- Source (來源)：輸入安全群組的 ID。

7. 選擇 Save rules (儲存規則)。

#### 使用主控台刪除規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 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. 選擇要刪除之規則右側的刪除按鈕 (「x」)。
6. 選擇 Save rules (儲存規則)。

當您使用主控台修改現有安全群組規則的通訊協定、連接埠範圍，或來源或目標時，主控台會刪除現有規則並為您建立新的規則。

#### 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 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. 依需求修改規則項目。
6. 選擇 Save rules (儲存規則)。

如果您是使用 Amazon EC2 API 或命令列工具，更新現有規則的通訊協定、連接埠範圍，或來源或目標，則無法修改規則。相反的，您必須刪除現有規則並新增新的規則。若要僅更新規則描述，您可以使用 [update-security-group-rule-descriptions-ingress](#) 和 [update-security-group-rule-descriptions-egress](#) 命令。

#### 使用命令列為安全群組新增規則

- [authorize-security-group-ingress](#) 以及 [authorize-security-group-egress](#) (AWS CLI)



- [Grant-EC2SecurityGroupIngress](#) 以及 [Grant-EC2SecurityGroupEgress](#) (適用於 Windows PowerShell 的 AWS 工具)

使用命令列從安全群組刪除規則

- [revoke-security-group-ingress](#) 以及 [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) 以及 [Revoke-EC2SecurityGroupEgress](#) (適用於 Windows PowerShell 的 AWS 工具)

使用命令列更新安全群組規則的描述

- [update-security-group-rule-descriptions-ingress](#) 以及 [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) 以及 [Update-EC2SecurityGroupRuleEgressDescription](#) (適用於 Windows PowerShell 的 AWS 工具)

## 變更執行個體的安全群組

在 VPC 內啟動執行個體之後，您可以變更與執行個體相關聯的安全群組。您可以在執行個體處於 `running` 或 `stopped` 狀態時變更執行個體的安全群組。

### Note

此程序會變更與執行個體主要網路界面 (eth0) 相關聯的安全群組。若要變更其他網路界面的安全群組，請參閱[變更安全群組](#)。

使用主控台變更執行個體的安全群組

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)。
3. 開啟執行個體的內容 (按右鍵) 選單，然後選擇 Networking (聯網)、Change Security Groups (變更安全群組)。
4. 在 Change Security Groups (變更安全群組) 對話方塊中，從清單選取一或多個安全群組，然後選擇 Assign Security Groups (指派安全群組)。

使用命令列變更執行個體的安全群組

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (適用於 Windows PowerShell 的 AWS 工具)

## 刪除安全群組

您只能在沒有任何執行個體指派給安全群組時 (執行中或停止) 才能刪除安全群組。您可以在刪除安全群組前將執行個體指派給另一個安全群組 (請參閱 [變更執行個體的安全群組](#) (p. 144))。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 Security Groups (安全群組)。
3. 選取一或多個安全群組，然後選擇 Security Group Actions (安全群組動作)、Delete Security Group (刪除安全群組)。
4. 在 Delete Security Group (刪除安全群組) 對話方塊中，選擇 Yes, Delete (是，刪除)。

使用命令列刪除安全群組

- `delete-security-group` (AWS CLI)
- `Remove-EC2SecurityGroup` (適用於 Windows PowerShell 的 AWS 工具)

## 刪除 2009-07-15-default 安全群組

任何使用比 2011-01-01 更早的 API 版本建立的 VPC 都具有 2009-07-15-default 安全群組。此安全群組會與每個 VPC 預設具有的一般 default 安全群組一同出現。您無法將網際網路閘道連接到具有 2009-07-15-default 安全群組的 VPC。因此，在您連接網際網路閘道到 VPC 前，您必須刪除此安全群組。

### Note

若您將此安全群組指派給任何執行個體，您必須為這些執行個體指派不同的安全群組，才能刪除此安全群組。

### 刪除 2009-07-15-default 安全群組

1. 確認此安全群組沒有指派給任何執行個體。
  - a. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
  - b. 在導覽窗格中，選擇 Network Interfaces (網路界面)。
  - c. 從清單選取執行個體的網路界面，然後選擇 Change Security Groups (變更安全群組)、Actions (動作)。
  - d. 在 Change Security Groups (變更安全群組) 對話方塊中，從清單選取新的安全群組，然後選擇 Save (儲存)。  
  
變更執行個體的安全群組時，您可以從清單選取多個群組。您選取的安全群組會取代執行個體目前的安全群組。
  - e. 為每個執行個體重複前述步驟。
2. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Security Groups (安全群組)。
4. 選擇 2009-07-15-default 安全群組，然後選擇 Security Group Actions (安全群組動作)、Delete Security Group (刪除安全群組)。
5. 在 Delete Security Group (刪除安全群組) 對話方塊中，選擇 Yes, Delete (是，刪除)。

## 使用 AWS Firewall Manager 集中管理 VPC 安全群組

使用 AWS Firewall Manager 簡化您多個帳戶和資源的 VPC 安全群組管理及維護工作。您可以使用 Firewall Manager 從單一中央系統管理員帳戶設定和稽核組織的安全群組。Firewall Manager 會自動將規則和保護套用至您的帳戶和資源，即使您新增資源也一樣。當您想要保護整個組織，或是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。您可以設定政策的範圍為稽核所有帳戶、特定帳戶，或組織內標記的資源。Firewall Manager 會自動偵測新帳戶和資源並進行稽核。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。

若要深入了解如何使用 Firewall Manager 來管理安全群組，請參閱AWS WAF 開發人員指南中的下列主題：

- [AWS Firewall Manager 先決條件](#)
- [AWS Firewall Manager Amazon VPC 安全群組政策入門](#)
- [安全群組政策如何在 AWS Firewall Manager 中運作](#)
- [安全群組政策使用案例](#)

## 網路 ACL

網路存取控制清單 (ACL) 是 VPC 中的選用安全層，作用就像防火牆，可控制一或多個子網路的傳入和傳出流量。您可以使用與您的安全群組相似的規則來設定網路 ACL，以為您的 VPC 新增額外的安全 layer。如需安全群組與網路 ACL 間差異的詳細資訊，請參閱[安全群組和網路 ACL 的比較 \(p. 122\)](#)。

### 內容

- [網路 ACL 基本概念 \(p. 146\)](#)
- [網路 ACL 規則 \(p. 147\)](#)
- [預設網路 ACL \(p. 147\)](#)
- [自訂網路 ACL \(p. 148\)](#)
- [自訂網路 ACL 和其他 AWS 服務 \(p. 151\)](#)
- [暫時性連接埠 \(p. 152\)](#)
- [路徑 MTU 探索 \(p. 152\)](#)
- [使用網路 ACL \(p. 152\)](#)
- [範例：控制對子網路中執行個體的存取 \(p. 156\)](#)
- [VPC 精靈案例的建議規則 \(p. 158\)](#)

## 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，並將其與子網路建立關聯。根據預設，在您新增規則之前，每個自訂網路 ACL 都會拒絕所有傳入和傳出流量。
- 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 包含規則編號清單。我們會按順序評估規則，從最低數字的規則開始，以判斷流量是否允許進出與網路 ACL 相關聯的任何子網路。您可以用於規則的最高數字為 32766。我們建議您先以增量方式建立規則 (例如 10 或 100 的增量)，以便稍後可在需要的位置插入新規則。
- 網路 ACL 具有個別的傳入和傳出規則，且每個規則都可以允許或拒絕流量。
- 網路 ACL 為無狀態，這表示，對於允許的傳入流量回應仍會受制於傳出流量規則 (反之亦然)。

每個 VPC 的網路 ACL 數目和每個網路 ACL 的規則數目有配額 (限制)。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。

## 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。
- 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)。
- 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

若您已修改預設的網路 ACL 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 流量的允許規則。同樣地，若您已修改傳出規則，我們就不會自動新增傳出 IPv6 流量的允許規則。

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
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

下表顯示 VPC 的自訂網路 ACL 範例，其僅支援 IPv4。其中包括的規則可允許 HTTP 和 HTTPS 流量進入 (傳入規則 100 和 110)。也有對應的傳出規則，可啟用對上述傳入流量的回應 (傳出規則 120，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](#) (p. 152)。

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 (傳入規則 140，其涵蓋暫時性連接埠 32768-65535)。

### Note

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	評論
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。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 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	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	評論
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	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。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 <a href="#">暫時性連接埠 (p. 152)</a> 。
*	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。

下表顯示相同的 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

在 IPv4 規則之後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	評論
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 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	<p>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)。</p> <p>此範圍僅為範例。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<a href="#">暫時性連接埠 (p. 152)</a>。</p>
145	自訂 TCP	TCP	32768-65535	::/0	允許	<p>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)。</p> <p>此範圍僅為範例。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<a href="#">暫時性連接埠 (p. 152)</a>。</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	評論
100	HTTP	TCP	80	0.0.0.0/0	允許	允許傳出 IPv4 HTTP 流量從子網路流向網際網路。
105	HTTP	TCP	80	::/0	允許	允許傳出 IPv6 HTTP 流量從子網路流向網際網路。
110	HTTPS	TCP	443	0.0.0.0/0	允許	允許傳出 IPv4 HTTPS 流量從子網路流向網際網路。
115	HTTPS	TCP	443	::/0	允許	允許傳出 IPv6 HTTPS 流量從子網路流向網際網路。
120	自訂 TCP	TCP	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。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<a href="#">暫時性連接埠 (p. 152)</a>。</p>
125	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。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<a href="#">暫時性連接埠 (p. 152)</a>。</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。

如需更多範例，請參閱 [VPC 精靈案例的建議規則 \(p. 158\)](#)。

## 自訂網路 ACL 和其他 AWS 服務

如您建立自訂網路 ACL，請了解其將如何影響您使用其他 AWS 服務建立的資源。

使用 Elastic Load Balancing 時，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 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) 使用連接埠 32768-61000。
- 來自 Elastic Load Balancing 的請求使用連接埠 1024-65535。
- Windows 作業系統到 Windows Server 2003 使用連接埠 1025-5000。
- Windows Server 2008 和更新版本使用連接埠 49152-65535。
- NAT 閘道使用連接埠 1024-65535。
- AWS Lambda 函式會使用連接埠 1024-65535。

例如，如果送達 VPC 之 Web 伺服器的請求來自網際網路的 Windows XP 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 1025-5000。

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) 的暫時性連接埠。

實際操作時，為了涵蓋各種可能初始化流量至 VPC 中公開發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 搜尋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。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傳回下列 ICMP 訊息：Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (類型 3，代碼 4)。如此原始主機就會調整 MTU 直到封包順利傳送。

如果子網路中主機之間的最大傳輸單位 (MTU) 不同，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 Linux 執行個體的 Amazon EC2 使用者指南 中的 [您 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。

工作

- [判斷網路 ACL 關聯 \(p. 153\)](#)
- [建立網路 ACL \(p. 153\)](#)
- [新增和刪除規則 \(p. 153\)](#)
- [將子網路與網路 ACL 建立關聯 \(p. 154\)](#)
- [取消子網路與網路 ACL 的關聯 \(p. 154\)](#)

- [變更子網路的網路 ACL \(p. 155\)](#)
- [刪除網路 ACL \(p. 155\)](#)
- [API 和命令概觀 \(p. 155\)](#)

## 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。

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。如需命令列界面與可用 API 清單的詳細資訊，請參閱[存取 Amazon VPC \(p. 1\)](#)。

### 為您的 VPC 建立網路 ACL

- [create-network-acl](#) (AWS CLI)
- [New-EC2NetworkAcl](#) (適用於 Windows PowerShell 的 AWS 工具)

### 說明一或多個網路 ACL

- [describe-network-acls](#) (AWS CLI)
- [Get-EC2NetworkAcl](#) (適用於 Windows PowerShell 的 AWS 工具)

### 新增規則至網路 ACL

- [create-network-acl-entry](#) (AWS CLI)
- [New-EC2NetworkAclEntry](#) (適用於 Windows PowerShell 的 AWS 工具)

### 刪除網路 ACL 中的規則

- [delete-network-acl-entry](#) (AWS CLI)

- [Remove-EC2NetworkAclEntry](#) (適用於 Windows PowerShell 的 AWS 工具)

取代網路 ACL 中的現有規則

- [replace-network-acl-entry](#) (AWS CLI)
- [Set-EC2NetworkAclEntry](#) (適用於 Windows PowerShell 的 AWS 工具)

取代網路 ACL 關聯

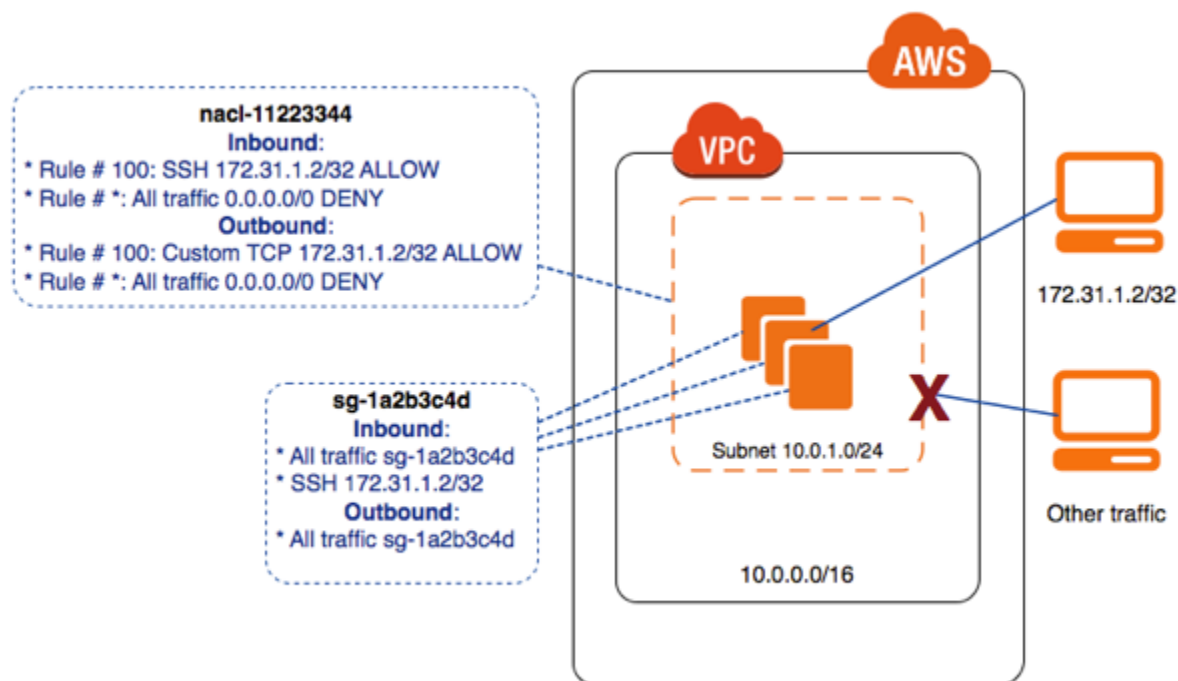
- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (適用於 Windows PowerShell 的 AWS 工具)

刪除網路 ACL

- [delete-network-acl](#) (AWS CLI)
- [Remove-EC2NetworkAcl](#) (適用於 Windows PowerShell 的 AWS 工具)

## 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。



所有執行個體都會使用相同安全群組 (sg-1a2b3c4d)，並使用下列規則：

傳入規則

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-1a2b3c4d	可讓與相同安全群組相關聯的執行個體彼此通訊。
SSH	TCP	22	172.31.1.2/32	允許來自遠端電腦的傳入 SSH 存取。如果執行個體是 Windows 電腦，則此規則必須改為對連接埠 3389 使用 RDP 通訊協定。

#### 傳出規則

通訊協定類型	通訊協定	連接埠範圍	目的地	評論
所有流量	全部	全部	sg-1a2b3c4d	可讓與相同安全群組相關聯的執行個體彼此通訊。安全群組有狀態。因此，您不需要允許傳入請求之回應流量的規則。

這個子網路會與具有下列規則的網路 ACL 相互關聯。

#### 傳入規則

規則 #	類型	通訊協定	連接埠範圍	來源	允許/拒絕	評論
100	SSH	TCP	22	172.31.1.2/32	允許	允許來自遠端電腦的傳入流量。如果執行個體是 Windows 電腦，則此規則必須改為對連接埠 3389 使用 RDP 通訊協定。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕所有其他不符合上述規格的傳入流量。

#### 傳出規則

規則 #	類型	通訊協定	連接埠範圍	目的地	允許/拒絕	評論
100	自訂 TCP	TCP	1024-65535	172.31.1.2/32	允許	允許對遠端電腦的傳出回應。網路 ACL 無狀態。因此，



						必須使用此規則才能允許傳入請求的回應流量。
*	所有流量	全部	全部	0.0.0.0/0	拒絕	拒絕所有其他不符合上述規格的傳出流量。

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。網路 ACL 規則會套用至子網路中的所有執行個體。如果您不小心將安全群組規則設得太寬鬆，網路 ACL 規則仍會持續只允許來自單一 IP 地址的存取。例如，下列規則比之前的規則更加寬鬆：它們允許來自任何 IP 地址的傳入 SSH 存取。

#### 傳入規則

類型	通訊協定	連接埠範圍	來源	評論
所有流量	全部	全部	sg-1a2b3c4d	可讓與相同安全群組相關聯的執行個體彼此通訊。
SSH	TCP	22	0.0.0.0/0	允許來自任何 IP 地址的 SSH 存取。

#### 傳出規則

類型	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。

不過，僅有子網路內的其他執行個體和遠端電腦可以存取此執行個體。網路 ACL 規則仍會阻擋所有前往子網路的傳入流量（來自遠端電腦的傳入流量除外）。

## VPC 精靈案例的建議規則

您可以使用 Amazon VPC 主控台其中的 VPC 精靈來實作 Amazon VPC 的常用案例。若您依照文件中的說明實作這些案例，您會使用預設網路存取控制清單 (ACL)，允許所有傳入及傳出流量。若您需要額外的安全 layer，您可以建立網路 ACL 並新增規則。如需詳細資訊，請參閱 [Amazon VPC 主控台精靈組態 \(p. 17\)](#)。

## VPC 流程日誌

VPC 流程日誌是一項可讓您擷取傳入及傳出您 VPC 中網路界面之 IP 流量相關資訊的功能。流程日誌資料可發佈至 Amazon CloudWatch Logs 或 Amazon S3。建立流量日誌之後，您可以在選擇的目的地中擷取及檢視其資料。

流程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
- 判斷網路界面往來流量的方向



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。

#### 內容

- [流程日誌基礎知識](#) (p. 159)
- [流程日誌記錄](#) (p. 160)
- [流程日誌記錄範例](#) (p. 163)
- [流程日誌限制](#) (p. 167)
- [流程日誌定價](#) (p. 168)
- [將流程日誌發佈至 CloudWatch Logs](#) (p. 168)
- [將流程日誌發佈至 Amazon S3](#) (p. 172)
- [使用流程日誌](#) (p. 176)
- [疑難排解](#) (p. 180)

## 流程日誌基礎知識

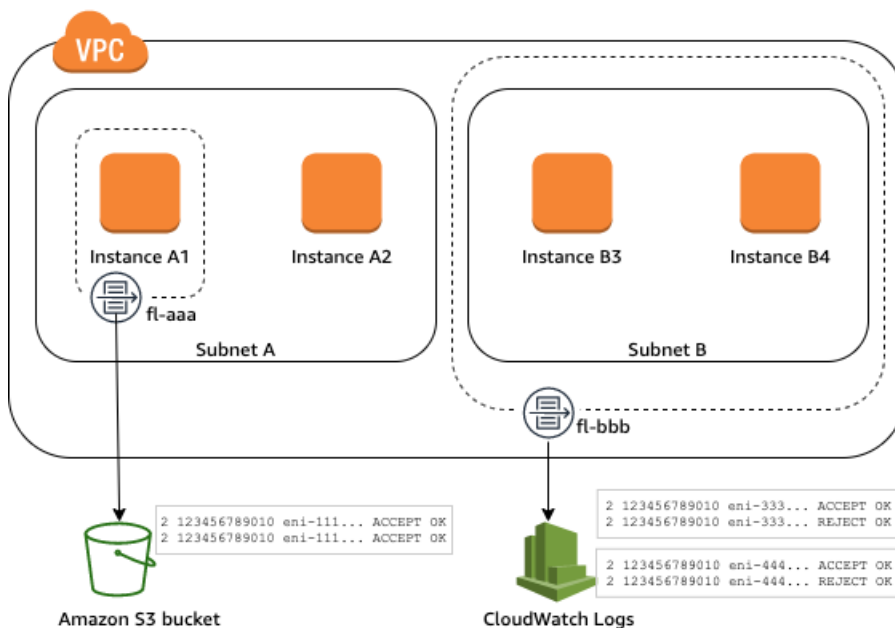
您可以建立 VPC、子網路或網路界面的流程日誌。如果建立子網路或 VPC 的流程日誌，則會監控該子網路或 VPC 中的每個網路界面。

監控之網路界面的流程日誌將記錄為流程日誌記錄，即由描述流量之欄位組成的日誌事件。如需詳細資訊，請參閱「[流程日誌記錄](#) (p. 160)」。

若要建立流程日誌，您要指定：

- 要建立流程日誌的資源
- 要擷取的流量類型 (接受的流量、拒絕的流量，或全部流量)
- 流程日誌資料的發佈目標

在下列範例中，您會建立流程日誌 (fl-aaa)，以擷取網路介面 (例如 A1) 的接受流量，並將流程記錄記錄發佈至 Amazon S3 儲存貯體。您可以建立第二個流程日誌，擷取子網路 B 的所有流量，並將流程日誌記錄發佈到 Amazon CloudWatch Logs。流程日誌 (fl-bbb) 會擷取子網路 B 中所有網路介面的流量，沒有可擷取執行個體 A2 網路介面流量的流量日誌。



在您建立流程日誌之後，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。流程日誌不會擷取您網路界面的即時日誌串流。如需更多詳細資訊，請參閱 [建立流程日誌 \(p. 177\)](#)。

如果在建立子網路或 VPC 的流程日誌後，在子網路中啟動多個執行個體，則會針對每個新的網路界面建立新的日誌串流 (在 CloudWatch Logs) 或日誌檔案物件 (在 Amazon S3)。一記錄到該網路界面的任何網路流量即會發生此情況。

您可以為其他 AWS 服務建立的網路界面建立流程日誌，例如：

- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- NAT 閘道
- 傳輸閘道

無論網路界面的類型為何，您都必須使用 Amazon EC2 主控台或 Amazon EC2 API 建立網路界面的流程日誌。

您可以將標籤套用至流程日誌。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程日誌，例如依據用途或擁有者整理日誌。

如果您不再需要流程日誌，即可將其刪除。刪除流程日誌會停用資源的流程日誌服務，並且將不會再建立新的流程日誌記錄或將其發佈至 CloudWatch Logs 或 Amazon S3。刪除流程日誌不會刪除網路界面的任何現有流程日誌紀錄或日誌串流 (在 CloudWatch Logs) 或日誌檔案物件 (在 Amazon S3)。若要刪除現有的日誌串流，請使用 CloudWatch Logs 主控台。若要刪除現有的檔案物件，請使用 Amazon S3 主控台。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。如需詳細資訊，請參閱 [刪除流程日誌 \(p. 179\)](#)。

## 流程日誌記錄

流程日誌紀錄代表您 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 (特徵為每個網路界面一個 5 元組)。

根據預設，紀錄包含 IP 流程不同元件的值，包括來源、目標和協定。

建立流程日誌時，您可以使用流程日誌紀錄的預設格式，或指定自訂格式。

主題

- [彙總時間間隔 \(p. 160\)](#)
- [預設格式 \(p. 161\)](#)
- [自訂格式 \(p. 161\)](#)
- [可用的欄位 \(p. 161\)](#)

## 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程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。建立流程日誌時，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 分鐘的流程日誌所產生的流程日誌記錄量會高於最大彙總時間間隔 10 分鐘的流程日誌。

當網路界面連接至 [Nitro 型執行個體](#) 時，無論指定的最大彙總時間間隔為何，彙總時間間隔一律為 1 分鐘或更短。

在彙總時間間隔內擷取資料之後，需要額外的時間來處理和發佈資料至 CloudWatch Logs 或 Amazon S3。發佈到 CloudWatch Logs 時，這段額外時間可能 5 分鐘左右，而發佈到 Amazon S3 可能 10 分鐘左右。流程日誌服務會在這個額外的時間內盡全力傳遞。在某些情況下，您的日誌可能會比先前提及的額外時間延遲超過 5 到 10 分鐘。

## 預設格式

根據預設，流程日誌紀錄的日誌行格式是以空格分隔的字串，具有以下依下列順序排列的欄位集。

```
<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol>  
<packets> <bytes> <start> <end> <action> <log-status>
```

如需欄位的相關資訊，請參閱[可用的欄位](#) (p. 161)。預設格式僅擷取流程日誌紀錄所有可用欄位的一部分。若要擷取全部可用欄位或其他不同的欄位，請指定自訂格式。您無法自訂或變更預設格式。

## 自訂格式

您可以選擇性指定流程日誌紀錄的自訂格式。如需自訂格式，您要指定在流程日誌紀錄中傳回哪些欄位，以及其應有的出現順序。這樣可讓您建立專門針對需求的流程日誌，省略不相關的欄位。自訂格式也有利於降低隔開處理序，從已發佈流程日誌擷取特定資訊的需求。您可指定任何數量的可用流程日誌欄位，但至少必須指定一個。

## 可用的欄位

下表描述流程日誌紀錄的所有可用欄位。版本欄表示導入此欄位的 VPC 流程日誌版本。

欄位	描述	版本
version	VPC 流程日誌版本。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。	2
account-id	為其記錄流量之來源網路介面的擁有者 AWS 帳戶 ID。如果網路介面是由 AWS 服務所建立，例如在建立 VPC 端點或網路負載平衡器時，記錄可能會在此欄位顯示 unknown。	2
interface-id	要記錄流量的網路介面 ID。	2
srcaddr	網路界面上傳入流量的來源地址，或傳出流量網路界面的 IPv4 或 IPv6 地址。網路界面的 IPv4 地址永遠都是其私有 IPv4 地址。另請參閱 pkt-srcaddr。	2
dstaddr	網路界面上傳出流量的目標地址，或傳入流量網路界面的 IPv4 或 IPv6 地址。網路界面的 IPv4 地址永遠都是其私有 IPv4 地址。另請參閱 pkt-dstaddr。	2
srcport	流量的來源連接埠。	2
dstport	流量的目標連接埠。	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> 。	2
packets	在流程期間傳輸的封包數。	2
bytes	在流程期間傳輸的位元組數。	2

欄位	描述	版本
start	彙總時間間隔內接收到第一個流量封包的時間 (以 Unix 秒為單位)。這個時間最長可能是在網路界面上傳送或接收封包之後 60 秒。	2
end	彙總時間間隔內接收到最後一個流量封包的時間 (以 Unix 秒為單位)。這個時間最長可能是在網路界面上傳送或接收封包之後 60 秒。	2
action	與流量相關聯的動作： <ul style="list-style-type: none"> <li>ACCEPT：記錄的流量已獲得安全群組和網路 ACL 的許可。</li> <li>REJECT：記錄的流量未獲得安全群組或網路 ACL 的許可。</li> </ul>	2
log-status	流程日誌的記錄狀態： <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界面的網路流量。</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>	2
vpc-id	包含要記錄流量之網路界面的 VPC ID。	3
subnet-id	包含要記錄流量之網路界面的子網路 ID。	3
instance-id	如果您擁有執行個體，則為與要記錄流量之網路界面相關聯的執行個體 ID。傳回申請者管理網路界面的 '-' 符號，例如，NAT 閘道的網路界面。	3
tcp-flags	下列 TCP 標記的位元遮罩值： <ul style="list-style-type: none"> <li>SYN：2</li> <li>SYN-ACK：18</li> <li>FIN：1</li> <li>RST：4</li> </ul> <p>只有伴隨 SYN 時才回報 ACK。</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，標記可能和流程日誌紀錄設在同一行，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 (p. 165)</a>」。</p>	3
type	流量類型：IPv4、IPv6 或 EFA。如需 Elastic Fabric Adapter (EFA) 的詳細資訊，請參閱 <a href="#">Elastic Fabric Adapter</a> 。	3
pkt-srcaddr	流量的封包層級 (原始) 來源 IP 地址。使用此欄位搭配 srcaddr 欄位來分辨流量流經之中繼 layer 的 IP 地址，以及流量的原始來源 IP 地址。例如，當流量流經 NAT 閘道的網路界面 (p. 165) 時，或 Amazon EKS 的 Pod IP 地址和 Pod 執行所在執行個體節點的網路界面 IP 地址不同時 (用於 VPC 內部通訊)。	3

欄位	描述	版本
pkt-dstaddr	流量的封包層級 (原始) 目標 IP 地址。使用此欄位搭配 dstaddr 欄位來分辨流量流經之中繼 layer 的 IP 地址，以及流量的最終目標 IP 地址。例如，當流量流經 <a href="#">NAT 閘道的網路界面 (p. 165)</a> 時，或 Amazon EKS 的 Pod IP 地址和 Pod 執行所在執行個體節點的網路界面 IP 地址不同時 (用於 VPC 內部通訊)。	3
region	包含記錄流量之網路介面的區域。	4
az-id	可用區域的識別碼，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。	4
sublocation-type	在 sublocation-id 欄位中傳回的子位置類型： <ul style="list-style-type: none"><li><a href="#">wavelength</a></li><li><a href="#">outpost</a></li><li><a href="#">localzone</a></li></ul> 如果流量不是來自子位置，則記錄會顯示此欄位的 '-' 符號。	4
sublocation-id	包含要記錄流量之網路介面的子位置 ID。如果流量不是來自子位置，則記錄會顯示此欄位的 '-' 符號。	4

#### Note

若欄位不適用於特定記錄，則記錄會針對該項目顯示一個 '-' 符號。

## 流程日誌記錄範例

以下是擷取特定流量的流程日誌紀錄範例。

如需流程日誌記錄格式的資訊，請參閱 [流程日誌記錄 \(p. 160\)](#)。

如需如何建立流程記錄的相關資訊，請參閱 [the section called “使用流程日誌” \(p. 176\)](#)。

#### 內容

- [接受與拒絕的流量 \(p. 163\)](#)
- [無任何資料及略過的紀錄 \(p. 164\)](#)
- [安全群組及網路 ACL 規則 \(p. 164\)](#)
- [IPv6 流量 \(p. 164\)](#)
- [TCP 標記序列 \(p. 165\)](#)
- [通過 NAT 閘道的流量 \(p. 165\)](#)
- [通過傳輸閘道的流量 \(p. 166\)](#)

## 接受與拒絕的流量

以下是預設流程日誌記錄的範例。

在本範例中，允許帳戶 123456789010 中網路界面 eni-1235b8ca123456789 的 SSH 流量 (目標連接埠 22，TCP 協定)。

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
1418530010 1418530070 ACCEPT OK
```

在本範例中，拒絕帳戶 123456789010 中網路界面 eni-1235b8ca123456789 的 RDP 流量 (目標連接埠 3389，TCP 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紀錄

以下是預設流程日誌記錄的範例。

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，彙總時間間隔內曾跳過記錄。

```
2 123456789010 eni-11111111aaaaaaaa - - - - - 1431280876 1431280934 - SKIPDATA
```

## 安全群組及網路 ACL 規則

如使用流程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 (網路界面的私有 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。在預設的流程日誌中，這會顯示為兩筆流程日誌紀錄：

- 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，則流程日誌會顯示兩個 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，則流程日誌會顯示單一 REJECT 記錄，因為流量未獲准能觸達您的執行個體。

## IPv6 流量

以下是預設流程日誌記錄的範例。在本範例中，允許來自帳戶 123456789010 中網路界面 eni-1235b8ca123456789 之 IPv6 地址 2001:db8:1234:a100:8d6e:3477:df66:f105 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

以下的自訂流程日誌範例，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
```

tcp-flags 欄位可協助您識別流量方向，例如哪部伺服器啟動了連線。在下列紀錄中 (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程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，私有子網路中的執行個體透過位在公有子網路中的 NAT 閘道存取網際網路。



以下 NAT 閘道網路界面的自訂流程日誌會依以下順序擷取下列欄位。

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

流程日誌顯示流量從執行個體 IP 地址 (10.0.1.5) 經由 NAT 閘道網路界面流向網際網路的主機 (203.0.113.5)。NAT 閘道網路界面是申請者管理的網路界面，因此流程日誌紀錄會在 instance-id 欄位顯示 '-' 符號。下行顯示從來源執行個體流向 NAT 閘道網路界面的流量。dstaddr 和 pkt-dstaddr 欄位的值不一樣。dstaddr 欄位顯示 NAT 閘道網路界面的私有 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 閘道網路界面流向網際網路目標主機的流量，以及從主機到 NAT 閘道網路界面的回應流量。

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

下行顯示從 NAT 閘道網路界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 閘道網路界面的私有 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，建立另一個自訂流程日誌。您為私有子網路中的執行個體建立網路界面的流程日誌。在本案例中，instance-id 欄位會傳回與網路界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 閘道的網路界面不同，此網路界面不是流量的中繼網路界面。

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5  
#Traffic from the source instance to host on the internet  
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5  
#Response traffic from host on the internet to the source instance
```

## 通過傳輸閘道的流量

在本範例中，VPC A 中的用戶端透過 transit gateway 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。因此，流量使用 eni-1111111111111111 到達 VPC B 的伺服器，但使用 eni-2222222222222222 離開 VPC B。

您使用以下格式建立 VPC B 的自訂流程日誌。

```
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
```

下列數行流程日誌紀錄示範 Web 伺服器網路界面上的流量。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-22222222bbbbbbbbbb  
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
```

下行是子網路 subnet-11111111aaaaaaaa 中，transit gateway申請者管理網路界面 eni-1111111111111111 上的請求流量。因此，流程日誌記錄在 instance-id 欄位會顯示 '-' 符號。srcaddr 欄位顯示transit gateway網路界面的私有 IP 地址，而 pkt-srcaddr 欄位則顯示 VPC A 中用戶端的 IP 地址。

```
3 eni-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaa -  
10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

下行是子網路 subnet-22222222bbbbbbbbbb 中，transit gateway申請者管理網路界面 eni-2222222222222222 上的回應流量。dstaddr 欄位顯示transit gateway網路界面的私有 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
```

## 流程日誌限制

若要使用流程日誌，您必須注意下列限制：

- 您無法啟用位於 EC2-Classic 平台中網路界面的流程日誌。這包含已透過 ClassicLink 連結到 VPC 的 EC2-Classic 執行個體。
- 您無法為已和您 VPC 互連之 VPC 啟用流程日誌，除非對等 VPC 位於您的帳戶中。
- 建立流程日誌之後，您即無法變更其組態或流程日誌記錄格式。例如，您無法建立不同 IAM 角色與流程日誌的關聯，或新增或移除流程日誌記錄的欄位。但是您可以刪除流程日誌，並使用需要的組態建立新的流程日誌。
- 您的網路界面如有多個 IPv4 地址，且流量會傳送到輔助私有 IPv4 地址，則流程日誌會在 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 欄位的流程日誌。
- 如果流量要傳送到網路界面，但目標不是任一網路界面的 IP 地址，則流程日誌會在 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 欄位的流程日誌。
- 如果流量來自網路界面，但來源不是任一網路界面的 IP 地址，則流程日誌會在 srcaddr 欄位中顯示主要私有 IPv4 地址。若要擷取原始來源 IP 地址，請建立具有 pkt-srcaddr 欄位的流程日誌。
- 若流量會傳送到或來自網路界面，則流程日誌的 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 欄位的流程日誌。
- 當您的網路界面連接至 [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。

流程日誌不會擷取所有 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。
- 流入預設 VPC 路由器預留 IP 地址的流量。如需詳細資訊，請參閱[VPC 和子網路大小調整 \(p. 76\)](#)。
- 端點網路界面和 網路負載平衡器 網路界面之間的流量。如需詳細資訊，請參閱[VPC 端點服務 \(AWS PrivateLink\) \(p. 294\)](#)。

## 流程日誌定價

當您將流程記錄發佈到或發佈到 CloudWatch Logs 或 Amazon S3 時，會套用付費日誌的資料擷取和存檔費用。如需詳細資訊和範例，請參閱 [Amazon CloudWatch 定價](#)。

若要追蹤從公佈流程日誌至 Amazon S3 儲存貯體的費用，您可以將成本分配標記套用至流程日誌訂閱。若要追蹤發佈至 CloudWatch Logs 的流程日誌費用，您可以將成本分配標記套用至目的地 CloudWatch Logs 日誌群組。此後，您的 AWS 成本分配報告將包含依這些標記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 AWS Billing and Cost Management 使用者指南中的 [使用成本分配標籤](#)。

## 將流程日誌發佈至 CloudWatch Logs

現在流程日誌可將流程日誌資料直接發佈至 Amazon CloudWatch。

發佈至 CloudWatch Logs 時，流程日誌資料會發佈至日誌群組，以及該日誌群組中每個具有唯一日誌串流的網路界面。日誌串流包含流程日誌記錄。您可以建立多個流程日誌，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程日誌內存在相同的網路界面，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。如需詳細資訊，請參閱「[流程日誌記錄 \(p. 160\)](#)」。

在 CloudWatch Logs 中，timestamp (時間戳記) 欄位對應到於流程日誌記錄中擷取的開始時間。ingestionTime (接收時間) 欄位指出 CloudWatch Logs 收到流程日誌記錄的日期和時間。這個時間戳記晚於流量日誌記錄中擷取的結束時間。

內容

- [用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色 \(p. 168\)](#)
- [建立發布到 CloudWatch Logs 的流程日誌 \(p. 169\)](#)
- [CloudWatch Logs 中的處理流程日誌記錄 \(p. 171\)](#)

## 用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色

與您流程日誌關聯的 IAM 角色必須具有足夠的許可，將流程日誌發佈到 CloudWatch Logs 中指定的日誌群組。IAM 角色必須隸屬於您的 AWS 帳戶。

連接到您 IAM 角色的 IAM 政策至少必須包含下列許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

同時確認您的角色具有允許流程日誌服務擔任角色的信任關係。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": "vpc-flow-logs.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
```

使用者也必須具備許可，能使用與此流程日誌相關聯之 IAM 角色的 iam:PassRole 動作。

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

您可以上傳現有的角色或使用下列程序建立新的角色以使用流程日誌。

## 建立流程日誌角色

### 建立流程日誌的 IAM 角色

1. 開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
2. 在導覽窗格中，選擇 Roles (角色)、Create role (建立新角色)。
3. 選擇 EC2 (EC2) 做為使用此角色的服務。在 Use case (使用案例) 中選擇 EC2 (EC2)。選擇 Next: Permissions (下一步：許可)。
4. 在 Attach permissions policies (連接許可政策) 頁面上，選擇 Next: Tags (下一步：標籤) 並選擇性新增標籤。選擇 Next: Review (下一步：檢閱)。
5. 輸入您角色的名稱 (例如 Flow-Logs-Role)，然後選擇性提供描述。選擇 Create Role (建立角色)。
6. 選取您角色的名稱。在 Permissions (許可) 中選擇 Add inline policy (新增內嵌政策)、JSON (JSON)。
7. 從 [用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色 \(p. 168\)](#) 複製第一個政策，然後在視窗中貼上。選擇 Review policy (檢閱政策)。
8. 輸入您政策的名稱，然後選擇 Create policy (建立政策)。
9. 選取您角色的名稱。針對 Trust relationships (信任關聯)，選擇 Edit trust relationship (編輯信任關聯)。在現有的政策文件中，將服務從 `ec2.amazonaws.com` 變更為 `vpc-flow-logs.amazonaws.com`。選擇 Update Trust Policy (更新信任政策)。
10. 在 Summary (摘要) 頁面上，記下您角色的 ARN。當您建立流程日誌時，會需要此 ARN。

## 建立發布到 CloudWatch Logs 的流程日誌

您可以建立 VPC、子網路或網路界面的流程日誌。

### 使用主控台建立網路界面的流程日誌

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 (網路界面)。
3. 選取一個或多個網路界面，然後選擇 Actions (動作)、Create flow log (建立流程日誌)。
4. 在 Filter (篩選條件) 中指定要記錄的 IP 流量資料類型。選擇 All (全部) 以記錄接受和拒絕的流量，選擇 Rejected (已拒絕) 以僅記錄拒絕的流量，或選擇 Accepted (已接受) 以僅記錄接受的流量。
5. 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。
6. 針對 Destination (目的地)，選擇 Send to CloudWatch Logs (傳送至 CloudWatch Logs)。
7. 在 Destination log group (目標日誌群組) 中輸入 CloudWatch Logs 中的日誌群組名稱，流程日誌會發佈至此群組。若您指定的日誌群組名稱不存在，我們會嘗試為您建立日誌群組。
8. 在 IAM role (IAM 角色) 中指定具備將日誌發佈至 CloudWatch Logs 之許可的角色名稱。
9. 針對 Format (格式)，指定流程日誌紀錄的格式。
  - 若要使用預設的流程日誌紀錄格式，請選擇 AWS default format (AWS 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)，請選擇要包含在流程日誌紀錄中的欄位。

#### Tip

若要建立包含預設格式欄位的自訂流程日誌，請先選擇 AWS default format (AWS 預設格式)，複製 Format preview (格式預覽) 中的欄位，然後選擇 Custom format (自訂格式) 將欄位貼入文字方塊。

10. (選用) 選擇 Add Tag (新增標籤) 將標籤套用至流程日誌。
11. 選擇 Create (建立)。

### 使用主控台建立 VPC 或子網路的流程日誌

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) 或 Subnets (子網路)。
3. 選取一個或多個 VPC 或子網路，然後選擇 Actions (動作)、Create flow log (建立流程日誌)。
4. 在 Filter (篩選條件) 中指定要記錄的 IP 流量資料類型。選擇 All (全部) 以記錄接受和拒絕的流量，選擇 Rejected (已拒絕) 以僅記錄拒絕的流量，或選擇 Accepted (已接受) 以僅記錄接受的流量。
5. 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。
6. 針對 Destination (目的地)，選擇 Send to CloudWatch Logs (傳送至 CloudWatch Logs)。
7. 在 Destination log group (目標日誌群組) 中輸入 CloudWatch Logs 中的日誌群組名稱，流程日誌會發佈至此群組。若您指定的日誌群組名稱不存在，我們會嘗試為您建立日誌群組。
8. 在 IAM role (角色) 中指定具備將日誌發佈至 CloudWatch Logs 之許可的 IAM 角色名稱。
9. 針對 Format (格式)，指定流程日誌紀錄的格式。
  - 若要使用預設的流程日誌紀錄格式，請選擇 AWS default format (AWS 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)，請選擇要包含在流程日誌紀錄中的欄位。

#### Tip

若要建立包含預設格式欄位的自訂流程日誌，請先選擇 AWS default format (AWS 預設格式)，複製 Format preview (格式預覽) 中的欄位，然後選擇 Custom format (自訂格式) 將欄位貼入文字方塊。

10. (選用) 選擇 Add Tag (新增標籤) 將標籤套用至流程日誌。
11. 選擇 Create (建立)。

### 使用命令列工具建立可發佈至 CloudWatch Logs 的流程日誌



請使用下列其中一個命令。

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateFlowLogs](#) (Amazon EC2 查詢 API)

以下 AWS CLI 範例建立的流程日誌，可擷取子網路 subnet-1a2b3c4d 接受的所有流量。流程日誌交付至 CloudWatch Logs 中稱為 my-flow-logs 的日誌群組，位於帳戶 123456789101，使用 IAM 角色 publishFlowLogs。

```
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
```

## CloudWatch Logs 中的處理流程日誌記錄

您可以以您使用其他由 CloudWatch Logs 收集之日誌事件的相同方式，使用流程日誌記錄。如需監控日誌資料和指標篩選條件的詳細資訊，請參閱 Amazon CloudWatch 使用者指南 中的 [搜尋及篩選日誌資料](#)。

### 範例：建立流程日誌的 CloudWatch 指標篩選條件和警示

在此範例中，您有一個 eni-1a2b3c4d 的流程日誌。您希望建立警示，在 1 個小時期間內嘗試透過 TCP 連接埠 22 (SSH) 連線到您的執行個體，其中有 10 次或超過 10 次嘗試遭到拒絕時提醒您。首先，您必須建立符合要建立警示之流量模式的指標篩選條件。然後，您可以建立指標篩選條件的警示。

建立拒絕 SSH 流量的指標篩選條件，及建立篩選條件的警示

1. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Logs (日誌)。
3. 選擇針對您的日誌群組和流程日誌關聯的 Metric Filters (指標篩選) 值，然後選擇 Add Metric Filter (新增指標篩選)。
4. 針對 Filter Pattern (篩選條件模式)，輸入：

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6",  
packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. 在 Select Log Data to Test (選取要測試的日誌資料) 中選取您網路界面的日誌串流。(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)。當您就緒時，請選擇 Assign Metric (指派指標)。
6. 提供指標命名空間與名稱，並確認指標值已設為 1 (1)。完成時，請選擇 Create Filter (建立篩選條件)。
7. 在導覽窗格中，選擇 Alarms (警示)、Create Alarm (建立警示)。
8. 在 Custom Metrics (自訂指標) 區段中，選擇您建立之指標篩選條件的命名空間。

可能要過幾分鐘時間，主控台中才會顯示新的指標。

9. 選取您建立的指標名稱，然後選擇 Next (下一步)。
10. 輸入警示的名稱與說明。在 is (是) 欄位中，選擇 >= (>=)，然後輸入 10 (10)。在 for (為) 欄位中，針對連續期間維持預設值的 1 (1)。
11. 在 Period (期間) 中選擇 1 Hour (1 小時)。在 Statistic (統計資料) 中選擇 Sum (總和)。Sum 統計可確保您擷取的是指定時間期間中的資料點總數。
12. 在 Actions (動作) 區段中，您可以選擇傳送通知給現有的清單。或者，您可以建立新的清單並輸入在觸發警示時應接收到通知的電子郵件地址。完成時，選擇 Create Alarm (建立警示)。

## 將流程日誌發佈至 Amazon S3

現在流程日誌可將流程日誌資料發佈至 Amazon S3。

當發佈至 Amazon S3 時，流程日誌資料將發佈至您指定的現有 Amazon S3 儲存貯體。所有受監控之網路界面的流程日誌記錄，都將發佈至存放在該儲存貯體的一系列日誌檔案物件。如果流程日誌擷取 VPC 的資料，該流程日誌將發佈所選擇之 VPC 中所有網路界面的流程日誌記錄。如需詳細資訊，請參閱[流程日誌記錄](#) (p. 160)。

若要建立用於流程日誌的 Amazon S3 儲存貯體，請參閱 Amazon Simple Storage Service 入門指南 中的[建立儲存貯體](#)。

### 內容

- [流程日誌檔](#) (p. 172)
- [將流程日誌發佈至 Amazon S3 之 IAM 委託人的 IAM 政策](#) (p. 173)
- [流程日誌的 Amazon S3 儲存貯體許可](#) (p. 173)
- [使用 SSE-KMS 儲存貯體必要的 CMK 金鑰政策](#) (p. 174)
- [Amazon S3 日誌檔案許可](#) (p. 174)
- [建立發布到 Amazon S3 的流程日誌](#) (p. 175)
- [Amazon S3 中的處理流程日誌記錄](#) (p. 176)

## 流程日誌檔

流程日誌會收集流程日誌記錄，將這些記錄整合為日誌檔，然後每隔五分鐘將日誌檔發佈至 Amazon S3 儲存貯體。每個日誌檔皆包含過去五分鐘所記錄之 IP 流量的流程日誌記錄。

日誌檔的大小上限為 75 MB。如果日誌檔案在 5 分鐘內達到檔案大小上限，則流程日誌會停止新增流程日誌紀錄。然後，將流程日誌發佈至 Amazon S3 儲存貯體，並建立新的日誌檔案。

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

```
bucket_ARN/optional_folder/AWSLogs/aws_account_id/  
vpcflowlogs/region/year/month/day/log_file_name.log.gz
```

同樣的，日誌檔案的檔案名稱取決於流程日誌的 ID、區域，以及流程日誌服務建立日誌檔案的日期與時間。檔案名稱使用下列格式。

```
aws_account_id_vpcflowlogs_region_flow_log_id_timestamp_hash.log.gz
```

### Note

時間戳記使用 YYYYMMDDTHHmmZ 格式。

例如，以下示範由 AWS 帳戶 123456789012 針對 us-east-1 區域中的資源，在 June 20, 2018 16:20 UTC 建立之流程日誌日誌檔案的資料夾結構與檔案名稱。它包含 16:15:00 到 16:19:59 的流程日誌記錄。

```
arn:aws:s3:::my-flow-log-bucket/AWSLogs/123456789012/  
vpcflowlogs/us-east-1/2018/06/20/123456789012_vpcflowlogs_us-  
east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

在 Amazon S3 中，流程日誌檔案的 Last modified (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。



## 將流程日誌發佈至 Amazon S3 之 IAM 委託人的 IAM 政策

您帳戶中的 IAM 委託人 (例如 IAM 使用者) 必須有足夠的許可才能將流程日誌發佈至 Amazon S3 儲存貯體。其中包括使用特定 logs: 動作來建立和發佈流量日誌的許可。IAM 政策必須包含下列許可。

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

## 流程日誌的 Amazon S3 儲存貯體許可

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

下列儲存貯體政策會提供流程日誌權限，以便將日誌發佈至其中。如果儲存貯體已具有下列權限的政策，則該政策會保持原狀。

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

如果建立流程記錄的使用者具有儲存貯體、具有儲存貯體的 PutBucketPolicy 權限，且儲存貯體沒有具備足夠日誌交付權限的政策，我們便會自動將先前的政策附加至儲存貯體。此政策會覆寫附加至儲存貯體的任何現有政策。

如果建立流程日誌的使用者並未擁有儲存貯體，或者沒有儲存貯體的 GetBucketPolicy 與 PutBucketPolicy 許可，流程日誌的建立將會失敗。在此情況下，儲存貯體擁有者必須將上述政策手動新增至儲存貯體，並指定流程日誌建立者的 AWS 帳戶 ID。如需詳細資訊，請參閱 Amazon Simple Storage Service 主控台使用者指南 中的 [如何新增 S3 儲存貯體政策](#)？如果儲存貯體從多個帳戶接收流程日誌，請將 Resource 元素項目新增至每個帳戶的 AWSLogDeliveryWrite 政策陳述式。例如，以下儲存貯體政策允許 AWS 帳戶 123123123123 與 456456456456 將流程日誌發佈至名為 flow-logs 之儲存貯體中的 log-bucket 資料夾。

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

#### Note

我們建議您將 `AWSLogDeliveryAclCheck` 與 `AWSLogDeliveryWrite` 許可授予日誌交付服務主體，而非個別 AWS 帳戶 ARN。

## 使用 SSE-KMS 儲存貯體必要的 CMK 金鑰政策

如果使用具備客戶受管客戶主金鑰 (CMK) 的 AWS KMS 受管金鑰 (SSE-KMS) 啟用 Amazon S3 儲存貯體伺服器端加密，您必須新增下列內容到 CMK 的金鑰政策，讓流程日誌可將日誌檔案寫入儲存貯體。

#### Note

將這些元素新增至您的 CMK 政策，而非儲存貯體的政策。

```
{
  "Sid": "Allow VPC Flow Logs to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

## Amazon S3 日誌檔案許可

除了必要的儲存貯體政策之外，Amazon S3 使用存取控制清單 (ACL) 來管理流程日誌所建立之日誌檔案的存取。根據預設，儲存貯體擁有者擁有各個日誌檔案的 `FULL_CONTROL` 許可。日誌交付擁有者與儲存貯體

擁有者不同時，就沒有任何許可。日誌交付帳戶擁有 READ 與 WRITE 許可。如需詳細資訊，請參閱 Amazon Simple Storage Service 開發人員指南 中的 [存取控制清單 \(ACL\) 概觀](#)。

## 建立發布到 Amazon S3 的流程日誌

建立並設定您的 Amazon S3 儲存貯體後，您可以建立 VPC、子網路或網路界面的流程日誌。

### 使用主控台建立網路界面的流程日誌

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 (網路界面)。
3. 選取一個或多個網路界面，然後選擇 Actions (動作)、Create flow log (建立流程日誌)。
4. 在 Filter (篩選條件) 中指定要記錄的 IP 流量資料類型。選擇 All (全部) 以記錄接受和拒絕的流量，選擇 Rejected (已拒絕) 以僅記錄拒絕的流量，或選擇 Accepted (已接受) 以僅記錄接受的流量。
5. 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。
6. 針對 Destination (目的地)，選擇 Send to an Amazon S3 bucket (傳送至 Amazon S3 儲存貯體)。
7. 針對 S3 bucket ARN (S3 儲存貯體 ARN)，指定現有 Amazon S3 儲存貯體的 Amazon Resource Name (ARN)。您也可以將子資料夾加入儲存貯體 ARN 中。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。

例如，若要指定名為 my-bucket 之儲存貯體中的 my-logs 子資料夾，請使用以下 ARN 格式：

```
arn:aws:s3:::my-bucket/my-logs/
```

若您擁有儲存貯體，我們會自動建立資源政策並將其連接至儲存貯體。如需更多詳細資訊，請參閱 [流程日誌的 Amazon S3 儲存貯體許可 \(p. 173\)](#)。

8. 針對 Format (格式)，指定流程日誌紀錄的格式。
  - 若要使用預設的流程日誌紀錄格式，請選擇 AWS default format (AWS 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)，請選擇要包含在流程日誌紀錄中的欄位。

#### Tip

若要建立包含預設格式欄位的自訂流程日誌，請先選擇 AWS default format (AWS 預設格式)，複製 Format preview (格式預覽) 中的欄位，然後選擇 Custom format (自訂格式) 將欄位貼入文字方塊。

9. (選用) 選擇 Add Tag (新增標籤) 將標籤套用至流程日誌。
10. 選擇 Create (建立)。

### 使用主控台建立 VPC 或子網路的流程日誌

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) 或 Subnets (子網路)。
3. 選取一個或多個 VPC 或子網路，然後選擇 Actions (動作)、Create flow log (建立流程日誌)。
4. 在 Filter (篩選條件) 中指定要記錄的 IP 流量資料類型。選擇 All (全部) 以記錄接受和拒絕的流量，選擇 Rejected (已拒絕) 以僅記錄拒絕的流量，或選擇 Accepted (已接受) 以僅記錄接受的流量。
5. 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。
6. 針對 Destination (目的地)，選擇 Send to an Amazon S3 bucket (傳送至 Amazon S3 儲存貯體)。
7. 針對 S3 bucket ARN (S3 儲存貯體 ARN)，指定現有 Amazon S3 儲存貯體的 Amazon Resource Name (ARN)。您也可以將子資料夾加入儲存貯體 ARN 中。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。

例如，若要指定名為 my-bucket 之儲存貯體中的 my-logs 子資料夾，請使用以下 ARN 格式：

```
arn:aws:s3:::my-bucket/my-logs/
```

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。如需更多詳細資訊，請參閱 [流程日誌的 Amazon S3 儲存貯體許可 \(p. 173\)](#)。

8. 針對 Format (格式)，指定流程日誌紀錄的格式。
  - 若要使用預設的流程日誌紀錄格式，請選擇 AWS default format (AWS 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)，請選擇要包含在流程日誌紀錄中的各個欄位。
9. (選用) 選擇 Add Tag (新增標籤) 將標籤套用至流程日誌。
10. 選擇 Create (建立)。

使用命令列工具建立可發佈至 Amazon S3 的流程日誌

請使用下列其中一個命令。

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateFlowLogs](#) (Amazon EC2 查詢 API)

以下 AWS CLI 範例建立的流程日誌，會擷取 VPC vpc-00112233344556677 的所有流量，並將流程日誌交付給稱為 flow-log-bucket 的 Amazon S3 儲存貯體。--log-format 參數會指定流程日誌紀錄的自訂格式。

```
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/my-custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

## Amazon S3 中的處理流程日誌記錄

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

您也可使用 Amazon Athena 查詢日誌檔案中的流程日誌記錄。Amazon Athena 是互動式查詢服務，可使用標準 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 流程日誌](#)。

## 使用流程日誌

您可以透過 Amazon EC2、Amazon VPC、CloudWatch 與 Amazon S3 主控台使用流程日誌。

內容

- [控制流程日誌的使用方式 \(p. 177\)](#)
- [建立流程日誌 \(p. 177\)](#)
- [檢視流程日誌 \(p. 177\)](#)
- [新增或移除流程日誌的標籤 \(p. 178\)](#)
- [檢視流程日誌記錄 \(p. 178\)](#)
- [搜尋流程日誌記錄 \(p. 178\)](#)

- [刪除流程日誌 \(p. 179\)](#)
- [API 和 CLI 概觀 \(p. 179\)](#)

## 控制流程日誌的使用方式

根據預設，IAM 使用者沒有使用流程日誌的許可。您可以建立 IAM 使用者政策，將建立、描述和刪除流程日誌的許可授予使用者。如需詳細資訊，請參閱 Amazon EC2 API Reference 中的[授予 IAM 使用者必要的 Amazon EC2 資源許可](#)。

以下是授予使用者建立、描述、刪除流程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": "*"
    }
  ]
}
```

依據您要發佈至 CloudWatch Logs 或 Amazon S3，將需要一些額外的 IAM 角色與許可組態。如需詳細資訊，請參閱[將流程日誌發佈至 CloudWatch Logs \(p. 168\)](#)及[將流程日誌發佈至 Amazon S3 \(p. 172\)](#)。

## 建立流程日誌

您可以建立 VPC、子網路或網路界面的流程日誌。現在流程日誌可發佈資料至 CloudWatch Logs 或 Amazon S3。

如需詳細資訊，請參閱[建立發布到 CloudWatch Logs 的流程日誌 \(p. 169\)](#)及[建立發布到 Amazon S3 的流程日誌 \(p. 175\)](#)。

## 檢視流程日誌

您可以在 Amazon EC2 和 Amazon VPC 主控台中透過檢視特定資源的 Flow Logs (流程日誌) 標籤，來檢視您流程日誌的相關資訊。當您選取資源時，便會列出所有該資源的流程日誌。顯示的資訊包含流程日誌的 ID、流程日誌組態，以及流程日誌狀態的相關資訊。

檢視您網路界面流程日誌的相關資訊

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 (網路界面)。
3. 選取網路界面，然後選擇 Flow Logs (流程日誌)。標籤上即會顯示流程日誌的相關資訊。Destination type (目的地類型) 欄位顯示發佈流程日誌之目的地。

檢視您 VPC 或子網路流程日誌的相關資訊

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC) 或 Subnets (子網路)。
3. 選取您的 VPC 或子網路，然後選擇 Flow Logs (流程日誌)。標籤上即會顯示流程日誌的相關資訊。Destination type (目的地類型) 欄位顯示發佈流程日誌之目的地。

## 新增或移除流程日誌的標籤

您可以在 Amazon EC2 和 Amazon VPC 主控台中新增或移除流程日誌的標籤。

若要新增或移除網路介面的流程日誌標籤

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. 選取網路介面，然後選擇 Flow Logs (流程日誌)。
4. 為所需的流程日誌選擇 Manage Tags (管理標籤)。
5. 若要新增新標籤，請選擇 Create Tag (建立標籤)。若要移除標籤，請選擇刪除按鈕 (x)。
6. 選擇 Save (儲存)。

若要新增或移除 VPC 或子網路的流程日誌標籤

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC) 或 Subnets (子網路)。
3. 選取您的 VPC 或子網路，然後選擇 Flow Logs (流程日誌)。
4. 選取流程日誌，再選擇 Actions (動作)、Add/Edit Tags (新增/編輯標籤)。
5. 若要新增新標籤，請選擇 Create Tag (建立標籤)。若要移除標籤，請選擇刪除按鈕 (x)。
6. 選擇 Save (儲存)。

## 檢視流程日誌記錄

依據所選擇的目的地類型，您可以使用 CloudWatch Logs 主控台或 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 CloudWatch Logs 的流程日誌記錄

1. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。
2. 在導覽窗格中選擇 Logs (日誌)，然後選取包含您流程日誌的日誌群組。即會顯示每個網路界面的日誌串流清單。
3. 選取包含您希望檢視流程日誌記錄之網路界面 ID 的日誌串流。如需詳細資訊，請參閱 [流程日誌記錄 \(p. 160\)](#)。

檢視發佈至 Amazon S3 的流程日誌記錄

1. 在 <https://console.aws.amazon.com/s3/> 開啟 Amazon S3 主控台。
2. 在 Bucket name (儲存貯體名稱) 中選擇發佈流程日誌之目的地儲存貯體。
3. 在 Name (名稱) 中選取日誌檔案旁邊的核取方塊。在物件概觀面板上，選擇 Download (下載)。

## 搜尋流程日誌記錄

您可以使用 CloudWatch Logs 主控台，搜尋在 CloudWatch Logs 中發佈的流程日誌記錄。您可以使用 [指標篩選條件](#) 來篩選流程日誌記錄。流程日誌記錄是以空格分隔。

使用 CloudWatch Logs 主控台搜尋流程日誌記錄

1. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。



2. 在導覽窗格中選擇 Log groups (日誌群組)，然後選取包含您流程日誌的日誌群組。即會顯示每個網路界面的日誌串流清單。
3. 如果您知道要搜尋的網路界面，請選取個別日誌串流。或者，選擇 Search Log Group (搜尋日誌群組) 以搜尋整個日誌群組。如果您的日誌群組中有許多網路界面，這可能需要一些時間，視您選取的時間範圍而定。
4. 對於 Filter events (篩選事件)，請輸入下列字串。這會假設流程日誌記錄使用預設格式 (p. 161)。

```
[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]
```

下列範例會依目的地連接埠、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]
```

## 刪除流程日誌

您可以使用 Amazon EC2 和 Amazon VPC 主控台刪除流程日誌。

### Note

這些程序會停用資源的流程日誌服務。刪除流程日誌不會從 CloudWatch Logs 刪除現有的日誌串流或從 Amazon S3 刪除現有的日誌檔案。現有的流程日誌資料必須使用各服務的主控台進行刪除。此外，刪除發佈至 Amazon S3 的流程日誌並不會移除儲存貯體政策與日誌檔案存取控制清單 (ACL)。

### 刪除網路界面的流程日誌

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 (網路界面)，然後選取網路界面。
3. 選擇 Flow Logs (流程日誌)，然後選擇要刪除之流程日誌的刪除按鈕 (打叉圖樣)。
4. 在確認對話方塊中，選擇 Yes, Delete (是，刪除)。

### 刪除 VPC 或子網路的流程日誌

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) 或 Subnets (子網路)，然後選取資源。
3. 選擇 Flow Logs (流程日誌)，然後選擇要刪除之流程日誌的刪除按鈕 (打叉圖樣)。
4. 在確認對話方塊中，選擇 Yes, Delete (是，刪除)。

## API 和 CLI 概觀

您可以使用命令行或 API 執行此頁面所述的任務。如需命令行界面的詳細資訊與可用的 API 動作清單，請參閱[存取 Amazon VPC \(p. 1\)](#)。



### 建立流程日誌

- [create-flow-logs](#) (AWS CLI)
- [新的 EC2 流程日誌](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateFlowLogs](#) (Amazon EC2 查詢 API)

### 描述您的流程日誌

- [describe-flow-logs](#) (AWS CLI)
- [獲得 EC2 流程日誌](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DescribeFlowLogs](#) (Amazon EC2 查詢 API)

### 檢視您的流程日誌記錄 (日誌事件)

- [get-log-events](#) (AWS CLI)
- [獲得 CWL 日誌事件](#) (適用於 Windows PowerShell 的 AWS 工具)
- [GetLogEvents](#) (CloudWatch API)

### 刪除流程日誌

- [delete-flow-logs](#) (AWS CLI)
- [移除 EC2 流程日誌](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DeleteFlowLogs](#) (Amazon EC2 查詢 API)

## 疑難排解

以下是使用流程日誌時可能會遇到的問題。

#### 問題

- [不完整的流程日誌記錄](#) (p. 180)
- [流程日誌作用中，但沒有任何流程日誌紀錄或日誌群組](#) (p. 181)
- ['LogDestinationNotFoundException' 或 'Access Denied for LogDestination' 錯誤](#) (p. 181)
- [超過 Amazon S3 儲存貯體政策限制](#) (p. 181)

## 不完整的流程日誌記錄

#### 問題

您的流程日誌記錄不完整，或已不再發佈。

#### 原因

傳遞流程日誌到 CloudWatch Logs 日誌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 Flow Logs (流程日誌) 索引標籤。如需詳細資訊，請參閱 [檢視流程日誌](#) (p. 177)。流程日誌表會在 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**：此錯誤可能會在套用 CloudWatch Logs 調節後時發生 — 即網路界面的流程日誌記錄數大於可在特定時間範圍內發佈的最大記錄數時。在您到達您可以建立的 CloudWatch Logs 日誌群組數配額時，也可能會發生此錯誤。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的 [CloudWatch 服務配額](#)。
  - **Access error**：此錯誤可能的發生原因如下：
    - 您流程日誌的 IAM 角色沒有足夠的許可，無法將流程日誌紀錄發佈到 CloudWatch 日誌群組。
    - IAM 角色與流程日誌服務沒有信任關係
    - 信任關係不指定流程日誌服務為委託人
- 如需更多詳細資訊，請參閱 [用於將流程日誌發佈至 CloudWatch Logs 的 IAM 角色 \(p. 168\)](#)。
- **Unknown error**：流程日誌服務發生內部錯誤。

## 流程日誌作用中，但沒有任何流程日誌紀錄或日誌群組

### 問題

您已建立流程日誌，且 Amazon VPC 或 Amazon EC2 主控台已顯示流程日誌狀態為 **Active**。但是，您無法看到 CloudWatch Logs 中的任何日誌串流或 Amazon S3 儲存貯體中的日誌檔案。

### 原因

原因可能為下列之一：

- 流程日誌仍在建立的程序中。在某些情況下，在您建立流程日誌之後，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界面的流量。CloudWatch Logs 中的日誌群組只有在記錄流量時才會建立。

### 解決方案

等待幾分鐘建立日誌群組或記錄流量。

## 'LogDestinationNotFoundException' 或 'Access Denied for LogDestination' 錯誤

### 問題

當您嘗試建立流程日誌時，您會收到 **Access Denied for LogDestination** 或 **LogDestinationNotFoundException** 錯誤。

### 原因

當建立發佈資料至 Amazon S3 儲存貯體的流程日誌時，可能會發生這些錯誤。此錯誤表示找不到指定的 S3 儲存貯體，或儲存貯體政策發生問題。

### 解決方案

請執行下列其中一項：

- 請確定您已指定現有 S3 儲存貯體的 ARN，而且此 ARN 的格式是正確的。
- 如果您沒有 S3 儲存貯體，請確認 [儲存貯體政策 \(p. 173\)](#) 具有足夠的權限可將記錄發佈至該儲存貯體。在儲存貯體政策中，驗證帳戶識別碼和儲存貯體名稱。

## 超過 Amazon S3 儲存貯體政策限制

### 問題

當您嘗試建立流程日誌時，得到下列錯誤：LogDestinationPermissionIssueException。

原因

Amazon S3 儲存貯體政策的大小限制為 20 KB。

每次您建立流程日誌發布到 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 新增到儲存貯體政策的 Resource 元素中。

建立多個發布到相同儲存貯體的流程日誌可能造成您超過儲存貯體政策限制。

解決方案

請執行下列其中一項：

- 移除不再需要的流程日誌以清除儲存貯體的政策。
- 以下列內容取代個別的流程日誌項目，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，新的流程日誌訂閱不會將新的許可加入到儲存貯體政策。

## 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。

以下是一般最佳實務：

- 使用多個可用區域部署，讓您擁有高可用性。
- 使用安全群組和網路 ACL。如需更多詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#) 及 [網路 ACL \(p. 146\)](#)。
- 使用 IAM 政策來控制存取
- 用 Amazon CloudWatch 於監控您的 VPC 元件和 VPN 連線。
- 用流量日誌可擷取您 VPC 中傳入和傳出網路介面之 IP 流量資訊。如需更多詳細資訊，請參閱 [VPC 流程日誌 \(p. 158\)](#)。

## 其他資源

- 使用聯合身分、IAM 使用者和 IAM 角色管理對 AWS 資源和 API 的存取。建立登入資料管理政策和程序以建立、分發、輪換和撤銷 AWS 存取登入資料。如需詳細資訊，請參閱 IAM 使用者指南 中的 [IAM 最佳實務](#)。
- 如需 VPC 安全常見問答集的解答，請參閱 [Amazon VPC 常見問答集](#)。

# VPC 聯網元件

您可以使用下列元件，在 VPC 中設定聯網。

## 主題

- [彈性網路界面 \(p. 183\)](#)
- [路由表 \(p. 184\)](#)
- [字首清單 \(p. 204\)](#)
- [網際網路閘道 \(p. 212\)](#)
- [輸出限定網際網路閘道 \(p. 218\)](#)
- [電信業者閘道 \(p. 221\)](#)
- [NAT \(p. 226\)](#)
- [DHCP 選項集 \(p. 251\)](#)
- [搭配使用 DNS 與 VPC \(p. 256\)](#)
- [VPC 互連 \(p. 260\)](#)
- [彈性 IP 地址 \(p. 260\)](#)
- [ClassicLink \(p. 264\)](#)

## 彈性網路界面

彈性網路界面 (本文件中稱為網路界面) 是包含下列屬性的虛擬網路界面：

- 主要私有 IPv4 地址
- 一或多個輔助私有 IPv4 地址
- 每個私有 IPv4 地址一個彈性 IP 地址
- 一個公有 IPv4 地址，可在您啟動執行個體時，自動指派給 eth0 的網路界面
- 一或多個 IPv6 地址
- 一或多個安全群組
- 一個 MAC 地址
- 一個來源/目標檢查標記
- 一項描述

您可以建立網路界面，連接到執行個體、與執行個體分離，然後再次連接到另一個執行個體。網路界面的屬性在網路界面連接到執行個體或與執行個體分離，然後重新連接到另一個執行個體時，會一直跟著網路界面。當您將網路界面從一個執行個體移至另一個執行個體時，網路流量會重新導向至新的執行個體。

您 VPC 中的每個執行個體有一個預設網路界面 (主要網路界面)，會被指派一個私有 IPv4 地址，而此地址來自您 VPC 的 IPv4 地址範圍。您無法分離主要網路界面和執行個體。您可以建立額外的網路界面，然後連接到您 VPC 中的任一執行個體。您可連接的網路界面數會隨執行個體類型而不同。如需詳細資訊，請參閱《Linux 執行個體的 Amazon EC2 使用者指南》中的[每個執行個體類型的每個網路界面 IP 地址](#)。

當您想要執行下列作業時，將多個網路界面連接到一個執行個體會很有用：

- 建立管理網路。
- 在您的 VPC 中使用網路和安全設備。

- 在不同的子網路上使用工作負載/角色建立雙主目錄的執行個體。
- 建立低預算、高可用性的解決方案。

如需網路界面的詳細資訊，以及利用 Amazon EC2 主控台使用網路界面的說明，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [彈性網路界面](#)。

## 路由表

路由表包含一組名為路由的規則，用來判斷來自子網路或閘道之網路流量的方向。

內容

- [路由表概念](#) (p. 184)
- [路由表的運作方式](#) (p. 184)
- [路由優先順序](#) (p. 189)
- [路由選項範例](#) (p. 191)
- [使用路由表](#) (p. 197)

## 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路的路由。
- 自訂路由表—您為 VPC 建立的路由表。
- 邊緣關聯—您用來將傳入 VPC 流量路由傳送至設備的路由表。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。
- 路由表關聯—路由表與子網路、網際網路閘道或虛擬私有閘道之間的關聯。
- 子網路路由表—與子網路相關聯的路由表。
- 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。
- 本機閘道路由表—與 Outposts 本機閘道相關聯的路由表。如需本機閘道的相關資訊，請參閱《AWS Outposts 使用者指南》中的 [本機閘道](#)。
- Destination (目的地)—您想要流量傳送的 IP 位址範圍 (目的地 CIDR)。例如，具有 172.16.0.0/12 CIDR 的外部公司網路。
- 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。這表示您不需要手動將 VPN 路由輸入到路由表。如需 VPN 路由選項的詳細資訊，請參閱 Site-to-Site VPN 使用者指南中的 [Site-to-Site VPN 路由選項](#)。
- Target (目標)—要透過其傳送目的地流量的閘道、網路介面或連線；例如，網際網路閘道。
- 本機路由—VPC 內用於通訊的預設路由。

例如路由選項，請參閱 [the section called “路由選項範例”](#) (p. 191)。

## 路由表的運作方式

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 中的每個子網路都必須與路由表相關聯，此路由表會控制子網路的路由 (子網路路由表)。您可以明確地將子網路與特定路由表建立關聯。否則，子網路會隱含地與主路由表相關聯。子網路只能一次與一個路由表建立關聯，但您可以將多個子網路與相同的子網路路由表建立關聯。

您可以選擇性地將路由表與網際網路閘道或虛擬私有閘道產生關聯 (閘道路由表)。這可讓您指定透過閘道進入 VPC 之傳入流量的路由規則。如需更多詳細資訊，請參閱 [閘道路由表 \(p. 188\)](#)。

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。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。

#### 主題

- [路由 \(p. 185\)](#)
- [主路由表 \(p. 186\)](#)
- [自訂路由表 \(p. 186\)](#)
- [子網路路由表關聯 \(p. 186\)](#)
- [閘道路由表 \(p. 188\)](#)

## 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，若要讓子網路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。

目的地	目標
0.0.0.0/0	igw-12345678901234567

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。

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。

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。您無法在子網路路由表或主路由表中修改或刪除這些路由。

如需閘道路由表中路由和本機路由的詳細資訊，請參閱 [閘道路由表 \(p. 188\)](#)。

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。

在以下範例中，所有 IPv6 CIDR 區塊都與您的 VPC 相關聯。在您的路由表中：

- 目標為留在 VPC (2001:db8:1234:1a00::/56) 內的 IPv6 流量都會涵蓋於 Local 路由之中，且會在 VPC 內路由。
- IPv4 和 IPv6 流量是分開處理的。因此，所有 IPv6 流量 (除了 VPC 內的流量) 都會路由至輸出限定網際網路閘道。
- 有一個指向對等連線之 172.31.0.0/16 IPv4 流量的路由。
- 所有 IPv4 流量 (0.0.0.0/0) 都有一個指向網際網路閘道的路由。
- 所有 IPv6 流量 (::/0) 都有一個指向僅限輸出之網際網路閘道的路由。

目的地	目標
10.0.0.0/16	區域
2001:db8:1234:1a00::/56	區域

目的地	目標
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccdde1122334

如果您經常在 AWS 資源中參考同一組 CIDR 區塊，則可以建立 [客戶管理的字首清單](#) (p. 204)，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。

## 主路由表

當您建立 VPC 時，便會自動隨附一個主路由表。主路由表會控制所有並未與任何其他路由表明確建立關聯之子網路的路由。在 Amazon VPC 主控台之 Route Tables (路由表) 頁面上，您可以透過尋找 Main (主要) 欄中的 Yes (是)，來檢視 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。當您在主控台中使用 VPC 精靈，以建立具有 NAT 閘道或虛擬私有閘道的非預設 VPC 時，精靈會自動將路由新增到這些閘道的主路由表。

您可以新增、移除和修改主路由表中的路由。您無法產生比本機路由更具體的路由。您無法刪除主路由表，但可以將主路由表取代為您已建立的自訂子網路路由表。您無法將閘道路由表設定為主路由表。

您可以明確將子網路與主路由表建立關聯，即使其已經隱含地建立關聯。如果你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路，或是任何尚未與其他路由表明確建立關聯之子網路的預設值。如需更多詳細資訊，請參閱 [取代主路由表](#) (p. 202)。

## 自訂路由表

依預設，自訂路由表是空的，您可以視需要新增路由。當您在主控台中使用 VPC 精靈，來建立具有網際網路閘道的 VPC 時，此精靈會建立自訂路由表，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路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路由流量的方式。

您可以新增、移除和修改主路由表中的路由。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 中的每個子網路都必須與路由表建立關聯。子網路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。如需檢視子網路和路由表關聯的詳細資訊，請參閱 [判斷與路由表明確相關聯的子網路及\(或\)閘道](#) (p. 198)。

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

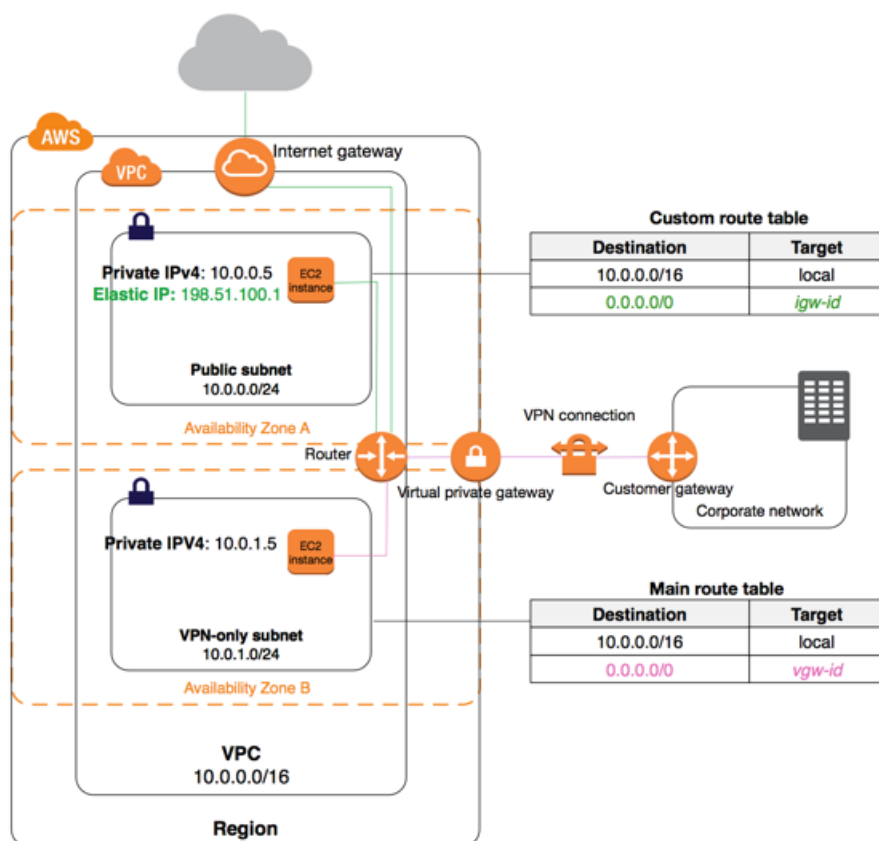
如果下列任一情況適用，您就無法將子網路與路由表建立關聯：

- 路由表包含比預設本機路由更具體的現有路由。
- 已取代預設本機路由的目標。

### 範例 1：隱含和明確的子網路關聯

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。主路由表具有虛擬私有閘道的路由。自訂路由表明確地與公有子網路相關聯。自訂路由表具有透過網際網路閘道前往網際網路的路由 (0.0.0.0/0)。



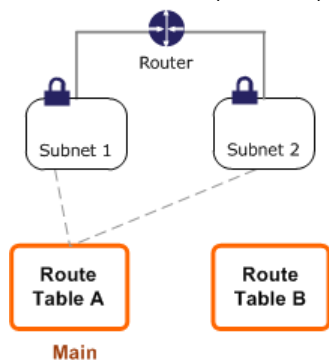


如果您在此 VPC 中建立新的子網路，子網路會自動隱含地與主路由表建立關聯，將流量路由至虛擬私有閘道。如果您設定反向組態 (其中主路由表具有前往網際網路閘道的路由，而自訂路由表具有前往虛擬私有閘道的路由)，則新的子網路便會自動具有前往網際網路閘道的路由。

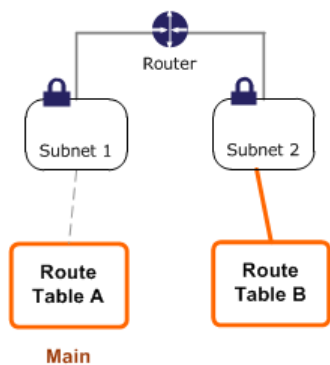
#### 範例 2：取代主路由表

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。

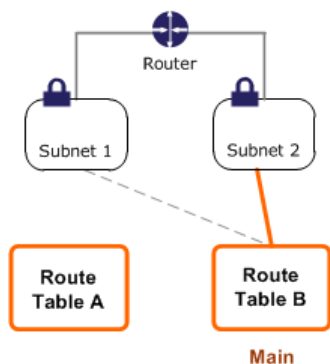
下表顯示具備兩個與主路由表 (路由表 A) 隱含地建立關聯之子網路的 VPC，以及一個沒有與任何子網路建立關聯的自訂路由表 (路由表 B)。



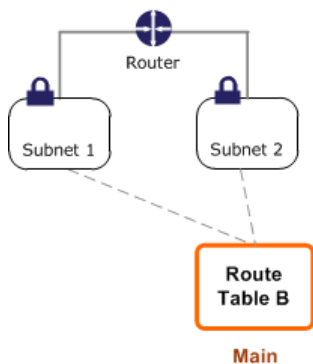
您可以建立子網路 2 和路由表 B 之間的明確關聯。



在您測試路由表 B 之後，您可以將之設為主路由表。請注意，子網路 2 和路由表 B 建立明確關聯，子網路 1 則和路由表 B 建立隱含關聯，因為路由表 B 為新的主路由表。路由表 A 已不再使用。



若您取消子網路 2 與路由表 B 的關聯，子網路 2 和路由表 B 之間仍然具有隱含關聯。若您不再需要路由表 A，您可以予以刪除。



## 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)。

閘道路由表支援目標是 `local` (預設本機路由) 或是 VPC 中連接到您中間設備的彈性網路界面 (網路界面) 的路由。當目標是網路界面時，系統允許下列目的地：

- 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 中子網路的整個 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[取代和還原本機路由的目標](#) (p. 203)。

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

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

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 內所有子網路的流量會路由至網路界面。

目的地	目標
172.31.0.0/16	eni-id

## 規則和考量

如果下列任一種情況適用，您就無法將路由表與閘道建立關聯：

- 路由表包含具有網路界面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。
- 您只能指定 `local` 或一個網路界面做為目標。您無法指定任何其他類型的目標，包括個別主機 IP 位址。
- 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](#) (p. 196)。
- 當您透過中間設備路由流量時，來自目的地子網路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。

如需安全設備的路由範例，請參閱[VPC 中的中間設備路由](#) (p. 195)。

## 路由優先順序

我們會使用您路由表中最明確且符合流量的路由，以判斷如何路由流量 (最長的前綴相符)。

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。

例如，下列子網路路由表具有適用於 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。任何來自子網路，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。任何來自子網路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	區域
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

若您已將虛擬私有閘道連接至您的 VPC，並在您的子網路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。如果傳播路由與靜態路由重疊，且無法套用最長字首比對，則靜態路由優先於傳播路由。如需詳細資訊，請參閱 AWS Site-to-Site VPN 使用者指南 中的 [路由表與 VPN 路由優先順序](#)。

在本範例中，您的路由表有網際網路閘道的靜態路由 (以手動方式新增)，以及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。在此情況下，所有以 172.31.0.0/24 為目標的流量都會路由到網際網路閘道 — 其為靜態路由，因此優先於傳播路由。

目的地	目標
10.0.0.0/16	區域
172.31.0.0/24	vgw-11223344556677889 (傳播)
172.31.0.0/24	igw-12345678901234567 (靜態)

如果您的路由表包含下列任何一個項目的靜態路由，則適用相同的規則：

- NAT 閘道
- 網路界面
- 執行個體 ID
- 閘道 VPC 端點
- Transit gateway
- VPC 對等連線

如果靜態和傳播路由的目的地相同，靜態路由優先。

## 字首清單的路由優先順序

如果您的路由表參考字首清單，則適用下列規則：

- 如果您的路由表包含與參考字首清單之另一個路由重疊的靜態路由，則具有目的地 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重疊的傳播路由，則參考字首清單的路由優先。
- 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。

- 如果字首清單項目中的 CIDR 區塊對路由表無效，則會忽略該 CIDR 區塊。例如，在子網路路由表中，如果字首清單包含比 VPC CIDR 更具體 CIDR 的項目，則會忽略該項目。

## 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。

### 選項

- [路由至網際網路閘道](#) (p. 191)
- [路由至 NAT 裝置](#) (p. 191)
- [路由至虛擬私有閘道](#) (p. 192)
- [路由至 AWS Outposts 本機閘道](#) (p. 192)
- [路由傳送至 Wavelength 區域電信業者閘道](#) (p. 192)
- [路由至 VPC 對等連線](#) (p. 193)
- [ClassicLink 的路由](#) (p. 194)
- [路由至閘道 VPC 端點](#) (p. 194)
- [路由至輸出限定網際網路閘道](#) (p. 194)
- [傳輸閘道的路由](#) (p. 195)
- [VPC 中的中間設備路由](#) (p. 195)
- [使用字首清單進行路由](#) (p. 197)

## 路由至網際網路閘道

您可以將子網路路由表中的路由新增至網際網路閘道，使子網路成為公有子網路。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-xxxxxxxxxxxxxxxxxx) 的目標。

目的地	目標
0.0.0.0/0	igw-id
::/0	igw-id

如需更多詳細資訊，請參閱 [網際網路閘道](#) (p. 212)。

## 路由至 NAT 裝置

若要讓私有子網路中的執行個體連線至網際網路，您可以在公有子網路中建立 NAT 閘道或啟動 NAT 執行個體。然後，為私有子網路的路由表新增一個路由，將 IPv4 網際網路流量 (0.0.0.0/0) 路由至 NAT 裝置。

目的地	目標
0.0.0.0/0	nat-gateway-id

您也可以對其他目標建立更具體的路由，以避免使用 NAT 閘道或私自路由特定流量時產生不必要的資料處理費用。在下列範例中，Amazon S3 流量 (pl-xxxxxxx；Amazon S3 的特定 IP 地址範圍) 會路由至閘道 VPC 端點，而 10.25.0.0/16 流量則會路由至 VPC 對等連線。pl-xxxxxxx 和 10.25.0.0/16 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 或對等 VPC 時，流量會傳送至閘道 VPC 端點或 VPC 對等連線。所有其他流量都會傳送至 NAT 閘道。

目的地	目標
0.0.0.0/0	nat-gateway-id
pl-xxxxxxx	vpce-id
10.25.0.0/16	pcx-id

如需更多詳細資訊，請參閱 [NAT 閘道 \(p. 226\)](#) 及 [NAT 執行個體 \(p. 243\)](#)。NAT 裝置無法用於 IPv6 流量。

## 路由至虛擬私有閘道

您可以使用 AWS Site-to-Site VPN 連接，讓您 VPC 中的執行個體可和您的網路通訊。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-xxxxxxxxxxxxxxxxxx)。

目的地	目標
10.0.0.0/16	vgw-id

您接著便可以建立和設定您的 Site-to-Site VPN 連接。如需詳細資訊，請參閱 [AWS Site-to-Site VPN 使用者指南](#) 中的 [何謂 AWS Site-to-Site VPN ?](#) 和 [路由表與 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

位於與 AWS Outposts 相關聯之 VPC 中的子網路可有額外目標類型的本機閘道。請考慮您想要讓本機閘道將目的地地址為 192.168.10.0/24 的流量路由至客戶網路的情況。若要這樣做，請新增下列路由，其中具有目的地網路和本機閘道目標 (lgw-xxxx)。

目的地	目標
192.168.10.0/24	lgw-id
2002:bc9:1234:1a00::/56	igw-id

## 路由傳送至 Wavelength 區域電信業者閘道

位於 Wavelength 區域的子網路可以有額外的電信業者閘道目標類型。請考慮以下情況：讓電信業者閘道路由傳送流量，以將所有非 VPC 流量路由傳送至電信業者網路。若要執行此動作，請建立電信業者閘道並將其附加至您的 VPC，然後新增下列路由：

目的地	目標
0.0.0.0/0	cagw-id

目的地	目標
::/0	cagw-id

## 路由至 VPC 對等連線

VPC 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 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)。如需更多詳細資訊，請參閱 [VPC 和子網路 \(p. 73\)](#)。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 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 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 互連連線的詳細資訊，請參閱 [Amazon VPC Peering Guide](#)。

## ClassicLink 的路由

ClassicLink 是一項可讓您將 EC2-Classic 執行個體連結至 VPC、允許 EC2-Classic 執行個體和 VPC 中執行個體之間透過私有 IPv4 地址通訊的功能。如需 ClassicLink 的詳細資訊，請參閱 [ClassicLink \(p. 264\)](#)。

當您為 ClassicLink 啟用 VPC 時，就會將目的地為 10.0.0.0/8 且目標為 local 的路由新增至所有的子網路路由表。這可讓 VPC 中的執行個體與任何連結至 VPC 的 EC2-Classic 執行個體通訊。若您將另一個路由表新增至啟用 ClassicLink 的 VPC，它會自動接收目標 (destination) 為 10.0.0.0/8 且目標 (target) 為 local 的路由。若停用 VPC 的 ClassicLink，此路由便會自動從所有子網路路由表中刪除。

若您的任何子網路路由表具有位於 10.0.0.0/8 CIDR 內地址範圍的現有路由，則您無法為您的 VPC 啟用 ClassicLink。這不包含具有 10.0.0.0/16 和 10.1.0.0/16 IP 地址範圍的 VPC 本機路由。

如果您已為 ClassicLink 啟用 VPC，您可能無法將其他更明確的路由新增至您 10.0.0.0/8 IP 地址範圍的路由表。

若您修改 VPC 互連連線以啟用您 VPC 中執行個體和對等 VPC 連結之 EC2-Classic 執行個體間的通訊，便會自動將目標 (destination) 為 10.0.0.0/8，目標 (target) 為 local 的靜態路由新增至您的路由表。若您修改 VPC 互連連線以啟用連結至您 VPC 之本機 EC2-Classic 執行個體和對等 VPC 中執行個體之間的通訊，您必須手動將目標 (destination) 為對等 VPC CIDR 區塊，目標 (target) 為 VPC 互連連線的路由新增至您的主路由表。EC2-Classic 執行個體依存主路由表以路由至對等 VPC。如需詳細資訊，請參閱 Amazon VPC Peering Guide 中的 [ClassicLink 的組態](#)。

## 路由至閘道 VPC 端點

閘道 VPC 端點可讓您建立您 VPC 和另一個 AWS 服務之間的私有連線。建立閘道端點時，您可以在 VPC 中指定閘道端點所使用的子網路路由表。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 \(p. 280\)](#)。

## 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，讓私有子網路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，請在私有子網路路由表中新增將 IPv6 網際網路流量 (::/0) 路由至輸出限定網際網路閘道的路由。

目的地	目標
::/0	eigw-id

如需更多詳細資訊，請參閱 [輸出限定網際網路閘道 \(p. 218\)](#)。

## 傳輸閘道的路由

當您將 VPC 連接至transit gateway時，您需要將路由新增至子網路路由表，才能透過transit gateway路由流量。

請考慮當您有三個 VPC 已連接至transit gateway 的情況。在此案例中，所有連接都會與transit gateway路由表建立關聯，並傳播至transit gateway路由表。因此，所有連接都可彼此路由封包，而transit gateway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-1111111111111111
- VPC B: 10.2.0.0/16, attachment ID tgw-attach-2222222222222222

為啟用 VPC 間的流量及允許存取transit gateway，VPC A 路由表設定如下。

目的地	目標
10.1.0.0/16	區域
10.0.0.0/8	tgw-id

下列為 VPC 附件的transit gateway路由表項目範例。

目的地	目標
10.1.0.0/16	tgw-attach-1111111111111111
10.2.0.0/16	tgw-attach-2222222222222222

如需 transit gateway 路由表的詳細資訊，請參閱 Amazon VPC 傳輸閘道中的[路由表](#)。

## VPC 中的中間設備路由

您可以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 的子網路中部署為 Amazon EC2 執行個體，並以子網路中的彈性網路界面 (網路界面) 表示。

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。如需更多詳細資訊，請參閱 [閘道路由表 \(p. 188\)](#)。您也可以將傳出流量從子網路路由至另一個子網路中的中間設備。

### Note

如果您已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。檢閱您的路由，以確保流量已正確路由，並確保不會因為啟用或停用路由傳播，而產生意外的後果 (例如，支援巨型訊框的 AWS Direct Connect 連線需要路由傳播)。

## 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路中。
- 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《Linux 執行個體的 Amazon EC2 使用者指南》中的 [變更來源或目標檢查](#)。
- 不支援服務鍵。
- 您無法透過設備在相同子網路中的主機之間路由流量。
- 您無法透過設備在子網路之間路由流量。
- 設備不需要執行網路位址轉譯 (NAT)。
- 若要攔截 IPv6 流量，請確定您針對 IPv6 設定 VPC、子網路和設備。如需更多詳細資訊，請參閱 [使用 VPC 和子網路 \(p. 81\)](#)。虛擬私有閘道不支援 IPv6 流量。

## 設備路由組態

若要将傳入流量路由至設備，請建立路由表格，並新增一個路由，將前往子網路的流量指向設備的網路界面。此路由比路由表的本機路由更為具體。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。下列路由表會將前往子網路的 IPv4 流量路由至設備的網路界面。

目的地	目標
10.0.0.0/16	區域
10.0.1.0/24	eni-id

或者，您可以將本機路由的目標取代為設備的網路界面。您可以這樣做，以確保所有流量都會自動路由至設備，包括前往您稍後新增至 VPC 之子網路的流量。

目的地	目標
10.0.0.0/16	eni-id

若要将流量從子網路路由到另一個子網路中的設備，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
10.0.0.0/16	區域
0.0.0.0/0	eni-id

然後，在與設備子網路相關聯的路由表中，新增一個路由，將流量路由回網際網路閘道或虛擬私有閘道。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	igw-id

您可以針對 IPv6 流量套用相同的路由組態。例如，在閘道路由表中，您可以將 IPv4 和 IPv6 本機路由的目標取代為設備的網路界面。

目的地	目標
10.0.0.0/16	eni-id
2001:db8:1234:1a00::/56	eni-id

在下圖中，於 VPC 的子網路 A 中的 Amazon EC2 執行個體上安裝和設定防火牆設備。此設備會檢查透過網際網路閘道進入和離開 VPC 的所有流量。路由表 A 與網際網路閘道相關聯。前往透過網際網路閘道進入 VPC 之子網路 B 的流量會路由至設備的網路界面 (eni-11223344556677889)。離開子網路 B 的所有流量也會路由至設備的網路界面。

下列範例具有與上述範例相同的設定，但包含 IPv6 流量。前往透過網際網路閘道進入 VPC 之子網路 B 的 IPv6 流量會路由至設備的網路界面 (eni-11223344556677889)。離開子網路 B 的所有流量 (IPv4 和 IPv6) 也會路由至設備的網路界面。

## 使用字首清單進行路由

如果您經常在 AWS 資源中參考同一組 CIDR 區塊，則可以建立[客戶管理的字首清單](#) (p. 204)，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。在子網路路由表中，您可以建立路由並指定字首清單作為目的地，並指定傳輸閘道指定為目標。

目的地	目標
172.31.0.0/16	區域
pl-123abc123abc123ab	tgw-id

字首清單的項目數目上限等於路由表中的相同項目數。

## 使用路由表

下列任務顯示如何使用路由表。

### Note

當您在主控台中使用 VPC 精靈建立具備閘道的 VPC 時，精靈會自動更新路由表以使用閘道。若您使用命令行工具或 API 設定您的 VPC，您必須自行更新路由表。

工作

- [判斷與子網路關聯的路由表 \(p. 198\)](#)
- [判斷與路由表明確相關聯的子網路及 \(或\) 閘道 \(p. 198\)](#)
- [建立自訂路由表 \(p. 199\)](#)
- [從路由表新增和移除路由 \(p. 199\)](#)
- [啟用和停用路由傳播 \(p. 200\)](#)
- [將子網路與路由表建立關聯 \(p. 201\)](#)
- [變更子網路路由表 \(p. 201\)](#)
- [取消子網路與路由表的關聯 \(p. 201\)](#)
- [取代主路由表 \(p. 202\)](#)
- [將閘道與路由表建立關聯 \(p. 202\)](#)
- [取消閘道與路由表的關聯 \(p. 203\)](#)
- [取代和還原本機路由的目標 \(p. 203\)](#)
- [刪除路由表 \(p. 204\)](#)

## 判斷與子網路關聯的路由表

您可以透過在 Amazon VPC 主控台中查看子網路詳細資訊，來判斷與子網路關聯的路由表。

### 判斷與子網路關聯的路由表

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 (子網路)。
3. 選擇 Route Table (路由表) 標籤以檢視路由表 ID 及其路由。若其為主路由表，主控台不會指出該關聯為隱含或明確。若要判斷與主路由表的關聯是否為明確關聯，請參閱 [判斷與路由表明確相關聯的子網路及 \(或\) 閘道 \(p. 198\)](#)。

## 判斷與路由表明確相關聯的子網路及 (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路或閘道。

主路由表可具有明確及隱含的子網路關聯。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路便會和主路由表建立隱含關聯。您可以明確地將子網路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 \(p. 202\)](#)。

### 使用主控台判斷哪些子網路明確關聯

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. 檢視 Explicit subnet association (明確的子網路關聯) 欄以判斷明確關聯的子網路。
4. 選取需要的路由表。
5. 在詳細資訊窗格中選擇 Subnet Associations (子網路關聯) 標籤。與表明確關聯的子網路會列在標籤上。所有沒有與任何路由表建立關聯 (並因此與主路由表建立隱含關聯) 的子網路也會列出。

### 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. 檢視 Edge associations (邊緣關聯) 欄以判斷關聯的閘道。
4. 選取需要的路由表。
5. 在詳細資訊窗格中選擇 Edge Associations (邊緣關聯) 標籤。這時會列出與路由表相關聯的閘道。

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](#) (適用於 Windows PowerShell 的 AWS 工具)

## 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) 針對名稱標籤，輸入您連接的名稱。
5. 在 VPC (VPC) 中，選擇您的 VPC。
6. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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」右邊的刪除按鈕 (「x」)。

7. 選擇 Create (建立)。

使用命令列建立自訂路由表

- [create-route-table](#) (AWS CLI)
- [New-EC2RouteTable](#) (適用於 Windows PowerShell 的 AWS 工具)

## 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 站台對站台 VPN 連線之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 站台對站台 VPN 連線的靜態路由](#)。

使用主控台修改路由或將路由新增至路由表

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
3. 選擇 Actions (動作)、Edit routes (編輯路由)。
4. 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。

- 若要修改現有路由，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。
- 選擇 Save routes (儲存路由)。

使用命令列將路由新增至路由表

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (適用於 Windows PowerShell 的 AWS 工具)

#### 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。

使用命令列取代路由表中的現有路由

- [replace-route](#) (AWS CLI)
- [Set-EC2Route](#) (適用於 Windows PowerShell 的 AWS 工具)

使用主控台從路由表中刪除路由

- 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
- 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
- 選擇 Actions (動作)、Edit routes (編輯路由)。
- 選擇要刪除之路由右側的刪除按鈕 (x)。
- 完成後，選擇 Save routes (儲存路由)。

使用命令列從路由表中刪除路由

- [delete-route](#) (AWS CLI)
- [Remove-EC2Route](#) (適用於 Windows PowerShell 的 AWS 工具)

## 啟用和停用路由傳播

路由傳播允許虛擬私有閘道自動將路由傳播到路由表。這表示您不需要手動將 VPN 路由輸入到路由表。您可以啟用或停用路由傳播。

如需 VPN 路由選項的詳細資訊，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

- 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
- 在導覽窗格中，選擇 Route Tables (路由表)，然後選取路由表。
- 選擇 Actions (動作)、Edit route propagation (編輯路由傳播)。
- 選取位於虛擬私有閘道旁邊的 Propagate (傳播) 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](#) (適用於 Windows PowerShell 的 AWS 工具)



### 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 Propagate (傳播) 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](#) (適用於 Windows PowerShell 的 AWS 工具)

## 將子網路與路由表建立關聯

若要將路由表路由套用至特定子網路，您必須將路由表與子網路建立關聯。路由表可以和多個子網路建立關聯。不過，子網路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路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路建立關聯

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 (子網路關聯) 標籤上，選擇 Edit subnet associations (編輯子網路關聯)。
4. 選取子網路的 Associate (關聯) 核取方塊以和路由表建立關聯，然後選擇 Save (儲存)。

### 使用命令列將子網路與路由表建立關聯

- [associate-route-table](#) (AWS CLI)
- [Register-EC2RouteTable](#) (適用於 Windows PowerShell 的 AWS 工具)

## 變更子網路路由表

您可以變更與子網路相關聯的路由表。

### 使用主控台變更子網路路由表關聯

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 (子網路)，然後選取子網路。
3. 在 Route Table (路由表) 標籤中，選擇 Edit route table association (編輯路由表關聯)。
4. 從 Route Table ID (路由表 ID) 清單中，選取要與子網路建立關聯的新路由表，然後選擇 Save (儲存)。

### 使用命令列變更與子網路關聯的路由表

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (適用於 Windows PowerShell 的 AWS 工具)

## 取消子網路與路由表的關聯

您可以取消子網路與路由表的關聯。直到您將子網路與另一個路由表建立關聯之前，子網路會與主路由表隱含建立關聯。

### 使用主控台取消子網路與路由表的關聯

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. 在 Subnet Associations (子網路關聯) 標籤中，選擇 Edit subnet associations (編輯子網路關聯)。
4. 清除子網路的 Associate (關聯) 核取方塊，然後選擇 Save (儲存)。

### 使用命令列取消子網路與路由表的關聯

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (適用於 Windows PowerShell 的 AWS 工具)

## 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)。
3. 選取應該成為新主路由表的子網路路由表，然後選擇 Actions (動作)、Set Main Route Table (設定主路由表)。
4. 在確認對話方塊中，選擇 Ok (確定)。

### 使用命令列取代主路由表

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (適用於 Windows PowerShell 的 AWS 工具)

以下程序說明如何移除子網路和主路由表之間的明確關聯。子網路和主路由表之間會形成隱含關聯。程序和取消子網路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. 在 Subnet Associations (子網路關聯) 標籤中，選擇 Edit subnet associations (編輯子網路關聯)。
4. 清除子網路的核取方塊，然後選擇 Save (儲存)。

## 將閘道與路由表建立關聯

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。如需更多詳細資訊，請參閱 [閘道路由表](#) (p. 188)。

### 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. 選擇 Actions (動作)、Edit edge associations (編輯邊緣關聯)。

4. 選擇 Internet gateways (網際網路閘道) 或 Virtual private gateways (虛擬私有閘道) 以顯示閘道清單。
5. 選擇閘道，然後選擇 Save (儲存)。

使用 AWS CLI 將閘道與路由表建立關聯

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. 選擇 Actions (動作)、Edit edge associations (編輯邊緣關聯)。
4. 針對 Associated gateways (關聯的閘道)，為您要取消關聯的閘道選擇刪除按鈕 (x)。
5. 選擇 Save (儲存)。

使用命令列取消閘道與路由表的關聯

- `disassociate-route-table` (AWS CLI)
- `Unregister-EC2RouteTable` (適用於 Windows PowerShell 的 AWS 工具)

## 取代和還原本機路由的目標

您可以變更 [閘道路由表](#) (p. 188) 中預設本機路由的目標，並改在與目標相同的 VPC 中指定網路界面或執行個體。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](#) (p. 77)，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。

您無法在子網路路由表中取代本機路由的目標。

使用控制台取代本機路由的目標

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. 針對 Target (目標)，選擇 Network Interface (網路界面) 以顯示網路界面清單，然後選擇網路界面。  
或者，選擇 Instance (執行個體)，以顯示執行個體清單，然後選擇執行個體。
5. 選擇 Save routes (儲存路由)。

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. 針對 Target (目標)，選擇 local (本機)。
5. 選擇 Save routes (儲存路由)。

使用 AWS CLI 取代本機路由的目標

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
```

使用 AWS CLI 還原本機路由的目標

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路相關聯時，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)。
3. 選取路由表，然後選擇 Actions (動作)、Delete Route Table (刪除路由表)。
4. 在確認對話方塊中，選擇 Delete Route Table (刪除路由表)。

使用主控台刪除路由表

- `delete-route-table` (AWS CLI)
- `Remove-EC2RouteTable` (適用於 Windows PowerShell 的 AWS 工具)

## 字首清單

字首清單是一或多個 CIDR 區塊的集合。字首清單有兩個類型：

- AWS 管理的字首清單 — 代表 AWS 服務的 IP 地址範圍。您可以在 VPC 安全群組規則和子網路路由表項目中參考 AWS 管理的字首清單。例如，透過 [開道 VPC 端點 \(p. 279\)](#) 連線至 AWS 服務時，您可以在輸出 VPC 安全群組規則中參考 AWS 管理的字首清單。您無法建立、修改、共用或刪除 AWS 管理的字首清單。
- 客戶管理的字首清單 — 由您定義和管理的一組 IPv4 或 IPv6 CIDR 區塊。您可以參考 VPC 安全群組規則、子網路路由表項目和傳輸開道路由表項目中的字首清單。這可讓您管理單一群組中經常用於這些資源的 IP 地址，而無須在每個資源中重複參考相同的 IP 地址。您可以與其他 AWS 帳戶共用您的字首清單，讓這些帳戶能夠在自己資源中參考字首清單。

下列主題說明如何建立及使用客戶管理的字首清單。

#### 主題

- [字首清單的概念和規則 \(p. 205\)](#)
- [使用字首清單 \(p. 205\)](#)
- [字首清單的識別與存取管理 \(p. 209\)](#)
- [使用共用字首清單 \(p. 210\)](#)

## 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。

下列規則適用於客戶管理的字首清單：

- 當您建立字首清單時，必須指定字首清單可支援的最大項目數。您稍後無法修改項目的數目上限。
- 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為該資源之規則或項目的相同數目。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。
- 您可以透過新增或移除項目或變更其名稱來修改字首清單。
- 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。
- 字首清單有相關的配額。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。
- 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 [字首清單的路由優先順序 \(p. 190\)](#)。

下列規則適用於 AWS 管理的字首清單：

- 您無法建立、修改、共用或刪除 AWS 管理的字首清單。
- 當您在資源中參考 AWS 管理的字首清單時，該清單計為資源的單一規則或項目。
- 您無法檢視 AWS 管理的字首清單的版本號碼。

## 字首清單版本

字首清單可以有多个版本。每次您新增或移除字首清單的項目時，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。您可以將舊版字首清單中的項目還原至新版本。

## 使用字首清單

下列主題說明如何建立及使用客戶管理的字首清單。您可以使用 Amazon VPC 主控台或 AWS CLI 來使用字首清單。

#### 主題

- [建立字首清單 \(p. 206\)](#)
- [檢視字首清單 \(p. 206\)](#)
- [檢視字首清單的項目 \(p. 206\)](#)
- [檢視字首清單的關聯 \(參考\) \(p. 207\)](#)
- [修改字首清單 \(新增和移除項目\) \(p. 207\)](#)
- [還原舊版的字首清單 \(p. 207\)](#)
- [刪除字首清單 \(p. 208\)](#)

- 在 [AWS 資源中參考字首清單 \(p. 208\)](#)

## 建立字首清單

當您建立新的字首清單時，必須指定字首清單可支援的最大項目數。請務必指定符合您需求的項目數目上限，因為稍後無法變更此數目。

### 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 AWS CLI 建立字首清單

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

## 檢視字首清單

您可以使用 Amazon VPC 主控台或 AWS CLI 檢視您的字首清單、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. Owner ID (擁有者 ID) 欄會顯示字首清單擁有者的 AWS 帳戶 ID。對於 AWS 管理的字首清單，Owner ID (擁有者 ID) 是 AWS。

### 使用 AWS CLI 檢視字首清單

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

## 檢視字首清單的項目

您可以使用 Amazon VPC 主控台或 AWS CLI 檢視字首清單的項目。

### 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。

4. 在下方窗格中，選擇 Entries (項目) 以檢視字首清單的項目。

使用 AWS CLI 檢視字首清單的項目

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

## 檢視字首清單的關聯 (參考)

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

您無法檢視 AWS 管理的字首清單的關聯資源。

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。
4. 在下方窗格中，選擇 Associations (關聯) 以檢視參考字首清單的資源。

使用 AWS CLI 檢視字首清單關聯

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

## 修改字首清單 (新增和移除項目)

您可以修改字首清單的名稱，也可以新增或移除項目。

您無法修改 AWS 管理的字首清單。

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，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)。

使用 AWS CLI 修改字首清單

使用 `modify-managed-prefix-list` 命令。

## 還原舊版的字首清單

您可以將舊版字首清單中的項目還原至新版本。

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，然後選擇 Actions (動作)、Restore prefix list (還原字首清單)。
4. 在下拉式清單中，選擇字首清單版本。
5. 選擇 Restore prefix list (還原字首清單)。

使用 AWS CLI 還原舊版的字首清單

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

## 刪除字首清單

若要刪除字首清單，您必須先移除資源中 (例如在路由表中) 對其進行的任何參考。如果您已使用 AWS RAM 共用字首清單，則必須先移除消費者擁有資源中的任何參考項目。若要檢視對字首清單的參考，請參閱[檢視字首清單的關聯 \(參考\)](#) (p. 207)。

您無法刪除 AWS 管理的字首清單。

使用主控台刪除字首清單

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

使用 AWS CLI 刪除字首清單

使用 `delete-managed-prefix-list` 命令。

## 在 AWS 資源中參考字首清單

您可以在下列 AWS 資源中參考字首清單：

Subnet route tables

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[路由表](#) (p. 184)。

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)。對於 Destination (目的地)，請輸入字首清單的 ID。
5. 針對 Target (目標)，選擇一個目標。
6. 選擇 Save routes (儲存路由)。

使用 AWS CLI 在路由表中參考字首清單

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。

## VPC security groups

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。如需安全群組的詳細資訊，請參閱[VPC 的安全群組 \(p. 138\)](#)。

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)。

使用 AWS CLI 在安全群組規則中參考字首清單

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

## Transit gateway route tables

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[字首清單參考資料](#)。

# 字首清單的識別與存取管理

根據預設，IAM 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字首清單的 IAM 政策。

若要查看可在 IAM 政策中使用的 Amazon VPC 動作清單以及資源和條件索引鍵，請參閱 IAM 使用者指南中的[適用於 Amazon EC2 的動作、資源及條件索引鍵](#)。

下列範例政策只允許使用者檢視和使用字首清單 `p1-123456abcde123456`。使用者無法建立或刪除字首清單。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeManagedPrefixLists",
      "ec2:ModifyManagedPrefixList",
      "ec2:GetManagedPrefixListEntries",
      "ec2:RestoreManagedPrefixListVersion",
      "ec2:GetManagedPrefixListAssociations"
    ],
    "Resource": "arn:aws:ec2:region:account:prefix-list/p1-123456abcde123456"
  }]
}
```

如需在 Amazon VPC 中使用 IAM 的詳細資訊，請參閱[Amazon VPC 的 Identity and Access Management \(p. 123\)](#)。

## 使用共用字首清單

客戶管理的字首清單可與 AWS Resource Access Manager (AWS RAM) 整合。您可以透過 AWS RAM 建立資源共享，以在各 AWS 帳戶間分享您擁有的資源。這會指定要分享的資源，以及共用它們的消費者。消費者可以是個別的 AWS 帳戶，或 AWS Organizations 中的組織單位或整個組織。

如需 AWS RAM 的詳細資訊，請參閱[AWS RAM 使用者指南](#)。

字首清單的擁有者可以與下列項目共用字首清單：

- AWS Organizations 組織內外的特定 AWS 帳戶
- AWS Organizations 之組織內的組織單位
- AWS Organizations 中的整個組織

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

內容

- [共用字首清單的先決條件 \(p. 210\)](#)
- [共用字首清單 \(p. 210\)](#)
- [識別共用的字首清單 \(p. 211\)](#)
- [識別共用字首清單的參考 \(p. 211\)](#)
- [取消共用字首清單 \(p. 211\)](#)
- [共用字首清單許可 \(p. 212\)](#)
- [計費和計量 \(p. 212\)](#)
- [配額 \(p. 212\)](#)

## 共用字首清單的先決條件

- 若要共用字首清單，您必須在您的 AWS 帳戶中擁有該字首清單。您無法將已分享給您的字首清單再分享出去。您無法共用 AWS 管理的字首清單。
- 若要與組織或 AWS Organizations 內的組織單位共用字首清單，您必須透過 AWS Organizations 啟用共用。如需詳細資訊，請參閱AWS RAM 使用者指南中的[透過 AWS Organizations 啟用共用](#)。

## 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 AWS Organizations 中組織的一分子，並已啟用與您所屬組織共用的功能，則組織中的消費者便能自動存取所共用的字首清單。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

請依照AWS RAM 使用者指南中[建立資源共享](#)的步驟執行。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。

使用 AWS CLI 共用您擁有的字首清單

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 主控台識別共用的字首清單

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. 此頁面會顯示您擁有的字首清單，以及與您共用的字首清單。Owner ID (擁有者 ID) 欄會顯示字首清單擁有者的 AWS 帳戶 ID。
4. 若要檢視字首清單的資源共享資訊，請選取字首清單，然後選擇下方窗格中的 Sharing (共用)。

使用 AWS CLI 識別共用字首清單

使用 [describe-managed-prefix-lists](#) 命令。此命令會傳回您擁有的字首清單，以及與您共用的字首清單。OwnerId 會顯示字首清單擁有者的 AWS 帳戶 ID。

## 識別共用字首清單的參考

擁有者可以使用 Amazon VPC 主控台和 AWS CLI 來識別參考共用字首清單的消費者擁有資源。

使用 Amazon VPC 主控台識別共用字首清單的參考

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

使用 AWS CLI 識別共用字首清單的參考

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

## 取消共用字首清單

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](#) (p. 211)。如果您將字首清單更新為新版本，則參考會使用最新版本。

若要取消共享您擁有的已共用字首清單，您必須從資源共享中移除它。您可以使用 AWS RAM 主控台或 AWS CLI 執行這項作業。

使用 AWS RAM 主控台取消共用您擁有的共用字首清單

請參閱《AWS RAM 使用者指南》中的[更新資源共享](#)。

使用 AWS CLI 取消共用您擁有的共用字首清單

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字首清單的 AWS 資源 ID。但是，他們無法在 AWS 資源中新增或移除對消費者擁有之字首清單的參考。

如果在消費者擁有的資源中參考了字首清單，則擁有者無法刪除該字首清單。

### 消費者的許可

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

## 計費和計量

共用字首清單無須額外收費。

## 配額

如需與 AWS RAM 相關配額 (限制) 的詳細資訊，請參閱 AWS RAM 使用者指南中的[服務限制](#)。

# 網際網路閘道

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。

網際網路閘道有兩種用途：在 VPC 路由表中提供可由網際網路路由之流量的目標，以及針對已獲指派公有 IPv4 地址的執行個體執行網路位址轉譯 (NAT)。

網際網路閘道支援 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。在您的帳戶中設有網際網路閘道，無需額外付費。

## 啟用網際網路存取

若要針對 VPC 內子網路中的執行個體啟用與網際網路之間的存取，您必須執行下列作業：

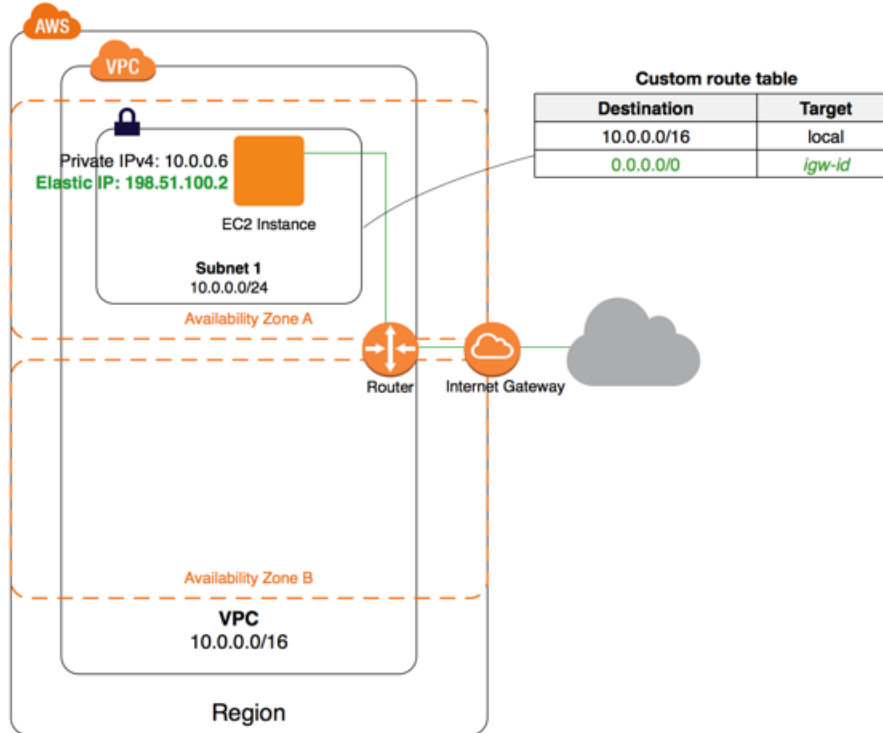
- 將網際網路閘道連接至 VPC。
- 新增路由至子網路路由表，將網際網路綁定型流量導向至網際網路閘道。如果子網路與路由至網際網路閘道的路由表建立關聯，即稱為公有子網路。如果子網路與未路由至網際網路閘道的路由表建立關聯，則稱為私有子網路。
- 確定子網路中的執行個體具有全域唯一 IP 地址 (公有 IPv4 地址、彈性 IP 地址或 IPv6 地址)。
- 確定您的網路存取控制清單和安全群組規則允許相關流量流向和流出您的執行個體。

在子網路路由表中，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，您可以將路由範圍限定為較窄的 IP 地址範圍。例如，您公司在 AWS 外部之公有端點的公有 IPv4 地址，或 VPC 外部之其他 Amazon EC2 執行個體的彈性 IP 地址。

若要針對 IPv4 啟用透過網際網路的通訊，您的執行個體必須要有公有 IPv4 地址，或是與執行個體上之私有 IPv4 地址建立關聯的彈性 IP 地址。您的執行個體只能辨識 VPC 和子網路內定義的私有 (內部) IP 地址空間。網際網路閘道邏輯上會代您的執行個體提供一對一 NAT，因此流量離開 VPC 子網路並前往網際網路時，回覆地址欄位會設定成您執行個體的公有 IPv4 地址或彈性 IP 地址，而非私有 IP 地址。相反地，目標設為您執行個體的公有 IPv4 地址或彈性 IP 地址的流量，會將其目標地址轉譯為執行個體的私有 IPv4 地址，再將流量交付給 VPC。

若要針對 IPv6 啟用透過網際網路的通訊，您的 VPC 和子網路必須具有相關聯的 IPv6 CIDR 區塊，而且必須有來自子網路範圍的 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。

在下圖中，VPC 中的子網路 1 是公有子網路。它與自訂路由表建立關聯，而自訂路由表會將所有網際網路綁定型 IPv4 流量指向網際網路閘道。執行個體具有彈性 IP 地址，以啟用與網際網路的通訊。



如要為您的執行個體提供網際網路存取，但不為其指派公有 IP 地址，您可以改用 NAT 裝置。如需更多詳細資訊，請參閱 [NAT \(p. 226\)](#)。

#### 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	如果您已使用 VPC 精靈中的第一個或第二個選項建立 VPC，則為「是」。否則，您必須手動建立並連接網際網路閘道。
將 IPv4 流量 (0.0.0.0/0) 路由至網際網路閘道的路由表	是	如果您已使用 VPC 精靈中的第一個或第二個選項建立 VPC，則為「是」。否則，您必須手動建立路由表，並新增路由。

元件	預設 VPC	非預設 VPC
將 IPv6 流量 (::/0) 路由至網際網路閘道的路由表	否	如果您已使用 VPC 精靈中的第一個或第二個選項建立 VPC，以及如果您已指定選項來建立 IPv6 CIDR 區塊與 VPC 的關聯，則為「是」。否則，您必須手動建立路由表，並新增路由。
自動指派給子網路中所啟動之執行個體的公有 IPv4 地址	是 (預設子網路)	否 (非預設子網路)
自動指派給子網路中所啟動之執行個體的 IPv6 地址	否 (預設子網路)	否 (非預設子網路)

如需預設 VPC 的詳細資訊，請參閱[預設 VPC](#) 和 [預設子網路](#) (p. 95)。如需使用 VPC 精靈利用網際網路閘道建立 VPC 的詳細資訊，請參閱[具有單一公有子網路的 VPC](#) (p. 18) 或 [具有公有和私有子網路 \(NAT\) 的 VPC](#) (p. 24)。

如需 VPC 中 IP 定址以及控制如何將公有 IPv4 或 IPv6 地址指派給執行個體的詳細資訊，請參閱 [您 VPC 中的 IP 定址](#) (p. 102)。

當您將新的子網路新增至 VPC 時，必須設定您要用於子網路的路由和安全。

## 將網際網路閘道新增至 VPC。

以下說明如何手動建立公有子網路並將網際網路閘道連接至 VPC，以支援網際網路存取。

### 任務

- [正在建立子網路](#) (p. 214)
- [建立並連接網際網路閘道](#) (p. 215)
- [建立自訂路由表](#) (p. 215)
- [建立適用於網際網路存取的安全群組](#) (p. 216)
- [新增彈性 IP 地址](#) (p. 216)
- [將網際網路閘道自 VPC 分離](#) (p. 217)
- [刪除網際網路閘道](#) (p. 217)
- [API 和命令概觀](#) (p. 217)

## 正在建立子網路

### 將子網路新增至 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 (子網路)、Create subnet (建立子網路)。
3. 視需要指定子網路詳細資料。
  - 名稱標籤：選擇性提供您子網路的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
  - VPC：選擇您希望為其建立子網路的 VPC。
  - Availability Zone (可用區域)：選擇性地選擇您子網路所在的可用區域或本機區域，或是使用預設的 No Preference (無偏好設定)，讓 AWS 為您選擇可用區域。



如需哪些區域支援本機區域的相關資訊，請參閱《Linux 執行個體的 Amazon EC2 使用者指南》中的[可用區域](#)。

- IPv4 CIDR 區塊：指定您子網路的 IPv4 CIDR 區塊，例如：10.0.1.0/24。如需詳細資訊，請參閱[IPv4 的 VPC 和子網路規模 \(p. 76\)](#)。
- IPv6 CIDR 區塊：(選用) 若您已將 IPv6 CIDR 區塊與您的 VPC 建立關聯，請選擇 Specify a custom IPv6 CIDR (指定自訂 IPv6 CIDR)。指定子網路的十六進位對值，或是使用預設值。

4. 選擇 Create (建立)。

如需子網路的詳細資訊，請參閱[VPC 和子網路 \(p. 73\)](#)。

## 建立並連接網際網路閘道

建立網際網路閘道後，請將其連接至您的 VPC。

建立網際網路閘道並連接至您的 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)，然後選擇 Create internet gateway (建立網際網路閘道)。
3. 選擇性命名您的網際網路閘道。
4. 選擇性新增或移除標籤。

[新增標籤] 選擇 Add tag (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. 選擇建立網際網路閘道。
6. 選取您剛建立的網際網路閘道，然後選擇 Actions, Attach to VPC (動作、連接到 VPC)。
7. 從清單選取您的 VPC，然後選擇連接網際網路閘道。

## 建立自訂路由表

當您建立子網路時，我們會自動建立子網路與 VPC 之主路由表的關聯。根據預設，主路由表不會包含網際網路閘道的路由。下列程序會建立自訂路由表，其中具有路由可將目標設為 VPC 外部的流量傳送至網際網路閘道，然後建立與您子網路的關聯。

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)，然後選擇 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 Yes, Create (是，建立)。
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 (編輯)、Add another route (新增另一個路由)，然後視需要新增下列路由。完成後，請選擇 Save (儲存)。
  - 對於 IPv4 流量，在 Destination (目標) 方塊中指定 0.0.0.0/0，然後在 Target (目標) 清單中選取網際網路閘道 ID。

- 對於 IPv6 流量，在 Destination (目標) 方塊中指定 `::/0`，然後在 Target (目標) 清單中選取網際網路開道 ID。
6. 在 Subnet Associations (子網路關聯) 標籤上，選擇 Edit (編輯)，並選取子網路的 Associate (關聯) 核取方塊，然後選擇 Save (儲存)。

如需更多詳細資訊，請參閱 [路由表 \(p. 184\)](#)。

## 建立適用於網際網路存取的安全群組

依預設，VPC 安全群組允許所有傳出流量。您可以建立新的安全群組，並新增允許來自網際網路之傳入流量的規則。然後，您可以將安全群組與公用子網路中的執行個體建立關聯。

建立新的安全群組並與您的執行個體建立關聯

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)，然後選擇 Create Security Group (建立安全群組)。
3. 在 Create Security Group (建立安全群組) 對話方塊中，指定安全群組的名稱和描述。從 VPC 清單選取您 VPC 的 ID，然後選擇 Yes, Create (是，建立)。
4. 選取安全群組。詳細資訊窗格會顯示安全群組的詳細資訊，以及使用其傳入規則和傳出規則的標籤。
5. 在 Inbound Rules (傳入規則) 標籤上，選擇 Edit (編輯)。選擇 Add Rule (新增規則)，然後完成必要資訊。例如，從 Type (類型) 清單選取 HTTP 或 HTTPS，然後將 Source (來源) 輸入為 `0.0.0.0/0` (適用於 IPv4 流量) 或 `::/0` (適用於 IPv6 流量)。完成後，請選擇 Save (儲存)。
6. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
7. 在導覽窗格中，選擇 Instances (執行個體)。
8. 選取執行個體，選擇 Actions (動作) 和 Networking (聯網)，然後選取 Change Security Groups (變更安全群組)。
9. 在 Change Security Groups (變更安全群組) 對話方塊中，清除目前選取的安全群組核取方塊，然後選取新的安全群組。選擇 Assign Security Groups (指派安全群組)。

如需更多詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。

## 新增彈性 IP 地址

在您於子網路中啟動執行個體之後，如果想要透過 IPv4 從網際網路存取該執行個體，則必須予以指派彈性 IP 地址。

### Note

如果您在啟動期間將公有 IPv4 地址指派給執行個體，則可以從網際網路存取該執行個體，而且不需要予以指派彈性 IP 地址。如需您執行個體之 IP 定址的詳細資訊，請參閱 [您 VPC 中的 IP 定址 \(p. 102\)](#)。

使用主控台配置彈性 IP 地址，並將其指派給執行個體

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 new address (配置新地址)。
4. 選擇 Allocate (配置)。

### Note

如果您的帳戶支援 EC2-Classic，則請先選擇 VPC。

5. 從清單選取彈性 IP 地址，並選擇 Actions (動作)，然後選擇 Associate address (與地址建立關聯)。

6. 選擇 Instance (執行個體) 或 Network interface (網路界面)，然後選取執行個體或網路界面 ID。選取要與彈性 IP 地址建立關聯的私有 IP 地址，然後選擇 Associate (關聯)。

如需更多詳細資訊，請參閱 [彈性 IP 地址](#) (p. 260)。

## 將網際網路閘道自 VPC 分離

如果您不再需要透過網際網路存取在非預設 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 Elastic IPs (彈性 IP)，然後選取彈性 IP 地址。
3. 選擇 Actions (動作)、Disassociate address (取消與地址的關聯)。選擇 Disassociate address (取消與地址的關聯)。
4. 在導覽窗格中，選擇 Internet Gateways (網際網路閘道)。
5. 選取網際網路閘道，然後選擇 Actions, Detach from VPC (動作、自 VPC 分離)。
6. 在從 VPC 分離對話方塊中，選擇分離網際網路閘道。

## 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. 選取網際網路閘道，然後選擇 Actions (動作)、Delete internet gateway (刪除網際網路閘道)。
4. 在刪除網際網路閘道對話方塊中，輸入 delete，然後選擇刪除網際網路閘道。

## 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 [存取 Amazon VPC](#) (p. 1)。

### 建立網際網路閘道

- [create-internet-gateway](#) (AWS CLI)
- [New-EC2InternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

### 將網際網路閘道連接至 VPC

- [attach-internet-gateway](#) (AWS CLI)
- [Add-EC2InternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

### 說明網際網路閘道

- [describe-internet-gateways](#) (AWS CLI)

- [Get-EC2InternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

將網際網路閘道自 VPC 分離

- [detach-internet-gateway](#) (AWS CLI)
- [Dismount-EC2InternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

刪除網際網路閘道

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

## 輸出限定網際網路閘道

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。如需更多詳細資訊，請參閱 [NAT 閘道](#) (p. 226)。

### 內容

- [輸出限定網際網路閘道基本概念](#) (p. 218)
- [使用輸出限定網際網路閘道](#) (p. 219)
- [API 和 CLI 概觀](#) (p. 220)

## 輸出限定網際網路閘道基本概念

如果公有子網路中的執行個體具有公有 IPv4 地址或 IPv6 地址，可以透過網際網路閘道連線至網際網路。同樣地，網際網路上的資源可以使用執行個體的公有 IPv4 地址或 IPv6 地址，來初始化與執行個體的連線；例如您使用本機電腦連線至執行個體時。

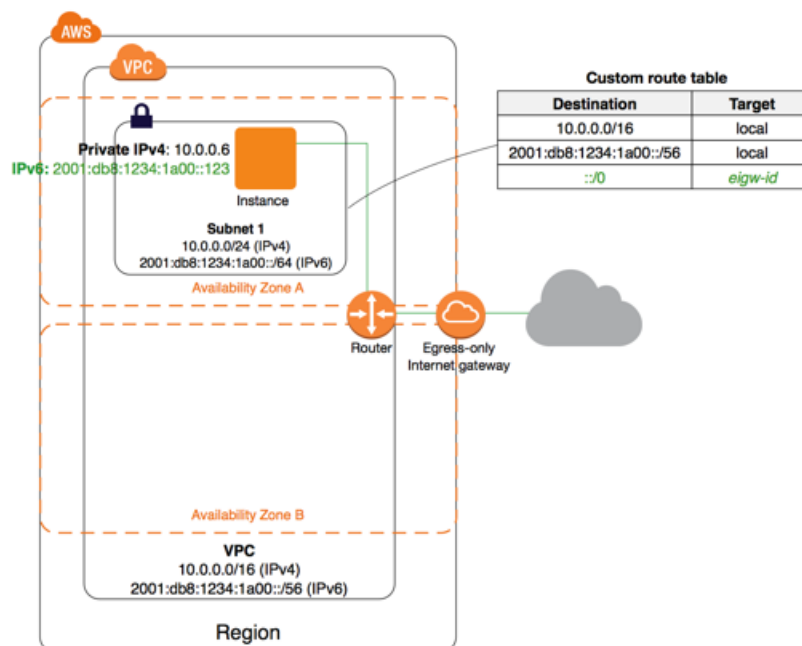
IPv6 地址是全域唯一的，因此預設是公開的。如果您想要執行個體可以存取網際網路，但想要防止網際網路上的資源啟動與您執行個體的通訊，則可以使用輸出限定網際網路閘道。若要執行此作業，請在 VPC 中建立輸出限定網際網路閘道，然後將路由新增至路由表，以將所有 IPv6 流量 (:::/0) 或特定範圍的 IPv6 地址指向輸出限定網際網路閘道。與路由表建立關聯之子網路中的 IPv6 流量會遞送至輸出限定網際網路閘道。

輸出限定網際網路閘道具有狀態：它會將流量從子網路中的執行個體轉送至網際網路或其他 AWS 服務，然後將回應送回執行個體。

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路由其流量之子網路的流量。

在下圖中，VPC 具有 IPv6 CIDR 區塊，而 VPC 中的子網路具有 IPv6 CIDR 區塊。自訂路由表與子網路 1 建立關聯，並將所有網際網路的 IPv6 流量 (:::/0) 指向 VPC 中的輸出限定網際網路閘道。



## 使用輸出限定網際網路閘道

下列各節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。

### 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

若要将目標設為 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，然後選擇是，建立。
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 (編輯)，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 (儲存)。
6. 在子網路關聯標籤上，選擇編輯，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 [路由表](#) (p. 184)。

## 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 [存取 Amazon VPC](#) (p. 1)。

### 建立輸出限定網際網路閘道

- [create-egress-only-internet-gateway](#) (AWS CLI)
- [New-EC2EgressOnlyInternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

### 說明輸出限定網際網路閘道

- [describe-egress-only-internet-gateways](#) (AWS CLI)
- [Get-EC2EgressOnlyInternetGatewayList](#) (適用於 Windows PowerShell 的 AWS 工具)



### 刪除輸出限定網際網路閘道

- [delete-egress-only-internet-gateway](#) (AWS CLI)
- [Remove-EC2EgressOnlyInternetGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

## 電信業者閘道

電信業者閘道有兩個用途。它允許從電信業者網路在特定位置的輸入流量，並允許輸出流量到電信業者網路和網際網路。沒有從網際網路到 Wavelength 區域通過電信業者閘道的輸入連線組態。

電信業者閘道支援 IPv4 流量。

電信業者閘道僅適用於 Wavelength 區域中包含子網路的 VPC。電信業者閘道提供您的 Wavelength 區域與電信運營商還有電信運營商網路上之裝置間的連線。電信業者閘道會從指派給網路邊界群組的集區執行 Wavelength 執行個體的 IP 位址的 NAT 到電信業者 IP 位址。電信業者閘道 NAT 功能類似於網際網路閘道在區域中的運作方式。

## 啟用電信運營商網路存取

若要針對 Wavelength 子網路中執行個體啟用網路存取或從電信運營商網路存取，您必須執行下列動作：

- 建立 VPC。
- 建立電信業者閘道，並將電信業者閘道連接到您的 VPC。建立電信業者閘道時，您可以選擇選擇哪些子網路要路由傳送至電信業者閘道。當您選取此選項時，我們會自動建立與電信業者閘道相關的資源，例如路由表和網路 ACL。如果您未選擇此選項，則必須執行下列工作：
  - 選取將流量路由傳送至電信業者閘道的子網路。
  - 確定您的子網路路由表具有將流量導向電信業者閘道的路由。
  - 確保子網路中的執行個體具有全域唯一的電信業者 IP 位址。
  - 確定您的網路存取控制清單和安全群組規則允許相關流量流向和流出您的執行個體。

## 使用電信業者閘道

以下各節說明如何為 VPC 手動建立電信業者閘道，以支援來自電信業者網路 (例如行動電話) 的入埠流量，以及支援流動電信業者網路和網際網路的出埠流量。

### 任務

- [建立 VPC](#) (p. 221)
- [建立電信業者閘道](#) (p. 222)
- [建立安全群組以存取電信運營商網路](#) (p. 223)
- [步驟 2：在 Wavelength 區域子網路中分配電信業者 IP 地址並將其與執行個體關聯](#) (p. 224)
- [檢視電信業者閘道詳細資料](#) (p. 225)
- [管理電信業者閘道標籤](#) (p. 225)
- [刪除電信業者閘道](#) (p. 225)

## 建立 VPC

您可以使用 Amazon VPC 主控台建立空白的 Wavelength VPC，或 AWS CLI。

### Amazon VPC console

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)、Create VPC (建立 VPC)。
3. 視需要指定下列 VPC 詳細資訊，然後選擇建立。
  - Name tag (名稱標籤)：選擇性提供您 VPC 的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
  - IPv4 CIDR block (IPv4 CIDR 區塊)：指定 VPC 的 IPv4 CIDR 區塊。我們建議您從 [RFC 1918](#) 中指定的私有 (非可公開路由) IP 地址範圍指定 CIDR 區塊；例如，10.0.0.0/16 或 192.168.0.0/16。

#### Note

您可以指定公開可路由傳送的 IPv4 位址範圍。但是，我們目前不支援從 VPC 中公開可路由傳送的 CIDR 區塊直接存取網際網路。若使用介於 224.0.0.0 和 255.255.255.255 之間 (類別 D 和類別 E IP 地址範圍) 的範圍在 VPC 中啟動，則 Windows 執行個體將無法正常開機。

## AWS CLI

### 建立 VPC

- 請使用 `create-vpc`。若要取得更多資訊，請參閱 AWS CLI Command Reference 中的 [create-vpc](#)。

## 建立電信業者閘道

建立 VPC 之後，請建立電信業者閘道，然後選取將流量路由至電信業者閘道的子網路。

如果您尚未選擇加入 Wavelength 區域，則 Amazon VPC 主控台 會提示您加入。如需詳細資訊，請參閱 [the section called “管理區域” \(p. 226\)](#)。

當您選擇將流量從子網路自動路由傳送至電信業者閘道時，我們會建立下列資源：

- 電信業者閘道
- 子網路。您可以選擇性地將沒有 Name 金鑰值的所有電信業者閘道標籤指派給子網路。
- 具有下列資源的網路 ACL：
  - 與 Wavelength 區域中的子網路相關聯的子網路
  - 所有流量的預設輸入和輸出規則。
- 具有以下資源的路由表：
  - 適用於所有本機流量的路由
  - 將所有非本機流量路由至電信業者閘道的路由
  - 與子網路的關聯

## Amazon VPC console

### 建立電信業者閘道

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在瀏覽窗格中，選擇電信業者閘道，然後選擇建立電信業者閘道。
3. 選用性：在名稱中，輸入電信業者閘道的名稱。
4. 對於 VPC，請選擇 VPC。
5. 選擇將子網路流量路由傳送到電信業者閘道，然後在要路由傳送的子網路下進行下列動作。

- a. 在 Wavelength 區域中的現有子網路下，選取每個 Wavelength 子網路以路由傳送至電信業者閘道的方塊。
- b. 若要在 Wavelength 區域中建立子網路，請選擇新增子網路，指定下列資訊，然後選擇新增子網路：
  - 名稱標籤：選擇性提供您子網路的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
  - VPC：選擇 VPC。
  - 可用區域：選擇 Wavelength 區域。
  - IPv4 CIDR 區塊：指定您子網路的 IPv4 CIDR 區塊，例如：10.0.1.0/24。
  - 若要將電信業者閘道標籤套用至子網路，請選取從這個電信業者閘道套用相同的標籤。
6. (選用) 若要將標籤新增至電信業者閘道，請選擇新增標籤，然後執行下列動作：
  - 對於 Key (金鑰)，輸入金鑰名稱。
  - 對於 Value (值)，進入金鑰值。
7. 選擇建立電信業者閘道。

## AWS CLI

### 建立電信業者閘道

- 請使用 `create-carrier-gateway`。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [create-carrier-gateway](#)。

建立電信業者閘道後，請使用下列資源新增 VPC 路由表：

- 適用於所有 VPC 本機流量的路由
- 將所有非本機流量路由至電信業者閘道的路由
- 與 Wavelength 區域中子網路的關聯

如需更多詳細資訊，請參閱 [the section called “路由傳送至 Wavelength 區域電信業者閘道” \(p. 192\)](#) 及 [the section called “使用路由表” \(p. 197\)](#)。

## 建立安全群組以存取 電信運營商 網路

依預設，VPC 安全群組允許所有傳出流量。您可以建立新的安全群組，並新增允許來自 電信運營商 之傳入流量的規則。然後，將安全群組與子網路中的執行個體產生關聯。

### Amazon VPC console

#### 建立新的安全群組並與您的執行個體建立關聯

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)，然後選擇 Create Security Group (建立安全群組)。
3. 若要建立安全群組，請選擇建立安全群組，指定下列資訊，然後選擇建立：
  - 安全群組名稱：輸入子網路的名稱。
  - 描述：輸入安全群組描述。
  - VPC：選擇 VPC。
4. 選取安全群組。詳細資訊窗格會顯示安全群組的詳細資訊，以及使用其傳入規則和傳出規則的標籤。

5. 在 Inbound Rules (傳入規則) 標籤上，選擇 Edit (編輯)。選擇 Add Rule (新增規則)，然後完成必要資訊。例如，從 Type (類型) 清單選取 HTTP 或 HTTPS，然後將 Source (來源) 輸入為 0.0.0.0/0 (適用於 IPv4 流量) 或 ::/0 (適用於 IPv6 流量)。選擇 Save (儲存)。
6. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
7. 在導覽窗格中，選擇執行個體。
8. 選取執行個體，選擇動作和聯網，然後選取變更安全群組。
9. 清除目前選取的安全群組的核取方塊，然後選取新的安全群組。選擇 Assign Security Groups (指派安全群組)。

## AWS CLI

### 建立安全群組

- 請使用 `create-security-group`。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [create-security-group](#)。

## 步驟 2：在 Wavelength 區域子網路中分配電信業者 IP 地址並將其與執行個體關聯

如果您使用 Amazon EC2 主控台來啟動執行個體，或者您未使用 AWS CLI 中的 `associate-carrier-ip-address` 選項，則必須配置 Carrier IP 位址並將其指派給執行個體：

### 配置並建立與電信業者 IP 位址的關聯

1. 使用 `allocate-address` 配置電信業者 IP 位址。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [allocate-address](#)。

#### 範例

```
aws ec2 allocate-address --region us-east-1 --domain vpc --network-border-group us-east-1-wl1-bos-wlz-1
```

#### 輸出

```
{
  "AllocationId": "eipalloc-05807b62acEXAMPLE",
  "PublicIpv4Pool": "amazon",
  "NetworkBorderGroup": "us-east-1-wl1-bos-wlz-1",
  "Domain": "vpc",
  "CarrierIp": "155.146.10.111"
}
```

2. 使用 `associate-address` 將電信業者 IP 位址與 EC2 執行個體建立關聯。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [associate-address](#)。

#### 範例

```
aws ec2 associate-address --allocation-id eipalloc-05807b62acEXAMPLE --network-interface-id eni-1a2b3c4d
```

#### 輸出

```
{
```

```
"AssociationId": "eipassoc-02463d08ceEXAMPLE",  
}
```

## 檢視電信業者閘道詳細資料

您可以檢視電信業者閘道的相關資訊，包括州和標籤。

Amazon VPC console

檢視電信業者閘道詳細資料

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇客戶閘道。
3. 選取電信業者閘道，然後依序選擇動作、檢視詳細資料。

AWS CLI

檢視電信業者閘道詳細資料

- 請使用 `describe-carrier-gateways`。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [describe-carrier-gateways](#)。

## 管理電信業者閘道標籤

標籤可協助您識別電信業者閘道。您可以新增或移除標籤。

Amazon VPC console

管理電信業者閘道標籤

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇客戶閘道。
3. 選取電信業者閘道，然後依序選擇動作、管理標籤。
4. 若要新增標籤，請選擇新增標籤，然後執行下列動作：
  - 對於 Key (金鑰)，輸入金鑰名稱。
  - 對於 Value (值)，進入金鑰值。
5. 若要移除標籤，請選擇標籤的「金鑰」和「值」右側的移除。
6. 選擇儲存。

AWS CLI

管理電信業者閘道標籤

- 若要建立標籤，請使用 `create-tag`。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [create-tag](#)。

若要刪除標籤，請使用 `delete-tags`。如需詳細資訊，請參閱 AWS CLI Command Reference 中的 [delete-tags](#)。

## 刪除電信業者閘道

若您不再需要 NAT 閘道，您可以予以刪除。

### Important

如果您沒有刪除以電信業者閘道作為目標, 的路由, 則路由為黑洞路由。

#### Amazon VPC console

##### 刪除電信業者閘道

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中, 選擇客戶閘道。
3. 選取電信業者閘道, 然後選擇動作、刪除電信業者閘道。
4. 在刪除電信業者閘道對話方塊中, 輸入刪除, 然後選擇刪除。

#### AWS CLI

##### 刪除電信業者閘道

- 請使用 `delete-carrier-gateway`。如需詳細資訊, 請參閱 AWS CLI Command Reference 中的 [delete-carrier-gateway](#)。

## 管理區域

在為資源或服務指定 Wavelength 區域之前, 必須選擇加入該區域。

在選擇加入之前, 您需要請求存取權才能使用 Wavelength 區域。有關如何請求 Wavelength 區域存取的資訊, 請參閱 [AWS Wavelength](#)。

## NAT

您可以使用 NAT 裝置來使私有子網路中的執行個體連線到網際網路 (例如進行軟體更新) 或其他 AWS 服務, 但防止網際網路初始化與執行個體的連線。NAT 裝置會將流量從私有子網路中的執行個體轉送至網際網路或其他 AWS 服務, 然後將回應送回執行個體。當流量傳向網際網路時, 來源 IPv4 地址會替換為 NAT 裝置的地址; 同樣, 當回應流量傳向這些執行個體時, NAT 裝置會將地址轉換為這些執行個體的私有 IPv4 地址。

NAT 裝置不支援 IPv6 流量, 請改用僅限傳出的網際網路閘道。如需詳細資訊, 請參閱 [輸出限定網際網路閘道 \(p. 218\)](#)。

### Note

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)。

AWS 提供兩種 NAT 裝置 — 「NAT 閘道」和「NAT 執行個體」。建議您使用 NAT 閘道, 因為相較於 NAT 執行個體, NAT 閘道可提供較佳的可用性和頻寬。NAT 閘道服務也是一種受管服務, 不需要您管理。NAT 執行個體從 NAT AMI 啟動。您可以選擇將 NAT 執行個體用於特別用途。

- [NAT 閘道 \(p. 226\)](#)
- [NAT 執行個體 \(p. 243\)](#)
- [NAT 執行個體和 NAT 閘道的比較 \(p. 250\)](#)

## NAT 閘道

您可以使用網路位址轉譯 (NAT) 閘道讓私有子網路中的執行個體連線至網際網路或其他 AWS 服務, 但防止網際網路啟動與這些執行個體的連線。如需 NAT 的詳細資訊, 請參閱「[NAT \(p. 226\)](#)」。

您將需要為您帳戶中建立及使用的 NAT 閘道支付費用。適用的費率為 NAT 閘道的每小時用量率及資料處理率。同時也適用 Amazon EC2 資料傳輸費。如需詳細資訊，請參閱 [Amazon VPC 定價](#)。

NAT 閘道不支援 IPv6 流量 — 請改用傳出限定 (僅限輸出) 的網際網路閘道。如需詳細資訊，請參閱「[輸出限定網際網路閘道 \(p. 218\)](#)」。

#### 內容

- [NAT 閘道基本概念 \(p. 227\)](#)
- [使用 NAT 閘道 \(p. 229\)](#)
- [控制 NAT 閘道的使用方式 \(p. 232\)](#)
- [為 NAT 閘道加上標籤 \(p. 232\)](#)
- [API 和 CLI 概觀 \(p. 232\)](#)
- [使用 Amazon CloudWatch 監控 NAT 閘道 \(p. 233\)](#)
- [為 NAT 閘道進行疑難排解 \(p. 237\)](#)

## NAT 閘道基本概念

若要建立 NAT 閘道，您必須指定 NAT 閘道所在的公有子網路。如需公有與私有子網路的詳細資訊，請參閱 [子網路路由 \(p. 81\)](#)。您也必須在建立時指定要與 NAT 閘道建立關聯的 [彈性 IP 地址 \(p. 260\)](#)。彈性 IP 地址與 NAT 閘道相關聯後即無法更改。在您建立 NAT 閘道之後，您必須更新與您一或多個私有子網路關聯的路由表，將網際網路的流量指向 NAT 閘道。這可讓您私有子網路中的執行個體與網際網路通訊。

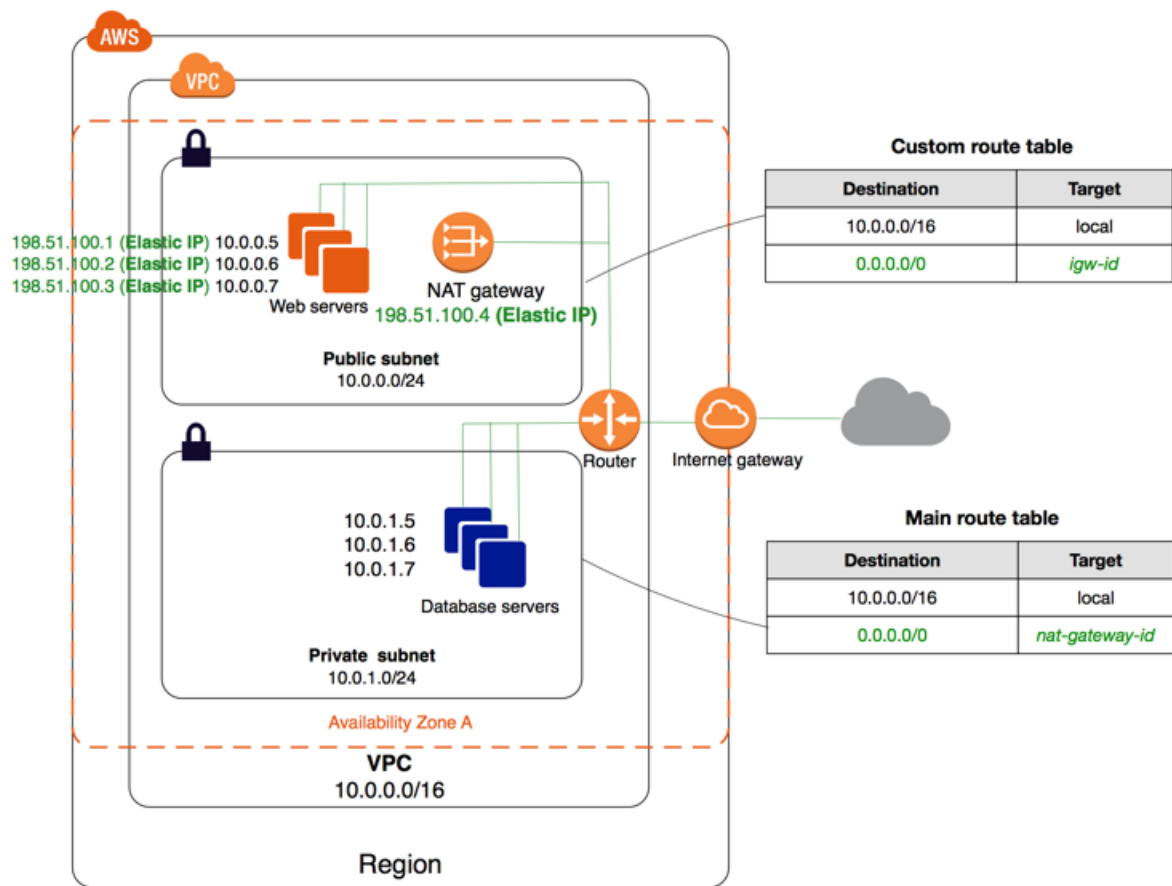
每個 NAT 閘道都是在特定的可用區域內建立，並且使用該區域中的備援實作。您能夠在可用區域中建立的 NAT 閘道數量具有配額。如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。

#### Note

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。若要建立獨立於可用區域外的架構，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。

若您不再需要 NAT 閘道，您可以予以刪除。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。

下圖說明具備 NAT 閘道的 VPC 架構。主路由表會將來自私有子網路中執行個體的網際網路流量傳送至 NAT 閘道。NAT 閘道會使用 NAT 閘道的彈性 IP 地址做為來源 IP 地址，將流量傳送到網際網路閘道。



## NAT 閘道規則與限制

NAT 閘道具有以下特性及限制：

- NAT 閘道支援 5 Gbps 的頻寬，並可自動擴展至 45 Gbps。若您需要更多頻寬，您可以透過將您的資源分割到多個子網路，並在每個子網路中建立 NAT 閘道，來分散工作負載。
- 您僅能將一個彈性 IP 地址與一個 NAT 閘道建立關聯。您無法在建立 NAT 閘道之後取消與彈性 IP 地址的關聯。若要針對您的 NAT 閘道使用不同的彈性 IP 地址，您必須使用需要的地址建立新的 NAT 閘道、更新您的路由表，然後刪除現有的 NAT 閘道 (若不再需要的話)。
- NAT 閘道支援以下通訊協定：TCP、UDP 和 ICMP。
- 您無法建立安全群組與 NAT 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 控制流入及流出 NAT 閘道所在之子網路的流量。網路 ACL 適用於 NAT 閘道的流量。NAT 閘道使用連接埠 1024–65535。如需詳細資訊，請參閱 [網路 ACL \(p. 146\)](#)。
- 當建立 NAT 閘道時，它會接收到從您子網路 IP 地址範圍獲得自動指派私有 IP 地址的網路介面。您可以在 Amazon EC2 主控台中檢視 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。
- NAT 閘道無法由與您 VPC 關聯的 ClassicLink 連線存取。
- 您無法透過 VPC 互連連線、Site-to-Site VPN 連接或 AWS Direct Connect 將流量路由至 NAT 閘道。NAT 閘道無法由這些連線另一端的資源使用。
- NAT 閘道可支援最多 55,000 個連至每個唯一目標的同時連線。若您每秒建立大約 900 個連至單一目標的連線 (即每分鐘約 55,000 個連線)，也適用此限制。若目標 IP 地址、目標連接埠，或是通訊協定 (TCP/UDP/ICMP) 發生變更，您可以建立額外 55,000 個連線。針對超過 55,000 個連線的情況，因連接埠配置



錯誤而產生連線錯誤的機率可能會提升。這些錯誤可透過檢視您 NAT 閘道的 `ErrorPortAllocation` CloudWatch 指標來監控。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控 NAT 閘道 \(p. 233\)](#)。

## 從 NAT 執行個體遷移

若您已在使用 NAT 執行個體，您可以使用 NAT 閘道予以取代。若要執行此作業，您可以在相同子網路中建立 NAT 閘道做為您的 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，您必須先取消與您 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。

### Note

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)。

## 傳送流量到相同區域中的 Amazon S3 或 DynamoDB 的最佳實務

為避免在存取位於相同區域的 Amazon S3 與 DynamoDB 時發生 NAT 閘道的資料處理費用，請設定閘道端點並將流量經由閘道端點路由，而非經由 NAT 閘道。使用閘道端點不需付費。如需詳細資訊，請參閱[閘道 VPC 端點 \(p. 279\)](#)。

## 使用 NAT 閘道

您可以使用 Amazon VPC 主控台來建立、檢視及刪除 NAT 閘道。您也可以使用 Amazon VPC 精靈來建立具有公有子網路、私有子網路，以及 NAT 閘道的 VPC。如需詳細資訊，請參閱[具有公有和私有子網路 \(NAT\) 的 VPC \(p. 24\)](#)。

### 工作

- [正在建立 NAT 閘道 \(p. 229\)](#)
- [正在更新路由表 \(p. 230\)](#)
- [刪除 NAT 閘道 \(p. 230\)](#)
- [測試 NAT 閘道 \(p. 230\)](#)

## 正在建立 NAT 閘道

若要建立 NAT 閘道，您必須指定子網路及彈性 IP 地址。確認彈性 IP 地址目前並未與執行個體或網路界面建立關聯。若您要從 NAT 執行個體遷移至 NAT 閘道，並希望一樣使用 NAT 執行個體的彈性 IP 地址，您必須先取消 NAT 執行個體與地址的關聯。

### 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 Gateways (NAT 閘道)、Create NAT Gateway (建立 NAT 閘道)。
3. 指定要建立 NAT 閘道的子網路，然後選取要和 NAT 閘道建立關聯的彈性 IP 地址配置 ID。
4. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

5. 選擇 建立 NAT 閘道。
6. NAT 閘道會顯示於主控台中。稍待片刻之後，其狀態會變更為 Available，表示準備好供您使用。

若 NAT 閘道的狀態變更為 `Failed` 狀態，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 \(p. 237\)](#)」。

## 正在更新路由表

在您建立 NAT 閘道之後，您必須更新您私有子網路的路由表，使其將網際網路流量指向 NAT 閘道。我們會使用最具體且符合流量的路由，從而判斷如何路由流量 (最長的字首相符)。如需詳細資訊，請參閱 [路由優先順序 \(p. 189\)](#)。

### 建立 NAT 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)。
3. 選取與您私有子網路關聯的路由表，然後選擇 Routes (路由)、Edit (編輯)。
4. 選擇 Add another route (新增其他路由)。針對 Destination (目標)，輸入 `0.0.0.0/0`。針對 Target (目標)，選取您 NAT 閘道的 ID。

#### Note

若您要從使用 NAT 執行個體遷移，可以使用指向 NAT 閘道的路由取代指向 NAT 執行個體的現有路由。

5. 選擇 Save (儲存)。

若要確保您的 NAT 閘道可存取網際網路，與您 NAT 閘道所在之子網路關聯的路由表必須包含將網際網路流量指向網際網路閘道的路由。如需詳細資訊，請參閱 [建立自訂路由表 \(p. 215\)](#)。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。如需詳細資訊，請參閱 [從路由表新增和移除路由 \(p. 199\)](#)。

## 刪除 NAT 閘道

您可以使用 Amazon VPC 主控台刪除 NAT 閘道。在您刪除 NAT 閘道之後，其項目仍會在 Amazon VPC 主控台中顯示一小段時間 (通常是一個小時)，之後便會自動移除。您無法自行移除此項目。

### 刪除 NAT 閘道

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，然後選擇 Actions (動作)、Delete NAT Gateway (刪除 NAT 閘道)。
4. 在確認對話方塊中，選擇 Delete NAT Gateway (刪除 NAT 閘道)。
5. 如果您不再需要與 NAT 閘道相關聯的彈性 IP 位址，建議您將其釋出。如需更多詳細資訊，請參閱 [釋放彈性 IP 地址 \(p. 263\)](#)。

## 測試 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路中的執行個體 ping 網際網路上的幾個遠端位址，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 \(p. 231\)](#)。

若您可以連線到網際網路，您也可以執行下列測試來判斷網際網路流量是否已透過 NAT 閘道路由：

- 您可以從私有子網路中的執行個體追蹤流量的路由。若要執行此作業，請從您私有子網路中的 Linux 執行個體執行 `traceroute` 命令。在輸出中，您會在其中一個躍點看見 NAT 閘道的私有 IP 地址 (通常是第一個躍點)。
- 在您從私有子網路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 地址應為您 NAT 閘道的彈性 IP 地址。您可以透過在 Amazon VPC 主控台 NAT Gateways (NAT 閘道) 頁面上檢視其資訊，來取得您 NAT 閘道的彈性 IP 地址及私有 IP 地址。

若先前的測試失敗，請參閱 [為 NAT 閘道進行疑難排解 \(p. 237\)](#)。

### 測試網際網路連線

以下範例會示範您私有子網路中的執行個體可否連線到網際網路的測試方式。

1. 在您的公有子網路中啟動執行個體 (您會用以做為堡壘主機)。如需詳細資訊，請參閱 [在您的子網路中啟動執行個體 \(p. 85\)](#)。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路 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. 在您的私有子網路中啟動執行個體。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路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路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路中的堡壘主機。如需詳細資訊，請參閱 [設定 Linux 或 macOS 的 SSH 代理程式轉送 \(p. 231\)](#) 或 [設定 Windows \(PuTTY\) 的 SSH 代理程式轉送 \(p. 231\)](#)。
4. 從您的堡壘主機連線到您私有子網路中的執行個體，然後從您私有子網路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 \(p. 231\)](#)。

### 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份驗證代理程式。

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路中的執行個體，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 (PuTTY) 的 SSH 代理程式轉送

1. 如果您尚未安裝 Pageant，請至 [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 Linux 執行個體的 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 地址連線到您公有子網路中的執行個體。如需詳細資訊，請參閱 [連接至 Linux 執行個體](#)。在 Auth (身份驗證) 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 (身份驗證的私有金鑰檔案) 方塊維持空白。

### 測試網際網路連線

1. 從您公有子網路中的執行個體，使用其私有 IP 地址連線到您私有子網路中的執行個體，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 \(p. 240\)](#)。

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 Linux 執行個體的 Amazon EC2 使用者指南 中的 [終止您的執行個體](#)。

## 控制 NAT 閘道的使用方式

根據預設，IAM 使用者沒有使用 NAT 閘道的許可。您可以建立 IAM 使用者政策，將建立、描述和刪除 NAT 閘道的許可授予使用者。我們目前不支援任何 `ec2:*NatGateway*` API 操作的資源層級許可。如需 Amazon VPC 的 IAM 政策之詳細資訊，請參閱 [Amazon VPC 的 Identity and Access Management \(p. 123\)](#)。

## 為 NAT 閘道加上標籤

您可為您的 NAT 閘道新增標籤，以利您根據組織需求識別或分類。如需使用標籤的資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [為您的 Amazon EC2 資源加上標記](#)。

NAT 閘道支援成本分配標籤。因此，您也可以使用標籤整理您的 AWS 帳單，並反映您自己的成本結構。如需詳細資訊，請參閱 AWS Billing and Cost Management 使用者指南 中的 [使用成本分配標籤](#)。如需使用標籤設定成本配置報告的詳細資訊，請參閱關於 AWS 帳戶帳單中的 [每月成本配置報告](#)。

## 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 操作清單，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

### 建立 NAT 閘道

- [create-nat-gateway](#) (AWS CLI)
- [New-EC2NatGateway](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateNatGateway](#) (Amazon EC2 查詢 API)

### 為 NAT 閘道新增標籤

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateTags](#) (Amazon EC2 查詢 API)

### 描述 NAT 閘道

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (適用於 Windows PowerShell 的 AWS 工具)

- [DescribeNatGateways](#) (Amazon EC2 查詢 API)

#### 刪除 NAT 閘道

- [delete-nat-gateway](#) (AWS CLI)
- [Remove-EC2NatGateway](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DeleteNatGateway](#) (Amazon EC2 查詢 API)

## 使用 Amazon CloudWatch 監控 NAT 閘道

您可以使用 CloudWatch 監控 NAT 閘道以收集來自 NAT 閘道的原始資料，並處理為可讀且近乎即時的指標。您可以使用此資訊來監控 NAT 閘道並進行故障診斷。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。

如需 Amazon CloudWatch 的詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。如需定價的詳細資訊，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。

指標	描述
<code>ActiveConnectionCount</code>	通過 NAT 閘道的並行作用中 TCP 連線的總數。  0 值表示沒有作用中連線通過 NAT 閘道。  單位：計數  統計資訊：最實用的統計資訊是 Max。
<code>BytesInFromDestination</code>	NAT 閘道接收到來自目的地的位元組數量。  如果 <code>BytesOutToSource</code> 的值小於 <code>BytesInFromDestination</code> 的值，可能有資料在 NAT 閘道處理期間流失，或有流量被 NAT 閘道主動封鎖。  單位：位元組  統計資訊：最實用的統計資訊是 Sum。
<code>BytesInFromSource</code>	NAT 閘道接收到來自您的 VPC 中的用戶端的位元組數量。  如果 <code>BytesOutToDestination</code> 的值小於 <code>BytesInFromSource</code> 的值，可能有資料在 NAT 閘道處理期間流失。  單位：位元組  統計資訊：最實用的統計資訊是 Sum。
<code>BytesOutToDestination</code>	透過 NAT 閘道送出至目的地的位元組數量。  大於 0 的值表示，有流量從 NAT 閘道之後的用戶端流出至網際網路。如果 <code>BytesOutToDestination</code>

指標	描述
	<p>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>
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>大於 0 的值可能表示，目前 NAT 閘道發生暫時性的問題。如果此值偏高，請參閱「<a href="#">AWS 服務運作狀態儀表板</a>」。</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>
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>



指標	描述
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>

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 閘道指標每間隔 1 分鐘傳送至 CloudWatch。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

指標會先依服務命名空間分組，再依各命名空間內不同的維度組合分類。

1. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇指標。
3. 在 All metrics (所有指標) 下，選擇 NAT gateway (NAT 閘道) 指標命名空間。
4. 若要檢視指標，請選取指標維度。

若要使用 AWS CLI 來檢視指標

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 警示來監控 NAT 閘道

您可以建立 CloudWatch 警示，其在警示變更狀態時傳送 Amazon SNS 訊息。警示會在您指定的期間監看單一指標。警示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. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Alarms (警示)、Create Alarm (建立警示)。
3. 選擇 NAT gateway (NAT 閘道)。

4. 選取 NAT 閘道和 BytesOutToDestination 指標，然後選擇 Next (下一步)。
5. 依如下所述設定警示，完成後選擇 Create Alarm (建立警示)：
  - 在 Alarm Threshold (警示閾值) 下，輸入警示的名稱和說明。針對 Whenever (每當)，選擇  $\geq$  並輸入 5000000。連續期間數輸入 1。
  - 在 Actions (動作) 下選取現有的通知清單，或選擇 New list (新增清單) 建立新的清單。
  - 在 Alarm Preview (警示預覽) 下，選取 15 分鐘期間，並指定 Sum (總和) 的統計資料。

您可以建立警示來監控 ErrorPortAllocation 指標，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. 前往 <https://console.aws.amazon.com/cloudwatch/>，開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Alarms (警示)、Create Alarm (建立警示)。
3. 選擇 NAT Gateway (NAT 閘道)。
4. 選取 NAT 閘道和 ErrorPortAllocation 指標，然後選擇 Next (下一步)。
5. 依如下所述設定警示，完成後選擇 Create Alarm (建立警示)：
  - 在 Alarm Threshold (警示閾值) 下，輸入警示的名稱和說明。針對 Whenever (每當)，選擇  $>$  並輸入 0。連續期間數輸入 3。
  - 在 Actions (動作) 下選取現有的通知清單，或選擇 New list (新增清單) 建立新的清單。
  - 在 Alarm Preview (警示預覽) 下，選取 5 分鐘期間，並指定 Maximum (最大) 的統計資料。

如需更多關於建立警示的範例，請參閱 Amazon CloudWatch 使用者指南 中的 [建立 Amazon CloudWatch 警示](#)。

## 為 NAT 閘道進行疑難排解

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 \(p. 237\)](#)
- [彈性 IP 地址和 NAT 閘道配額 \(p. 238\)](#)
- [不支援此可用區域 \(p. 239\)](#)
- [NAT 閘道無法顯示 \(p. 239\)](#)
- [NAT 閘道沒有回應 ping 命令 \(p. 239\)](#)
- [執行個體無法存取網路 \(p. 240\)](#)
- [TCP 連線到目標失敗 \(p. 241\)](#)
- [Traceroute 輸出沒有顯示 NAT 閘道私有 IP 地址 \(p. 241\)](#)
- [網際網路連線在 350 秒之後卸除 \(p. 242\)](#)
- [無法建立 IPsec 連線 \(p. 242\)](#)
- [無法初始化更多的連線 \(p. 242\)](#)

## NAT 閘道建立失敗

#### 問題

您建立 NAT 閘道並進入 Failed 狀態。

#### 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，請到 Amazon VPC 主控台，然後選擇 NAT Gateways (NAT 閘道) 選取您的 NAT 閘道，然後在詳細窗格中 狀態 訊息欄位檢視錯誤訊息。

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。

#### Note

失敗的 NAT 閘道會自動在一小段時間後刪除 (通常是一個小時)。

顯示的錯誤	原因	解決方案
子網路擁有的可用地址數不足以建立此 NAT 閘道	您指定的子網路中沒有任何可用的私有 IP 地址。NAT 閘道需要網路界面具備從子網路的範圍配置的私有 IP 地址。	透過 Amazon VPC 主控台的 子網路 頁面檢查您的子網路中有多少可用的 IP 地址。您可以在詳細窗格中檢視子網路的 可用的 IPs。若要在您的子網路中建立可用的 IP 地址，您可以刪除未使用的網路界面，或是終止您不再需要的執行個體。
網路 vpc-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。如需詳細資訊，請參閱 <a href="#">建立並連接網際網路閘道 (p. 215)</a> 。
彈性 IP 地址 eipalloc-xxxxxxx 無法與此 NAT 閘道建立關聯	您指定的彈性 IP 地址不存在或找不到。	請檢查彈性 IP 地址的配置 ID，確認您已輸入正確。確認您指定的彈性 IP 地址位於您建立 NAT 閘道的相同的 AWS 區域內。
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 IPs 頁面，檢視執行個體 ID 或網路介面 ID 指定的值。若您不需要針對該資源使用彈性 IP 地址，您可以取消其關聯。或者，將新的彈性 IP 地址配置到您的帳戶。如需詳細資訊，請參閱 <a href="#">使用彈性 IP 地址 (p. 261)</a> 。
此 NAT 閘道建立並在內部使用的網路界面 eni-xxxxxxx 處於無效狀態。請再試一次。	在建立或使用 NAT 閘道的網路界面時發生問題。	您無法解決此錯誤。請嘗試再次建立 NAT 閘道。

## 彈性 IP 地址和 NAT 閘道配額

#### 問題

當您嘗試配置彈性 IP 地址時，得到下列錯誤。

```
The maximum number of addresses has been reached.
```

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

有兩項可能原因：

- 您已達到該區域帳戶彈性 IP 地址的數量配額。
- 您已達到該可用區域帳戶 NAT 閘道的數量配額。

#### 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 [Amazon VPC 限制表單](#) 請求提高配額。

如果您已達 NAT 閘道配額，您可以執行以下任一作業：

- 使用 [Amazon VPC 限制表單](#) 請求提高配額。每個可用區域都會強制套用 NAT 閘道配額。
- 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。

如需更多詳細資訊，請參閱 [Amazon VPC 配額 \(p. 320\)](#)。

## 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。您可以在另一個可用區域中建立 NAT 閘道，並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

在您建立 NAT 閘道時可能發生錯誤，導致其失敗。您可以在 Amazon VPC 主控台中短時間內看見狀態為 Failed 的 NAT 閘道 (通常為一小時)。在一小時後，會自動刪除。

#### 解決方案

請檢閱 [NAT 閘道建立失敗 \(p. 237\)](#) 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 NAT 閘道 \(p. 230\)](#)。

### 執行個體無法存取網路

#### 問題

您已建立 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人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 Gateways (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 \(p. 237\)](#)。
- 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。如需詳細資訊，請參閱 [建立自訂路由表 \(p. 215\)](#)。
  - 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。如需詳細資訊，請參閱 [正在更新路由表 \(p. 230\)](#)。
  - 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。

#### Note

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。

#### Note

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。如需更多詳細資訊，請參閱 [VPC 流程日誌 \(p. 158\)](#)。

- 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 閘道目前不支援 TCP 或 ICMP 的 IP 分段。如需更多詳細資訊，請參閱 [NAT 執行個體和 NAT 閘道的比較 \(p. 250\)](#)。
- `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：

- 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。
- 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。

#### Note

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。

- 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：

- 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。

- 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。

### 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 TPC 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 閘道現存的連線至目標，但無法建立更多連線。

### 原因

您可能已達單一 NAT 閘道同時連線的上限。如需更多詳細資訊，請參閱 [NAT 閘道規則與限制 \(p. 228\)](#)。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

請執行下列其中一項：

- 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 \(p. 233\)](#) 指標來監控閒置連線的增量。關閉閒置連線已釋出容量。



## NAT 執行個體

您可在您的 VPC 中使用公有子網路的網路地址轉譯 (NAT) 執行個體，讓私有子網路的執行個體初始化傳出 IPv4 流量至網際網路或其他 AWS 服務，但防止執行個體接收他人在網際網路起始的傳入流量。

如需公有與私有子網路的詳細資訊，請參閱 [子網路路由 \(p. 81\)](#)。如需 NAT 的詳細資訊，請參閱「[NAT \(p. 226\)](#)」。

NAT 不支援 IPv6 流量—請改用僅限傳出的網際網路閘道。如需詳細資訊，請參閱「[輸出限定網際網路閘道 \(p. 218\)](#)」。

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 [EC2 常見問答集](#)。

### Note

您也可以使用 NAT 閘道，它是可提供更佳可用性、更高頻寬，卻減輕管理負擔的受管 NAT 服務。如需常用案例，建議您使用 NAT 閘道而非 NAT 執行個體。如需更多詳細資訊，請參閱 [NAT 閘道 \(p. 226\)](#) 及 [NAT 執行個體和 NAT 閘道的比較 \(p. 250\)](#)。

### 內容

- [NAT 執行個體基本概念 \(p. 243\)](#)
- [NAT 執行個體 AMI \(p. 244\)](#)
- [設定 NAT 執行個體 \(p. 245\)](#)
- [建立 NATSG 安全群組 \(p. 246\)](#)
- [停用來源/目標檢查 \(p. 247\)](#)
- [更新主路由表 \(p. 248\)](#)
- [測試 NAT 執行個體組態 \(p. 248\)](#)

## NAT 執行個體基本概念

下圖說明 NAT 執行個體基本概念。主路由表與私有子網路相關聯，將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到 VPC 的網際網路閘道。流量在於 NAT 執行個體的彈性 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。

來自私有子網路中執行個體的網際網路流量會路由至 NAT 執行個體，然後再與網際網路通訊。因此，NAT 執行個體必須具有網際網路存取權。它必須位於公用子網路 (具有路由表且具有通往網際網路閘道的子網路) 中，且必須具有公用 IP 位址或彈性 IP 位址。



或者，您可以使用 AWS CLI。使用 `describe-images` 命令，並使用篩選器僅傳回 Amazon 擁有且名稱中包含 `amzn-ami-vpc-nat-2018.03` 字串之 AMI 的結果。下列範例使用 `--query` 參數，在輸出中僅顯示 AMI ID、名稱和建立日期，以協助您快速識別最新的 AMI。

```
aws ec2 describe-images --filter Name="owner-alias",Values="amazon" --
filter Name="name",Values="amzn-ami-vpc-nat-2018.03*" --query "Images[*].
[ImageId,Name,CreationDate]"
```

## 更新您現有的 NAT 執行個體

如果您已經有 NAT 執行個體，請執行下列命令，在執行個體上套用安全更新。

```
sudo yum update --security
```

您也可以使用 AWS Systems Manager 修補程式管理員來自動化安裝安全相關更新的程序。如需詳細資訊，請參閱 AWS Systems Manager 使用者指南中的 [AWS Systems Manager 修補程式管理員](#)。

## 設定 NAT 執行個體

您可使用 VPC 精靈設定具有 NAT 執行個體的 VPC，如需詳細資訊，請參閱 [具有公有和私有子網路 \(NAT\) 的 VPC \(p. 24\)](#)。精靈會為您執行許多設定步驟，包括啟動 NAT 執行個體及設定路由。但若您喜歡，可使用下面的步驟手動建立與設定 VPC 和 NAT 執行個體。

開始之前，請先取得設定為以 NAT 執行個體執行之 AMI 的 ID。如需更多詳細資訊，請參閱 [取得 NAT AMI 的 ID \(p. 244\)](#)。

1. 建立包含兩個子網路的 VPC。

### Note

下面的步驟適用於手動建立與設定 VPC，不適用於使用 VPC 精靈建立 VPC。

- a. 建立 VPC (請參閱 [建立 VPC \(p. 82\)](#))
  - b. 建立兩個子網路 (請參閱 [正在建立子網路 \(p. 214\)](#))
  - c. 將網際網路閘道連接至 VPC (請參閱 [建立並連接網際網路閘道 \(p. 215\)](#))
  - d. 建立將目標 VPC 外部的流量傳送至網際網路閘道的自訂路由表，然後建立它與一個子網路的關聯，使其成為公有子網路 (請參閱 [建立自訂路由表 \(p. 215\)](#))
2. 建立 NATSG 安全群組 (請參閱 [建立 NATSG 安全群組 \(p. 246\)](#))。當您啟動 NAT 執行個體時，會指定此安全群組。
  3. 從已設定執行為 NAT 執行個體的 AMI 中，在您的公有子網路中啟動執行個體。
    - a. 開啟 Amazon EC2 主控台。
    - b. 在儀表板上，選擇 Launch Instance (啟動執行個體) 按鈕，然後如下完成精靈：
      - i. 在 Choose an Amazon Machine Image (AMI) (選擇 Amazon Machine Image (AMI)) 頁面上，選取 Community AMIs (社群 AMI) 分類。在搜尋欄位中，輸入您先前識別的 (p. 244) AMI ID。選擇 Select (選取)。
      - ii. 在 Choose an Instance Type (選擇執行個體類型) 頁面上，選取執行個體類型，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
      - iii. 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Network (網路) 清單選取您建立的 VPC，然後從 Subnet (子網路) 清單選取您的公有子網路。
      - iv. (選用) 選取 Public IP (公有 IP) 核取方塊，請求您的 NAT 執行個體接收公有 IP 地址。如果您選擇現在不指派公有 IP 地址，您可以在您的執行個體啟動後，配置並指派彈性 IP 地址給它。如需在啟動時指派公有 IP 的詳細資訊，請參閱 [在啟動執行個體期間指派公有 IPv4 地址 \(p. 105\)](#)。選擇 Next: Add Storage (下一步：新增儲存體)。

- v. 您可以選擇在執行個體中新增儲存體，並在後續頁面中新增標籤。當完成時，請選擇 Next: Configure Security Group (下一步：設定安全群組)。
  - vi. 在 Configure Security Group (設定安全群組) 頁面上，選取 Select an existing security group (選取現有安全群組) 選項，並選取您建立的 NATSG 安全群組。選擇 Review and Launch (檢閱和啟動)。
  - vii. 檢閱您選擇的設定。進行任何所需的變更，然後選擇 Launch (啟動) 來選擇金鑰對並啟動您的執行個體。
4. (選用) 連線至 NAT 執行個體，執行任何需要的修改，然後建立您專用之設定執行 NAT 執行個體的 AMI。您下次需要啟動 NAT 執行個體時，可使用此 AMI。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [建立 Amazon EBS 後端 AMI](#)。
  5. 停用 NAT 執行個體的 SrcDestCheck 屬性 (請參閱 [停用來源/目標檢查 \(p. 247\)](#))
  6. 如果您不在啟動期間將公有 IP 地址指派給 NAT 執行個體 (步驟 3)，您即需要建立彈性 IP 地址與它的關聯。
    - a. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
    - b. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)，然後選擇 Allocate new address (配置新地址)。
    - c. 選擇 Allocate (配置)。
    - d. 從清單選取彈性 IP 地址，然後選擇 Actions (動作)、Associate address (與地址建立關聯)。
    - e. 選取網路界面資源，然後選取 NAT 執行個體的網路界面。從 Private IP (私有 IP) 清單選取要與彈性 IP 建立關聯的地址，然後選擇 Associate (關聯)。
  7. 更新主路由表，將流量傳送到 NAT 執行個體。如需更多詳細資訊，請參閱 [更新主路由表 \(p. 248\)](#)。

## 使用命令列啟動 NAT 執行個體

使用下列其中一項命令，在您的子網路中啟動 NAT 執行個體。如需更多詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。若要取得設定為以 NAT 執行個體執行之 AMI 的 ID，請參閱 [取得 NAT AMI 的 ID \(p. 244\)](#)。

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (適用於 Windows PowerShell 的 AWS 工具)

## 建立 NATSG 安全群組

如下表所述定義 NATSG 安全群組，讓您的 NAT 執行個體接收來自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。

NATSG：建議的規則

Inbound			
Source	Protocol	Port range	Comments
10.0.1.0/24	TCP	80	允許來自私有子網路伺服器的傳入 HTTP 流量
10.0.1.0/24	TCP	443	允許來自私有子網路伺服器的傳入 HTTPS 流量
您家用網路的公有 IP 地址範圍	TCP	22	允許傳入 SSH 由您的家用網路存取 NAT 執行個體 (透過網際網路閘道)
Outbound			
Destination	Protocol	Port range	Comments

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 NATSG 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 Security Groups (安全群組)，然後選擇 Create Security Group (建立安全群組)。
3. 在 Create Security Group (建立安全群組) 對話方塊中，指定 NATSG 為安全群組的名稱並提供描述。從 VPC 清單選取您 VPC 的 ID，然後選擇 Yes, Create (是，建立)。
4. 選取您剛剛建立的 NATSG 安全群組。詳細資訊窗格會顯示安全群組的詳細資訊，以及操作傳入和傳出規則的標籤。
5. 使用 Inbound Rules (傳入規則) 標籤新增傳入流量的規則，如下所示：
  - a. 選擇 Edit (編輯)。
  - b. 選擇 Add another rule (新增其他規則)，並從 Type (類型) 清單選取 HTTP。在 Source (來源) 欄位中，指定您私有子網路的 IP 地址範圍。
  - c. 選擇 Add another rule (新增其他規則)，並從 Type (類型) 清單選取 HTTPS。在 Source (來源) 欄位中，指定您私有子網路的 IP 地址範圍。
  - d. 選擇 Add another rule (新增其他規則)，並從 Type (類型) 清單選取 SSH。在 Source (來源) 欄位中，指定您網路的公有 IP 地址範圍。
  - e. 選擇 Save (儲存)。
6. 使用 Outbound Rules (傳出規則) 標籤新增傳出流量的規則，如下所示：
  - a. 選擇 Edit (編輯)。
  - b. 選擇 Add another rule (新增其他規則)，並從 Type (類型) 清單選取 HTTP。在 Destination (目標) 欄位中，指定 0.0.0.0/0
  - c. 選擇 Add another rule (新增其他規則)，並從 Type (類型) 清單選取 HTTPS。在 Destination (目標) 欄位中，指定 0.0.0.0/0
  - d. 選擇 Save (儲存)。

如需更多詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。

## 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。

您可以使用主控台或命令列，停用執行中或已停止之 NAT 執行個體的 SrcDestCheck 屬性。

### 使用主控台停用來源/目標檢查

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)。
3. 選取 NAT 執行個體，然後選擇 Actions (動作)、Networking (聯網)、Change Source/Dest.Check (變更來源/目標檢查)。
4. 檢查 NAT 執行個體的此一屬性是否停用。否則，請選擇 Yes, Disable (是，停用)。
5. 如果 NAT 執行個體有輔助網路界面，請從 Description (描述) 標籤的 Network interfaces (網路界面) 中選擇它，然後選擇界面 ID 前往網路界面頁面。選擇 Actions (動作)、Change Source/Dest.Check (變更來源/目標檢查)、停用設定，然後選擇 Save (儲存)。

### 使用命令列停用來源/目標檢查

您可以使用下列其中一個命令。如需詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (適用於 Windows PowerShell 的 AWS 工具)

## 更新主路由表

您 VPC 中的私有子網路與自訂的路由表不相關聯，因此它會使用主路由表。根據預設，主路由表能讓您 VPC 內的執行個體互相通訊。您必須將傳送所有其他子網路流量的路由新增到 NAT 執行個體。

### 更新主路由表

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)。
3. 選取您 VPC 的主路由表 (Main (主要) 欄位會顯示 Yes (是))。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。
4. 在 Routes (路由) 標籤上，選擇 Edit (編輯)，並在 Destination (目標) 方塊中指定 0.0.0.0/0，然後從 Target (目標) 清單選取 NAT 執行個體的執行個體 ID，再選擇 Save (儲存)。
5. 在 Subnet Associations (子網路關聯) 標籤上，選擇 Edit (編輯)，然後選取私有子網路的 Associate (關聯) 核取方塊。選擇 Save (儲存)。

如需更多詳細資訊，請參閱 [路由表 \(p. 184\)](#)。

## 測試 NAT 執行個體組態

在您啟動 NAT 執行個體並完成上述設定步驟後，您就可以執行測試，檢查您私有子網路中的執行個體是否可以將 NAT 執行個體做為堡壘伺服器使用，透過 NAT 執行個體存取網際網路。若要執行此作業，請更新您的 NAT 執行個體安全群組規則，允許傳入和傳出 ICMP 流量以及允許傳出 SSH 流量，在您的私有子網路中啟動執行個體，設定 SSH 代理程式轉送以存取您私有子網路的執行個體，連線到您的執行個體，然後測試網際網路連線。

### 更新您的 NAT 執行個體安全群組

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 尋找與您 NAT 執行個體相關聯的安全群組，然後在 Inbound (傳入) 標籤中選擇 Edit (編輯)。
4. 選擇 Add Rule (新增規則)，然後從 Type (類型) 清單選取 All ICMP - IPv4 (所有 ICMP - IPv4)，從 Source (來源) 清單選取 Custom (自訂)。輸入您私有子網路的 IP 地址範圍，例如 10.0.1.0/24。選擇 Save (儲存)。
5. 在 Outbound (傳出) 標籤中，選擇 Edit (編輯)。
6. 選擇 Add Rule (新增規則)，然後從 Type (類型) 清單選取 SSH，從 Destination (目標) 清單選取 Custom (自訂)。輸入您私有子網路的 IP 地址範圍，例如 10.0.1.0/24。選擇 Save (儲存)。
7. 選擇 Add Rule (新增規則)，然後從 Type (類型) 清單選取 All ICMP - IPv4 (所有 ICMP - IPv4)，從 Destination (目標) 清單選取 Custom (自訂)。輸入 0.0.0.0/0，然後選擇 Save (儲存)。

### 在您的私有子網路中啟動執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Instances (執行個體)。



3. 在您的私有子網路中啟動執行個體。如需詳細資訊，請參閱 [在您的子網路中啟動執行個體 \(p. 85\)](#)。確定在啟動精靈中設定下列選項，然後選擇 Launch (啟動)：
  - 在 Choose an Amazon Machine Image (AMI) (選擇 Amazon Machine Image (AMI)) 頁面上，從 Quick Start (快速入門) 類別選取 Amazon Linux AMI。
  - 在 Configure Instance Details (設定執行個體詳細資訊) 頁面上，從 Subnet (子網路) 清單選取您的私有子網路，不要將公有 IP 地址指派給您的執行個體。
  - 在 Configure Security Group (設定安全群組) 頁面上，確定您的安全群組包含此傳入規則：允許來自您 NAT 執行個體私有 IP 地址或您公有子網路 IP 地址範圍的 SSH 存取，以及確定您有允許傳出 ICMP 流量的傳出規則。
  - 在 Select an existing key pair or create a new key pair (選取現有金鑰對或建立新的金鑰對) 對話方塊中，選取啟動 NAT 執行個體所用的相同金鑰對。

### 設定 Linux 或 OS X 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份驗證代理程式。

若為 Linux，請使用下列命令：

```
ssh-add -c mykeypair.pem
```

OS X 請使用下列命令：

```
ssh-add -K mykeypair.pem
```

2. 使用 -A 選項連線到您的 NAT 執行個體，以啟用 SSH 代理程式轉送，例如：

```
ssh -A ec2-user@54.0.0.123
```

### 設定 Windows (PuTTY) 的 SSH 代理程式轉送

1. 如果您尚未安裝 Pageant，請至 [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 [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 工作階段來連線您的 NAT 執行個體。在 Auth (身份驗證) 類別中，確定選取 Allow agent forwarding (允許代理程式轉送) 選項，將 Private key file for authentication (要身份驗證的私有金鑰檔案) 欄位留白。

### 測試網際網路連線

1. 針對已啟用 ICMP 的網站執行 ping 命令，測試您的 NAT 執行個體能否與網際網路通訊，例如：

```
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=48 time=74.9 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=48 time=75.1 ms  
...
```

按下鍵盤上的 Ctrl+C 取消 ping 命令。



2. 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，例如：

```
ssh ec2-user@10.0.1.123
```

3. 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：

```
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。

如果 ping 命令失敗，請檢查下列資訊：

- 檢查您 NAT 執行個體的安全群組規則，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 執行個體即收不到您私有執行個體的 ping 命令。
  - 確認您已正確設定路由表。如需更多詳細資訊，請參閱 [更新主路由表 \(p. 248\)](#)。
  - 確定已停用您 NAT 執行個體的來源/目標檢查。如需更多詳細資訊，請參閱 [停用來源/目標檢查 \(p. 247\)](#)。
  - 確定您 ping 的是已啟用 ICMP 的網站。若為啟用，您將無法接收到回覆封包。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。
4. (選用) 您可以終止不再需要的私有執行個體。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [終止您的執行個體](#)。

## NAT 執行個體和 NAT 閘道的比較

下列是 NAT 執行個體和 NAT 閘道之間差異的高階摘要。

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	可擴展到 45 Gbps。	取決於執行個體類型的頻寬。
維護	管理者為 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 Amazon Linux AMI。
費用	費用取決於您使用的 NAT 閘道數目、使用持續時間以及您透過 NAT 閘道傳送的資料量。	費用取決於您使用的 NAT 執行個體數目、使用持續時間以及執行個體類型和大小。
類型和大小	統一提供；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 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。

屬性	NAT 閘道	NAT 執行個體
私有 IP 地址	當您建立閘道時，自動從子網路的 IP 地址範圍內選取。	當您啟動執行個體時，從子網路 IP 地址範圍內指派特定的私有 IP 地址。
安全群組	無法與 NAT 閘道建立關聯。您可以將安全群組與 NAT 閘道後的資源建立關聯，以控制傳入和傳出流量。	與您 NAT 執行個體和 NAT 執行個體後的資源相關聯，以控制傳入和傳出流量。
網路 ACL	使用網路 ACL 來控制進出 NAT 閘道所在子網路的流量。	使用網路 ACL 來控制進出 NAT 執行個體所在子網路的流量。
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 (p. 233)</a> 。	檢視執行個體的 CloudWatch 指標。
逾時行為	如果連線逾時，NAT 閘道會對 NAT 閘道後的任何資源傳回 RST 封包來嘗試繼續連線 (不會傳送 FIN 封包)。	如果連線逾時，NAT 執行個體會對 NAT 執行個體後的資源傳送 FIN 封包來關閉連線。
IP 分段	支援轉送 UDP 通訊協定的 IP 分段封包。  不支援 TCP 和 ICMP 通訊協定的分段。這些通訊協定的分段封包會遭刪除。	支援 UDP、TCP 和 ICMP 通訊協定 IP 分段封包的重組。

## DHCP 選項集

動態主機設定通訊協定 (DHCP) 提供在 TCP/IP 網路內傳遞組態資訊到主機的標準協定。DHCP 訊息的 options 欄位包含組態參數，包括網域名稱、網域名稱伺服器和 netbios 節點類型。

您可以為 Virtual Private Cloud (VPC) 設定 DHCP 選項集。

內容

- [DHCP 選項集概觀 \(p. 251\)](#)
- [Amazon DNS 伺服器 \(p. 253\)](#)
- [變更 DHCP 選項 \(p. 253\)](#)
- [使用 DHCP 選項集 \(p. 253\)](#)
- [API 和命令概觀 \(p. 256\)](#)

## DHCP 選項集概觀

依預設，您啟動到非預設 VPC 中的 Amazon EC2 執行個體為私有執行個體。它們並未指派公有 IPv4 地址，除非您在啟動期間特別為其指派公有 IPv4 地址，或修改子網路的公有 IPv4 地址屬性。根據預設，AWS 會為非預設 VPC 中所有執行個體指派無法解析的主機名稱 (例如 ip-10-0-0-202)。您可以為執行個體指定您自己的網域名稱，最多可使用四個您自己的 DNS 伺服器。若要執行此作業，您必須指定特別的 DHCP 選項集以在 VPC 中使用。

下表列出 DHCP 選項集的所有支援選項。您可在 DHCP 選項集中僅指定所需的選項。如需這些選項的詳細資訊，請參閱 [RFC 2132](#)。

DHCP 選項名稱	描述
domain-name-servers	<p>最多四個網域名稱伺服器 (或稱 AmazonProvidedDNS) 的 IP 地址。預設 DHCP 選項集會指定 AmazonProvidedDNS。如果指定超過一個網域名稱伺服器，請使用逗號分隔。您雖然可以指定最多四個網域名稱伺服器，但請注意，某些作業系統可能會限制較低的數量。</p> <p>如果您希望讓執行個體接收在 domain-name 中指定的自訂 DNS 主機名稱，則必須將 domain-name-servers 設定為自訂 DNS 伺服器。</p> <p>若要使用此選項，請將其設定為 AmazonProvidedDNS 或自訂網域名稱伺服器。如果將此選項設定為兩者，結果可能會導致非預期的行為。</p>
domain-name	<p>如果您是在 us-east-1 中使用 AmazonProvidedDNS，請指定 ec2.internal。如果您是在其他區域中使用 AmazonProvidedDNS，請指定 region.compute.internal (例如 ap-northeast-1.compute.internal)。否則，請指定網域名稱 (例如 example.com)。該值用於完成不符資格的 DNS 主機名稱。如需 DNS 主機名稱和 VPC 中 DNS 支援的詳細資訊，請參閱 <a href="#">搭配使用 DNS 與 VPC (p. 256)</a>。</p> <p><b>Important</b></p> <p>部分 Linux 作業系統接受多個網域名稱，以空格分隔。但是，其他 Linux 作業系統與 Windows 將值視為單一網域，將導致意外行為發生。如果您的 DHCP 選項集與 VPC 相關聯，而該 VPC 具有多個作業系統的執行個體，請僅指定一個網域名稱。</p>
ntp-servers	<p>最多四個網路時間通訊協定 (NTP) 伺服器的 IP 地址。如需詳細資訊，請參閱 <a href="#">RFC 2132</a> 的第 8.3 節。您可在 169.254.169.123 取得 Amazon Time Sync Service。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 <a href="#">設定時間</a>。</p>
netbios-name-servers	<p>最多四個 NetBIOS 名稱伺服器的 IP 地址。</p>
netbios-node-type	<p>NetBIOS 節點類型 (1、2、4 或 8)。建議您指定 2 (點對點或 P 節點)。目前不支援廣播和多點傳播。如需這些節點類型的詳細資訊，請參閱 <a href="#">RFC 2132</a> 的第 8.7 節，以及 <a href="#">RFC1001</a> 的第 10 節。</p>

## Amazon DNS 伺服器

當您建立 VPC 時，我們會自動建立 DHCP 選項集，並將其與 VPC 建立關聯。此組合包括兩個選項：`domain-name-servers=AmazonProvidedDNS` 與 `domain-name=domain-name-for-your-region`。AmazonProvidedDNS 是 Amazon Route 53 Resolver 伺服器，此選項會為需要透過 VPC 網際網路閘道進行通訊的執行個體啟用 DNS。AmazonProvidedDNS 字串會映射到在預留 IP 地址 (以 VPC IPv4 網路範圍 +2 為基礎) 中執行的 DNS 伺服器。例如，在 10.0.0.0/16 網路上的 DNS 伺服器日誌位於 10.0.0.2。對於包含多個 IPv4 CIDR 區塊的 VPC，DNS 伺服器的 IP 地址位於主要 CIDR 區塊中。此 DNS 伺服器的位置不在 VPC 的特定子網路或可用區域。

### Note

您無法使用網路 ACL 或安全群組來篩選與 DNS 伺服器往來的流量。

當您在 VPC 中啟動執行個體時，如果該執行個體接收公有 IPv4 地址，我們會為該執行個體提供私有 DNS 主機名稱和公有 DNS 主機名稱。如果將 DHCP 選項中的 `domain-name-servers` 設定為 AmazonProvidedDNS，則公有 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。私有主機名稱會對 us-east-1 區域採用 `ip-private-ipv4-address.ec2.internal` 格式，對其他區域則採用 `ip-private-ipv4-address.region.compute.internal` 格式。若要將這些變更為自訂 DNS 主機名稱，您必須將 `domain-name-servers` 設定為自訂 DNS 伺服器。

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](#)。

使用 Hadoop 框架的服務 (如 Amazon EMR)，會要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](#)。

### Note

您可以使用 Amazon DNS 伺服器 IP 地址 169.254.169.253，不過部分伺服器不允許其使用。例如，Windows Server 2008 不允許使用位於 169.254.x.x 網路範圍內的 DNS 伺服器。

## 變更 DHCP 選項

建立 DHCP 選項集之後，便無法再進行修改。如果您希望 VPC 使用不同的 DHCP 選項集，則必須建立新選項集，並與 VPC 建立關聯。您也可以將 VPC 設定為完全不使用 DHCP 選項。

您可以有多個 DHCP 選項集，但您每次只能將一個 DHCP 選項集與 VPC 建立關聯。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。

在您將新的 DHCP 選項集與 VPC 建立關聯之後，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 DHCP 選項集

本節為您示範如何使用 DHCP 選項集。

### 工作

- [建立 DHCP 選項集 \(p. 254\)](#)

- [變更 VPC 使用的 DHCP 選項集 \(p. 254\)](#)
- [變更 VPC 以使用無 DHCP 選項 \(p. 255\)](#)
- [修改 DHCP 選項集的標籤 \(p. 255\)](#)
- [刪除 DHCP 選項集 \(p. 255\)](#)

## 建立 DHCP 選項集

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。建立 DHCP 選項集之後，您必須設定您的 VPC 以便使用。如需詳細資訊，請參閱 [變更 VPC 使用的 DHCP 選項集 \(p. 254\)](#)。

### 建立 DHCP 選項集

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)。
3. 在對話方塊中，輸入您要使用的選項值。

#### Important

如果您的 VPC 具有網際網路閘道，請務必指定您自己的 DNS 伺服器或 Amazon DNS 伺服器 (AmazonProvidedDNS) 用於 Domain name servers (網域名稱伺服器) 值。否則，需要與網際網路通訊的執行個體將無法存取 DNS。

4. 選擇性新增或移除標籤。

[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. 選擇 Create DHCP options set (建立 DHCP 選項集)。

DHCP 選項清單會隨即顯示新的 DHCP 選項集。

6. 記下新 DHCP 選項集的 ID (dopt-xxxxxxx)。在您為新選項集與 VPC 建立關聯時，會需要用到此 ID。

即使已建立了 DHCP 選項集，您還必須將其與 VPC 建立關聯，以使選項生效。您可以建立多個 DHCP 選項集，但您每次只能將一個 DHCP 選項集與您的 VPC 建立關聯。

## 變更 VPC 使用的 DHCP 選項集

您可以變更 VPC 使用的 DHCP 選項集。如果您希望 VPC 設定不使用 DHCP 選項，請參閱 [變更 VPC 以使用無 DHCP 選項 \(p. 255\)](#)。

#### Note

下列程序假設您希望變更的 DHCP 選項集已建立。如果您尚未建立該選項集，請現在建立。如需詳細資訊，請參閱 [建立 DHCP 選項集 \(p. 254\)](#)。

### 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，然後選取 Actions，Edit DHCP options set (動作、編輯 DHCP 選項集)。
4. 在 DHCP Options Set (DHCP 選項集) 清單中，選取所需的選項集，然後選擇 Save (儲存)。

在您將新的 DHCP 選項集與 VPC 建立關聯之後，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。

## 變更 VPC 以使用無 DHCP 選項

您可以設定 VPC，使其不使用一組 DHCP 選項。

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，然後選取 Actions，Edit DHCP options set (動作、編輯 DHCP 選項集)。
4. 在 DHCP Options Set (DHCP 選項集) 清單中，選取 No DHCP Options Set (無 DHCP 選項集)，然後選擇 Save (儲存)。

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。

## 修改 DHCP 選項集的標籤

您可以新增標籤以輕鬆識別您的選項集。將標籤新增至 DHCP 選項集，或從 DHCP 選項集中移除標籤。

### 修改 DHCP 選項集的標籤

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)。
3. 選取 DHCP 選項集，然後選取 Actions, Manage tags (動作、管理標籤)。
4. 新增或移除標籤。

[新增標籤] 選擇 Add new tag (新增標籤)，然後執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 對於 Value (值)，進入金鑰值。

[移除標籤] 在標籤旁邊，選擇 Remove tag (移除標籤)。

5. 選擇 Save (儲存)。

## 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。請確定您將使用這些選項的 VPC 變更為另一個選項集，或沒有選項，如需詳細資訊，請參閱 [the section called “變更 VPC 使用的 DHCP 選項集” \(p. 254\)](#) 和 [the section called “變更 VPC 以使用無 DHCP 選項” \(p. 255\)](#)。

### 刪除 DHCP 選項集

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)。
3. 選取要刪除的 DHCP 選項集，然後選擇 Actions, Delete DHCP options set (動作、刪除 DHCP 選項集)。
4. 在確認對話方塊中，輸入 delete (刪除)，然後選擇 Delete DHCP options set (刪除 DHCP 選項集)。



## API 和命令概觀

您可以使用命令列或 API 執行此主題所述的任務。如需命令列界面與可用 API 清單的詳細資訊，請參閱[存取 Amazon VPC \(p. 1\)](#)。

### 建立 VPC 的 DHCP 選項集

- [create-dhcp-options](#) (AWS CLI)
- [New-EC2DhcpOption](#) (適用於 Windows PowerShell 的 AWS 工具)

將 DHCP 選項集與指定的 VPC 建立關聯，或無 DHCP 選項

- [associate-dhcp-options](#) (AWS CLI)
- [Register-EC2DhcpOption](#) (適用於 Windows PowerShell 的 AWS 工具)

### 說明一或多個 DHCP 選項集

- [describe-dhcp-options](#) (AWS CLI)
- [Get-EC2DhcpOption](#) (適用於 Windows PowerShell 的 AWS 工具)

### 刪除 DHCP 選項集

- [delete-dhcp-options](#) (AWS CLI)
- [Remove-EC2DhcpOption](#) (適用於 Windows PowerShell 的 AWS 工具)

## 搭配使用 DNS 與 VPC

網域名稱系統 (DNS) 是一種標準；網際網路上的名稱會據此解析為對應的 IP 地址。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 (EC2-Classic 或 VPC) 內的通訊。如需更多詳細資訊，請參閱 [您 VPC 中的 IP 定址 \(p. 102\)](#)。

我們提供 Amazon DNS 伺服器。若要使用您自己的 DNS 伺服器，請為 VPC 建立一組新的 DHCP 選項。如需更多詳細資訊，請參閱 [DHCP 選項集 \(p. 251\)](#)。

### 內容

- [DNS 主機名稱 \(p. 256\)](#)
- [VPC 中的 DNS 支援 \(p. 257\)](#)
- [DNS 配額 \(p. 258\)](#)
- [檢視 EC2 執行個體的 DNS 主機名稱 \(p. 258\)](#)
- [檢視並更新 VPC 的 DNS 支援 \(p. 259\)](#)
- [使用私有託管區域 \(p. 259\)](#)

## DNS 主機名稱

當您在預設 VPC 中啟動執行個體時，我們會為該執行個體提供公有和私有 DNS 主機名稱 (其對應於執行個體的公有 IPv4 和私有 IPv4 地址)。當您在非預設 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，並可能會提供公有 DNS 主機名稱 (依據您為 VPC 指定的 [DNS 屬性 \(p. 257\)](#) 以及執行個體是否含公有 IPv4 地址而定)。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [公有 IPv4 地址和外部 DNS 主機名稱](#)。

Amazon 提供的私有 (內部) DNS 主機名稱會解析為執行個體的私有 IPv4 地址，並對 us-east-1 區域採用 `ip-private-ipv4-address.ec2.internal` 格式，而對其他區域採用 `ip-private-ipv4-address.region.compute.internal` 格式 (其中 `private-ipv4-address` 是反向查詢的 IP 地址)。您可以使用私有 DNS 主機名稱以在相同網路的執行個體之間通訊，但我們無法在執行個體所在的網路外部解析 DNS 主機名稱。

公有 (外部) 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。

我們不提供適用於 IPv6 地址的 DNS 主機名稱。

## VPC 中的 DNS 支援

您的 VPC 具有以下屬性，可決定在 VPC 中啟動的執行個體是否接收對應至其公有 IP 地址的公有 DNS 主機名稱，以及 VPC 是否支援透過 Amazon DNS 伺服器解析 DNS。

屬性	描述
<code>enableDnsHostnames</code>	<p>指出具有公有 IP 地址的執行個體是否取得對應的公有 DNS 主機名稱。</p> <p>如果此屬性為 <code>true</code> 且 <code>enableDnsSupport</code> 屬性也設為 <code>true</code> 時，VPC 中的執行個體會取得公有 DNS 主機名稱。</p>
<code>enableDnsSupport</code>	<p>指出是否支援 DNS 解析。</p> <p>如果此屬性為 <code>false</code>，則不會啟用可將公有 DNS 主機名稱解析為 IP 地址的 Amazon Route 53 Resolver 伺服器。</p> <p>如果此屬性為 <code>true</code>，則對 Amazon 提供的 DNS 伺服器 (IP 地址為 169.254.169.253) 或預留 IP 地址 (以 VPC IPv4 網路範圍 +2 為基礎) 的查詢會成功。如需詳細資訊，請參閱 <a href="#">Amazon DNS 伺服器 (p. 253)</a>。</p>

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 伺服器可以解析 Amazon 提供的公有 DNS 主機名稱。

如果其中一或兩個屬性設定為 `false`，會發生下列情況：

- 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 Amazon 提供的私有 DNS 主機名稱。
- 如果 [DHCP 選項集 \(p. 251\)](#) 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。

根據預設，在預設 VPC 或由 VPC 精靈建立的 VPC 中，這兩個屬性皆為 `true`。預設情況下，只有在以其他任何方式建立的 VPC 中，`enableDnsSupport` 屬性才會設為 `true`。為確認您的 VPC 是否啟用這些屬性，請參閱 [檢視並更新 VPC 的 DNS 支援 \(p. 259\)](#)。

#### Important

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` 屬性設為 `true`。

Amazon Route 53 Resolver 可針對所有地址空間將私有 DNS 主機名稱解析為私有 IPv4 地址，包括當 VPC 的 IPv4 地址範圍不在 [RFC 1918](#) 指定之私有 IPv4 地址範圍內的情況。

#### Important

如果您的 VPC 是在 2016 年 10 月之前建立，當 VPC 的 IPv4 地址範圍不在 RFC 1918 指定的私有 IPv4 地址範圍內時，Amazon DNS 伺服器就無法解析私有 DNS 主機名稱。如果您要讓 Amazon DNS 伺服器解析這些地址的私有 DNS 主機名稱，請聯絡 [AWS Support](#)。

若您在 VPC 中啟用對 DNS 主機名稱和 DNS 的支援 (VPC 原本並不支援)，則您已在 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)。

## DNS 配額

每個 EC2 執行個體會將可傳送至 Amazon Route 53 Resolver (亦即 .2 位址，例如 10.0.0.2) 的封包數限制為每秒、每個網路界面最多 1024 個封包。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，Amazon 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 架構建議事項，請參閱 [適用於 Amazon VPC 的混合雲端 DNS 解決方案白皮書](#)。

## 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界面的 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 支援” \(p. 257\)](#)。

### 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 Instances (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。如需這些命令列界面的詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (適用於 Windows PowerShell 的 AWS 工具)

## 網路界面

使用主控台檢視網路界面的私有 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 (網路界面)。
3. 從清單選取網路界面。
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界面的 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界面的詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

- [describe-network-interfaces](#) (AWS CLI)
- [Get-EC2NetworkInterface](#) (適用於 Windows PowerShell 的 AWS 工具)

## 檢視並更新 VPC 的 DNS 支援

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. 從清單選取 VPC。
4. 檢閱 Description (描述) 標籤中的資訊。在此範例中，會啟用兩種設定。

DNS resolution	Enabled
DNS hostnames	Enabled

5. 若要更新這些設定，請選擇 Actions (動作)，然後選擇 Edit DNS Resolution (編輯 DNS 解析) 或 Edit DNS Hostnames (編輯 DNS 主機名稱)。在開啟的對話方塊中，選擇 Yes (是) 或 No (否)，然後選擇 Save (儲存)。

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。如需這些命令列界面的詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

- [describe-vpc-attribute](#) (AWS CLI)
- [Get-EC2VpcAttribute](#) (適用於 Windows PowerShell 的 AWS 工具)

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。如需這些命令列界面的詳細資訊，請參閱 [存取 Amazon VPC \(p. 1\)](#)。

- [modify-vpc-attribute](#) (AWS CLI)
- [Edit-EC2VpcAttribute](#) (適用於 Windows PowerShell 的 AWS 工具)

## 使用私有託管區域

如果您想要使用自訂 DNS 網域名稱 (如 example.com) 而不使用私有 IPv4 地址或 AWS 提供的私有 DNS 主機名稱來存取 VPC 中的資源，您可以在 Route 53 中建立私有託管區域。私有託管區域是一種容器，其中包

含的資訊說明您可以如何在一或多個 VPC 中路由某個網域及其子網域的流量，而不用將資源公開至網際網路。接著，您可以建立 Route 53 資源紀錄集，以決定 Route 53 如何回應網域和子網域的查詢。舉例來說，如果您想將 example.com 的瀏覽器請求路由至 VPC 中的 Web 伺服器，您可以在私有託管區域中建立 A 記錄，然後指定該 Web 伺服器的 IP 地址。如需如何建立私有託管區域的詳細資訊，請參閱 Amazon Route 53 開發人員指南 中的 [使用私有託管區域](#)。

若要使用自訂 DNS 網域名稱來存取資源，您必須連線至 VPC 內的執行個體。您可以在執行個體中使用 ping 命令 (例如 ping mywebserver.example.com)，來測試私有託管區域中的資源是否可透過其自訂 DNS 名稱來存取。(您必須確認執行個體的安全群組允許傳入 ICMP 流量，ping 命令才能運作。)

如果您的 VPC 已啟用 ClassicLink DNS 支援，您即可使用 ClassicLink 從連結至 VPC 的 EC2-Classic 執行個體來存取私有託管區域。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [啟用 ClassicLink DNS 支援](#)。否則，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 連接另一端存取資源。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [ClassicLink 限制](#)。

#### 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，enableDnsHostnames 與 enableDnsSupport 屬性必須設為 true。

## VPC 互連

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。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。

AWS 使用現有的 VPC 基礎設施建立 VPC 互連連線，既不是閘道，也不是 AWS Site-to-Site VPN 連接，且不倚賴獨立的實體硬體。因此不會有通訊的單一故障點或頻寬瓶頸問題。

如需使用 VPC 互連連線的詳細資訊，以及可使用 VPC 互連連線的案例範例，請參閱 [《Amazon VPC Peering Guide》](#)。

## 彈性 IP 地址

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 位址會持續配置給您的 AWS 帳戶直到您明確將其釋出為止。

彈性 IP 地址是網路界面的屬性。您可以透過更新連接至執行個體的網路界面，將彈性 IP 地址與執行個體建立關聯。將彈性 IP 位址與網路介面 (而不是直接與執行個體) 建立關聯的好處在於只要一個步驟，即可將網路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 [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。

- 為了確保有效率地使用彈性 IP 地址，當它們未與執行中的執行個體相關聯，或是與停止的執行個體或未連接的網路界面相關聯時，我們每小時會收取少許費用。在您的執行個體執行期間，您可以免費使用一個與該執行個體相關聯的彈性 IP 地址，但若有任何額外的彈性 IP 地址與該執行個體相關聯，則需要支付相關費用。如需詳細資訊，請參閱 [Amazon EC2 定價](#)。
- 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 [NAT \(p. 226\)](#)。
- 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。
- 彈性 IP 位址是透過 VPC 網際網路閘道存取。如果您已在您的 VPC 和網路之間設定 AWS Site-to-Site VPN 連線，VPN 流量會周遊虛擬私有閘道，而非網際網路閘道，因而無法存取彈性 IP 位址。
- 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。如需使用自有 IP 地址的相關資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南中的 [使用自有 IP 地址 \(BYOIP\)](#)。

您在 VPC 中和 EC2-Classic 中使用的彈性 IP 地址有所不同。如需詳細資訊，請參閱 Linux 執行個體的 Amazon EC2 使用者指南 中的 [EC2-Classic 與 VPC 之間的差異](#)。您可以將已配置供 EC2-Classic 平台使用的彈性 IP 地址移至 VPC 平台。如需詳細資訊，請參閱 [從 EC2-Classic 遷移彈性 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。

### 主題

- [配置彈性 IP 地址 \(p. 261\)](#)
- [建立彈性 IP 地址的關聯 \(p. 262\)](#)
- [描述您的彈性 IP 位址 \(p. 262\)](#)
- [建立彈性 IP 地址標籤 \(p. 263\)](#)
- [解除與彈性 IP 地址的關聯 \(p. 263\)](#)
- [釋放彈性 IP 地址 \(p. 263\)](#)
- [復原彈性 IP 地址 \(p. 264\)](#)

## 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。

### Console

#### 配置用於 VPC 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. 選擇 Allocate Elastic IP address (配置彈性 IP 位址)。
4. (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—若您要從已帶入您 AWS 帳戶的 IP 地址集區配置一個 IPv4 地址。如果您沒有任何 IP 地址集區，則會停用此選項。



- Customer owned pool of IPv4 addresses (客戶擁有的 IPv4 地址集區)—若您要從內部部署網路建立的集區配置 IPv4 地址，以搭配使用 AWS Outpost。如果您沒有 AWS Outpost，則會停用此選項。

5. 選擇 Allocate (配置)。

Note

如果您的帳戶支援 EC2-Classical，則請先選擇 VPC。

CLI and API

配置彈性 IP 地址

- [allocate-address](#) (AWS CLI)
- [New-EC2Address](#) (適用於 Windows PowerShell 的 AWS 工具)

## 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 [搭配使用 DNS 與 VPC \(p. 256\)](#)。

Console

將彈性 IP 位址與 VPC 中的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 (建立關聯)。

CLI and API

將彈性 IP 位址與執行個體或網路介面建立關聯

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (適用於 Windows PowerShell 的 AWS 工具)

## 描述您的彈性 IP 位址

您可以檢視分配給您帳戶的彈性 IP 位址。

Console

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。

#### CLI and API

檢視一或多個彈性 IP 位址

- [describe-addresses](#) (AWS CLI)
- [Get-EC2Address](#) (適用於 Windows PowerShell 的 AWS 工具)

## 建立彈性 IP 地址標籤

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。

#### Console

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)。

#### CLI and API

為彈性 IP 地址套用標籤

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (適用於 Windows PowerShell 的 AWS 工具)

## 解除與彈性 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。

#### Console

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)。

#### CLI and API

取消與彈性 IP 地址的關聯

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (適用於 Windows PowerShell 的 AWS 工具)

## 釋放彈性 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。



## Console

### 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 (釋出彈性 IP 位址)。
4. 出現提示時，請選擇 Release (釋出)。

## CLI and API

### 釋出彈性 IP 地址

- [release-address](#) (AWS CLI)
- [Remove-EC2Address](#) (適用於 Windows PowerShell 的 AWS 工具)

## 復原彈性 IP 地址

如果您釋出您的彈性 IP 地址，您也許能夠予以復原。如果彈性 IP 地址已配置給其他 AWS 帳戶，或是會導致您超過彈性 IP 地址配額，您便無法復原彈性 IP 地址。

目前，您只能使用 Amazon EC2 API 或命令列工具來復原彈性 IP 地址。

### 使用 AWS CLI 復原彈性 IP 地址

- 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
```

# ClassicLink

ClassicLink 可讓您將相同區域內的 EC2-Classic 執行個體連結至您帳戶中的 VPC。這麼做可使您將 VPC 安全群組與 EC2-Classic 執行個體建立關聯，讓 EC2-Classic 執行個體使用私有 IPv4 地址與 VPC 中的執行個體通訊。ClassicLink 不必使用公有 IPv4 地址或彈性 IP 地址，即可啟用這些平台之間的執行個體通訊。如需私有和公有 IPv4 地址的詳細資訊，請參閱[您 VPC 中的 IP 定址 \(p. 102\)](#)。

只要使用者具備支援 EC2-Classic 平台的帳戶，都可以使用 ClassicLink 並搭配使用任何 EC2-Classic 執行個體。

使用 ClassicLink 無需額外收費。收取標準數據傳輸費和執行個體鐘點使用費。

如需各 ClassicLink 及使用方法的詳細資訊，請參閱 Amazon EC2 使用者指南中的下列主題：

- [ClassicLink 基本概念](#)
- [ClassicLink 限制](#)
- [使用 ClassicLink](#)
- [ClassicLink API 和 CLI 概觀](#)

# VPC 端點 和 VPC 端點服務 (AWS PrivateLink)

VPC 端點 可讓您將 VPC 私下連線至支援的 AWS 服務以及具有 AWS PrivateLink 功能的 VPC 端點服務，而不需要網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，即可與服務中的資源通訊。VPC 與另一個服務之間的流量都會保持在 Amazon 網路的範圍內。

端點是虛擬裝置。這些端點是水平擴展、冗餘且高度可用的 VPC 元件。其可讓您 VPC 中的執行個體與服務進行通訊，而不會強加網路流量的可用性風險或頻寬限制。

## 主題

- [VPC 端點概念 \(p. 265\)](#)
- [使用 VPC 端點 \(p. 265\)](#)
- [VPC 端點 \(p. 266\)](#)
- [VPC 端點服務 \(AWS PrivateLink\) \(p. 294\)](#)
- [適用於 VPC 端點 和 VPC 端點 服務的 Identity and Access Management \(p. 305\)](#)
- [端點服務的私有 DNS 名稱 \(p. 306\)](#)
- [可與 AWS PrivateLink 搭配使用的 AWS 服務 \(p. 314\)](#)

## VPC 端點概念

以下是 VPC 端點的重要概念：

- 端點服務：您在 VPC 中所擁有的應用程式。其他 AWS 委託人可以從其 VPC 建立與您端點服務的連線。
- 閘道端點 — [閘道端點 \(p. 279\)](#)是做為路由表中路由您指定之目標的閘道通往支援之 AWS 服務的流量。
- 界面端點 — [界面端點 \(p. 266\)](#)是包含私有 IP 地址從您的子網路 IP 地址範圍的彈性網路界面，做為通往支援之服務的流量進入點。

## 使用 VPC 端點

您可以使用以下任何一種方式來建立、存取和管理 VPC 端點：

- AWS 管理主控台：提供您可以用來存取 VPC 端點的 web 界面。
- AWS Command Line Interface (AWS CLI)：提供多種 AWS 服務的命令，包括 Amazon VPC。Windows、macOS 和 Linux 都支援 AWS CLI。如需詳細資訊，請參閱[AWS Command Line Interface](#)。
- AWS 開發套件：提供語言特定的 API。AWS 開發套件會處理許多連線詳細資訊，例如計算簽章、處理請求重試和處理錯誤。如需詳細資訊，請參閱 AWS 開發套件。
- 查詢 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。不過，查詢 API 需要您的應用程式處理低階詳細資訊，例如產生雜湊以簽署要求以及處理錯誤。如需詳細資訊，請參閱 [Amazon EC2 API Reference](#)。

## VPC 端點

VPC 端點可讓您將 VPC 私下連線至支援的 AWS 服務以及具有 AWS PrivateLink 功能的 VPC 端點服務，而不需要網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，即可與服務中的資源通訊。VPC 與另一個服務之間的流量都會保持在 Amazon 網路的範圍內。

端點是虛擬裝置。這些端點是水平擴展、冗餘且高度可用的 VPC 元件。其可讓您 VPC 中的執行個體與服務進行通訊，而不會強加網路流量的可用性風險或頻寬限制。

有兩種 VPC 端點類型：「界面端點」和「閘道端點」。請建立支援的服務所需要的 VPC 端點類型。

**界面端點** (p. 266) 是包含私有 IP 地址從您的子網路 IP 地址範圍的彈性網路界面，做為通往支援之服務的流量進入點。界面端點採用 AWS PrivateLink 技術，該技術能讓您使用私有 IP 地址來私下存取服務。AWS PrivateLink 會將 VPC 與服務間的所有網路流量限於 Amazon 網路。您不需要網際網路閘道、NAT 裝置或虛擬私有閘道。

如需與 AWS PrivateLink 整合之 AWS 服務的資訊，請參閱 [the section called “可與 AWS PrivateLink 搭配使用的 AWS 服務” \(p. 314\)](#)。

### 閘道端點

**閘道端點** (p. 279) 是做為路由表中路由您指定之目標的閘道通往支援之 AWS 服務的流量。支援下列 AWS 服務：

- Amazon S3
- DynamoDB

若要檢視所有可用的 AWS 服務名稱，請參閱 [檢視可用的 AWS 服務名稱 \(p. 271\)](#)。

## 界面 VPC 端點 (AWS PrivateLink)

界面 VPC 端點 (界面端點) 可讓您連線至採用 AWS PrivateLink 技術的服務。這些服務包含一些 AWS 服務、其他 AWS 客戶和合作夥伴在其專屬 VPC 中託管的服務 (稱為「端點服務」)，以及支援的 AWS Marketplace 合作夥伴服務。服務擁有者是服務提供者，而您 (做為建立界面端點的委託人) 是服務消費者。

下列為設定界面端點的一般步驟：

1. 選擇要在其中建立界面端點的 VPC，並提供您連線的 AWS 服務、端點服務或 AWS Marketplace 服務名稱。
2. 選擇 VPC 中要使用界面端點的子網路。我們會在子網路中建立端點網路界面。您可以指定不同可用區域中的多個子網路 (服務所支援)，協助確保界面端點在可用區域失敗的狀況下保有彈性。在該情況下，我們會在您指定的每個子網路中建立端點網路界面。

### Note

端點網路界面是申請者受管網路界面。您可以在您的帳戶中予以檢視，但無法由您管理。如需詳細資訊，請參閱 [彈性網路界面](#)。

3. 指定要與端點網路界面建立關聯的安全群組。安全群組規則可控制從 VPC 中之資源流向端點網路界面的流量。如果您未指定安全群組，則會建立與 VPC 預設安全群組的關聯。
4. (選用，僅限 AWS 服務和 AWS Marketplace 合作夥伴服務) 啟用端點的 [私有 DNS \(p. 267\)](#)，可讓您使用服務的預設 DNS 主機名稱以對服務提出請求。

### Important

針對為 AWS 服務和 AWS Marketplace 合作夥伴服務建立的端點，私有 DNS 根據預設為啟用。私有 DNS 會在位於相同 VPC 和可用區域或本機區域的其他子網路中啟用。

5. 服務供應商與消費者的帳戶不同時，請參閱 [the section called “界面端點與可用區域的考量” \(p. 270\)](#) 了解如何使用可用區域 ID 來辨識可用區域介面端點的資訊。
6. 在您建立界面端點之後，可於服務提供者接受界面端點後使用之。服務提供者必須設定其服務自動接受請求或手動操作。AWS 服務和 AWS Marketplace 服務一般會自動接受所有端點請求。如需端點生命週期的詳細資訊，請參閱 [界面端點生命週期 \(p. 270\)](#)。

服務無法透過端點初始化對 VPC 的資源請求。端點只會傳回從 VPC 中資源初始化流量的回應。在您整合服務和端點之前，請參閱特定服務的 VPC 端點文件，以了解特定服務的組態和限制。

#### 內容

- [界面端點的私有 DNS \(p. 267\)](#)
- [界面端點屬性和限制 \(p. 269\)](#)
- [連線至內部部署的資料中心 \(p. 270\)](#)
- [界面端點生命週期 \(p. 270\)](#)
- [界面端點與可用區域的考量 \(p. 270\)](#)
- [界面端點定價 \(p. 270\)](#)
- [檢視可用的 AWS 服務名稱 \(p. 271\)](#)
- [建立界面端點 \(p. 272\)](#)
- [檢視界面端點 \(p. 275\)](#)
- [建立和管理界面端點的通知 \(p. 275\)](#)
- [透過界面端點存取服務 \(p. 277\)](#)
- [修改界面端點 \(p. 277\)](#)

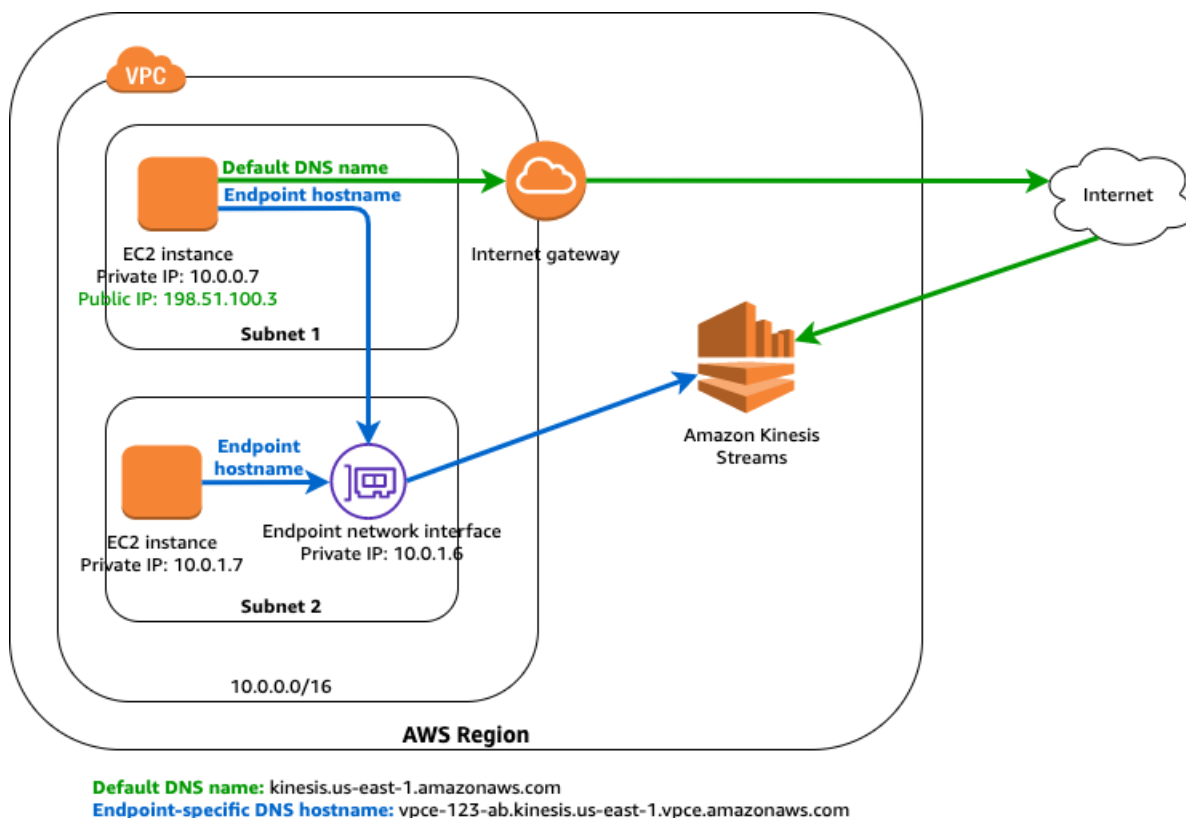
## 界面端點的私有 DNS

當您建立界面端點時，會產生您可用來與服務通訊的端點特定 DNS 主機名稱。針對 AWS 服務和 AWS Marketplace 合作夥伴服務，私有 DNS 選項 (預設為啟用) 會將某個私有託管區域與您的 VPC 建立關聯。託管區域包含服務之預設 DNS 名稱的記錄集 (例如 `ec2.us-east-1.amazonaws.com`)，可解析為 VPC 中端點網路界面的私有 IP 地址。這可讓您使用服務的預設 DNS 主機名稱以對服務提出請求，而非端點特定 DNS 主機名稱。例如，如果您的現有應用程式對 AWS 服務提出請求，則可以透過界面端點持續提出請求，而不需要任何組態變更。

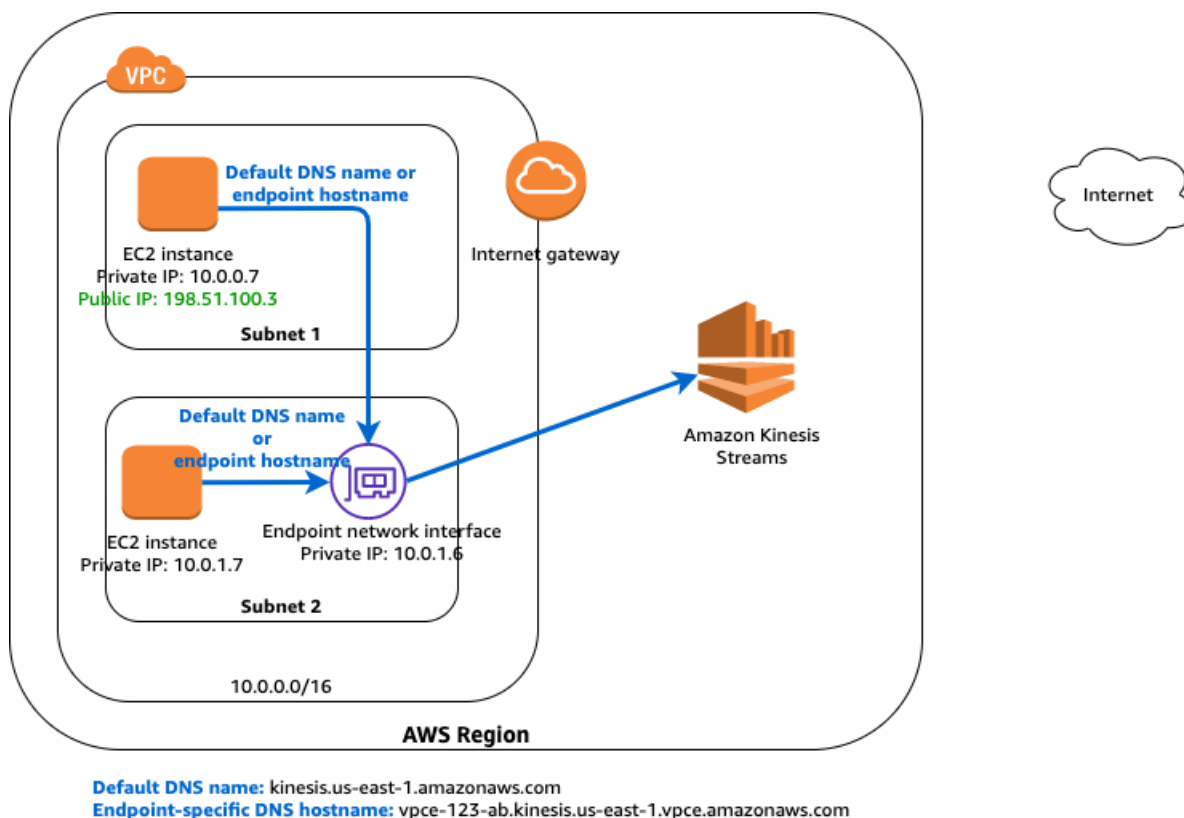
在下圖中顯示的範例，有一個 Amazon Kinesis Data Streams 的界面端點，以及一個在子網路 2 中的端點網路界面。界面端點的私有 DNS 未啟用。子網路的路由表具備下列路由。

子網路 1	
目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	internet-gateway-id
子網路 2	
目的地	目標
10.0.0.0/16	區域

任一子網路中的執行個體都可以透過界面端點，使用端點特定 DNS 主機名稱將要求傳送給 Amazon Kinesis Data Streams。子網路 1 中的執行個體可以使用預設 DNS 名稱，透過 AWS 區域中的公有 IP 地址空間與 Amazon Kinesis Data Streams 通訊。



在下圖中，端點的私有 DNS 已啟用。任一子網路中的執行個體都可以透過界面端點，使用預設的 DNS 主機名稱，或端點特定 DNS 主機名稱將要求傳送給 Amazon Kinesis Data Streams。



### Important

若要使用私有 DNS，您必須將下列 VPC 屬性設定為 `true`：`enableDnsHostnames` 和 `enableDnsSupport`。如需詳細資訊，請參閱 [檢視並更新 VPC 的 DNS 支援](#) (p. 259)。IAM 使用者必須具有使用託管區域的許可。如需詳細資訊，請參閱 [Route 53 的身份驗證和存取控制](#)。

## 界面端點屬性和限制

若要使用界面端點，您需要知道其屬性和目前限制：

- 針對每個界面端點，一個可用區域只能選擇一個子網路。
- 某些服務支援以端點政策控制服務存取權。如需支援端點政策之服務的詳細資訊，請參閱 [the section called “使用 VPC 端點 控制服務的存取”](#) (p. 292)。
- 透過界面端點，可能無法在所有可用區域中使用服務。若要了解支援的可用區域，請使用 `describe-vpc-endpoint-services` 命令或使用 Amazon VPC 主控台。如需詳細資訊，請參閱 [建立界面端點](#) (p. 272)。
- 當您建立界面端點時，即會在映射到您帳戶的可用區域中建立端點，並且獨立於其他帳戶。服務供應商與消費者的帳戶不同時，請參閱 [the section called “界面端點與可用區域的考量”](#) (p. 270) 了解如何使用可用區域 ID 來辨識可用區域界面端點的資訊。
- 當服務提供者和消費者擁有不同的帳戶並使用多個可用區域，且消費者檢視 VPC 端點服務資訊時，回應僅包含常見的可用區域。例如，當服務提供者帳戶使用 `us-east-1a` 和 `us-east-1c` 且消費者使用 `us-east-1a` 和 `us-east-1b` 時，回應會包含常見可用區域 `us-east-1a` 中的 VPC 端點服務。
- 根據預設，每個可用區域的每個界面端點可支援最多 10 Gbps 的頻寬。而頻寬暴增最高可達 40 Gbps。如果您的應用程式需要更高的暴增次數或持續的輸送量，請連絡 AWS 支援。
- 如果您子網路的網路 ACL 限制流量，則可能無法透過端點網路界面傳送流量。請確定您新增適當的規則，以允許進出子網路之 CIDR 區塊的流量。



- 請確定與端點網路介面相關聯的安全群組允許端點網路界面與 VPC 中的資源 (可與服務通訊) 之間的通訊。如果安全群組限制來自 VPC 資源的傳入 HTTPS 流量 (連接埠 443)，您可能無法透過端點網路介面傳送流量。
- 界面端點僅支援 TCP 流量。
- 當您建立端點時，可以將端點政策連接至閘道端點，以控制存取您要連線的服務。如需詳細資訊，請參閱[政策最佳實務](#)和 [the section called “使用 VPC 端點 控制服務的存取” \(p. 292\)](#)。
- 檢閱您端點服務的服務特定限制。
- 只在相同的區域內支援端點。您無法在 VPC 和位於不同區域內的服務之間建立端點。
- 端點僅支援 IPv4 流量。
- 您無法在 VPC 與 VPC 之間或是服務與服務之間轉移端點。
- 每個 VPC 可建立的端點數量都有配額。如需更多詳細資訊，請參閱 [VPC 端點 \(p. 323\)](#)。

## 連線至內部部署的資料中心

您可以使用下列連線類型來在界面端點和您的內部部署資料中心間進行連線。

- [AWS Direct Connect](#)
- [AWS Site-to-Site VPN](#)

## 界面端點生命週期

從您建立界面端點時開始，界面端點會經過多個階段 (端點連線請求)。在每個階段，都可能會有服務消費者和服務提供者可採取的動作。

適用的規定如下：

- 服務提供者可以設定其服務自動接受界面端點請求或手動操作。AWS 服務和 AWS Marketplace 服務一般會自動接受所有端點請求。
- 服務提供者無法刪除其服務的界面端點。只有已請求界面端點連線的服務消費者才能刪除界面端點。
- 在手動或自動接受界面端點且界面端點處於 `available` 狀態時，服務提供者可以拒絕該界面端點。

## 界面端點與可用區域的考量

當您建立界面端點時，即會在映射到您帳戶的可用區域中建立端點，並且獨立於其他帳戶。服務供應商與消費者的帳戶不同時，使用可用區域 ID 的唯一性及一致性以及識別可用區域的端點介面。例如，`us-east-1` 是 `us-east-1` 區域的可用區域 ID，並且在每一個 AWS 帳戶中都會映射到相同的位置。如需有關如何識別您可用區域 ID 的資訊，請參閱 AWS RAM 使用者指南 中的 [對您資源的 AZ ID](#) 或使用 [說明可用的區域](#)。

透過界面端點，可能無法在所有可用區域中使用服務。您可以使用下列操作，找出服務支援哪個可用區域：

- [describe-vpc-endpoint-services](#) (AWS CLI)
- [DescribeVpcEndpointServices](#) (API)
- 建立界面端點時的 Amazon VPC 主控台。如需詳細資訊，請參閱[the section called “建立界面端點” \(p. 272\)](#)。

## 界面端點定價

會向您收取建立和使用服務之界面端點的費用。每小時用量率和資料處理率都適用。如需有關界面端點定價的詳細資訊，請參閱[AWS PrivateLink 定價](#)。您可以使用 Amazon VPC 主控台或 AWS CLI 檢視界面端點總數。



## 檢視可用的 AWS 服務名稱

當您使用 Amazon VPC 主控台建立端點時，您可以取得可用 AWS 服務名稱的清單。

當您使用 AWS CLI 來建立端點時，可以使用 `describe-vpc-endpoint-services` 命令來檢視服務名稱，然後使用 `create-vpc-endpoint` 命令建立端點。

### Console

使用主控台檢視可用的 AWS 服務

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，Create Endpoint (建立端點)。
3. 在 Service Name (服務名稱) 區段中，會列出可用的服務。

### Command line

使用 AWS CLI 檢視可用的 AWS 服務

- 使用 `describe-vpc-endpoint-services` 命令，以取得可用服務清單。在傳回的輸出中，記下要連線之服務的名稱。ServiceType 欄位指出您透過界面端點還是閘道端點連線至服務。ServiceName 欄位提供服務的名稱。

```
aws ec2 describe-vpc-endpoint-services
```

```
{
  "VpcEndpoints": [
    {
      "VpcEndpointId": "vpce-08a979e28f97a9f7c",
      "VpcEndpointType": "Interface",
      "VpcId": "vpc-06e4ab6c6c3b23ae3",
      "ServiceName": "com.amazonaws.us-east-2.monitoring",
      "State": "available",
      "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\n\", \n\n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\n\": \"*\"\n    }\n  ]\n}",
      "RouteTableIds": [],
      "SubnetIds": [
        "subnet-0931fc2fa5f1cbe44"
      ],
      "Groups": [
        {
          "GroupId": "sg-06e1d57ab87d8f182",
          "GroupName": "default"
        }
      ],
      "PrivateDnsEnabled": false,
      "RequesterManaged": false,
      "NetworkInterfaceIds": [
        "eni-019b0bb3ede80ebfd"
      ],
      "DnsEntries": [
        {
          "DnsName": "vpce-08a979e28f97a9f7c-4r5zme9n.monitoring.us-east-2.vpce.amazonaws.com",
          "HostedZoneId": "ZC8PGOKIFKBRI"
        },
        {
          "DnsName": "vpce-08a979e28f97a9f7c-4r5zme9n-us-east-2c.monitoring.us-east-2.vpce.amazonaws.com",

```

```
        "HostedZoneId": "ZC8PG0KIFKBRI"
      },
    ],
    "CreationTimestamp": "2019-06-04T19:10:37.000Z",
    "Tags": [],
    "OwnerId": "123456789012"
  }
]
```

使用適用於 Windows PowerShell 的 AWS 工具 檢視可用的 AWS 服務

- [Get-EC2VpcEndpointService](#)

使用 API 檢視可用的 AWS 服務

- [DescribeVpcEndpointServices](#)

## 建立界面端點

若要建立界面端點，您必須指定在其中建立界面端點的 VPC，以及與其建立連線的服務。

針對 AWS 服務或 AWS Marketplace 合作夥伴服務，您可以啟用端點的[私有 DNS \(p. 267\)](#)，以使用服務的預設 DNS 主機名稱對服務提出請求。

### Important

針對為 AWS 服務和 AWS Marketplace 合作夥伴服務建立的端點，私有 DNS 根據預設為啟用。

### Console

使用主控台建立 AWS 服務的界面端點

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，Create Endpoint (建立端點)。
3. 對於 Service category (服務類別)，請確定您已選擇 AWS services (AWS 服務)。
4. 針對 Service Name (服務名稱)，選擇要連線的服務。對於 Type (類型)，請確定其顯示 Interface (界面)。
5. 完成下列資訊，然後選擇 Create endpoint (建立端點)。

- 針對 VPC，選取要在其中建立端點的 VPC。
- 針對 Subnets (子網路)，選取要在其中建立端點網路界面的子網路 (可用區域)。

並非全部的可用區域都支援所有 AWS 服務。

- 針對 Enable Private DNS Name (啟用私有 DNS 名稱)，選取核取方塊，以啟用界面端點的私有 DNS。

此選項預設為啟用。若要使用私有 DNS 選項，您 VPC 的下列屬性都必須設為 true: `enableDnsHostnames` 和 `enableDnsSupport`。如需詳細資訊，請參閱[檢視並更新 VPC 的 DNS 支援 \(p. 259\)](#)。

- 針對 Security group (安全群組)，選取要與端點網路界面建立關聯的安全群組。
- (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

若要建立端點服務的界面端點，您必須有要連線之服務的名稱。服務提供者可以提供名稱。

#### 建立端點服務的界面端點

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，Create Endpoint (建立端點)。
3. 針對 Service category (服務類別)，選擇 Find service by name (依名稱尋找服務)。
4. 針對 Service Name (服務名稱)，輸入服務的名稱 (例如 `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`)，然後選擇 Verify (驗證)。
5. 完成下列資訊，然後選擇 Create endpoint (建立端點)。

- 針對 VPC，選取要在其中建立端點的 VPC。
- 針對 Subnets (子網路)，選取要在其中建立端點網路界面的子網路 (可用區域)。

並非全部的可用區域都支援該服務。

- 針對 Security group (安全群組)，選取要與端點網路界面建立關聯的安全群組。
- (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

#### 建立 AWS Marketplace 合作夥伴服務的界面端點

1. 前往 AWS Marketplace 上的 [PrivateLink](#) 頁面，並訂閱軟體即服務 (SaaS) 提供者的服務。支援界面端點的服務包含透過端點連線的選項。
2. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Endpoints (端點)，Create Endpoint (建立端點)。
4. 針對 Service category (服務類別)，選擇 Your AWS Marketplace services (您的 AWS Marketplace 服務)。
5. 選擇您已訂閱的 AWS Marketplace 服務。
6. 完成下列資訊，然後選擇 Create endpoint (建立端點)。

- 針對 VPC，選取要在其中建立端點的 VPC。
- 針對 Subnets (子網路)，選取要在其中建立端點網路界面的子網路 (可用區域)。

並非全部的可用區域都支援該服務。

- 針對 Security group (安全群組)，選取要與端點網路界面建立關聯的安全群組。
- (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

## Command line

## 使用 AWS CLI 建立界面端點

1. 使用 `describe-vpc-endpoint-services` 命令，以取得可用服務清單。在傳回的輸出中，記下要連線之服務的名稱。ServiceType 欄位指出您透過界面端點還是閘道端點連線至服務。ServiceName 欄位提供服務的名稱。
2. 若要建立界面端點，請使用 `create-vpc-endpoint` 命令，並指定 VPC ID、VPC 端點 類型 (界面)、服務名稱、將使用端點的子網路，以及要與端點網路界面建立關聯的安全群組。

下列範例會建立 Elastic Load Balancing 服務的界面端點。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
--service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-
abababab --security-group-id sg-1a2b3c4d
```

```
{
  "VpcEndpoint": {
    "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\",\n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\": \"*\n    }\n  ]\n}",
    "VpcId": "vpc-ec43eb89",
    "NetworkInterfaceIds": [
      "eni-bf8aa46b"
    ],
    "SubnetIds": [
      "subnet-abababab"
    ],
    "PrivateDnsEnabled": true,
    "State": "pending",
    "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
    "RouteTableIds": [],
    "Groups": [
      {
        "GroupName": "default",
        "GroupId": "sg-1a2b3c4d"
      }
    ],
    "VpcEndpointId": "vpce-088d25a4bbf4a7abc",
    "VpcEndpointType": "Interface",
    "CreationTimestamp": "2017-09-05T20:14:41.240Z",
    "DnsEntries": [
      {
        "HostedZoneId": "Z7HUB22UULQXV",
        "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
      },
      {
        "HostedZoneId": "Z7HUB22UULQXV",
        "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
      },
      {
        "HostedZoneId": "Z1K56Z6FNPJRR",
        "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
      }
    ]
  }
}
```

或者，下列範例會建立另一個 AWS 帳戶中端點服務的界面端點 (服務提供者會提供端點服務的名稱)。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface  
--service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-  
id subnet-abababab --security-group-id sg-1a2b3c4d
```

在傳回的輸出中，記下 `DnsName` 欄位。您可以使用這些 DNS 名稱存取 AWS 服務。

使用適用於 Windows PowerShell 的 AWS 工具 說明可用的服務並建立 VPC 端點

- [Get-EC2VpcEndpointService](#)
- [New-EC2VpcEndpoint](#)

使用 API 說明可用的服務並建立 VPC 端點

- [DescribeVpcEndpointServices](#)
- [CreateVpcEndpoint](#)

## 檢視界面端點

在您建立界面端點之後，即可檢視其相關資訊。

### Console

使用主控台檢視界面端點的相關資訊

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的界面端點。
3. 若要檢視界面端點的相關資訊，請選擇 Details (詳細資訊)。DNS Names (DNS 名稱) 欄位會顯示用來存取服務的 DNS 名稱。
4. 若要檢視已在其中建立界面端點的子網路，以及每個子網路中端點網路界面的 ID，請選擇 Subnets (子網路)。
5. 若要檢視與端點網路界面建立關聯的安全群組，請選擇 Security Groups (安全群組)。

### Command line

使用 AWS CLI 說明界面端點

- 您可以使用 [describe-vpc-endpoints](#) 命令來說明端點。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

使用適用於 PowerShell 的 AWS 工具 或 API 說明 VPC 端點

- [Get-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的工具)
- [DescribeVpcEndpoints](#) (Amazon EC2 查詢 API)

## 建立和管理界面端點的通知

您可以建立通知，於界面端點發生特定事件時接收提醒。例如，服務提供者接受界面端點時，您可以接收電子郵件。若要建立通知，您必須建立 [Amazon SNS 主題](#) 與通知的關聯。您可以訂閱 SNS 主題，在端點事件發生時收到電子郵件通知。

您用於通知的 Amazon SNS 主題必須有主題政策，允許 Amazon VPC 端點服務代您發佈通知。確定您的主題政策中包含下列陳述式。如需詳細資訊，請參閱 Amazon Simple Notification Service 開發人員指南 中的 [Amazon SNS 的 Identity and Access Management](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

## Console

### 建立界面端點的通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的界面端點。
3. 選擇 Actions (動作)、Create notification (建立通知)。
4. 選擇要與通知建立關聯的 SNS 主題 ARN。
5. 針對 Events (事件)，選取要接收通知的端點事件。
6. 選擇 Create Notification (建立通知)。

在您建立通知後，您可以變更與通知建立關聯的 SNS 主題。您也可以為通知指定不同的端點事件。

### 修改端點服務的通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的界面端點。
3. 選擇 Actions (動作)、Modify Notification (修改通知)。
4. 指定 SNS 主題的 ARN，並視需要變更端點事件。
5. 選擇 Modify Notification (修改通知)。

您可以刪除不再需要的通知。

### 刪除通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的界面端點。
3. 選擇 Actions (動作)、Delete notification (刪除通知)。
4. 選擇 Yes, Delete (是，刪除)。

## Command line

### 使用 AWS CLI 建立與管理通知

1. 如要建立界面端點的通知，請使用 [create-vpc-endpoint-connection-notification](#) 命令。指定 SNS 主題的 ARN、要通知的事件，以及端點的 ID，如下範例所示。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
```

2. 如要檢閱您的通知，請使用 `describe-vpc-endpoint-connection-notifications` 命令。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

3. 如要變更通知的 SNS 主題或端點事件，請使用 `modify-vpc-endpoint-connection-notification` 命令。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-arn arn:aws:sns:us-east-2:123456789012:mytopic
```

4. 如要刪除通知，請使用 `delete-vpc-endpoint-connection-notifications` 命令。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-ids vpce-nfn-008776de7e03f5abc
```

## 透過界面端點存取服務

在您建立界面端點之後，即可透過端點 URL 對支援的服務提交請求。您可以使用下列項目：

- 如果您已啟用端點的私有 DNS (私有託管區域，只適用於 AWS 服務和 AWS Marketplace 合作夥伴服務)，則為區域 AWS 服務的預設 DNS 主機名稱。例如，`ec2.us-east-1.amazonaws.com`。
- 我們針對界面端點所產生的端點特定區域 DNS 主機名稱。主機名稱會在其名稱中包含唯一端點識別符、服務識別符、區域和 `vpce.amazonaws.com`。例如，`vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com`。
- 我們針對可使用端點之每個可用區域，所產生的端點特定區域 DNS 主機名稱。主機名稱會在其名稱中包含可用區域。例如，`vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com`。如果您的架構隔離可用區域 (例如為了故障包容或減少區域數據傳輸成本)，您可以使用此選項。

區域 DNS 主機名稱請求的目標設為服務提供者帳戶中的對應可用區域位置，其可用區域名稱可能與您的帳戶不同。如需詳細資訊，請參閱 [區域與可用區域的概念](#)。

- VPC 中端點網路界面的私有 IP 地址。

若要取得地區和區域 DNS 名稱，請參閱 [檢視界面端點](#) (p. 275)。

例如，在您有 Elastic Load Balancing 界面端點的子網路以及您尚未啟用私有 DNS 選項的子網路，請從執行個體使用下列 AWS CLI 命令，以說明負載平衡器。此命令使用端點特定的區域 DNS 主機名稱，使用界面端點提出請求。

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

如果您啟用私有 DNS 選項，則不需要在請求中指定端點 URL。AWS CLI 會使用區域之 AWS 服務的預設端點 (`elasticloadbalancing.us-east-1.amazonaws.com`)。

## 修改界面端點

您可以修改界面端點的下列屬性：

- 界面端點所在的子網路



- 與端點網路界面相關聯的安全性群組
- 此標籤
- 私有 DNS 選項

#### Note

當您啟用私有 DNS 時，私有 IP 地址可能需要幾分鐘才能使用。

- 端點策略 (如果服務支援)

如果您移除界面端點的子網路，則會刪除子網路中的對應端點網路界面。

#### Console

##### 變更界面端點的子網路

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取界面端點。
3. 選擇 Actions (動作)、Manage Subnets (管理子網路)。
4. 視需要選取或取消選取子網路，然後選擇 Modify Subnets (修改子網路)。

##### 新增或移除要與界面端點建立關聯的安全群組

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取界面端點。
3. 選擇 Actions (動作)、Manage security groups (管理安全群組)。
4. 視需要選取或取消選取安全群組，然後選擇 Save (儲存)。

##### 若要新增或移除界面端點標籤

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 Endpoints (端點)。
3. 選取界面端點並選擇 Actions (動作)、Add/Edit Tags (新增/編輯標籤)。
4. 新增或移除標籤。

[新增標籤] 選擇 Create tag (建立標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 對於 Value (值)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

##### 修改私有 DNS 選項

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取界面端點。
3. 選擇 Actions (動作)、Modify Private DNS names (修改私有 DNS 名稱)。
4. 視需要啟用或停用此選項，並選擇 Modify Private DNS names (修改私有 DNS 名稱)。

##### 更新端點政策

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取界面端點。

3. 選擇 Actions (動作)、Edit policy (編輯政策)。
4. 選擇 Full Access (完整存取) 以允許服務的完整存取權，或選擇 Custom (自訂) 並指定自訂政策。選擇 Save (儲存)。

#### Command line

若要使用 AWS CLI 修改 VPC 端點

1. 使用 [describe-vpc-endpoints](#) 命令來取得界面端點的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 下列範例使用 [modify-vpc-endpoint](#) 命令將子網路 subnet-aabb1122 新增至界面端點。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-id subnet-aabb1122
```

使用 適用於 Windows PowerShell 的 AWS 工具 或 API 修改 VPC 端點

- [Edit-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的 AWS 工具)
- [ModifyVpcEndpoint](#) (Amazon EC2 查詢 API)

若要使用 適用於 Windows PowerShell 的 AWS 工具 或 API 移除 VPC 端點

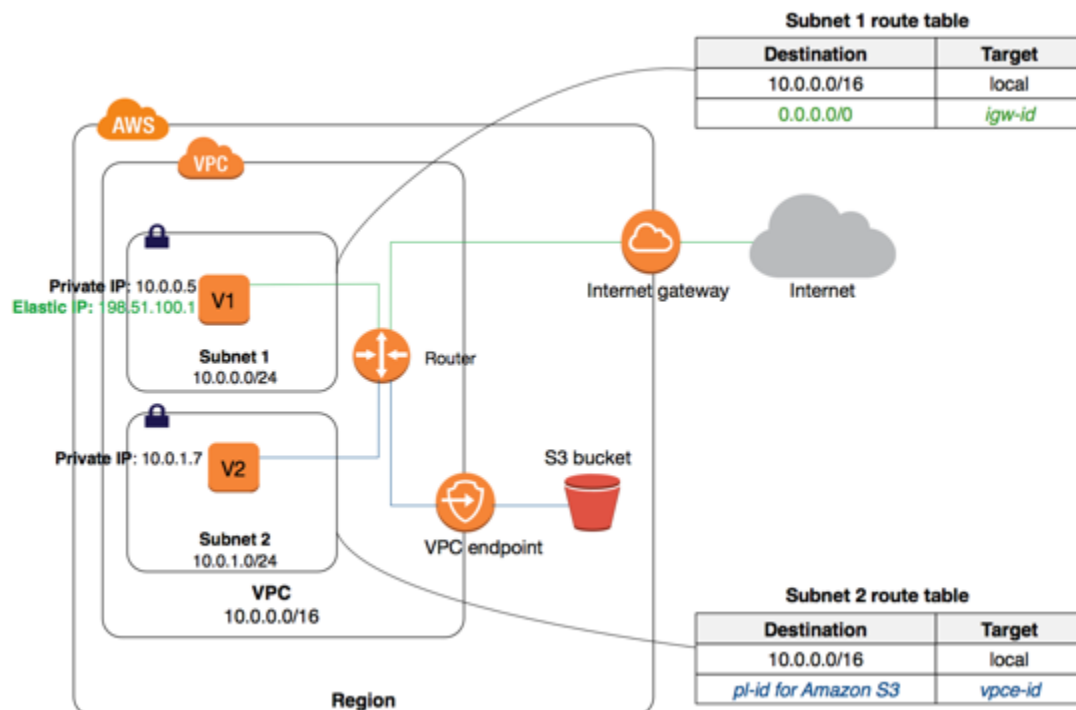
- [tag-resource](#) (AWS CLI)
- [TagResource](#) (適用於 Windows PowerShell 的 AWS 工具)
- [untag-resource](#) (AWS CLI)
- [TagResource](#) (適用於 Windows PowerShell 的 AWS 工具)

## 閘道 VPC 端點

若要建立和設定閘道端點，請遵循下列一般步驟：

1. 指定要在其中建立端點的 VPC，以及您要連線的服務。AWS 管理的字首清單所識別的服務 — 區域之服務的名稱和 ID。AWS 字首清單 ID 使用 p1-xxxxxxx 形式，而 AWS 字首清單名稱使用 "com.amazonaws.##.##" 形式。使用 AWS 字首清單名稱 (服務名稱) 建立端點。
2. 將端點政策附加至端點，以允許存取您要連線的部分或所有服務。如需詳細資訊，請參閱「[使用 VPC 端點政策](#) (p. 292)」。
3. 指定一個或多個路由表來建立路由至服務。路由表控制 VPC 與其他服務之間的流量路由。每個路由表相關聯的子網路可以存取端點，從這些子網路中之執行個體的流量即可透過端點路由至服務。

在下圖中，子網路 2 中的執行個體可以透過閘道端點存取 Amazon S3。



例如，您可以在多個服務的單一 VPC 中建立多個端點。您也可以為單一服務建立多個端點，並使用不同的路由表，於同個服務對不同的子網路行使不一樣的存取政策。

在您建立端點之後，即可修改連接至端點的端點政策，以及新增或移除端點所使用的路由表。

#### 內容

- [閘道端點的定價 \(p. 280\)](#)
- [閘道端點的路由 \(p. 280\)](#)
- [閘道端點限制 \(p. 282\)](#)
- [Amazon S3 的端點 \(p. 283\)](#)
- [Amazon DynamoDB 的端點 \(p. 287\)](#)
- [建立閘道端點 \(p. 289\)](#)
- [修改安全群組 \(p. 290\)](#)
- [修改閘道端點 \(p. 291\)](#)
- [新增或移除閘道端點標籤 \(p. 292\)](#)

## 閘道端點的定價

使用閘道端點不需額外付費。需支付標準數據傳輸與資源使用費。如需定價的詳細資訊，請參閱「[Amazon EC2 定價](#)」。

## 閘道端點的路由

當您建立或修改端點時，會指定用以透過端點存取服務的 VPC 路由表。路由會自動新增至所有路由表，其中路由表具有指定服務 AWS 字首清單 ID (p1-xxxxxxx) 的目標 (destination)，以及具有端點 ID (vpce-xxxxxxx) 的目標 (target)，例如：

目的地	目標
10.0.0.0/16	區域
pl-1a2b3c4d	vpce-11bb22cc

AWS 字首清單 ID 邏輯上代表服務所使用之公有 IP 地址的範圍。與指定路由表相關聯子網路中的所有執行個體，都會自動使用端點來存取服務。未與指定路由表建立關聯的子網路則不會使用端點。這可讓您的端點自其他子網路中的資源隔離。

若要檢視服務的目前公有 IP 地址範圍，您可以使用 `describe-prefix-lists` 命令中的 [AWS IP 地址範圍](#)。

#### Note

服務的公有 IP 地址範圍會不時變更。請先將之納入考量，再根據服務目前的 IP 地址範圍來做出路由或其他決策。

適用的規定如下：

- 您可以在路由表中讓多個端點路由至不同服務，也可以在不同的路由表中讓多個端點路由至相同服務。但您無法在單一路由表中讓多個端點路由至相同服務。例如，如果您的 VPC 中建立兩個端點至 Amazon S3，則您不能在相同的路由表中為兩個端點建立兩個端點路由。
- 您無法使用路由表 API，或使用 Amazon VPC 主控台內的 Route Tables (路由表) 頁面，來明確地新增、修改或刪除路由表中的端點路由。您只能透過建立路由表與端點的關聯，來新增端點路由。若要變更與您端點建立關聯的路由表，您可以 [修改端點](#) (p. 291)。
- 當您從端點移除路由表關聯時 (修改端點) 或刪除端點時，會自動刪除端點路由。

我們會使用最具體且符合流量的路由，從而判斷如何路由流量 (最長的字首相符)。如果您的路由表中有一個適用於所有網際網路流量 (0.0.0.0/0) 的現有路由，且流量指向網際網路開道，則該端點路由對於所有以服務為目標的流量具有優先權，因為服務的 IP 地址範圍比 0.0.0.0/0 更具體。所有其他網際網路流量都會流向網際網路開道，包括以其他區域中的服務為目標的流量。

不過，如果您有 IP 地址範圍的現有更具體路由，而 IP 地址範圍指向網際網路開道或 NAT 裝置，則這些路由具有優先權。如果您有以 IP 地址範圍為目標的現有路由，而此 IP 地址範圍與服務所使用的 IP 地址範圍相同，則您的路由具有優先權。

範例：路由表中的端點路由

在此情況下，您的路由表中有適用於所有網際網路流量 (0.0.0.0/0) 且指向網際網路開道的現有路由。來自以另一個 AWS 服務為目標之子網路的所有流量都會使用網際網路開道。

目的地	目標
10.0.0.0/16	區域
0.0.0.0/0	igw-1a2b3c4d

您可以建立支援之 AWS 服務的端點，並建立路由表與端點的關聯。端點路由會自動新增至目標為 pl-1a2b3c4d 的路由表 (假設這代表您已建立端點的服務)。現在，來自以相同區域中該 AWS 服務為目標之子網路的所有流量都會前往端點，而不會前往網際網路開道。所有其他網際網路流量都會流向網際網路開道，包括以其他服務為目標的流量，以及以其他區域中 AWS 服務為目標的流量。

目的地	目標
10.0.0.0/16	區域

目的地	目標
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

#### 範例：調整端點的路由表

在此情況下，54.123.165.0/24 是在 Amazon S3 IP 地址範圍中，而且您已設定路由表，讓子網路中的執行個體透過網際網路閘道與 Amazon S3 儲存貯體通訊。您已新增路由，其中以 54.123.165.0/24 做為目的地，且以網際網路閘道做為目標。您接著可以建立端點，並建立此路由表與端點的關聯。端點路由會自動新增至路由表。您接著可以使用 [describe-prefix-lists](#) 命令來檢視 Amazon S3 的 IP 地址範圍。範圍為 54.123.160.0/19，此範圍較不具體（相較於指向網際網路閘道的範圍）。這表示以 54.123.165.0/24 IP 地址範圍為目標的任何流量都會持續使用網際網路閘道，而且不會使用端點（只要這保有 Amazon S3 的公有 IP 地址範圍）。

目的地	目標
10.0.0.0/16	區域
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

若要確保以相同區域中 Amazon S3 為目標的所有流量是透過端點路由，您必須調整路由表中的路由。若要執行此作業，您可以刪除網際網路閘道的路由。現在，所有流向相同區域中 Amazon S3 的流量會使用端點，而且與路由表建立關聯的子網路是私有子網路。

目的地	目標
10.0.0.0/16	區域
pl-1a2b3c4d	vpce-11bb22cc

## 閘道端點限制

若要使用閘道端點，您需要知道目前的限制：

- 您無法在網路 ACL 的傳出規則中使用 AWS 字首清單 ID，來允許或拒絕流向端點中指定之服務的傳出流量。如果您的網路 ACL 規則限制流量，則您必須改為指定服務的 CIDR 區塊 (IP 地址範圍)。不過，您可以在傳出安全群組規則中使用 AWS 字首清單 ID。如需更多詳細資訊，請參閱 [安全群組 \(p. 293\)](#)。
- 只在相同的區域內支援端點。您無法在 VPC 和位於不同區域內的服務之間建立端點。
- 端點僅支援 IPv4 流量。
- 您無法在 VPC 與 VPC 之間或是服務與服務之間轉移端點。
- 每個 VPC 可建立的端點數量都有配額。如需更多詳細資訊，請參閱 [VPC 端點 \(p. 323\)](#)。
- 端點連線不能延伸出 VPC。VPC 中 VPN 連線、VPC 對等連線、transit gateway、AWS Direct Connect 連線或 ClassicLink 連線另一側的資源無法使用端點與端點服務中的資源通訊。
- 您必須在 VPC 中啟用 DNS 解析，或者如果您使用自有的 DNS 伺服器，請確定向必要服務 (例如 Amazon S3) 提出的 DNS 請求會正確地解析為 AWS 所維護的 IP 地址。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 [搭配使用 DNS 與 VPC \(p. 256\)](#) 與 [AWS IP 地址範圍](#)。
- 檢閱您端點服務的服務特定限制。

如需 Amazon S3 特有規則和限制的詳細資訊，請參閱 [Amazon S3 的端點 \(p. 283\)](#)。

如需 DynamoDB 特有規則和限制的詳細資訊，請參閱 [Amazon DynamoDB 的端點 \(p. 287\)](#)。

## Amazon S3 的端點

如果您已從 VPC 設定對 Amazon S3 資源的存取權，您即可在設定端點之後繼續使用 Amazon S3 DNS 名稱來存取這些資源。但是，請記得下列事項：

- 您端點的政策可控制如何使用端點來存取 Amazon S3 資源。預設政策允許 VPC 內的任何使用者或服務使用任意 AWS 帳戶的登入資料來存取所有 Amazon S3 資源，包括 AWS 帳戶的 Amazon S3 資源，而帳戶不是與 VPC 建立關聯的帳戶。如需詳細資訊，請參閱 [使用 VPC 端點 控制服務的存取 \(p. 292\)](#)。
- Amazon S3 所接收之受影響子網路中執行個體的來源 IPv4 地址，會從公有 IPv4 地址變更為 VPC 中的私有 IPv4 地址。端點會切換網路路由，以及中斷連線開啟的 TCP 連線。使用公有 IPv4 地址的先前連線不會繼續。建議您在建立或修改端點時不要執行重要任務，或者建議您進行測試，確保軟體在斷線之後可以自動重新連線至 Amazon S3。
- 您無法使用 IAM 政策或儲存貯體政策來允許從 VPC IPv4 CIDR 範圍存取 (私有 IPv4 地址範圍)。VPC CIDR 區塊可以重疊或相同，這樣可能會導致未預期的結果。因此，您無法在透過 VPC 端點請求 Amazon S3 的 IAM 政策中使用 `aws:SourceIp` 條件。這適用於使用者和角色的 IAM 政策，以及任何儲存貯體政策。如果陳述式包含 `aws:SourceIp` 條件，則值不符合任何提供的 IP 地址或範圍。相反地，您可以執行下列作業：
  - 使用路由表來控制哪些執行個體可以透過端點來存取 Amazon S3 中的資源。
  - 對於儲存貯體政策，您可以限制存取特定端點或特定 VPC。如需更多詳細資訊，請參閱 [使用 Amazon S3 儲存貯體政策 \(p. 286\)](#)。
- 端點目前不支援跨區域請求。請確定您在與儲存貯體相同的區域中建立端點。您可以使用 Amazon S3 主控台或使用 `get-bucket-location` 命令來找到儲存貯體的位置。使用區域特定 Amazon S3 端點來存取儲存貯體，例如 `mybucket.s3-us-west-2.amazonaws.com`。如需 Amazon S3 區域特定端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 [Amazon Simple Storage Service \(S3\)](#)。如果您使用 AWS CLI 向 Amazon S3 提出請求，請將預設區域設為與您儲存貯體相同的區域，或在請求中使用 `--region` 參數。

### Note

將 Amazon S3 的美國標準區域視為映射至 `us-east-1` 區域。

- 目前只有端點才支援 IPv4 流量。

在您於 Amazon S3 使用端點之前，請確定您已閱讀下列一般限制：[閘道端點限制 \(p. 282\)](#)。如需建立和檢視 S3 儲存貯體的相關資訊，請參閱 Amazon Simple Storage Service 主控台使用者指南中的 [如何建立 S3 儲存貯體](#) 和 [如何檢視 S3 儲存貯體的屬性](#)。

如果您在 VPC 中使用其他 AWS 服務，端點可能會將 S3 儲存貯體用於特定任務。請確定您的端點政策允許完整存取 Amazon S3 (預設政策)，或允許存取這些服務所使用的特定儲存貯體。或者，只在所有這些服務未使用的子網路中建立端點，以允許服務繼續使用公有 IP 地址來存取 S3 儲存貯體。

下表列出端點可能影響的 AWS 服務，以及每項服務的特定資訊。

AWS 服務	注意
Amazon AppStream 2.0	您的端點政策必須允許存取 AppStream 2.0 用來存放使用者內容的特定儲存貯體。如需詳細資訊，請參閱 Amazon AppStream 2.0 管理指南 中的 <a href="#">將 Amazon S3 VPC 端點用於主資料夾和應用程式設定持續性</a> 。
AWS CloudFormation	如果您 VPC 中的資源必須回應等待條件或自訂資源請求，則端點政策必須允許至少存取這些資源所



AWS 服務	注意
	使用的特定儲存貯體。如需詳細資訊，請參閱 <a href="#">設定 AWS CloudFormation 的 VPC 端點</a> 。
CodeDeploy	您的端點政策必須允許完整存取 Amazon S3，或允許存取您已為 CodeDeploy 部署所建立的任何 S3 儲存貯體。
Elastic Beanstalk	您的端點政策必須允許至少存取用於 Elastic Beanstalk 應用程式的任何 S3 儲存貯體。如需詳細資訊，請參閱 AWS Elastic Beanstalk 開發人員指南中的 <a href="#">於 Amazon S3 使用 Elastic Beanstalk</a> 。
Amazon EMR	您的端點政策必須允許存取 Amazon EMR 所使用的 Amazon Linux 儲存庫和其他儲存貯體。如需詳細資訊，請參閱 Amazon EMR 管理指南中的 <a href="#">私有子網路的 Amazon S3 政策下限</a> 。
AWS OpsWorks	您的端點政策必須允許至少存取 AWS OpsWorks 所使用的特定儲存貯體。如需詳細資訊，請參閱 AWS OpsWorks User Guide 中的 <a href="#">在 VPC 中執行堆疊</a> 。
AWS Systems Manager	<p>您的端點政策必須允許存取修補程式管理員所使用的 Amazon S3 儲存貯體，以便在您的 AWS 區域修補基準操作。這些儲存貯體包含修補程式基準服務所擷取並在執行個體上執行的程式碼。如需詳細資訊，請參閱 AWS Systems Manager 使用者指南中的<a href="#">建立 Virtual Private Cloud 端點</a>。</p> <p>如需 SSM 代理程式對此操作所要求的 S3 儲存貯體許可清單，請參閱 AWS Systems Manager 使用者指南中的<a href="#">SSM 代理程式的最低 S3 儲存貯體許可</a>。</p>
Amazon Elastic Container Registry	您的端點政策必須允許存取 Amazon ECR 用來的儲存 Docker 影像 layer 的 Amazon S3 儲存貯體。如需詳細資訊，請參閱 Amazon Elastic Container Registry 使用者指南中的 <a href="#">Amazon ECR 的最低 Amazon S3 儲存貯體許可</a> 。
Amazon WorkDocs	如果您在 Amazon WorkSpaces 中使用 Amazon WorkDocs 用戶端或是 EC2 執行個體，則端點政策必須允許完整存取 Amazon S3。
Amazon WorkSpaces	Amazon WorkSpaces 未直接相依於 Amazon S3。不過，如果您提供具有網際網路存取權的 Amazon WorkSpaces 使用者，則請注意其他公司的網站、HTML 電子郵件和網際網路服務可能相依於 Amazon S3。請確定您的端點政策允許完整存取 Amazon S3，以允許這些服務繼續正常運作。

您的 VPC 與 S3 儲存貯體之間的流量會在 Amazon 網路的範圍內。

## 使用 Amazon S3 的端點政策

下列範例端點政策用於存取 Amazon S3。如需詳細資訊，請參閱「[使用 VPC 端點 政策 \(p. 292\)](#)」。符合業務需求的政策限制，由使用者決定。例如，您可以指定區域 ("packages.us-west-1.amazonaws.com") 來避免不明確的 S3 儲存貯體名稱。



## Important

所有類型的政策 — IAM 使用者政策、端點政策、S3 儲存貯體政策和 Amazon S3 ACL 政策 (如果有的話) 都必須授予成功存取 Amazon S3 的必要許可。

### Example 範例：限制特定儲存貯體的存取

您可以建立政策，以限制只存取特定 S3 儲存貯體。如果您在 VPC 中具有使用 S3 儲存貯體的其他 AWS 服務，這會十分有用。下列政策範例僅限存取 `my_secure_bucket`。

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3::my_secure_bucket",
        "arn:aws:s3::my_secure_bucket/*"
      ]
    }
  ]
}
```

### Example 範例：啟用 Amazon Linux AMI 儲存庫的存取

Amazon Linux AMI 儲存庫是每個區域中的 Amazon S3 儲存貯體。如果您想要 VPC 中的執行個體透過端點存取儲存庫，請建立啟用存取這些儲存貯體的端點政策。

下列政策允許存取 Amazon Linux 儲存庫。

您需要將 `region` 更換為 AWS 區域，例如 `us-east-1`。

```
{
  "Statement": [
    {
      "Sid": "AmazonLinuxAMIRepositoryAccess",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3::packages.region.amazonaws.com/*",
        "arn:aws:s3::repo.region.amazonaws.com/*"
      ]
    }
  ]
}
```

下列政策允許存取 Amazon Linux 2 儲存庫。

您需要將 `region` 更換為 AWS 區域，例如 `us-east-1`。

```
{
  "Statement": [
    {
```

```

        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.region.amazonaws.com/*"
        ]
    }
}

```

## 使用 Amazon S3 儲存貯體政策

您可以使用儲存貯體政策，從特定端點或特定 VPC 控制對儲存貯體的存取。

您無法在透過 VPC 端點請求 Amazon S3 的儲存貯體政策中使用 `aws:SourceIp` 條件。條件不符合任何指定的 IP 地址或 IP 地址範圍，而且當您請求 Amazon S3 儲存貯體時，可能會有非預期的效果。例如：

- 您儲存貯體政策的 Deny 效果和 NotIpAddress 條件是要授予僅來自單一或有限 IP 地址範圍的存取權。對於透過端點請求儲存貯體，NotIpAddress 條件一律必須相符，並且基於政策中之其他限制相符的假設，套用陳述式的效果。儲存貯體的存取會遭拒。
- 您儲存貯體政策的 Deny 效果和 IpAddress 條件是要拒絕僅存取單一或有限 IP 地址範圍。對於透過端點請求儲存貯體，條件不相符，而且不會套用陳述式。允許存取儲存貯體，但假設有其他陳述式允許在沒有 IpAddress 條件的情況下存取。

請改為調整儲存貯體政策，以限制存取特定 VPC 或特定 VPC 端點。

如需 Amazon S3 之儲存貯體政策的詳細資訊，請參閱 Amazon Simple Storage Service 開發人員指南 中的 [使用儲存貯體政策和使用者政策](#)。

以下是限制存取特定 VPC 端點或特定 VPC 的儲存貯體政策範例。若要讓 IAM 使用者能夠使用儲存貯體政策，您必須授予他們使用 `s3:GetBucketPolicy` 和 `s3:PutBucketPolicy` 動作的許可。

### Example 範例：限制特定端點的存取

下列 S3 儲存貯體政策範例只允許從端點 `vpce-1a2b3c4d` 存取特定儲存貯體 `my_secure_bucket`。如果未使用指定的端點，政策會拒絕所有對儲存貯體的存取。`aws:sourceVpce` 條件用來指定端點。`aws:sourceVpce` 條件不需要 VPC 端點資源的 ARN，其只需要端點 ID。

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::my_secure_bucket",
        "arn:aws:s3:::my_secure_bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}

```

```
}
```

#### Example 範例：限制特定 VPC 的存取

您可以使用 `aws:sourceVpc` 條件，建立可限制存取特定 VPC 的儲存貯體政策。如果您在相同的 中設定多個 VPC 端點，而且想要管理所有端點的 S3 儲存貯體存取，則這十分有用。下列政策範例允許 VPC `vpc-111bbb22` 存取 `my_secure_bucket` 和其物件。如果未使用指定的 VPC，政策會拒絕所有對儲存貯體的存取。`aws:sourceVpc` 條件不需要 VPC 資源的 ARN，其只需要 VPC ID。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3::my_secure_bucket",
                   "arn:aws:s3::my_secure_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

## Amazon DynamoDB 的端點

若您已設定從您的 VPC 存取 DynamoDB 資料表，您可以在設定完閘道端點之後繼續像平常一樣存取資料表。但是，請記得下列事項：

- 您端點的政策可控制如何使用端點來存取 DynamoDB 資源。預設政策允許 VPC 中任何使用者或服務使用任何 AWS 帳戶的登入資料存取任何 DynamoDB 資源。如需詳細資訊，請參閱 [使用 VPC 端點 控制服務的存取 \(p. 292\)](#)。
- DynamoDB 不支援以資源為基礎的政策 (例如：以資料表為基礎)。DynamoDB 的存取由端點政策和個別 IAM 使用者和角色的 IAM 政策控制。
- 您無法透過 VPC 端點存取 Amazon DynamoDB 串流。
- 端點目前不支援跨區域請求。請確定您在與 DynamoDB 資料表相同的區域中建立端點。
- 若您使用 AWS CloudTrail 記錄 DynamoDB 操作的日誌，日誌檔案會包含 VPC 中 EC2 執行個體的私有 IP 地址，以及任何透過端點執行之動作的端點 ID。
- 受影響子網路中執行個體的來源 IPv4 地址，會從公有 IPv4 地址變更為 VPC 中的私有 IPv4 地址。端點會切換網路路由，以及中斷開啟的 TCP 連線。使用公有 IPv4 地址的先前連線不會繼續。建議您未在建立或修改端點時執行任何重要任務，或者建議您測試以確保軟體在斷線之後可以自動重新連線至 DynamoDB。

在您於 DynamoDB 使用端點之前，請確定您已閱讀下列一般限制：[閘道端點限制 \(p. 282\)](#)。

如需建立閘道 VPC 端點的詳細資訊，請參閱[閘道 VPC 端點 \(p. 279\)](#)。

### 使用 DynamoDB 的端點政策

端點政策是您可以附加至端點的 IAM 政策，以允許存取您要連線的部分或所有服務。下列範例端點政策用於存取 DynamoDB。

## Important

所有類型的政策 — IAM 使用者政策和端點政策都必須授予成功存取 DynamoDB 的必要許可。

### Example 範例：唯讀存取

您可以建立政策，將動作限制在僅能透過 VPC 端點列出和說明 DynamoDB 資料表。

```
{
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

### Example 範例：限制特定資料表的存取

您可以建立政策，限制特定 DynamoDB 資料表的存取。在此範例中，端點政策只會允許存取 StockTable。

```
{
  "Statement": [
    {
      "Sid": "AccessToSpecificTable",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"
    }
  ]
}
```

## 使用 IAM 政策控制 DynamoDB 的存取

您可以為您的 IAM 使用者、群組或角色建立 IAM 政策，限制只能從特定 VPC 端點存取 DynamoDB 資料表。若要執行此作業，您可以在您的 IAM 政策中針對資料表資源使用 `aws:sourceVpce` 條件鍵。

如需管理 DynamoDB 存取的詳細資訊，請參閱 Amazon DynamoDB 開發人員指南 中的 [Amazon DynamoDB 身分驗證及存取控制](#)。

### Example 範例：限制來自特定端點的存取

在此範例中，除非透過 `vpce-11aa22bb` 端點進行存取，否則會拒絕使用者使用 DynamoDB 資料表的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessFromSpecificEndpoint",
      "Action": "dynamodb:*",
      "Effect": "Deny",
      "Resource": "arn:aws:dynamodb:region:account-id:table/*",
      "Condition": { "StringNotEquals" : { "aws:sourceVpce": "vpce-11aa22bb" } }
    }
  ]
}
```

## 建立閘道端點

若要建立端點，您必須指定要在其中建立端點的 VPC，以及要與其建立連線的服務。

### 使用主控台建立閘道端點

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，Create Endpoint (建立端點)。
3. 針對 Service Name (服務名稱)，選擇要連線的服務。若要建立 DynamoDB 或 Amazon S3 的閘道端點，請確定 Type (類型) 欄指出 Gateway (閘道)。
4. 完成下列資訊，然後選擇 Create endpoint (建立端點)。
  - 針對 VPC，選取要在其中建立端點的 VPC。
  - 針對 Configure route tables (設定路由表)，選取要供端點使用的路由表。我們會自動新增路由，將以服務為目標的流量指向所選取之路由表的端點。
  - 針對 Policy (政策)，選擇政策類型。您可以保留預設選項 Full Access (完整存取)，允許完整存取服務。或者，您可以選取 Custom (自訂)，然後使用 AWS 政策產生器來建立自訂政策，或是在政策視窗中輸入您自己的政策。
  - (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

在您建立端點之後，即可檢視其相關資訊。

### 使用主控台檢視閘道端點的相關資訊

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的端點。
3. 若要檢視端點的相關資訊，請選擇 Summary (摘要)。您可以在 Service (服務) 方塊中取得服務的 AWS 字首清單名稱。
4. 若要檢視端點所使用之路由表的相關資訊，請選擇 Route Tables (路由表)。
5. 若要檢視連接至端點的 IAM 政策，請選擇 Policy (政策)。

#### Note

Policy (政策) 標籤只會顯示端點政策。針對具有端點使用許可的 IAM 使用者，標籤內不會顯示任何 IAM 政策的資訊。也不會顯示服務特定政策 (例如 S3 儲存貯體政策)。

## 使用 AWS CLI 建立和檢視端點

1. 使用 [describe-vpc-endpoint-services](#) 命令，以取得可用服務清單。在傳回的輸出中，記下要連線之服務的名稱。serviceType 欄位會指出您透過界面端點還是閘道端點連線至服務。

```
aws ec2 describe-vpc-endpoint-services
```

```
{
  "serviceDetailSet": [
    {
      "serviceType": [
        {
          "serviceType": "Gateway"
        }
      ]
    }
  ]
}
```

2. 若要建立 Amazon S3 這類項目的閘道端點，請使用 [create-vpc-endpoint](#) 命令，並指定 VPC ID、服務名稱以及將使用端點的路由表。您可以選擇性地使用 --policy-document 參數指定自訂政策，以控制對服務的存取。如果未使用參數，則會連接允許完整存取服務的預設政策。

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-east-1.s3 --route-table-ids rtb-11aa22bb
```

3. 使用 [describe-vpc-endpoints](#) 命令來說明端點。

```
aws ec2 describe-vpc-endpoints
```

## 使用適用於 Windows PowerShell 的 AWS 工具 或 API 說明可用的服務

- [Get-EC2VpcEndpointService](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DescribeVpcEndpointServices](#) (Amazon EC2 查詢 API)

## 使用適用於 Windows PowerShell 的 AWS 工具 或 API 建立 VPC 端點

- [New-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的 AWS 工具)
- [CreateVpcEndpoint](#) (Amazon EC2 查詢 API)

## 使用適用於 Windows PowerShell 的 AWS 工具 或 API 說明 VPC 端點

- [Get-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DescribeVpcEndpoints](#) (Amazon EC2 查詢 API)

## 修改安全群組

如果與執行個體建立關聯的 VPC 安全群組限制傳出流量，您必須新增規則，允許以 AWS 服務為目標的流量離開執行個體。

### 新增閘道端點的傳出規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選取 VPC 安全群組，並選擇 Outbound Rules (傳出規則) 標籤，然後選擇 Edit (編輯)。

4. 從 Type (類型) 清單選取流量類型，然後在需要時輸入連接埠範圍。例如，如果您使用執行個體從 Amazon S3 擷取物件，請從 Type (類型) 清單選擇 HTTPS (HTTPS)。
5. 針對 Destination (目的地)，請開始輸入 p1- 以顯示可用 AWS 服務的前置詞清單 ID 和名稱清單。選擇 AWS 服務的字首清單 ID，或是進行輸入。
6. 選擇 Save (儲存)。

如需安全群組的詳細資訊，請參閱 [VPC 的安全群組 \(p. 138\)](#)。

使用命令列或 API 取得 AWS 服務的 AWS 字首清單名稱、ID 和 IP 地址範圍

- [describe-prefix-lists](#) (AWS CLI)
- [Get-EC2PrefixList](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DescribePrefixLists](#) (Amazon EC2 查詢 API)

## 修改閘道端點

您可以變更或移除閘道端點的政策，以及新增或移除端點所使用的路由表，藉以修改閘道端點。

變更與閘道端點建立關聯的政策

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的端點。
3. 選擇 Actions (動作)、Edit policy (編輯政策)。
4. 您可以選擇 Full Access (完整存取) 允許完整存取。或者，選擇 Custom (自訂)，然後使用 AWS 政策產生器來建立自訂政策，或是在政策視窗中輸入您自己的政策。完成後，選擇 Save (儲存)。

Note

政策變更生效可能需要幾分鐘。

新增或移除閘道端點所使用的路由表

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的端點。
3. 選擇 Actions (動作)、Manage route tables (管理路由表)。
4. 選取或取消選取必要的路由表，然後選擇 Modify Route Tables (修改路由表)。

使用 AWS CLI 修改閘道端點

1. 使用 [describe-vpc-endpoints](#) 命令來取得閘道端點的 ID。

```
aws ec2 describe-vpc-endpoints
```

2. 下列範例使用 [modify-vpc-endpoint](#) 命令建立路由表 rtb-aaa222bb 與閘道端點的關聯，並重設政策文件。

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

使用 適用於 Windows PowerShell 的 AWS 工具 或 API 修改 VPC 端點

- [Edit-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的 AWS 工具)



- [ModifyVpcEndpoint](#) (Amazon EC2 查詢 API)

## 新增或移除閘道端點標籤

標籤可供識別閘道端點。您可以新增或移除標籤。

若要新增或移除閘道端點標籤

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 Endpoints (端點)。
3. 選取閘道端點並選擇 Actions (動作)、Add/Edit Tags (新增/編輯標籤)。
4. 新增或移除標籤。

[新增標籤] 選擇 Create tag (建立標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 對於 Value (值)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

使用 適用於 Windows PowerShell 的 AWS 工具 或 API 來新增或移除標籤

- [create-tags](#) (AWS CLI)
- [CreateTags](#) (適用於 Windows PowerShell 的 AWS 工具)
- [delete-tags](#) (AWS CLI)
- [DeleteTags](#) (適用於 Windows PowerShell 的 AWS 工具)

## 使用 VPC 端點 控制服務的存取

當您建立端點時，可以將端點政策連接至閘道端點，以控制存取您要連線的服務。端點政策必須以 JSON 格式撰寫。並非所有服務都支援端點策略。

如果您使用 Amazon S3 的端點，也可以使用 Amazon S3 儲存貯體政策，從特定端點或特定 VPC 控制對儲存貯體的存取。如需詳細資訊，請參閱[使用 Amazon S3 儲存貯體政策](#) (p. 286)。

內容

- [使用 VPC 端點 政策](#) (p. 292)
- [安全群組](#) (p. 293)

## 使用 VPC 端點 政策

當您建立或修改端點時，VPC 端點 政策是您連接至端點的 IAM 資源政策。如果您未在建立端點時連接政策，則會連接預設政策以允許完整存取服務。如果服務不支援端點政策，則端點會允許服務的完整存取權。端點政策不會覆寫或取代 IAM 使用者政策或服務特定政策 (例如 S3 儲存貯體政策)。這個另行區分的政策會控制從端點到所指定之服務的存取。

您無法將一個以上的政策連接至端點。但是，您可以隨時修改政策。如果您修改政策，則變更生效需費時幾分鐘。如需編寫政策的詳細資訊，請參閱 IAM 使用者指南 中的 [IAM 政策概觀](#)。

您的端點政策就像任何 IAM 政策；不過，請記下下列各項：

- 只有與所指定之服務相關的政策部分才會作用。您無法使用端點政策來允許 VPC 中的資源執行其他動作；例如，如果您將 EC2 動作新增至 Amazon S3 之端點的端點政策，則不會生效。

- 您的政策必須包含 [Principal](#) 元素。如需相關閘道端點的其他資訊，請參閱 [閘道端點的端點政策 \(p. 293\)](#)。
- 端點政策的大小不可超過 20,480 個字元 (包含空格)。

如需支援端點政策之 AWS 服務的詳細資訊，請參閱 [the section called “可與 AWS PrivateLink 搭配使用的 AWS 服務” \(p. 314\)](#)。

## 閘道端點的端點政策

對於套用至閘道端點的端點原則，您無法將 [Principal](#) 元素限制為特定的 IAM 角色或使用者。您可指定 "\*" 來為所有的 IAM 角色或使用者授予存取權限。如果您以 "AWS": "[AWS-account-ID](#)" 或 "AWS": "arn:aws:iam::[AWS-account-ID](#):root" 格式指定 [Principal](#)，則只會將存取權授予 AWS 帳戶的根使用者，而不是帳戶的所有 IAM 使用者和角色。

若要將閘道端點的使用限制為特定主體，您可以使用端點原則中的 [Condition](#) 元素，並指定 [aws:PrincipalArn](#) 條件金鑰，例如：

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
  }
}
```

如需 Amazon S3 和 DynamoDB 的端點政策範例，請參閱下列主題：

- [使用 Amazon S3 的端點政策 \(p. 284\)](#)
- [使用 DynamoDB 的端點政策 \(p. 287\)](#)

## 安全群組

除非您特別限制傳出存取，否則根據預設，Amazon VPC 安全群組會允許所有傳出流量。

當您建立界面端點時，可以建立安全群組與 VPC 中所建立之端點網路界面的關聯。如果您未指定安全群組，將會自動建立 VPC 的預設安全群組與端點網路界面的關聯。您必須確定安全群組的規則允許端點網路界面與 VPC 中的資源 (可與服務通訊) 之間的通訊。

針對閘道端點，如果限制您安全群組的傳出規則，則您必須新增規則，允許流量從 VPC 傳出至端點中指定的服務。若要執行此作業，您可以在傳出規則中使用服務的 AWS 字首清單 ID 做為目標。如需更多詳細資訊，請參閱 [修改安全群組 \(p. 290\)](#)。

## 刪除 VPC 端點

如果您不再需要端點，可以將其刪除。刪除閘道端點也會刪除路由表中由端點使用的端點路由，但不會影響任何已經與端點所在之 VPC 建立關聯的安全群組。刪除界面端點也會刪除端點網路界面。

### 刪除端點

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints (端點)，然後選取您的端點。
3. 選擇 Actions (動作)、Delete Endpoint (刪除端點)。
4. 在確認畫面中，選擇 Yes, Delete (是，刪除)。

### 刪除 VPC 端點

- [delete-vpc-endpoints](#) (AWS CLI)

- [Remove-EC2VpcEndpoint](#) (適用於 Windows PowerShell 的 AWS 工具)
- [DeleteVpcEndpoints](#) (Amazon EC2 查詢 API)

## VPC 端點服務 (AWS PrivateLink)

您可以在您的 VPC 中建立您自己的應用程式，並將其設為具備 AWS PrivateLink 功能的服務 (稱為「端點服務」)。其他 AWS 委託人可使用[界面 VPC 端點 \(p. 266\)](#)建立由其 VPC 到您端點服務的連線。您是「服務提供者」，而建立與您服務連線的 AWS 委託人是「服務消費者」。

### 內容

- [概觀 \(p. 294\)](#)
- [端點服務可用區域的考量 \(p. 296\)](#)
- [端點服務 DNS 名稱 \(p. 296\)](#)
- [連線至內部部署的資料中心 \(p. 270\)](#)
- [透過 VPC 對等連線存取服務 \(p. 296\)](#)
- [使用 Proxy Protocol \(代理通訊協定\) 取得連線資訊 \(p. 296\)](#)
- [端點服務限制 \(p. 297\)](#)
- [建立 VPC 端點服務組態 \(p. 297\)](#)
- [為您的端點服務新增和移除許可 \(p. 298\)](#)
- [變更 網路負載平衡器 和接受設定 \(p. 300\)](#)
- [接受與拒絕界面端點連線請求 \(p. 300\)](#)
- [建立與管理端點服務的通知 \(p. 301\)](#)
- [新增或移除 VPC 端點服務標籤 \(p. 303\)](#)
- [刪除端點服務組態 \(p. 304\)](#)

## 概觀

下列為建立端點服務的一般步驟。

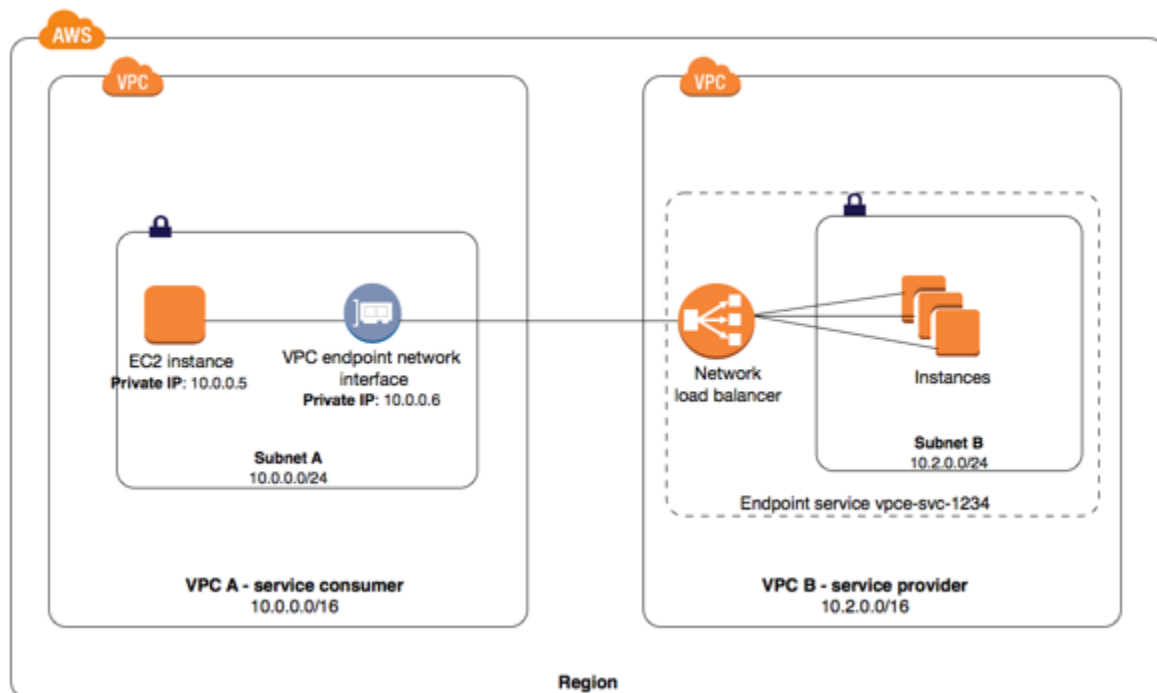
1. 在您的 VPC 中為您的應用程式建立 網路負載平衡器，然後為每個應可使用該服務的子網路 (可用區域) 設定它。網路負載平衡器會收到來自服務消費者的請求，將它路由至您的服務。如需詳細資訊，請參閱 [網路負載平衡器 使用者指南](#) 中的[網路負載平衡器入門](#)。我們建議您在區域內的所有可用區域中都設定您的服務。
2. 建立 VPC 端點服務組態並指定您的 網路負載平衡器。

下列為讓服務消費者連線到您服務的一般步驟。

1. 將許可授予特定的服務消費者 (AWS 帳戶、IAM 使用者和 IAM 角色)，建立與您端點服務的連線。
2. 已獲得許可的服務消費者會建立您服務的界面端點，有可能建立在每個您已設定服務的可用區域中。
3. 請接受界面端點連線請求，以啟用連線。根據預設，連線請求必須以手動方式接受。不過，您可以設定您端點服務的接受設定，以自動接受任何連線請求。

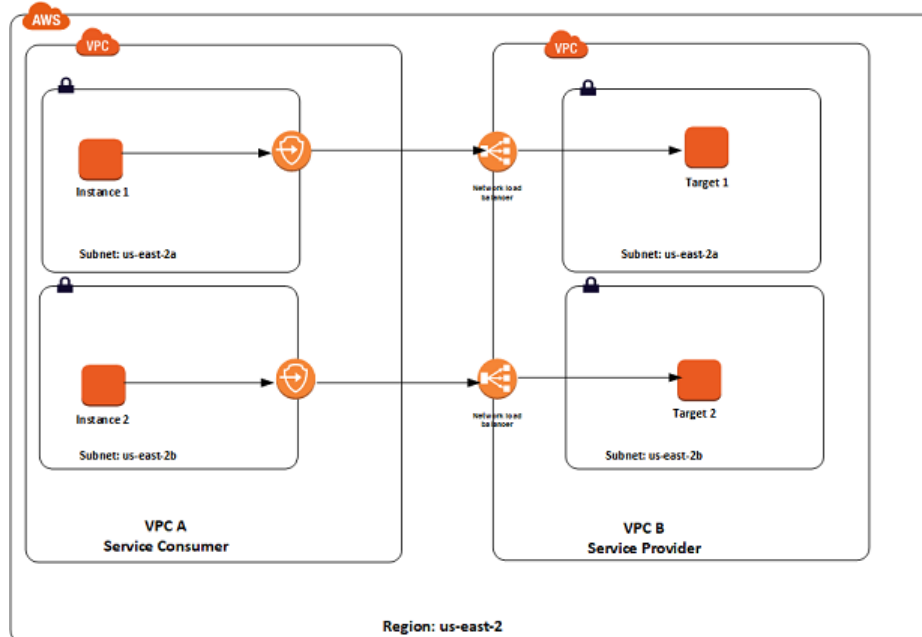
許可與接受設定的組合可幫助您控管哪些服務消費者 (AWS 委託人) 能夠存取您的服務。例如，您可將許可授予您信任的已選取委託人，自動接受所有連線請求，或者可將許可授予較多群組的委託人，以手動方式接受您信任的特定連線請求。

在下圖中，VPC B 的帳戶擁有者是服務提供者，擁有在子網路 B 之執行個體上執行的服務。VPC B 擁有者擁有與 網路負載平衡器 相關聯的服務端點 (vpce-svc-1234)，指向子網路 B 的執行個體為目標。VPC A 之子網路 A 中的執行個體使用界面端點存取子網路 B 中的服務。



至於低延遲和容錯能力，建議您使用在 AWS 區域每個可用區域都有目標的網路負載平衡器。為協助使用 [區域 DNS 主機名稱](#) (p. 277) 的服務消費者取得高可用性以存取服務，您可啟用跨區域負載平衡。跨區域負載平衡能讓負載平衡器將流量分配到所有已啟用之可用區域內的已註冊目標。如需詳細資訊，請參閱 [網路負載平衡器 使用者指南](#) 中的 [跨區負載平衡](#)。當您啟用跨區域負載平衡時，您的帳戶可能要支付區域數據傳輸費。

在下圖中，VPC B 的擁有者是服務提供者，已設定於兩個不同可用區域中具有目標的網路負載平衡器。服務消費者 (VPC A) 已在其 VPC 的相同兩個可用區域中建立界面端點。VPC A 中執行個體提出的服務請求可以使用任一界面端點。



如需設定服務以及讓服務消費者透過 VPC 對等連線存取服務的範例，請參閱[範例：使用的服務 AWS PrivateLink 和 VPC 對等](#) (p. 56)。

## 端點服務可用區域的考量

當您建立端點服務時，即會在您對應帳戶的可用區域中建立服務，並且從其他帳戶中獨立。服務供應商與消費者的帳戶不同時，使用可用區域 ID 的唯一性及一致性來識別可用區域的端點服務。例如，us-east-1 是 us-east-1 區域的 AZ ID，它在每一個 AWS 帳戶的位置都相對應。如需有關如何識別您可用區域 ID 的資訊，請參閱 AWS RAM 使用者指南 中的 [對您資源的 AZ ID](#) 或使用 [說明可用的區域](#)。

當服務提供者和消費者擁有不同的帳戶並使用多個可用區域，且消費者檢視 VPC 端點服務資訊時，回應僅包含常見的可用區域。例如，當服務提供者帳戶使用 us-east-1a 和 us-east-1c 且消費者使用 us-east-1a 和 us-east-1b 時，回應會包含常見可用區域 us-east-1a 中的 VPC 端點服務。

## 端點服務 DNS 名稱

在您建立 VPC 端點時，AWS 會產生端點特定的 DNS 主機名稱，讓您用來和服務通訊。這些名稱包含 VPC 端點 ID、可用區域名稱和 區域名稱，例如 vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com。根據預設，您的消費者會使用該 DNS 名稱來存取服務，並且通常需要修改應用程式組態。

如果端點服務是 AWS 服務的端點服務，或是 AWS Marketplace 中可用服務的端點服務，則會有預設 DNS 名稱。針對其他服務，服務提供者可以設定私有 DNS 名稱，讓消費者可以使用現有的 DNS 名稱來存取服務，而無須對其應用程式進行變更。如需詳細資訊，請參閱[the section called “端點服務的私有 DNS 名稱”](#) (p. 306)。

服務提供者可以在 IAM 政策陳述式中使用 ec2:VpceServicePrivateDnsName 條件內容金鑰來控制可建立的私有 DNS 名稱。如需詳細資訊，請參閱《IAM 使用者指南》中的 [Amazon EC2 定義的動作](#)。

## 私有 DNS 名稱需求

服務提供者可以為新的端點服務，或是現有的端點服務指定私有 DNS 名稱。如要使用私有 DNS 名稱，請啟用此功能，然後指定私有 DNS 名稱。您必須驗證您具有網域/子網域的控制權，才能讓消費者使用私有 DNS 名稱。您可以使用 Amazon VPC 主控台 或 API 啟動網域所有權驗證。在網域所有權驗證完成後，消費者便可以使用私有 DNS 名稱來存取端點。

## 連線至內部部署的資料中心

您可以使用下列連線類型來在界面端點和您的內部部署資料中心間進行連線。

- AWS Direct Connect
- AWS Site-to-Site VPN

## 透過 VPC 對等連線存取服務

您可以將 VPC 對等連線與 VPC 端點搭配使用，以允許透過 VPC 對等連線對消費者進行私人存取。如需更多詳細資訊，請參閱 [範例：使用的服務 AWS PrivateLink 和 VPC 對等](#) (p. 56)。

## 使用 Proxy Protocol (代理通訊協定) 取得連線資訊

為您的應用程式 (您的服務) 提供來源 IP 地址的網路負載平衡器。當服務消費者透過界面端點向您的服務傳送流量時，提供給您應用程式的來源 IP 地址，會是網路負載平衡器節點的私有 IP 地址，不是服務消費者的 IP 地址。



如果您需要服務消費者的 IP 地址及其對應的界面端點 ID，請啟用您負載平衡器上的 Proxy Protocol (代理通訊協定)，並且從 Proxy Protocol (代理通訊協定) 標頭取得用戶端的 IP 地址。如需詳細資訊，請參閱 [網路負載平衡器 使用者指南 中的 Proxy Protocol \(代理通訊協定\)](#)。

## 端點服務限制

若要使用端點服務，您需要知道目前的規則與限制：

- 端點服務僅支援 TCP 上的 IPv4 流量。
- 服務消費者可以使用端點特定的 DNS 主機名稱來存取端點服務，或是私有 DNS 名稱。
- 如果端點服務與多個網路負載平衡器相關聯，則對於特定的可用區域而言，界面端點只會建立一個負載平衡器的連線。
- 若為端點服務，則相關聯的 Network Load Balancer 可支援 55,000 條同時連線，或每分鐘 55,000 條連線連至唯一目標 (IP 地址和連接埠)。若超過上述連線數量，將提高連接埠配置錯誤機率。若發生連接埠配置錯誤，請將更多目標新增至目標群組。如需網路負載平衡器目標群組的詳細資訊，請參閱 [網路負載平衡器 使用者指南中的 Network Load Balancers 的目標群組及透過目標群組來註冊目標](#)。
- 您帳戶中的可用區域可能並未對應至其他帳戶的相同位置。例如，可用區域 us-east-1a 與其他帳戶的 us-east-1a 可能不是相同的位置。如需詳細資訊，請參閱 [區域與可用區域的概念](#)。當您設定端點服務時，它是在映射到您帳戶的可用區域中設定。
- 檢閱您端點服務的服務特定限制。
- 檢閱端點服務的安全最佳實務和範例。如需詳細資訊，請參閱 [政策最佳實務](#) 和 [the section called “使用 VPC 端點 控制服務的存取” \(p. 292\)](#)。

## 建立 VPC 端點服務組態

您可使用 Amazon VPC 主控台或命令列建立端點服務組態。開始之前，請確定您已為您的服務在您的 VPC 中建立一或多個網路負載平衡器。如需詳細資訊，請參閱 [網路負載平衡器 使用者指南 中的網路負載平衡器入門](#)。

在您的組態中，您可選擇性指定您服務的任何界面端點連線請求都必須由您手動接受。您可以 [建立通知 \(p. 301\)](#) 以在有連線請求時收到提醒。如果您不接受連線，服務消費者即無法存取您的服務。

### Note

無論接受設定為何，服務消費者還必須要有 [許可 \(p. 298\)](#) 才能建立與您服務的連線。

在您建立端點服務組態之後，您必須新增許可讓服務消費者建立您服務的界面端點。

### Console

#### 使用主控台建立端點服務

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務)、Create Endpoint Service (建立端點服務)。
3. 針對 Associate Network Load Balancers (建立網路負載平衡器關聯)，選取要與端點服務建立關聯的網路負載平衡器。
4. 針對 Require acceptance for endpoint (要求接受端點)，選取核取方塊以手動方式接受對您服務的連線請求。如不選取此選項，即會自動接受端點連線。
5. 如要將私有 DNS 名稱與服務建立關聯，請選取 Enable private DNS (啟用私有 DNS) 名稱，然後針對 Private DNS name (私有 DNS 名稱)，輸入私有 DNS 名稱。
6. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (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)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

7. 選擇 Create service (建立服務)。

## AWS CLI

使用 AWS CLI 建立端點服務

使用 `create-vpc-endpoint-service-configuration` 命令並為您的網路負載平衡器指定一個或多個 ARN。您可以選用地指定連線到您的服務是否需要接受，以及服務是否擁有私有 DNS 名稱。

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532 --acceptance-required --privateDnsName exampleservice.com
```

```
{
  "ServiceConfiguration": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532"
    ],
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
    "ServiceState": "Available",
    "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
    "PrivateDnsName": "exampleservice.com",
    "AcceptanceRequired": true,
    "AvailabilityZones": [
      "us-east-1d"
    ],
    "BaseEndpointDnsNames": [
      "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
    ]
  }
}
```

適用於 Windows PowerShell 的 AWS 工具

使用 `New-EC2VpcEndpointServiceConfiguration`。

API

使用 `CreateVpcEndpointServiceConfiguration`。

## 為您的端點服務新增和移除許可

在您建立端點服務組態之後，您可控制哪些服務消費者可以建立界面端點連線到您的服務。服務消費者是 IAM 委託人 — IAM 使用者、IAM 角色和 AWS 帳戶。若要新增或移除委託人許可，您需要其 Amazon Resource Name (ARN)。

- AWS 帳戶 (及此帳戶中所有委託人) 的 ARN 格式為 `arn:aws:iam::aws-account-id:root`。
- 若為特定的 IAM 使用者，則 ARN 格式為 `arn:aws:iam::aws-account-id:user/user-name`。
- 若為特定的 IAM 角色，則 ARN 格式為 `arn:aws:iam::aws-account-id:role/role-name`。



## Note

如果您將許可設為「任何人皆可存取」，並將接受模型設為「接受所有請求」，您便是將您的 NLB 設為公開。因為取得 AWS 帳戶相當容易，即使沒有公有 IP 地址，針對可以存取您 NLB 的人員實際上不會有限制。

## Console

使用主控台新增或移除許可

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Actions (動作)、Add principals to whitelist (新增委託人至允許清單)。
4. 指定委託人的 ARN 以針對其新增許可。若要新增更多委託人，請選擇 Add principal (新增委託人)。若要移除委託人，請選擇項目旁邊的交叉圖示。

## Note

指定 \* 來為所有委託人新增許可。這可讓所有 AWS 帳戶中的所有委託人在您的端點服務中建立界面端點。

5. 選擇 Add to Whitelisted principals (新增至允許清單的委託人)。
6. 若要移除委託人，請在清單中選取它，然後選擇 Delete (刪除)。

## AWS CLI

若要新增您端點服務的許可，請使用 [modify-vpc-endpoint-service-permissions](#) 命令，並使用 `--add-allowed-principals` 參數為委託人新增一或多個 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

若要檢視您為端點服務新增的許可，請使用 [describe-vpc-endpoint-service-permissions](#) 命令。

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
```

```
{
  "AllowedPrincipals": [
    {
      "PrincipalType": "Account",
      "Principal": "arn:aws:iam::123456789012:root"
    }
  ]
}
```

若要移除您端點服務的許可，請使用 [modify-vpc-endpoint-service-permissions](#) 命令，並使用 `--remove-allowed-principals` 參數移除委託人的一或多個 ARN。

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3 --remove-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

## 適用於 Windows PowerShell 的 AWS 工具

使用 [Edit-EC2EndpointServicePermission](#)。

## API

使用 [ModifyVpcEndpointServicePermissions](#)。

## 變更 網路負載平衡器 和接受設定

您可以變更與端點服務相關聯的 網路負載平衡器，以及變更請求是否需要接受才能連線您的端點服務，來修改您的端點服務組態。

如果界面端點連接到您的端點服務，您即無法取消關聯負載平衡器。

### Console

使用主控台變更您端點服務的網路負載平衡器

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Actions (動作)、Associate/Disassociate Network Load Balancers (關聯/取消關聯網路負載平衡器)。
4. 視需要選取或取消選取負載平衡器，然後選擇 Save (儲存)。

使用主控台修改接受設定

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Actions (動作)、Modify endpoint acceptance setting (修改端點接受設定)。
4. 選取或取消選取 Require acceptance for endpoint (要求接受端點)，然後選擇 Modify (修改)。

### AWS CLI

如要變更您端點服務的負載平衡器，請使用 `modify-vpc-endpoint-service-configuration` 命令，並使用 `--add-network-load-balancer-arn` 或 `--remove-network-load-balancer-arn` 參數。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-vpce/e94221227f1ba532
```

如要變更是否需要接受，請使用 `modify-vpc-endpoint-service-configuration` 命令並指定 `--acceptance-required` 或 `--no-acceptance-required`。

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-svc-09222513e6e77dc86 --no-acceptance-required
```

適用於 Windows PowerShell 的 AWS 工具

使用 `Edit-EC2VpcEndpointServiceConfiguration`。

### API

使用 `ModifyVpcEndpointServiceConfiguration`。

## 接受與拒絕界面端點連線請求

在您建立端點服務之後，您已新增許可之服務消費者即可建立界面端點來連線到您的服務。如需建立界面端點的詳細資訊，請參閱 [界面 VPC 端點 \(AWS PrivateLink\) \(p. 266\)](#)。

如已指定連線請求需要接受，您即必須手動接受或拒絕您端點服務的界面端點連線請求。接受界面端點之後，它會變成 `available`。

在它變成 available 狀態後，您可拒絕界面端點連線。

#### Console

使用主控台接受或拒絕連線請求

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. Endpoint Connections (端點連線) 標籤會列出目前待您核准的端點連線。選取端點，選擇 Actions (動作)，然後選擇 Accept endpoint connection request (接受端點連線請求) 接受連線或選擇 Reject endpoint connection request (拒絕端點連線請求) 拒絕連線。

#### AWS CLI

待定接受的端點連線檢視，請使用 `describe-vpc-endpoint-connections` 命令並依 `pendingAcceptance` 狀態篩選。

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-  
state,Values=pendingAcceptance
```

```
{  
  "VpcEndpointConnections": [  
    {  
      "VpcEndpointId": "vpce-0c1308d7312217abc",  
      "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",  
      "CreationTimestamp": "2017-11-30T10:00:24.350Z",  
      "VpcEndpointState": "pendingAcceptance",  
      "VpcEndpointOwner": "123456789012"  
    }  
  ]  
}
```

若要接受端點連線請求，請使用 `accept-vpc-endpoint-connections` 命令，並指定端點 ID 和端點服務 ID。

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-  
endpoint-ids vpce-0c1308d7312217abc
```

若要拒絕端點連線請求，請使用 `reject-vpc-endpoint-connections` 命令。

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-  
endpoint-ids vpce-0c1308d7312217abc
```

適用於 Windows PowerShell 的 AWS 工具

使用 `Confirm-EC2EndpointConnection` 和 `Deny-EC2EndpointConnection`。

#### API

使用 `AcceptVpcEndpointConnections` 和 `RejectVpcEndpointConnections`。

## 建立與管理端點服務的通知

您可建立通知以接收特定事件的提醒，這些事件發生在連接到您端點服務的端點上。例如，當您的端點服務接受或拒絕端點請求時，您會收到電子郵件。若要建立通知，您必須建立 Amazon SNS 主題與通知的關聯。您可以訂閱 SNS 主題，在端點事件發生時收到電子郵件通知。如需詳細資訊，請參閱 [Amazon Simple Notification Service 開發人員指南](#)。

您用於通知的 Amazon SNS 主題必須有主題政策，允許 Amazon VPC 端點服務代您發佈通知。確定您的主題政策中包含下列陳述式。如需詳細資訊，請參閱 Amazon Simple Notification Service 開發人員指南 中的 [管理您的 Amazon SNS 主題存取權](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

## Console

### 建立端點服務的通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Notifications (通知)、Create Notification (建立通知)。
4. 選擇要與通知建立關聯的 SNS 主題 ARN。
5. 針對 Events (事件)，選取要接收通知的端點事件。
6. 選擇 Create Notification (建立通知)。

在您建立通知後，您可以變更與通知建立關聯的 SNS 主題。您也可以為通知指定不同的端點事件。

### 修改端點服務的通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Notifications (通知)、Actions (動作)、Modify Notification (修改通知)。
4. 指定 SNS 主題的 ARN，並視需要選取或取消選取端點事件。
5. 選擇 Modify Notification (修改通知)。

您可以刪除不再需要的通知。

### 刪除通知

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. 選擇 Notifications (通知)、Actions (動作)、Delete Notification (刪除通知)。
4. 選擇 Yes, Delete (是，刪除)。

## AWS CLI

### 使用 AWS CLI 建立與管理通知

1. 如要建立端點服務的通知，請使用 [create-vpc-endpoint-connection-notification](#) 命令，並指定 SNS 主題的 ARN、要通知的事件，以及端點服務的 ID。

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

```
{
  "ConnectionNotification": {
    "ConnectionNotificationState": "Enabled",
    "ConnectionNotificationType": "Topic",
    "ServiceId": "vpce-svc-1237881c0d25a3abc",
    "ConnectionEvents": [
      "Reject",
      "Accept",
      "Delete",
      "Connect"
    ],
    "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
    "ConnectionNotificationArn": "arn:aws:sns:us-east-2:123456789012:VpceNotification"
  }
}
```

2. 如要檢閱您的通知，請使用 [describe-vpc-endpoint-connection-notifications](#) 命令。

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

3. 如要變更通知的 SNS 主題或端點事件，請使用 [modify-vpc-endpoint-connection-notification](#) 命令。

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-arn arn:aws:sns:us-east-2:123456789012:mytopic
```

4. 如要刪除通知，請使用 [delete-vpc-endpoint-connection-notifications](#) 命令。

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-ids vpce-nfn-008776de7e03f5abc
```

適用於 Windows PowerShell 的 AWS 工具

使用 [New-EC2VpcEndpointConnectionNotification](#)、[Get-EC2EndpointConnectionNotification](#)、[Edit-EC2VpcEndpointConnectionNotification](#)，以及 [Remove-EC2EndpointConnectionNotification](#)。

API

使用

[CreateVpcEndpointConnectionNotification](#)、[DescribeVpcEndpointConnectionNotifications](#)、[ModifyVpcEndpointConnectionNotification](#) 以及 [DeleteVpcEndpointConnectionNotifications](#)。

## 新增或移除 VPC 端點服務標籤

標籤可供識別 VPC 端點服務。您可以新增或移除標籤。

Console

若要新增或移除 VPC 端點服務標籤

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

2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取 VPC 端點服務並選擇 Actions (動作)、Add/Edit Tags (新增/編輯標籤)。
4. 新增或移除標籤。

[新增標籤] 選擇 Create tag (建立標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 對於 Value (值)，輸入金鑰值

[移除標籤] 選擇標籤 Key (金鑰) 和 Value (值) 右邊的刪除按鈕 (「x」)。

適用於 Windows PowerShell 的 AWS 工具

使用 [CreateTags](#) 及 [DeleteTags](#)。

若要接受端點連線請求，請使用 [accept-vpc-endpoint-connections](#) 命令，並指定端點 ID 和端點服務 ID。

API

使用 [create-tags](#) 及 [delete-tags](#)。

## 刪除端點服務組態

您可以刪除端點服務組態。刪除組態不會刪除您 VPC 中託管的應用程式或相關聯的負載平衡器。

刪除端點服務組態之前，您必須先拒絕連接到服務的任何 available 或 pending-acceptance VPC 端點。如需詳細資訊，請參閱[接受與拒絕界面端點連線請求](#) (p. 300)。

Console

使用主控台刪除端點服務組態

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取服務。
3. 選擇 Actions (動作)、Delete (刪除)。
4. 選擇 Yes, Delete (是，刪除)。

AWS CLI

使用 AWS CLI 刪除端點服務組態

- 使用 [delete-vpc-endpoint-service-configurations](#) 命令並指定服務的 ID。

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-  
svc-03d5ebb7d9579a2b3
```

適用於 Windows PowerShell 的 AWS 工具

使用 [Remove-EC2EndpointServiceConfiguration](#)。

API

使用 [DeleteVpcEndpointServiceConfigurations](#)。

## 適用於 VPC 端點 和 VPC 端點 服務的 Identity and Access Management

使用 IAM 管理 VPC 端點 和 VPC 端點 服務的存取權。

### 控制 VPC 端點 的使用

根據預設，IAM 使用者沒有使用端點的許可。您可以建立 IAM 使用者政策，將建立、修改、說明和刪除端點的許可授予使用者。以下是範例。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:*VpcEndpoint*",
    "Resource": "*"
  }]
}
```

如需使用 VPC 端點控制服務存取的資訊，請參閱 [the section called “使用 VPC 端點 控制服務的存取” \(p. 292\)](#)。

### 根據服務擁有者控制 VPC 端點 的建立

您可以根據誰擁有該服務 (amazon、aws-marketplace 或 aws-account-id)，使用 ec2:VpceServiceOwner 條件金鑰控制可建立的 VPC 端點。在下列範例中，您只能在服務擁有者為 amazon 時建立 VPC 端點。若要使用此範例，請替換帳戶 ID、服務擁有者和區域 (除非您位於 us-east-1 區域)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:accountId:vpc-endpoint/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServiceOwner": [
            "amazon"
          ]
        }
      }
    }
  ]
}
```

### 控制可為 VPC 端點服務指定的私有 DNS 名稱

您可以根據與 VPC 端點服務相關聯的私有 DNS 名稱，使用 ec2:VpceServicePrivateDnsName 條件金鑰控制可修改或建立的 VPC 端點服務。在下列範例中，只有當私有 DNS 名稱為 example.com 時，才能建立或 VPC 端點 服務。若要使用此範例，請替換帳戶 ID、私有 DNS 名稱和區域 (除非您位於 us-east-1 區域)。

```
{
```



```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyVpcEndpointServiceConfiguration",
      "ec2:CreateVpcEndpointServiceConfiguration"
    ],
    "Resource": [
      "arn:aws:ec2:us-east-1:accountId:vpc-endpoint-service/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:VpceServicePrivateDnsName": [
          "example.com"
        ]
      }
    }
  }
]
```

控制可為 VPC 端點服務指定的服務名稱

您可以根據 VPC 端點服務名稱，使用 `ec2:VpceServiceName` 條件金鑰控制可建立的 VPC 端點。在下列範例中，您只能在服務名稱為 `com.amazonaws.us-east-1.s3` 時建立或 VPC 端點。若要使用此範例，請替換帳戶 ID、服務名稱和區域 (除非您位於 `us-east-1` 區域)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:accountId:vpc-endpoint/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServiceName": [
            "com.amazonaws.us-east-1.s3"
          ]
        }
      }
    }
  ]
}
```

## 端點服務的私有 DNS 名稱

在您建立 VPC 端點時，AWS 會產生端點特定的 DNS 主機名稱，讓您用來和服務通訊。這些名稱包含 VPC 端點 ID、可用區域名稱和區域名稱，例如 `vpce-1234-abcdev-us-east-1.vpce-svc-123345.us-east-1.vpce.amazonaws.com`。根據預設，您的消費者會使用該 DNS 名稱來存取服務，並且通常需要修改應用程式組態。

如果端點服務是 AWS 服務的端點服務，或是 AWS Marketplace 中可用服務的端點服務，則會有預設 DNS 名稱。針對其他服務，服務提供者可以設定私有 DNS 名稱，讓消費者可以使用現有的 DNS 名稱來存取服務，而無須對其應用程式進行變更。如需更多詳細資訊，請參閱 [the section called “VPC 端點服務 \(AWS PrivateLink\)” \(p. 294\)](#)。

服務提供者可以為新的端點服務，或是現有的端點服務指定私有 DNS 名稱。如要使用私有 DNS 名稱，請啟用此功能，然後指定私有 DNS 名稱。您必須驗證您具有網域/子網域的控制權，才能讓消費者使用私有 DNS 名稱。您可以使用 Amazon VPC 主控台 或 API 啟動網域所有權驗證。在網域所有權驗證完成後，消費者便可以使用私有 DNS 名稱來存取端點。

#### Note

為了驗證網域，你需要公有託管名稱，或公有 DNS 提供者。

高階程序如下：

1. 新增私有 DNS 名稱。如需更多詳細資訊，請參閱 [the section called “建立 VPC 端點服務組態” \(p. 297\)](#) 或 [the section called “修改現有的端點服務私有 DNS 名稱” \(p. 309\)](#)。
2. 請注意您針對 DNS 伺服器記錄所需要的 Domain verification value (網域驗證值) 和 Domain verification name (網域驗證名稱)。如需詳細資訊，請參閱 [the section called “檢視端點服務私有 DNS 名稱組態” \(p. 309\)](#)。
3. 將記錄新增至 DNS 伺服器。如需更多詳細資訊，請參閱 [the section called “VPC 端點服務私有 DNS 名稱驗證” \(p. 308\)](#)。
4. 驗證私有 DNS 名稱。如需更多詳細資訊，請參閱 [the section called “手動啟動端點服務私有 DNS 名稱網域驗證” \(p. 310\)](#)。

您可以使用 Amazon VPC 主控台或 Amazon VPC API 來管理驗證程序。

- [the section called “VPC 端點服務私有 DNS 名稱驗證” \(p. 308\)](#)
- [the section called “修改現有的端點服務私有 DNS 名稱” \(p. 309\)](#)
- [the section called “移除端點服務私有 DNS 名稱” \(p. 310\)](#)
- [the section called “檢視端點服務私有 DNS 名稱組態” \(p. 309\)](#)
- [Amazon VPC 私有 DNS 名稱網域驗證 TXT 記錄 \(p. 311\)](#)

## 網域名稱驗證考量

請記下下列與網域所有權驗證相關的重點：

- 消費者只有在驗證狀態是 verified (已驗證) 時，才能使用私有 DNS 名稱來存取端點服務。
- 如果驗證狀態從 verified (已驗證) 變更為 pendingVerification (等待驗證) 或 failed (已失敗)，則現有的消費者連線仍會保留，但會拒絕任何新的連線請求。

#### Important

針對擔心與不再處於 verified (已驗證) 狀態端點服務連線的服務提供者，我們建議您使用 [DescribeVpcEndpoints](#) 來定期檢查驗證狀態。我們建議您至少每天執行這個檢查一次。

- 端點服務只能擁有一個私有 DNS 名稱。
- 您可以為新的端點服務，或是現有的端點服務指定私有 DNS 名稱。
- 您只能使用公有網域名稱伺服器。
- 您可以在網域名稱中使用萬用字元，例如 `*.myexampleservice.com`。
- 您必須為每個端點服務分別執行網域所有權驗證檢查。
- 您可以驗證子網域的網域。例如，您可以驗證 `example.com`，而非 `a.example.com`。如 [RFC 1034](#) 中所述，每個 DNS 標籤最多可以有 63 個字元，而整個網域名稱的總長度不得超過 255 個字元。

如果您新增其他子網域，您必須驗證子網域或是網域。例如，假設您有一個 `a.example.com` 及已驗證的 `example.com`。您現在將 `b.example.com` 做為私有 DNS 名稱新增。您必須先驗證 `example.com` 或 `b.example.com`，您的消費者才能使用該名稱。

- 網域名稱必須是小寫。

## VPC 端點服務私有 DNS 名稱驗證

您的網域與一組網域名稱系統 (DNS) 記錄相關，而您透過 DNS 供應商來管理這些記錄。TXT 記錄是一種 DNS 記錄類型，可提供關於您的網域的更多資訊。每個 TXT 記錄皆以名稱與值組成。

當您使用 Amazon VPC 主控台 或 API 啟動網域所有權驗證時，我們會為您提供可用於 TXT 記錄的名稱和值。例如，如果您的網域是 myexampleservice.com，則我們產生的 TXT 記錄設定看起來會與以下範例相似：

### 端點私有 DNS 名稱 TXT 記錄

網域驗證名稱	類型	網域驗證值
_vpce:akslджа21i1	TXT	vpce:asjdakjshd78126eu21

使用指定的 Domain verification name (網域驗證名稱) 和 Domain verification value (網域驗證值) 將 TXT 記錄新增到您的網域的 DNS 伺服器。當我們在您網域的 DNS 設定中偵測到存在 TXT 記錄時，網域所有權驗證便已完成。

如果您的 DNS 提供者不允許 DNS 記錄名稱包含底線，您可以在 Domain verification name (網域驗證名稱) 中省略 aksldja21i1。在這種情況下，針對先前的範例，TXT 記錄名稱將會是 myexampleservice.com，而非 \_vpce:akslджа21i1.myexampleservice.com。

## 新增 TXT 記錄到您的網域的 DNS 伺服器

新增 TXT 記錄到您的網域的 DNS 伺服器之程序將根據您的 DNS 服務供應商而有不同。您的 DNS 提供者可能是 Amazon Route 53 或其他網域名稱註冊商。本節提供將 TXT 記錄新增至 Route 53 的程序，以及適用於其他 DNS 提供者的一般程序。

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 選擇 Endpoint Services (端點服務)。
3. 選取端點服務。
4. 在 Details (詳細資訊) 標籤上，記下顯示在 Domain verification value (網域驗證值) 和 Domain verification name (網域驗證名稱) 旁邊的值。
5. 如果 Route 53 為您正在驗證的網域提供 DNS 服務，而且您使用與 Route 53 相同的帳戶來登入 AWS 管理主控台，我們會提供在 Amazon VPC 主控台中立即更新您 DNS 伺服器的選項。

如果您使用不同的 DNS 提供者，則更新 DNS 記錄的程序會根據您使用的 DNS 或 Web 託管提供者而異。下表列出幾個常見 DNS 供應商的文件連結。這不是完整清單，且列在此清單中並不表示贊同或推薦任何公司的產品或服務。如果您的提供者並未列在表格中，您或許可以搭配端點使用網域。

DNS/託管供應商	文件連結
GoDaddy	<a href="#">新增 TXT 記錄 (外部連結)</a>
Dreamhost	<a href="#">如何新增自訂 DNS 記錄？ (外部連結)</a>
Cloudflare	<a href="#">管理 CloudFlare 中的 DNS 記錄 (外部連結)</a>
HostGator	<a href="#">使用 HostGator/eNom 管理 DNS 記錄 (外部連結)</a>
Namecheap	<a href="#">如何為我的網域新增 TXT/SPF/DKIM/DMARC 記錄 (外部連結)</a>
Names.co.uk	<a href="#">變更您的網域 DNS 設定 (外部連結)</a>

DNS/託管供應商	文件連結
Wix	在您的 Wix 帳戶中新增或更新 TXT 記錄 (外部連結)

驗證完成後，Amazon VPC 主控台中網域的狀態會從 Pending (待定) 變更為 Verified (已驗證)。

6. 您現在可以使用 VPC 端點服務的私有網域名稱。

如果 DNS 設定未正確更新，Details (詳細資訊) 標籤上的網域狀態會顯示狀態為 failed (已失敗)。如果發生上述情況，請完成故障診斷頁面上的步驟：[the section called “針對常見的網域驗證問題進行疑難排解” \(p. 312\)](#)。在您驗證您的 TXT 記錄已正確建立後，請重試操作。

## 修改現有的端點服務私有 DNS 名稱

您可以為新的端點服務或是現有的端點服務修改端點服務私有 DNS 名稱。

使用主控台修改端點服務私有 DNS 名稱

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務，然後選擇 Actions (動作)、Modify private DNS name (修改私有 DNS 名稱)。
4. 選取 Enable private DNS name (啟用私有 DNS 名稱)，然後針對 Private DNS name (私有 DNS 名稱)，輸入私有 DNS 名稱。
5. 選擇 Modify (修改)。

在更新名稱後，請在您的 DNS 伺服器上更新網域的項目。我們會自動輪詢 DNS 伺服器來驗證伺服器上存在記錄。DNS 記錄更新可能需要多達 48 小時才可生效，但是生效時間通常會較快。如需更多詳細資訊，請參閱 [the section called “私有 DNS 名稱網域驗證 TXT 記錄” \(p. 311\)](#) 及 [the section called “VPC 端點服務私有 DNS 名稱驗證” \(p. 308\)](#)。

使用 AWS CLI 或 API 修改端點服務私有 DNS 名稱

- [modify-vpc-endpoint-service-configuration](#)
- [ModifyVpcEndpointServiceConfiguration](#)

## 檢視端點服務私有 DNS 名稱組態

您可以檢視端點服務的端點服務私有 DNS 名稱。

Console

使用主控台檢視端點服務私有 DNS 名稱組態

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoint Services (端點服務) 並選取您的端點服務。
3. Details (詳細資訊) 標籤會顯示私有 DNS 網域所有權檢查的以下資訊：
  - Domain verification status (網域驗證組態)：驗證狀態。
  - Domain verification type (網域驗證類型)：驗證類型。
  - Domain verification value (網域驗證值)：DNS 值。
  - Domain verification name (網域驗證名稱)：記錄子網域的名稱。

#### AWS CLI

使用 [describe-vpc-endpoint-service-configurations](#)。

#### API

使用 [DescribeVpcEndpointServiceConfigurations](#)。

## 手動啟動端點服務私有 DNS 名稱網域驗證

服務提供者必須先證明其擁有私有 DNS 名稱網域，消費者才能使用私有 DNS 名稱。

#### Console

使用主控台啟動私有 DNS 名稱網域的驗證程序

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務，然後選擇 Actions (動作)、Verify domain ownership for Private DNS Name (驗證私有 DNS 名稱的網域所有權)。
4. 選擇 Verify (驗證)。

如果 DNS 設定未正確更新，Details (詳細資訊) 標籤上的網域將會顯示狀態為 failed (已失敗)。如果發生上述情況，請完成故障診斷頁面上的步驟：[the section called “針對常見的網域驗證問題進行疑難排解” \(p. 312\)](#)。

#### AWS CLI

使用 [start-vpc-endpoint-service-private-dns-verification](#)。

#### API

使用 [StartVpcEndpointServicePrivateDnsVerification](#)。

## 移除端點服務私有 DNS 名稱

您只能在服務沒有任何連線之後，才能移除端點服務私有 DNS 名稱。

#### Console

使用主控台移除端點服務私有 DNS 名稱

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務，然後選擇 Actions (動作)、Modify private DNS name (修改私有 DNS 名稱)。
4. 清除 Enable private DNS name (啟用私有 DNS 名稱)，然後清除 Private DNS name (私有 DNS 名稱)。
5. 選擇 Modify (修改)。

#### AWS CLI

使用 [modify-vpc-endpoint-service-configuration](#)。

#### API

使用 [ModifyVpcEndpointServiceConfiguration](#)。

## Amazon VPC 私有 DNS 名稱網域驗證 TXT 記錄

您的網域與一組網域名稱系統 (DNS) 記錄相關，而您透過 DNS 供應商來管理這些記錄。TXT 記錄是一種 DNS 記錄類型，可提供關於您的網域的更多資訊。每個 TXT 記錄皆以名稱與值組成。

當您使用 Amazon VPC 主控台 或 API 啟動網域所有權驗證時，我們會為您提供可用於 TXT 記錄的名稱和值。例如，如果您的網域是 myexampleservice.com，則 Amazon VPC 產生的 TXT 記錄設定看起來會與以下範例相似：

### 端點私有 DNS 名稱 TXT 記錄

網域驗證名稱	類型	網域驗證值
_vpce:akslidja21i1.myexampleservice.com	TXT	vpce:asjdakjshd78126eu21

使用指定的 Domain verification name (網域驗證名稱) 和 Domain verification value (網域驗證值) 來將 TXT 記錄新增至您網域的 DNS 伺服器。當 Amazon VPC 偵測到您網域的 DNS 設定中含有 TXT 記錄時，Amazon VPC 網域驗證便已完成。

如果您的 DNS 提供者不允許 DNS 記錄名稱包含底線，您可以使用 Domain verification name (網域驗證名稱) 的網域名稱。在這種情況下，對於上述範例而言，TXT 記錄名稱將會是 myexampleservice.com。

您可以在 [針對常見的私有 DNS 網域驗證問題進行疑難排解 \(p. 312\)](#) 中找到故障診斷資訊和如何檢查您網域所有權驗證設定的說明。

### Amazon Route 53

新增 TXT 記錄到您的網域的 DNS 伺服器之程序將根據您的 DNS 服務供應商而有不同。您的 DNS 提供者可能是 Amazon Route 53 或其他網域名稱註冊商。本節提供將 TXT 記錄新增至 Route 53 的程序，以及適用於其他 DNS 提供者的一般程序。

#### 將 TXT 記錄新增至 Route 53 受管網域的 DNS 記錄

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 選擇 Endpoint Services (端點服務)。
3. 選取端點服務。
4. 在 Details (詳細資訊) 標籤上，記下顯示在 Domain verification value (網域驗證值) 和 Domain verification name (網域驗證名稱) 旁邊的值。
5. 在 <https://console.aws.amazon.com/route53/> 開啟 Route 53 主控台。
6. 在導覽窗格中，選擇 Hosted Zones (託管區域)。
7. 選取您要對其新增 TXT 記錄的網域，然後選擇 Go to Record Sets (移至記錄集)。
8. 選擇 Create Record Set (建立記錄集)。
9. 在 Create Record Set (建立記錄集) 窗格中，選取下列項目：
  - a. 針對 Name (名稱)，輸入 Amazon VPC 主控台的端點服務 Domain verification name (網域驗證名稱)。
  - b. 針對 Type (類型)，選擇 TXT – Text (TXT – 文字)。
  - c. 針對 TTL (Seconds) (TTL (秒))，輸入 **1800**。
  - d. 針對 Value (值)，輸入 Amazon VPC 主控台的 Domain verification value (網域驗證值)。
  - e. 選擇 Create (建立)。
10. 在 Amazon VPC 主控台中 Endpoint Services (端點服務) 頁面的 Details (詳細資訊) 標籤上，檢查端點旁邊 Domain verification status (網域驗證狀態) 欄中的值。如果狀態是 "pending



verification" (等待驗證)，請等待幾分鐘，然後選擇 refresh (重新整理)。重複這個程序，直到狀態欄的值為 "verified" (已驗證) 為止。您可以手動啟動驗證程序。如需詳細資訊，請參閱 [the section called “手動啟動端點服務私有 DNS 名稱網域驗證”](#) (p. 310)。

#### Generic procedures for other DNS providers

將 TXT 記錄新增至 DNS 組態的程序各家供應商均不同。如需具體的步驟，請參閱您的 DNS 供應商文件。本節程序提供在將 TXT 記錄新增到網域的 DNS 組態時您可以採取的步驟基本概觀。

若要新增 TXT 記錄到您的網域的 DNS 伺服器 (一般程序)

1. 前往您的 DNS 供應商的網站。如果您不確定提供網域的 DNS 供應商是哪一家，可使用免費的 [Whois 服務](#) 來查詢。
2. 在供應商的網站上，登入您的帳戶。
3. 尋找更新網域的 DNS 記錄的頁面。此頁面通常會有名稱，例如 DNS 記錄、DNS 區域檔或進階 DNS。如果您不確定，請參閱供應商的文件。
4. 以 AWS 所提供的名稱和值來新增 TXT 記錄。

#### Important

部分 DNS 供應商會自動將網域名稱附加至 DNS 記錄的尾端。新增已包含網域名稱 (例如 \_pmBGN/7Mjnf.example.com) 的記錄可能會導致網域名稱重複 (例如 \_pmBGN/7Mjnfexample.com.example.com)。為了避免重複的網域名稱，請加入句號 (.) 至 DNS 記錄中的網域名稱結尾處。這將向您的 DNS 提供者指出記錄名稱完全符合資格 (也就是不再與網域名稱相關)，並可避免 DNS 提供者附加額外的網域名稱。

5. 儲存您的變更。DNS 記錄更新可能需要多達 48 小時才可生效，但是生效時間通常會較快。

## 針對常見的私有 DNS 網域驗證問題進行疑難排解

如要搭配 Amazon VPC 驗證端點服務私有 DNS 網域名稱，您可以使用 Amazon VPC 主控台或 API 來啟動程序。本節包含可能有助您解決驗證程序問題的資訊。

### 常見的網域驗證問題

如果您嘗試驗證網域，並且發生問題，請檢閱下列可能的原因和解決方案。

- 您正在嘗試驗證您未擁有的網域。除非您擁有網域，否則您無法進行驗證。
- 您的 DNS 提供者不允許在 TXT 記錄名稱中使用底線。有些 DNS 提供者不允許在您網域的 DNS 記錄名稱中包含底線字元。如果您的提供者正是如此，您可以從 TXT 記錄的名稱中省略 \_amazonvpc。
- 您的 DNS 提供者將網域名稱附加到了 TXT 記錄的結尾。有些 DNS 提供者會自動將您網域的名稱附加到 TXT 記錄的屬性名稱。例如，如果您建立了屬性名稱是 \_amazonvpc.example.com 的記錄，提供者可能會附加網域名稱，產生 \_amazonvpc.example.com.example.com)。為了避免重複的網域名稱，請在建立 TXT 記錄時於網域名稱結尾處加上句號。此步驟可告知您的 DNS 供應商，他們不需要將網域名稱附加到 TXT 記錄。
- 您的 DNS 提供者修改了 DNS 記錄值。有些提供者會自動修改 DNS 記錄值，以僅使用小寫字母。我們只會在驗證記錄的屬性值與您啟動網域所有權驗證程序時，我們所提供的值完全相符時，才會驗證您的網域。如果您網域的 DNS 供應商將 TXT 記錄值變更為只使用小寫字母，請聯絡 DNS 供應商以尋求額外的協助。
- 您希望驗證相同的網域多次。您可能需要驗證您的網域超過一次，因為您正在不同的 AWS 區域中傳送，或是因為您正在從多個 AWS 帳戶使用相同的網域進行傳送。如果您的 DNS 供應商不允許您擁有多個含相同屬性名稱的 TXT 記錄，您仍有可能驗證兩個網域。如果您的 DNS 供應商允許的話，您可以指定多個屬性值給相同的 TXT 記錄。例如，如果您的 DNS 是由 Amazon Route 53 管理，您可以完成下列步驟為相同的 TXT 記錄設定多個值：



1. 在 Route 53 主控台中，選擇您在第一個區域中驗證網域時所建立的 TXT 記錄。
2. 在 Value (值) 方塊中，移至現有的屬性值結尾，然後按 Enter 鍵。
3. 新增其他區域的屬性值，然後儲存記錄集。

如果您的 DNS 提供者不允許您將多個值指派給相同的 TXT 記錄，您可以使用 TXT 記錄屬性名稱中的值驗證網域一次，並在另一次驗證中從屬性名稱中移除該值。例如，您先使用 “\_asnbcdasd” 進行驗證，然後再使用 “asnbcdasd” 進行驗證。這個解決方案的缺點是，相同的網域您只能驗證兩次。

## 如何檢查網域驗證設定

您可以使用以下程序，驗證您的私有 DNS 名稱網域所有權驗證 TXT 記錄已正確發佈到您的 DNS 伺服器。此程序使用 [nslookup](#) 工具，適用於 Windows 和 Linux。在 Linux 上，您也可以使用 [dig](#)。

這些說明中的命令是在 Windows 7 上執行，並且我們使用的範例網域是 example.com。

在此程序中，您會先看到您的網域使用的 DNS 伺服器，然後查詢這些伺服器以檢視 TXT 記錄。之所以查詢提供您的網域的 DNS 伺服器，是因為這些伺服器包含您的網域之最新資訊，可能需要時間才能傳播到其他 DNS 伺服器。

驗證您的網域所有權驗證 TXT 記錄已發佈到您的 DNS 伺服器

1. 執行以下步驟來尋找網域的名稱伺服器。
  - a. 前往命令列。如要前往 Windows 7 上的命令列，請選擇 Start (開始)，然後輸入 cmd。在以 Linux 為基礎的作業系統上，開啟終端機視窗。
  - b. 在命令提示中輸入以下內容，其中 <domain> 是您的網域。

```
nslookup -type=NS <domain>
```

例如，如果您的網域是 example.com，命令看起來會如下。

```
nslookup -type=NS example.com
```

命令的輸出將列出提供您網域的名稱伺服器。您將在後續步驟中查詢其中一個伺服器。

2. 執行下列步驟來確認 TXT 記錄已正確發佈。
  - a. 在命令提示中輸入以下內容，其中 <domain> 是您的網域，<name server> 是您在步驟 1 中找到的其中一個名稱伺服器。

```
nslookup -type=TXT _aksldja21i1.<domain> <name server>
```

在我們的 \_aksldja21i1.example.com 範例中，如果我們在步驟 1 中找到的名稱伺服器稱為 ns1.name-server.net，我們會輸入以下內容。

```
nslookup -type=TXT _aksldja21i1.example.com ns1.name-server.net
```

- b. 在命令的輸出中，驗證 text = 之後的字串與您在 Amazon VPC 主控台的身分清單中選擇網域時所看到的 TXT 值相符。















在我們的範例中，我們會使用 asjdakjshd78126eu21 的值，尋找 \_aksldja21i1.example.com 下的 TXT 記錄。如果記錄已正確發佈，我們預期命令會有以下輸出。

```
_aksldja21i1.example.com text = "asjdakjshd78126eu21"
```

## 可與 AWS PrivateLink 搭配使用的 AWS 服務

下列服務與 AWS PrivateLink 整合。



當該服務與 AWS PrivateLink 整合，但不支援 VPC 端點政策時，「支援 VPC 端點政策」欄會顯示「No (否)」。

AWS 服務	支援 VPC 端點政策
<a href="#">Amazon API Gateway</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon AppStream 2.0</a>	 No
<a href="#">AWS App Mesh</a>	 No
<a href="#">Application Auto Scaling</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon Athena</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon Aurora</a>	 Yes <a href="#">進一步了解</a>
<a href="#">AWS Auto Scaling</a>	 Yes <a href="#">進一步了解</a>
<a href="#">AWS Certificate Manager 私有憑證授權機構</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon Cloud Directory</a>	 Yes <a href="#">進一步了解</a>
<a href="#">AWS CloudFormation</a>	 No
<a href="#">AWS CloudTrail</a>	 No
<a href="#">Amazon CloudWatch</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon CloudWatch Events</a>	 Yes <a href="#">進一步了解</a>
<a href="#">Amazon CloudWatch Logs</a>	 Yes <a href="#">進一步了解</a>

AWS 服務	支援 VPC 端點政策
AWS CodeArtifact	 Yes <a href="#">進一步了解</a>
AWS CodeBuild	 Yes <a href="#">進一步了解</a>
AWS CodeCommit	 Yes <a href="#">進一步了解</a>
AWS CodeDeploy	 Yes <a href="#">進一步了解</a>
Amazon CodeGuru Profiler	 No
Amazon CodeGuru Reviewer	 No
AWS CodePipeline	 No
Amazon Comprehend	 Yes <a href="#">進一步了解</a>
AWS Config	 No
AWS Data Exchange	 Yes <a href="#">進一步了解</a>
AWS DataSync	 No
AWS Device Farm	 No
Amazon EBS 直接 API	 No
Amazon EC2	 Yes <a href="#">進一步了解</a>
EC2 映像建置器	 Yes <a href="#">進一步了解</a>
Amazon EC2 Auto Scaling	 Yes <a href="#">進一步了解</a>
AWS Elastic Beanstalk	 Yes <a href="#">進一步了解</a>

AWS 服務	支援 VPC 端點政策
Amazon Elastic File System	 Yes <a href="#">進一步了解</a>
Elastic Load Balancing	 Yes <a href="#">進一步了解</a>
Amazon Elastic Container Registry	 Yes <a href="#">進一步了解</a>
Amazon Elastic Container Service	 No
Amazon EMR	 Yes <a href="#">進一步了解</a>
Amazon Fraud Detector	 Yes <a href="#">進一步了解</a>
AWS Glue	 No
AWS IoT SiteWise	 No
AWS Key Management Service	 Yes <a href="#">進一步了解</a>
Amazon Keyspaces (適用於 Apache Cassandra)	 Yes <a href="#">進一步了解</a>
Amazon Kinesis Data Firehose	 Yes <a href="#">進一步了解</a>
Amazon Kinesis Data Streams	 Yes <a href="#">進一步了解</a>
AWS License Manager	 Yes <a href="#">進一步了解</a>
Amazon Managed Blockchain	 No
Amazon Quantum Ledger Database (Amazon QLDB)	 Yes <a href="#">進一步了解</a>
Amazon RDS	 Yes <a href="#">進一步了解</a>

AWS 服務	支援 VPC 端點政策
Amazon RDS 資料 API	 Yes <a href="#">進一步了解</a>
Amazon Redshift	 Yes <a href="#">進一步了解</a>
Amazon Rekognition	 Yes <a href="#">進一步了解</a>
Amazon SageMaker 和 Amazon SageMaker 執行時間	 Yes <a href="#">進一步了解</a>
Amazon SageMaker 筆記本	 Yes <a href="#">進一步了解</a>
AWS Secrets Manager	 Yes <a href="#">進一步了解</a>
AWS Security Token Service	 Yes <a href="#">進一步了解</a>
AWS Server Migration Service	 No
AWS Service Catalog	 No
Amazon Simple Email Service (Amazon SES)	 No
Amazon SNS	 Yes <a href="#">進一步了解</a>
Amazon SQS	 Yes <a href="#">進一步了解</a>
AWS Step Functions	 Yes <a href="#">進一步了解</a>
AWS Systems Manager	 No
AWS Storage Gateway	 No
Amazon Transcribe	 Yes <a href="#">進一步了解</a>

AWS 服務	支援 VPC 端點政策
<a href="#">Amazon Transcribe Medical</a>	 Yes <a href="#">進一步了解</a>
<a href="#">AWS 轉移至 SFTP</a>	 No
<a href="#">Amazon WorkSpaces</a>	 No
由其他 AWS 帳戶託管的 <a href="#">端點服務 (p. 294)</a>	 No
支援的 AWS Marketplace 合作夥伴服務	 No

# VPN 連接

您可以使用下列 VPN 連線選項將您的 Amazon 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 連線的遠端設定您的客戶閘道裝置。如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》 <a href="https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html">https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html</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 資源或內部部署網路。您可以藉由 AWS Client VPN，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《AWS Site-to-Site VPN 使用者指南》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放式資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？](#)。



# Amazon VPC 配額

下表列出您 AWS 帳戶每個區域的 Amazon VPC 資源配額 (先前稱為限制)。除非另做說明，否則您可以[請求提高](#)這些配額。針對其中一部分配額，您可以使用 Amazon EC2 主控台的 Limits (限制) 頁面來檢視您目前的配額。

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

資源	預設	註解
每個區域的 VPC 數	5	每個區域的網際網路閘道配額與此直接相關。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。  雖然預設配額為每個區域 5 個 VPC，但您可根據自己的需求，在每個區域擁有 100 個 VPC。
每個 VPC 的子網路數	200	-
每個 VPC 的 IPv4 CIDR 區塊數	5	此主要 CIDR 區塊及所有輔助 CIDR 區塊合計趨近此配額。此配額可提高至上限 50。
每個 VPC 的 IPv6 CIDR 區塊數	1	此配額無法增加。

## DNS

每個 EC2 執行個體會將可傳送至 Amazon Route 53 Resolver (亦即 .2 位址，例如 10.0.0.2) 的封包數限制為每秒、每個網路界面最多 1024 個封包。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，Amazon 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 架構建議事項，請參閱[適用於 Amazon VPC 的混合雲端 DNS 解決方案](#)白皮書。

## 彈性 IP 地址 (IPv4)

資源	預設	註解
每個區域的彈性 IP 地址數	5	這是 EC2-VPC 中使用彈性 IP 地址數量的配額。針對在 EC2-Classic 中使用的彈性 IP 地址，請參閱《Amazon Web Services 一般參考》中的 <a href="#">Amazon Elastic Compute Cloud 端點和配額</a> 。  此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。

## 閘道

資源	預設	註解
每個區域的客戶閘道數	-	如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的 <a href="#">Site-to-Site VPN 配額</a> 。
每個區域的出口限定網際網路閘道數	5	此配額與每個區域 VPC 的配額直接相關。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出口限定網際網路閘道至 VPC。
每個區域的網際網路閘道數	5	此配額與每個區域 VPC 的配額直接相關。若要增加此配額，請增加每個區域的 VPC 配額。一次只有一個網際網路閘道可以連接至 VPC。
每個可用區域的 NAT 閘道數	5	pending、active 或 deleting 狀態中的 NAT 閘道會根據您的配額來計數。
每個區域的虛擬私有閘道數	-	如需詳細資訊，請參閱《AWS Site-to-Site VPN 使用者指南》中的 <a href="#">Site-to-Site VPN 配額</a> 。
每個 VPC 的電信業者閘道	1	

## 客戶管理的字首清單

資源	預設	註解
每個區域的字首清單	100	-
每個字首清單的版本數目	1,000	-
每個資源類型的字首清單的參照	5,000	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 個字首清單的參考，以及在所有子網路路由表中對字首清單的 5,000 個參考。如果您與其他 AWS 帳戶共用字首清單，則其他帳戶對您字首清單的參考會計入此配額。

## 網路 ACL

資源	預設	註解
每個 VPC 的網路 ACL 數	200	您可以將一個網路 ACL 關聯至 VPC 中的一或多個子網路。此配額與每個網路 ACL 的規則數不同。
每個網路 ACL 的規則數	20	這是單一網路 ACL 的單向配額。此配額會分別針對 IPv4 規則和 IPv6 規則執行；例如，

資源	預設	註解
		<p>您可在 IPv4 流量有 20 個傳入規則，IPv6 流量也有 20 個傳入規則。此配額包含預設拒絕規則 (IPv4 的規則編號 32767，IPv6 的規則編號 32768，或 Amazon VPC 主控台<span></span>中的星號 *)。</p> <p>此配額最多可增加至 40，但由於要處理額外規則而增加工作負載，因此網路效能可能會受到影響。</p>

## 網路界面

資源	預設	評論
每個執行個體的網路介面	-	此配額因執行個體類型而異。如需詳細資訊，請參閱 <a href="#">每個執行個體類型每個 ENI 的 IP 地址</a> 。
每個區域的網路介面	5000	此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。

## 路由表

資源	預設	評論
每個 VPC 的路由表	200	主要路由表計數趨近此配額。
每個路由表的路由數 (非傳播路由)	50	<p>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。</p> <p>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。</p> <p>如果您在路由中參考客戶管理的字首清單，則字首清單的項目數目上限等於相同的路由數目。</p>
每個路由表的 BGP 公告路由數 (非傳播路由)	100	此配額無法增加。如果您需要超過 100 個字首，請公告預設路由。

## 安全群組

資源	預設	註解
每個區域的 VPC 安全群組	2500	此配額適用於個別 AWS 帳戶 VPC 和共用 VPC。

資源	預設	註解
		如果您在區域中增加的此配額超過 5000 個安全群組，我們建議您對呼叫進行分頁來說明您的安全群組，以便提升效能。
每個安全群組的傳入或傳出規則	60	<p>每個安全群組可以有 60 個傳入和 60 個傳出規則 (共計 120 個規則)。此配額會分別針對 IPv4 規則和 IPv6 規則執行；例如，安全群組在 IPv4 流量可有 60 個傳入規則，IPv6 流量也有 60 個傳入規則。參考安全群組或 AWS 管理之字首清單 ID 的規則會計為 IPv4 的一個規則和 IPv6 的一個規則。</p> <p>配額變更會同時套用至傳入和傳出規則。此配額乘以每個網路界面的安全群組數量配額，不得超過 1000。例如，如果您將配額提高到 100，則每個網路界面的安全群組數配額就要降至 10。</p> <p>如果您在安全群組規則中參考客戶管理字首清單，則字首清單的項目數上限等於相同數目的安全群組規則。</p>
每個網路界面的安全群組數	5	最多 16 個。此配額會分別針對 IPv4 和 IPv6 規則強制執行。每個網路界面安全群組配額和每個安全群組規則配額的乘積，不能超過 1000。例如，如果您將配額提高到 10，則每個安全群組的規則數配額就要降至 100。

## VPC 對等連線

資源	預設	評論
每個 VPC 的作用中 VPC 對等連接數	50	配額上限是每個 VPC 125 個對等連接數。每個路由表項目數量應據此增加；不過，網路效能可能會受到影響。
未完成的 VPC 對等連接請求數	25	這是您從帳戶請求的未完成 VPC 對等連接請求數配額。
未接受 VPC 對等連接請求的過期時間	1 星期 (168 小時)	此配額無法增加。

## VPC 端點

資源	預設	註解
每個區域的閘道 VPC 端點	20	每個 VPC 您不可有超過 255 個閘道端點。
每個 VPC 的界面 VPC 端點	50	這是 VPC 中端點數量上限的配額。若要增加此配額，請連絡 AWS 支援。

資源	預設	註解
VPC 端點政策大小	20,480 個字元 (包括空格)	此配額無法增加。

## AWS 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 [Site-to-Site VPN 配額](#)。

## VPC 共享

所有標準 VPC 配額均適用於共享 VPC。

資源	預設	註解
每個 VPC 的參與者帳戶	100	<p>這是 VPC 中的子網路可以與其共享的不同參與者帳戶數量的配額。這是每個 VPC 的配額，並且會套用至 VPC 中共享的所有子網路。若要提高此配額，請聯絡 AWS Support。</p> <p>VPC 擁有者可以檢視連接到參與者資源的網路界面和安全群組。因此，AWS 建議您先為 <code>DescribeSecurityGroups</code> 和 <code>DescribeNetworkInterfaces</code> API 呼叫分頁，之後才請求提高此配額。</p>
可與帳戶共享的子網路	100	<p>這是可以與 AWS 帳戶共享的子網路數量上限的配額。若要提高此配額，請聯絡 AWS Support。AWS 建議您先為 <code>DescribeSecurityGroups</code> 和 <code>DescribeSubnets</code> API 呼叫分頁，之後才請求提高此配額。</p>

## Amazon EC2 API 調節

如需 Amazon EC2 調節的相關資訊，請參閱 Amazon EC2 API Reference 中的 [API 請求調節](#)。

# 文件歷史記錄

下表說明《Amazon VPC 使用者指南》和《Amazon VPC Peering Guide》每個版本的重要變更。

update-history-change	update-history-description	update-history-date
電信業者閘道	建立電信業者閘道以允許來自特定位置的電信業者網路的輸入流量，並允許輸出流量到電信業者網路和網際網路。	August 6, 2020
建立時的標籤 (p. 325)	您可以在建立 VPC 對等連線和路由表時新增標籤。	July 20, 2020
建立時的標籤 (p. 325)	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。	June 30, 2020
受管理的字首清單	您可以在字首清單中建立和管理一組 CIDR 區塊。	June 29, 2020
流程日誌增強功能	新的流程記錄欄位可用，您可以為發佈至 CloudWatch Logs 的流程記錄指定自訂格式。	May 4, 2020
流量日誌的標記支援	您可以將標籤新增至流量日誌。	March 16, 2020
在建立 NAT 閘道時套用標籤	您可以在建立 NAT 閘道時新增標籤。	March 9, 2020
VPC 端點和端點服務的條件金鑰	您可以使用 EC2 條件金鑰來控管 VPC 端點和端點服務的存取權。	March 6, 2020
建立 VPC 端點或 VPC 端點服務時新增標籤	您可以在建立 VPC 端點或 VPC 端點服務時新增標籤。	February 5, 2020
流程日誌的最大彙總時間間隔	您可以指定擷取流程並彙總至流程日誌記錄的最長期間。	February 4, 2020
網路邊界群組組態	您可以從 Amazon VPC 主控台為您的 VPC 設定網路邊界群組。	January 22, 2020
私有 DNS 名稱	現在，您可以使用私有 DNS 名稱，從 VPC 內私密存取 AWS PrivateLink 服務。	January 6, 2020
閘道路由表	您可以將路由表與閘道建立關聯，並將傳入 VPC 流量路由至 VPC 中的特定網路界面。	December 3, 2019
流程日誌增強功能	您可指定流程日誌的自訂格式，並選擇在流程日誌紀錄中傳回的欄位。	September 11, 2019
區域間的互連	DNS 主機名稱解析支援 亞太區域 (香港) 區域中的內部區域 VPC 互連連線。	August 26, 2019

<a href="#">AWS Site-to-Site VPN</a>	AWS 受管 VPN 現在稱為 AWS Site-to-Site VPN。	December 18, 2018
<a href="#">VPC 共享</a>	您可以和位於同一個 AWS 組織的多個帳戶共享在相同的 VPC 中的子網路。	November 27, 2018
<a href="#">區域間的互連</a>	您可在不同 AWS 區域中的 VPC 間建立 VPC 互連連線。	November 29, 2017
<a href="#">VPC 端點服務</a>	您可以在 VPC 中建立自有的 AWS PrivateLink 服務，讓其他 AWS 帳戶和使用者透過界面 VPC 端點連線到您的服務。	November 28, 2017
<a href="#">建立預設子網路</a>	您可以在沒有預設子網路的可用區域中建立預設子網路。	November 9, 2017
<a href="#">適用於 AWS 服務的界面 VPC 端點</a>	您可以建立界面端點，私下連線某些 AWS 服務。界面端點是包含私有 IP 地址的網路界面，做為服務的流量進入點。	November 8, 2017
<a href="#">NAT 閘道的標籤支援</a>	您可以標記 NAT 閘道。	September 7, 2017
<a href="#">NAT 閘道的 Amazon CloudWatch 指標</a>	您可以檢視 NAT 閘道的 CloudWatch 指標。	September 7, 2017
<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。	August 31, 2017
<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。	August 29, 2017
<a href="#">DynamoDB 的 VPC 端點</a>	您可以使用 VPC 端點從您的 VPC 存取 Amazon DynamoDB。	August 16, 2017
<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。	August 11, 2017
<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。	July 27, 2017
<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。	December 1, 2016
<a href="#">非 RFC 1918 IP 地址範圍的 DNS 解析支援 (p. 325)</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。	October 24, 2016
<a href="#">VPC 互連的 DNS 解析支援</a>	當對等 VPC 中的執行個體查詢時，您可讓本機 VPC 將公有 DNS 主機名稱解析為私有 IP 地址。	July 28, 2016
<a href="#">過時的安全群組規則</a>	您可識別對等 VPC 中的安全群組規則是否參考您的安全群組，而且可找出過時的安全群組規則。	May 12, 2016



<a href="#">透過 VPC 互連連線使用 ClassicLink</a>	您可以修改 VPC 互連連線，讓本機連結的 EC2-Classic 執行個體與對等 VPC 中的執行個體通訊，反之亦然。	April 26, 2016
<a href="#">NAT 閘道</a>	您可在公有子網路中建立 NAT 閘道，讓私有子網路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。	December 17, 2015
<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。	June 10, 2015
<a href="#">VPC 端點</a>	端點可讓您在 VPC 與另一個 AWS 服務之間建立私有連線，而不需要透過網際網路、透過 VPN 連接、透過 NAT 執行個體或透過 AWS Direct Connect 進行存取。	May 11, 2015
<a href="#">ClassicLink</a>	ClassicLink 可讓您將 EC2-Classic 執行個體連結至您帳戶中的 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。	January 7, 2015
<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。	November 5, 2014
<a href="#">修改子網路的公有 IP 定址屬性</a>	您可以修改您子網路的公有 IP 定址屬性，指出在該子網路中啟動的執行個體是否應該接收公有 IP 地址。	June 21, 2014
<a href="#">VPC 互連</a>	您可在兩個 VPC 之間建立 VPC 互連連線，讓任一 VPC 中的執行個體能使用私有 IP 地址互相通訊。	March 24, 2014
<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。	August 20, 2013
<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。	March 11, 2013
<a href="#">VPC 無所不在 (p. 325)</a>	新增支援五個 AWS 區域的 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 連接。	August 3, 2011
<a href="#">專用執行個體 (p. 325)</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。	March 27, 2011