



AWS PrivateLink

# Amazon Virtual Private Cloud



# Amazon Virtual Private Cloud: AWS PrivateLink

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

# Table of Contents

什麼是 AWS PrivateLink ? .....	1
使用案例 .....	1
使用 VPC 端點 .....	2
定價 .....	2
概念 .....	3
架構圖 .....	3
服務提供者 .....	4
服務消費者 .....	4
AWS PrivateLink 連接 .....	6
私有託管區域 .....	6
開始使用 .....	8
步驟 1：建立包含子網路的 VPC .....	9
步驟 2：啟動執行個體 .....	9
步驟 3：測試 CloudWatch 存取 .....	10
步驟 4：建立要存取的 VPC 端點 CloudWatch .....	11
步驟 5：測試 VPC 端點 .....	12
步驟 6：清除 .....	13
访问 AWS 服務 .....	14
概要 .....	14
DNS 主機名稱 .....	16
DNS 解析 .....	18
私有 DNS .....	18
子網路與可用區域 .....	18
IP 地址類型 .....	21
整合的服務 .....	22
檢視可用的 AWS 服務 名稱 .....	36
檢視服務相關資訊 .....	37
檢視端點政策支援 .....	38
檢視 IPv6 支援 .....	40
建立介面端點 .....	41
必要條件 .....	41
建立 VPC 端點 .....	42
共用子網路 .....	43
設定介面端點 .....	43

新增或移除子網路 .....	44
關聯安全群組 .....	44
編輯 VPC 端點政策 .....	45
啟用私有 DNS 名稱 .....	45
管理標籤 .....	46
接收介面端點事件的提醒 .....	47
建立 SNS 通知 .....	47
新增存取政策 .....	48
新增金鑰政策 .....	48
刪除介面端點 .....	49
閘道端點 .....	50
概要 .....	50
路由 .....	52
安全 .....	52
適用於 Amazon S3 的端點 .....	53
DynamoDB 的端點 .....	62
存取 SaaS 產品 .....	69
概要 .....	69
建立介面端點 .....	70
存取虛擬設備 .....	71
概觀 .....	71
IP 地址類型 .....	73
路由 .....	73
建立 Gateway Load Balancer 端點服務 .....	75
考量事項 .....	75
必要條件 .....	75
建立端點服務 .....	76
讓您的端點服務可用 .....	76
建立 Gateway Load Balancer 端點 .....	77
考量事項 .....	77
必要條件 .....	78
建立端點 .....	78
設定路由 .....	79
管理標籤 .....	80
刪除端點 .....	81
分享您的服務 .....	82

概要 .....	82
DNS 主機名稱 .....	83
私有 DNS .....	84
IP 地址類型 .....	84
建立端點服務 .....	85
考量事項 .....	85
必要條件 .....	86
建立端點服務 .....	86
讓服務消費者可以使用您的端點服務 .....	87
設定端點服務 .....	89
管理許可 .....	89
接受或拒絕連線請求 .....	91
管理負載平衡器 .....	92
關聯私有 DNS 名稱 .....	93
修改支援的 IP 地址類型 .....	94
管理標籤 .....	95
管理 DNS 名稱 .....	96
網域所有權驗證 .....	96
獲取名稱和值 .....	97
新增 TXT 記錄到您的 DNS 伺服器 .....	98
檢查 TXT 記錄是否已發佈 .....	99
對網域驗證問題進行疑難排解 .....	100
接收端點服務事件的提醒 .....	100
建立 SNS 通知 .....	101
新增存取政策 .....	101
新增金鑰政策 .....	102
刪除端點服務 .....	103
身分與存取管理 .....	104
物件 .....	104
使用身分驗證 .....	104
AWS 帳戶 根使用者 .....	105
聯合身分 .....	105
IAM 使用者和群組 .....	106
IAM 角色 .....	106
使用政策管理存取權 .....	107
身分型政策 .....	108

資源型政策 .....	108
存取控制清單 (ACL) .....	108
其他政策類型 .....	108
多種政策類型 .....	109
如何與 IAM AWS PrivateLink 搭配使用 .....	109
身分型政策 .....	110
資源型政策 .....	110
政策動作 .....	111
政策資源 .....	112
政策條件索引鍵 .....	112
ACL .....	113
ABAC .....	113
臨時憑證 .....	114
主體許可 .....	114
服務角色 .....	114
服務連結角色 .....	115
身分型政策範例 .....	115
控制 VPC 端點的使用 .....	115
根據服務擁有者控制 VPC 端點建立 .....	116
控制可為 VPC 端點服務指定的私有 DNS 名稱 .....	117
控制可為 VPC 端點服務指定的服務名稱 .....	117
端點政策 .....	118
考量事項 .....	119
預設端點政策 .....	119
介面端點政策 .....	119
閘道端點的主體 .....	119
更新 VPC 端點政策 .....	120
CloudWatch 指標 .....	121
端點指標和維度 .....	121
端點服務指標和維度 .....	124
檢視 CloudWatch 指標 .....	126
使用內建的 Contributor Insights 規則 .....	127
啟用 Contributor Insights 規則 .....	128
停用 Contributor Insights 規則 .....	129
刪除 Contributor Insights 規則 .....	130
配額 .....	131

---

文件歷史紀錄 .....	132
.....	CXXXIV

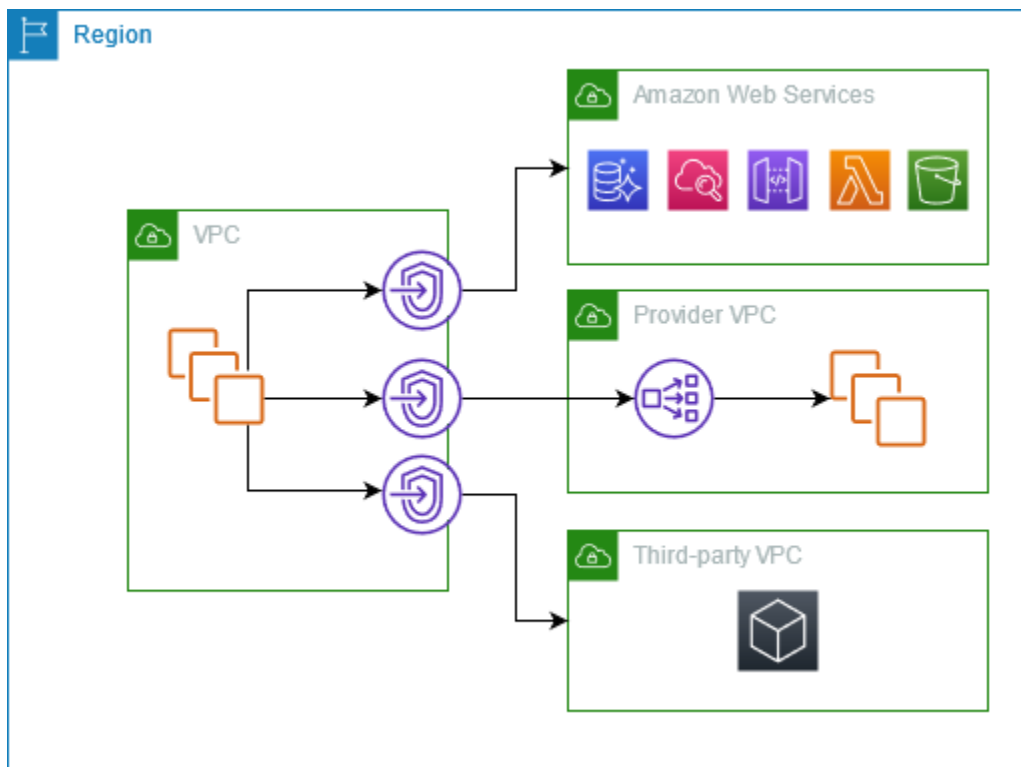
# 什麼是 AWS PrivateLink ?

AWS PrivateLink 這是一種高可用性、可擴充的技術，可讓您將 VPC 私有連線到服務，就像它們位於 VPC 中一樣。您不需要使用網際網路閘道、NAT 裝置、公用 IP 位址、AWS Direct Connect 連線或 AWS Site-to-Site VPN 連線，即可從您的私人子網路與服務進行通訊。因此，您可以控制可從 VPC 連線的特定 API 端點、站點和服務。

## 使用案例

您可以建立 VPC 端點，將 VPC 中的資源連線到與之整合的服務。AWS PrivateLink 您可以建立自己的 VPC 端點服務，並將其提供給其他 AWS 客戶。如需詳細資訊，請參閱 [the section called “概念”](#)。

在下圖中，左側的 VPC 在私有子網中有多個 EC2 執行個體和三個介面 VPC 端點。最頂端的 VPC 端點連線到 Amazon Web Services 服務中間 VPC 端點會連線至由另一個 AWS 帳戶 (VPC 端點服務) 託管的服務。底部 VPC 端點會連線至 AWS Marketplace 合作夥伴服務。



### 進一步了解

- [the section called “概念”](#)
- [访问 AWS 服務](#)



- [存取 SaaS 產品](#)
- [存取虛擬設備](#)
- [分享您的服務](#)

## 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 Management Console— 提供可用於訪問 AWS PrivateLink 資源的 Web 界面。開啟 Amazon VPC 主控台，然後選擇端點或端點服務。
- AWS Command Line Interface (AWS CLI) — 提供一組廣泛的指令 AWS 服務，包括 AWS PrivateLink。如需有關的命令的詳細資訊 AWS PrivateLink，請參閱《AWS CLI 命令參考》中的 [ec2](#)。
- AWS CloudFormation - 建立範本說明您的 AWS 資源。您可以使用範本，佈建並管理這些資源做為單一單位。如需詳細資訊，請參閱下列 AWS PrivateLink 資源：
  - [AWS::EC2::VPCEndpoint](#)
  - [AWS::EC2::EndpointConnection VPC 通知](#)
  - [AWS::EC2::VPCEndpointService](#)
  - [AWS::EC2::EndpointService VPC 許可](#)
  - [AWS::ElasticLoadBalancingV2::LoadBalancer](#)
- AWS SDK — 提供特定於語言的 API。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[建置在其上的工具 AWS](#)。
- Query API — 提供您可以使用 HTTPS 請求呼叫的低層級 API 動作。使用 Query 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 參考》中的[AWS PrivateLink 動作](#)。

## 定價

如需關於 VPC 端點定價的資訊，請參閱 [AWS PrivateLink 定價](#)。

# AWS PrivateLink 概念

您可以使用 Amazon VPC 來定義虛擬私有雲端 (VPC)，這是一個邏輯上隔離的虛擬網路。您可以在 VPC 中啟動 AWS 資源。您可以允許 VPC 中的資源連接至該 VPC 外部的資源。例如，將網際網路閘道新增至 VPC 以允許存取網際網路，或新增 VPN 連線以允許存取您的內部部署網路。或者，使用 AWS PrivateLink 允許 VPC 中的資源使用私有 IP 地址連接到其他 VPC 中的服務，就好像這些服務直接託管在 VPC 中一樣。

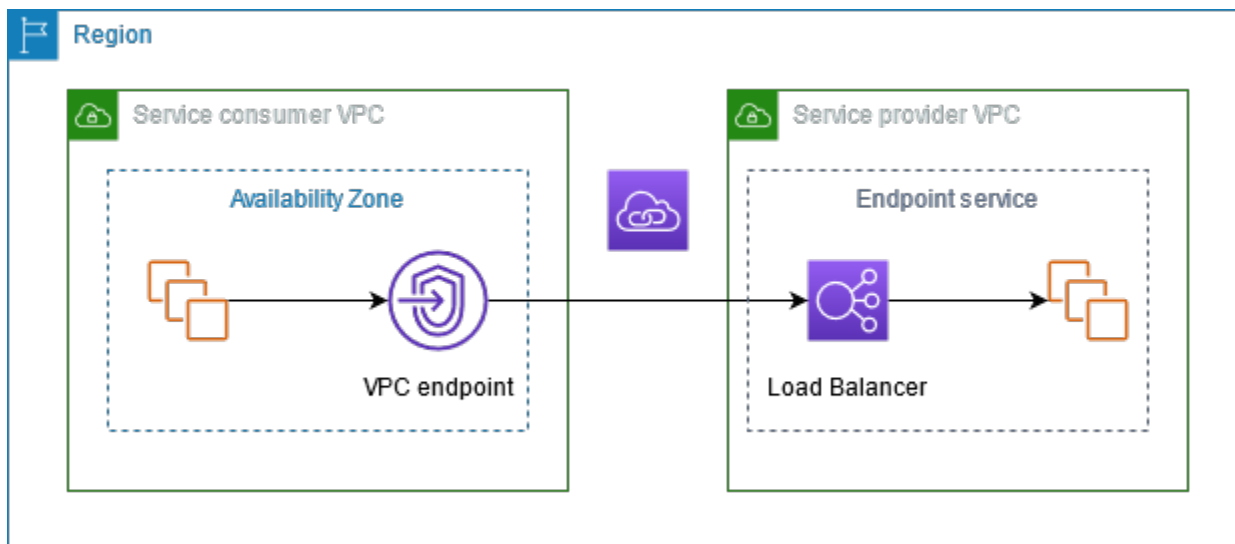
以下是開始使用 AWS PrivateLink 時需要了解的重要概念。

## 目錄

- [架構圖](#)
- [服務提供者](#)
- [服務消費者](#)
- [AWS PrivateLink 連接](#)
- [私有託管區域](#)

## 架構圖

下圖提供 AWS PrivateLink 運作方式的高階概觀。服務消費者可建立介面 VPC 端點，以連接至服務提供者託管的端點服務。



## 服務提供者

服務所有者是服務提供者。服務供應商包括 AWS 合作夥伴和其他 AWS 帳戶。服務提供者可以使用 AWS 資源 (例如 EC2 執行個體) 或使用現場部署伺服器來託管其服務。

### 概念

- [端點服務](#)
- [服務名稱](#)
- [服務狀態](#)

## 端點服務

服務提供者建立端點服務，使其服務在區域中可用。建立端點服務時，服務提供者必須指定負載平衡器。負載平衡器會收到來自服務消費者的請求，並將它們傳送至您的服務。

根據預設，服務消費者無法使用您的端點服務。您必須新增允許特定 AWS 主體連線到端點服務的權限。

## 服務名稱

每個端點服務均由服務名稱識別。服務消費者在建立 VPC 端點時必須指定服務名稱。服務用戶可以查詢的服務名稱 AWS 服務。服務提供者必須向服務消費者分享其服務名稱資訊。

## 服務狀態

以下是端點服務的可能狀態：

- Pending - 正在建立端點服務。
- Available - 端點服務可用。
- Failed - 無法建立端點服務。
- Deleting - 服務提供者已刪除端點服務，且正在進行刪除。
- Deleted - 端點服務已刪除。

## 服務消費者

服務的使用者是服務消費者。服務消費者可以從 AWS 資源 (例如 EC2 執行個體) 或現場部署伺服器存取端點服務。

## 概念

- [VPC 端點](#)
- [端點網路介面](#)
- [端點政策](#)
- [端點狀態](#)

## VPC 端點

服務消費者可以建立 VPC 端點，將其 VPC 連接到端點服務。服務消費者在建立 VPC 端點時必須指定端點服務的服務名稱。有多種類型的 VPC 端點。您必須建立端點服務需要的 VPC 端點類型。

- **Interface** – 建立介面端點以將 TCP 流量傳送至端點服務。使用 DNS 來解析目的地為端點服務的流量。
- **GatewayLoadBalancer** - 建立 Gateway Load Balancer 端點，使用私有 IP 地址將流量傳送至虛擬設備機群。您可以使用路由表將流量從您的 VPC 路由至 Gateway Load Balancer 端點。Gateway Load Balancer 會將流量分配給虛擬設備，並可隨需擴展。

還有另一種 Gateway VPC 端點類型，這種類型的端點會建立閘道端點，將流量傳送至 Amazon S3 或 DynamoDB。與其他類型的 VPC 端點不同 AWS PrivateLink，閘道端點不會使用。如需詳細資訊，請參閱 [the section called “閘道端點”](#)。

## 端點網路介面

端點網路介面是一個由請求者管理的網路介面，可作為目的地為端點服務的流量進入點。對於您在建立 VPC 端點時指定的每個子網，我們會在子網中建立端點網路介面。

如果 VPC 端點支援 IPv4，其端點網路介面具有 IPv4 地址。如果 VPC 端點支援 IPv6，其端點網路介面具有 IPv6 地址。無法從網際網路連線端點網路界面的 IPv6 地址。如果您使用 IPv6 地址描述端點網路介面，請注意 denyAllIgwTraffic 已啟用。

端點網路介面的 IP 地址在其 VPC 端點的存留期間不會變更。

## 端點政策

VPC 端點政策為 IAM 資源政策，您可將其連接至 VPC 端點。它會決定哪些主體可以使用 VPC 端點存取端點服務。預設的 VPC 端點政策允許 VPC 端點上所有資源的所有主體進行所有操作。

## 端點狀態

建立 VPC 端點時，端點服務會收到連線請求。服務提供者可以接受或拒絕該請求。如果服務提供者接受該請求，服務消費者可以在 VPC 端點進入 Available 狀態後使用它。

以下是 VPC 端點的可能狀態：

- PendingAcceptance - 連線請求處於待處理狀態。這是手動接受請求的初始狀態。
- Pending - 服務提供者接受連線請求。這是自動接受請求的初始狀態。如果服務消費者修改 VPC 端點，則 VPC 端點會回到此狀態。
- Available - VPC 端點可供使用。
- Rejected - 服務提供者拒絕連線請求。服務提供者也可以在其可供使用之後拒絕連線。
- Expired - 連線請求已過期。
- Failed - 無法使 VPC 端點可用。
- Deleting - 服務消費者已刪除 VPC 端點，且正在進行刪除。
- Deleted - 已刪除 VPC 端點。

## AWS PrivateLink 連接

VPC 的流量會使用 VPC 端點與端點服務之間的連線，傳送到端點服務。VPC 端點和端點服務之間的流量會保留在 AWS 網路內，而不會遍歷公用網際網路。

服務提供者會新增[權限](#)，供服務取用者存取端點服務。服務取用者會啟動連線，而服務提供者會接受或拒絕連線請求。

有了介面 VPC 端點，服務取用者可以使用[端點政策](#)控制哪些 IAM 主體可以使用 VPC 端點存取端點服務。

## 私有託管區域

託管區域是一個 DNS 記錄容器，它定義如何路由網域或子網域的流量。對於公有託管區域，記錄指定如何在網際網路上路由流量。對於私有託管區域，記錄指定如何在您的 VPC 中路由流量。

您可以設定 Amazon Route 53，將網域流量路由到 VPC 端點。如需詳細資訊，請參閱[使用網域名稱將流量路由到 VPC 端點](#)。

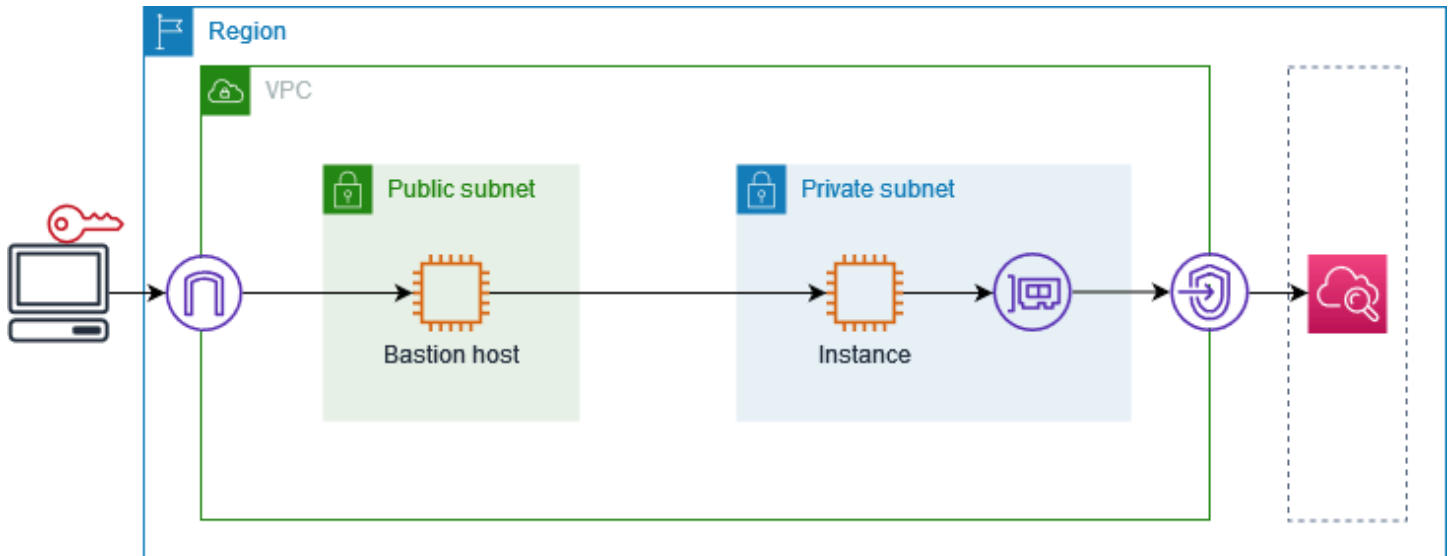
您可以使用 Route 53 來設定分割地平線 DNS，您可以在其中針對公用網站和提供支援的端點服務使用相同的網域名稱。AWS PrivateLink 來自消費者 VPC 的公有主機名稱的 DNS 請求會解析為端點網路

介面的私有 IP 地址，但來自 VPC 外部的請求仍會繼續解析為公有端點。如需詳細資訊，請參閱[檢閱路由流量的 DNS 機制並對 AWS PrivateLink 部署啟用容錯移轉](#)。

# 開始使用 AWS PrivateLink

本教學課程示範如何使用將私有子網路中的 EC2 執行個體傳送請求至 CloudWatch Amazon AWS PrivateLink。

下圖提供此情況如何運作的概觀。若要從電腦連線到私有子網路中的執行個體，您必須先連線到公有子網路中的堡壘主機。堡壘主機和執行個體都必須使用相同的金鑰對。由於私密金鑰的 .pem 檔案位於您的電腦，而不是堡壘主機上，因此您將使用 SSH 金鑰轉送。然後，您可以從堡壘主機連線至執行個體，而無需在 ssh 命令中指定 .pem 檔案。在您為其設定 VPC 端點之後 CloudWatch，來自目的地執行個體的流量會解析 CloudWatch 為端點網路介面，然後 CloudWatch 使用 VPC 端點傳送至。



針對測試目的，您可以使用單一可用區域。在生產環境中，建議您使用至少兩個可用區域以獲得低延遲和高可用性。

## 任務

- [步驟 1：建立包含子網路的 VPC](#)
- [步驟 2：啟動執行個體](#)
- [步驟 3：測試 CloudWatch 存取](#)
- [步驟 4：建立要存取的 VPC 端點 CloudWatch](#)
- [步驟 5：測試 VPC 端點](#)
- [步驟 6：清除](#)

## 步驟 1：建立包含子網路的 VPC

按照以下程序建立包含公有子網路和私有子網路的 VPC。

若要建立 VPC

1. 前往 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 選擇建立 VPC。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 針對自動產生名稱標籤，輸入 VPC 的名稱。
5. 若要設定子網路，請執行下列動作：
  - a. 對於 Number of Availability Zones (可用區域數量)，請根據您的需求選擇 1 或 2。
  - b. 針對 Number of public subnets (公用子網路數量)，請確定每個可用區域有一個公用子網路。
  - c. 針對 Number of private subnets (私有子網路數量)，請確定每個可用區域有一個私有子網路。
6. 選擇建立 VPC。

## 步驟 2：啟動執行個體

使用您在上一個步驟中建立的 VPC，在公有子網路中啟動堡壘主機，並在私有子網路中啟動執行個體。

必要條件

- 使用 .pem 格式建立金鑰對。啟動堡壘主機和執行個體時，您必須選擇此金鑰對。
- 為堡壘主機建立安全群組，以允許來自您電腦 CIDR 區塊的傳入 SSH 流量。
- 為執行個體建立安全群組，以允許來自您堡壘主機安全群組的傳入 SSH 流量。
- 建立 IAM 執行個體設定檔並附加 CloudWatchReadOnly 存取政策。

啟動堡壘主機

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 選擇啟動執行個體。
3. 針對 Name (名稱)，輸入堡壘主機的名稱。



- 保留預設映像和執行個體類型。
- 針對 Key pair (金鑰對)，選擇您的金鑰對。
- 針對 Network settings (網路設定)，執行下列操作：
  - 在 VPC 中，選擇您的 VPC。
  - 針對 Subnet (子網路)，選擇公有子網路。
  - 在 Auto-assign public IP (自動指派公有 IP) 中，選擇 Enable (啟用)。
  - 對於 Firewall (防火牆)，請選擇 Select existing security group (選取現有的安全群組)，然後選擇堡壘主機的安全群組。
- 選擇啟動執行個體。

### 啟動執行個體

- 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
- 選擇啟動執行個體。
- 對於 Name (名稱)，請輸入執行個體名稱。
- 保留預設映像和執行個體類型。
- 針對 Key pair (金鑰對)，選擇您的金鑰對。
- 針對 Network settings (網路設定)，執行下列操作：
  - 在 VPC 中，選擇您的 VPC。
  - 針對 Subnet (子網路)，選擇私有子網路。
  - 針對 Auto-assign public IP (自動指派公有 IP) 中，選擇 Disable (停用)。
  - 對於 Firewall (防火牆)，請選擇 Select existing security group (選取現有的安全群組)，然後選擇執行個體的安全群組。
- 展開 Advanced Details (進階詳細資訊)。在 IAM instance profile (IAM 執行個體設定檔) 中，選擇您的 IAM 執行個體設定檔。
- 選擇啟動執行個體。

## 步驟 3：測試 CloudWatch 存取

請使用下列程序來確認執行個體無法存取 CloudWatch。您將使用的唯讀 AWS CLI 命令來執行此操作 CloudWatch。

## 若要測試 CloudWatch 存取

1. 從您的電腦中，使用下列命令將金鑰對新增至 SSH 代理程式，其中 *key.pem* 是 .pem 檔案的名稱。

```
ssh-add ./key.pem
```

如果您收到金鑰對權限過於開放的錯誤訊息，請執行下列命令，然後重試上一個命令。

```
chmod 400 ./key.pem
```

2. 從您的電腦連接至堡壘主機。您必須指定 -A 選項、執行個體使用者名稱 (例如 ec2-user) 和堡壘主機的公用 IP 地址。

```
ssh -A ec2-user@bastion-public-ip-address
```

3. 從堡壘主機連接至執行個體。您必須指定執行個體使用者名稱 (例如 ec2-user) 和執行個體的私有 IP 地址。

```
ssh ec2-user@instance-private-ip-address
```

4. 在執行個體 CloudWatch [體上執行清單公制指令](#)，如下所示。針對 --region 選項，請指定您建立 VPC 的「區域」。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

5. 命令會在幾分鐘後逾時。這表明您無法使用目前的 VPC 組態 CloudWatch 從執行個體存取。

```
Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
```

6. 與您的執行個體保持連線。建立 VPC 端點後，您將再次嘗試此 list-metrics 命令。

## 步驟 4：建立要存取的 VPC 端點 CloudWatch

使用下列程序建立連線到的 VPC 端點。CloudWatch

### 先決條件

為允許流量傳輸的 VPC 端點建立安全群組。CloudWatch 例如，新增規則，允許來自 VPC CIDR 區塊的 HTTPS 流量。

若要為以下項目建立 VPC 端點 CloudWatch

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. 選擇建立端點。
4. 在 Name tag (名稱標籤) 中，輸入端點的名稱。
5. 對於 Service category (服務類別)，選擇 AWS 服務。
6. 針對 Service (服務)，請選取 com.amazonaws.*region*.monitoring。
7. 針對 VPC，選取您的 VPC。
8. 針對 Subnets (子網路)，請選取可用區域，然後選取私有子網路。
9. 針對 Security group (安全群組)，請選取 VPC 端點的安全群組。
10. 對於 Policy (政策)，選取 Full access (完整存取)，以允許 VPC 端點上所有資源的所有主體進行所有操作。
11. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
12. 選擇建立端點。初始狀態為 Pending (等待中)。在進行下一個步驟之前，請先等待狀態變為 Available (可用)。這可能需要幾分鐘的時間。

## 步驟 5：測試 VPC 端點

確認 VPC 端點正在將要求從您的執行個體傳送到 CloudWatch。

若要測試 VPC 端點

在執行個體上執行以下命令。針對 `--region` 選項，請指定您建立 VPC 端點的區域。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

如果你得到一個響應，即使是空結果的響應，那麼你連接到 CloudWatch 使用 AWS PrivateLink。

如果出 UnauthorizedOperation 現錯誤，請確保執行個體具有允許存取的 IAM 角色 CloudWatch。

如果請求逾時，請確認下列事項：

- 端點的安全性群組允許流量到達 CloudWatch。
- `--region` 選項可指定您在其中建立 VPC 端點的區域。

## 步驟 6：清除

如果您不再需要針對此教學課程建立的堡壘主機和執行個體，則可以將其終止。

### 終止執行個體

1. 在 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選取兩個測試執行個體，然後選取 Instance state (執行個體狀態)、Terminate instance (終止執行個體)。
4. 出現確認提示時，請選擇終止。

如果您不再需要該 VPC 端點，可以將其刪除。

### 刪除 VPC 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)。
3. 選取 VPC 端點。
4. 選擇 Actions (動作)、Delete VPC endpoints (刪除 VPC 端點)。
5. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

# AWS 服務 通過訪問 AWS PrivateLink

您存取 AWS 服務 使用端點。預設服務端點為公有介面，因此您必須將網際網路閘道新增至 VPC，以便流量可以從 VPC 傳送到 AWS 服務。如果此組態無法滿足您的網路安全性需求，您可 AWS PrivateLink 以使用將 VPC 連線到 AWS 服務 如同 VPC 中一樣，無需使用網際網路閘道。

您可以私下存取 AWS 服務 與 AWS PrivateLink 使用 VPC 端點整合的。您可以建置和管理應用程式堆疊的所有層級，而無需使用網際網路閘道。

## 定價

您需按每個可用區域佈建介面 VPC 端點的每小時計費。您還需要按處理的 GB 資料計費。如需詳細資訊，請參閱 [AWS PrivateLink 定價](#)。

## 目錄

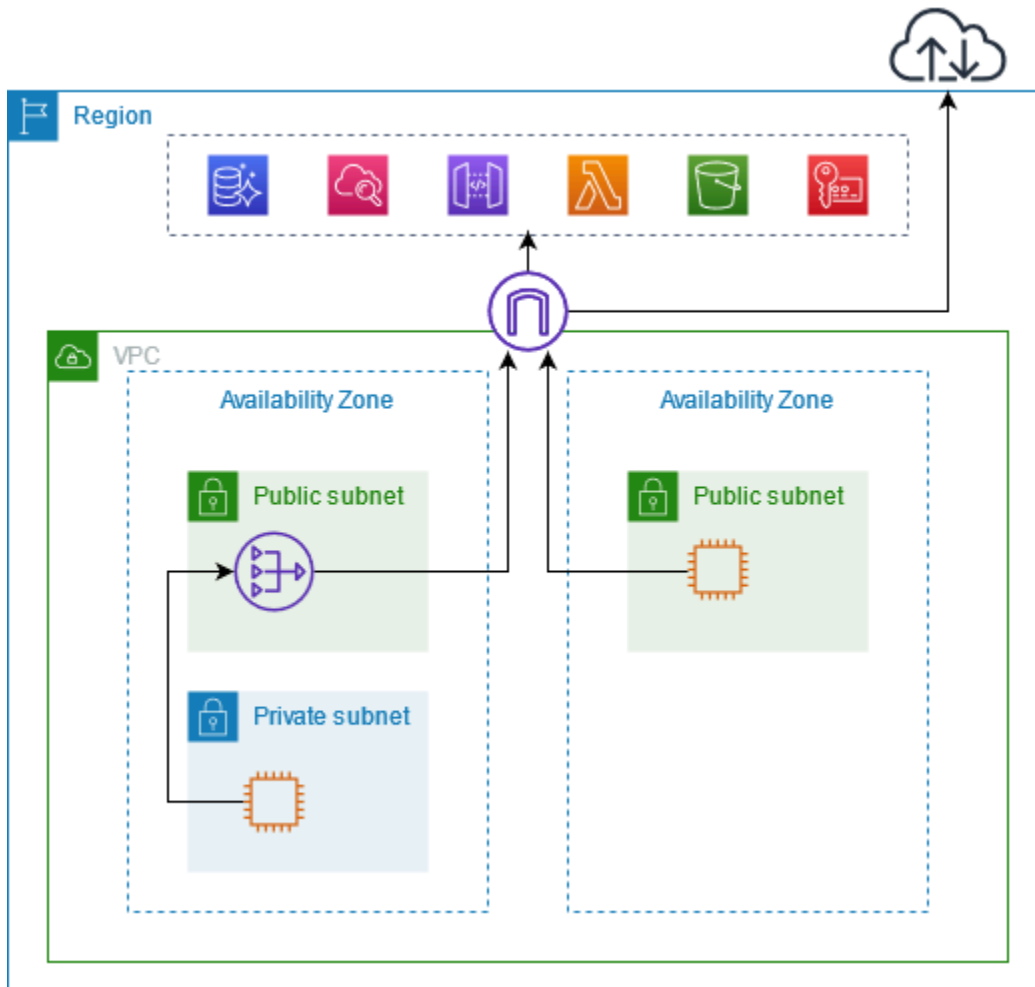
- [概要](#)
- [DNS 主機名稱](#)
- [DNS 解析](#)
- [私有 DNS](#)
- [子網路與可用區域](#)
- [IP 地址類型](#)
- [AWS 服務 與整合 AWS PrivateLink](#)
- [AWS 服務 使用接口 VPC 端點訪問](#)
- [設定介面端點](#)
- [接收介面端點事件的提醒](#)
- [刪除介面端點](#)
- [閘道端點](#)

## 概要

您可以通 AWS 服務 過其公共服務端點訪問，也可以 AWS 服務 使用 AWS PrivateLink. 此概觀會比較這些方法。

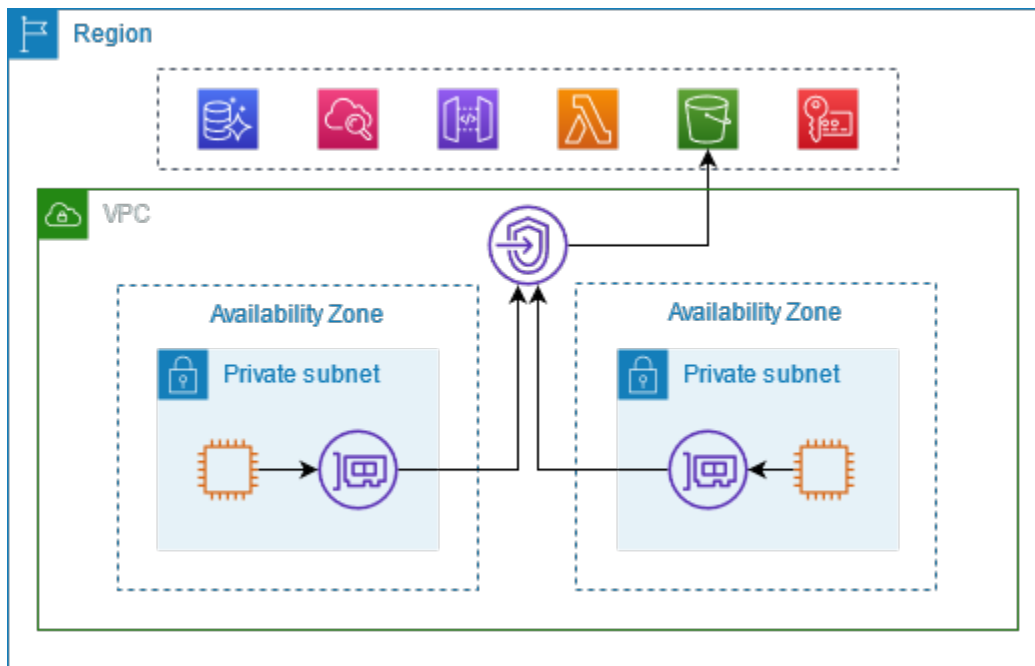
### 透過公有服務端點存取

下圖顯示執行個體如何透過 AWS 服務 過公用服務端點存取。AWS 服務 從公用子網路中執行個體傳送至的流量會路由至 VPC 的網際網路閘道，然後路由至 . AWS 服務從私有子網中的執行個體到 AWS 服務的流量會路由到 NAT 閘道，然後路由至 VPC 的網際網路閘道，最後再路由至 AWS 服務。雖然此流量遍歷 Internet 閘道，但不會離開 AWS 網路。



## 通過 Connect AWS PrivateLink

下圖顯示執行個體的存取方 AWS 服務 式 AWS PrivateLink。首先，您要建立介面 VPC 端點，該端點會在 VPC 中的子網路與 AWS 服務 使用網路介面之間建立連線。目的地的流量會使用 DNS 解析為端點網路介面的私有 IP 位址，然後 AWS 服務 使用 VPC 端點與 . AWS 服務 AWS 服務



AWS 服務 自動接受連線要求。服務無法透過 VPC 端點向資源發起請求。

## DNS 主機名稱

大多數 AWS 服務 提供公共區域端點，其語法如下。

```
protocol://service_code.region_code.amazonaws.com
```

例如，us-east-2 CloudWatch 中 Amazon 的公共端點如下。

```
https://monitoring.us-east-2.amazonaws.com
```

使用時 AWS PrivateLink，您可以使用私有端點將流量傳送到服務。當您建立介面 VPC 端點時，我們會建立區域和區域 DNS 名稱，您可以使用這些名稱與 VPC 進行 AWS 服務 通訊。

介面 VPC 端點的區域 DNS 名稱具有下列語法：

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

區域 DNS 名稱具有下列語法：

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

當您建立的介面 VPC 端點時 AWS 服務，您可以啟用[私有 DNS](#)。使用私有 DNS，您可以繼續使用其公有端點的 DNS 名稱向服務發出請求，同時利用經由介面 VPC 端點的私有連線。如需詳細資訊，請參閱 [the section called “DNS 解析”](#)。

以下 [describe-vpc-endpoints](#) 命令會顯示介面端點的 DNS 項目。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
  VpcEndpoints[*].DnsEntries
```

以下是啟用私 CloudWatch 有 DNS 名稱之 Amazon 介面端點的範例輸出。第一項是私有區域端點 (private Regional endpoint)。接下來的三項是私有區域端點 (private zonal endpoint)。最後一項來自隱藏的私有託管區域，它將針對公有端點的請求解析為端點網路介面的私有 IP 地址。

```
[
  [
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
      "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
      "DnsName": "monitoring.us-east-2.amazonaws.com",
      "HostedZoneId": "Z06320943MM0WYG6MAVL9"
    }
  ]
]
```



## DNS 解析

我們為您的介面 VPC 端點建立的 DNS 記錄是公開的。因此，這些 DNS 名稱可公開解析。不過，來自 VPC 外部的 DNS 請求仍會傳回端點網路介面的私有 IP 地址，因此除非您可以存取 VPC，否則這些 IP 地址無法用於存取端點服務。

## 私有 DNS

如果您為介面 VPC 端點啟用私有 DNS，且您的 VPC 同時啟用了 [DNS 主機名稱和 DNS 解析](#)，我們會為您建立隱藏的 AWS 受管私有託管區域。託管區域包含服務之預設 DNS 名稱的記錄集，該服務可將其解析為 VPC 中端點網路介面的私有 IP 地址。因此，如果您現有的應用程式會 AWS 服務使用公用區域端點傳送要求至，則這些要求現在會透過端點網路介面進行，而不需要您對這些應用程式進行任何變更。

建議您為 VPC 端點啟用私人 DNS 名稱。AWS 服務如此可確保使用公用服務端點的要求 (例如透過 AWS SDK 發出的要求) 會解析至您的 VPC 端點。

Amazon 為您的 VPC 提供 DNS 伺服器，名為 [Route 53 Resolver](#)。Route 53 Resolver 會自動解析本機 VPC 網域名稱和私有託管區域中的記錄。但是，您無法從 VPC 外部使用 Route 53 Resolver。如果想要從內部部署網路存取 VPC 端點，可以使用 Route 53 Resolver 端點和 Resolver 規則。如需詳細資訊，請參閱 [AWS Transit Gateway 與 AWS PrivateLink 與整合 Amazon Route 53 Resolver](#)。

## 子網路與可用區域

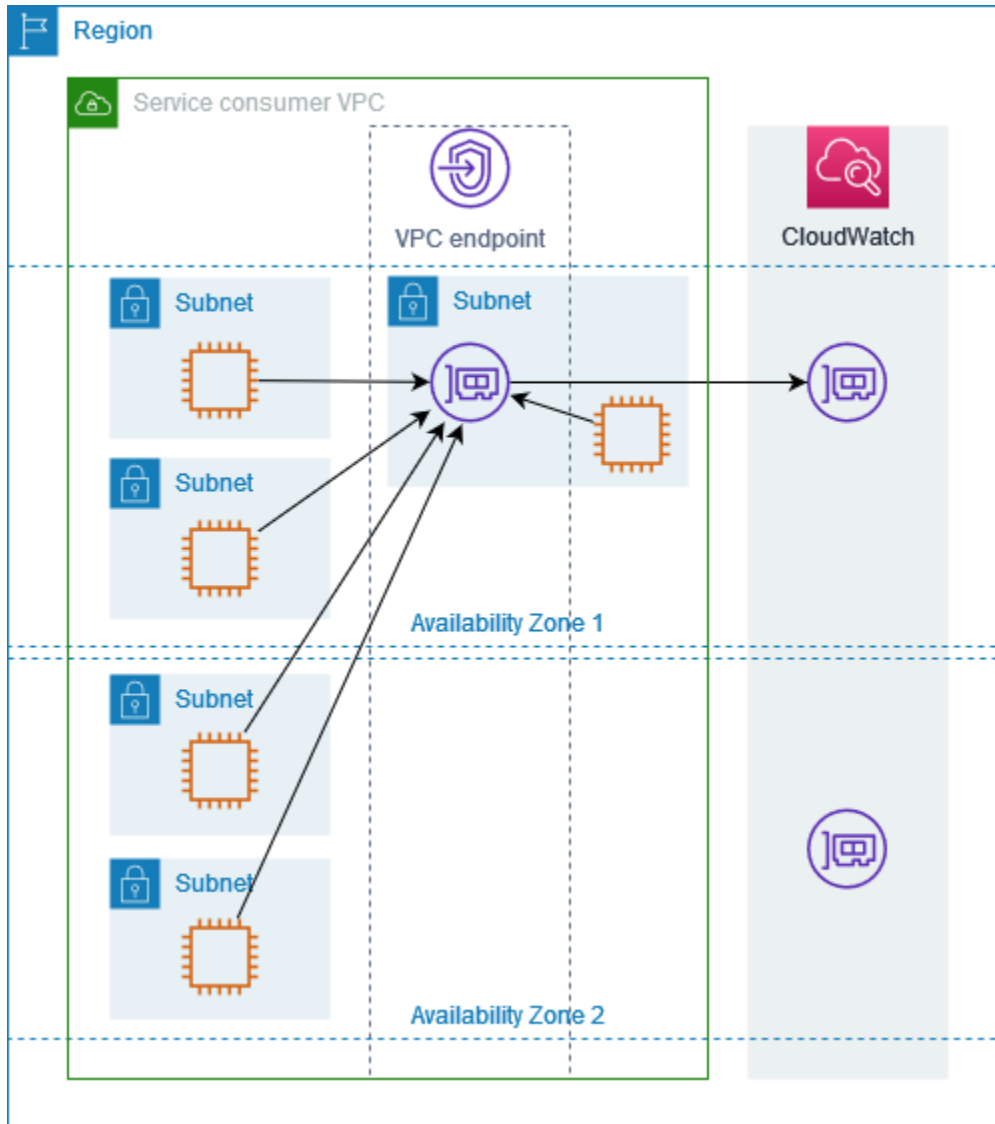
您可以將 VPC 端點設定為每個可用區域一個子網路。我們會在子網路中建立 VPC 端點的端點網路介面。我們會根據 VPC 端點的 [IP 地址類型](#)，從其子網路中將 IP 地址指派給每個端點網路介面。端點網路介面的 IP 地址在其 VPC 端點的存留期間不會變更。

在生產環境中，為了獲得高可用性和彈性，建議您執行以下操作：

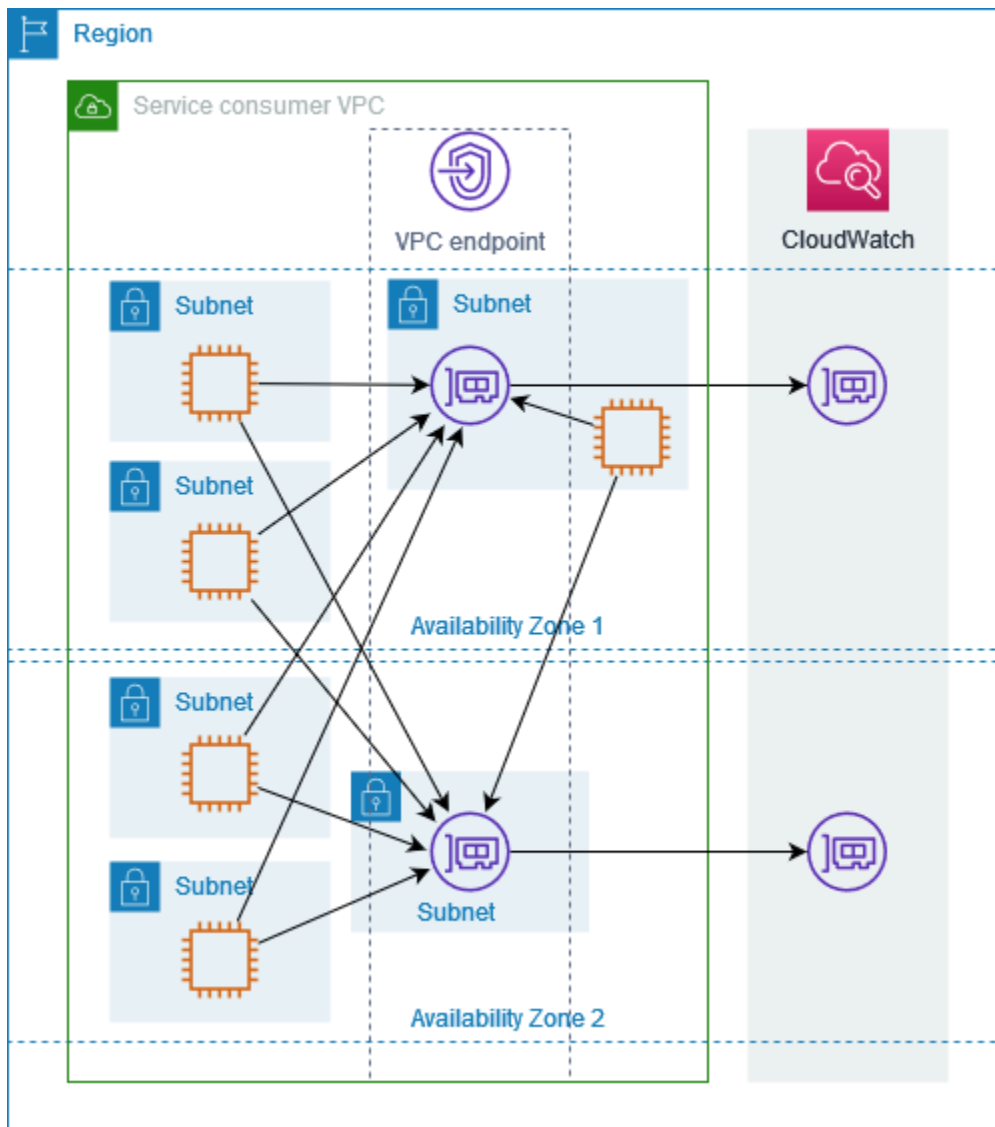
- 每個 VPC 端點至少設定兩個可用區域，並部署必須存取這些可用區域 AWS 服務中的 AWS 資源。
- 設定 VPC 端點的私有 DNS 名稱。
- 使用其區域 DNS 名稱 (也稱為公用端點) AWS 服務來存取。

下圖顯示在單一可用區域中 CloudWatch 具有端點網路界面的 Amazon VPC 端點。當 VPC 中任何子網路中的任何資源 CloudWatch 使用其公有端點存取 Amazon 時，我們會將流量解析為端點網路界面的

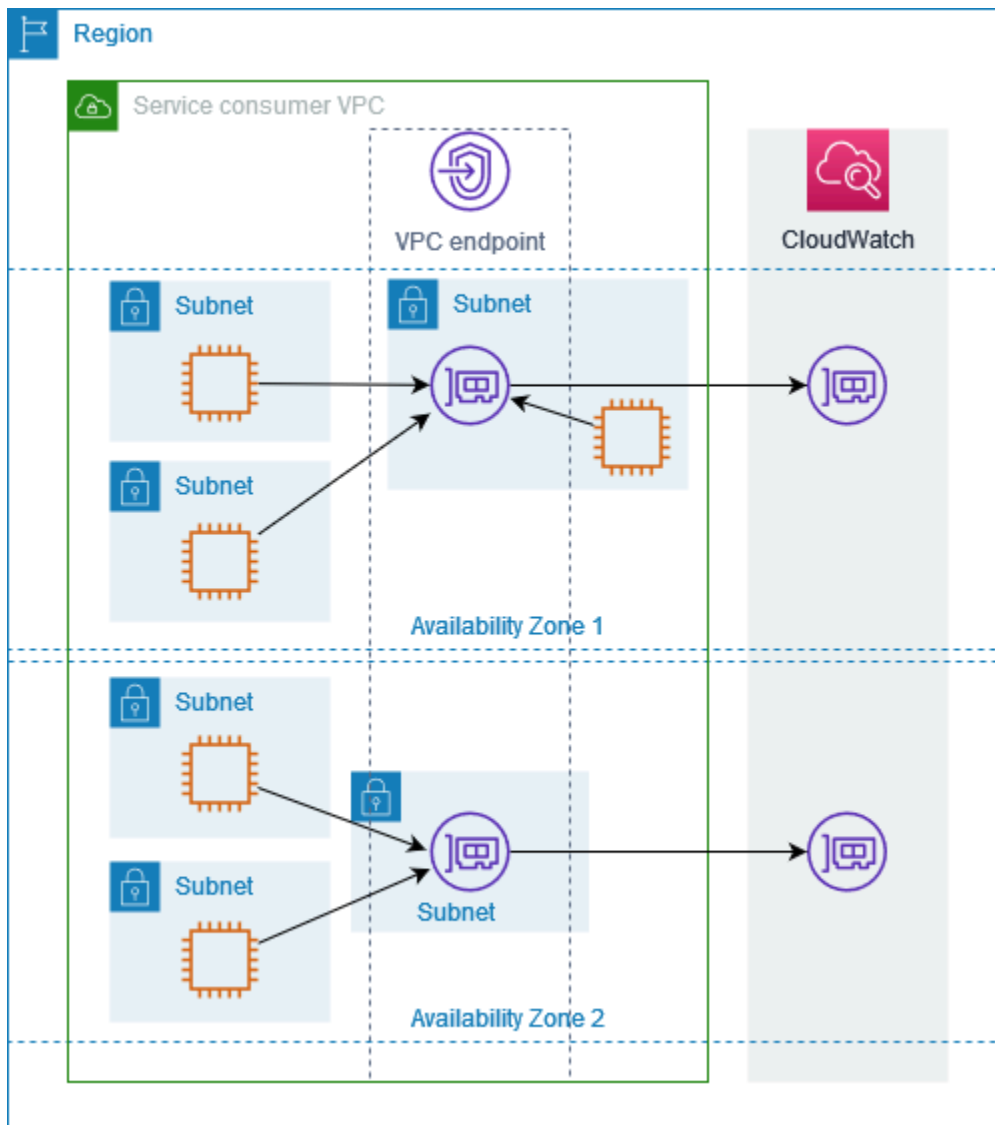
IP 位址。這包括來自其他可用區域中子網路的流量。但是，如果可用區域 1 受損，可用區域 2 中的資源將無法存取 Amazon CloudWatch。



下圖顯示在兩個可用區域中 CloudWatch 具有端點網路界面的 Amazon VPC 端點。當 VPC 中任何子網路中的任何資源使用其公有端點存取 Amazon CloudWatch 時，我們會使用循環配置資源演算法在它們之間交替選取運作良好的端點網路界面。接著，我們會將流量解析為所選端點網路界面的 IP 地址。



如果這更適合您的使用案例，則可以使用同一可用區域中的端點網路介面，將資源的流量傳送到 AWS 服務。若要執行此操作，請使用私有區域端點或端點網路介面的 IP 地址。



## IP 地址類型

AWS 服務 可以通過其私有端點支持 IPv6，即使它們不通過其公共端點支持 IPv6。支援 IPv6 的端點可以使用 AAAA 記錄回應 DNS 查詢。

為介面端點啟用 IPv6 的要求

- AWS 服務 必須使其服務端點可透過 IPv6 使用。如需詳細資訊，請參閱 [the section called “檢視 IPv6 支援”](#)。
- 介面端點的 IP 地址類型必須與介面端點的子網相容，如下所述：
  - IPv4 - 將 IPv4 地址指派給您的端點網路介面。只有當所有選取子網都具有 IPv4 地址範圍時，才支援此選項。

- IPv6 - 將 IPv6 地址指派給您的端點網路介面。只有當所有選取的子網都是 IPv6 子網時，才支援此選項。
- Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路介面。只有當所有選取的子網都具有 IPv4 和 IPv6 地址範圍時，才支援此選項。

如果介面 VPC 端點支援 IPv4，則端點網路介面具有 IPv4 地址。如果介面 VPC 端點支援 IPv6，則端點網路介面具有 IPv6 地址。無法從網際網路連線端點網路介面的 IPv6 地址。如果您使用 IPv6 地址描述端點網路介面，請注意 denyAllIgwTraffic 已啟用。

## AWS 服務 與整合 AWS PrivateLink

以下內容 AWS 服務 與 AWS PrivateLink. 您可以建立 VPC 端點以便私下連接這些服務，就好像在您自己的 VPC 中執行一樣。

選擇AWS 服務欄中的連結，以查看與之整合之服務的說明文件 AWS PrivateLink。[服務名稱] 資料行包含您在建立介面 VPC 端點時指定的服務名稱，或指示服務管理端點。

AWS 服務	服務名稱
Access Analyzer	com.amazonaws. <i>region</i> .access-analyzer
<a href="#">AWS Account Management</a>	com.amazonaws. <i>region</i> .account
<a href="#">Amazon API Gateway</a>	com.amazonaws. <i>region</i> .execute-api
<a href="#">AWS AppConfig</a>	com.amazonaws. <i>region</i> .appconfig com.amazonaws. <i>region</i> .appconfigdata
<a href="#">AWS App Mesh</a>	com.amazonaws. <i>region</i> .appmesh com.amazonaws. <i>region</i> .appmesh-envoy-management
<a href="#">AWS 應用亞軍</a>	com.amazonaws. <i>region</i> .apprunner
<a href="#">AWS App Runner 服務</a>	com.amazonaws. <i>region</i> .apprunner.requests
<a href="#">Application Auto Scaling</a>	com.amazonaws. <i>region</i> .application-autoscaling

AWS 服務	服務名稱
<a href="#">AWS 應用程式遷移</a>	com.amazonaws. <i>region</i> .mgn
<a href="#">Amazon AppStream 2.0</a>	com.amazonaws. <i>region</i> .appstream.api
	com.amazonaws. <i>region</i> .appstream.streaming
<a href="#">AWS AppSync</a>	com.amazonaws. <i>region</i> .appsync-api
<a href="#">Amazon Athena</a>	com.amazonaws. <i>region</i> .athena
<a href="#">AWS Audit Manager</a>	com.amazonaws. <i>region</i> .auditmanager
<a href="#">Amazon Aurora</a>	com.amazonaws. <i>region</i> .rds
<a href="#">AWS Auto Scaling</a>	com.amazonaws. <i>region</i> .autoscaling-plans
<a href="#">AWS B2B 資料交換</a>	com.amazonaws. <i>region</i> .b2bi
<a href="#">AWS Backup</a>	com.amazonaws. <i>region</i> .backup
	com.amazonaws. <i>region</i> .backup-gateway
<a href="#">AWS Batch</a>	com.amazonaws. <i>region</i> .batch
<a href="#">Amazon Bedrock</a>	com.amazonaws. <i>region</i> .bedrock
	COM. 亞馬遜。 ##. 基礎代理
	com.amazonaws. <i>region</i> .bedrock-agent-runtime
	com.amazonaws. <i>region</i> .bedrock-runtime
AWS Billing Conductor	com.amazonaws. <i>region</i> .billingconductor
<a href="#">Amazon Braket</a>	com.amazonaws. <i>region</i> .braket
<a href="#">AWS Clean Rooms</a>	com.amazonaws. <i>region</i> .cleanrooms
<a href="#">AWS 無塵室 ML</a>	COM. 亞馬遜。 ##. 無塵室毫升

AWS 服務	服務名稱
<a href="#">AWS Cloud Control API</a>	com.amazonaws. <i>region</i> .cloudcontrolapi
	com.amazonaws. <i>region</i> .cloudcontrolapi-fips
<a href="#">Amazon 雲端目錄</a>	com.amazonaws. <i>region</i> .clouddirectory
<a href="#">AWS CloudFormation</a>	com.amazonaws. <i>region</i> .cloudformation
<a href="#">AWS CloudHSM</a>	com.amazonaws. <i>region</i> .cloudhsmv2
<a href="#">AWS Cloud Map</a>	com.amazonaws. <i>region</i> .servicediscovery
	com.amazonaws. <i>region</i> .servicediscovery-fips
	com.amazonaws. <i>region</i> .data-servicediscovery
	com.amazonaws. <i>region</i> .data-servicediscovery-fips
<a href="#">AWS CloudTrail</a>	com.amazonaws. <i>region</i> .cloudtrail
<a href="#">Amazon CloudWatch</a>	com.amazonaws. <i>region</i> .evidently
	com.amazonaws. <i>region</i> .evidently-dataplane
	com.amazonaws. <i>region</i> .monitoring
	com.amazonaws. <i>region</i> .rum
	com.amazonaws. <i>region</i> .rum-dataplane
	com.amazonaws. <i>region</i> .synthetics
<a href="#">Amazon CloudWatch 日誌</a>	com.amazonaws. <i>region</i> .logs
Amazon CloudWatch 網絡監控	COM. 亞馬遜。 ##. ###視器
<a href="#">AWS CodeArtifact</a>	com.amazonaws. <i>region</i> .codeartifact.api
	com.amazonaws. <i>region</i> .codeartifact.repositories

AWS 服務	服務名稱
<a href="#">AWS CodeBuild</a>	com.amazonaws. <i>region</i> .codebuild
	com.amazonaws. <i>region</i> .codebuild-fips
<a href="#">AWS CodeCommit</a>	com.amazonaws. <i>region</i> .codecommit
	com.amazonaws. <i>region</i> .codecommit-fips
	com.amazonaws. <i>region</i> .git-codecommit
	com.amazonaws. <i>region</i> .git-codecommit-fips
<a href="#">AWS CodeConnections</a>	COM. 亞馬遜。 ##. ##連接 .api
	com.amazonaws. <i>region</i> .codestar-connections.api
<a href="#">AWS CodeDeploy</a>	com.amazonaws. <i>region</i> .codedeploy
	com.amazonaws. <i>region</i> .codedeploy-commands-secure
<a href="#">Amazon CodeGuru 分析器</a>	com.amazonaws. <i>region</i> .codeguru-profiler
<a href="#">Amazon 評論 CodeGuru 家</a>	com.amazonaws. <i>region</i> .codeguru-reviewer
<a href="#">AWS CodePipeline</a>	com.amazonaws. <i>region</i> .codepipeline
<a href="#">Amazon CodeWhisperer</a>	com.amazonaws. <i>region</i> .codewhisperer
<a href="#">Amazon Comprehend</a>	com.amazonaws. <i>region</i> .comprehend
<a href="#">Amazon Comprehend Medical</a>	com.amazonaws. <i>region</i> .comprehendmedical
<a href="#">AWS Config</a>	com.amazonaws. <i>region</i> .config
<a href="#">Amazon Connect</a>	com.amazonaws. <i>region</i> .app-integrations
	com.amazonaws. <i>region</i> .cases
	com.amazonaws. <i>region</i> .connect-campaigns



AWS 服務	服務名稱
	com.amazonaws. <i>region</i> .profile
	com.amazonaws. <i>region</i> .voiceid
	com.amazonaws. <i>region</i> .wisdom
AWS Connector Service	com.amazonaws. <i>region</i> .awsconnector
<a href="#">AWS 控制目錄</a>	COM. 亞馬遜。##. #制目錄
<a href="#">AWS Data Exchange</a>	com.amazonaws. <i>region</i> .dataexchange
<a href="#">Amazon 數據 Firehose</a>	com.amazonaws. <i>region</i> .kinesis-firehose
<a href="#">AWS Database Migration Service</a>	com.amazonaws. <i>region</i> .dms
	com.amazonaws. <i>region</i> .dms-fips
<a href="#">AWS DataSync</a>	com.amazonaws. <i>region</i> .datasync
<a href="#">Amazon DataZone</a>	com.amazonaws. <i>region</i> .datazone
AWS Deadline Cloud	COM. 亞馬遜。##. #線. 管理
	COM. 亞馬遜。##. 限制. 排程
<a href="#">Amazon DevOps 大師</a>	com.amazonaws. <i>region</i> .devops-guru
<a href="#">AWS Directory Service</a>	com.amazonaws. <i>region</i> .ds
<a href="#">Amazon DynamoDB</a>	COM. 亞馬遜。##. 動態
<a href="#">Amazon EBS direct API</a>	com.amazonaws. <i>region</i> .ebs
<a href="#">Amazon EC2</a>	com.amazonaws. <i>region</i> .ec2
<a href="#">Amazon EC2 Auto Scaling</a>	com.amazonaws. <i>region</i> .autoscaling
<a href="#">EC2 Image Builder</a>	com.amazonaws. <i>region</i> .imagebuilder

AWS 服務	服務名稱
<a href="#">Amazon ECR</a>	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
<a href="#">Amazon ECS</a>	com.amazonaws. <i>region</i> .ecs
	com.amazonaws. <i>region</i> .ecs-agent
	com.amazonaws. <i>region</i> .ecs-telemetry
<a href="#">Amazon EKS</a>	com.amazonaws. <i>region</i> .eks
	com.amazonaws. <i>region</i> .eks-auth
<a href="#">AWS Elastic Beanstalk</a>	com.amazonaws. <i>region</i> .elasticbeanstalk
	com.amazonaws. <i>region</i> .elasticbeanstalk-health
<a href="#">AWS Elastic Disaster Recovery</a>	com.amazonaws. <i>region</i> .drs
<a href="#">Amazon Elastic File System</a>	com.amazonaws. <i>region</i> .elasticfilesystem
	com.amazonaws. <i>region</i> .elasticfilesystem-fips
<a href="#">Amazon Elastic Inference</a>	com.amazonaws. <i>region</i> .elastic-inference.runtime
<a href="#">Elastic Load Balancing</a>	com.amazonaws. <i>region</i> .elasticloadbalancing
<a href="#">Amazon ElastiCache</a>	com.amazonaws. <i>region</i> .elasticache
	com.amazonaws. <i>region</i> .elasticache-fips
<a href="#">AWS Elemental MediaConnect</a>	com.amazonaws. <i>region</i> .mediaconnect
<a href="#">Amazon EMR</a>	com.amazonaws. <i>region</i> .elasticmapreduce
<a href="#">Amazon EMR on EKS</a>	com.amazonaws. <i>region</i> .emr-containers
Amazon EMR Serverless	com.amazonaws. <i>region</i> .emr-serverless

AWS 服務	服務名稱
<a href="#">Amazon EMR 沃爾</a>	COM. 亞馬遜。##. ###爾.
<a href="#">AWS Entity Resolution</a>	com.amazonaws. <i>region</i> .entityresolution
<a href="#">Amazon EventBridge</a>	com.amazonaws. <i>region</i> .events
	COM. 亞馬遜。##. 管道數據
<a href="#">AWS Fault Injection Service</a>	com.amazonaws. <i>region</i> .fis
<a href="#">Amazon FinSpace</a>	com.amazonaws. <i>region</i> .finspace
	com.amazonaws. <i>region</i> .finspace-api
<a href="#">Amazon Forecast</a>	com.amazonaws. <i>region</i> .forecast
	com.amazonaws. <i>region</i> .forecastquery
	com.amazonaws. <i>region</i> .forecast-fips
	com.amazonaws. <i>region</i> .forecastquery-fips
<a href="#">Amazon Fraud Detector</a>	com.amazonaws. <i>region</i> .frauddetector
Amazon FSx	com.amazonaws. <i>region</i> .fsx
	com.amazonaws. <i>region</i> .fsx-fips
<a href="#">AWS Glue</a>	com.amazonaws. <i>region</i> .glue
<a href="#">AWS Glue DataBrew</a>	com.amazonaws. <i>region</i> .databrew
<a href="#">Amazon Managed Grafana</a>	com.amazonaws. <i>region</i> .grafana
	com.amazonaws. <i>region</i> .grafana-workspace
AWS Ground Station	com.amazonaws. <i>region</i> .groundstation
Amazon GuardDuty	com.amazonaws. <i>region</i> .guardduty-data

AWS 服務	服務名稱
	com.amazonaws. <i>region</i> .guardduty-data-fips
<a href="#">AWS HealthImaging</a>	COM. 亞馬遜。##. ###學影像
	com.amazonaws. <i>region</i> .medical-imaging
	com.amazonaws. <i>region</i> .runtime-medical-imaging
<a href="#">AWS HealthLake</a>	com.amazonaws. <i>region</i> .healthlake
<a href="#">AWS HealthOmics</a>	com.amazonaws. <i>region</i> .analytics-omics
	com.amazonaws. <i>region</i> .control-storage-omics
	com.amazonaws. <i>region</i> .storage-omics
	com.amazonaws. <i>region</i> .tags-omics
	com.amazonaws. <i>region</i> .workflows-omics
IAM Identity Center	com.amazonaws. <i>region</i> .identitystore
<a href="#">IAM Roles Anywhere</a>	com.amazonaws. <i>region</i> .rolesanywhere
Amazon Inspector	com.amazonaws. <i>region</i> .inspector2
<a href="#">AWS IoT Core</a>	com.amazonaws. <i>region</i> .iot.data
	com.amazonaws. <i>region</i> .iot.credentials
	com.amazonaws. <i>region</i> .iot.fleethub.api
<a href="#">AWS IoT Core Device Advisor</a>	com.amazonaws. <i>region</i> .deviceadvisor.iot
<a href="#">AWS IoT Core for LoRaWAN</a>	com.amazonaws. <i>region</i> .iotwireless.api
	com.amazonaws. <i>region</i> .lorawan.cups
	com.amazonaws. <i>region</i> .lorawan.lns

AWS 服務	服務名稱
AWS IoT FleetWise	com.amazonaws. <i>region</i> .iotfleetwise
<a href="#">AWS IoT Greengrass</a>	com.amazonaws. <i>region</i> .greengrass
AWS IoT RoboRunner	com.amazonaws. <i>region</i> .iotroborunner
<a href="#">AWS IoT SiteWise</a>	com.amazonaws. <i>region</i> .iotsitewise.api
	com.amazonaws. <i>region</i> .iotsitewise.data
<a href="#">AWS IoT TwinMaker</a>	com.amazonaws. <i>region</i> .iottwinmaker.api
	com.amazonaws. <i>region</i> .iottwinmaker.data
<a href="#">Amazon Kendra</a>	com.amazonaws. <i>region</i> .kendra
	aws.api. <i>region</i> .kendra-ranking
<a href="#">AWS Key Management Service</a>	com.amazonaws. <i>region</i> .kms
	com.amazonaws. <i>region</i> .kms-fips
<a href="#">Amazon Keyspaces (適用於 Apache Cassandra)</a>	com.amazonaws. <i>region</i> .cassandra
	com.amazonaws. <i>region</i> .cassandra-fips
<a href="#">Amazon Kinesis Data Streams</a>	com.amazonaws. <i>region</i> .kinesis-streams
<a href="#">AWS Lake Formation</a>	com.amazonaws. <i>region</i> .lakeformation
<a href="#">AWS Lambda</a>	com.amazonaws. <i>region</i> .lambda
<a href="#">Amazon Lex</a>	com.amazonaws. <i>region</i> .models-v2-lex
	com.amazonaws. <i>region</i> .runtime-v2-lex
<a href="#">AWS License Manager</a>	com.amazonaws. <i>region</i> .license-manager
	com.amazonaws. <i>region</i> .license-manager-fips

AWS 服務	服務名稱
	com.amazonaws. <i>region</i> .license-manager-user-subscriptions
<a href="#">Amazon Lookout for Equipment</a>	com.amazonaws. <i>region</i> .lookoutequipment
<a href="#">Amazon Lookout for Metrics</a>	com.amazonaws. <i>region</i> .lookoutmetrics
<a href="#">Amazon Lookout for Vision</a>	com.amazonaws. <i>region</i> .lookoutvision
<a href="#">Amazon Macie</a>	com.amazonaws. <i>region</i> .macie2
<a href="#">AWS Mainframe Modernization</a>	com.amazonaws. <i>region</i> .m2
Amazon Managed Blockchain	com.amazonaws. <i>region</i> .managedblockchain-query
	com.amazonaws. <i>region</i> .managedblockchain.bitcoin.mainnet
	com.amazonaws. <i>region</i> .managedblockchain.bitcoin.testnet
<a href="#">Amazon Managed Service for Prometheus</a>	com.amazonaws. <i>region</i> .aps
	com.amazonaws. <i>region</i> .aps-workspaces
<a href="#">Amazon Managed Workflows for Apache Airflow</a>	com.amazonaws. <i>region</i> .airflow.api
	com.amazonaws. <i>region</i> .airflow.env
	com.amazonaws. <i>region</i> .airflow.ops
<a href="#">AWS Management Console</a>	com.amazonaws. <i>region</i> .console
	com.amazonaws. <i>region</i> .signin
<a href="#">Amazon MemoryDB for Redis</a>	com.amazonaws. <i>region</i> .memory-db
	com.amazonaws. <i>region</i> .memorydb-fips

AWS 服務	服務名稱
<a href="#">AWS Migration Hub Orchestrator</a>	com.amazonaws. <i>region</i> .migrationhub-orchestrator
<a href="#">AWS Migration Hub Refactor Spaces</a>	com.amazonaws. <i>region</i> .refactor-spaces
<a href="#">Migration Hub 策略建議</a>	com.amazonaws. <i>region</i> .migrationhub-strategy
Amazon Neptune Analytics	com.amazonaws. <i>region</i> .neptune-graph
Amazon Nimble Studio	com.amazonaws. <i>region</i> .nimble
<a href="#">Amazon OpenSearch 服務</a>	這些端點由服務管理
<a href="#">AWS Organizations</a>	COM. 亞馬遜。 ##. 組織
	COM. 亞馬遜。 ##. 組織-FIPS
AWS Outposts	COM. 亞馬遜。 ##. 前哨
<a href="#">AWS Panorama</a>	com.amazonaws. <i>region</i> .panorama
AWS 支付密碼學	com.amazonaws. <i>region</i> .payment-cryptography.contr olplane
	com.amazonaws. <i>region</i> .payment-cryptography.datap lane
<a href="#">Amazon Personalize</a>	com.amazonaws. <i>region</i> .personalize
	com.amazonaws. <i>region</i> .personalize-events
	com.amazonaws. <i>region</i> .personalize-runtime
<a href="#">AWS Supply Chain</a>	COM. 亞馬遜。 ## .scn
<a href="#">Amazon Pinpoint</a>	com.amazonaws. <i>region</i> .pinpoint
	com.amazonaws. <i>region</i> .pinpoint-sms-voice-v2
<a href="#">Amazon Polly</a>	com.amazonaws. <i>region</i> .polly

AWS 服務	服務名稱
AWS 私人 5G	com.amazonaws. <i>region</i> .private-networks
<a href="#">AWS Private Certificate Authority</a>	com.amazonaws. <i>region</i> .acm-pca com.amazonaws. <i>region</i> .pca-connector-ad
<a href="#">AWS Proton</a>	com.amazonaws. <i>region</i> .proton
<a href="#">Amazon Q Business</a>	Aw.api. ## .q 業務
<a href="#">Amazon QLDB</a>	com.amazonaws. <i>region</i> .qldb.session
<a href="#">Amazon QuickSight</a>	COM. 亞馬遜。 ##. ##視線網站
<a href="#">Amazon RDS</a>	com.amazonaws. <i>region</i> .rds
<a href="#">Amazon RDS Data API</a>	com.amazonaws. <i>region</i> .rds-data
AWS RE: 私人貼文	COM. 亞馬遜。 ##. 重新發佈空間
<a href="#">Amazon Redshift</a>	com.amazonaws. <i>region</i> .redshift com.amazonaws. <i>region</i> .redshift-fips
<a href="#">Amazon Redshift 資料 API</a>	com.amazonaws. <i>region</i> .redshift-data COM. 亞馬遜。 ##. #動數據 FIPS
<a href="#">Amazon Rekognition</a>	com.amazonaws. <i>region</i> .rekognition com.amazonaws. <i>region</i> .rekognition-fips com.amazonaws. <i>region</i> .streaming-rekognition com.amazonaws. <i>region</i> .streaming-rekognition-fips
<a href="#">AWS RoboMaker</a>	com.amazonaws. <i>region</i> .robomaker
<a href="#">Amazon Simple Storage Service (Amazon S3)</a>	com.amazonaws. <i>region</i> .s3



AWS 服務	服務名稱
<a href="#">Amazon S3 多區域存取點</a>	com.amazonaws.s3-global.accesspoint
<a href="#">Amazon S3 on Outposts</a>	com.amazonaws. <i>region</i> .s3-outposts
<a href="#">Amazon SageMaker</a>	aws.sagemaker. <i>region</i> .notebook
	aws.sagemaker. <i>region</i> .studio
	com.amazonaws. <i>region</i> .sagemaker.api
	com.amazonaws. <i>region</i> .sagemaker.featurestore-runtime
	com.amazonaws. <i>region</i> .sagemaker.metrics
	com.amazonaws. <i>region</i> .sagemaker.runtime
	com.amazonaws. <i>region</i> .sagemaker.runtime-fips
<a href="#">AWS Secrets Manager</a>	com.amazonaws. <i>region</i> .secretsmanager
<a href="#">AWS Security Hub</a>	com.amazonaws. <i>region</i> .securityhub
<a href="#">AWS Security Token Service</a>	com.amazonaws. <i>region</i> .sts
Service Catalog	com.amazonaws. <i>region</i> .servicecatalog
	com.amazonaws. <i>region</i> .servicecatalog-appregistry
<a href="#">Amazon SES</a>	com.amazonaws. <i>region</i> .email-smtp
AWS SimSpace Weaver	com.amazonaws. <i>region</i> .simspaceweaver
AWS Snow Device Management	com.amazonaws. <i>region</i> .snow-device-management
<a href="#">Amazon SNS</a>	com.amazonaws. <i>region</i> .sns
<a href="#">Amazon SQS</a>	com.amazonaws. <i>region</i> .sqs
<a href="#">Amazon SWF</a>	com.amazonaws. <i>region</i> .swf

AWS 服務	服務名稱
	com.amazonaws. <i>region</i> .swf-fips
<a href="#">AWS Step Functions</a>	com.amazonaws. <i>region</i> .states
	com.amazonaws. <i>region</i> .sync-states
AWS Storage Gateway	com.amazonaws. <i>region</i> .storagegateway
<a href="#">AWS Systems Manager</a>	com.amazonaws. <i>region</i> .ec2messages
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> .ssm-contacts
	com.amazonaws. <i>region</i> .ssm-incidents
	com.amazonaws. <i>region</i> .ssmmessages
AWS 電信網絡生成器	com.amazonaws. <i>region</i> .tnb
<a href="#">Amazon Textract</a>	com.amazonaws. <i>region</i> .textract
	com.amazonaws. <i>region</i> .textract-fips
<a href="#">Amazon Timestream</a>	com.amazonaws. <i>region</i> .timestream.ingest- <i>cell</i>
	com.amazonaws. <i>region</i> .timestream.query- <i>cell</i>
<a href="#">Amazon Timestream 為 InfluxDB</a>	COM. 亞馬遜。 ##. 時間流
<a href="#">Amazon Transcribe</a>	com.amazonaws. <i>region</i> .transcribe
	com.amazonaws. <i>region</i> .transcribestreaming
<a href="#">Amazon Transcribe Medical</a>	com.amazonaws. <i>region</i> .transcribe
	com.amazonaws. <i>region</i> .transcribestreaming
AWS Transfer for SFTP	com.amazonaws. <i>region</i> .transfer

AWS 服務	服務名稱
	com.amazonaws. <i>region</i> .transfer.server
<a href="#">Amazon Translate</a>	com.amazonaws. <i>region</i> .translate
AWS Trusted Advisor	com.amazonaws. <i>region</i> .trustedadvisor
<a href="#">Amazon Verified Permissions</a>	com.amazonaws. <i>region</i> .verifiedpermissions
<a href="#">Amazon VPC Lattice</a>	com.amazonaws. <i>region</i> .vpc-lattice
<a href="#">Amazon WorkSpaces</a>	com.amazonaws. <i>region</i> .workspaces
<a href="#">Amazon WorkSpaces 瘦客戶端</a>	COM. 亞馬遜。 ##. #考客戶 .api
<a href="#">AWS X-Ray</a>	com.amazonaws. <i>region</i> .xray

## 檢視可用的 AWS 服務 名稱

您可以使用 [describe-vpc-endpoint-services](#) 命令來檢視支援 VPC 端點的服務名稱。

下列範例顯示在指定「區域」中支援介面端點的。AWS 服務 `--query` 選項會將輸出限制為服務名稱。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

下列為範例輸出：

```
[
  "aws.api.us-east-1.kendra-ranking",
  "aws.sagemaker.us-east-1.notebook",
  "aws.sagemaker.us-east-1.studio",
  "com.amazonaws.s3-global.accesspoint",
  "com.amazonaws.us-east-1.access-analyzer",
  "com.amazonaws.us-east-1.account",
  ...
]
```

]

## 檢視服務相關資訊

取得服務名稱之後，您可以使用 [describe-vpc-endpoint-services](#) 命令來檢視有關各項端點服務的詳細資訊。

下列範例顯示指定區域中 Amazon CloudWatch 界面端點的相關資訊。

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

以下為範例輸出。VpcEndpointPolicySupported 表示是否支援[端點政策](#)。SupportedIpAddressTypes 表示支援的 IP 地址類型。

```
{
  "ServiceDetails": [
    {
      "ServiceName": "com.amazonaws.us-east-1.monitoring",
      "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
      "ServiceType": [
        {
          "ServiceType": "Interface"
        }
      ],
      "AvailabilityZones": [
        "us-east-1a",
        "us-east-1b",
        "us-east-1c",
        "us-east-1d",
        "us-east-1e",
        "us-east-1f"
      ],
      "Owner": "amazon",
      "BaseEndpointDnsNames": [
        "monitoring.us-east-1.vpce.amazonaws.com"
      ],
      "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
      "PrivateDnsNames": [
        {
          "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
        }
      ]
    }
  ]
}
```

```
    }
    ],
    "VpcEndpointPolicySupported": true,
    "AcceptanceRequired": false,
    "ManagesVpcEndpoints": false,
    "Tags": [],
    "PrivateDnsNameVerificationState": "verified",
    "SupportedIpAddressTypes": [
        "ipv4"
    ]
}
],
"ServiceNames": [
    "com.amazonaws.us-east-1.monitoring"
]
}
```

## 檢視端點政策支援

若要確認服務是否支援端點政策，呼叫 [describe-vpc-endpoint-services](#) 命令，並檢查 `VpcEndpointPolicySupported` 的值。可能的值為 `true` 和 `false`。

下列範例會檢查指定的服務是否支援指定區域中的端點政策。 `--query` 選項會將輸出限制為 `VpcEndpointPolicySupported` 的值。

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

下列為範例輸出。

```
True
```

下列範例列出在指定區域中支援端點策略的範例。 AWS 服務 `--query` 選項會將輸出限制為服務名稱。若要使用 Windows 命令提示字元執行此命令，請移除查詢字串周圍的單引號，並將行接續字元從 `\` 變更為 `^`。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
```

```
--query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

下列為範例輸出。

```
[  
  "aws.api.us-east-1.kendra-ranking",  
  "aws.sagemaker.us-east-1.notebook",  
  "aws.sagemaker.us-east-1.studio",  
  "com.amazonaws.s3-global.accesspoint",  
  "com.amazonaws.us-east-1.access-analyzer",  
  "com.amazonaws.us-east-1.account",  
  ...  
]
```

下列範例會列出 AWS 服務 指定區域中不支援端點策略的項目。--query 選項會將輸出限制為服務名稱。若要使用 Windows 命令提示字元執行此命令，請移除查詢字串周圍的單引號，並將行接續字元從 \ 變更為 ^。

```
aws ec2 describe-vpc-endpoint-services \  
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \  
  --region us-east-1 \  
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

下列為範例輸出。

```
[  
  "com.amazonaws.us-east-1.appmesh-envoy-management",  
  "com.amazonaws.us-east-1.apprunner.requests",  
  "com.amazonaws.us-east-1.appstream.api",  
  "com.amazonaws.us-east-1.appstream.streaming",  
  "com.amazonaws.us-east-1.awsconnector",  
  "com.amazonaws.us-east-1.cleanrooms",  
  "com.amazonaws.us-east-1.cleanrooms-ml",  
  "com.amazonaws.us-east-1.cloudtrail",  
  "com.amazonaws.us-east-1.codeguru-profiler",  
  "com.amazonaws.us-east-1.codeguru-reviewer",  
  "com.amazonaws.us-east-1.codepipeline",  
  "com.amazonaws.us-east-1.codewhisperer",  
  "com.amazonaws.us-east-1.datasync",  
  "com.amazonaws.us-east-1.datazone",  
  "com.amazonaws.us-east-1.deadline.management",  
  "com.amazonaws.us-east-1.deadline.scheduling",  
]
```

```
"com.amazonaws.us-east-1.deviceadvisor.iot",
"com.amazonaws.us-east-1.eks",
"com.amazonaws.us-east-1.elastic-inference.runtime",
"com.amazonaws.us-east-1.email-smtp",
"com.amazonaws.us-east-1.grafana-workspace",
"com.amazonaws.us-east-1.iot.credentials",
"com.amazonaws.us-east-1.iot.data",
"com.amazonaws.us-east-1.iotwireless.api",
"com.amazonaws.us-east-1.lorawan.cups",
"com.amazonaws.us-east-1.lorawan.lns",
"com.amazonaws.us-east-1.macie2",
"com.amazonaws.us-east-1.neptune-graph",
"com.amazonaws.us-east-1.nimble",
"com.amazonaws.us-east-1.organizations",
"com.amazonaws.us-east-1.outposts",
"com.amazonaws.us-east-1.pipes-data",
"com.amazonaws.us-east-1.redshift-data",
"com.amazonaws.us-east-1.redshift-data-fips",
"com.amazonaws.us-east-1.refactor-spaces",
"com.amazonaws.us-east-1.sagemaker.runtime-fips",
"com.amazonaws.us-east-1.storagegateway",
"com.amazonaws.us-east-1.transfer",
"com.amazonaws.us-east-1.transfer.server",
"com.amazonaws.us-east-1.verifiedpermissions"
]
```

## 檢視 IPv6 支援

您可以使用下列[描述-vpc-端點服務](#)命令來檢視您可以在指定區域中透過 IPv6 存取 AWS 服務的項目。--query 選項會將輸出限制為服務名稱。

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
  Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

下列為範例輸出：

```
[
  "aws.api.us-east-1.kendra-ranking",
  "aws.api.us-east-1.qbusiness",
```

```
"com.amazonaws.us-east-1.athena",  
"com.amazonaws.us-east-1.data-servicediscovery",  
"com.amazonaws.us-east-1.data-servicediscovery-fips",  
"com.amazonaws.us-east-1.eks-auth",  
"com.amazonaws.us-east-1.glue",  
"com.amazonaws.us-east-1.lakeformation",  
"com.amazonaws.us-east-1.quicksight-website",  
"com.amazonaws.us-east-1.s3-outposts",  
"com.amazonaws.us-east-1.servicediscovery",  
"com.amazonaws.us-east-1.servicediscovery-fips",  
"com.amazonaws.us-east-1.timestream-influxdb"
```

```
]
```

## AWS 服務 使用接口 VPC 端點訪問

您可以創建一個接口 VPC 端點來連接到提供支持的服務 AWS PrivateLink，包括許多 AWS 服務。如需概觀，請參閱 [the section called “概念”](#) 和 [访问 AWS 服務](#)。

對於您從 VPC 中指定的每個子網，我們會在子網中建立端點網路介面，並從子網地址範圍中為其指派私有 IP 地址。端點網路界面是請求者管理的網路介面；您可以在 AWS 帳戶中檢視它，但不能自己管理它。

我們會向您收取每小時用量率及資料處理費。如需詳細資訊，請參閱 [界面端點定價](#)。

### 目錄

- [必要條件](#)
- [建立 VPC 端點](#)
- [共用子網路](#)

## 必要條件

- 部署將存取 VPC AWS 服務 中的資源。
- 若要使用私有 DNS，您必須啟用 VPC 的 DNS 主機名稱和 DNS 解析。如需更多資訊，請參閱《Amazon VPC 使用者指南》中的 [檢視和更新 DNS 屬性](#)。
- 若要為介面端點啟用 IPv6，AWS 服務 必須支援透過 IPv6 存取。如需詳細資訊，請參閱 [the section called “IP 地址類型”](#)。
- 為端點網路介面建立安全群組，以允許來自 VPC 中資源的預期流量。例如，若要確保 AWS CLI 可以傳送 HTTPS 要求至 AWS 服務，安全性群組必須允許輸入 HTTPS 流量。



- 如果您的資源位於具有網路 ACL 的子網路中，請確認網路 ACL 允許 VPC 中的資源和端點網路介面之間的流量。
- 您的 AWS PrivateLink 資源有配額。如需詳細資訊，請參閱 [AWS PrivateLink 配額](#)。

## 建立 VPC 端點

使用下列程序建立連線至 AWS 服務的介面 VPC 端點。

若要建立介面端點 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)。
3. 選擇建立端點。
4. 對於 Service category (服務類別)，選擇 AWS 服務。
5. 對於 Service name (服務名稱)，請選取服務。如需詳細資訊，請參閱 [the section called “整合的服務”](#)。
6. 對於 VPC，請選取您要從中存取 AWS 服務的 VPC。
7. 如果您在步驟 5 中選取 Amazon S3 的服務名稱，並且想要設定 [私有 DNS 支援](#)，請選取其他設定、啟用 DNS 名稱。進行此選取後，系統會自動選取僅針對傳入端點啟用私有 DNS。您只能為 Amazon S3 的介面端點設定具有傳入 Resolver 端點的私有 DNS。如果您沒有 Amazon S3 的閘道端點，且選取僅針對傳入端點啟用私有 DNS，則您在嘗試執行此程序的最後一個步驟時會收到錯誤訊息。

如果您在步驟 5 中選取 Amazon S3 以外的任何服務的服務名稱，則系統會預設選取其他設定、啟用 DNS 名稱。建議您保留預設。如此可確保使用公用服務端點的要求 (例如透過 AWS SDK 發出的要求) 會解析至您的 VPC 端點。

8. 對於 Subnets (子網)，為每個可用區域選取一個子網，您將從中存取 AWS 服務。您無法在相同的可用區域內選取多個子網路。如需詳細資訊，請參閱 [the section called “子網路與可用區域”](#)。

我們會在您選取的每個子網路中建立端點網路介面。依預設，我們會從子網路 IP 地址範圍選取 IP 地址，並將它們指派給端點網路介面。若要選擇端點網路介面的 IP 地址，請選取指定 IP 地址並從子網路地址範圍輸入 IPv4 地址。如果端點服務支援 IPv6，您也可以從子網路地址範圍輸入 IPv6 地址。請注意，子網路 CIDR 區塊中的前四個 IP 位址和最後一個 IP 位址會保留供內部使用，因此您無法為端點網路介面指定這些位址。

9. 針對 IP address type (IP 地址類型)，從下列選項中選擇：

- IPv4 - 將 IPv4 地址指派給您的端點網路介面。只有當所有選取的子網路都具有 IPv4 地址範圍，且此服務接受 IPv4 請求時，才支援此選項。
  - IPv6 - 將 IPv6 地址指派給您的端點網路介面。只有當所有選取的子網路都是僅限 IPv6 子網路，且此服務接受 IPv6 請求時，才支援此選項。
  - Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路介面。只有當所有選取的子網路都具有 IPv4 和 IPv6 地址範圍，且此服務接受 IPv4 和 IPv6 請求時，才支援此選項。
10. 對於安全群組，選取要與 VPC 端點的端點網路界面建立關聯的安全群組。根據預設，會與 VPC 的預設安全群組相關聯。
  11. 對於 Policy (政策)，選取 Full access (完整存取)，以允許 VPC 端點上所有資源的所有主體進行所有操作。否則，選取 Custom (自訂) 以連接 VPC 端點政策，該政策控制主體在 VPC 端點上對資源執行動作時所具有的許可。只有服務支援 VPC 端點政策時，此選項才可用。如需詳細資訊，請參閱 [端點政策](#)。
  12. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
  13. 選擇建立端點。

### 使用命令列建立介面端點

- [create-vpc-endpoint](#) (AWS CLI)
- [New-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。

## 設定介面端點

建立介面 VPC 端點之後，您可更新其組態。

### 任務

- [新增或移除子網路](#)
- [關聯安全群組](#)
- [編輯 VPC 端點政策](#)
- [啟用私有 DNS 名稱](#)

- [管理標籤](#)

## 新增或移除子網路

對於介面端點，一個可用區域只能選擇一個子網。如果您新增子網，我們會在子網中建立端點網路介面，並從子網的 IP 地址範圍中為其指派私有 IP 地址。如果您移除子網，我們會刪除其端點網路介面。如需詳細資訊，請參閱 [the section called “子網路與可用區域”](#)。

若要使用主控台變更子網

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. 選取介面端點。
4. 選擇 Actions (動作)、Manage Subnets (管理子網)。
5. 您可視需要選取或取消選取可用區域。針對每個可用區域，選取一個子網路。依預設，我們會從子網路 IP 地址範圍選取 IP 地址，並將它們指派給端點網路介面。若要選擇端點網路介面的 IP 地址，請選取指定 IP 地址並從子網路地址範圍輸入 IPv4 地址。如果端點服務支援 IPv6，您也可以從子網路地址範圍輸入 IPv6 地址。

如果您為已具有此 VPC 端點端點網路介面的子網路指定 IP 地址，我們會以新的端點網路介面取代端點網路介面。這個程序會暫時中斷子網路和 VPC 端點的連線。

6. 選擇 Modify subnets (修改子網)。

若要使用命令列變更子網

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 關聯安全群組

您可以變更與介面端點的網路介面相關聯的安全群組。安全群組規則可控制允許從 VPC 中之資源流向端點網路介面的流量。

若要使用主控台變更安全群組

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)。
3. 選取介面端點。
4. 選擇 Actions (動作)、Manage security groups (管理安全群組)。
5. 視需要選取或取消選取安全群組。
6. 選擇 Modify security groups (修改安全群組)。

若要使用命令列變更安全群組

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 編輯 VPC 端點政策

如果 AWS 服務支援端點策略，您可以編輯端點的端點策略。更新端點政策後，變生效需費時幾分鐘。如需詳細資訊，請參閱 [端點政策](#)。

若要使用主控台變更端點政策

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)。
3. 選取介面端點。
4. 選擇 Actions (動作)、Manage policy (管理政策)。
5. 選擇 Full Access (完整存取) 以允許完整存取服務，或選擇 Custom (自訂) 並連接自訂政策。
6. 選擇儲存。

若要使用命令列變更端點政策

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 啟用私有 DNS 名稱

建議您為 VPC 端點啟用私人 DNS 名稱。AWS 服務如此可確保使用公用服務端點的要求 (例如透過 AWS SDK 發出的要求) 會解析至您的 VPC 端點。

若要使用私有 DNS，您必須啟用 VPC 的 [DNS 主機名稱和 DNS 解析](#)。啟用私有 DNS 名稱之後，私有 IP 地址可能需要幾分鐘才能使用。當您啟用私有 DNS 名稱時，我們建立的 DNS 記錄為私有。因此，私有 DNS 名稱不可公開解析。

若要使用主控台變更私有 DNS 名稱選項

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)。
3. 選取介面端點。
4. 選擇 Actions (動作)、Modify private DNS name (修改私有 DNS 名稱)。
5. 根據需要選取或清除 Enable for this endpoint (為此端點啟用)。
6. 如果服務是 Amazon S3，在上一步中選取為此端點啟用，同時選取僅針對傳入端點啟用私有 DNS。如果您偏好使用標準私有 DNS 功能，請清除僅針對傳入端點啟用私有 DNS。如果除了 Amazon S3 的介面端點之外，沒有 Amazon S3 的閘道端點，並且選取僅針對傳入端點啟用私有 DNS，則您在下一個步驟中儲存變更時會收到錯誤訊息。如需詳細資訊，請參閱 [the section called “私有 DNS”](#)。
7. 選擇 Save changes (儲存變更)。

若要使用命令列變更私有 DNS 名稱選項

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 管理標籤

您可標記您的介面端點，以幫助您根據組織需求進行識別或分類。

若要使用主控台管理標籤

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. 選取介面端點。
4. 選擇 Actions (動作)、Manage tags (管理標籤)。
5. 對於要新增的每個標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤金鑰和標籤值。
6. 若要移除標籤，請選擇標籤金鑰和值右側的 Remove (移除)。

## 7. 選擇儲存。

若要使用命令列來管理標籤

- [create-tags](#) 和 [delete-tags](#) (AWS CLI)
- [New-EC2Tag](#)和 [Remove-EC2Tag](#)(視窗工具 PowerShell)

## 接收介面端點事件的提醒

您可以建立通知，接收與介面端點相關的特定事件的提醒。例如，當接受或拒絕連線請求時，您會收到電子郵件。

任務

- [建立 SNS 通知](#)
- [新增存取政策](#)
- [新增金鑰政策](#)

## 建立 SNS 通知

使用以下步驟即可為通知建立 Amazon SNS 主題，並訂閱該主題。

若要使用主控台建立介面端點的通知

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)。
3. 選取介面端點。
4. 在 Notifications (通知) 索引標籤中，選擇 Create notification (建立通知)。
5. 對於 Notification ARN (通知 ARN)，請選擇您建立的 SNS 主題的 ARN。
6. 若要訂閱事件，請從 Events (事件) 中選取。
  - Connect (連接) - 服務消費者建立的介面端點。這會將連線請求傳送至服務提供者。
  - Accept (接受) - 服務提供者接受連線請求。
  - Reject (拒絕) - 服務提供者拒絕連線請求。
  - Delete (刪除) - 服務消費者刪除介面端點。
7. 選擇 Create notification (建立通知)。

## 若要使用命令列建立介面端點的通知

- [create-vpc-endpoint-connection-notification](#) (AWS CLI)
- [New-EC2VpcEndpointConnectionNotification](#)(視窗工具 PowerShell)

## 新增存取政策

將存取政策新增至 Amazon SNS 主題，AWS PrivateLink 以便代表您發佈通知，如下所示。如需詳細資訊，請參閱[如何編輯我的 Amazon SNS 主題的存取政策？](#) 使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件金鑰，以防止發生[混淆代理人](#)的情況。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

## 新增金鑰政策

如果您使用加密的 SNS 主題，則 KMS 金鑰的資源原則必須信任 AWS PrivateLink 才能呼叫 AWS KMS API 作業。金鑰政策範例如下。

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

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "vpce.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey*",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:region:account-id:key/key-id",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account-id:vpc-endpoint/endpoint-id"
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
]
```

## 刪除介面端點

VPC 端點結束使用後即可刪除。刪除介面端點也會刪除其端點網路介面。

若要使用主控台刪除介面端點

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)。
3. 選取介面端點。
4. 選擇 Actions (動作)、Delete VPC endpoints (刪除 VPC 端點)。
5. 出現確認提示時，請按一下 **delete**。
6. 選擇刪除。

若要使用命令列刪除介面端點

- [delete-vpc-endpoints](#) (AWS CLI)



- [Remove-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 閘道端點

閘道 VPC 端點不需要您的 VPC 有網際網路閘道或 NAT 裝置，就可以提供與 Amazon S3 和 DynamoDB 的可靠連線。與其他類型的 VPC 端點不同 AWS PrivateLink，閘道端點不會使用。

Amazon S3 和 DynamoDB 同時支援閘道端點和界面端點。有關選項的比較，請參閱以下內容：

- [Amazon S3 的虛擬私人雲端節點類型](#)
- [適用於 Amazon DynamoDB 的虛擬私人雲端節點類型](#)

### 定價

使用閘道端點不需額外付費。

### 目錄

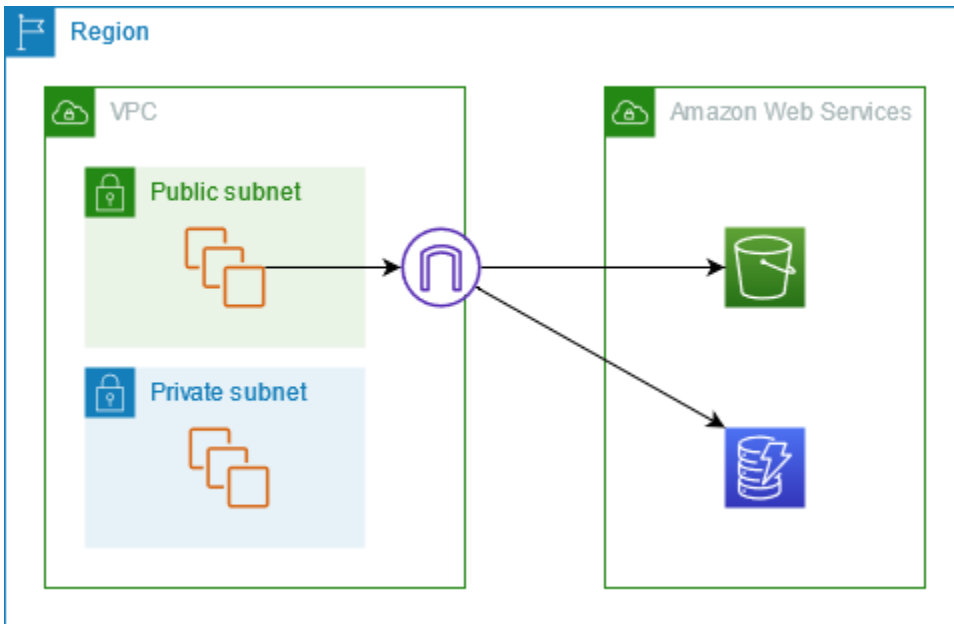
- [概要](#)
- [路由](#)
- [安全](#)
- [適用於 Amazon S3 的閘道端點](#)
- [Amazon DynamoDB 的閘道端點](#)

## 概要

您可以透過公有服務端點或透過閘道端點來存取 Amazon S3 和 DynamoDB。此概觀會比較這些方法。

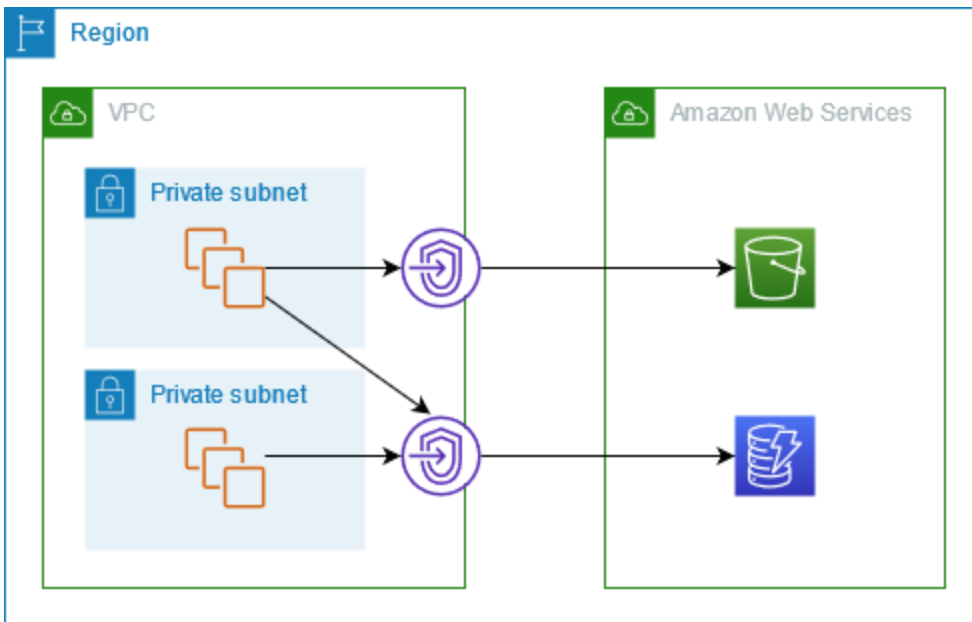
### 透過網際網路閘道進行存取

下圖顯示執行個體如何透過其公有服務端點存取 Amazon S3 和 DynamoDB。從公有子網中的執行個體到 Amazon S3 或 DynamoDB 的流量會路由到 VPC 的網際網路閘道，然後路由至該服務。私有子網中的執行個體無法將流量傳送到 Amazon S3 或 DynamoDB，因為根據定義，私有子網沒有通往網際網路閘道的路由。若要讓私有子網路中的執行個體將流量傳送到 Amazon S3 或 DynamoDB，您需要將 NAT 裝置新增到公有子網路，並將私有子網路中的流量路由到 NAT 裝置。雖然 Amazon S3 或 DynamoDB 的流量會周遊網際網路閘道，但不會離開網路。AWS



### 透過閘道端點進行存取

下圖顯示執行個體如何透過閘道端點來存取 Amazon S3 和 DynamoDB。從您的 VPC 到 Amazon S3 或 DynamoDB 的流量會路由至閘道端點。每個子網路路由表都必須有一個路由，該路由會使用服務的字首清單，將目的地為該服務的流量傳送到閘道端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [AWS 受管字首清單](#)。



## 路由

建立閘道端點時，您可以為啟用的子網選擇 VPC 路由表。下列路由會自動新增至您選取的每個路由表。目的地是所擁有之服務的前置詞清單 AWS，目標是閘道端點。

目的地	目標
<i>prefix_list_id</i>	<i>gateway_endpoint_id</i>

### 考量事項

- 您可以查看我們新增到路由表中的端點路由，但無法修改或刪除它們。若要將端點路由新增至路由表，請將其與閘道端點建立關聯。當您取消路由表與閘道端點的關聯或刪除閘道端點時，我們會刪除端點路由。
- 與閘道端點相關聯的路由表關聯的子網中的所有執行個體會自動使用閘道端點來存取服務。與這些路由表沒有關聯的子網中的執行個體會使用公有服務端點，而不是閘道端點。
- 路由表可以同時具有到 Amazon S3 的端點路由和到 DynamoDB 的端點路由。您可以在多個路由表中擁有相同服務 (Amazon S3 或 DynamoDB) 的端點路由。您不能在單一路由表中擁有相同服務 (Amazon S3 或 DynamoDB) 的多個端點路由。
- 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)。對於具有端點路由的路由表，這意味著以下內容：
  - 如果有一個路由將所有網際網路流量 (0.0.0.0/0) 傳送至網際網路閘道，則該端點路由對於目的地為當前區域中的服務 (Amazon S3 或 DynamoDB) 的流量具有優先權。目的地為不同的流量 AWS 服務使用互聯網閘道。
  - 目的地為不同區域中服務 (Amazon S3 或 DynamoDB) 的流量會前往網際網路閘道，因為字首清單是特定於某個區域。
  - 如果有一個路由會為相同區域中的服務 (Amazon S3 或 DynamoDB) 指定確切的 IP 地址範圍，則該路由優先於端點路由。

## 安全

當執行個體透過閘道端點存取 Amazon S3 或 DynamoDB 時，會使用其公有端點來存取服務。這些執行個體的安全群組必須允許進出服務的流量。以下是傳出規則範例。其會參照服務的[字首清單 ID](#)。

目的地	通訊協定	連接埠範圍
<i>prefix_list_id</i>	TCP	443

這些執行個體之子網路的網路 ACL 也必須允許進出服務的流量。以下是傳出規則範例。您無法在網路 ACL 規則中參照字首清單，但可以從服務的字首清單中取得服務的 IP 地址範圍。

目的地	通訊協定	連接埠範圍
<i>service_cidr_block_1</i>	TCP	443
<i>service_cidr_block_2</i>	TCP	443
<i>service_cidr_block_3</i>	TCP	443

## 適用於 Amazon S3 的閘道端點

您可以使用閘道 VPC 端點從 VPC 中存取 Amazon S3。建立閘道端點後，您可以將其新增為路由表中的目標，用於從 VPC 到 Amazon S3 的流量。

使用閘道端點不需額外付費。

Amazon S3 支援閘道端點和界面端點。您可以使用閘道端點從您的 VPC 存取 Amazon S3，而無需為 VPC 使用網際網路閘道或 NAT 裝置，並無需支付額外費用。但是，閘道端點不允許從內部部署網路、其他 AWS 區域的對等 VPC 或透過傳輸閘道進行存取。這些情況下，您必須利用界面端點 (需額外付費)。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的[適用於 Amazon S3 的 VPC 端點類型](#)。

### 目錄

- [考量事項](#)
- [私有 DNS](#)
- [建立閘道端點](#)
- [使用儲存貯體政策控制存取](#)
- [關聯路由表](#)
- [編輯 VPC 端點政策](#)

## • [刪除閘道端點](#)

### 考量事項

- 閘道端點只能在您建立該端點的區域中使用。請務必在與 S3 儲存貯體相同的區域中建立閘道端點。
- 如果您使用的是 Amazon DNS 伺服器，則必須同時啟用 VPC 的 [DNS 主機名稱和 DNS 解析](#)。如果您使用自己的 DNS 伺服器，請確保對 Amazon S3 提出的請求可正確解析為 AWS 所維護的 IP 地址。
- 對於透過閘道端點存取 Amazon S3 的執行個體，安全群組的規則必須允許進出 Amazon S3 的流量。您可以在安全群組規則中參照 Amazon S3 的 [字首清單](#) ID。
- 對於透過閘道端點存取 Amazon S3 的執行個體，子網路的網路 ACL 必須允許進出 Amazon S3 的流量。您無法在網路 ACL 規則中參照字首清單，但可以從 Amazon S3 的 [字首清單](#) 中取得 Amazon S3 的 IP 地址範圍。
- 檢查您使用的是否需 AWS 服務 要存取 S3 儲存貯體。例如，服務可能需要存取含有日誌檔案的儲存貯體，或者可能會要求您將驅動程式或代理程式下載到 EC2 執行個體。如果是這樣，請確保您的端點策略允許 AWS 服務 或資源使用 `s3:GetObject` 動作存取這些值區。
- 您不能針對周遊 VPC 端點的 Amazon S3 請求，在身分政策或儲存貯體政策中使用 `aws:SourceIp` 條件。請改用 `aws:VpcSourceIp` 條件。或者，您也可以使用路由表，控制哪些 EC2 執行個體可透過 VPC 端點存取 Amazon S3。
- 閘道端點僅支援 IPv4 流量。
- 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。
- 端點連線不能延伸出 VPC。VPN 連線、VPC 對等連線、傳輸閘道或 AWS Direct Connect VPC 中連線另一端的資源無法使用閘道端點與 Amazon S3 通訊。
- 您的帳戶對於每個區域的預設配額為 20 個閘道端點，此配額可進行調整。每個 VPC 也有 255 個閘道端點的限制。

### 私有 DNS

為 Amazon S3 建立閘道端點和介面端點後，可以設定私有 DNS 以最佳化成本。

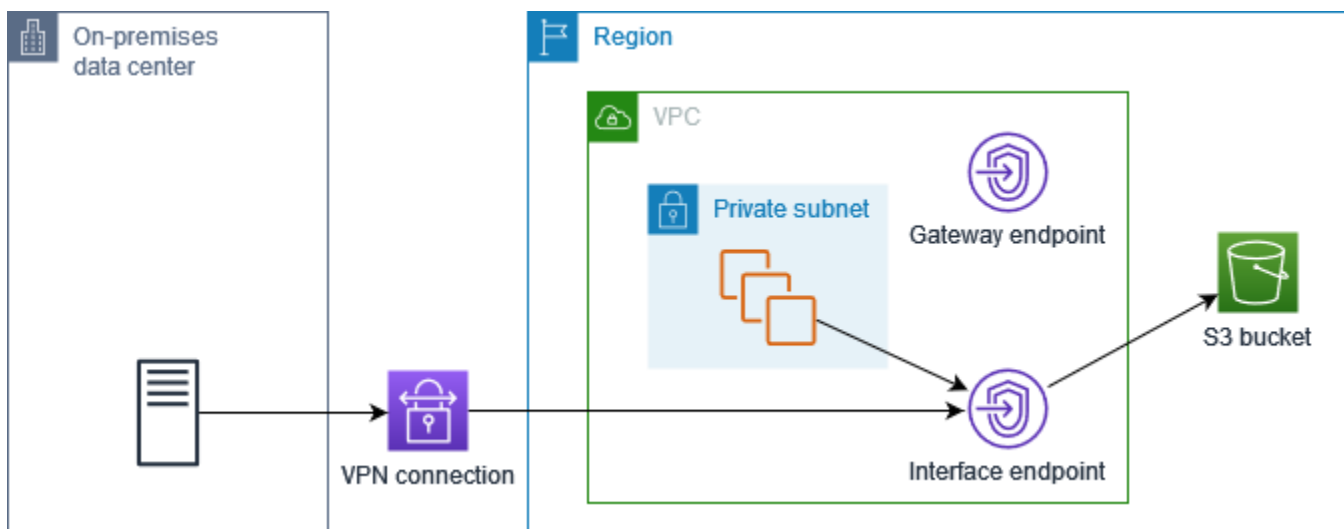
### Route 53 Resolver

Amazon 會為您的 VPC 提供 DNS 伺服器，名為 [Route 53 Resolver](#)。Route 53 Resolver 會自動解析本機 VPC 網域名稱和私有託管區域中的記錄。但是，您無法從 VPC 外部使用 Route 53 Resolver。Route 53 會提供 Resolver 端點和 Resolver 規則，讓您可以從 VPC 外部使用 Route 53 Resolver。傳入 Resolver 端點會將 DNS 查詢從內部部署網路轉送至 Route 53 Resolver。傳出 Resolver 端點會將 DNS 查詢從 Route 53 Resolver 轉送至內部部署網路。

當您將 Amazon S3 的介面端點設定為僅針對傳入 Resolver 端點使用私有 DNS 後，我們會建立傳入 Resolver 端點。傳入 Resolver 端點會將從內部部署向 Amazon S3 發出的 DNS 查詢解析為介面端點的私有 IP 地址。我們也會將 Route 53 Resolver 的 ALIAS 記錄新增至 Amazon S3 的公有託管區域，以便來自 VPC 的 DNS 查詢解析為 Amazon S3 公有 IP 地址，並將流量路由到閘道端點。

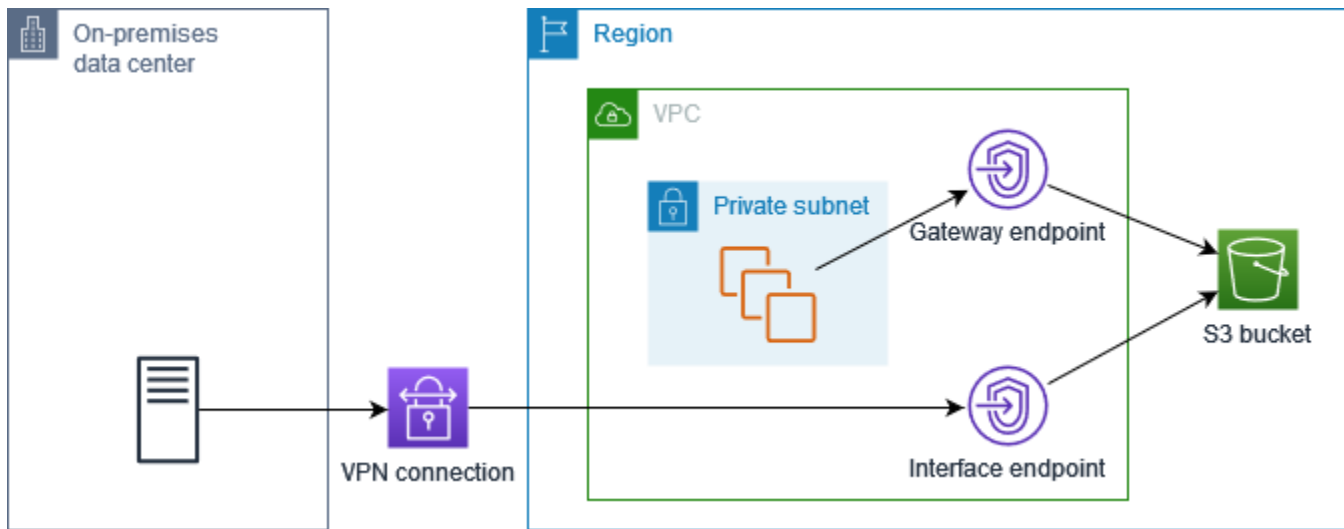
## 私有 DNS

如果您為 Amazon S3 的介面端點設定私有 DNS，但並未僅針對傳入 Resolver 端點設定私有 DNS，則來自內部部署網路和 VPC 的請求都會使用介面端點存取 Amazon S3。因此，來自 VPC 的流量都會使用介面端點，您需要為此付費；如果流量使用閘道端點，則您無需額外付費。



## 僅適用於傳入 Resolver 端點的私有 DNS

如果您僅針對傳入 Resolver 端點設定私有 DNS，則來自內部部署網路的請求會使用介面端點存取 Amazon S3，而來自 VPC 的請求會使用閘道端點存取 Amazon S3。因此，您可以最佳化成本，因為只有在無法使用閘道端點的流量使用介面端點時，您才需要付費。



## 設定私有 DNS

您可以在建立 Amazon S3 的介面端點之時或之後為其設定私有 DNS。如需詳細資訊，請參閱 [the section called “建立 VPC 端點”](#) (建立期間設定) 或 [the section called “啟用私有 DNS 名稱”](#) (建立後設定)。

## 建立閘道端點

使用下列程序建立連線至 Amazon S3 的閘道端點。

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)。
3. 選擇建立端點。
4. 對於 Service category (服務類別)，選擇 AWS 服務。
5. 對於「服務」，請新增篩選器類型 = 閘道，然後選取 com.amazonaws. ##.s3。
6. 針對 VPC，選取要在其中建立端點的 VPC。
7. 針對 Route tables (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端點網路介面。
8. 對於 Policy (政策)，選取 Full access (完整存取)，以允許 VPC 端點上所有資源的所有主體進行所有操作。否則，選取 Custom (自訂)，連接 VPC 端點政策，該政策控制主體必須在 VPC 端點上對資源執行操作的權限。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。

## 10. 選擇建立端點。

若要使用命令列建立閘道端點

- [create-vpc-endpoint](#) (AWS CLI)
- [New-EC2VpcEndpoint](#)(視窗工具 PowerShell)

### 使用儲存貯體政策控制存取

您可以使用值區政策來控制來自特定端點、VPC、IP 位址範圍和 AWS 帳戶值區的存取。這些範例假定還有政策聲明允許您的使用案例所需的存取權限。

Example 範例：限制特定端點的存取

您可以使用 [aws:sourceVpce](#) 條件金鑰，建立儲存貯體政策來限制對特定端點的存取。除非使用指定的閘道端點，否則以下政策會拒絕使用指定動作存取指定的儲存貯體。請注意，此政策會封鎖透過 AWS Management Console 使用指定動作來存取指定的儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                  "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example 範例：限制特定 VPC 的存取

您可以使用 [aws:sourceVpc](#) 條件金鑰，建立儲存貯體政策來限制對特定 VPC 的存取。如果您在相同的 VPC 中設定多個端點，這將十分有用。除非請求是來自指定的 VPC，否則以下政策會拒絕使用指定動



作存取指定的儲存貯體。請注意，此政策會封鎖透過 AWS Management Console 使用指定動作來存取指定的儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                  "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
    }
  ]
}
```

#### Example 範例：限制對特定 IP 地址範圍的存取

您可以使用 [aws: IP 條件金鑰建立政策](#)，限制對特定 VpcSource IP 位址範圍的存取。除非請求是來自指定的 IP 地址，否則以下政策會拒絕使用指定動作存取指定的儲存貯體。請注意，此政策會封鎖透過 AWS Management Console 使用指定動作來存取指定的儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                  "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

```
}
]
}
```

### Example 範例：限制對特定值區的存取 AWS 帳戶

您可以使用 `s3:ResourceAccount` 條件金鑰，建立政策來限制對特定 AWS 帳戶中 S3 儲存貯體的存取。除非指定的動作為 AWS 帳戶所擁有，否則以下政策會拒絕使用指定動作存取 S3 儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

## 關聯路由表

您可變更與閘道端點關聯的路由表。當您關聯路由表時，我們會自動新增路由，將以服務為目標的流量指向端點網路介面。當您取消路由表的關聯時，我們會自動從路由表中移除端點路由。

若要使用主控台來關聯路由表

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Manage route tables (管理路由表)。
5. 視需要選取或取消選取路由表。
6. 選擇 Modify route tables (修改路由表)。

若要使用命令列來關聯路由表

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 編輯 VPC 端點政策

您可以編輯閘道端點的端點政策，以控制從 VPC 中透過端點對 Amazon S3 的存取。預設政策允許完整存取。如需詳細資訊，請參閱 [端點政策](#)。

若要使用主控台變更端點政策

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Manage policy (管理政策)。
5. 選擇 Full Access (完整存取) 以允許完整存取服務，或選擇 Custom (自訂) 並連接自訂政策。
6. 選擇儲存。

下列範例端點原則用於存取 Amazon S3。

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。如果您的 VPC AWS 服務 中有其他使用 S3 儲存貯體的話，這會很有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
```

```
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
    ]
}
]
```

### Example 範例：限制特定 IAM 角色的存取

您可以建立政策，限制特定 IAM 角色的存取。您必須使用 `aws:PrincipalArn` 來授予對主體的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

### Example 範例：限制對特定帳戶中使用者的存取

您可以建立政策，限制特定帳戶的存取。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",

```

```
    "Condition": {
      "StringEquals": {
        "aws:PrincipalAccount": "111122223333"
      }
    }
  ]
}
```

## 刪除閘道端點

閘道端點結束使用後即可刪除。當您刪除閘道端點時，我們會從子網路由表中移除端點路由。

如果啟用私有 DNS，則無法刪除閘道端點。

若要使用主控台刪除閘道端點

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Delete VPC endpoints (刪除 VPC 端點)。
5. 出現確認提示時，請按一下 **delete**。
6. 選擇刪除。

若要使用命令列刪除閘道端點

- [delete-vpc-endpoints](#) (AWS CLI)
- [Remove-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## Amazon DynamoDB 的閘道端點

您可以使用閘道 VPC 端點從 VPC 中存取 Amazon DynamoDB。建立閘道端點後，您可以將其新增為路由表中的目標，用於從 VPC 到 DynamoDB 的流量。

使用閘道端點不需額外付費。

DynamoDB 同時支援閘道端點和介面端點。使用閘道端點，您可以從 VPC 存取 DynamoDB，而無需為 VPC 使用網際網路閘道或 NAT 裝置，而且無需額外費用。但是，閘道端點不允許從內部部署網路、其他 AWS 區域的對等 VPC 或透過傳輸閘道進行存取。這些情況下，您必須利用介面端點 (需額

外付費)。如需詳細資訊，請參閱 Amazon DynamoDB 開發人員指南中的[適用於 DynamoDB 的 VPC 擬私人雲端節點類型](#)。

## 目錄

- [考量事項](#)
- [建立閘道端點](#)
- [使用 IAM 政策控制存取](#)
- [關聯路由表](#)
- [編輯 VPC 端點政策](#)
- [刪除閘道端點](#)

## 考量事項

- 閘道端點只能在您建立該端點的區域中使用。請務必在與 DynamoDB 資料表相同的區域中建立閘道端點。
- 如果您使用的是 Amazon DNS 伺服器，則必須同時啟用 VPC 的 [DNS 主機名稱和 DNS 解析](#)。如果您使用自己的 DNS 伺服器，請確保對 DynamoDB 提出的請求可正確解析為 AWS 所維護的 IP 地址。
- 對於透過閘道端點存取 DynamoDB 的執行個體，安全群組的規則必須允許進出 DynamoDB 的流量。您可以在安全群組規則中參照 DynamoDB 的 [字首清單 ID](#)。
- 對於透過閘道端點存取 DynamoDB 的執行個體，子網路的網路 ACL 必須允許進出 DynamoDB 的流量。您無法在網路 ACL 規則中參照字首清單，但可以從 DynamoDB 的 [字首清單](#) 中取得 DynamoDB 的 IP 地址範圍。
- 如果您使 AWS CloudTrail 用記錄 DynamoDB 作業，記錄檔會包含服務取用者 VPC 中 EC2 執行個體的私有 IP 地址，以及透過端點執行之任何請求的閘道端點 ID。
- 閘道端點僅支援 IPv4 流量。
- 受影響子網中執行個體的來源 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。建議您在建立或修改閘道端點時不要執行重要任務。或者，測試以確保您的軟體可在連線中斷時自動重新連線至 DynamoDB。
- 端點連線不能延伸出 VPC。VPN 連線、VPC 對等連線、傳輸閘道或 AWS Direct Connect VPC 中連線另一端的資源無法使用閘道端點與 DynamoDB 通訊。
- 您的帳戶對於每個區域的預設配額為 20 個閘道端點，此配額可進行調整。每個 VPC 也有 255 個閘道端點的限制。

## 建立閘道端點

使用下列程序建立連線至 DynamoDB 的閘道端點。

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)。
3. 選擇建立端點。
4. 對於 Service category (服務類別)，選擇 AWS 服務。
5. 對於「服務」，請新增篩選器類型 = 閘道，然後選取 com. amazonaws。##. 動態。
6. 針對 VPC，選取要在其中建立端點的 VPC。
7. 針對 Route tables (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端點網路介面。
8. 對於 Policy (政策)，選取 Full access (完整存取)，以允許 VPC 端點上所有資源的所有主體進行所有操作。否則，選取 Custom (自訂)，連接 VPC 端點政策，該政策控制主體必須在 VPC 端點上對資源執行操作的權限。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
10. 選擇建立端點。

若要使用命令列建立閘道端點

- [create-vpc-endpoint](#) (AWS CLI)
- [New-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 使用 IAM 政策控制存取

您可以建立 IAM 政策，以控制哪些 IAM 主體可以使用特定 VPC 端點存取 DynamoDB 資料表。

Example 範例：限制特定端點的存取

您可以使用 [aws:sourceVpce](#) 條件金鑰，建立政策來限制對特定 VPC 端點的存取。除非使用指定的 VPC 端點，否則下列政策會拒絕存取帳戶中的 DynamoDB 資料表。此示例假定還有一個政策聲明，允許您的使用案例所需的存取權限。

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

```

"Statement": [
  {
    "Sid": "Allow-access-from-specific-endpoint",
    "Effect": "Deny",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:region:account-id:table/*",
    "Condition": {
      "StringNotEquals" : {
        "aws:sourceVpce": "vpce-11aa22bb"
      }
    }
  }
]
}

```

### Example 範例：允許來自特定 IAM 角色的存取

您可以建立允許使用特定 IAM 角色進行存取的政策。下列政策會授予存取指定的 IAM 角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-from-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}

```

### Example 範例：允許來自特定帳戶的存取

您可以建立僅允許從特定帳戶進行存取的政策。下列政策會對指定帳戶中的使用者授予存取權。

```

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

```



```
"Statement": [  
  {  
    "Sid": "Allow-access-from-account",  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": "*",  
    "Resource": "*",  
    "Condition": {  
      "StringEquals": {  
        "aws:PrincipalAccount": "111122223333"  
      }  
    }  
  }  
]
```

## 關聯路由表

您可變更與閘道端點關聯的路由表。當您關聯路由表時，我們會自動新增路由，將以服務為目標的流量指向端點網路介面。當您取消路由表的關聯時，我們會自動從路由表中移除端點路由。

若要使用主控台來關聯路由表

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Manage route tables (管理路由表)。
5. 視需要選取或取消選取路由表。
6. 選擇 Modify route tables (修改路由表)。

若要使用命令列來關聯路由表

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 編輯 VPC 端點政策

您可以編輯閘道端點的端點政策，以控制從 VPC 透過端點對 DynamoDB 的存取。預設政策允許完整存取。如需詳細資訊，請參閱 [端點政策](#)。

## 若要使用主控台變更端點政策

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Manage policy (管理政策)。
5. 選擇 Full Access (完整存取) 以允許完整存取服務，或選擇 Custom (自訂) 並連接自訂政策。
6. 選擇儲存。

## 若要使用命令列修改閘道端點

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

下列範例端點原則用於存取 DynamoDB。

### Example 範例：允許唯讀存取權

您可以建立將存取限制為唯讀存取的政策。下列政策會授予許可，以列出和描述 DynamoDB 資料表。

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

### Example 範例：限制特定資料表的存取

您可以建立原則，限制特定 DynamoDB 資料表的存取。下列政策允許存取指定的 DynamoDB 資料表。

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

## 刪除閘道端點

閘道端點結束使用後即可刪除。當您刪除閘道端點時，我們會從子網路路由表中移除端點路由。

若要使用主控台刪除閘道端點

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)。
3. 選取閘道端點。
4. 選擇 Actions (動作)、Delete VPC endpoints (刪除 VPC 端點)。
5. 出現確認提示時，請按一下 **delete**。
6. 選擇刪除。

若要使用命令列刪除閘道端點

- [delete-vpc-endpoints](#) (AWS CLI)
- [Remove-EC2VpcEndpoint](#)(視窗工具 PowerShell)

# 透過以下方式存取 SaaS AWS PrivateLink

使用時 AWS PrivateLink，您可以私下存取 SaaS 產品，就像在您自己的 VPC 中執行一樣。

## 目錄

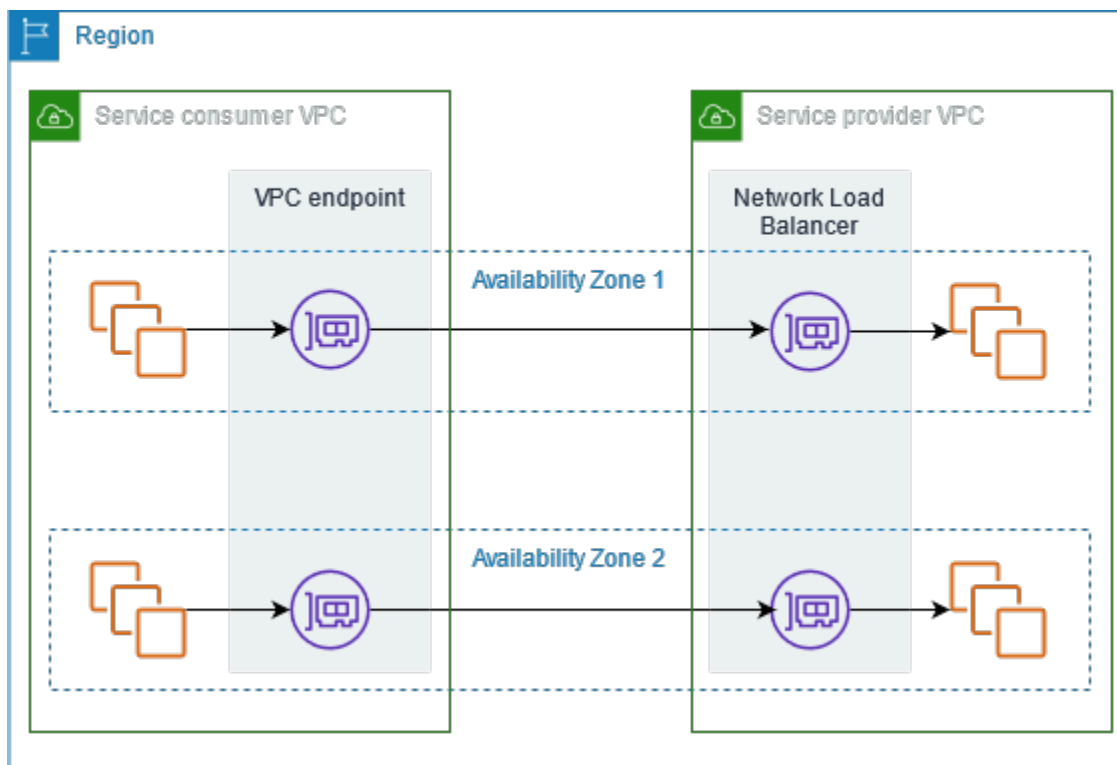
- [概要](#)
- [建立介面端點](#)

## 概要

您可以探索、購買和佈建 SaaS 產品搭 AWS PrivateLink 載 AWS Marketplace。如需詳細資訊，請參閱 [AWS Marketplace : - PrivateLink](#)。

您也可以找到由 AWS 合作夥伴提供支援 AWS PrivateLink 的 SaaS 產品。如需詳細資訊，請參閱 [AWS PrivateLink 合作夥伴](#)。

下圖顯示如何使用 VPC 端點來連接 SaaS 產品。服務提供者會建立端點服務，並授予客戶對端點服務的存取權。作為服務消費者，您可以建立介面 VPC 端點，它可在 VPC 中的一個或多個子網與端點服務之間建立連線。



## 建立介面端點

使用下列程序建立連線至 SaaS 產品的介面 VPC 端點。

需求

訂閱該服務。

若要建立合作夥伴服務的介面端點

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)。
3. 選擇建立端點。
4. 如果您從中購買服務 AWS Marketplace，請執行以下操作：
  - a. 在 Service category (服務類別) 中，選擇 AWS Marketplace services。
  - b. 輸入服務名稱。
5. 如果您使用「服務就緒」指定訂閱 AWS 服務，請執行下列動作：
  - a. 對於「服務」類別，請選擇「PrivateLink 就緒合作夥伴
  - b. 輸入服務名稱，然後選擇 Verify service (驗證服務)。
6. 對於 VPC，選取您要從中存取產品的 VPC。
7. 對於 Subnets (子網)，為每個可用區域選取一個子網，您將從中存取產品。
8. 針對 Security group (安全群組)，選取要與端點網路介面建立關聯的安全群組。安全群組規則必須允許 VPC 中的資源和端點網路介面之間的流量。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
10. 選擇建立端點。

若要建立界面端點

如需有關設定介面端點的資訊，請參閱 [the section called “設定介面端點”](#)。

# 透過存取虛擬設備 AWS PrivateLink

您可以使用 Gateway Load Balancer，將流量散發給網路虛擬設備的機群。設備可用於安全檢查、合規、政策控制和其他聯網服務。您可以在建立 VPC 端點服務時指定 Gateway Load Balancer。其他 AWS 主體會透過建立 Gateway Load Balancer 端點來存取端點服務。

## 定價

您需按每個可用區域佈建閘道 Load Balancer 端點的每小時計費。您還需要按處理的 GB 資料計費。如需詳細資訊，請參閱 [AWS PrivateLink 定價](#)。

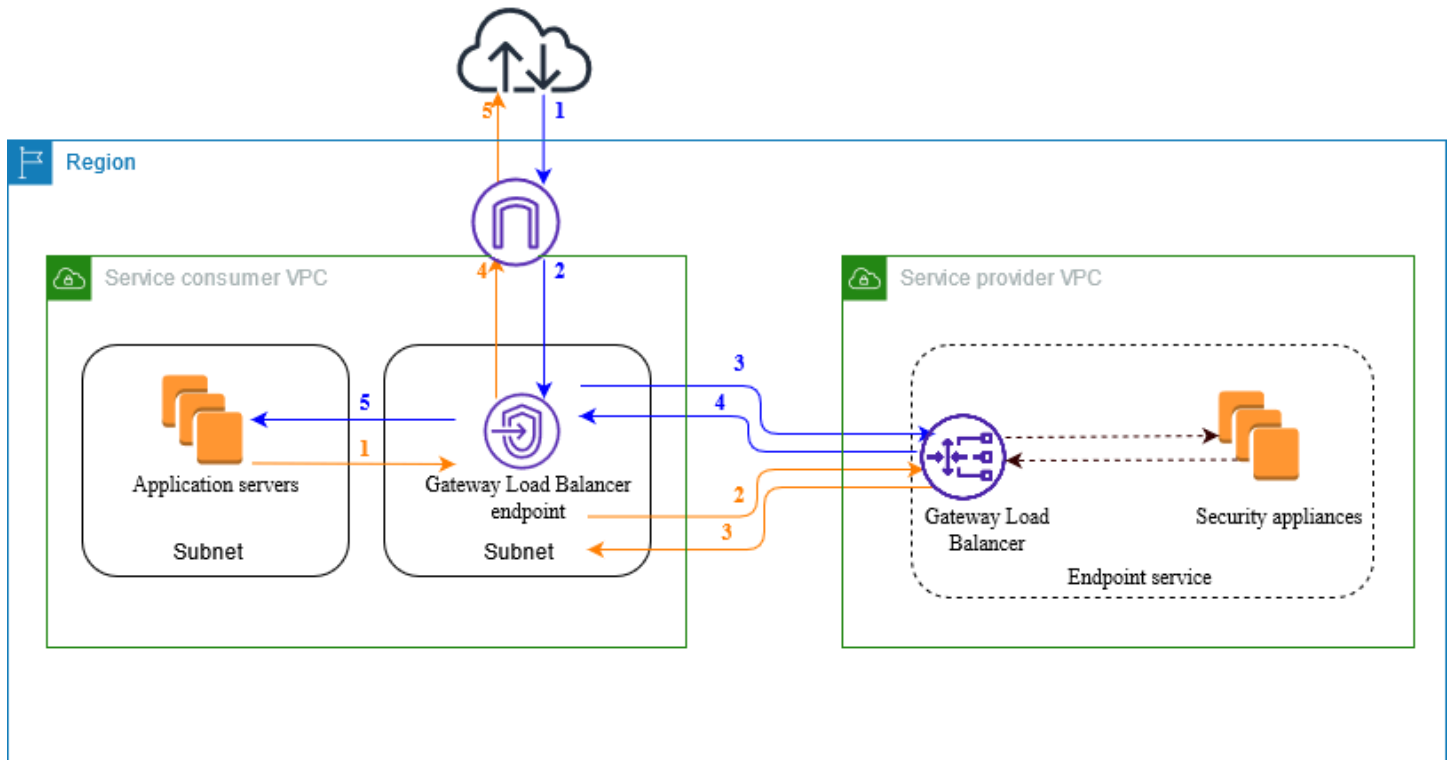
## 目錄

- [概觀](#)
- [IP 地址類型](#)
- [路由](#)
- [建立檢查系統作為 Gateway Load Balancer 端點服務](#)
- [使用 Gateway Load Balancer 端點來存取檢查系統](#)

如需詳細資訊，請參閱 [Gateway Load Balancer](#)。

## 概觀

下圖顯示應用程式伺服器如何透過存取安全設備 AWS PrivateLink。應用程式伺服器在服務消費者 VPC 的子網中執行。您可以在相同 VPC 的另一個子網中建立 Gateway Load Balancer 端點。所有透過網際網路閘道進入服務消費者 VPC 的流量會先路由至 Gateway Load Balancer 端點以便進行檢查，然後再路由至目的地子網。同樣，離開應用程式伺服器的所有流量會路由至 Gateway Load Balancer 端點，以便進行檢查，然後再透過網際網路閘道傳回。



從網際網路到應用程式伺服器的流量 (藍色箭頭)：

1. 流量透過網際網路閘道進入服務消費者 VPC。
2. 根據路由表組態，將流量傳送至 Gateway Load Balancer 端點。
3. 流量透過安全設備傳送至 Gateway Load Balancer 進行檢查。
4. 流量會在檢查之後傳回到 Gateway Load Balancer 端點。
5. 根據路由表組態，將流量傳送至應用程式伺服器。

從應用程式伺服器到網際網路的流量 (橙色箭頭)：

1. 根據路由表組態，將流量傳送至 Gateway Load Balancer 端點。
2. 流量透過安全設備傳送至 Gateway Load Balancer 進行檢查。
3. 流量會在檢查之後傳回到 Gateway Load Balancer 端點。
4. 根據路由表組態，將流量傳送至網際網路閘道。
5. 流量會傳回網際網路。

## IP 地址類型

服務提供者可以透過 IPv4、IPv6、或者同時使用 IPv4 和 IPv6 向服務取用者提供其服務端點，即使其安全設備僅支援 IPv4 也一樣。如果您啟用雙堆疊支援，現有消費者可以繼續使用 IPv4 存取您的服務，而新客戶可以選擇使用 IPv6 存取您的服務。

如果 Gateway Load Balancer 端點支援 IPv4，則端點網路界面具有 IPv4 地址。如果 Gateway Load Balancer 端點支援 IPv6，則端點網路界面具有 IPv6 地址。無法從網際網路連線端點網路界面的 IPv6 地址。如果您使用 IPv6 地址描述端點網路界面，請注意 denyAllIgwTraffic 已啟用。

為端點服務啟用 IPv6 的要求

- 端點服務的 VPC 和子網必須具有相關聯的 IPv6 CIDR 區塊。
- 端點服務的所有 Gateway Load Balancer 都必須使用雙堆疊 IP 地址類型。安全設備不需要支援 IPv6 流量。

為 Gateway Load Balancer 端點啟用 IPv6 的要求

- 端點服務必須具有包含 IPv6 支援的 IP 地址類型。
- Gateway Load Balancer 的 IP 地址類型必須與 Gateway Load Balancer 的子網路相容，如下所述：
  - IPv4 - 將 IPv4 地址指派給您的端點網路界面。只有當所有選取的子網都具有 IPv4 地址範圍時，才支援此選項。
  - IPv6 - 將 IPv6 地址指派給您的端點網路界面。只有當所有選取的子網都是 IPv6 子網時，才支援此選項。
  - Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路界面。只有當所有選取的子網都具有 IPv4 和 IPv6 地址範圍時，才支援此選項。
- 服務取用者 VPC 中的子網路路由表必須路由 IPv6 流量，而這些子網路的網路 ACL 必須允許 IPv6 流量。

## 路由

若要將流量路由至端點服務，請使用其 ID，將 Gateway Load Balancer 端點指定為路由表中的目標。對於上圖，將路由新增到路由表中，如下所示。請注意，雙堆疊組態包含 IPv6 路由。

網際網路閘道的路由表

此路由表必須具有路由，將目的地為應用程式伺服器的流量傳送至 Gateway Load Balancer 端點。



目的地	目標
<i>VPC A IPv4 CIDR</i>	區域
<i>VPC A IPv6 CIDR</i>	區域
<i>##### IPv4 CIDR</i>	<i>vpc-endpoint-id</i>
<i>##### IPv6 CIDR</i>	<i>vpc-endpoint-id</i>

### 具有應用程式伺服器的子網路路由表

此路由表必須具有路由，將應用程式伺服器傳出的所有流量傳送至 Gateway Load Balancer 端點。

目的地	目標
<i>VPC A IPv4 CIDR</i>	區域
<i>VPC A IPv6 CIDR</i>	區域
0.0.0.0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

### 具有 Gateway Load Balancer 端點的子網路路由表

此路由表必須將檢查傳回的流量傳送至其最終目的地。對於源自網際網路的流量，本機路由會將流量傳送至應用程式伺服器。對於源自應用程式伺服器的流量，請新增路由，將所有流量傳送至網際網路閘道。

目的地	目標
<i>VPC A IPv4 CIDR</i>	區域
<i>VPC A IPv6 CIDR</i>	區域
0.0.0.0/0	<i>internet-gateway-id</i>

目的地	目標
::/0	<i>internet-gateway-id</i>

## 建立檢查系統作為 Gateway Load Balancer 端點服務

您可以建立自己的服務 AWS PrivateLink，稱為端點服務。您是服務提供者，而建立服務連線的 AWS 主體就是服務取用者。

端點服務需要 Network Load Balancer 或 Gateway Load Balancer。在此情況下，您將使用 Gateway Load Balancer 建立端點服務。如需使用 Network Load Balancer 建立端點服務的詳細資訊，請參閱 [建立端點服務](#)。

### 目錄

- [考量事項](#)
- [必要條件](#)
- [建立端點服務](#)
- [讓您的端點服務可用](#)

## 考量事項

- 端點服務在您建立該服務的區域中可用。
- 當服務消費者擷取端點服務的相關資訊時，他們只能看到與服務提供者共同的可用區域。服務提供者與服務消費者處於不同帳戶時，可將區域名稱 (例如 us-east-1a) 對應至每個 AWS 帳戶中的不同實體可用區域。您可以使用 AZ ID 一致地識別服務的可用區域。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [AZ ID](#)。
- 您的 AWS PrivateLink 資源有配額。如需詳細資訊，請參閱 [AWS PrivateLink 配額](#)。

## 必要條件

- 在可用區域中建立至少具有兩個子網的服務提供者 VPC，而該服務在其中應可用。一個子網用於安全設備執行個體，另一個子網用於 Gateway Load Balancer。

- 在服務提供者 VPC 中建立 Gateway Load Balancer。如果您打算在端點服務上啟用 IPv6 支援，則必須在 Gateway Load Balancer 上啟用雙堆疊支援。如需詳細資訊，請參閱[開始使用 Gateway Load Balancer](#)。
- 在服務提供者 VPC 中啟動安全設備，並向負載平衡器目標群組註冊它們。

## 建立端點服務

使用下列程序，利用 Gateway Load Balancer 建立端點服務。

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 Endpoints Services (端點服務)。
3. 選擇 Create Endpoint Service (建立端點服務)。
4. 針對 Load balancer type (負載平衡器類型)，選取 Gateway (閘道)。
5. 針對 Available load balancers (可用的負載平衡器)，請選取您的 Gateway Load Balancer。
6. 對於 Require acceptance for endpoint (要求接受端點)，選取 Acceptance required (要求接受)，以要求手動接受對端點服務的連線請求。否則，系統會自動接受。
7. 針對 Supported IP address types (支援的 IP 地址類型)，執行下列其中一個操作：
  - 選取 IPv4 - 啟用端點服務以接受 IPv4 請求。
  - 選取 IPv6 - 啟用端點服務以接受 IPv6 請求。
  - 選取 IPv4 和 IPv6 - 啟用端點服務以接受 IPv4 和 IPv6 請求。
8. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
9. 選擇 Create (建立)。

若要使用命令列建立端點服務

- [create-vpc-endpoint-service-configuration](#) (AWS CLI)
- [New-EC2VpcEndpointServiceConfiguration](#) (視窗工具 PowerShell)

## 讓您的端點服務可用

服務提供者必須執行下列操作，才能向服務消費者提供服務。

- 新增允許每個服務消費者連接到端點服務的許可。如需詳細資訊，請參閱 [the section called “管理許可”](#)。
- 為服務消費者提供服務名稱和受支援的可用區域，以便他們可以建立介面端點，從而連接到您的服務。如需詳細資訊，請參閱下面的程序。
- 接受來自服務消費者的端點連線請求。如需詳細資訊，請參閱 [the section called “接受或拒絕連線請求”](#)。

AWS 主體可以透過建立閘道 Load Balancer 端點，私下連線到您的端點服務。如需詳細資訊，請參閱 [建立 Gateway Load Balancer 端點](#)。

## 使用 Gateway Load Balancer 端點來存取檢查系統

您可以建立 Gateway Load Balancer 端點以連線至 AWS PrivateLink 支援的 [端點服務](#)。

對於您從 VPC 中指定的每個子網，我們會在子網中建立端點網路介面，並從子網地址範圍中為其指派私有 IP 地址。端點網路介面是由請求者管理的網路介面；您可以在您的網路介面中檢視 AWS 帳戶，但無法自行管理。

我們會向您收取每小時用量率及資料處理費。如需詳細資訊，請參閱 [Gateway Load Balancer 端點定價](#)。

### 目錄

- [考量事項](#)
- [必要條件](#)
- [建立端點](#)
- [設定路由](#)
- [管理標籤](#)
- [刪除 Gateway Load Balancer 端點](#)

## 考量事項

- 您只能在服務消費者 VPC 中選擇一個可用區域。您之後無法變更此子網。若要在不同子網中使用 Gateway Load Balancer 端點，則必須建立新的 Gateway Load Balancer 端點。
- 您可以為每個服務的每個可用區域建立單一 Gateway Load Balancer 端點，但必須選擇 Gateway Load Balancer 支援的可用區域。服務提供者與服務消費者處於不同帳戶時，可將區域名稱 (例如

- us-east-1a) 對應至每個 AWS 帳戶中的不同實體可用區域。您可以使用 AZ ID 一致地識別服務的可用區域。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [AZ ID](#)。
- 必須在服務提供者接受連線請求之後，您才能使用端點服務。服務無法透過 VPC 端點向您的 VPC 中的資源發起請求。端點只會傳回 VPC 中的資源啟動的流量的回應。
  - 每個閘道負載平衡器端點可支援每個可用區域 (AZ) 高達 10 Gbps 的頻寬，並自動擴充至 100 Gbps。
  - 如果端點服務與多個 Gateway Load Balancer 相關聯，則 Gateway Load Balancer 端點在每個可用區域僅與一個負載平衡器建立連線。
  - 若要將流量保留在相同的可用區域內，建議您在要向其傳送流量的每個可用區域中建立 Gateway Load Balancer 端點。
  - 當流量透過 Gateway Load Balancer 端點路由傳送時，不支援 Network Load Balancer 用戶端 IP 保留，即使目標與 Network Load Balancer 位於相同的 VPC 中也一樣。
  - 您的 AWS PrivateLink 資源有配額。如需詳細資訊，請參閱 [AWS PrivateLink 配額](#)。

## 必要條件

- 在可用區域中建立至少具有兩個子網的服務消費者 VPC，您可以從中存取服務。一個子網用於應用程式伺服器，另一個子網用於 Gateway Load Balancer 端點。
- 若要確認端點服務支援哪些可用區域，請使用主控台或 [describe-vpc-endpoint-services](#) 命令描述端點服務。
- 如果您的資源位於具有網路 ACL 的子網中，請確認網路 ACL 允許端點網路介面和 VPC 中資源之間的流量。

## 建立端點

使用下列程序建立連線至檢查系統端點服務的 Gateway Load Balancer 端點。

若要使用主控台建立 Gateway Load Balancer 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)。
3. 選擇建立端點。
4. 針對 Service category (服務類別) 中，選擇 Other endpoint services (其他端點服務)。
5. 針對 Service Name (服務名稱)，請輸入服務名稱，然後選擇 Verify Service (驗證服務)。

6. 針對 VPC，選取要在其中建立端點的 VPC。
7. 針對 Subnets (子網路)，請選取要在其中建立端點的子網路。
8. 針對 IP address type (IP 地址類型)，從下列選項中選擇：
  - IPv4 - 將 IPv4 地址指派給您的端點網路介面。只有當所有選取子網都具有 IPv4 地址範圍時，才支援此選項。
  - IPv6 - 將 IPv6 地址指派給您的端點網路介面。只有當所有選取子網都是 IPv6 子網時，才支援此選項。
  - Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路介面。只有當所有選取子網都具有 IPv4 和 IPv6 地址範圍時，才支援此選項。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
10. 選擇建立端點。起始狀態為 pending acceptance。

若要使用命令列建立 Gateway Load Balancer 端點

- [create-vpc-endpoint](#) (AWS CLI)
- [New-EC2VpcEndpoint](#) (視窗工具 PowerShell)

## 設定路由

使用以下程序為服務消費者 VPC 設定路由表。如此可讓安全設備針對傳送至應用程式伺服器的傳入流量執行安全檢查。如需詳細資訊，請參閱 [the section called “路由”](#)。

若要使用主控台設定路由

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. 選取網際網路閘道路由表並執行以下操作：
  - a. 選擇 Actions (動作)、Edit routes (編輯路由)。
  - b. 如果您支援 IPv4，請選擇 Add route (新增路由)。針對 Destination (目的地)，請輸入應用程式伺服器子網的 IPv4 CIDR 區塊。針對 Target (目標)，請選取 VPC 端點。
  - c. 如果您支援 IPv6，請選擇 Add route (新增路由)。針對 Destination (目的地)，請輸入應用程式伺服器子網的 IPv6 CIDR 區塊。針對 Target (目標)，請選取 VPC 端點。
  - d. 選擇儲存變更。

4. 為具有應用程式伺服器的子網選取路由表並執行以下操作：
  - a. 選擇 Actions (動作)、Edit routes (編輯路由)。
  - b. 如果您支援 IPv4，請選擇 Add route (新增路由)。針對 Destination (目標)，輸入 **0.0.0.0/0**。針對 Target (目標)，請選取 VPC 端點。
  - c. 如果您支援 IPv6，請選擇 Add route (新增路由)。針對 Destination (目標)，輸入 **::/0**。針對 Target (目標)，請選取 VPC 端點。
  - d. 選擇儲存變更。
5. 選取具有 Gateway Load Balancer 端點之子網路的路由表，並執行以下操作：
  - a. 選擇 Actions (動作)、Edit routes (編輯路由)。
  - b. 如果您支援 IPv4，請選擇 Add route (新增路由)。針對 Destination (目標)，輸入 **0.0.0.0/0**。針對 Target (目標)，請選取網際網路閘道。
  - c. 如果您支援 IPv6，請選擇 Add route (新增路由)。針對 Destination (目標)，輸入 **::/0**。針對 Target (目標)，請選取網際網路閘道。
  - d. 選擇儲存變更。

若要使用命令列設定路由

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (視窗工具 PowerShell)

## 管理標籤

您可標記您的 Gateway Load Balancer 端點，以幫助您根據組織需求進行識別或分類。

若要使用主控台管理標籤

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. 選取介面端點。
4. 選擇 Actions (動作)、Manage tags (管理標籤)。
5. 對於要新增的每個標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤金鑰和標籤值。
6. 若要移除標籤，請選擇標籤金鑰和值右側的 Remove (移除)。
7. 選擇儲存。

## 若要使用命令列來管理標籤

- [create-tags](#) 和 [delete-tags](#) (AWS CLI)
- [New-EC2Tag](#)和 [Remove-EC2Tag](#)(視窗工具 PowerShell)

## 刪除 Gateway Load Balancer 端點

端點結束使用後即可刪除。刪除 Gateway Load Balancer 端點也會刪除端點網路介面。如果路由表中有指向端點的路由，則無法刪除 Gateway Load Balancer 端點。

### 若要刪除 Gateway Load Balancer 端點

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

### 若要刪除 Gateway Load Balancer 端點

- [delete-vpc-endpoints](#) (AWS CLI)
- [Remove-EC2VpcEndpoint](#) (AWS Tools for Windows PowerShell)



# 透過以下方式分享您 AWS PrivateLink

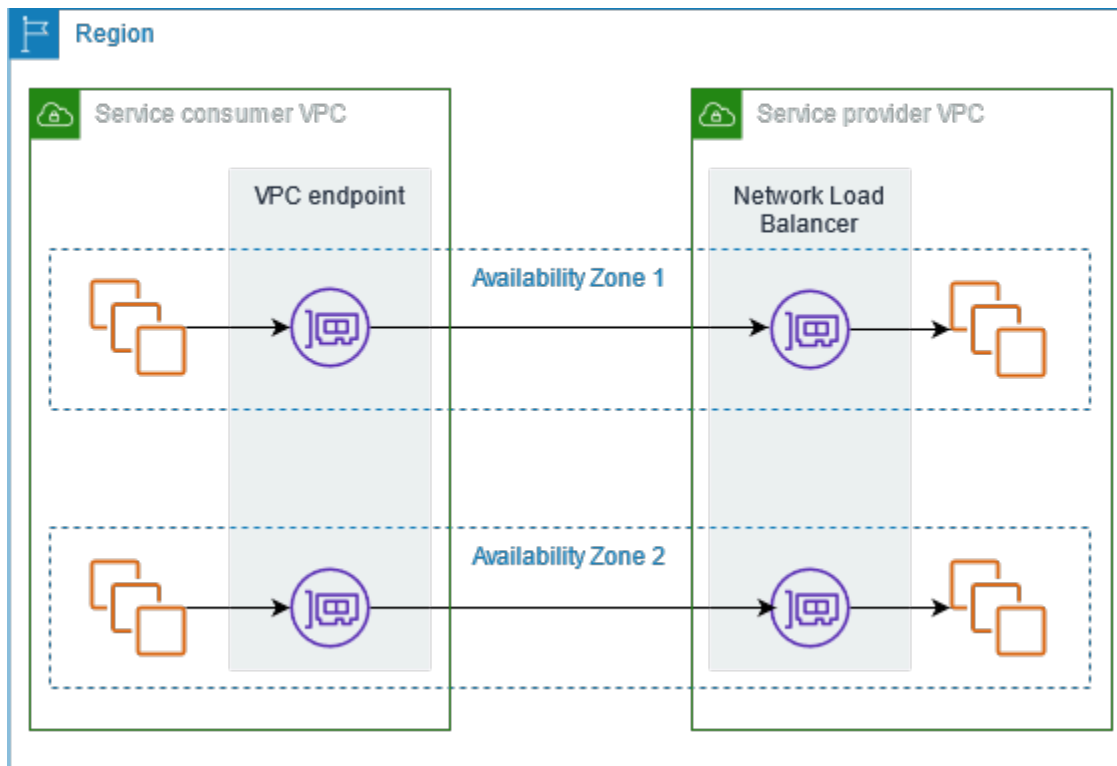
您可以託管自己的 AWS PrivateLink 供電服務 (稱為端點服務)，並與其他 AWS 客戶共用。

## 目錄

- [概要](#)
- [DNS 主機名稱](#)
- [私有 DNS](#)
- [IP 地址類型](#)
- [建立提供支援的服務 AWS PrivateLink](#)
- [設定端點服務](#)
- [管理 VPC 端點服務的 DNS 名稱](#)
- [接收端點服務事件的提醒](#)
- [刪除端點服務](#)

## 概要

下圖顯示您如何 AWS 與其他 AWS 客戶共用託管的服務，以及這些客戶如何連接到您的服務。作為服務提供者，您可以在 VPC 中建立 Network Load Balancer 作為服務前端。然後，您可以在建立 VPC 端點服務組態時選取此負載平衡器。您可以對特定 AWS 主體授予權限，以便他們連接到您的服務。作為服務消費者，客戶可建立界面 VPC 端點，它可在他們從其 VPC 中選取的子網與您的端點服務之間建立連線。負載平衡器會收到來自服務消費者的請求，並將它們傳送至託管您服務的目標。



為了實現低延遲和高可用性，建議您在至少兩個可用區域提供您的服務。

## DNS 主機名稱

當服務提供者建立 VPC 端點服務時，AWS 會為服務產生端點特定的 DNS 主機名稱。這些名稱具有下列語法：

```
endpoint_service_id.region.vpce.amazonaws.com
```

以下是 us-east-2 區域中 VPC 端點服務的 DNS 主機名稱範例：

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

當服務消費者建立介面 VPC 端點時，我們會建立區域名稱和區域 DNS 名稱，服務消費者可使用它們與端點服務通訊。區域名稱具有下列語法：

```
endpoint_id.endpoint_service_id.region.vpce.amazonaws.com
```

分區名稱具有下列語法：

```
endpoint_id-zone.endpoint_service_id.region.vpce.amazonaws.com
```

## 私有 DNS

服務提供者也可以關聯其端點服務的私有 DNS 名稱，以便服務消費者可以繼續使用其現有 DNS 名稱來存取服務。如果服務提供者將私有 DNS 名稱與其端點服務相關聯，則服務消費者可以為其介面端點啟用私有 DNS 名稱。如果服務提供者未啟用私有 DNS，服務消費者可能需要更新其應用程式，才能使用 VPC 端點服務的公有 DNS 名稱。如需詳細資訊，請參閱 [管理 DNS 名稱](#)。

## IP 地址類型

服務提供者可以透過 IPv4、IPv6、或者同時使用 IPv4 和 IPv6 向服務消費者提供其服務端點，即使其後端伺服器僅支援 IPv4。如果您啟用雙堆疊支援，現有消費者可以繼續使用 IPv4 存取您的服務，而新客戶可以選擇使用 IPv6 存取您的服務。

如果介面 VPC 端點支援 IPv4，則端點網路介面具有 IPv4 地址。如果介面 VPC 端點支援 IPv6，則端點網路介面具有 IPv6 地址。無法從網際網路連線端點網路介面的 IPv6 地址。如果您使用 IPv6 地址描述端點網路介面，請注意 denyAllIgwTraffic 已啟用。

### 為端點服務啟用 IPv6 的要求

- 端點服務的 VPC 和子網必須具有相關聯的 IPv6 CIDR 區塊。
- 端點服務的所有 Network Load Balancer 都必須使用雙堆疊 IP 地址類型。目標不需要支援 IPv6 流量。如果服務處理來自代理通訊協定第 2 版標頭的來源 IP 地址，則它必須處理 IPv6 地址。

### 為介面端點啟用 IPv6 的要求

- 端點服務必須支援 IPv6 請求。
- 介面端點的 IP 地址類型必須與介面端點的子網相容，如下所述：
  - IPv4 - 將 IPv4 地址指派給您的端點網路介面。只有當所有選取子網都具有 IPv4 地址範圍時，才支援此選項。
  - IPv6 - 將 IPv6 地址指派給您的端點網路介面。只有當所有選取子網都是 IPv6 子網時，才支援此選項。
  - Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路介面。只有當所有選取子網都具有 IPv4 和 IPv6 地址範圍時，才支援此選項。

## 介面端點的 DNS 記錄 IP 地址類型

介面端點支援的 DNS 記錄 IP 地址類型會決定我們建立的 DNS 記錄。介面端點的 DNS 記錄 IP 地址類型必須與介面端點的 IP 地址類型相容，如下所述：

- IPv4 - 建立私有名稱、區域名稱和分區 DNS 名稱的 A 記錄。IP 地址類型必須為 IPv4 或者 Dualstack。
- IPv6 - 建立私有名稱、區域名稱和分區 DNS 名稱的 AAAA 記錄。IP 地址類型必須為 IPv6 或者 Dualstack。
- Dualstack - 建立私有名稱、區域名稱和分區 DNS 名稱的 A 和 AAAA 記錄。IP 地址類型必須為 Dualstack。

## 建立提供支援的服務 AWS PrivateLink

您可以建立自己的服務 AWS PrivateLink，稱為端點服務。您是服務提供者，而與您的服務建立連線的 AWS 主體是服務消費者。

端點服務需要 Network Load Balancer 或 Gateway Load Balancer。負載平衡器會收到來自服務消費者的請求，並將它們傳送至您的服務。在這種情況下，您將使用 Network Load Balancer 建立端點服務。如需使用 Gateway Load Balancer 建立端點服務的詳細資訊，請參閱 [存取虛擬設備](#)。

### 目錄

- [考量事項](#)
- [必要條件](#)
- [建立端點服務](#)
- [讓服務消費者可以使用您的端點服務](#)

## 考量事項

- 端點服務在您建立該服務的區域中可用。您可以使用 VPC 互連從其他區域存取端點服務。
- 端點服務僅支援 TCP 上的流量。
- 當服務消費者擷取端點服務的相關資訊時，他們只能看到與服務提供者共同的可用區域。服務提供者與服務消費者處於不同帳戶時，可將區域名稱 (例如 us-east-1a) 對應至每個 AWS 帳戶中的不同實體可用區域。您可以使用 AZ ID 一致地識別服務的可用區域。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 [AZ ID](#)。

- 當服務消費者透過介面端點向服務傳送流量時，提供給應用程式的來源 IP 地址為負載平衡器節點的私有 IP 地址，而不是服務消費者的 IP 地址。如果您在負載平衡器上啟用代理通訊協定，則可以從代理通訊協定標頭中取得服務消費者的地址和介面端點的識別碼。如需詳細資訊，請參閱 [Network Load Balancer 使用者指南](#) 中的 [Proxy 通訊協定](#)。
- 如果端點服務與多個 Network Load Balancer 相關聯，則每個端點網路介面會與一個負載平衡器相關聯。啟動來自端點網路介面的第一個連線時，我們會隨機選取相同可用區域中的其中一個 Network Load Balancer 作為端點網路介面。來自此端點網路介面的所有後續連線請求都會使用選取的負載平衡器。建議您針對端點服務的所有負載平衡器使用相同的接聽程式和目標群組組態，如此一來，無論選擇哪一個負載平衡器，消費者都能成功使用端點服務。
- 您的 AWS PrivateLink 資源有配額。如需詳細資訊，請參閱 [AWS PrivateLink 配額](#)。

## 必要條件

- 在提供服務的每個可用區域中建立至少具有一個子網的端點服務的 VPC。
- 若要讓服務消費者能夠為您的端點服務建立 IPv6 介面 VPC 端點，VPC 和子網必須具有相關聯的 IPv6 CIDR 區塊。
- 在您的 VPC 中建立 Network Load Balancer。為每個可用區域選取一個子網，在該子網中服務應可供服務消費者使用。為了實現低延遲和容錯，建議您在該區域的至少兩個可用區域提供您的服務。
- 如果您的 Network Load Balancer 具有安全性群組，則必須允許來自用戶端 IP 位址的輸入流量。或者，您也可以關閉傳入安全性群組規則的評估，以便透過流量 AWS PrivateLink。如需詳細資訊，請參閱網路負載平衡器使用者指南中的 [安全性群組](#)。
- 若要讓端點服務能夠接受 IPv6 請求，其 Network Load Balancer 必須使用雙堆疊 IP 地址類型。目標不需要支援 IPv6 流量。如需詳細資訊，請參閱《Network Load Balancer 使用者指南》中的 [IP 地址類型](#)。

如果您處理來自代理通訊協定第 2 版標頭的來源 IP 地址，請確認您可處理 IPv6 地址。

- 在應該提供服務的每個可用區域中啟動執行個體，並向負載平衡器目標群組註冊它們。如果您未在所有啟用的可用區域中啟動執行個體，您可啟用跨區域負載平衡，以支援使用區域 DNS 主機名稱存取服務的服務消費者。當您啟用跨區域負載平衡時，應支付區域資料傳輸費用。如需詳細資訊，請參閱網路 [負載平衡器使用者指南](#) 中的 [跨區域負載平衡](#)。

## 建立端點服務

使用下列程序，利用 Network Load Balancer 建立端點服務。

## 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 Endpoints Services (端點服務)。
3. 選擇 Create Endpoint Service (建立端點服務)。
4. 針對 Load balancer type (負載平衡器類型)，選擇 Network (網路)。
5. 針對 Available load balancers (可用的負載平衡器)，選取要與端點服務建立關聯的 Network Load Balancer。包含的可用區域會列出針對所選網路負載平衡器啟用的可用區域。您的端點服務將在這些可用區域中提供。
6. 對於 Require acceptance for endpoint (要求接受端點)，選取 Acceptance required (要求接受)，以要求手動接受對端點服務的連線請求。否則，系統會自動接受這些請求。
7. 針對 Enable private DNS name (啟用私有 DNS 名稱)，選取 Associate a private DNS name with the service (將私有 DNS 名稱與服務建立關聯)，以關聯服務消費者可用於存取服務的私有 DNS 名稱，然後輸入私有 DNS 名稱。否則，服務消費者可以使用由提供的端點特定 DNS 名稱。AWS 在服務消費者使用私有 DNS 名稱之前，服務提供者必須確認他們擁有該網域。如需詳細資訊，請參閱 [管理 DNS 名稱](#)。
8. 針對 Supported IP address types (支援的 IP 地址類型)，執行下列其中一個操作：
  - 選取 IPv4 - 啟用端點服務以接受 IPv4 請求。
  - 選取 IPv6 - 啟用端點服務以接受 IPv6 請求。
  - 選取 IPv4 和 IPv6 - 啟用端點服務以接受 IPv4 和 IPv6 請求。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
10. 選擇 Create (建立)。

## 若要使用命令列建立端點服務

- [create-vpc-endpoint-service-configuration](#) (AWS CLI)
- [New-EC2VpcEndpointServiceConfiguration](#)(視窗工具 PowerShell)

## 讓服務消費者可以使用您的端點服務

AWS 主體可以透過建立介面 VPC 端點來私下連線到您的端點服務。服務提供者必須執行下列操作，才能向服務消費者提供服務。

- 新增允許每個服務消費者連接到端點服務的許可。如需詳細資訊，請參閱 [the section called “管理許可”](#)。
- 為服務消費者提供服務名稱和受支援的可用區域，以便他們可以建立介面端點，從而連接到您的服務。如需詳細資訊，請參閱下列程序。
- 接受來自服務消費者的端點連線請求。如需詳細資訊，請參閱 [the section called “接受或拒絕連線請求”](#)。

## 以服務消費者身分連接到端點服務

服務消費者使用下列程序建立介面端點以連接到您的端點服務。

若要使用主控台建立介面端點

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)。
3. 選擇建立端點。
4. 針對 Service category (服務類別) 中，選擇 Other endpoint services (其他端點服務)。
5. 針對 Service name (服務名稱)，輸入服務名稱 (例如 com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc)，然後選擇 Verify (驗證服務)。
6. 針對 VPC，選取要在其中建立端點的 VPC。
7. 針對 Subnets (子網)，選取您將從其中存取端點服務的子網 (可用區域)。
8. 針對 IP address type (IP 地址類型)，從下列選項中選擇：
  - IPv4 - 將 IPv4 地址指派給您的端點網路介面。只有當所有選取子網路都具有 IPv4 地址範圍，且端點服務接受 IPv4 請求時，才支援此選項。
  - IPv6 - 將 IPv6 地址指派給您的端點網路介面。只有當所有選取子網路都是僅限 IPv6 子網路，且端點服務接受 IPv6 請求時，才支援此選項。
  - Dualstack - 將 IPv4 和 IPv6 地址指派給您的端點網路介面。只有當所有選取子網路都具有 IPv4 和 IPv6 地址範圍，且端點服務接受 IPv4 和 IPv6 請求時，才支援此選項。
9. 針對 DNS record IP type (DNS 記錄 IP 類型)，選擇以下其中一個選項：
  - IPv4 - 建立私有名稱、區域名稱和分區 DNS 名稱的 A 記錄。IP 地址類型必須為 IPv4 或者 Dualstack。
  - IPv6 - 建立私有名稱、區域名稱和分區 DNS 名稱的 AAAA 記錄。IP 地址類型必須為 IPv6 或者 Dualstack。



- Dualstack - 建立私有名稱、區域名稱和分區 DNS 名稱的 A 和 AAAA 記錄。IP 地址類型必須為 Dualstack。
  - Service defined (已定義服務) — 為私有名稱、區域名稱和區域 DNS 名稱建立 A 記錄，為區域名稱和區域 DNS 名稱建立 AAAA 記錄。IP 地址類型必須為 Dualstack。
10. 針對 Security group (安全群組)，選取要與端點網路介面建立關聯的安全群組。
  11. 選擇建立端點。

使用命令列建立介面端點

- [create-vpc-endpoint](#) (AWS CLI)
- [New-EC2VpcEndpoint](#)(視窗工具 PowerShell)

## 設定端點服務

建立端點服務之後，您可更新其組態。

任務

- [管理許可](#)
- [接受或拒絕連線請求](#)
- [管理負載平衡器](#)
- [關聯私有 DNS 名稱](#)
- [修改支援的 IP 地址類型](#)
- [管理標籤](#)

## 管理許可

使用權限和接受設定的組合可協助您控制哪些服務取用者 (AWS 主體) 可以存取您的端點服務。例如，您可將許可授予您信任的特定主體，自動接受所有連線請求，或者可將許可授予更大的主體群組，以手動方式接受您信任的特定連線請求。

根據預設，服務消費者無法使用您的端點服務。您必須新增允許特定 AWS 主體建立介面 VPC 端點以連線到端點服務的權限。若要為 AWS 主體新增許可，您需要其 Amazon 資源名稱 (ARN)。以下清單包含適用於支援的 AWS 主體的範例 ARN。



## 主 AWS 參與者的 ARN

AWS 帳戶 (包括帳戶中的所有主參與者)

```
arn:aws:iam::account_id:root
```

角色

```
arn:aws:iam::account_id:role/role_name
```

使用者

```
arn:aws:iam::account_id:user/user_name
```

全部中的所有主參與者 AWS 帳戶

\*

## 考量事項

- 如果您授予所有人存取端點服務的許可，並將端點服務設定為接受所有請求，即使負載平衡器沒有公有 IP 地址，它也將是公有的。
- 如果您移除權限，則不會影響端點與先前接受的服務之間的現有連線。

使用主控台為您的端點服務管理許可

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務，然後選擇 Allow principals (允許主體) 索引標籤。
4. 若要新增權限，請選擇 Allow principals (允許主體)。針對 Principals to add (要新增的主體)，輸入主體的 ARN。若要新增其他委託人，請選擇 Add principal (新增委託人)。您完成新增主體時，請選擇 Allow principals (允許主體)。
5. 若要移除許可，請選取主體，然後選擇 Actions (動作)、Delete (刪除)。出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

若要使用命令列為您的端點服務新增許可

- [modify-vpc-endpoint-service-permissions](#) (AWS CLI)
- [Edit-EC2EndpointServicePermission](#)(視窗工具 PowerShell)

## 接受或拒絕連線請求

使用權限和接受設定的組合可協助您控制哪些服務取用者 (AWS 主體) 可以存取您的端點服務。例如，您可將許可授予您信任的特定主體，自動接受所有連線請求，或者可將許可授予更大的主體群組，以手動方式接受您信任的特定連線請求。

您可以設定端點服務以自動接受連線請求。否則，您必須手動接受或拒絕它們。如果您不接受連線請求，服務消費者就無法存取您的端點服務。

當接受或拒絕連線請求時，您會收到通知。如需詳細資訊，請參閱 [the section called “接收端點服務事件的提醒”](#)。

### 考量事項

- 如果您授予所有人存取端點服務的許可，並將端點服務設定為接受所有請求，即使負載平衡器沒有公有 IP 地址，它也將是公有的。
- 如果您拒絕已接受的要求，則不會影響端點與服務之間的連線。

### 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 Endpoints Services (端點服務)。
3. 選取端點服務。
4. 選擇 Actions (動作)、Modify endpoint acceptance setting (修改端點接受設定)。
5. 選擇或清除 Acceptance required (需要接受)。
6. 選擇 Save changes (儲存變更)

### 若要使用命令列修改接受設定

- [modify-vpc-endpoint-service-configuration](#) (AWS CLI)
- [Edit-EC2VpcEndpointServiceConfiguration](#) (視窗工具 PowerShell)

### 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 Endpoints Services (端點服務)。

3. 選取端點服務。
4. 從 Endpoint connections (端點連線) 標籤中，選取端點連線。
5. 若要接受連線請求，請選擇 Actions (動作)、Accept endpoint connection request (接受端點連線請求)。出現確認提示時，請輸入 **accept**，然後選擇 Accept (接受)。
6. 若要拒絕連線請求，請選擇 Actions (動作)、Reject endpoint connection request (拒絕端點連線請求)。出現確認提示時，請輸入 **reject**，然後選擇 Reject (拒絕)。

若要使用命令列接受或拒絕連線請求

- [accept-vpc-endpoint-connections](#) 或 [reject-vpc-endpoint-connections](#) (AWS CLI)
- [Approve-EC2EndpointConnection](#) 或 [Deny-EC2EndpointConnection](#) (視窗工具 PowerShell)

## 管理負載平衡器

您可以管理與端點服務相關聯的負載平衡器。如果端點已連接到您的端點服務，則無法取消關聯負載平衡器。

如果您為 Network Load Balancer 啟用其他可用區域，也可以為您的端點服務啟用可用區域。為端點服務啟用可用區域後，服務取用者可以將子網路從該可用區域新增至其介面 VPC 端點。

使用主控台管理端點服務的負載平衡器

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務。
4. 選擇 Actions (動作)、Associate or disassociate load balancers (關聯/取消關聯負載平衡器)。
5. 視需要變更端點服務組態。例如：
  - 選取負載平衡器的核取方塊，以將其與端點服務產生關聯。
  - 清除負載平衡器的核取方塊，以取消其與端點服務的關聯。您必須保持至少選取一個負載平衡器。
  - 如果您最近為負載平衡器啟用了另一個可用區域，它會出現在包含的可用區域下。如果您在下一個步驟中儲存變更，這會啟用新可用區域的端點服務。
6. 選擇 Save changes (儲存變更)

## 使用命令列管理端點服務的負載平衡器

- [modify-vpc-endpoint-service-configuration](#) (AWS CLI)
- [Edit-EC2VpcEndpointServiceConfiguration](#)(視窗工具 PowerShell)

若要在最近為負載平衡器啟用的可用區域中啟用端點服務，只需使用端點服務的 ID 呼叫命令即可。

## 關聯私有 DNS 名稱

您可以將私有 DNS 名稱與您的端點服務建立關聯。在關聯私有 DNS 名稱之後，您必須在您的 DNS 伺服器上更新網域項目。在服務消費者使用私有 DNS 名稱之前，服務提供者必須確認他們擁有該網域。如需詳細資訊，請參閱 [管理 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。
4. 選擇 Actions (動作)、Modify private DNS name (修改私有 DNS 名稱)。
5. 選取 Associate a private DNS name with the service (將私有 DNS 名稱與服務建立關聯)，並輸入私有 DNS 名稱。
  - 網域名稱必須為小寫。
  - 您可以在網域名稱中使用萬用字元 (例如，**\*.myexampleservice.com**)。
6. 選擇儲存變更。
7. 當驗證狀態為 verified (已驗證) 時，私有 DNS 名稱即可供服務消費者使用。如果驗證狀態變更，新的連線請求會遭到拒絕，但現有的連線不受影響。

### 若要使用命令列修改端點服務私有 DNS 名稱

- [modify-vpc-endpoint-service-configuration](#) (AWS CLI)
- [Edit-EC2VpcEndpointServiceConfiguration](#)(視窗工具 PowerShell)

### 若要使用主控台來啟動網域驗證程序

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。
4. 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)。
5. 出現確認提示時，請輸入 **verify**，然後選擇 Verify (確認)。

若要使用命令列來啟動網域驗證程序

- [start-vpc-endpoint-service-private-dns-verification](#) (AWS CLI)
- [Start-EC2VpcEndpointServicePrivateDnsVerification](#)(視窗工具 PowerShell)

## 修改支援的 IP 地址類型

您可以變更端點服務支援的 IP 地址類型。

### 考量事項

若要讓端點服務能夠接受 IPv6 請求，其 Network Load Balancer 必須使用雙堆疊 IP 地址類型。目標不需要支援 IPv6 流量。如需詳細資訊，請參閱《Network Load Balancer 使用者指南》中的 [IP 地址類型](#)。

若要使用主控台修改支援的 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 Endpoints Services (端點服務)。
3. 選取 VPC 端點服務。
4. 選擇 Actions (動作)、Modify supported IP address types (修改支援的 IP 地址類型)。
5. 針對 Supported IP address types (支援的 IP 地址類型)，執行下列其中一個操作：
  - 選取 IPv4 - 啟用端點服務以接受 IPv4 請求。
  - 選取 IPv6 - 啟用端點服務以接受 IPv6 請求。
  - 選取 IPv4 和 IPv6 - 啟用端點服務以接受 IPv4 和 IPv6 請求。
6. 選擇儲存變更。

## 使用命令列修改支援的 IP 地址類型

- [modify-vpc-endpoint-service-configuration](#) (AWS CLI)
- [Edit-EC2VpcEndpointServiceConfiguration](#)(視窗工具 PowerShell)

## 管理標籤

您可標記您的資源，以幫助您根據組織需求來進行識別或分類。

### 使用主控台為您的端點服務管理標籤

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。
4. 選擇 Actions (動作)、Manage tags (管理標籤)。
5. 針對每個要新增的標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
6. 若要移除標籤，請選擇標籤金鑰和值右側的 Remove (移除)。
7. 選擇儲存。

### 使用主控台為您的端點連線管理標籤

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，然後選擇 Endpoint connections (端點連線) 索引標籤。
4. 選取端點連線，然後選擇 Actions (動作)、Manage tags (管理標籤)。
5. 針對每個要新增的標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
6. 若要移除標籤，請選擇標籤金鑰和值右側的 Remove (移除)。
7. 選擇儲存。

### 使用主控台為您的端點服務許可管理標籤

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，然後選擇 Allow principals (允許主體) 索引標籤。

4. 選取主體，然後選擇 Actions (動作)、Manage tags (管理標籤)。
5. 針對每個要新增的標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
6. 若要移除標籤，請選擇標籤金鑰和值右側的 Remove (移除)。
7. 選擇儲存。

若要使用命令列新增和移除標籤

- [create-tags](#) 和 [delete-tags](#) (AWS CLI)
- [New-EC2Tag](#)和 [Remove-EC2Tag](#)(視窗工具 PowerShell)

## 管理 VPC 端點服務的 DNS 名稱

服務提供者可以為其端點服務設定私有 DNS 名稱。當服務提供者使用現有的公有 DNS 名稱作為其端點服務的私有 DNS 名稱時，服務消費者不需要變更使用現有公有 DNS 名稱的任何應用程式。在為您的端點服務設定私有 DNS 名稱之前，您必須執行網域所有權驗證檢查，以證明您擁有該網域。

### 考量事項

- 端點服務只能擁有一個私有 DNS 名稱。
- 您不得為私有 DNS 名稱建立 A 記錄，以便只有服務消費者 VPC 中的伺服器才能解析私有 DNS 名稱。
- Gateway Load Balancer 端點不支援私有 DNS 名稱。
- 為了驗證網域，您必須擁有公有主機名稱或公有 DNS 提供者。
- 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。每個 DNS 標籤最多可包含 63 個字元，而且整個網域名稱不得超過 255 個字元的總長度。

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，服務消費者才能使用該名稱。

## 網域所有權驗證

您的網域與一組網域名稱服務 (DNS) 記錄相關，而您透過 DNS 提供者來管理這些記錄。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。由名稱和值組成。在驗證過程中，您必須將 TXT 記錄新增至公有網域的 DNS 伺服器。



當我們在網域的 DNS 設定中偵測到存在 TXT 記錄時，網域所有權驗證便已完成。

新增記錄後，您可以使用 Amazon VPC 主控台檢查網域驗證程序的狀態。在導覽窗格中，選擇 Endpoints Services (端點服務)。選取端點服務，並檢查 Details (詳細資訊) 標籤中 Domain verification status (網域驗證狀態) 的值。如果網域驗證處於擱置狀態，請等待幾分鐘並重新整理畫面。如果需要，您可以手動啟動驗證程序。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)。

當驗證狀態為 verified (已驗證) 時，私有 DNS 名稱即可供服務消費者使用。如果驗證狀態變更，新的連線請求會遭到拒絕，但現有的連線不受影響。

如果驗證狀態為 failed (失敗)，請參閱 [the section called “對網域驗證問題進行疑難排解”](#)。

## 獲取名稱和值

我們會提供您在 TXT 記錄中使用的名稱和值。例如，資訊在 AWS Management Console 中可用。選取端點服務，然後參閱端點服務 Details (詳細資訊) 標籤中的 Domain verification name (網域驗證名稱) 和 Domain verification value (網域驗證值)。您也可以使用下列[描述-vpc-端點服務組態 AWS CLI 命令](#)，擷取有關指定端點服務之私人 DNS 名稱組態的資訊。

```
aws ec2 describe-vpc-endpoint-service-configurations \
  --service-ids vpce-svc-071afff70666e61e0 \
  --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

下列為範例輸出。您將在建立 TXT 記錄時將使用 Value 和 Name。

```
[
  {
    "State": "pendingVerification",
    "Type": "TXT",
    "Value": "vpce:l6p0ERx1Tt45jevFw0Cp",
    "Name": "_6e86v84tqgqubxbwii1m"
  }
]
```

例如，假設您的網域名稱為 example.com，而 Value 和 Name 如前面的範例輸出所示。下表是 TXT 記錄設定範例。



名稱	Type	Value
_6e86v84tggqubxbwii1m.example.com	TXT	VPCE: L6P0E 45 RxITt 日元

我們建議您使用 Name 作為記錄子網域，因為基礎網域名稱可能已在使用中。不過，如果您的 DNS 提供者不允許 DNS 記錄名稱包含底線，您可以省略 "\_6e86v84tggqubxbwii1m"，而在 TXT 記錄中僅使用 "example.com"。

在我們驗證 "\_6e86v84tggqubxbwii1m.example.com" 之後，服務消費者可以使用 "example.com" 或子網域 (例如，"service.example.com" 或 "my.service.example.com")。

## 新增 TXT 記錄到您網域的 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 供應商可能是 Amazon Route 53 或另一個網域名稱註冊商。

### Amazon Route 53

為您的公有託管區域建立記錄。使用下列的值：

- 對於 Type (類型)，選擇 TXT。
- 針對 TTL (Seconds) (TTL (秒))，輸入 **1800**。
- 對於 Routing policy (路由政策)，請選擇 Simple routing (簡便路由)。
- 針對 Record name (記錄名稱)，請輸入網域或子網域。
- 針對 Value/Route traffic to (值/將流量路由到)，請輸入網域驗證值。

如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[使用主控台建立記錄](#)。

### 一般程序

前往您的 DNS 提供者的網站並登入您的帳戶。查找頁面以更新網域的 DNS 記錄。以我們提供的名稱和值來新增 TXT 紀錄。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。

如需更具體的指示，請參閱 DNS 提供者的文件。下表提供幾個常見 DNS 提供者的文件連結。此清單並不全面，也不是對這些公司提供的產品或服務的建議。

DNS/託管供應商	文件連結
GoDaddy	<a href="#">新增 TXT 記錄</a>
Dreamhost	<a href="#">新增自訂 DNS 記錄</a>
Cloudflare	<a href="#">管理 DNS 記錄</a>
HostGator	<a href="#">使用 HostGator /ENOM 管理 DNS 記錄</a>
Namecheap	<a href="#">如何為我的網域新增 TXT/SPF/DKIM/DMARC 記錄？</a>
Names.co.uk	<a href="#">變更您網域的 DNS 設定</a>
Wix	<a href="#">在您的 Wix 帳戶中新增或更新 TXT 記錄</a>

## 檢查 TXT 記錄是否已發佈

您可以使用以下步驟，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。您將運行該 `nslookup` 命令，該命令可用於視窗和 Linux。

您將查詢為您的網域提供服務的 DNS 伺服器，因為這些伺服器包含您網域的最多 up-to-date 資訊。網域資訊傳播到其他 DNS 伺服器可能需要一些時間。

若要確認您的 TXT 記錄已發佈到您的 DNS 伺服器

1. 使用以下命令來查找網域的名稱伺服器。

```
nslookup -type=NS example.com
```

輸出會列出提供您網域的名稱伺服器。您在下一步驟將查詢其中一個伺服器。

2. 使用以下命令，確認 TXT 記錄已正確發佈，其中 *name\_server* 是您在上一個步驟中找到的名稱伺服器之一。

```
nslookup -type=TXT _6e86v84tqqqubxbwii1m.example.com name_server
```

3. 在上一步輸出中，確認 `text` = 後面的字串與 TXT 值相符。

在我們的範例中，如果記錄已正確發佈，輸出會包括以下內容。

```
_6e86v84tqqqubxbwii1m.example.com text = "vpce:l6p0ERx1Tt45jevFw0Cp"
```

## 對網域驗證問題進行疑難排解

如果網域驗證程序失敗，下列資訊有助於對問題進行疑難排解。

- 確認您的 DNS 提供者是否允許在 TXT 記錄名稱中使用底線。如果您的 DNS 提供者不允許使用底線，您可以省略 TXT 記錄中的網域驗證名稱 (例如，"\_6e86v84tqqqubxbwii1m")。
- 確認您的 DNS 提供者是否已將網域名稱附加到 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。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。這會告知您的 DNS 提供者，無需將網域名稱附加到 TXT 記錄。
- 確認您的 DNS 提供者是否已將 DNS 記錄值修改為僅使用小寫字母。只有當驗證記錄的屬性值與我們提供的值完全相符時，我們才會驗證您的網域。如果 DNS 提供者將 TXT 記錄值變更為只使用小寫字母，請聯絡他們以尋求協助。
- 您可能需要多次驗證您的網域，因為您支援多個區域或多個 AWS 帳戶。如果您的 DNS 提供者不允許您擁有多個含相同屬性名稱的 TXT 記錄，請確認您的 DNS 提供者是否允許您將多個屬性值指派給相同的 TXT 記錄。例如，如果您的 DNS 由 Amazon Route 53 受管，您可以使用下列程序。
  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. 針對 Value (值)，移至現有屬性值的結尾，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一次網域，並在另一次驗證中從屬性名稱中移除該值。不過，您只能驗證相同的網域兩次。

## 接收端點服務事件的提醒

您可以建立通知，接收與端點服務相關的特定事件的提醒。例如，當接受或拒絕連線請求時，您會收到電子郵件。

### 任務

- [建立 SNS 通知](#)
- [新增存取政策](#)
- [新增金鑰政策](#)

## 建立 SNS 通知

使用以下步驟即可為通知建立 Amazon SNS 主題，並訂閱該主題。

若要使用主控台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 Endpoints Services (端點服務)。
3. 選取端點服務。
4. 在 Notifications (通知) 索引標籤中，選擇 Create notification (建立通知)。
5. 對於 Notification ARN (通知 ARN)，請選擇您建立的 SNS 主題的 ARN。
6. 若要訂閱事件，請從 Events (事件) 中選取。
  - Connect (連接) - 服務消費者建立的介面端點。這會將連線請求傳送至服務提供者。
  - Accept (接受) - 服務提供者接受連線請求。
  - Reject (拒絕) - 服務提供者拒絕連線請求。
  - Delete (刪除) - 服務消費者刪除介面端點。
7. 選擇 Create notification (建立通知)。

若要使用命令列建立端點服務的通知

- [create-vpc-endpoint-connection-notification](#) (AWS CLI)
- [New-EC2VpcEndpointConnectionNotification](#)(視窗工具 PowerShell)

## 新增存取政策

將存取原則新增至 SNS 主題，AWS PrivateLink 以便代表您發佈通知，如下所示。如需詳細資訊，請參閱[如何編輯我的 Amazon SNS 主題的存取政策？](#) 使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件金鑰，以防止發生[混淆代理人](#)的情況。

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

```

    "Service": "vpce.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:region:account-id:topic-name",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:ec2:region:account-id:vpce-endpoint-service/service-
id"
    },
    "StringEquals": {
      "aws:SourceAccount": "account-id"
    }
  }
}
]
}

```

## 新增金鑰政策

如果您使用加密的 SNS 主題，則 KMS 金鑰的資源原則必須信任 AWS PrivateLink 才能呼叫 AWS KMS API 作業。金鑰政策範例如下。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:region:account-id:vpce-endpoint-service/service-
id"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}

```

```
    }  
  }  
]  
}
```

## 刪除端點服務

端點服務結束使用後即可刪除。如果有任何端點連接到處於 `available` 或者 `pending-acceptance` 狀態的端點服務，則無法刪除端點服務。

刪除端點服務不會刪除關聯的負載平衡器，也不會影響向負載平衡器目標群組註冊的應用程式伺服器。

若要使用主控台刪除端點服務

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Endpoints Services (端點服務)。
3. 選取端點服務。
4. 選擇 Actions (動作)、Delete endpoint services (刪除端點服務)。
5. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

若要使用命令列刪除端點服務

- [delete-vpc-endpoint-service-configurations](#) (AWS CLI)
- [Remove-EC2EndpointServiceConfiguration](#)(視窗工具 PowerShell)

# 的身分識別與存取管理 AWS PrivateLink

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 AWS PrivateLink 資源。您可以使用 IAM AWS 服務，無需額外付費。

## 目錄

- [物件](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [如何與 IAM AWS PrivateLink 搭配使用](#)
- [以身分識別為基礎的原則範例 AWS PrivateLink](#)
- [使用端點政策搭配 VPC 端點來控制存取權](#)

## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS PrivateLink。

**服務使用者** — 如果您使用 AWS PrivateLink 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS PrivateLink 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。

**服務管理員** — 如果您負責公司的 AWS PrivateLink 資源，您可能擁有完整的存取權 AWS PrivateLink。決定您的服務使用者應該存取哪些 AWS PrivateLink 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。

**IAM 管理員**：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS PrivateLink 存取權的詳細資訊。

## 使用身分驗證

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

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

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 [AWS 登入 使用者指南中的如何登入您 AWS 帳戶](#) 的。

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

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

## AWS 帳戶 根使用者

建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的 [需要根使用者憑證的任務](#)。

## 聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identity Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。AWS Directory Service 同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [什麼是 IAM Identity Center ?](#)。



## IAM 使用者和群組

[IAM 使用者](#)是您內部的身分，具 AWS 帳戶有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

## IAM 角色

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

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 [IAM 使用者指南](#) 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 [IAM 角色與資源類型政策的差異](#)。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。

- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的 [建立角色以委派許可給 AWS 服務](#)。
- 服務連結角色 — 服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的 [利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

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

## 使用政策管理存取權

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

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

## 身分型政策

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

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

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

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

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

## 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 實體許可範圍](#)。

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

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

## 如何與 IAM AWS PrivateLink 搭配使用

在您使用 IAM 管理存取權限之前 AWS PrivateLink，請先了解哪些 IAM 功能可搭配使用 AWS PrivateLink。

您可以搭配使用的 IAM 功能 AWS PrivateLink

IAM 功能	AWS PrivateLink 支持
<a href="#">身分型政策</a>	是
<a href="#">資源型政策</a>	是
<a href="#">政策動作</a>	是
<a href="#">政策資源</a>	是
<a href="#">政策條件索引鍵 (服務特定)</a>	是
<a href="#">ACL</a>	否
<a href="#">ABAC (政策中的標籤)</a>	是

IAM 功能	AWS PrivateLink 支持
<a href="#">臨時憑證</a>	是
<a href="#">主體許可</a>	是
<a href="#">服務角色</a>	否
<a href="#">服務連結角色</a>	否

若要深入瞭解如何以 AWS PrivateLink 及其他如何使 AWS 服務用大多數 IAM 功能，請參閱 IAM 使用者指南中的與 IAM 搭配使用的[AWS 服務](#)。

## 以身分識別為基礎的原則 AWS PrivateLink

支援身分型政策	是
---------	---

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 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](#)。

## 以身分識別為基礎的原則範例 AWS PrivateLink

若要檢視以 AWS PrivateLink 身分為基礎的原則範例，請參閱。[以身分識別為基礎的原則範例 AWS PrivateLink](#)

## 以資源為基礎的政策 AWS PrivateLink

支援以資源基礎的政策	是
------------	---

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

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，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 角色與資源型政策有何差異](#)。

AWS PrivateLink 服務支持一種類型的資源為基礎的策略，稱為端點策略。端點政策控制哪些 AWS 主體可以使用端點存取端點服務。如需詳細資訊，請參閱 [the section called “端點政策”](#)。

## 的政策動作 AWS PrivateLink

支援政策動作 是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

AWS PrivateLink 與 Amazon EC2 共享其 API 命名空間。中的策略動作在動作之前 AWS PrivateLink 使用下列前置詞：

```
ec2
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"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 AWS PrivateLink 動作清單，請參閱 Amazon EC2 API 參考中的 [AWS PrivateLink 動作](#)。如需詳細資訊，請參閱《服務授權參考》中 [Amazon EC2 定義的動作](#)。

## 的政策資源 AWS PrivateLink

支援政策資源 是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

## 的政策條件索引鍵 AWS PrivateLink

支援服務特定政策條件金鑰 是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

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

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

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

下列條件金鑰是特定於 AWS PrivateLink：

- ec2:VpceServiceName
- ec2:VpceServiceOwner
- ec2:VpceServicePrivateDnsName

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](#)。

## ACL 在 AWS PrivateLink

支援 ACL	否
--------	---

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

## 阿巴克與 AWS PrivateLink

支援 ABAC (政策中的標籤)	是
------------------	---

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws: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。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。



如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC?](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的[使用屬性型存取控制 \(ABAC\)](#)。

## 使用臨時登入資料 AWS PrivateLink

支援臨時憑證 是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料[搭配AWS 服務 使用](#)，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的[切換至角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

## 的跨服務主體權限 AWS PrivateLink

支援轉寄存取工作階段 (FAS) 是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。

## 的服務角色 AWS PrivateLink

支援服務角色 否

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的[建立角色以委派許可給 AWS 服務](#)。

## 服務連結角色 AWS PrivateLink

支援服務連結角色。 否

服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

## 以身分識別為基礎的原則範例 AWS PrivateLink

根據預設，使用者和角色不具備建立或修改 AWS PrivateLink 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策](#)。

有關由定義的動作和資源類型的詳細資訊 AWS PrivateLink，包括每種資源類型的 ARN 格式，請參閱服務授權參考中[適用於 Amazon EC2 的動作、資源和條件金鑰](#)。

### 範例

- [控制 VPC 端點的使用](#)
- [根據服務擁有者控制 VPC 端點建立](#)
- [控制可為 VPC 端點服務指定的私有 DNS 名稱](#)
- [控制可為 VPC 端點服務指定的服務名稱](#)

## 控制 VPC 端點的使用

根據預設，使用者沒有使用端點的許可。您可以建立身分型政策，將建立、修改、說明和刪除端點的權限授予使用者。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 “端點政策”](#)。

## 根據服務擁有者控制 VPC 端點建立

您可以根據誰擁有該服務 (amazon、aws-marketplace 或帳戶 ID)，使用 ec2:VpceServiceOwner 條件金鑰控制可建立的 VPC 端點。下列範例授會與使用指定的服務擁有者建立 VPC 端點的許可。若要使用此範例，請替換區域、帳戶 ID 和服務擁有者。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:region:account-id:vpc/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:route-table/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:region:account-id: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。下列範例會授與使用指定的私有 DNS 名稱建立 VPC 端點服務的許可。若要使用此範例，請替換區域、帳戶 ID 和私有 DNS 名稱。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource": [
        "arn:aws:ec2:region:account-id: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。下列範例會授與使用指定的服務名稱建立 VPC 端點的許可。若要使用此範例，請替換區域、帳戶 ID 和服務名稱。

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

```
    "Effect": "Allow",
    "Action": "ec2:CreateVpcEndpoint",
    "Resource": [
      "arn:aws:ec2:region:account-id:vpc/*",
      "arn:aws:ec2:region:account-id:security-group/*",
      "arn:aws:ec2:region:account-id:subnet/*",
      "arn:aws:ec2:region:account-id:route-table/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateVpcEndpoint",
    "Resource": [
      "arn:aws:ec2:region:account-id:vpc-endpoint/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:VpceServiceName": [
          "com.amazonaws.region.s3"
        ]
      }
    }
  }
]
```

## 使用端點政策搭配 VPC 端點來控制存取權

端點策略是一種以資源為基礎的策略，您可以將其連接到 VPC 端點，以控制哪些 AWS 主體可以使用該端點來存取 AWS 服務。

端點政策不會覆寫或取代身分型政策或資源型政策。例如，如果您使用界面端點連接至 Amazon S3，您也可使用 Amazon S3 儲存貯體政策來控制特定端點或特定 VPC 對儲存貯體的存取權。

### 目錄

- [考量事項](#)
- [預設端點政策](#)
- [介面端點政策](#)
- [閘道端點的主體](#)
- [更新 VPC 端點政策](#)

## 考量事項

- 端點政策是使用 IAM 政策語言的 JSON 政策文件。其必須包含 [Principal](#) 元素。端點政策的大小不可超過 20,480 個字元 (包含空格)。
- 當您建立的介面或閘道端點時 AWS 服務，可以將單一端點策略附加到端點。您可以隨時[更新端點政策](#)。如果您未連接端點政策，則我們會連接[預設端點政策](#)。
- 並非所有 AWS 服務 支援端點策略。如果 AWS 服務 不支援端點政策，我們會允許對服務的任何端點進行完整存取。如需詳細資訊，請參閱 [the section called “檢視端點政策支援”](#)。
- 當您為 AWS 服務以外的端點服務建立 VPC 端點時，我們會允許完整存取該端點。

## 預設端點政策

預設端點政策會授予端點的完整存取權。

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

## 介面端點政策

如需端點策略的範例 AWS 服務，請參閱[the section called “整合的服務”](#)。表格中的第一欄包含各自 AWS PrivateLink 文件的連結 AWS 服務。如果 AWS 服務 支援端點策略，則其說明文件會包含端點策略範例。

## 閘道端點的主體

使用閘道端點時，Principal元素必須設定為\*。若要指定主體，請使用aws:PrincipalArn條件索引鍵。

```
"Condition": {
  "StringEquals": {
```

```
    "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"  
  }  
}
```

如果您以下列格式指定主參與者，則只會將存取權授予帳戶的 AWS 帳戶根使用者 唯一使用者和角色，而非所有使用者和角色。

```
"AWS": "account_id"
```

如需閘道端點的端點政策範例，請參閱下列主題：

- [適用於 Amazon S3 的端點](#)
- [DynamoDB 的端點](#)

## 更新 VPC 端點政策

使用下列程序來更新 AWS 服務的端點政策。更新端點政策後，變生效需費時幾分鐘。

若要使用主控台更新端點政策

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)。
3. 選取 VPC 端點。
4. 選擇 Actions (動作)、Manage policy (管理政策)。
5. 選擇 Full Access (完整存取) 以允許完整存取服務，或選擇 Custom (自訂) 並連接自訂政策。
6. 選擇儲存。

若要使用命令列更新端點政策

- [modify-vpc-endpoint](#) (AWS CLI)
- [Edit-EC2VpcEndpoint](#)(視窗工具 PowerShell)

# AWS PrivateLink 的 CloudWatch 指標

AWS PrivateLink 將您的介面端點、Gateway Load Balancer 端點和端點服務的資料點發佈到 Amazon CloudWatch。CloudWatch 可讓使用一組時間序列資料的形式來擷取這些資料點的相關統計資料，也就是指標。您可以將指標視為要監控的變數，且資料點是該變數在不同時間點的值。每個資料點都有相關聯的時間戳記和可選的測量單位。

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

針對所有介面端點、Gateway Load Balancer 端點和端點服務發佈指標。不會為閘道端點發佈它們。預設情況下，AWS PrivateLink 每隔一分鐘向 CloudWatch 傳送指標，無需額外費用。

如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

## 內容

- [端點指標和維度](#)
- [端點服務指標和維度](#)
- [檢視 CloudWatch 指標](#)
- [使用內建的 Contributor Insights 規則](#)

## 端點指標和維度

AWS/PrivateLinkEndpoints 命名空間包含下列介面端點和 Gateway Load Balancer 端點的指標。

指標	描述
ActiveConnections	<p>作用中並行連線的數目。這包含處於 SYN_SENT 與 ESTABLISHED 狀態的連線。</p> <p>報告條件：端點在一分鐘內接收的流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Maximum 與 Minimum。</p> <p>維度</p> <ul style="list-style-type: none"><li>• Endpoint Type, Service Name, VPC Endpoint Id, VPC Id</li></ul>



指標	描述
BytesProcessed	<p>端點和端點服務之間交換的位元組數，在兩個方向上聚合。這是端點所有者需付費的位元組數。帳單會以 GB 為單位顯示此值。</p> <p>報告條件：端點在一分鐘內接收的流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum、Maximum 和 Minimum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Endpoint Type, Service Name, VPC Endpoint Id, VPC Id</li> <li>Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id</li> </ul>
NewConnections	<p>透過端點建立的新連線數量。</p> <p>報告條件：端點在一分鐘內接收的流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum、Maximum 和 Minimum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Endpoint Type, Service Name, VPC Endpoint Id, VPC Id</li> <li>Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id</li> </ul>

指標	描述
PacketsDropped	<p>端點捨棄的封包數量。此指標可能不會擷取所有封包捨棄。增加的值可能表示端點或端點服務運行狀況不佳。</p> <p>報告條件：端點在一分鐘內接收的流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Endpoint Type, Service Name, VPC Endpoint Id, VPC Id</li> <li>Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id</li> </ul>
RstPacketsReceived	<p>端點接收的 RST 封包數量。增加的值可能表示端點服務運行狀況不佳。</p> <p>報告條件：端點在一分鐘內接收的流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Endpoint Type, Service Name, VPC Endpoint Id, VPC Id</li> <li>Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id</li> </ul>

若要篩選這些指標，請使用下列維度。

維度	描述
Endpoint Type	依端點類型篩選指標資料 (Interface   GatewayLoadBalancer )。
Service Name	依服務名稱篩選指標資料。
Subnet Id	依子網路篩選指標資料。
VPC Endpoint Id	依 VPC 端點篩選指標資料。

維度	描述
VPC Id	依 VPC 篩選指標資料。

## 端點服務指標和維度

AWS/PrivateLinkServices 命名空間包含端點服務的下列指標。

指標	描述
ActiveConnections	<p>透過端點從用戶端到目標的作用中連線的最大數目。增加的值可能表示需要向負載均衡器新增目標。</p> <p>報告條件：連線到端點服務的端點在一分鐘內傳送流量。</p> <p>統計資訊：最實用的統計資訊是 Average 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>• Service Id</li> <li>• Az, Service Id</li> <li>• Load Balancer Arn, Service Id</li> <li>• Az, Load Balancer Arn, Service Id</li> <li>• Service Id, VPC Endpoint Id</li> </ul>
BytesProcessed	<p>在兩個方向上，端點服務和端點之間交換的位元組數。</p> <p>報告條件：連線到端點服務的端點在一分鐘內傳送流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>• Service Id</li> <li>• Az, Service Id</li> <li>• Load Balancer Arn, Service Id</li> <li>• Az, Load Balancer Arn, Service Id</li> </ul>

指標	描述
	<ul style="list-style-type: none"> <li>Service Id, VPC Endpoint Id</li> </ul>
EndpointsCount	<p>連線到端點服務的端點數。</p> <p>報告條件：五分鐘內有非零值。</p> <p>統計資訊：最實用的統計資訊是 Average 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Service Id</li> </ul>
NewConnections	<p>透過端點從用戶端到目標所建立的新連線數目。增加的值可能表示需要向負載均衡器新增目標。</p> <p>報告條件：連線到端點服務的端點在一分鐘內傳送流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>Service Id</li> <li>Az, Service Id</li> <li>Load Balancer Arn, Service Id</li> <li>Az, Load Balancer Arn, Service Id</li> <li>Service Id, VPC Endpoint Id</li> </ul>

指標	描述
RstPacketsSent	<p>端點服務傳送到端點的 RST 封包數量。增加的值可能表示存在狀況不佳的目標。</p> <p>報告條件：連線到端點服務的端點在一分鐘內傳送流量。</p> <p>統計資訊：最實用的統計資訊是 Average、Sum 與 Maximum。</p> <p>維度</p> <ul style="list-style-type: none"> <li>• Service Id</li> <li>• Az, Service Id</li> <li>• Load Balancer Arn, Service Id</li> <li>• Az, Load Balancer Arn, Service Id</li> <li>• Service Id, VPC Endpoint Id</li> </ul>

若要篩選這些指標，請使用下列維度。

維度	描述
Az	依可用區域篩選指標資料。
Load Balancer Arn	依負載平衡器篩選指標資料。
Service Id	依端點服務篩選指標資料。
VPC Endpoint Id	依 VPC 端點篩選指標資料。

## 檢視 CloudWatch 指標

您可以使用 Amazon VPC 主控台、CloudWatch 主控台或 AWS CLI 來檢視這些 CloudWatch 指標，如下所示。

## 若要使用 Amazon VPC 主控台檢視指標

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 Endpoints (端點)。選取您的端點，然後選擇 Monitoring (監控) 標籤。
3. 在導覽窗格中，選擇 Endpoints Services (端點服務)。選取您的端點服務，然後選擇 Monitoring (監控) 標籤。

## 使用 CloudWatch 主控台檢視指標

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Metrics (指標)。
3. 選取 AWS/PrivateLinkEndpoints 命名空間。
4. 選取 AWS/PrivateLinkServices 命名空間。

## 若要使用 AWS CLI 來檢視指標

使用下列 [list-metrics](#) 命令列出介面端點和 Gateway Load Balancer 端點的可用指標：

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

使用下列 [list-metrics](#) 命令列出端點服務的可用指標：

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

## 使用內建的 Contributor Insights 規則

AWS PrivateLink 為您的端點服務提供內建的 Contributor Insights 規則，以幫助您找到哪些端點是每個受支援指標的最大貢獻者。如需更多資訊，請參閱《Amazon CloudWatch 使用者指南》中的 [Contributor Insights](#)。

AWS PrivateLink 提供下列規則：

- VpcEndpointService-ActiveConnectionsByEndpointId-v1 – 按照作用中連線數目對端點分類。
- VpcEndpointService-BytesByEndpointId-v1 – 按照已處理的位元組數對端點分類。
- VpcEndpointService-NewConnectionsByEndpointId-v1 – 按照新連線數對端點分類。

- VpcEndpointService-RstPacketsByEndpointId-v1 – 按照傳送到端點的 RST 封包數量對端點分類。

您必須先啟用內建規則才能加以使用。啟用規則後，規則會開始收集參與者資料。如需 Contributor Insights 費用的資訊，請參閱 [Amazon CloudWatch 定價](#)。

您必須擁有下列許可才能使用 Contributor Insights：

- cloudwatch:DeleteInsightRules – 刪除 Contributor Insights 規則。
- cloudwatch:DisableInsightRules – 停用 Contributor Insights 規則。
- cloudwatch:GetInsightRuleReport – 取得資料。
- cloudwatch:ListManagedInsightRules – 列出可用的 Contributor Insights 規則。
- cloudwatch:PutManagedInsightRules – 啟用 Contributor Insights 規則。

## 任務

- [啟用 Contributor Insights 規則](#)
- [停用 Contributor Insights 規則](#)
- [刪除 Contributor Insights 規則](#)

## 啟用 Contributor Insights 規則

透過 AWS Management Console 或 AWS CLI，為 AWS PrivateLink 使用下列程序來啟用內建規則。

使用主控台為 AWS PrivateLink 啟用 Contributor Insights 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 Endpoints Services (端點服務)。
3. 選取您的端點服務。
4. 在 Contributor Insights 索引標籤上，選擇 Enable (啟用)。
5. (選用) 根據預設，所有規則都已啟用。若要僅啟用特定規則，請選取不應啟用的規則，然後選擇 Actions (動作)、Disable rule (停用規則)。出現確認提示時，請選擇 Disable (停用)。

## 使用 AWS CLI 為 AWS PrivateLink 啟用 Contributor Insights 規則

1. 使用如下列的 [list-managed-insight-rules](#) 命令可列舉可用的規則。對於 `--resource-arn` 選項，指定端點服務的 ARN。

```
aws cloudwatch list-managed-insight-rules --resource-arn
arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. 在 `list-managed-insight-rules` 命令的輸出中，從 `TemplateName` 欄位複製範本的名稱。以下為此欄位的範例。

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. 使用如下列的 [put-managed-insight-rules](#) 命令可啟用規則。您必須指定端點服務的範本名稱和 ARN。

```
aws cloudwatch put-managed-insight-rules --managed-rules
TemplateName=VpcEndpointService-NewConnectionsByEndpointId-v1,
ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

## 停用 Contributor Insights 規則

您可以隨時為 AWS PrivateLink 停用內建規則。停用規則後，它會停止收集參與者資料，但現有的參與者資料會保留 15 天。停用規則後，您可以將它再次啟用，以繼續收集參與者資料。

### 使用主控台為 AWS PrivateLink 停用 Contributor Insights 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 Endpoints Services (端點服務)。
3. 選取您的端點服務。
4. 在 Contributor Insights 索引標籤上，選擇 Disable all (全部停用)可停用所有規則。或者，也可以展開 Rules (規則) 面板，選取要停用的規則，然後選擇 Actions (動作)、Disable rule (停用規則)
5. 出現確認提示時，請選擇 Disable (停用)。

### 使用 AWS CLI 為 AWS PrivateLink 停用 Contributor Insights 規則

使用 [disable-insight-rules](#) 命令可停用規則。



## 刪除 Contributor Insights 規則

透過 AWS Management Console 或 AWS CLI，為 AWS PrivateLink 使用下列程序來刪除內建規則。刪除規則後，規則將停止收集參與者資料，我們則會刪除現有的參與者資料。

使用主控台為 AWS PrivateLink 刪除 Contributor Insights 規則

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Insights (洞察)，然後選擇 Contributor Insights。
3. 展開 Rules (規則) 面板，然後選取規則。
4. 依序選擇 Actions (動作)、Delete rules (刪除規則)。
5. 出現確認提示時，請選擇 Delete (刪除)。

使用 AWS CLI 為 AWS PrivateLink 刪除 Contributor Insights 規則

使用 [delete-insight-rules](#) 命令可刪除規則。

## AWS PrivateLink 配額

下表列出您帳戶每個區域的 AWS PrivateLink 資源配額 (先前稱為限額)。除非另做說明，否則您可以請求提高這些配額。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的[請求提高配額](#)。

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。

名稱	預設	可調整	說明
每個 VPC 的介面和 Gateway Load Balancer 端點	50	<a href="#">是</a>	這是介面端點和 Gateway Load Balancer 端點的合併配額
每個區域的閘道 VPC 端點	20	<a href="#">是</a>	每個 VPC 最多可以建立 255 個閘道端點
每個 VPC 端點政策的字元	20,480	否	VPC 端點政策的大小上限，包含空格

下列考量適用於通過 VPC 端點的流量。

- 根據預設，每個 VPC 端點可支援每個可用區域高達 10 Gbps 的頻寬，且可自動擴展至高達 100 Gbps。將負載分配到所有可用區域時，VPC 端點的最大頻寬為可用區域數目乘以 100 Gbps。如果您的應用程式需要更高的輸送量，請連絡 AWS 支援。
- 網路連線的最大傳輸單位 (MTU) 是允許通過 VPC 端點的最大封包大小 (以位元組為單位)。MTU 越大，單一封包能傳遞的資料也越多。VPC 端點支援 8500 位元組的 MTU。大小大於 8500 位元組且到達 VPC 端點的封包會被丟棄。
- 不支援路徑 MTU 探索 (PMTUD)。VPC 端點不會產生下列 ICMP 訊息：Destination Unreachable: Fragmentation needed and Don't Fragment was Set (類型 3，代碼 4)。
- VPC 端點會強制執行所有封包的最大區段大小 (MSS) 限制。如需詳細資訊，請參閱 [RFC879](#)。

## 的文件歷史記錄 AWS PrivateLink

下表說明的版本 AWS PrivateLink。

變更	描述	日期
<a href="#">指定的 IP 地址</a>	您可以在建立或修改 VPC 端點時指定端點網路介面的 IP 地址。	2023 年 8 月 17 日
<a href="#">IPv6 支援</a>	您可以設定 Gateway Load Balancer 端點服務和 Gateway Load Balancer 端點，以同時支援 IPv4 和 IPv6 位址，或僅支援 IPv6 位址。	2022 年 12 月 12 日
<a href="#">Contributor Insights</a>	您可以使用內建的「參與者見解」規則來識別特定端點，這些端點是 CloudWatch 指標的主要貢獻者。AWS PrivateLink	2022 年 8 月 18 日
<a href="#">IPv6 支援</a>	服務提供者可以讓其端點服務接受 IPv6 請求，即使其後端服務僅支援 IPv4。如果端點服務接受 IPv6 請求，服務消費者可以為其介面端點啟用 IPv6 支援，以便他們可以透過 IPv6 存取端點服務。	2022 年 5 月 11 日
<a href="#">CloudWatch 度量</a>	AWS PrivateLink 發佈介面端點、閘道 Load Balancer 端點和端點服務的 CloudWatch 指標。	2022 年 1 月 27 日
<a href="#">Gateway Load Balancer 端點</a>	您可以在 VPC 中建立閘道負載平衡器端點，以將流量路由至	2020 年 11 月 10 日

	您使用閘道負載平衡器設定的 VPC 端點服務。	
<a href="#">VPC 端點政策</a>	您可以將 IAM 政策連接到 AWS 服務的介面 VPC 端點，以控制服務存取權。	2020 年 3 月 23 日
<a href="#">VPC 端點和端點服務的條件金鑰</a>	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。	2020 年 3 月 6 日
<a href="#">建立 VPC 端點或端點服務時新增標籤</a>	您可以在建立 VPC 端點和端點服務時新增標籤。	2020 年 2 月 5 日
<a href="#">私有 DNS 名稱</a>	您可以使用私人 DNS 名稱從 VPC 中存取 AWS PrivateLink 基於服務。	2020 年 1 月 6 日
<a href="#">VPC 端點服務</a>	您可以建立自有的端點服務，讓其他 AWS 帳戶 和使用者透過介面 VPC 端點連線到您的服務。您可以提供您的端點服務，以便在 AWS Marketplace 中訂閱。	2017 年 11 月 28 日
<a href="#">下列項目的介面 VPC 端點 AWS 服務</a>	您可以建立介面端點來連線到 AWS 服務 該整合，AWS PrivateLink 而無需使用網際網路閘道或 NAT 裝置。	2017 年 11 月 8 日
<a href="#">DynamoDB 的 VPC 端點</a>	您可以建立閘道 VPC 端點，以便從您的 VPC 存取 Amazon DynamoDB，而無需使用網際網路閘道或 NAT 設備。	2017 年 8 月 16 日
<a href="#">Amazon S3 的 VPC 端點</a>	您可以建立閘道 VPC 端點，以便從您的 VPC 存取 Amazon S3，而無需使用網際網路閘道或 NAT 設備。	2015 年 5 月 11 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。