



管理員指南

# AWS Client VPN



# AWS Client VPN: 管理員指南

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

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

# Table of Contents

什麼是 AWS Client VPN? .....	1
Client VPN 的功能 .....	1
Client VPN 的元件 .....	1
使用 Client VPN .....	3
Client VPN 的定價 .....	3
規則和最佳做法 .....	4
Client VPN 的運作方式 .....	6
用戶端身分驗證 .....	7
Active Directory 身分驗證 .....	7
交互身分驗證 .....	8
單一登入 (SAML 2.0 型聯合身分驗證) .....	13
客戶端授權 .....	17
安全群組 .....	17
以網路為基礎的授權 .....	18
連線授權 .....	18
需求和考量事項 .....	19
Lambda 界面 .....	19
使用用戶端連線處理常式評估狀態 .....	21
啟用用戶端連線處理常式 .....	22
服務連結角色 .....	22
監視連線授權失敗 .....	22
分割通道 Client VPN .....	22
分割隧道的優點 .....	23
路由傳送考量 .....	23
啟用分割隧道 .....	23
連線日誌記錄 .....	24
連線日誌項目 .....	24
擴展考量 .....	26
案例和範例 .....	28
存取 VPC .....	28
存取對等 VPC .....	29
存取內部部署網路 .....	30
存取網際網路 .....	32
Client-to-client 訪問權限 .....	33

限制存取您的網路 .....	35
使用安全群組限制存取 .....	35
根據使用者群組限制存取 .....	36
入門教學課程 .....	38
必要條件 .....	39
步驟 1：產生伺服器和用戶端憑證及金鑰 .....	39
步驟 2：建立 Client VPN 端點 .....	39
步驟 3：建立目標網路關聯 .....	40
步驟 4：新增 VPC 的授權規則 .....	41
步驟 5：提供對網際網路的存取權限 .....	42
步驟 6：驗證安全群組要求 .....	42
步驟 7：下載 Client VPN 端點組態檔案 .....	43
步驟 8：連線到 Client VPN 端點 .....	44
使用 Client VPN .....	45
存取自助式入口網站 .....	45
授權規則 .....	46
將授權規則新增至 Client VPN 端點 .....	46
從 Client VPN 端點移除授權規則 .....	47
檢視授權規則 .....	48
範例方案 .....	48
用戶端憑證撤銷清單 .....	57
產生用戶端憑證撤銷清單 .....	58
匯入用戶端憑證撤銷清單 .....	60
匯出用戶端憑證撤銷清單 .....	60
用戶端連線 .....	61
查看用戶端連線 .....	61
終止用戶端連線 .....	61
用戶端登入橫幅 .....	62
設定建立 Client VPN 端點期間的用戶端登入橫幅 .....	62
設定現有 Client VPN 端點的用戶端登入橫幅 .....	62
停用現有 Client VPN 端點的用戶端登入橫幅 .....	63
修改 Client VPN 端點上的現有橫幅文字 .....	63
檢視當前設定的登入橫幅 .....	64
Client VPN 端點 .....	64
建立 Client VPN 端點。 .....	65
修改 Client VPN 端點 .....	68

檢視Client VPN 端點 .....	70
建立 Client VPN 端點 .....	71
連線日誌 .....	71
啟用新 Client VPN 端點的連線日誌記錄 .....	72
啟用現有 Client VPN 端點的連線日誌記錄 .....	73
檢視連線日誌 .....	73
關閉連線日誌記錄 .....	74
匯出和設定用戶端組態檔 .....	74
匯出用戶端組態檔 .....	75
新增用戶端憑證和金鑰資訊 (交互身分驗證) .....	75
路由 .....	77
Client VPN 端點上的分割通道考量 .....	77
建立端點路由 .....	77
檢視端點路由 .....	78
刪除端點路由 .....	79
目標網路 .....	79
建立目標網路與 Client VPN 端點的關聯 .....	79
將安全群組套用到目標網路 .....	81
取消目標網路與 Client VPN 端點的關聯 .....	81
檢視目標網路 .....	82
VPN 工作階段最長持續時間 .....	82
設定 Client VPN 端點建立期間的 VPN 工作階段上限 .....	83
檢視目前 VPN 工作階段持續時間上限 .....	83
修改 VPN 工作階段持續時間上限 .....	83
安全性 .....	85
資料保護 .....	85
傳輸中加密 .....	86
網際網路流量隱私權 .....	86
身分與存取管理 .....	87
物件 .....	87
使用身分驗證 .....	88
使用政策管理存取權 .....	90
AWS Client VPN 如何與 IAM 搭配使用 .....	92
身分型政策範例 .....	98
故障診斷 .....	100
使用服務連結角色 .....	102

彈性 .....	106
提供高可用性的多個目標網路 .....	106
基礎設施安全性 .....	106
最佳實務 .....	106
IPv6 考量因素 .....	107
監控 Client VPN .....	109
CloudWatch 指標 .....	109
檢視 CloudWatch 指標 .....	111
CloudTrail 日誌 .....	112
CloudTrail 中的 Client VPN 資訊 .....	112
了解 Client VPN 日誌檔案項目 .....	113
配額 .....	114
Client VPN 配額 .....	114
使用者和群組配額 .....	115
一般考量 .....	115
故障診斷 .....	116
無法解析 Client VPN 端點 DNS 名稱 .....	116
流量不會在子網路之間分割 .....	117
Active Directory 群組的授權規則未如預期般運作 .....	118
用戶端無法存取對等 VPC、Amazon S3 或網際網路 .....	119
對等 VPC、Amazon S3 或網際網路的存取斷斷續續 .....	122
用戶端軟體傳回 TLS 錯誤 .....	122
用戶端軟體傳回使用者名稱和密碼錯誤 (Active Directory 身分驗證) .....	123
用戶端軟體傳回使用者名稱和密碼錯誤 (聯合驗證) .....	124
用戶端無法連線 (交互身分驗證) .....	124
用戶端傳回的登入資料超過大小上限錯誤 (聯合身分驗證) .....	124
用戶端無法開啟瀏覽器 (聯合身分驗證) .....	125
用戶端傳回沒有可用的連接埠錯誤 (聯合身分驗證) .....	125
VPN 連接由於 IP 不匹配而終止 .....	126
將流量路由到 LAN 無法如預期般運作 .....	126
確認 Client VPN 端點的頻寬限制 .....	126
文件歷史紀錄 .....	128
.....	CXXX

# 什麼是 AWS Client VPN ？

AWS Client VPN 是受管用戶端型 VPN 服務，可讓您安全地存取內部部署網路中的資 AWS 源和資源。透過 Client VPN，您可以從任何地方使用以 OpenVPN 為基礎的 VPN 用戶端存取您的資源。

## 內容

- [Client VPN 的功能](#)
- [Client VPN 的元件](#)
- [使用 Client VPN](#)
- [Client VPN 的定價](#)
- [規則和最佳做法 AWS Client VPN](#)

## Client VPN 的功能

Client VPN 提供以下特色和功能：

- 安全連線 – 支援從任何地方使用 OpenVPN 用戶端建立安全的 TLS 連線。
- 託管服務 — 這是一項 AWS 託管服務，因此可消除部署和管理第三方遠端存取 VPN 解決方案的操作負擔。
- 高可用性和彈性 — 它會自動擴展到連接到您的 AWS 資源和內部部署資源的用戶數量。
- 身分驗證 – 支援使用 Active Directory、聯合身分驗證和以憑證為基礎的身分驗證進行用戶端身分驗證。
- 精細控制 – 可讓您定義以網路為基礎的存取規則，以實作自訂安全控制。這些規則的設定可達到 Active Directory 群組的精細度。您也可以使用安全群組來實作存取控制。
- 易於使用 — 它可讓您使用單一 VPN 通道存取資 AWS 源和內部部署資源。
- 可管理性 – 可讓您查看連線日誌，其中提供用戶端連線嘗試的詳細資訊。您也可以管理作用中用戶端連線，允許您終止作用中用戶端連線。
- 深度整合 — 它與包括 AWS Directory Service Amazon VPC 在內的現有 AWS 服務整合。

## Client VPN 的元件

以下是 Client VPN 的重要概念：

## 用戶端 VPN 端點

Client VPN 端點是您為了啟用和管理 Client VPN 工作階段而建立及設定的資源。它是所有用戶端 VPN 工作階段的終止點。

### 目標網路

目標網路是與 Client VPN 端點相關聯的網路。始於 VPC 的子網路是目標網路。將子網路與 Client VPN 端點建立關聯可讓您建立 VPN 工作階段。您可以將多個子網路與 Client VPN 端點建立關聯，以獲得高可用性。所有子網路必須來自相同的 VPC。每個子網路必須屬於不同的可用區域。

### 路由

每個用戶端 VPN 端點都有路由表來描述可用的目標網路路由。路由表中的每個路由指定流量流向特定資源或網路的路徑。

### 授權規則

授權規則限制可存取網路的使用者。針對指定的網路，您可以設定允許存取的 Active Directory 或身分提供者 (IdP) 群組。只有屬於此群組的使用者才能存取指定的網路。在預設情況下沒有授權規則，您必須設定授權規則讓使用者存取資源和網路。

### 用戶端

連線到 Client VPN 端點以建立 VPN 工作階段的最終使用者。最終使用者需要下載 OpenVPN 用戶端，並使用您建立的用戶端 VPN 組態檔案來建立 VPN 工作階段。

### 用戶端 CIDR 範圍

要指派用戶端 IP 地址的來源 IP 地址範圍。每個與 Client VPN 端點的連線都會從用戶端 CIDR 範圍指派唯一的 IP 地址。您可以選擇用戶端 CIDR 範圍，例如 10.2.0.0/16。

### 用戶端 VPN 連接埠

AWS Client VPN 支援連接埠 443 和 1194，適用於 TCP 和 UDP。預設值為連接埠 443。

### Client VPN 網路界面

當您將子網路與 Client VPN 端點建立關聯時，我們會在該子網路中建立 Client VPN 網路界面。從 Client VPN 端點傳送至 VPC 的流量是透過 Client VPN 網路界面傳送。接著會套用來源網路位址轉譯 (SNAT)，其中來源 IP 地址會從用戶端 CIDR 範圍轉譯成 Client VPN 網路界面 IP 地址。

### 連線日誌記錄

您可以啟用 Client VPN 端點的連線日誌，以記錄連線事件。您可以使用此資訊來執行鑑識、分析 Client VPN 端點的使用方式，或偵錯連線問題。



## 自助式入口網站

Client VPN 提供自助式入口網站做為網頁，讓最終使用者能夠下載 AWS VPN 桌面用戶端的最新版本，以及 Client VPN 端點組態檔案的最新版本，其中包含連線至端點所需的設定。Client VPN 端點管理員可以啟用或停用 Client VPN 端點的自助式入口網站。自助入口網站是以下區域的服務堆疊支援的全球服務：美國東部 (維吉尼亞北部)、亞太區域 (東京)、歐洲 (愛爾蘭) 及 AWS GovCloud (美國西部)。

## 使用 Client VPN

您可以透過以下任何方式來使用 Client VPN：

### AWS Management Console

主控台為 Client VPN 提供 Web 型使用者界面。如果您已註冊 AWS 帳戶，則可以登入 [Amazon VPC 主控台](#)，然後在導覽窗格中選取 Client VPN。

### AWS Command Line Interface (AWS CLI)

提 AWS CLI 供對 Client VPN 公用 API 的直接存取。Windows、macOS 和 Linux 都提供支援。若要取得有關入門的更多資訊 AWS CLI，請參閱 [《AWS Command Line Interface 使用者指南》](#)。如需 Client VPN 命令的詳細資訊，請參閱 [《AWS CLI 命令參考》](#)。

### AWS Tools for Windows PowerShell

AWS 為在PowerShell 環境中編寫指令碼的使用者提供廣泛的 AWS 產品組合的命令。如需 AWS Tools for Windows PowerShell入門的詳細資訊，請參閱 [AWS Tools for Windows PowerShell 使用者指南](#)。如需 Client VPN 專用 Cmdlet 的詳細資訊，請參閱 [AWS Tools for Windows PowerShell Cmdlet 參考](#)。

### 查詢 API

Client VPN HTTPS 查詢 API 可讓您以程式設計方式存取 Client VPN 和 AWS。HTTPS 查詢 API 可讓您直接向該服務發出 HTTPS 請求。當您使用 HTTPS API 時，必須包含使用您的登入資料來數位簽署請求的程式碼。如需詳細資訊，請參閱 [AWS Client VPN 動作](#)。

## Client VPN 的定價

系統會針對每個端點關聯和每個 VPN 連接來向您收取費用 (以小時為計費單位)。如需詳細資訊，請參閱 [AWS Client VPN 定價](#)。

系統會針對從 Amazon EC2 傳輸資料至網際網路來向您收取費用。如需詳細資訊，請參閱「Amazon EC2 隨需定價」頁面上的[資料傳輸](#)

如果您為 Client VPN 端點啟用連線記錄，則必須在帳戶中建立記錄 CloudWatch 檔記錄群組。使用日誌群組需支付費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#) (在「付費方案」下，選擇「日誌」)。

如果您為 Client VPN 端點啟用用戶端連線處理器，就必須建立並呼叫 Lambda 函數。呼叫 Lambda 函數需支付費用。如需詳細資訊，請參閱 [AWS Lambda 定價](#)。

Client VPN 端點與目標網路 (VPC 中的子網路) 相關聯。如果此 VPC 具有網 Internet Gateway，我們會將彈性 IP 位址與用戶端 VPN 的彈性網路介面 (ENI) 建立關聯。這些彈性 IP 位址會以使用中的公用 IPv4 位址計費。如需詳細資訊，請參閱 [VPC 定價](#) 頁面上的公用 IPv4 位址索引標籤。

## 規則和最佳做法 AWS Client VPN

以下是規則和最佳實踐 AWS Client VPN

- 每個使用者連線支援最低 10 Mbps 的頻寬。每個使用者連線的最大頻寬取決於要與 Client VPN 端點建立的連線數目。
- 用戶端 CIDR 範圍與相關聯子網路所在的 VPC 的本機 CIDR 不可重疊，或與手動新增到 Client VPN 端點路由表的任何路由不可重疊。
- 用戶端 CIDR 範圍必須有至少為 /22 且不可大於 /12 的區塊大小。
- 用戶端 CIDR 範圍中的一部分位址用於支援 Client VPN 端點的可用性模型，而且無法指派給用戶端。因此，建議您指派 CIDR 區塊，其中包含您計劃在 Client VPN 端點上支援同時連線數目上限所需 IP 地址數目兩倍的 IP 地址數目。
- 建立 Client VPN 端點之後，就無法變用戶端 CIDR 範圍。
- 與 Client VPN 端點相關聯的子網路必須位於同一個 VPC 中。
- 您不能將來自相同可用區域的多個子網路與一個 Client VPN 端點建立關聯。
- Client VPN 端點不支援專用租用 VPC 中的子網路關聯。
- Client VPN 僅支援 IPv4 流量。請參閱 [AWS Client VPN 的 IPv6 考量因素](#) 以取得有關 IPv6 的詳細資訊。
- Client VPN 不符合聯邦資訊處理標準 (FIPS)。
- 使用交互身分驗證進行身分驗證的用戶端無法使用自助式入口網站。

- 我們不建議使用 IP 位址連線到 Client VPN 端點。由於 Client VPN 是受管服務，因此您偶爾會看到 DNS 名稱解析出的 IP 地址發生變更。此外，您會在 CloudTrail 記錄檔中看到 Client VPN 網路介面已刪除並重新建立。建議使用提供的 DNS 名稱來連線到 Client VPN 端點。
- 使用 AWS Client VPN 桌面應用程式時，目前不支援 IP 轉送。其他用戶端支援 IP 轉送。
- Client VPN 不支援在 AWS Managed Microsoft AD 中使用多區域複寫功能。Client VPN 端點必須與 AWS Managed Microsoft AD 資源位於相同的區域。
- 如果您的 Active Directory 停用多重要素驗證 (MFA)，則使用者密碼不能使用下列格式。

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- 如果有多個使用者已登入作業系統，則無法從電腦建立 VPN 連線。
- Client VPN 服務要求用戶端連線的 IP 位址與 Client VPN 端點的 DNS 名稱解析為的 IP 相符。換句話說，如果您為 Client VPN 端點設定自訂 DNS 記錄，然後將流量轉送到端點 DNS 名稱解析為的實際 IP 位址，則此設定將無法使用最近 AWS 提供的用戶端運作。新增此規則是為了緩解伺服器 IP 攻擊，如下所述：[TunnelCrack](#)。
- Client VPN 服務要求用戶端裝置的區域網路 (LAN) IP 位址範圍必須在下列標準私有 IP 位址範圍內：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、或 169.254.0.0/16。如果偵測到用戶端區域網路位址範圍超出上述範圍，Client VPN 端點會自動將 OpenVPN 指令「重新導向閘道區塊本機」推送至用戶端，強制將所有區域網路流量導入 VPN。因此，如果您在 VPN 連線期間需要 LAN 存取，建議您針對 LAN 使用上述常規位址範圍。強制執行此規則以減輕本機網路攻擊的可能性，如下所述：[TunnelCrack](#)。

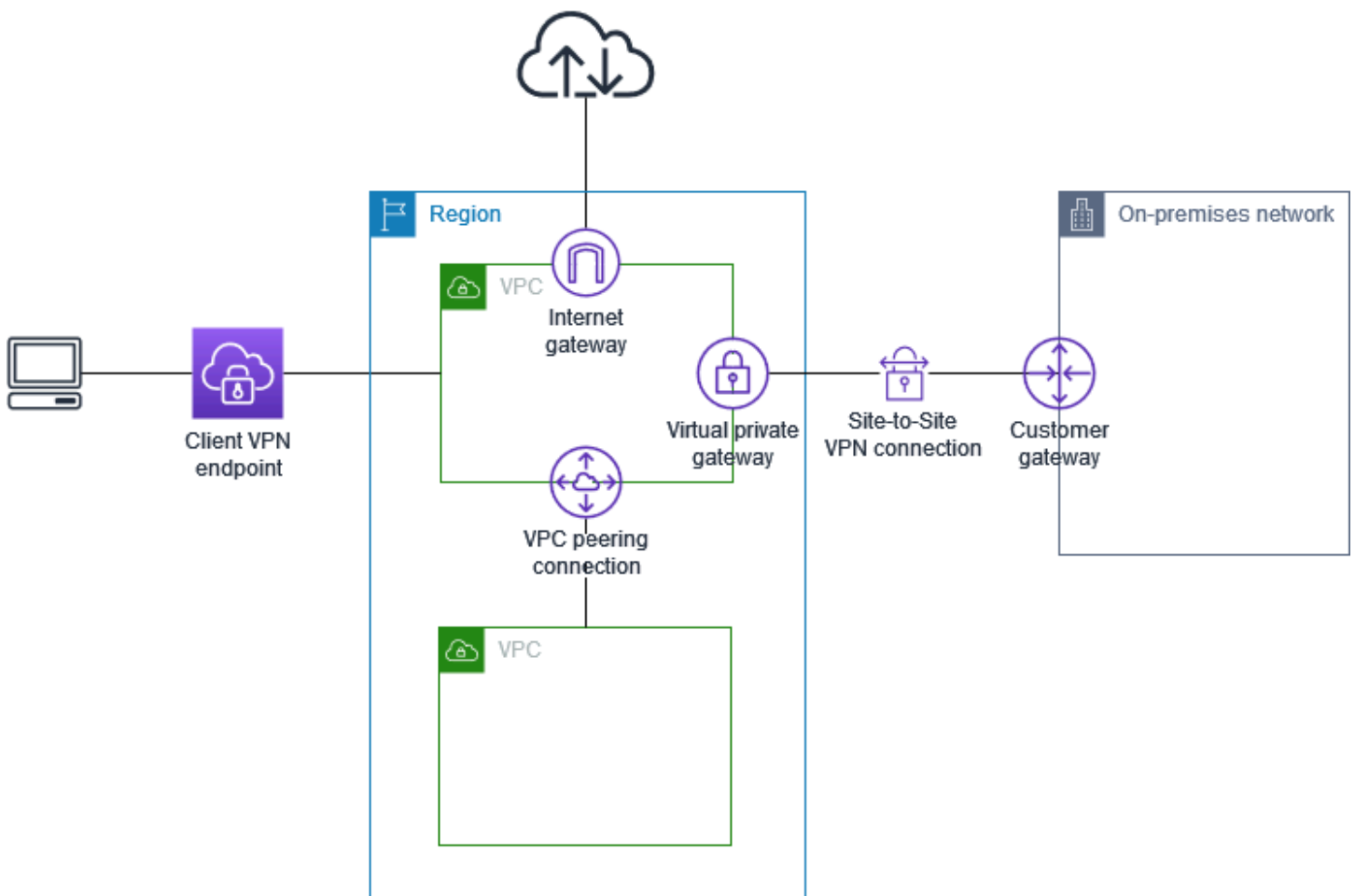
# AWS Client VPN 的運作方式

在 AWS Client VPN 中，有兩種類型的使用者角色會與 Client VPN 端點互動：管理員和用戶端。

管理員負責安裝和設定服務。這包括建立 Client VPN 端點、與目標網路建立關聯、設定授權規則，以及設定額外的路由 (如果需要)。在安裝和設定 Client VPN 端點後，管理員會下載 Client VPN 端點組態檔案，並分配給需要存取的用戶端。Client VPN 端點組態檔案包含 Client VPN 端點的 DNS 名稱，以及建立 VPN 工作階段所需的身分驗證資訊。如需設定此服務的詳細資訊，請參閱[AWS Client VPN 入門](#)。

用戶端是終端使用者。這是連線到 Client VPN 端點以建立 VPN 工作階段的人。用戶端從本機電腦或行動裝置，使用以 OpenVPN 為基礎的 VPN 用戶端應用程式建立 VPN 工作階段。他們建立 VPN 工作階段後，就可以安全地存取相關聯子網路所在 VPC 中的資源。如果已設定必要的路由和授權規則，他們也可以存取 AWS 中的其他資源、內部部署網路，或其他用戶端。如需有關連線到 Client VPN 端點以建立 VPN 工作階段的詳細資訊，請參閱《AWS Client VPN 使用者指南》中的[入門](#)。

下圖說明基本的 Client VPN 架構。



## 用戶端身分驗證

用戶端驗證是在進入 AWS 雲端的第一個點實作。其會用於決定是否允許用戶端連線到 Client VPN 端點。如果身分驗證成功，則用戶端會連線到 Client VPN 端點並建立 VPN 工作階段。如果身分驗證失敗，則拒絕連線，並防止用戶端建立 VPN 工作階段。

Client VPN 提供下列類型的用戶端身分驗證：

- [Active Directory 身分驗證](#) (以使用者為基礎)
- [交互身分驗證](#) (以憑證為基礎)
- [單一登入 \(SAML 型聯合身分驗證\)](#) (以使用者為基礎)

您可以單獨使用上面列出的方法之一，也可以將相互身分驗證與基於使用者的方法結合使用，如下所示：

- 交互身分驗證和聯合身分驗證
- 交互身分驗證和 Active Directory 身分驗證

### Important

若要建立 Client VPN 端點，您必須在中佈建伺服器憑證 AWS Certificate Manager，而不論您使用的驗證類型為何。如需建立和佈建伺服器憑證的詳細資訊，請參閱[交互身分驗證](#)中的步驟。

## Active Directory 身分驗證

Client VPN 通過集成提供活動目錄支持 AWS Directory Service。透過 Active Directory 身分驗證，將會根據現有的 Active Directory 群組來驗證用戶端。使用時 AWS Directory Service，Client VPN 可以連線到內部部署網路 AWS 或內部部署網路中佈建的現有作用中目錄。這可讓您使用現有的用戶端身分驗證基礎設施。如果您正在使用內部部署作用中目錄，而且您沒有現有的 AWS 受管理 Microsoft AD，則必須設定作用中目錄連接器 (AD Connector)。您可以使用一個 Active Directory 伺服器來驗證使用者。如需 Active Directory 整合的詳細資訊，請參閱《[AWS Directory Service 管理指南](#)》。

為 AWS 受管 Microsoft AD 或 AD Connector 啟用多重要素驗證 (MFA) 時，Client VPN 支援多重要素驗證 (MFA)。如果啟用 MFA，用戶端必須在連線到 Client VPN 端點時輸入使用者名稱、密碼和 MFA

代碼。如需啟用 MFA 的詳細資訊，請參閱《AWS Directory Service 管理指南》中的[為 AWS 受管 Microsoft AD 啟用多重要素驗證](#)和[為 AD Connector 啟用多重要素驗證](#)。

如需在 Active Directory 中設定使用者和群組的配額和規則，請參閱[使用者和群組配額](#)。

## 交互身分驗證

透過交互身分驗證，Client VPN 使用憑證在用戶端和伺服器之間執行身分驗證。憑證為憑證授權機構 (CA) 發出的數位形式身分證明。當用戶端嘗試連線到 Client VPN 端點時，伺服器會使用用戶端憑證來對用戶端進行身分驗證。您必須建立伺服器憑證和金鑰，以及至少一個用戶端憑證和金鑰。

您必須將伺服器憑證上傳至 AWS Certificate Manager (ACM)，並在建立 Client VPN 端點時加以指定。將伺服器憑證上傳至 ACM 時，您也可以指定憑證授權機構 (CA)。只有當用戶端憑證的 CA 和伺服器憑證的 CA 不同時，您才需要將用戶端憑證上傳到 ACM。如需 ACM 的詳細資訊，請參閱《[AWS Certificate Manager ACM 使用者指南](#)》。

您可以為將連線至 Client VPN 端點的每個用戶端建立個別的用戶端憑證和金鑰。這可讓您在使用者離開您的組織時撤銷特定的用戶端憑證。在這種情況下，當您建立 Client VPN 端點時，您可以為用戶端憑證指定伺服器憑證 ARN，前提是用戶端憑證是由與伺服器憑證相同的 CA 所發行。

### Note

Client VPN 端點僅支援 1024 位元和 2048 位元 RSA 金鑰大小。此外，用戶端憑證必須在「主旨」欄位中具有 CN 屬性。

在 Client VPN 服務使用的憑證透過 ACM 自動輪換、手動匯入新憑證或是將中繼資料更新至 IAM Identity Center，進行更新時，Client VPN 服務將使用更新的憑證來自動更新用戶端 VPN 端點。此自動化程序最多可能需要 24 小時。

## Linux/macOS

下列程序使用 OpenVPN easy-rsa 產生伺服器和用戶端憑證及金鑰，然後將伺服器憑證和金鑰上傳到 ACM。如需詳細資訊，請參閱 [Easy-RSA 3 Quickstart README](#)。

產生伺服器和用戶端憑證及金鑰並上傳到 ACM

1. 將 OpenVPN easy-rsa 儲存庫複製到本機電腦並導覽至 easy-rsa/easyrsa3 資料夾。

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. 初始化新的 PKI 環境。

```
$ ./easyrsa init-pki
```

3. 若要建置新的憑證授權機構 (CA)，請執行此命令並依照提示執行。

```
$ ./easyrsa build-ca nopass
```

4. 產生伺服器憑證和金鑰。

```
$ ./easyrsa --san=DNS:server build-server-full server nopass
```

5. 產生用戶端憑證和金鑰。

務必儲存用戶端憑證和用戶端私有金鑰，因為您在設定用戶端時需要它們。

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

您可以選擇性地為每個需要用戶端憑證和金鑰的用戶端 (終端使用者) 重複此步驟。

6. 將伺服器憑證和金鑰及用戶端憑證和金鑰複製到自訂資料夾，然後導覽到自訂資料夾。

複製憑證和金鑰之前，請使用 `mkdir` 命令建立自訂資料夾。下列範例會在您的主目錄中建立自訂資料夾。

```
$ mkdir ~/custom_folder/  
$ cp pki/ca.crt ~/custom_folder/  
$ cp pki/issued/server.crt ~/custom_folder/  
$ cp pki/private/server.key ~/custom_folder/  
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder/  
$ cp pki/private/client1.domain.tld.key ~/custom_folder/  
$ cd ~/custom_folder/
```

7. 將伺服器憑證和金鑰，以及用戶端憑證和金鑰上傳至 ACM。請務必在與您想要建立 Client VPN 端點的相同區域中，將其上傳。下列命令使用 AWS CLI 上傳憑證。若要改為使用 ACM 主控台上傳憑證，請參閱《AWS Certificate Manager 使用者指南》中的[匯入憑證](#)。

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key  
fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --  
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

您不一定需要將用戶端憑證上傳至 ACM。如果伺服器 and 用戶端憑證是由發行的同一家憑證授權機構 (CA) 所發行，則當您建立 Client VPN 端點時，您可以為伺服器和用戶端使用伺服器憑證 ARN。在上述步驟中，已使用相同的 CA 來建立這兩個憑證。然而，系統為了完整性，會包含上傳用戶端憑證的步驟。

## Windows

下列程序會安裝 Easy-RSA 3.x 軟體，然後使用它來產生伺服器和用戶端憑證和金鑰。

產生伺服器和用戶端憑證及金鑰並上傳到 ACM

1. 開啟 [EasyRSA 版本](#) 頁面，下載並擷取適用於您 Windows 版本的 ZIP 檔案。
2. 開啟命令提示，然後導覽至 EasyRSA-3.x 資料夾被擷取到的位置。
3. 執行下列命令以開啟 EasyRAS 3 殼層。

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. 初始化新的 PKI 環境。

```
# ./easyrsa init-pki
```

5. 若要建置新的憑證授權機構 (CA)，請執行此命令並依照提示執行。

```
# ./easyrsa build-ca nopass
```

6. 產生伺服器憑證和金鑰。

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. 產生用戶端憑證和金鑰。

```
# ./easyrsa build-client-full client1.domain.tld nopass
```



您可以選擇性地為每個需要用戶端憑證和金鑰的用戶端 (終端使用者) 重複此步驟。

8. 退出 EasyRSA 3 shell。

```
# exit
```

9. 將伺服器憑證和金鑰及用戶端憑證和金鑰複製到自訂資料夾，然後導覽到自訂資料夾。

複製憑證和金鑰之前，請使用 `mkdir` 命令建立自訂資料夾。下列範例會在您的 C:\ 磁碟機中建立自訂資料夾。

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. 將伺服器憑證和金鑰，以及用戶端憑證和金鑰上傳至 ACM。請務必在與您想要建立 Client VPN 端點的相同區域中，將其上傳。下列指令會使用 AWS CLI 來上傳憑證。若要改為使用 ACM 主控台上傳憑證，請參閱《AWS Certificate Manager 使用者指南》中的[匯入憑證](#)。

```
aws acm import-certificate --certificate fileb://server.crt --private-key
fileb://server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

您不一定需要將用戶端憑證上傳至 ACM。如果伺服器和用戶端憑證是由發行的同一家憑證授權機構 (CA) 所發行，則當您建立 Client VPN 端點時，您可以為伺服器和用戶端使用伺服器憑證 ARN。在上述步驟中，已使用相同的 CA 來建立這兩個憑證。然而，系統為了完整性，會包含上傳用戶端憑證的步驟。

## 更新您的伺服器憑證

您可以更新並重新匯入已過期的伺服器憑證。根據您使用的 OpenVPN 易於 RSA 的版本，該過程將有所不同。有關更多詳細信息，請參閱 [Easy-RSA 3 證書更新和撤銷文檔](#)。

### 更新您的伺服器憑證

1. 執行下列其中一項作業：

- 簡易 RSA 版本 3.1.x
  - 執行憑證更新命令。

```
$ ./easyrsa renew server nopass
```

- 簡易 RSA 版本 3.2.x
  - a. 運行過期命令。

```
$ ./easyrsa expire server
```

- b. 簽署新憑證。

```
$ ./easyrsa sign-req server server
```

2. 建立自訂資料夾，將新檔案複製到該資料夾中，然後導覽至該資料夾。

```
$ mkdir ~/custom_folder2  
$ cp pki/ca.crt ~/custom_folder2/  
$ cp pki/issued/server.crt ~/custom_folder2/  
$ cp pki/private/server.key ~/custom_folder2/  
$ cd ~/custom_folder2/
```

3. 將新檔案匯入 ACM。請務必將它們與 Client VPN 端點匯入至相同區域中。

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key  
fileb://server.key --certificate-chain fileb://ca.crt
```

## 單一登入 (SAML 2.0 型聯合身分驗證)

AWS Client VPN 針對 Client VPN 端點，支援使用安全宣告標記語言 2.0 (SAML 2.0) 的身分識別聯合。您可以使用支援 SAML 2.0 的身分識別提供者 (IdPs) 來建立集中式使用者身分識別。然後，您可以將 Client VPN 端點設為使用 SAML 類型聯合身分驗證，並將其與 IdP 建立關聯。然後，使用者可使用其集中式登入資料連線至 Client VPN 端點。

若要讓 SAML 類型的 IdP 使用 Client VPN 端點，您必須執行下列作業。

1. 在您選擇的 IdP 中建立 SAML 型應用程式以搭配使用 AWS Client VPN，或使用現有的應用程式。
2. 設定 IdP 與建立信任關係 AWS 如需資源，請參閱 [SAML 型 IdP 組態資源](#)。
3. 在 IdP 中產生並下載聯合中繼資料文件，以將您的組織描述為 IdP。此已簽署的 XML 文件可用來建立與 IdP 之間 AWS 的信任關係。
4. 在與 Client VPN 端點相同的 AWS 帳戶中建立 IAM SAML 身分識別提供者。IAM SAML 身分識別提供者會使用 IdP 產生的中繼資料文件來定義組織的 IdP 對 AWS 信任關係。如需詳細資訊，請參閱《IAM 使用者指南》中的 [建立 IAM SAML 身分提供者](#)。如果您稍後更新 IdP 中的應用程式組態，請產生新的中繼資料文件並更新 IAM SAML 身分提供者。

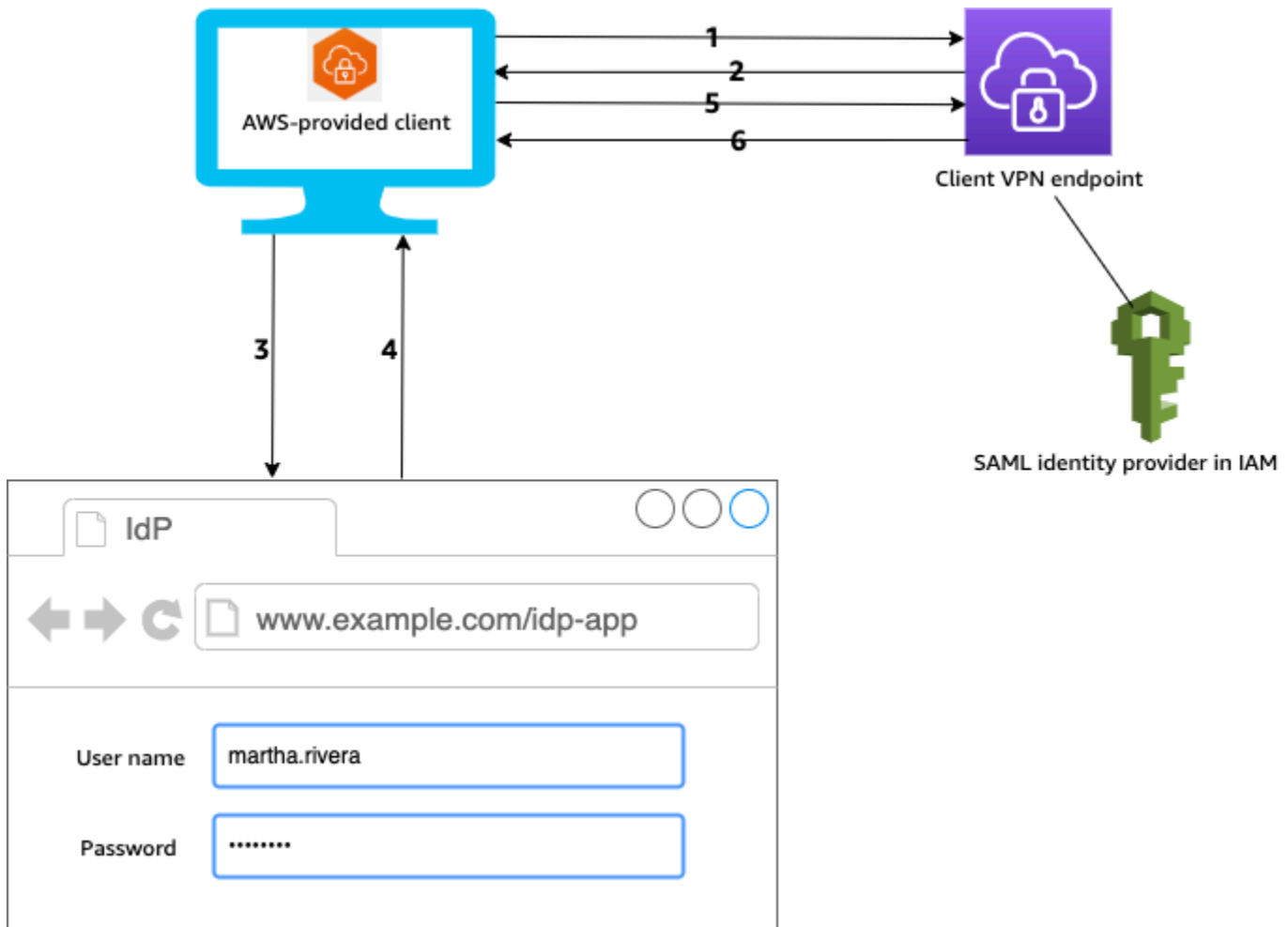
### Note

您不需要建立 IAM 角色即可使用 IAM SAML 身分提供者。

5. 建立 Client VPN 端點。指定聯合身分驗證做為身分驗證類型，並指定您建立的 IAM SAML 身分提供者。如需更多詳細資訊，請參閱 [建立 Client VPN 端點](#)。
6. 匯出 [用戶端組態檔案](#)，並將其分配到您的使用者。指示使用者下載 [AWS 提供的用戶端](#) 之最新版本，並使用其來載入組態檔案並連線到 Client VPN 端點。或者，如果您為 Client VPN 端點啟用自助入口網站，請指示您的使用者前往自助入口網站以取得設定檔和 AWS 提供的用戶端。如需詳細資訊，請參閱 [存取自助式入口網站](#)。

## 身分驗證工作流程

下圖提供身分驗證工作流程概觀，適用於使用 SAML 類型聯合身分驗證的 Client VPN 端點。建立和設定 Client VPN 端點時，請指定 IAM SAML 身分提供者。



1. 使用者會在其裝置上開啟 AWS 提供的用戶端，並啟動與 Client VPN 端點的連線。
2. Client VPN 端點會根據 IAM SAML 身分提供者中提供的資訊，將 IdP URL 和身分驗證請求傳回用戶端。
3. AWS 提供的客戶端在用戶的設備上打開一個新的瀏覽器窗口。瀏覽器向 IdP 發出請求並顯示登入頁面。
4. 使用者在登入頁面上輸入登入資料，且 IdP 會將簽署的 SAML 聲明傳回給用戶端。
5. AWS 提供的用戶端會將 SAML 宣告傳送至 Client VPN 端點。
6. Client VPN 端點會驗證聲明，並允許或拒絕對使用者的存取。

## SAML 型聯合身分驗證的需求和考量

以下是 SAML 型聯合身分驗證的需求和考量。

- 如需在 SAML 類型 IdP 中設定使用者和群組的配額和規則，請參閱[使用者和群組配額](#)。

- 必須簽署 SAML 聲明和 SAML 文件。
- AWS Client VPN 僅支援 SAML 宣告中的 NotOnOrAfter "" NotBefore 和 "和" 條件。AudienceRestriction
- SAML 回應的支援大小上限為 128 KB。
- AWS Client VPN 不提供已簽署的驗證要求。
- 不支援 SAML 單一登入。使用者可以從 AWS 提供的用戶端中斷連線來登入，或者您也可以[終止連線](#)。
- Client VPN 端點僅支援單一 IdP。
- 在 IdP 中啟用多重要素驗證 (MFA) 時，即支援多重要素驗證 (MFA)。
- 使用者必須使用 AWS 提供的用戶端連線到 Client VPN 端點。您必須使用版本 1.2.0 或更新的版本。如需詳細資訊，請參閱使用[AWS 提供的用戶端進行 Connect](#)。
- 以下瀏覽器支援 IdP 身分驗證：Apple Safari，Google Chrome，Microsoft Edge 和 Mozilla Firefox。
- AWS 提供的用戶端會在使用者裝置上保留 TCP 連接埠 35001，以供 SAML 回應使用。
- 如果使用不正確或惡意的 URL 更新 IAM SAML 身分提供者的中繼資料文件，這可能會導致使用者身分驗證問題，或導致網路釣魚攻擊。因此，我們建議您使用 AWS CloudTrail 監視對 IAM SAML 身分提供者所做的更新。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 AWS CloudTrail 記錄 IAM 和 AWS STS 呼叫](#)。
- AWS Client VPN 透過 HTTP 重新導向繫結，將 AuthN 要求傳送至 IdP。因此，IdP 應該支援 HTTP 重新導向繫結，而且它應該存在於 IdP 的中繼資料文件中。
- 針對 SAML 聲明，您必須使用 NameID 屬性的電子郵件地址格式。

## SAML 型 IdP 組態資源

下表列出我們已經測試過 IdPs 可搭配使用的 SAML AWS Client VPN，以及可協助您設定 IdP 的資源。

IdP	資源
Okta	<a href="#">AWS Client VPN 使用 SAML 驗證使用者</a>
Microsoft Azure Active Directory	如需詳細資訊，請參閱 Microsoft 文件網站上的 <a href="#">教學課程：Azure 作用中目錄單一登入 (SSO) 與用 AWS 戶端 VPN 整合</a> 。

IdP	資源
JumpCloud	<a href="#">單一登入 (SSO) AWS Client VPN</a>
AWS IAM Identity Center	<a href="#">使用 IAM 身分中心進行身 AWS Client VPN 份驗證和授權</a>

### 建立應用程式的服務提供者資訊

若要使用上表未列出的 IdP 建立 SAML 應用程式，請使用下列資訊來設定 AWS Client VPN 服務提供者資訊。

- 聲明消費者服務 (ACS) URL : `http://127.0.0.1:35001`
- 對象 URI : `urn:amazon:webservices:clientvpn`

IdP 的 SAML 回應中必須包含至少一個屬性。範例屬性如下。

屬性	描述
FirstName	使用者的名字。
LastName	使用者的姓氏。
memberOf	使用者所屬的一或多個群組。

#### Note

使用 Active Directory 或 SAML IdP 群組型授權規則需要 `memberOf` 屬性。該屬性亦區分大小寫，且必須完全按照指定進行設定。如需詳細資訊，請參閱 [以網路為基礎的授權](#) 和 [授權規則](#)。

### 自助入口網站支援

如果您為 Client VPN 端點啟用自助入口網站，使用者可以使用其 SAML 類型的 IdP 登入資料登入入口網站。

如果您的 IdP 支援多個聲明消費者服務 (ACS) URL，請將下列 ACS URL 新增到您的應用程式。

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

如果您在某個 GovCloud 區域中使用 Client VPN 端點，請改用下列 ACS URL。如果您使用相同的 IDP 應用程式來驗證標準和 GovCloud 區域，則可以同時新增這兩個 URL。

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

如果您的 IdP 不支援多個 ACS URL，請執行下列作業：

1. 在您的 IdP 中建立額外的 SAML 類型應用程式，並指定下列 ACS URL。

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

2. 產生並下載聯合身分中繼資料文件。
3. 在與 Client VPN 端點相同的 AWS 帳戶中建立 IAM SAML 身分識別提供者。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立 IAM SAML 身分提供者](#)。

#### Note

除了您為[主要應用程式建立的](#)之外，您還建立了這個 IAM SAML 身分提供者。

4. [建立 Client VPN 端點](#)，並指定您建立的 IAM SAML 身分提供者。

## 客戶端授權

Client VPN 支援兩種用戶端授權類型：安全群組和聯網類型授權 (使用授權規則)。

### 安全群組

建立 Client VPN 端點時，您可以從特定 VPC 指定要套用至 Client VPN 端點的安全群組。當您將子網路與 Client VPN 端點建立關聯時，我們會自動套用 VPC 的預設安全群組。您可以在建立 Client VPN 端點後變更安全群組。如需更多詳細資訊，請參閱[將安全群組套用到目標網路](#)。安全群組與 Client VPN 網路界面相關聯。

您可以將規則新增到應用程式的安全群組以允許套用到關聯安全群組所傳來的流量，讓 Client VPN 使用者可以存取 VPC 中的應用程式。

新增規則，允許來自 Client VPN 端點安全群組的流量

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇與您的資源或應用程式相關聯的安全群組，然後選擇動作、編輯傳入規則。
4. 選擇 Add rule (新增規則)。
5. 針對 Type (類型)，選擇 All traffic (所有流量)。或者，您可以限制存取特定類型的流量，例如 SSH。

針對 Source (來源)，指定與 Client VPN 端點目標網路 (子網路) 相關聯的安全群組 ID。

6. 選擇 Save rules (儲存規則)。

相反地，您可以藉由不指定套用至關聯的安全群組，或是移除參考 Client VPN 端點安全群組的規則，來限制 Client VPN 使用者的存取。您需要的安全群組規則也可能取決於您要設定的 VPN 存取種類。如需更多詳細資訊，請參閱 [AWS Client VPN 的案例和範例](#)。

如需安全群組的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [VPC 的安全群組](#)。

## 以網路為基礎的授權

以網路為基礎的授權是使用授權規則來實作。對於您想要啟用存取的每個網路，您必須設定授權規則來限制有存取權的使用者。對於指定的網路，請設定允許存取的 Active Directory 群組或 SAML 型 IdP 群組。只有屬於指定群組的使用者，才可以存取指定的網路。如果您不是使用 Active Directory 或 SAML 型聯合身分驗證，或是您希望開放所有使用者的存取權，您可以指定規則來將存取權授與給所有用戶端。如需更多詳細資訊，請參閱 [授權規則](#)。

## 連線授權

您可以為 Client VPN 端點設定「用戶端連線處理常式」。處理常式可讓您根據裝置、使用者和連線屬性，執行可授權新連線的自訂邏輯。用戶端連線處理常式會在 Client VPN 服務驗證過裝置和使用者身分後執行。

若要為 Client VPN 端點設定用戶端連線處理常式，請建立將裝置、使用者和連線屬性視為輸入的 AWS Lambda 函數，並將允許或拒絕新連線的決定傳回 Client VPN 服務。您可以在 Client VPN 端點中指定 Lambda 函數。當裝置連線到 Client VPN 端點時，Client VPN 服務會代您叫用 Lambda 函數。只有經 Lambda 函數授權的連線才可以連線到 Client VPN 端點。



**Note**

目前唯一支援的用戶端連線處理常式類型是 Lambda 函數。

## 需求和考量事項

下列是用戶端連線處理常式的需求和考量事項：

- Lambda 函數的名稱必須以 `AWSCliientVPN-` 前綴開頭。
- 支援合格的 Lambda 函數。
- Lambda 函數必須位於與 Client VPN 端點位於相同 AWS 區域且 AWS 帳戶相同。
- Lambda 函數會在 30 秒後逾時。此值無法變更。
- 會以同步方式呼叫 Lambda 函數。在驗證設備和使用者身分後、評估授權規則前呼叫。
- 如果為新連線呼叫 Lambda 函數，但 Client VPN 服務未從函數獲取得預期的回應，則 Client VPN 服務會拒絕此連線要求。例如，如果 Lambda 函數被調節、逾時或遇到其他未預期的錯誤，或者函數的回應格式不正確，就會發生這個問題。
- 建議您為 Lambda 函數設定 [佈建並行](#)，使其能在不造成延遲波動的情況下擴展。
- 如果您更新 Lambda 函數，現有的 Client VPN 端點連線不會受到影響。您可以終止現有的連線，然後指示用戶端建立新的連線。如需詳細資訊，請參閱 [終止用戶端連線](#)。
- 如果用戶端使用 AWS 提供的用戶端連線至 Client VPN 端點，則必須為 Windows 使用 1.2.6 或更新版本，而 macOS 則必須使用 1.2.4 或更新版本。如需詳細資訊，請參閱 [使用 AWS 提供的用戶端連線](#)。

## Lambda 界面

Lambda 函數會將裝置屬性、使用者屬性和連線屬性視為來自 Client VPN 服務的輸入。然後，必須將允許或拒絕連線的決定傳回 Client VPN 服務。

### 請求結構描述

Lambda 函數將包含下列欄位的 JSON blob 視為輸入。

```
{
  "connection-id": <connection ID>,
  "endpoint-id": <client VPN endpoint ID>,
}
```

```
"common-name": <cert-common-name>,  
"username": <user identifier>,  
"platform": <OS platform>,  
"platform-version": <OS version>,  
"public-ip": <public IP address>,  
"client-openvpn-version": <client OpenVPN version>,  
"aws-client-version": <AWS client version>,  
"groups": <group identifier>,  
"schema-version": "v3"  
}
```

- `connection-id` – 連線到 Client VPN 端點的用戶端 ID。
- `endpoint-id` – Client VPN 端點的 ID。
- `common-name` – 裝置識別符。在您為裝置建立的用戶端憑證中，通用名稱只能識別裝置。
- `username` – 使用者識別符 (如果適用)。若為 Active Directory 身分驗證，這是使用者名稱。若為 SAML 型聯合身分驗證，這是 NameID。若要交互身分驗證，此欄位為空白。
- `platform` – 用戶端作業系統平台。
- `platform-version` – 作業系統的版本。當用戶端連線至 Client VPN 端點，且用戶端正在執行 Windows 平台時，Client VPN 服務會在 OpenVPN 用戶端組態中出現 `--push-peer-info` 指令時提供一個值。
- `public-ip` – 要連線裝置的公有 IP 地址。
- `client-openvpn-version` – 用戶端正在使用的 OpenVPN 版本。
- `aws-client-version` – 用 AWS 用戶端版本。
- `groups` – 群組識別符 (如果適用)。若為 Active Directory 身分驗證，這將是 Active Directory 群組的清單。若為 SAML 型聯合身分驗證，這將是身分提供者 (IdP) 群組的清單。若要交互身分驗證，此欄位為空白。
- `schema-version` – 結構描述版本。預設值為 `v3`。

## 回應結構描述

Lambda 函數必須傳回下列欄位。

```
{  
  "allow": boolean,  
  "error-msg-on-denied-connection": "",  
  "posture-compliance-statuses": [],
```

```
"schema-version": "v3"  
}
```

- `allow` – 必要。布林值 (`true` | `false`)，指出允許或拒絕新連線。
- `error-msg-on-denied-connection` – 必要。如果 Lambda 函數拒絕連線，您可以向用戶端提供步驟和指導說明，長度不超過 255 個字元。如果 Lambda 函數執行期間發生故障 (例如，因為調節)，則下列預設訊息會傳回用戶端。

```
Error establishing connection. Please contact your administrator.
```

- `posture-compliance-statuses` – 必要。如果您使用 Lambda 函數 [評估狀態](#)，此即為連線裝置的狀態清單。您可以根據裝置的狀態評估類別定義狀態名稱，例如 `compliant`、`quarantined`、`unknown` 等等。每個名稱的長度上限為 255 個字元。您最多可以指定 10 種狀態。
- `schema-version` – 必要。結構描述版本。預設值為 `v3`。

您可以為相同區域中的多個 Client VPN 端點使用相同的 Lambda 函數。

如需建立 Lambda 函數的詳細資訊，請參閱《AWS Lambda 開發人員指南》中的 [AWS Lambda 入門](#)。

## 使用用戶端連線處理常式評估狀態

您可以使用用戶端連線處理常式整合 Client VPN 端點和現有的裝置管理解決方案，以評估連線裝置的狀態合規性。若要讓 Lambda 函數做為裝置授權處理常式運作，請在 Client VPN 端點使用 [交互身分驗證](#)。您可以為要連線至 Client VPN 端點的每個用戶端 (裝置) 建立唯一的用戶端憑證和金鑰。Lambda 函數可使用用戶端憑證的唯一通用名稱 (從 Client VPN 服務傳出) 來識別裝置，並從您的裝置管理解決方案擷取其狀態合規狀態。您可以將交互身分驗證與使用者型身分驗證結合使用。

或者，您可以在 Lambda 函數中執行基本的狀態評估。例如，您可以評估 Client VPN 服務傳遞給 Lambda 函數的 `platform` 和 `platform-version` 欄位。

### Note

雖然連線處理常式可用來強制執行最低 AWS Client VPN 應用程式版本，但連線處理常式 `aws-client-version` 中的欄位僅適用於 AWS Client VPN 應用程式，且會從使用者裝置上的環境變數填入。

## 啟用用戶端連線處理常式

若要啟用用戶端連線處理常式，請建立或修改 Client VPN 端點，並指定 Lambda 函數的 Amazon Resource Name (ARN)。如需更多詳細資訊，請參閱[建立 Client VPN 端點](#)。及[修改 Client VPN 端點](#)。

## 服務連結角色

AWS Client VPN 自動在您的AWSServiceRoleForClientVPNConnections帳戶中建立服務連結角色。連線到 Client VPN 端點時，角色具有呼叫 Lambda 函數的許可。如需更多詳細資訊，請參閱[在 Client VPN 使用服務連結角色](#)。

## 監視連線授權失敗

您可以檢視 Client VPN 端點連線的連線授權狀態。如需更多詳細資訊，請參閱[查看用戶端連線](#)。

使用用戶端連線處理常式評估狀態時，您也可以連線日誌中檢視連線至 Client VPN 端點之裝置的狀態合規狀態。如需更多詳細資訊，請參閱[連線日誌記錄](#)。

如果裝置連線授權失敗，則連線日誌中的 connection-attempt-failure-reason 欄位會傳回下列失敗原因的其中之一：

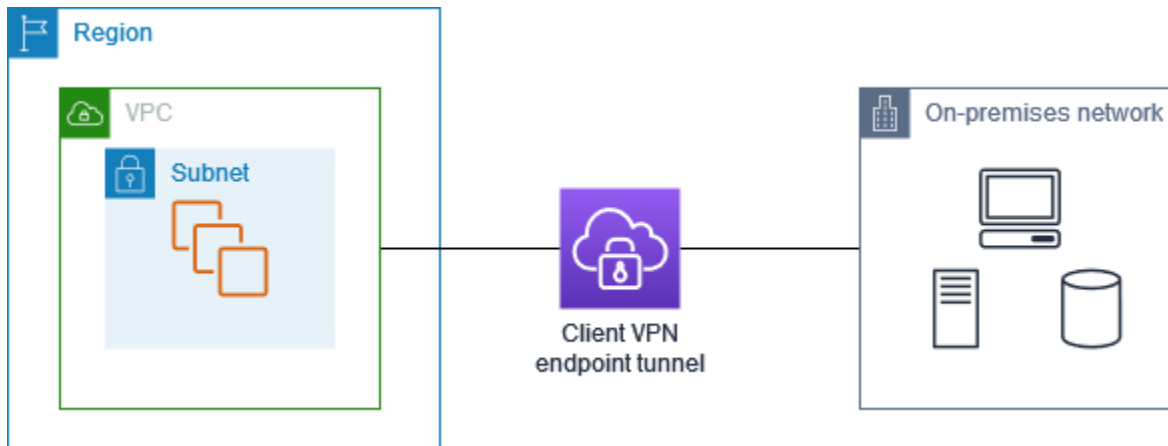
- client-connect-failed – 防止建立連線的 Lambda 函數。
- client-connect-handler-timed-out – Lambda 函數已逾時。
- client-connect-handler-other-execution-error – Lambda 函數發生未預期的錯誤。
- client-connect-handler-throttled – 經過調節的 Lambda 函數。
- client-connect-handler-invalid-response – 傳回無效回應的 Lambda 函數。
- client-connect-handler-service-error – 嘗試連線期間在服務端發生錯誤。

## AWS Client VPN 端點上的分割通道

根據預設，當您有 Client VPN 端點時，來自用戶端的所有流量都會透過 Client VPN 通道路由。當您啟用 Client VPN 端點上的分割通道時，我們會將[Client VPN 端點路由表](#)上的路由推送到連線至 Client VPN 端點的裝置。這可確保只有網路目標與 Client VPN 端點路由表之路由相符的流量，才可以透過 Client VPN 通道路由。

如果不希望所有使用者的流量皆透過 Client VPN 端點路由，您可以使用分割通道 Client VPN 端點。

以下範例在 Client VPN 端點上啟用了分割通道。只有以 VPC (172.31.0.0/16) 為目標的流量才可以透過 Client VPN 通道路由。目標為現場部署資源的流量，不會透過 Client VPN 通道路由。



## 分割隧道的優點

Client VPN 端點上的分割通道有下列優點：

- 您可以只讓目的地為 AWS 的流量周遊 VPN 通道，以最佳化來自用戶端的流量路由。
- 您可以減少來自 AWS 的傳出流量，進而降低資料傳輸成本。

## 路由傳送考量

- 如果啟用分割通道模式，則在建立 VPN 連接時，Client VPN 端點路由表中的所有路由都會新增至用戶端路由表。此操作不同於預設行為，也就是以項目 0.0.0.0/0 覆寫用戶端路由表，以透過 VPN 路由傳送所有流量。

### Note

使用分割通道模式時，建議不要新增連至 Client VPN 端點路由表的 0.0.0.0/0 路由。

- 啟用分割通道模式時，對 Client VPN 端點路由表的任何修改都會導致重設所有用戶端連線。

## 啟用分割隧道

您可以在新的或現有的 Client VPN 端點上啟用分割通道。如需詳細資訊，請參閱下列主題：

- [建立 Client VPN 端點。](#)
- [修改 Client VPN 端點](#)

## 連線日誌記錄

連線日誌記錄是一項 AWS Client VPN 的功能，可讓您擷取 Client VPN 端點的連線日誌。

連線日誌包含連線日誌項目。每個連線日誌項目都包含連線事件的相關資訊，即用戶端 (最終使用者) 連線、嘗試連線或中斷 Client VPN 端點的連線時。您可以使用此資訊來執行鑑識、分析 Client VPN 端點的使用方式，或偵錯連線問題。

您可以在提供 AWS Client VPN 的所有地區中使用連線日誌。連線日誌會發佈到您帳戶中的 CloudWatch Logs 日誌群組。

### Note

不會記錄失敗的相互驗證嘗試。

## 連線日誌項目

連線日誌項目是索引鍵/值組的 JSON 格式 Blob。以下是連線日誌項目範例。

```
{
  "connection-log-type": "connection-attempt",
  "connection-attempt-status": "successful",
  "connection-reset-status": "NA",
  "connection-attempt-failure-reason": "NA",
  "connection-id": "cvpn-connection-abc123abc123abc12",
  "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
  "transport-protocol": "udp",
  "connection-start-time": "2020-03-26 20:37:15",
  "connection-last-update-time": "2020-03-26 20:37:15",
  "client-ip": "10.0.1.2",
  "common-name": "client1",
  "device-type": "mac",
  "device-ip": "98.247.202.82",
  "port": "50096",
  "ingress-bytes": "0",
  "egress-bytes": "0",
  "ingress-packets": "0",
  "egress-packets": "0",
  "connection-end-time": "NA",
  "username": "joe"
```

```
}
```

連線日誌項目包含下列金鑰：

- `connection-log-type`：連線日誌項目的類型 (`connection-attempt` 或 `connection-reset`)。
- `connection-attempt-status`：連線請求的狀態 (`successful`、`failed`、`waiting-for-assertion`，或 `NA`)。
- `connection-reset-status`：連線重設事件的狀態 (`NA` 或 `assertion-received`)。
- `connection-attempt-failure-reason`：連線失敗的原因 (如適用)。
- `connection-id`：連線的 ID。
- `client-vpn-endpoint-id`：建立連線的 Client VPN 端點 ID。
- `transport-protocol`：用於連線的傳輸通訊協定。
- `connection-start-time`：連線的開始時間。
- `connection-last-update-time`：連線的上次更新時間。此值在日誌中會定期更新。
- `client-ip`：從 Client VPN 端點的用戶端 IPv4 CIDR 範圍配置的用戶端 IP 地址。
- `common-name`：用於憑證類型身分驗證的憑證常用名稱。
- `device-type`：用於最終使用者連線的裝置類型。
- `device-ip`：裝置的公有 IP 地址。
- `port`：連線的連接埠號碼。
- `ingress-bytes`：連線的輸入 (傳入) 位元組數。此值在日誌中會定期更新。
- `egress-bytes`：連線的輸出 (傳輸) 位元組數。此值在日誌中會定期更新。
- `ingress-packets`：連線的輸入 (傳入) 封包數。此值在日誌中會定期更新。
- `egress-packets`：連線的輸出 (傳出) 封包數。此值在日誌中會定期更新。
- `connection-end-time`：連線的結束時間。若連線仍在進行中，或連線嘗試失敗，則此值為 `NA`。
- `posture-compliance-statuses`：[用戶端連線處理器](#)傳回的狀態合規狀態 (如適用)。
- `username` — 使用者型驗證 (AD 或 SAML) 用於端點時，會記錄使用者名稱。
- `connection-duration-seconds` — 持續時間 (以秒為單位)。等於「連接開始時間」和「連接結束時間」之間的差異。

如需啟用連線記錄日誌的詳細資訊，請參閱[使用連線日誌](#)。

## Client VPN 擴展考量

當您建立 Client VPN 端點時，請考慮您計劃支援的並行 VPN 連線數量上限。您應該考慮目前支援的用戶端數目，以及您的 Client VPN 端點是否能滿足額外需求 (如果需要)。

下列因素會影響 Client VPN 端點上可支援的並行 VPN 連線數量上限。

### 用戶端 CIDR 範圍大小

當您[建立 Client VPN 端點](#)時，必須指定用戶端 CIDR 範圍，該範圍是介於 /12 和 /22 網路遮罩之間的 IPv4 CIDR 區塊。每個與 Client VPN 端點的 VPN 連線都會從用戶端 CIDR 範圍指派唯一的 IP 地址。用戶端 CIDR 範圍中的一部分地址也用於支援 Client VPN 端點的可用性模型，而且無法指派給用戶端。建立 Client VPN 端點後，您無法變用戶端 CIDR 範圍。

一般而言，我們建議您指定用戶端 CIDR 範圍，其中包含您計劃在 Client VPN 端點上支援的 IP 地址 (以及並行連線) 的兩倍。

### 關聯子網路數量

當您將[子網路與 Client VPN 端點建立關聯](#)時，您可以讓使用者建立 VPN 工作階段至 Client VPN 端點。您可以將多個子網路與 Client VPN 端點建立關聯，以取得高可用性，並啟用額外的連線容量。

以下是基於 Client VPN 端點的子網路關聯數量之受支援的並行 VPN 連線數量。

子網路關聯	支援的連線數量
1	7,000
2	36,500
3	66,500
4	96,500
5	126,000

您不能將來自相同可用區域的多個子網路與一個 Client VPN 端點建立關聯。因此，子網路關聯的數量也取決於 AWS 區域中可用的可用區域數量。



例如，如果您預期支援 8,000 個 VPN 連線至 Client VPN 端點，請指定 /18 的最小用戶端 CIDR 範圍大小 (16,384 個 IP 地址)，並將至少 2 個子網路與 Client VPN 端點建立關聯。

如果您不確定 Client VPN 端點的預期 VPN 連線數量，建議您指定 /16 CIDR 區塊的大小或更大範圍。

如需使用用戶端 CIDR 範圍和目標網路的規則和限制的詳細資訊，請參閱 [規則和最佳做法 AWS Client VPN](#)。

如需 Client VPN 端點配額的詳細資訊，請參閱 [AWS Client VPN 配額](#)。

# AWS Client VPN 的案例和範例

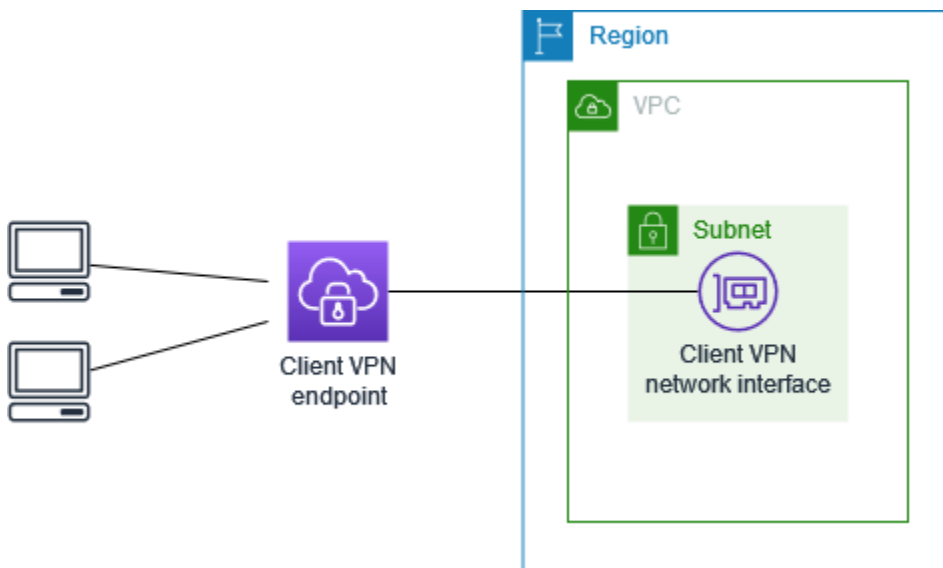
本節提供範例來示範為您的用戶端建立和設定 Client VPN 存取。

## 目錄

- [使用 AWS Client VPN 存取 VPC](#)
- [使用 AWS Client VPN 存取對等 VPC](#)
- [使用 AWS Client VPN 存取內部部署網路](#)
- [使用 AWS 用戶端 VPC 存取網際網路](#)
- [使用 AWS Client VPN client-to-client 訪問 C](#)
- [使用 AWS Client VPN 限制存取您的網路](#)

## 使用 AWS Client VPN 存取 VPC

此案例的組態包含單一目標 VPC。如果您需要讓用戶端只存取單一 VPC 內的資源，我們建議使用此組態。



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別與 Client VPN 端點關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。
- 識別與 VPC CIDR 不重疊的用戶端 IP 地址適當的 CIDR 範圍。

- 於 [規則和最佳做法 AWS Client VPN](#) 檢閱 Client VPN 端點的規則和限制。

### 實作此組態

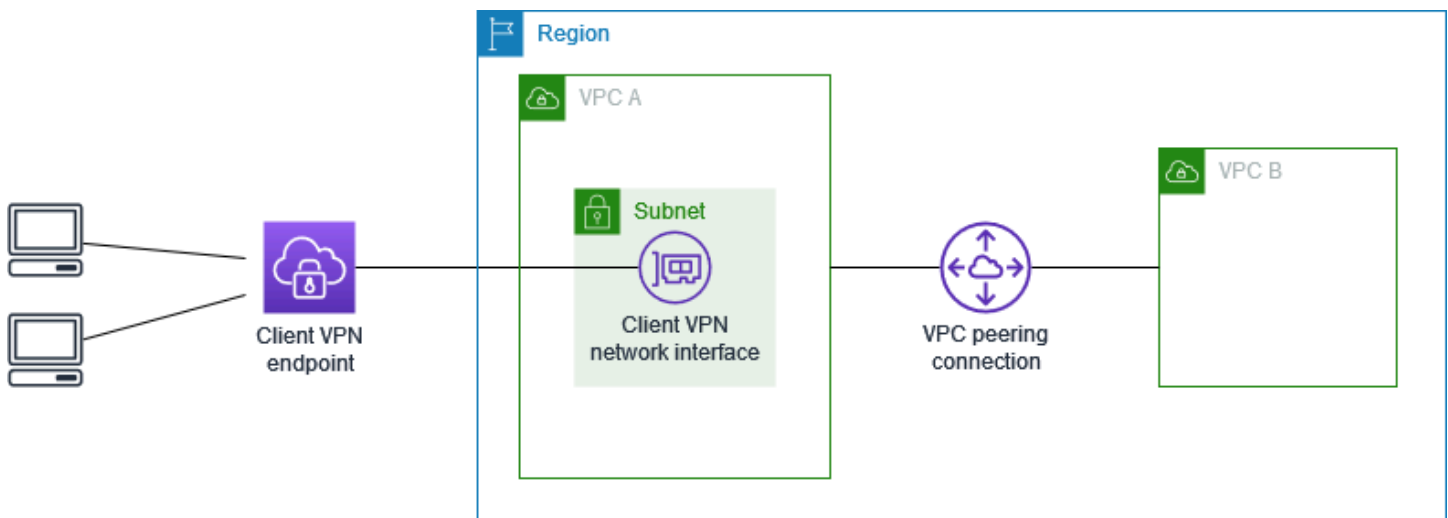
- 在與 VPC 相同的區域中建立 Client VPN 端點。若要執行此作業，請執行[建立 Client VPN 端點](#)中所述的步驟。
- 將子網路與 Client VPN 端點建立關聯。若要執行此作業，請執行[建立目標網路與 Client VPN 端點的關聯](#)中所述的步驟，然後選擇您稍早所識別的子網路和 VPC。
- 新增授權規則讓用戶端存取 VPC。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟；並對於目的地網路，輸入 VPC 的 IPv4 CIDR 範圍。
- 將規則新增至資源的安全群組，以允許來自步驟 2 中套用至子網路關聯的安全性群組的流量。如需更多詳細資訊，請參閱 [安全群組](#)。

## 使用 AWS Client VPN 存取對等 VPC

此案例的組態包括與其他 VPC (VPC B) 對等的目標 VPC (VPC A)。如果您需要讓用戶端存取目標 VPC 和其他對等 VPC 內 (例如 VPC B) 的資源，我們建議您使用此組態。

### Note

只有在 Client VPN 端點已設定為分割通道模式時，才需要允許下述對等 VPC 存取權的程序。在完整通道模式下，依預設會允許對等 VPC 存取權。



開始之前，請執行以下動作：

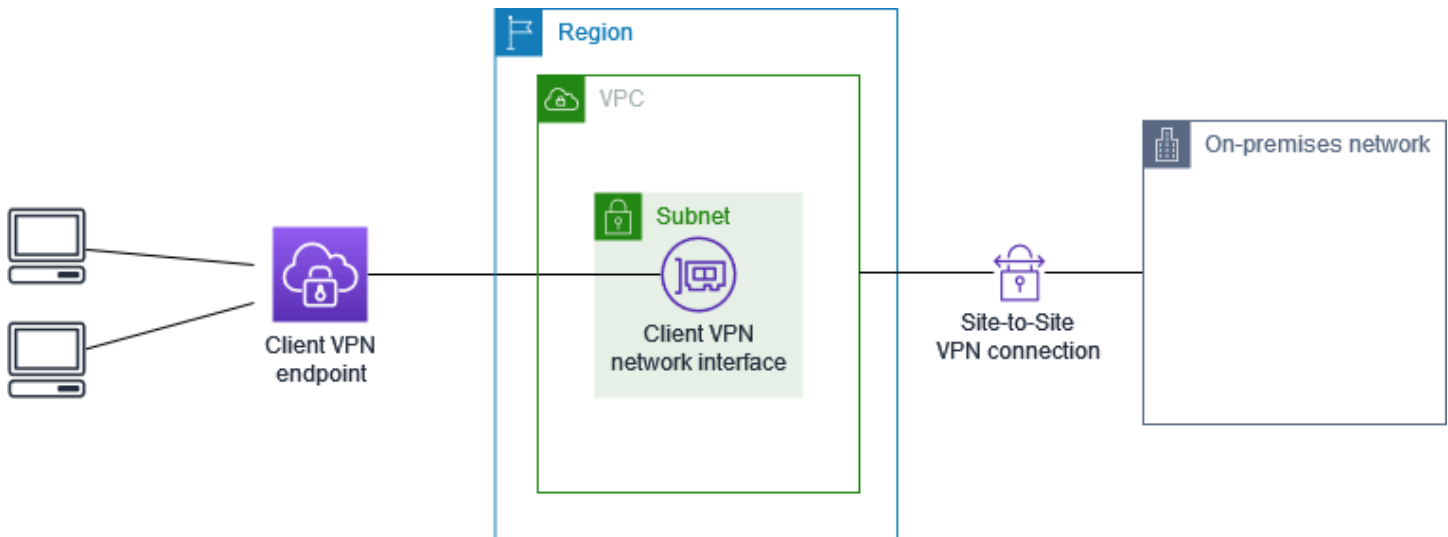
- 建立或識別至少具有一個子網路的 VPC。識別與 Client VPN 端點關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。
- 識別與 VPC CIDR 不重疊的用戶端 IP 地址適當的 CIDR 範圍。
- 於 [規則和最佳做法 AWS Client VPN](#) 檢閱 Client VPN 端點的規則和限制。

實作此組態

1. 在 VPC 之間建立 VPC 對等連線。遵循《Amazon VPC 對等連線指南》中的[建立和接受 VPC 對等連線](#)的步驟。確認 VPC A 中的執行個體可以使用對等連線與 VPC B 中的執行個體通訊。
2. 在與目標 VPC 相同的區域中建立 Client VPN 端點。在圖表中，這是 VPC A。請執行 [建立 Client VPN 端點](#) 中所述的步驟。
3. 將您稍早識別的子網路與您建立的 Client VPN 端點建立關聯。若要執行此作業，請執行 [建立目標網路與 Client VPN 端點的關聯](#) 中所述的步驟，選取 VPC 和子網路。依預設，我們會將 VPC 的預設安全群組與 Client VPN 端點建立關聯。您可以使用 [the section called “將安全群組套用到目標網路”](#) 中所述步驟來關聯不同安全群組。
4. 新增授權規則讓用戶端存取目標 VPC。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟。在要啟用的目的地網路中，輸入 VPC 的 IPv4 CIDR 範圍。
5. 新增路由將流量引導至對等 VPC。在圖表中，這是 VPC B。如要執行此操作，請執行 [建立端點路由](#) 中所述的步驟。在路由目的地中，輸入對等 VPC 的 IPv4 CIDR 範圍。在目標 VPC 子網路 ID，選取與 Client VPN 端點關聯的子網路。
6. 新增授權規則讓用戶端存取對等 VPC。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟。在目的地網路中，輸入對等 VPC 的 IPv4 CIDR 範圍。
7. 在 VPC A 和 VPC B 中為您的執行個體新增規則至安全群組，以允許來自步驟 3 中套用 Client VPN 端點的安全群組流量。如需詳細資訊，請參閱 [安全群組](#)。

## 使用 AWS Client VPN 存取內部部署網路

此案例的組態只包含存取現場部署網路。如果您需要讓用戶端只存取現場部署網路內的資源，我們建議使用此組態。



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別與 Client VPN 端點關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。
- 識別與 VPC CIDR 不重疊的用戶端 IP 地址適當的 CIDR 範圍。
- 於 [規則和最佳做法 AWS Client VPN](#) 檢閱 Client VPN 端點的規則和限制。

### 實作此組態

1. 允許 VPC 和您自己的內部部署網路之間透過 AWS Site-to-Site VPN 連接進行通訊。若要執行此動作，請執行 AWS Site-to-Site VPN 使用者指南中 [入門](#) 所述的步驟。

#### Note

或者，您可以使用 VPC 與內部部署網路之間的 AWS Direct Connect 連線來實作此案例。如需詳細資訊，請參閱 [《AWS Direct Connect 使用者指南》](#)。

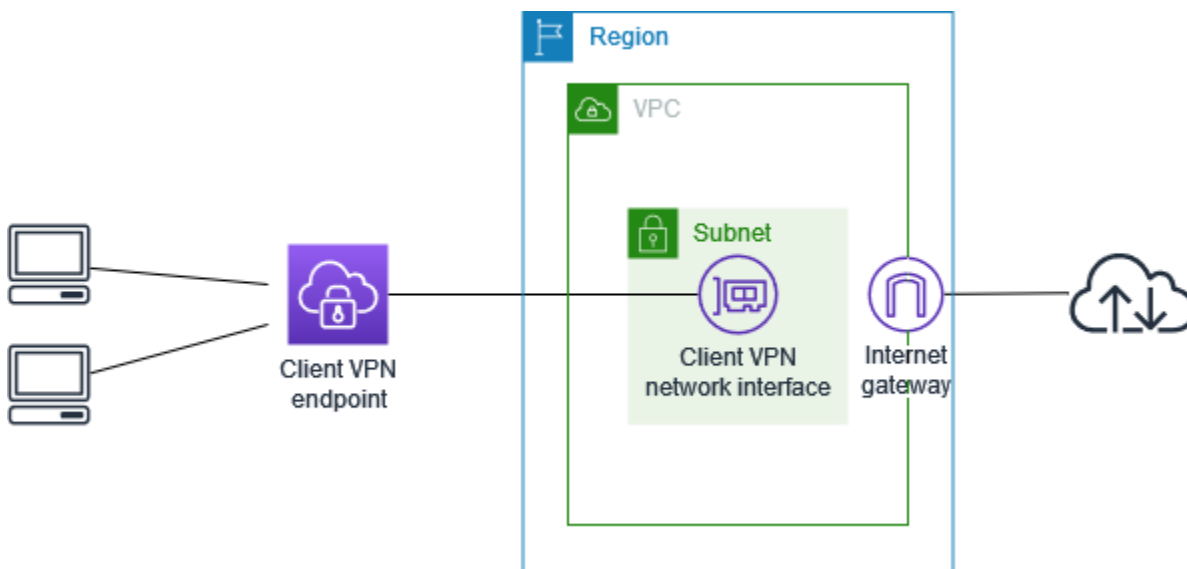
2. 測試您在上一個步驟建立的 AWS Site-to-Site VPN 連接。若要執行此作業，請執行 AWS Site-to-Site VPN 使用者指南中 [測試 Site-to-Site VPN 連接](#) 所述的步驟。如果 VPN 連接的運作符合預期，請繼續下一個步驟。
3. 在與 VPC 相同的區域中建立 Client VPN 端點。若要執行此作業，請執行 [建立 Client VPN 端點](#) 中所述的步驟。
4. 將您稍早所識別的子網路與 Client VPN 端點建立關聯。若要執行此作業，請執行 [建立目標網路與 Client VPN 端點的關聯](#) 中所述的步驟，然後選取 VPC 和子網路。

5. 新增路由以允許存取 AWS Site-to-Site VPN 連接。若要執行此作業，請執行[建立端點路由](#)中所述的步驟；對於路由目的地，輸入 AWS Site-to-Site VPN 連接的 IPv4 CIDR 範圍，對於目標 VPC 子網路 ID，選擇與 Client VPN 端點相關聯的子網路。
6. 新增授權規則讓用戶端存取 AWS Site-to-Site VPN 連接。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟；對於目的地網路，輸入 AWS Site-to-Site VPN 連接 IPv4 CIDR 範圍。

## 使用 AWS 用戶端 VPC 存取網際網路

此案例的組態包含單一目標 VPC 和存取網際網路。如果您需要讓用戶端存取單一目標 VPC 內的資源和允許存取網際網路，我們建議您使用此組態。

如果您已完成 [AWS Client VPN 入門教學課程](#)，則您已實作此案例。



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別與 Client VPN 端點關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。
- 識別與 VPC CIDR 不重疊的用戶端 IP 地址適當的 CIDR 範圍。
- 於 [規則和最佳做法 AWS Client VPN](#) 檢閱 Client VPN 端點的規則和限制。

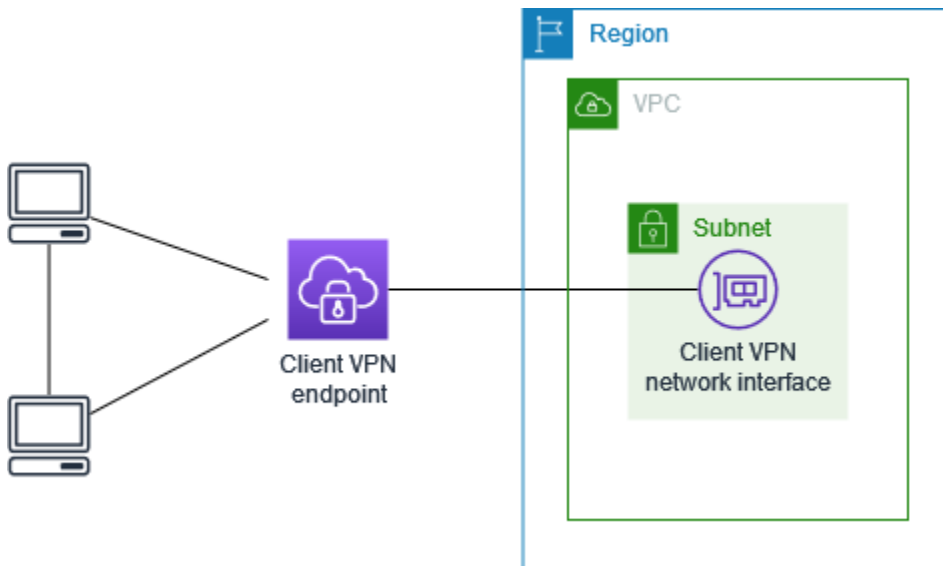
### 實作此組態

1. 確定您將用於 Client VPN 端點的安全群組允許進出網際網路的傳出流量。若要這樣做，請新增允許 HTTP 和 HTTPS 流量進出 0.0.0.0/0 的傳出流量規則。

2. 建立網際網路閘道，並將它連接至您的 VPC。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[建立和連接網際網路閘道](#)。
3. 將網際網路閘道的路由新增到其路由表，以公開您的子網路。在 VPC 主控台，選擇 Subnets (子網路)，選取要與 Client VPN 端點相關聯的子網路，選擇 Route Table (路由表)，然後選擇路由表 ID。選擇 Actions (動作)，選擇 Edit routes (編輯路由)，然後選擇 Add route (新增路由)。對於 Destination (目的地)，輸入 `0.0.0.0/0`，對於 Target (目標)，選擇上一個步驟中的網際網路閘道。
4. 在與 VPC 相同的區域中建立 Client VPN 端點。若要執行此作業，請執行[建立 Client VPN 端點](#)中所述的步驟。
5. 將您稍早所識別的子網路與 Client VPN 端點建立關聯。若要執行此作業，請執行[建立目標網路與 Client VPN 端點的關聯](#)中所述的步驟，然後選取 VPC 和子網路。
6. 新增授權規則讓用戶端存取 VPC。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟；並對於要啟用的目的地網路，輸入 VPC 的 IPv4 CIDR 範圍。
7. 新增路由以允許流向網際網路的流量。若要執行此作業，請執行[建立端點路由](#)中所述的步驟；並對於路由目的地，輸入 `0.0.0.0/0`，對於目標 VPC 子網路 ID，選擇與 Client VPN 相關聯的子網路。
8. 新增授權規則讓用戶端存取網際網路。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟；對於目的地網路，輸入 `0.0.0.0/0`。
9. 確定 VPC 中資源的安全群組具有允許從與 Client VPN 端點關聯的安全群組存取的規則。這可讓您的用戶端存取 VPC 中的資源。

## 使用 AWS Client VPN client-to-client 訪問 C

此案例的設定可讓用戶端存取單一 VPC，並讓用戶端彼此路由傳送流量。如果連線到相同 Client VPN 端點的用戶端也需要彼此通訊，建議您使用此設定。當用戶端連線到 Client VPN 端點時，您可以使用從用戶端 CIDR 範圍指派給用戶端的唯一 IP 地址彼此通訊。



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別與 Client VPN 端點關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。
- 識別與 VPC CIDR 不重疊的用戶端 IP 地址適當的 CIDR 範圍。
- 於 [規則和最佳做法 AWS Client VPN](#) 檢閱 Client VPN 端點的規則和限制。

#### Note

在此案例中不支援使用 Active Directory 群組或 SAML 型 IdP 群組的網路授權規則。

### 實作此組態

1. 在與 VPC 相同的區域中建立 Client VPN 端點。若要執行此作業，請執行[建立 Client VPN 端點](#)中所述的步驟。
2. 將您稍早所識別的子網路與 Client VPN 端點建立關聯。若要執行此作業，請執行[建立目標網路與 Client VPN 端點的關聯](#)中所述的步驟，然後選取 VPC 和子網路。
3. 在路由表中新增路由至區域網路。若要執行此作業，請執行[建立端點路由](#)中所述的步驟。在路由傳送目的地中，輸入用戶端 CIDR 範圍，並在目標 VPC 子網路 ID 中指定 local。
4. 新增授權規則讓用戶端存取 VPC。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟。在要啟用的目的地網路中，輸入 VPC 的 IPv4 CIDR 範圍。



5. 新增授權規則，以讓用戶端存取用戶端 CIDR 範圍。若要執行此作業，請執行[將授權規則新增至 Client VPN 端點](#)中所述的步驟。在要啟用的目的地網路中，輸入用戶端的 CIDR 範圍。

## 使用 AWS Client VPN 限制存取您的網路

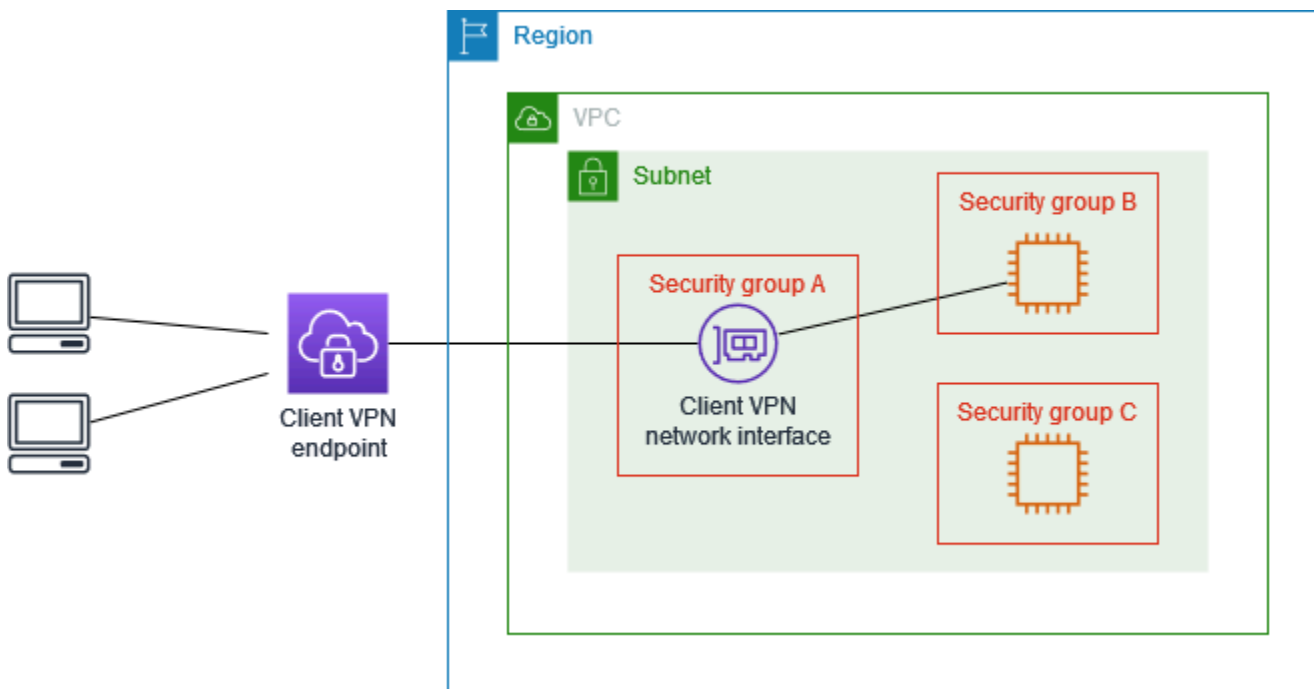
您可以設定您的 Client VPN 端點，限制對 VPC 中特定資源的存取。針對使用者類型身分驗證，您也可以根據存取 Client VPN 端點的使用者群組，將存取限制在一部分的網路。

### 使用安全群組限制存取

您可以透過新增或移除參考套用至目標網路關聯之安全群組 (Client VPN 安全群組) 的安全群組規則，來授與或拒絕 VPC 中特定資源的存取權。此組態闡明[使用 AWS Client VPN 存取 VPC](#)中所述的案例。除了該案例中設定的授權規則，還會套用此組態。

若要授與特定資源的存取權，請識別與執行資源的執行個體相關聯的安全群組。然後，建立允許來自 Client VPN 安全群組的流量的規則。

在下圖中，安全群組 A 是 Client VPN 安全群組，安全群組 B 與 EC2 執行個體相關聯，而安全群組 C 則與 EC2 執行個體相關聯。若您將規則新增至安全群組 B，允許來自安全群組 A 的存取權限，則用戶端可以存取與安全群組 B 關聯的執行個體。若安全群組 C 沒有規則允許來自安全群組 A 的存取權限，則用戶端無法存取與安全群組 C 關聯的執行個體。



開始之前，請先檢查 Client VPN 安全群組是否與 VPC 中的其他資源相關聯。如果您新增或移除參考 Client VPN 安全群組的規則，您可能也會授與或拒絕其他關聯資源的存取權。若要避免這種情況，請使用特別建立以搭配 Client VPN 端點使用的安全群組。

### 建立安全群組規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇與執行資源之執行個體相關聯的安全群組。
4. 選擇 Actions (動作)、Edit inbound rules (編輯傳入規則)。
5. 選擇 Add rule (新增規則)，然後執行下列動作：
  - 在 Type (類型) 中，選擇 All traffic (所有流量) 或您要允許的特定流量類型。
  - 在 Source (來源) 中，選擇 Custom (自訂)，然後輸入或選擇 Client VPN 安全群組的 ID。
6. 選擇 Save rules (儲存規則)

若要移除特定資源的存取權，請檢查與執行資源之執行個體相關聯的安全群組。如果規則允許來自 Client VPN 安全群組的流量，請將其刪除。

### 檢查安全群組規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)。
3. 選擇 Inbound Rules (傳入規則)。
4. 檢閱規則清單。如果有規則的 Source (來源) 是 Client VPN 安全群組，請選擇 Edit Rules (編輯規則)，然後選擇規則的 Delete (刪除) (x 圖示)。選擇 Save rules (儲存規則)。

## 根據使用者群組限制存取

如果您的 Client VPN 端點設定為使用者型的身分驗證，您可以授與特定使用者群組對網路特定部分的存取權。若要執行此動作，請執行下列步驟。

1. 在 AWS Directory Service 或您的 IdP 中設定使用者和群組。如需詳細資訊，請參閱下列主題：
  - [Active Directory 身分驗證](#)
  - [SAML 型聯合身分驗證的需求和考量](#)

2. 為您的 Client VPN 端點建立授權規則，以允許指定的群組存取全部或部分網路。如需更多詳細資訊，請參閱 [授權規則](#)。

如果您的 Client VPN 端點設定為進行交互身分驗證，則無法設定使用者群組。當您建立授權規則時，您必須將存取權授與所有使用者。若要讓特定使用者群組存取您的網路的特定部分，您可以建立多個 Client VPN 端點。例如，對於存取您網路的每個使用者群組，請執行下列動作：

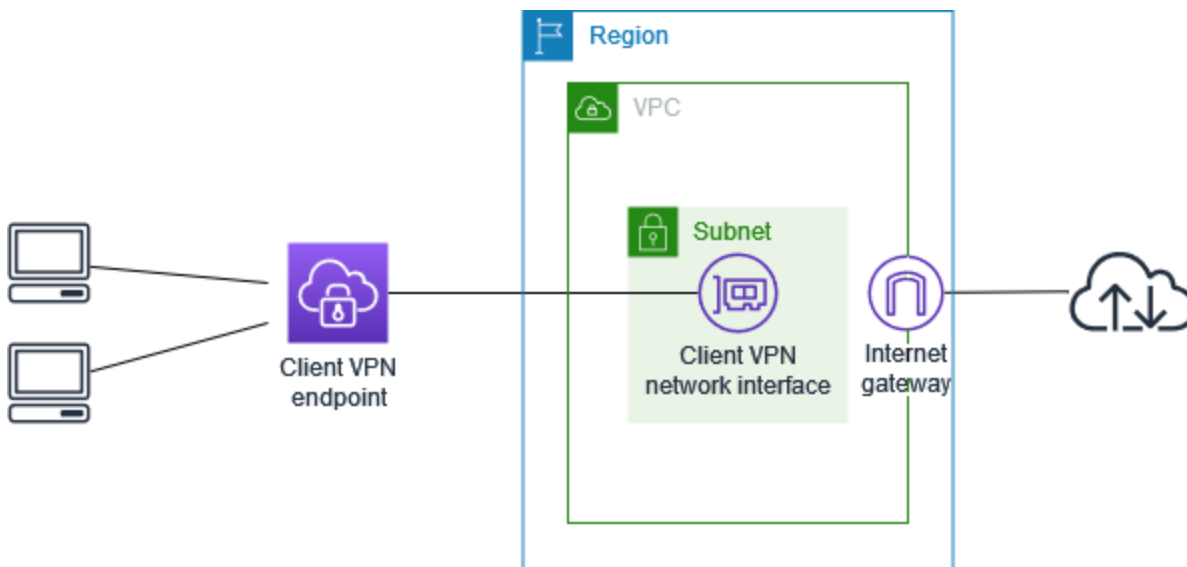
1. 為該使用者群組建立一組伺服器 and 用戶端憑證和金鑰。如需更多詳細資訊，請參閱 [交互身分驗證](#)。
2. 建立 Client VPN 端點。如需更多詳細資訊，請參閱 [建立 Client VPN 端點](#)。
3. 建立授權規則，授與全部或部分網路的存取權。例如，對於系統管理員所使用的 Client VPN 端點，您可以建立授權規則來授與整個網路的存取權。如需更多詳細資訊，請參閱 [將授權規則新增至 Client VPN 端點](#)。

# AWS Client VPN 入門

在本教學中，您將會建立執行下列作業的 Client VPN 端點：

- 提供所有用戶端對單一 VPC 的存取權。
- 提供所有用戶端存取網際網路。
- 使用[交互身分驗證](#)。

以下圖表顯示在您完成本教學後，VPC 和 Client VPN 端點的組態。



## 步驟

- [必要條件](#)
- [步驟 1：產生伺服器和用戶端憑證及金鑰](#)
- [步驟 2：建立 Client VPN 端點](#)
- [步驟 3：建立目標網路關聯](#)
- [步驟 4：新增 VPC 的授權規則](#)
- [步驟 5：提供對網際網路的存取權限](#)
- [步驟 6：驗證安全群組要求](#)
- [步驟 7：下載 Client VPN 端點組態檔案](#)
- [步驟 8：連線到 Client VPN 端點](#)

## 必要條件

開始本教學課程之前，請確定您有：

- 使用 Client VPN 端點的必要許可。
- 將憑證導入 AWS Certificate Manager 的許可。
- 具有至少一個子網路和一個網際網路閘道的 VPC。與子網路相關聯的路由表必須具有通往網際網路閘道的路由。

## 步驟 1：產生伺服器 and 用戶端憑證及金鑰

此教學課程使用交互身分驗證。透過交互身分驗證，Client VPN 使用憑證在用戶端和 Client VPN 端點之間執行身分驗證。您必須建立伺服器憑證和金鑰，以及至少一個用戶端憑證和金鑰。至少需要將伺服器憑證匯入 AWS Certificate Manager (ACM)，並在您建立 Client VPN 端點時指定。將客戶端憑證匯入 ACM 是選擇性的。

如果您還沒有使用於此用途的憑證，則可使用 OpenVPN easy-rsa 實用程序建立這些憑證。有關使用 [OpenVPN easy-rsa 實用程序](#) 產生伺服器 and 用戶端憑證及金鑰，然後將它們匯入 ACM 中的詳細步驟，請參閱 [交互身分驗證](#)。

### Note

伺服器憑證必須佈建或匯入相同的 AWS 區域內的 AWS Certificate Manager (ACM)，您將在此建立 Client VPN 端點。

## 步驟 2：建立 Client VPN 端點

Client VPN 端點是您為了啟用和管理 Client VPN 工作階段而建立及設定的資源。它是所有用戶端 VPN 工作階段的終止點。

### 建立 Client VPN 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 Client VPN Endpoints (Client VPN 端點)，然後選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。
3. (選用) 提供 Client VPN 端點的名稱標籤和說明。

- 對於 Client IPv4 CIDR (用戶端 IPv4 CIDR)，以 CIDR 標記法指定 IP 地址範圍，以從中指派用戶端 IP 地址。

#### Note

地址範圍不得與目標網路地址範圍、VPC 地址範圍或任何將與 Client VPN 端點關聯的路由重疊。用戶端地址範圍必須至少為 /22 且不大於 /12 CIDR 區塊大小。建立 Client VPN 端點後，您無法變用戶端地址範圍。

- 對於伺服器憑證 ARN，選取您在 [步驟 1](#) 中產生的伺服器憑證。
- 在 Authentication options (身分驗證選項) 下，選擇 Use mutual authentication (使用交互身分驗證)，然後對於 Client certificate ARN (用戶端憑證 ARN)，選取您想要使用為用戶端憑證的憑證 ARN。

如果伺服器和用戶端憑證是由同一家憑證授權機構 (CA) 所發行，則您可指定用戶端和伺服器憑證兩者的憑證 ARN。在這種情況下，與伺服器憑證對應的任何客戶端憑證均可用於進行身分驗證。

- 保留其他預設設定，然後選擇 Create Client VPN endpoint (建立 Client VPN 端點)。

在您建立 Client VPN 端點後，其狀態為 pending-associate。只有在您將至少一個目標網路相關聯後，用戶端才能建立 VPN 連接。

如需 Client VPN 端點可指定的選項詳細資訊，請參閱 [建立 Client VPN 端點](#)。

## 步驟 3：建立目標網路關聯

若要讓用戶端建立 VPN 工作階段，您必須將目標網路與 Client VPN 端點關聯。目標網路是 VPC 中的子網路。

建立目標網路與 Client VPN 端點的關聯

- 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
- 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
- 選取您在先前的步驟中所建立的 Client VPN 端點，然後選擇 Target network associations (目標網路關聯)、Associate target network (關聯目標網路)。
- 對於 VPC，選擇子網路所在的 VPC。

5. 對於 Choose a subnet to associate (選擇要關聯的子網路)，選擇要和 Client VPN 端點關聯的子網路。
6. 選擇 Associate target network (關聯目標網路)。
7. 如果授權規則允許，一個子網路關聯就足以讓用戶端存取 VPC 的整個網路。您可以關聯其他子網路，以在一個可用區域發生故障時提供高可用性。

當您將第一個子網路與 Client VPN 端點建立關聯時，會發生下列情況：

- Client VPN 端點的狀態會變更為 available。用戶端現在可以建立 VPN 連線，但在您新增授權規則之前，無法存取 VPC 中的任何資源。
- VPC 的本機路由會自動新增到 Client VPN 端點路由表。
- Client VPN 端點會自動套用 VPC 的預設安全群組。

## 步驟 4：新增 VPC 的授權規則

若要讓客戶端存取 VPC，Client VPN 終端節點的路由表中需要指向 VPC 的路由和授權規則。路由已經在上一個步驟中自動新增。在本教學課程中，我們想要將存取權授予所有使用者。

若要新增 VPC 的授權規則

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要新增授權規則的 Client VPN 端點。選擇 Authorization rules (授權規則)，然後選擇 Add authorization rule (新增授權規則)。
4. 對於 Destination network to enable access (要啟用存取權限的目的地網路)，請輸入您要允許存取之網路的 CIDR。例如，若要允許存取整個 VPC，請指定 VPC 的 IPv4 CIDR 區塊。
5. 在授與存取權限中，選擇允許所有使用者存取權限。
6. (選用) 對於 Description (描述)，輸入授權規則的簡短描述。
7. 選擇 Add authorization rule (新增授權規則)。

## 步驟 5：提供對網際網路的存取權限

您可以提供對與 VPC 相連的其他網路的存取，例如 AWS 服務、對等 VPC、現場部署網路和網際網路。對於每個額外的網路，您必須在 Client VPN 端點的路由表中新增到該網路的路由，並設定將存取權限授予用戶端的授權規則。

在本教程中，我們希望授予所有使用者對網際網路和 VPC 的存取權限。您已設定對 VPC 的存取權限，因此此步驟是用於存取網際網路。

### 提供對網際網路的存取

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您為本教學建立的 Client VPN 端點。選擇 Route Table (路由表)，然後選擇 Create Route (建立路由)。
4. 對於 Route destination (路由目的地)，輸入 `0.0.0.0/0`。對於 Subnet ID for target network association (目標網路關聯的子網路 ID)，指定路由流量經過的子網路的 ID。
5. 選擇 Create Route (建立路由)。
6. 選擇 Authorization rules (授權規則)，然後選擇 Add authorization rule (新增授權規則)。
7. 對於 Destination network to enable access (要啟用存取權限的目的地網路)，請輸入 `0.0.0.0/0`，然後選擇 Allow access to all users (允許所有使用者存取)。
8. 選擇 Add authorization rule (新增授權規則)。

## 步驟 6：驗證安全群組要求

在本教程中，在步驟 2 中建立 Client VPN 端點時並未指定任何安全群組。這意味著當目標網路關聯時，VPC 的預設安全群組會自動套用到 Client VPN 端點。因此，VPC 的預設安全群組現在應該與 Client VPN 端點關聯。

### 驗證下列安全群組要求

- 與您路由流量經過的子網路關聯的安全群組 (在本例中為預設 VPC 安全群組) 允許傳出流量傳入網際網路。為此，請新增允許所有流量傳入目的地 `0.0.0.0/0` 的傳出規則。
- VPC 中資源的安全群組有一條規則，允許從套用至 Client VPN 端點的安全群組 (在此例中為預設的 VPC 安全群組) 進行存取。這可讓您的用戶端存取 VPC 中的資源。



如需詳細資訊，請參閱 [安全群組](#)。

## 步驟 7：下載 Client VPN 端點組態檔案

下一個步驟是下載和準備 Client VPN 端點組態檔案。組態檔案包含 Client VPN 端點詳細資訊，以及建立 VPN 連接所需的憑證資訊。您可以提供此檔案給需要連線到 Client VPN 端點的最終使用者。最終使用者使用該檔案來設定其 VPN 用戶端應用程式。

### 下載及準備 Client VPN 端點組態檔案

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您為本教學建立的 Client VPN 端點，然後選擇 Download client configuration (下載用戶端組態)。
4. 找出 [步驟 1](#) 中產生的用戶端憑證和金鑰。在複製的 OpenVPN easy-rsa 儲存庫的下列位置中，可以找到用戶端憑證和金鑰：
  - 用戶端憑證：easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt
  - 用戶端金鑰：easy-rsa/easyrsa3/pki/private/client1.domain.tld.key
5. 使用您偏好的文字編輯器開啟 Client VPN 端點組態檔案。將 `<cert></cert>` 和 `<key></key>` 標籤新增至檔案中。將用戶端憑證的內容和私有金鑰的內容放在相應的標籤之間，如下所示：

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. 儲存並關閉 Client VPN 端點組態檔案。
7. 將 Client VPN 端點組態檔案分配給您的最終使用者。

如需 Client VPN 端點組態檔案的詳細資訊，請參閱 [匯出和設定用戶端組態檔](#)。

## 步驟 8：連線到 Client VPN 端點

您可以使用 AWS 提供的用戶端或其他 OpenVPN 類型的用戶端應用程式，以及您剛建立的組態檔案來連線到 Client VPN 端點。如需詳細資訊，請參閱 [《AWS Client VPN 使用者指南》](#)。

# 使用 AWS Client VPN

下列主題說明如何使用 Client VPN。

## 目錄

- [存取自助式入口網站](#)
- [授權規則](#)
- [用戶端憑證撤銷清單](#)
- [用戶端連線](#)
- [用戶端登入橫幅](#)
- [Client VPN 端點](#)
- [使用連線日誌](#)
- [匯出和設定用戶端組態檔](#)
- [路由](#)
- [目標網路](#)
- [VPN 工作階段最長持續時間](#)

## 存取自助式入口網站

如已為 Client VPN 端點啟用自助式入口網站，您可以為用戶端提供自助式入口網站的 URL。用戶端可以在 web 瀏覽器中存取入口網站，並使用自己的使用者型登入資料登入。在入口網站中，用戶端可以下載 Client VPN 端點組態檔案，也可以下載 AWS 提供的用戶端最新版本。

適用的規定如下：

- 使用交互身分驗證進行身分驗證的用戶端無法使用自助式入口網站。
- 自助式入口網站所提供的組態檔案，與您使用 Amazon VPC 主控台或 AWS CLI 匯出的組態檔案相同。如果您需要先自訂組態檔案，再發佈給用戶端，您即必須自行將此自訂的檔案發佈給用戶端。
- 您必須啟用 Client VPN 端點的自助式入口網站選項，否則用戶端無法存取入口網站。如未啟用此選項，您可以修改 Client VPN 端點以啟用選項。

啟用自助式入口網站選項之後，請為用戶端提供下列其中一個 URL：

- <https://self-service.clientvpn.amazonaws.com/>

如果用戶端使用此 URL 存取入口網站，其必須先輸入 Client VPN 端點的 ID，才能登入。

- <https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>>

使用您 Client VPN 端點的 ID (例如 cvpn-endpoint-0123456abcd123456) 取代前述 URL 中的 `<## id>`。

您也可以從 [describe-client-vpn-endpoints](#) AWS CLI 命令的輸出中檢視自助式入口網站的 URL。或者，您可從 Amazon VPC 主控台中 Client VPN Endpoints (Client VPN 端點) 頁面的 Details (詳細資訊) 索引標籤中取得 URL。

如需設定自助式入口網站搭配聯合身分驗證使用的詳細資訊，請參閱 [自助入口網站支援](#)。

## 授權規則

授權規則做為授與存取網路的防火牆規則。透過新增授權規則，您可以授與特定的用戶端存取至指定的網路。您應該要有每個欲授與存取權之網路的授權規則。您可以使用主控台和 AWS CLI，將授權規則新增至 Client VPN 端點。

### Note

評估授權規則時，Client VPN 會使用最長字首比對。請參閱 [《Amazon VPC 使用者指南》](#) 中的故障診斷主題 [Active Directory 群組的授權規則未如預期般運作](#) 和路由優先順序以取得更多詳細資訊。

## 目錄

- [將授權規則新增至 Client VPN 端點](#)
- [從 Client VPN 端點移除授權規則](#)
- [檢視授權規則](#)
- [授權規則的範例案例](#)

## 將授權規則新增至 Client VPN 端點

使用 AWS Management Console 將授權規則新增至 Client VPN 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 Client VPN Endpoints (Client VPN 端點)。
  3. 選取要新增授權規則的 Client VPN 端點，選擇 Authorization rules (授權規則)，然後選擇 Add authorization rule (新增授權規則)。
  4. 對於 Destination network to enable access (要啟用存取權限的目的地網路)，請以 CIDR 標記法輸入您希望使用者存取的網路 IP 地址 (例如 VPC 的 CIDR 區塊)。
  5. 指定允許哪些用戶端存取指定的網路。對於 For grant access to (將存取權授與)，請執行以下其中一項：
    - 若准許所有用戶端存取，請選擇 Allow access to all users (允許所有使用者存取)。
    - 若要限制特定用戶端的存取權，請選擇 Allow access to users in a specific access group (允許特定存取群組中使用者的存取權)，然後在 Access group ID (存取群組 ID) 中，輸入要授與存取權的群組 ID。例如，Active Directory 群組的安全性識別符 (SID)，或在 SAML 型身分提供者 (IdP) 中定義的群組 ID/名稱。
      - (Active Directory) 若要取得 SID，您可以使用 Microsoft Powershell [Get-ADGroup](#) cmdlet，例如：
- ```
Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
```
- 或者，開啟 Active Directory 使用者和電腦工具，檢視群組的內容，移至「屬性編輯器」索引標籤，然後取得 objectSID 的值。如有必要，請先選擇檢視、進階功能以啟用「屬性編輯器」標籤。
- (SAML 型聯合身分驗證) 群組 ID/名稱應與 SAML 聲明中傳回的群組屬性資訊相符。
6. 對於 Description (描述)，輸入授權規則的簡短描述。
  7. 選擇 Add authorization rule (新增授權規則)。

將授權規則新增至用戶端 VPN 端點 (AWS CLI)

使用 [authorize-client-vpn-ingress](#) 命令。

## 從 Client VPN 端點移除授權規則

透過刪除授權規則，您可以移除對指定網路的存取權。

您可以使用主控台和 AWS CLI，從 Client VPN 端點移除授權規則。

## 從 Client VPN 端點移除授權規則 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取已新增授權規則的 Client VPN 端點，然後選擇 Authorization rule (授權規則)。
4. 選取要刪除的授權規則，選擇 Remove authorization rule (移除授權規則)，然後選擇 Remove authorization rule (移除授權規則)。

## 從 Client VPN 端點移除授權規則 (AWS CLI)

使用 [revoke-client-vpn-ingress](#) 命令。

## 檢視授權規則

您可以使用主控台和 AWS CLI 檢視特定 Client VPN 端點的授權規則。

### 檢視授權規則 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要檢視授權規則的 Client VPN 端點，然後選擇 Authorization rules (授權規則)。

### 檢視授權規則 (AWS CLI)

使用 [describe-client-vpn-authorization-rules](#) 命令。

## 授權規則的範例案例

本節說明 AWS Client VPN 授權規則的運作方式。其中包括了解授權規則的要點、範例架構，以及對應至範例架構的範例案例討論。

### 目錄

- [了解授權規則的要點](#)
- [授權規則案例的範例架構](#)
- [案例 1：存取單一目的地](#)
- [案例 2：使用任何目的地 \(0.0.0.0/0\) CIDR](#)

- [案例 3：較長 IP 字首相符](#)
- [案例 4：重疊 CIDR \(相同群組\)](#)
- [案例 5：其他 0.0.0.0/0 規則](#)
- [案例 6：新增 192.168.0.0/24 的規則](#)
- [案例 7：所有使用者群組的存取權](#)

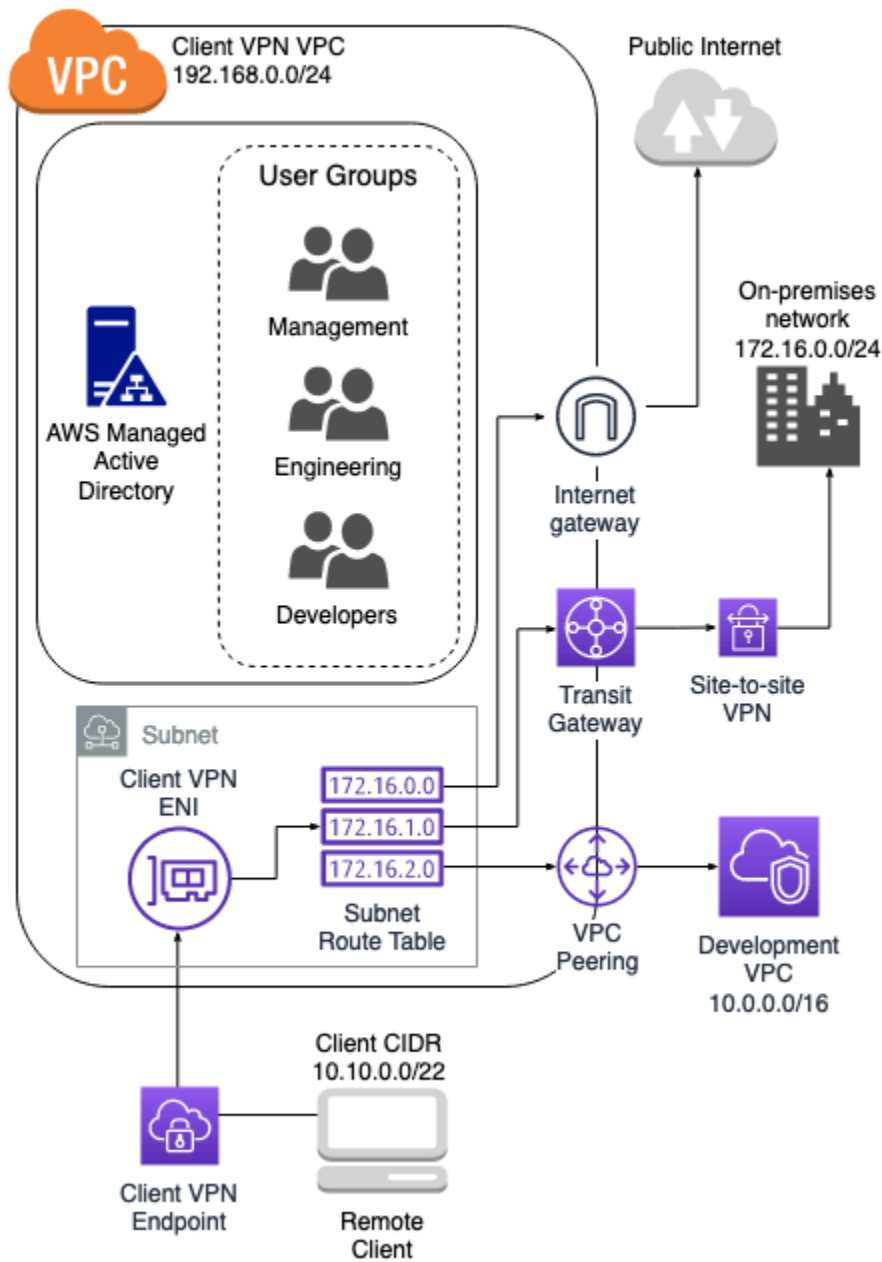
## 了解授權規則的要點

以下幾點解釋了授權規則的一些行為：

- 若要允許存取目的地網路，必須明確新增授權規則。預設行為是拒絕存取。
- 您無法將授權規則新增至限制存取目的地網路。
- 0.0.0.0/0 CIDR 會作為特殊情況來處理。不論建立授權規則的順序為何，這都是最後處理。
- 0.0.0.0/0 CIDR 可以被視為「任何目的地」或「未由其他授權規則定義的任何目的地」。
- 最長字首相符是優先執行的規則。

## 授權規則案例的範例架構

下圖顯示用於本節中範例案例的範例架構。



### 案例 1：存取單一目的地

| 規則說明           | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR      |
|----------------|-----------|-----------|---------------|
| 提供工程群組存取內部部署網路 | S-xxxxx14 | False     | 172.16.0.0/24 |



| 規則說明                     | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR       |
|--------------------------|-----------|-----------|----------------|
| 提供開發群組存取開發 VPC           | S-xxxxx15 | False     | 10.0.0.0/16    |
| 提供管理員群組存取 Client VPN VPC | S-xxxxx16 | False     | 192.168.0.0/24 |

### 產生行為

- 工程群組只能存取 172.16.0.0/24。
- 開發群組只能存取 10.0.0.0/16。
- 管理員群組只能存取 192.168.0.0/24。
- 所有其他流量都會由 Client VPN 端點捨棄。

#### Note

在這個案例中，沒有使用者群組可以存取公有網際網路。

### 案例 2：使用任何目的地 (0.0.0.0/0) CIDR

| 規則說明           | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR      |
|----------------|-----------|-----------|---------------|
| 提供工程群組存取內部部署網路 | S-xxxxx14 | False     | 172.16.0.0/24 |
| 提供開發群組存取開發 VPC | S-xxxxx15 | False     | 10.0.0.0/16   |
| 提供管理員群組存取任何目的地 | S-xxxxx16 | False     | 0.0.0.0/0     |

## 產生行為

- 工程群組只能存取 172.16.0.0/24。
- 開發群組只能存取 10.0.0.0/16。
- 管理員群組可以存取公有網際網路和 192.168.0.0/24，但無法存取 172.16.0.0/24 或 10.0.0.0/16。

### Note

在這個案例中，因為沒有任何規則參考 192.168.0.0/24，對該網路的存取也由 0.0.0.0/0 規則提供。

無論規則的建立順序為何，包含 0.0.0.0/0 的規則一律最後評估。因此，請記住，在 0.0.0.0/0 之前評估的規則，會在決定 0.0.0.0/0 存取授予哪些網路方面發揮作用。

## 案例 3：較長 IP 字首相符

| 規則說明                   | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR      |
|------------------------|-----------|-----------|---------------|
| 提供工程群組存取內部部署網路         | S-xxxxx14 | False     | 172.16.0.0/24 |
| 提供開發群組存取開發 VPC         | S-xxxxx15 | False     | 10.0.0.0/16   |
| 提供管理員群組存取任何目的地         | S-xxxxx16 | False     | 0.0.0.0/0     |
| 提供管理員群組存取開發 VPC 中的單一主機 | S-xxxxx16 | False     | 10.0.0.55/32  |

## 產生行為

- 工程群組只能存取 172.16.0.0/24。
- 開發群組可以存取 10.0.0.0/16，除了單一主機 10.0.2.119/32。
- 管理員群組可以存取公有網際網路 192.168.0.0/24 以及開發 VPC 內的單一主機 (10.0.2.119/32)，但無法存取 172.16.0.0/24 或開發 VPC 中的其餘主機。

### Note

在這裡，您會看到具有較長 IP 字首的規則如何優先於具有較短 IP 字首的規則。如果您希望開發群組可以存取 10.0.2.119/32，則需新增授予開發團隊存取 10.0.2.119/32 的額外規則。

## 案例 4：重疊 CIDR (相同群組)

| 規則說明                   | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR        |
|------------------------|-----------|-----------|-----------------|
| 提供工程群組存取內部部署網路         | S-xxxxx14 | False     | 172.16.0.0/24   |
| 提供開發群組存取開發 VPC         | S-xxxxx15 | False     | 10.0.0.0/16     |
| 提供管理員群組存取任何目的地         | S-xxxxx16 | False     | 0.0.0.0/0       |
| 提供管理員群組存取開發 VPC 中的單一主機 | S-xxxxx16 | False     | 10.0.0.55/32    |
| 提供工程群組存取內部部署網路中較小的子網路  | S-xxxxx14 | False     | 172.16.0.128/25 |

## 產生行為

- 開發群組可以存取 10.0.0.0/16，除了單一主機 10.0.2.119/32。
- 管理員群組可以存取公有網際網路 192.168.0.0/24 以及 10.0.0.0/16 網路內的單一主機 (10.0.2.119/32)，但無法存取 172.16.0.0/24 或 10.0.0.0/16 網路中的其餘主機。
- 工程群組可存取 172.16.0.0/24，包括更明確的子網路 172.16.0.128/25。

## 案例 5：其他 0.0.0.0/0 規則

| 規則說明                   | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR        |
|------------------------|-----------|-----------|-----------------|
| 提供工程群組存取內部部署網路         | S-xxxxx14 | False     | 172.16.0.0/24   |
| 提供開發群組存取開發 VPC         | S-xxxxx15 | False     | 10.0.0.0/16     |
| 提供管理員群組存取任何目的地         | S-xxxxx16 | False     | 0.0.0.0/0       |
| 提供管理員群組存取開發 VPC 中的單一主機 | S-xxxxx16 | False     | 10.0.0.55/32    |
| 提供工程群組存取內部部署網路中較小的子網路  | S-xxxxx14 | False     | 172.16.0.128/25 |
| 提供工程群組存取任何目的地          | S-xxxxx14 | False     | 0.0.0.0/0       |

## 產生行為

- 開發群組可以存取 `10.0.0.0/16`，除了單一主機 `10.0.2.119/32`。
- 管理員群組可以存取公有網際網路 `192.168.0.0/24` 以及 `10.0.0.0/16` 網路內的單一主機 (`10.0.2.119/32`)，但無法存取 `172.16.0.0/24` 或 `10.0.0.0/16` 網路中的其餘主機。
- 工程群組可以存取公有網際網路 `192.168.0.0/24` 以及 `172.16.0.0/24`，包括更明確的子網路 `172.16.0.128/25`。

### Note

請注意，工程和管理員群組現在都可以存取 `192.168.0.0/24`。這是因為兩個群組都可以存取 `0.0.0.0/0` (任何目的地) 且沒有其他規則正在參考 `192.168.0.0/24`。

## 案例 6：新增 `192.168.0.0/24` 的規則

| 規則說明                   | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR        |
|------------------------|-----------|-----------|-----------------|
| 提供工程群組存取內部部署網路         | S-xxxxx14 | False     | 172.16.0.0/24   |
| 提供開發群組存取開發 VPC         | S-xxxxx15 | False     | 10.0.0.0/16     |
| 提供管理員群組存取任何目的地         | S-xxxxx16 | False     | 0.0.0.0/0       |
| 提供管理員群組存取開發 VPC 中的單一主機 | S-xxxxx16 | False     | 10.0.0.55/32    |
| 提供工程群組存取內部部署網路中的子網路    | S-xxxxx14 | False     | 172.16.0.128/25 |

| 規則說明                     | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR       |
|--------------------------|-----------|-----------|----------------|
| 提供工程群組存取任何目的地            | S-xxxxx14 | False     | 0.0.0.0/0      |
| 提供管理員群組存取 Client VPN VPC | S-xxxxx16 | False     | 192.168.0.0/24 |

### 產生行為

- 開發群組可以存取 10.0.0.0/16，除了單一主機 10.0.2.119/32。
- 管理員群組可以存取公有網際網路 192.168.0.0/24 以及 10.0.0.0/16 網路內的單一主機 (10.0.2.119/32)，但無法存取 172.16.0.0/24 或 10.0.0.0/16 網路中的其餘主機。
- 工程組可以存取公有網際網路 172.16.0.0/24 以及 172.16.0.128/25。

#### Note

請注意，為管理員群組新增存取 192.168.0.0/24 的規則如何導致開發群組不再具有該目的地網路的存取權限。

### 案例 7：所有使用者群組的存取權

| 規則說明           | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR      |
|----------------|-----------|-----------|---------------|
| 提供工程群組存取內部部署網路 | S-xxxxx14 | False     | 172.16.0.0/24 |
| 提供開發群組存取開發 VPC | S-xxxxx15 | False     | 10.0.0.0/16   |
| 提供管理員群組存取任何目的地 | S-xxxxx16 | False     | 0.0.0.0/0     |

| 規則說明                     | 群組 ID     | 允許所有使用者存取 | 目的地 CIDR        |
|--------------------------|-----------|-----------|-----------------|
| 提供管理員群組存取開發 VPC 中的單一主機   | S-xxxxx16 | False     | 10.0.0.55/32    |
| 提供工程群組存取內部部署網路中的子網路      | S-xxxxx14 | False     | 172.16.0.128/25 |
| 提供工程群組存取所有網路             | S-xxxxx14 | False     | 0.0.0.0/0       |
| 提供管理員群組存取 Client VPN VPC | S-xxxxx16 | False     | 192.168.0.0/24  |
| 提供所有群組的存取權               | N/A       | True      | 0.0.0.0/0       |

## 產生行為

- 開發群組可以存取 10.0.0.0/16，除了單一主機 10.0.2.119/32。
- 管理員群組可以存取公有網際網路 192.168.0.0/24 以及 10.0.0.0/16 網路內的單一主機 (10.0.2.119/32)，但無法存取 172.16.0.0/24 或 10.0.0.0/16 網路中的其餘主機。
- 工程組可以存取公有網際網路 172.16.0.0/24 以及 172.16.0.128/25。
- 任何其他使用者群組 (例如「admin group」) 都可以存取公有網際網路，但不能存取其他規則中定義的任何其他目的地網路。

## 用戶端憑證撤銷清單

您可以使用用戶端憑證撤銷清單來撤銷特定用戶端憑證對 Client VPN 端點的存取權。

**Note**

如需有關產生伺服器 and 用戶端憑證及金鑰的詳細資訊，請參閱 [交互身分驗證](#)

如需可新增至用戶端憑證撤銷清單的項目數詳細資訊，請參閱 [Client VPN 配額](#)。

## 目錄

- [產生用戶端憑證撤銷清單](#)
- [匯入用戶端憑證撤銷清單](#)
- [匯出用戶端憑證撤銷清單](#)

## 產生用戶端憑證撤銷清單

### Linux/macOS

在下列程序中，您可以使用 OpenVPN easy-rsa 命令列公用程式產生用戶端憑證撤銷清單。

使用 OpenVPN easy-rsa 產生用戶端憑證撤銷清單

1. 登入用於產生憑證之託管 easyrsa 安裝的伺服器。
2. 導覽到本機儲存庫中的 easy-rsa/easyrsa3 資料夾。

```
$ cd easy-rsa/easyrsa3
```

3. 撤銷用戶端憑證並產生用戶端撤銷清單。

```
$ ./easyrsa revoke client1.domain.tld  
$ ./easyrsa gen-crl
```

出現提示時，輸入 yes。

### Windows

下列程序會使用 OpenVPN 軟體來產生用戶端撤銷清單。它假設您遵循 [使用 OpenVPN 軟體的步驟](#) 來產生用戶端和伺服器憑證和金鑰。



## 使用 EasyRSA 版本 3.x.x 產生用戶端憑證撤銷清單

1. 開啟命令提示並巡覽至 EasyRSA-3.x.x 目錄，此目錄為在您的系統上安裝的位置。

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. 執行「EasyRSA-Start.bat」檔案，開始 EasyRSA shell。

```
C:\> .\EasyRSA-Start.bat
```

3. 在 EasyRSA shell 中，撤銷用戶端憑證。

```
# ./easyrsa revoke client_certificate_name
```

4. 出現提示時，輸入「是」。

5. 產生用戶端撤銷清單。

```
# ./easyrsa gen-crl
```

6. 系統會在下列位置建立用戶端撤銷清單：

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

## 使用 EasyRSA 版本產生用戶端憑證撤銷清單

1. 開啟命令提示，然後導覽至 OpenVPN 目錄。

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. 執行 vars.bat 檔案。

```
C:\> vars
```

3. 撤銷用戶端憑證並產生用戶端撤銷清單。

```
C:\> revoke-full client_certificate_name  
C:\> more crl.pem
```

## 匯入用戶端憑證撤銷清單

您必須有可匯入的用戶端憑證撤銷清單檔案。如需有關產生用戶端憑證撤銷清單的詳細資訊，請參閱[產生用戶端憑證撤銷清單](#)。

您可以使用主控台和 AWS CLI 來匯入用戶端憑證撤銷清單。

### 匯入用戶端憑證撤銷清單 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要匯入用戶端憑證撤銷清單的 Client VPN 端點。
4. 選擇 Actions (動作)，然後選擇 Import Client Certificate CRL (匯入用戶端憑證 CRL)。
5. 對於 Certificate Revocation List (憑證撤銷清單)，輸入用戶端憑證撤銷清單檔案的內容，然後選擇 Import client certificate CRL (匯入用戶端憑證 CRL)。

### 匯入用戶端憑證撤銷清單 (AWS CLI)

使用 [import-client-vpn-client-certificate-revocation-list](#) 命令。

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --region region
```

## 匯出用戶端憑證撤銷清單

您可以使用主控台和 AWS CLI 來匯出用戶端憑證撤銷清單。

### 匯出用戶端憑證撤銷清單 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要匯出用戶端憑證撤銷清單的 Client VPN 端點。
4. 選擇 Actions (動作)，選擇 Export Client Certificate CRL (匯出用戶端憑證 CRL)，然後選擇 Export Client Certificate CRL (匯出用戶端憑證 CRL)。

### 匯出用戶端憑證撤銷 (AWS CLI)

使用 [export-client-vpn-client-certificate-revocation-list](#) 命令。

## 用戶端連線

連線是用戶端已建立的 VPN 工作階段。用戶端成功連線到 Client VPN 端點時，即表示已建立連線。

### 目錄

- [查看用戶端連線](#)
- [終止用戶端連線](#)

## 查看用戶端連線

您可以使用主控台和 AWS CLI 來檢視用戶端連線。連線資訊包括從用戶端 CIDR 範圍指派的 IP 位址。

### 查看用戶端連線 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要檢視用戶端連線的 Client VPN 端點。
4. 選擇 Connections (連線) 索引標籤。Connections (連線) 索引標籤列出所有作用中和已終止的用戶端連線。

### 查看用戶端連線 (AWS CLI)

使用 [describe-client-vpn-connections](#) 命令。

## 終止用戶端連線

當您終止用戶端連線時，VPN 工作階段會結束。

您可以使用主控台和 AWS CLI 來終止用戶端連線。

### 終止用戶端連線 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取用戶端要連線的 Client VPN 端點，然後選擇 Connections (連線)。

4. 選取要終止的連線，選擇 Terminate Connection (終止連線)，然後選擇 Terminate Connection (終止連線)。

### 終止用戶端連線 (AWS CLI)

使用 [terminate-client-vpn-connections](#) 命令。

## 用戶端登入橫幅

AWS Client VPN 提供了在 AWS 提供的 Client VPN 桌面應用程式上顯示文字橫幅的選項 (當系統建立了 VPN 工作階段時)。您可以定義文字橫幅的內容來滿足法規與合規的需求。最多可以使用 1400 個 UTF-8 編碼字元。

### Note

啟用了用戶端登入橫幅後，橫幅僅會顯示在新建立的 VPN 工作階段上。現有 VPN 工作階段不會中斷，但此橫幅會在重新建立現有工作階段時顯示。

請參閱《AWS Client VPN 使用者指南》中的「[AWS 提供的用戶端版本備註](#)」，瞭解用戶端桌面應用程式的詳細資訊。

### 目錄

- [設定建立 Client VPN 端點期間的用戶端登入橫幅](#)
- [設定現有 Client VPN 端點的用戶端登入橫幅](#)
- [停用現有 Client VPN 端點的用戶端登入橫幅](#)
- [修改 Client VPN 端點上的現有橫幅文字](#)
- [檢視當前設定的登入橫幅](#)

## 設定建立 Client VPN 端點期間的用戶端登入橫幅

如需啟用建立 Client VPN 端點期間的用戶端登入橫幅之詳細步驟，請參閱 [建立 Client VPN 端點](#)。

## 設定現有 Client VPN 端點的用戶端登入橫幅

使用下列步驟，設定現有 Client VPN 端點的用戶端登入橫幅。

## 啟用 Client VPN 端點 (主控台) 上的用戶端登入橫幅

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要修改的 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 向下捲動頁面到 Other parameters (其他參數) 區段。
5. 開啟 Enable client login banner (啟用用戶端登入橫幅)。
6. 對於 Client Login Banner Text (用戶端登入橫幅文字)，輸入當系統建立 VPN 工作階段時會在 AWS 提供的用戶端的橫幅中顯示的文字。僅限使用 UTF-8 編碼字元，最多允許 1400 個字元。
7. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

## 啟用 Client VPN 端點 (AWS CLI) 上的用戶端登入橫幅

使用 [modify-client-vpn-endpoint](#) 命令。

## 停用現有 Client VPN 端點的用戶端登入橫幅

使用下列步驟，停用現有 Client VPN 端點的用戶端登入橫幅。

### 停用 Client VPN 端點 (主控台) 上的用戶端登入橫幅

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要修改的 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 向下捲動頁面到 Other parameters (其他參數) 區段。
5. 關閉 Enable client login banner? (啟用用戶端登入橫幅?)。
6. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

### 停用 Client VPN 端點 (AWS CLI) 上的用戶端登入橫幅

使用 [modify-client-vpn-endpoint](#) 命令。

## 修改 Client VPN 端點上的現有橫幅文字

使用下列步驟修改用戶端登入橫幅上的現有文字。

## 修改 Client VPN 端點 (主控台) 上的現有橫幅文字

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要修改的 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 對於 Enable client login banner? (啟用用戶端登入橫幅?)，驗證它是否已開啟。
5. 對於 Client login banner text (用戶端登入橫幅文字)，以您想要在 AWS 提供的用戶端的橫幅中顯示的全新文字來取代現有文字 (當系統建立了 VPN 工作階段)。僅限使用 UTF-8 編碼字元，上限為 1400 個字元。
6. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

## 修改 Client VPN 端點 (AWS CLI) 上的用戶端登入橫幅

使用 [modify-client-vpn-endpoint](#) 命令。

## 檢視當前設定的登入橫幅

使用下列步驟檢視目前設定的登入橫幅。

### 檢視 Client VPN 端點 (主控台) 的目前登入橫幅

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要檢視的 Client VPN 端點。
4. 請確認選取了 Details (詳細資訊) 索引標籤。
5. 檢視 Client login banner text (用戶端登入橫幅文字) 旁目前設定的登入橫幅文字。

### 檢視 Client VPN 端點 (AWS CLI) 目前設定的登入橫幅

使用 [describe-client-vpn-endpoints](#) 命令。

## Client VPN 端點

所有用戶端的 VPN 工作階段都會在 Client VPN 端點終止。請設定 Client VPN 端點來管理和控制所有用戶端的 VPN 工作階段。

## 目錄

- [建立 Client VPN 端點。](#)
- [修改 Client VPN 端點](#)
- [檢視 Client VPN 端點](#)
- [建立 Client VPN 端點](#)

## 建立 Client VPN 端點。

建立 Client VPN 端點，讓您的用戶端建立 VPN 工作階段。

您必須在佈建所需目標網路的同一個 AWS 帳戶中建立 Client VPN。

### 必要條件

開始之前，請務必備妥下列項目：

- 檢閱[規則和最佳做法 AWS Client VPN](#)中的規則和限制。
- 產生伺服器憑證，並視需要取得用戶端憑證。如需詳細資訊，請參閱[用戶端身分驗證](#)。

### 建立 Client VPN 端點 (主控台)

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 Client VPN Endpoints (Client VPN 端點)，然後選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。
3. (選用) 提供 Client VPN 端點的名稱標籤和說明。
4. 對於 Client IPv4 CIDR (用戶端 IPv4 CIDR)，以 CIDR 標記法指定 IP 地址範圍，以從中指派用戶端 IP 地址。例如，10.0.0.0/22。

#### Note

IP 地址範圍不可以與目標網路或任何將與 Client VPN 端點建立關聯的路由重疊。用戶端地址範圍必須至少為 /22 且不大於 /12 CIDR 區塊大小。建立 Client VPN 端點後，您無法變用戶端地址範圍。

5. 對於 Server certificate ARN (伺服器憑證 ARN)，指定要由伺服器使用的 TLS 憑證的 ARN。用戶端使用伺服器憑證來對其連線的 Client VPN 端點進行身分驗證。

**Note**

伺服器憑證必須在您要建立 Client VPN 端點的區域中之 AWS Certificate Manager (ACM) 中存在。憑證可以使用 ACM 佈建，也可以匯入至 ACM。

6. 指定當用戶端建立 VPN 連接時，用來驗證用戶端的身分驗證方法。您必須選取身分驗證方法。
  - 若要使用使用者型身分驗證，請選取 Use user-based authentication (使用使用者型身分驗證)，然後選擇下列其中一項：
    - Active Directory authentication (Active Directory 身分驗證)：為 Active Directory 身分驗證選擇此選項。針對 Directory ID (目錄 ID)，指定要使用的 Active Directory ID。
    - Federated authentication (聯合身分驗證)：為 SAML 型聯合身分驗證選擇此選項。

若為 SAML provider ARN (SAML 提供者 ARN)，請指定 IAM SAML 身分提供者的 ARN。

(選用) 在 Self-service SAML provider ARN (自助式 SAML 提供者 ARN) 中指定您為 [支援自助式入口網站](#) 所建立之 IAM SAML 身分提供者的 ARN (如果適用)。
  - 若要使用交互憑證驗證，請選取 Use mutual authentication (使用交互身分驗證)，然後對於 Client certificate ARN (用戶端憑證 ARN)，指定於 AWS Certificate Manager (ACM) 中佈建的用戶端憑證 ARN。

**Note**

如果伺服器和用戶端憑證是由同一家憑證授權機構 (CA) 所發行，則您可同時為伺服器和用戶端使用伺服器憑證 ARN。如果用戶端憑證是由不同的 CA 發出，則應該指定用戶端憑證 ARN。

7. (選擇性) 對於連線記錄，請指定是否使用 Amazon CloudWatch logs 記錄有關用戶端連線的資料。開啟 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。在 CloudWatch 錄檔記錄群組名稱中，輸入要使用的記錄群組名稱。對於 CloudWatch 記錄檔資料流名稱，請輸入要使用的記錄串流名稱，或將此選項保留空白，讓我們為您建立記錄資料流。
8. (選用) 對於 Client Connect Handler (用戶端連線處理常式)，開啟 Enable client connect handler (啟用用戶端連線處理常式) 以執行自訂程式碼，允許或拒絕新的 Client VPN 端點連線。在 Client Connect Handler ARN (用戶端連線處理常式 ARN) 中指定 Lambda 函數的 Amazon 資源名稱 (ARN)，此函數包含允許或拒絕連線的邏輯。




9. (選用) 指定哪些 DNS 伺服器要用於 DNS 解析。若要使用自訂 DNS 伺服器，對於 DNS Server 1 IP address (DNS 伺服器 1 IP 地址)和 DNS Server 2 IP address (DNS 伺服器 2 IP 地址)，請指定要使用的 DNS 伺服器 IP 地址。若要使用 VPC DNS 伺服器，對於 DNS Server 1 IP address (DNS 伺服器 1 IP 地址)或 DNS Server 2 IP address (DNS 伺服器 2 IP 地址)，請指定 IP 地址，並新增 VPC DNS 伺服器 IP 地址。

 Note

請確定用戶端可以觸達 DNS 伺服器。

10. (選用) 根據預設，Client VPN 端點會使用 UDP 傳輸協定。若要改用 TCP 傳輸通訊協定，對於 Transport Protocol (傳輸通訊協定)，請選擇 TCP。

 Note

UDP 的效能通常比 TCP 更好。建立 Client VPN 端點之後，即無法變更傳輸協定。

11. (選用) 若要讓端點成為分割通道 Client VPN 端點，請開啟 Enable split-tunnel (啟用分割通道)。根據預設，Client VPN 端點上的分割通道會停用。
12. (選用) 請為 VPC ID 選擇要與 Client VPN 端點建立關聯的 VPC。Security Group IDs (安全群組識別碼) 請選擇一或多個要套用至 Client VPN 端點的 VPC 安全群組。
13. (選用) 對於 VPN port (VPN 連接埠)，請選擇 VPN 連接埠號碼。預設為 443。
14. (選用) 若要產生用戶端的 [自助式入口網站 URL](#)，請選擇 Enable self-service portal (啟用自助式入口網站)。
15. (選用) 對於 Session timeout hours (工作階段逾時時數)，從可用選項中選擇所需的 VPN 工作階段持續時間上限 (以小時為單位)，或保留設定為預設的 24 小時。
16. (選用) 指定是否啟用用戶端登入橫幅文字。開啟 Enable client login banner (啟用用戶端登入橫幅)。對於 Client Login Banner Text (用戶端登入橫幅文字)，輸入當系統建立了 VPN 工作階段時，會在 AWS 提供的用戶端的橫幅中顯示的文字。僅限 UTF-8 編碼字元。最多 1400 個字元。
17. 選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。

建立 Client VPN 端點之後，請執行下列動作以完成組態並讓用戶端連線：

- Client VPN 端點的初始狀態為 pending-associate。只有在您建立第一個 [目標網路](#) 的關聯後，用戶端才能連線到 Client VPN 端點。
- 建立 [授權規則](#)，以指定哪些用戶端具有網路的存取權。

- 下載並準備 Client VPN 端點組態檔案，以發佈給用戶端。
- 指示您的用戶端使用 AWS 提供的用戶端或其他 OpenVPN 型用戶端應用程式以連線到 Client VPN 端點。如需詳細資訊，請參閱《[使用者指南](#)》[AWS Client VPN](#)。

## 建立 Client VPN 端點 (AWS CLI)

使用 [create-client-vpn-endpoint](#) 命令。

## 修改 Client VPN 端點

建立 Client VPN 之後，您就可以修改下列任一設定：

- 描述
- 伺服器憑證
- 用戶端連線日誌記錄選項
- 用戶端連線處理常式選項
- DNS 伺服器
- 分割通道選項
- 路由 (使用分割通道選項時)
- 憑證撤銷清單 (CRL)
- 授權規則
- VPC 和安全群組關聯
- VPN 連接埠號碼
- 自助式入口網站選項
- 最長 VPN 工作階段持續時間
- 啟用或停用用戶端登入橫幅文字
- 用戶端登入橫幅文字

### Note

對 Client VPN 端點進行的修改，包括憑證撤銷清單 (CRL) 變更在內，將於 Client VPN 服務接受要求後的 4 小時內生效。

在建立 Client VPN 端點之後，您即無法修改用戶端 IPv4 CIDR 範圍、驗證選項、用戶端憑證或傳輸協定。

當您修改 Client VPN 端點上的下列參數時，連線會重設：

- 伺服器憑證
- DNS 伺服器
- 分割通道選項 (開啟或關閉支援)
- 路由 (當您使用分割通道選項時)
- 憑證撤銷清單 (CRL)
- 授權規則
- VPN 連接埠號碼

您可以使用主控台或 AWS CLI 修改 Client VPN 端點。

#### 修改 Client VPN 端點 (主控台)


1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要修改的 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 在 Description (描述) 中輸入 Client VPN 端點的簡短描述。
5. 對於 Server certificate ARN (伺服器憑證 ARN)，指定要由伺服器使用的 TLS 憑證的 ARN。用戶端使用伺服器憑證來對其連線的 Client VPN 端點進行身分驗證。

#### Note

伺服器憑證必須在您要建立 Client VPN 端點的區域中之 AWS Certificate Manager (ACM) 中存在。憑證可以使用 ACM 佈建，也可以匯入至 ACM。

6. 指定是否使用 Amazon CloudWatch 日誌記錄有關用戶端連線的資料。對於 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)，請執行以下其中一項：
  - 若要啟用用戶端連線的日誌記錄，請開啟 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。在記 CloudWatch 錄檔記錄群組名稱中，選取要使用的記錄群組名稱。對於 CloudWatch 記錄檔資料流名稱，請選取要使用的記錄串流名稱，或將此選項保留空白，讓我們為您建立記錄資料流。
  - 若要停用用戶端連線的日誌記錄，請關閉 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。

- 對於 Client connect handler (Client 連線處理常式)，若要啟用 [client connect handler](#) (用端連線處理常式)，請開啟 Enable client connect handler (啟用用戶端連線處理常式)。在 Client Connect Handler ARN (用戶端連線處理常式 ARN) 中指定 Lambda 函數的 Amazon 資源名稱 (ARN)，此函數包含允許或拒絕連線的邏輯。
- 開啟或關閉 Enable DNS servers (啟用 DNS 伺服器)。若要使用自訂 DNS 伺服器，對於 DNS Server 1 IP address (DNS 伺服器 1 IP 地址)和 DNS Server 2 IP address (DNS 伺服器 2 IP 地址)，請指定要使用的 DNS 伺服器 IP 地址。若要使用 VPC DNS 伺服器，對於 DNS Server 1 IP address (DNS 伺服器 1 IP 地址)或 DNS Server 2 IP address (DNS 伺服器 2 IP 地址)，請指定 IP 地址，並新增 VPC DNS 伺服器 IP 地址。

 Note

請確定用戶端可以觸達 DNS 伺服器。

- 開啟或關閉 Enable split-tunnel (啟用分割通道)。根據預設，VPN 端點上的分割通道會關閉。
- 對於 VPC ID，選擇要與 Client VPN 端點關聯的 VPC。Security Group IDs (安全群組識別碼) 請選擇一或多個要套用至 Client VPN 端點的 VPC 安全群組。
- 對於 VPN port (VPN 連接埠)，請選擇 VPN 連接埠號碼。預設為 443。
- 若要產生用戶端的 [自助式入口網站 URL](#)，請選擇 Enable self-service portal (啟用自助式入口網站)。
- 對於 Session timeout hours (工作階段逾時時數)，從可用選項中選擇所需的 VPN 工作階段持續時間上限 (以小時為單位)，或保留設定為預設的 24 小時。
- 開啟或關閉 Enable client login banner (啟用用戶端登入橫幅)。如果您想要使用用戶端登入橫幅，輸入當系統建立 VPN 工作階段時，會在 AWS 提供的用戶端的橫幅中顯示的文字。僅限 UTF-8 編碼字元。最多 1400 個字元。
- 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

修改 Client VPN 端點 (AWS CLI)

使用 [modify-client-vpn-endpoint](#) 命令。

## 檢視 Client VPN 端點

您可以使用主控台或 AWS CLI 來檢視 Client VPN 端點的相關資訊。

## 若要檢視 Client VPN 端點 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要檢視的 Client VPN 端點。
4. 使用 Details (詳細資訊)、Target network associations (目標網路關聯)、Security groups (安全群組)、Authorization rules (授權規則)、Route table (路由表)、Connections (連線) 和 Tags (標籤) 標籤來查看有關現有 Client VPN 端點的資訊。

您可以使用篩選條件來協助縮小搜尋範圍。

## 若要檢視 Client VPN 端點 (AWS CLI)

使用 [describe-client-vpn-endpoints](#) 命令。

## 建立 Client VPN 端點

您必須取消所有關聯的目標網路，才能刪除 Client VPN 端點。當您刪除 Client VPN 端點後，其狀態會變更為 deleting，而且用戶端無法再連線到該端點。

您可以使用主控台或 AWS CLI 刪除 Client VPN 端點。

## 刪除 Client VPN 端點 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要刪除的 Client VPN 端點。選擇 Actions (動作)、Delete Client VPN endpoint (刪除 Client VPN 端點)。
4. 在確認視窗中輸入 delete (刪除)，然後選擇 Delete (刪除)。

## 刪除 Client VPN 端點 (AWS CLI)

使用 [delete-client-vpn-endpoint](#) 命令。

## 使用連線日誌

您可以啟用新的或現有的 Client VPN 端點連線記錄日誌，開始擷取連線日誌。

開始之前，您的帳戶中必須有 CloudWatch Logs 日誌群組。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的[使用日誌群組和日誌串流](#)。CloudWatch Logs 為付費服務。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#)。

啟用連線日誌記錄時，您可以在日誌群組中指定日誌串流的名稱。如未指定日誌串流，Client VPN 服務會為您建立一個日誌串流。

## 啟用新 Client VPN 端點的連線日誌記錄

使用主控台或命令列建立新的 Client VPN 端點時，您可以啟用連線日誌記錄。

使用主控台啟用新 Client VPN 端點的連線日誌記錄

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)，然後選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。
3. 完成選項，直到您到達 Connection Logging (連線日誌記錄) 區段為止。如需選項的詳細資訊，請參閱 [建立 Client VPN 端點](#)。
4. 在 Connection logging (連線日誌記錄) 下，開啟 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。
5. CloudWatch Logs log group name (CloudWatch Logs 日誌群組名稱) 請選擇 CloudWatch Logs 日誌群組的名稱。
6. (選用) CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱) 請選擇 CloudWatch Logs 日誌串流的名稱。
7. 選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。

使用 AWS CLI 啟用新 Client VPN 端點的連線日誌記錄

使用 [create-client-vpn-endpoint](#) 命令，並指定 `--connection-log-options` 參數。您可以指定 JSON 格式的連線日誌資訊，如下列範例所示。

```
{
  "Enabled": true,
  "CloudwatchLogGroup": "ClientVpnConnectionLogs",
  "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

## 啟用現有 Client VPN 端點的連線日誌記錄

您可以使用主控台或命令列啟用現有 Client VPN 端點的連線日誌記錄。

使用主控台啟用現有 Client VPN 端點的連線日誌記錄

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 在 Connection logging (連線日誌記錄) 下，開啟 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。
5. CloudWatch Logs log group name (CloudWatch Logs 日誌群組名稱) 請選擇 CloudWatch Logs 日誌群組的名稱。
6. (選用) CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱) 請選擇 CloudWatch Logs 日誌串流的名稱。
7. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

使用 AWS CLI 啟用現有 Client VPN 端點的連線日誌記錄

使用 [modify-client-vpn-endpoint](#) 命令，並指定 `--connection-log-options` 參數。您可以指定 JSON 格式的連線日誌資訊，如下列範例所示。

```
{
  "Enabled": true,
  "CloudwatchLogGroup": "ClientVpnConnectionLogs",
  "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

## 檢視連線日誌

您可以使用 CloudWatch Logs 主控台檢視連線日誌。

使用主控台檢視連線日誌

1. 前往 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中選擇 Log groups (日誌群組)，然後選取包含您連線日誌的日誌群組。

### 3. 選取 Client VPN 端點的日誌串流。

#### Note

Timestamp (時間戳記) 欄位顯示連線日誌發佈到 CloudWatch Logs 的時間，不是連線的時間。

如需搜尋日誌資料的詳細資訊，請參閱 Amazon CloudWatch Logs User Guide 《Amazon CloudWatch Logs 使用者指南》中的 [Search Log Data Using Filter Patterns](#) (使用篩選條件模式搜尋日誌資料)。

## 關閉連線日誌記錄

您可以使用主控台或命令列關閉 Client VPN 端點的連線日誌記錄。當您關閉連線日誌記錄時，並不會刪除 CloudWatch Logs 中現有的連線日誌。

### 使用主控台關閉連線日誌記錄

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 在 Connection logging (連線日誌記錄) 下，關閉 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)。
5. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

### 使用 AWS CLI 關閉連線日誌記錄

使用 [modify-client-vpn-endpoint](#) 命令，並指定 `--connection-log-options` 參數。請確定 Enabled 已設為 false。

## 匯出和設定用戶端組態檔

Client VPN 端點組態檔案是用戶端 (使用者) 以 Client VPN 端點建立 VPN 連接時所用的檔案。您必須下載 (匯出) 此檔案，並分發給所有需要存取 VPN 的用戶端。或者，如果您已為 Client VPN 端點啟用自助式入口網站，則用戶端可以登入入口網站並自行下載組態檔案。如需詳細資訊，請參閱 [存取自助式入口網站](#)。



如果您的 Client VPN 端點使用交互身分驗證，您必須將用戶端憑證和用戶端私有金鑰新增至您下載的 [.ovpn 組態檔案](#)。在您新增資訊之後，用戶端可以將 .ovpn 檔案匯入到 OpenVPN 用戶端軟體。

#### Important

如果您未將用戶端憑證和用戶端私有金鑰資訊新增至檔案，則使用交互身分驗證進行驗證的用戶端將無法連線至 Client VPN 端點。

根據預設，OpenVPN 用戶端組態中的「remote-random-hostname」選項會啟用萬用字元 DNS。由於萬用字元 DNS 已啟用，用戶端不會快取端點的 IP 地址，而您將無法以 Ping 偵測端點的 DNS 名稱。

如果您的 Client VPN 端點使用 Active Directory 身分驗證，而且您在發佈用戶端組態檔案之後，在目錄上啟用了多重要素驗證 (MFA)，則必須下載新檔案並將其重新發佈至用戶端。用戶端無法使用先前的組態檔案連線到 Client VPN 端點。

## 匯出用戶端組態檔

您可以使用主控台或 AWS CLI 來匯出用戶端組態。

### 匯出用戶端組態 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選擇要下載用戶端組態的 Client VPN 端點，然後選擇 Download Client Configuration (下載用戶端組態)。

### 匯出用戶端組態 (AWS CLI)

使用 [export-client-vpn-client-configuration](#) 指令並指定輸出檔案名稱。

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id --output text>config_filename.ovpn
```

## 新增用戶端憑證和金鑰資訊 (交互身分驗證)

如果您的 Client VPN 端點使用交互身分驗證，您必須將用戶端憑證和用戶端私有金鑰新增至您下載的 .ovpn 組態檔案。

當您使用相互身分驗證時，無法修改用戶端憑證。

### 新增用戶端憑證和金鑰資訊 (交互身分驗證)

您可以使用下列其中一個選項。

(選項 1) 將用戶端憑證和金鑰與 Client VPN 端點組態檔案一起發佈給用戶端。在此情況下，請在組態檔案中指定憑證和金鑰的路徑。使用您偏好的文字編輯器開啟組態檔案，並將以下內容新增到檔案尾端。以用戶端憑證和金鑰的位置取代 */path/* (位置是相對於連線至端點的用戶端)。

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(選項 2) 將 `<cert></cert>` 標籤之間的用戶端憑證內容與 `<key></key>` 標籤之間的私有金鑰內容新增至組態檔案。如果您選擇此選項，則只會將組態檔案分發給用戶端。

如果您為要連線至 Client VPN 端點的每個使用者都產生了個別的用戶端憑證和金鑰，請為每個使用者重複此步驟。

以下是包含用戶端憑證和金鑰的 Client VPN 組態檔案格式範例。

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

```
reneg-sec 0
```

## 路由

每個用戶端 VPN 端點都有路由表來描述可用的目標網路路由。路由表中的每個路由決定網路流量導向何處。您必須為每個 Client VPN 端點路由設定授權規則，以指定哪些用戶端可以存取目標網路。

當您建立 VPC 的子網路與 Client VPN 端點的關聯時，VPC 的路由會自動新增到 Client VPN 端點的路由表。若要啟用對等 VPC、現場部署網路、區域網路 (讓用戶端彼此通訊) 或網際網路等其他網路的存取權限，您必須將路由手動新增至 Client VPN 端點的路由表。

### Note

如果您要將多個子網路關聯至 Client VPN 端點，請務必為每個子網路建立路由，如此處所述 [對等 VPC、Amazon S3 或網際網路的存取斷斷續續](#)。每個關聯的子網路應該有一組相同的路由。

## 目錄

- [Client VPN 端點上的分割通道考量](#)
- [建立端點路由](#)
- [檢視端點路由](#)
- [刪除端點路由](#)

## Client VPN 端點上的分割通道考量

如果在 Client VPN 端點上使用分割通道，則在建立 VPN 時，Client VPN 路由表中的所有路由都會新增至用戶端路由表。如果您在建立 VPN 之後新增路由，您必須重設連線，以便將新路由傳送至用戶端。

建議您在修改 Client VPN 端點路由表之前，先考慮用戶端裝置可以處理的路由數目。

## 建立端點路由

當您建立路由時，請指定如何引導目的地網路的流量。

若要允許用戶端存取網際網路，請新增目的地 `0.0.0.0/0` 路由。

您可以使用主控台和 AWS CLI 將路由新增至 Client VPN 端點。

### 建立 Client VPN 端點路由 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要新增路由的 Client VPN 端點，選擇 Route Table (路由表)，然後選擇 Create Route (建立路由)。
4. 對於 Route destination (路由目的地)，指定目的地網路的 IPv4 CIDR 範圍。例如：
  - 若要新增 Client VPN 端點的 VPC 的路由，請輸入 VPC 的 IPv4 CIDR 範圍。
  - 若要新增網際網路存取的路由，請輸入 `0.0.0.0/0`
  - 若要新增對等端 VPC 的路由，請輸入對等端 VPC 的 IPv4 CIDR 範圍。
  - 若要新增內部部署網路的路由，請輸入 AWS Site-to-Site VPN 連接的 IPv4 CIDR 範圍。
5. 對於 Subnet ID for target network association (目標網路關聯的子網路 ID)，選取與 Client VPN 端點關聯的子網路。

或者，如果您要新增區域 Client VPN 端點網路的路由，請選取 `local`。

6. (選用) 對於 Description (描述)，輸入路由的簡短描述。
7. 選擇 Create route (建立路由)。

### 建立 Client VPN 端點路由 (AWS CLI)

使用 [create-client-vpn-route](#) 命令。

## 檢視端點路由

您可以使用主控台或 AWS CLI 來檢視特定 Client VPN 端點的路由。

### 檢視 Client VPN 端點路由 (主控台)

1. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
2. 選取要檢視路由的 Client VPN 端點，然後選擇 Route Table (路由表)。

### 檢視 Client VPN 端點路由 (AWS CLI)

使用 [describe-client-vpn-routes](#) 命令。

## 刪除端點路由

只能刪除您手動新增的路由。無法刪除在建立子網路與 Client VPN 端點關聯時自動新增的路由。若要刪除自動新增的路由，您必須取消與在 Client VPN 端點建立之子網路的關聯。

您可以使用主控台或 AWS CLI 從 Client VPN 端點刪除路由。

### 刪除 Client VPN 端點路由 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要刪除路由的來源 Client VPN 端點，然後選擇 Route Table (路由表)。
4. 選取要刪除的路由，選擇 Delete Route (刪除路由)，然後選擇 Delete Route (刪除路由)。

### 刪除 Client VPN 端點路由 (AWS CLI)

使用 [delete-client-vpn-route](#) 命令。

## 目標網路

目標網路是 VPC 中的子網路。Client VPN 端點至少必須有一個目標網路，才能讓用戶端連線並建立 VPN 連接。

如需可設定之存取類型的詳細資訊 (例如讓用戶端存取網際網路)，請參閱 [AWS Client VPN 的案例和範例](#)。

### 目錄

- [建立目標網路與 Client VPN 端點的關聯](#)
- [將安全群組套用到目標網路](#)
- [取消目標網路與 Client VPN 端點的關聯](#)
- [檢視目標網路](#)

## 建立目標網路與 Client VPN 端點的關聯

您可以將一或多個目標網路 (子網路) 與 Client VPN 端點建立關聯。

適用的規定如下：

- 子網路必須具有至少 /27 位元遮罩的 CIDR 區塊，例如 10.0.0.0/27。子網路也必須隨時至少有 20 個可用的 IP 地址。
- 子網路的 CIDR 區塊不得與 Client VPN 端點的用戶端 CIDR 範圍重疊。
- 如果將多個子網路與 Client VPN 端點建立關聯，則每個子網路必須位於不同的可用區域。我們建議您與至少兩個子網路建立關聯，來提供可用區域備援。
- 如果您在建立 Client VPN 端點時指定了 VPC，則子網路必須位於相同的 VPC 中。如果您尚未建立 VPC 與 Client VPN 端點的關聯，您可選擇任一 VPC 中的任一子網路。

所有其他子網路關聯都必須來自相同的 VPC。若要從不同 VPC 建立子網路關聯，您必須先修改 Client VPN 端點並變更與其相關聯的 VPC。如需更多詳細資訊，請參閱 [修改 Client VPN 端點](#)。

當您將子網路與 Client VPN 端點建立關聯時，我們會自動將其中佈建相關聯子網路的 VPC 本機路由新增到 Client VPN 端點的路由表。

#### Note

關聯目標網路之後，當您向連接的 VPC 新增或移除其他 CIDR 時，您必須執行以下其中一個操作，以更新用戶端 VPN 端點路由表的本機路由：

- 從目標網路取消關聯 Client VPN 端點，然後將 Client VPN 端點關聯至目標網路。
- 手動將路由新增至用戶端 VPN 端點路由表或從用戶端 VPN 端點路由表移除路由。

當您將第一個子網路與 Client VPN 端點建立關聯後，Client VPN 端點的狀態會從 pending-associate 變成 available，而且用戶端能夠建立 VPN 連接。

建立目標網路與 Client VPN 端點的關聯 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要與目標網路關聯的 Client VPN 端點，選擇 Target network associations (目標網路關聯)，然後選擇 Associate target network (關聯目標網路)。
4. 對於 VPC，選擇子網路所在的 VPC。如果您在建立 Client VPN 端點時指定了 VPC，或者您有先前的子網路關聯，則其必須是相同的 VPC。
5. 對於 Choose a subnet to associate (選擇要關聯的子網路)，選擇要和 Client VPN 端點關聯的子網路。

## 6. 選擇 Associate target network (關聯目標網路)。

建立目標網路與 Client VPN 端點 (AWS CLI) 的關聯

使用 [associate-client-vpn-target-network](#) 命令。

## 將安全群組套用到目標網路

建立 Client VPN 端點時，您可以指定要套用至目標網路的安全群組。當您將第一個目標網路與 Client VPN 端點建立關聯時，我們會自動套用相關聯子網路所在 VPC 的預設安全群組。如需更多詳細資訊，請參閱 [安全群組](#)。

您可以變更 Client VPN 端點的安全群組。您需要的安全群組規則，取決於您要設定的 VPN 存取種類。如需更多詳細資訊，請參閱 [AWS Client VPN 的案例和範例](#)。

將安全群組套用到目標網路 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取要套用安全群組的 Client VPN 端點。
4. 選擇 Security Groups (安全群組)，然後選擇 Apply Security Group (套用安全群組)。
5. 從 Security group IDs (安全群組 ID) 選擇適當的安全群組。
6. 選擇 Apply Security Groups (套用安全群組)。

將安全群組套用到目標網路 (AWS CLI)

使用 [apply-security-groups-to-client-vpn-target-network](#) 命令。

## 取消目標網路與 Client VPN 端點的關聯

在您取消目標網路的關聯時，系統會刪除手動新增至 Client VPN 端點路由表的任何路由，以及建立目標網路關聯時自動建立的路由 (VPC 的本機路由)。如果您取消所有目標網路與 Client VPN 端點的關聯，用戶端就無法再建立 VPN 連接。

取消目標網路與 Client VPN 端點的關聯 (主控台)

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

3. 選取目標網路要關聯的 Client VPN 端點，然後選擇 Target network associations (目標網路關聯)。
4. 選取要取消關聯的目標網路，選擇 Disassociate (取消關聯)，然後選擇 Disassociate target network (取消關聯目標網路)。

取消目標網路與 Client VPN 端點 (AWS CLI) 的關聯

使用 [disassociate-client-vpn-target-network](#) 命令。

## 檢視目標網路

您可以使用主控台或 AWS CLI 來檢視與 Client VPN 端點相關聯的目標。

檢視目標網路 (主控台)

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取 Client VPN 端點，然後選擇 Target network associations (目標網路關聯)。

使用 AWS CLI 來檢視目標網路

使用 [describe-client-vpn-target-networks](#) 命令。

## VPN 工作階段最長持續時間

AWS Client VPN 為 VPN 工作階段持續時間上限提供了多種選項。您可以設定較短的 VPN 工作階段持續時間上限來滿足安全性與合規的要求。根據預設，VPN 工作階段最長持續時間為 24 小時。

### Note

當 VPN 工作階段持續時間上限值減少時，若作用中 VPN 工作階段的逾時值較新的逾時值長，系統就會中斷這些工作階段。

請參閱《[AWS Client VPN 使用者指南](#)》中的「AWS 提供的用戶端版本備註」，瞭解用戶端桌面應用程式的詳細資訊。

目錄



- [設定 Client VPN 端點建立期間的 VPN 工作階段上限](#)
- [檢視目前 VPN 工作階段持續時間上限](#)
- [修改 VPN 工作階段持續時間上限](#)

## 設定 Client VPN 端點建立期間的 VPN 工作階段上限

如需設定 Client VPN 端點建立期間的 VPN 工作階段上限之詳細步驟，請參閱 [建立 Client VPN 端點](#)。

## 檢視目前 VPN 工作階段持續時間上限

請使用下列步驟來檢視目前 VPN 工作階段持續時間上限。

檢視 Client VPN 端點 (主控台) 目前的 VPN 工作階段持續時間上限

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要檢視的 Client VPN 端點。
4. 請確認選取了 Details (詳細資訊) 索引標籤。
5. 檢視 Session timeout hours (工作階段逾時時數) 旁的目前 VPN 工作階段持續時間上限。

檢視 Client VPN 端點 (AWS CLI) 目前的 VPN 工作階段持續時間上限

使用 [describe-client-vpn-endpoints](#) 命令。

## 修改 VPN 工作階段持續時間上限

請使用下列步驟來修改現有 VPN 工作階段持續時間上限。

修改 Client VPN 端點 (主控台) 現有的 VPN 工作階段持續時間上限

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Client VPN Endpoints (Client VPN 端點)。
3. 選取您要修改的 Client VPN 端點，選擇 Actions (動作)，然後選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。
4. 對於 Session timeout hours (工作階段逾時時數)，選擇所需的 VPN 工作階段持續時間上限 (以小時為單位)。

## 5. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

修改 Client VPN 端點 (AWS CLI) 現有的 VPN 工作階段持續時間上限

使用 [modify-client-vpn-endpoint](#) 命令。

# AWS Client VPN 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 的客戶，您將能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而設計的。

安全是 AWS 與您共同肩負的責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 [AWS 合規計劃](#) 的一部分。若要了解適用於 AWS Client VPN 的合規計劃，請參閱 [合規計劃的 AWS 服務範圍](#)。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

AWS Client VPN 為 Amazon VPC 服務的一部分。如需 Amazon VPC 安全性的詳細資訊，請參閱 Amazon VPC 使用者指南中的 [安全性](#)。

本文件有助於您了解如何在使用 Client VPN 時套用共同的責任模型。下列各主題將說明如何設定 Client VPN，以達成您的安全性與合規目標。您也將了解如何使用其他 AWS 服務，幫助您監控並保護 Client VPN 資源。

## 內容

- [AWS Client VPN 中的資料保護](#)
- [AWS Client VPN 的身分識別與存取管理](#)
- [AWS Client VPN 中的恢復能力](#)
- [AWS Client VPN 中的基礎設施安全](#)
- [AWS Client VPN 的安全最佳實務](#)
- [AWS Client VPN 的 IPv6 考量因素](#)

## AWS Client VPN 中的資料保護

AWS [共同的責任模型](#)適用於 AWS Client VPN 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端的全球基礎設施。您必須負責維護在此基礎設施上託管之內容的控制權。您也必須負責您使用的 AWS 服務的安全性設定和管理工作。如需有關資料隱私權的詳細資訊，請參閱 [資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR 部落格文章](#)。

基於資料保護目的，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶憑證，並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制項。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如 Name (名稱) 欄位。這包括當您使用 Client VPN 時，或使用主控台、API、AWS CLI 或 AWS 開發套件的其他 AWS 服務時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

## 傳輸中加密

AWS Client VPN 使用 Transport Layer Security (TLS) 1.2 或更新版本提供安全連接。

## 網際網路流量隱私權

### 啟用網際網路存取

您可以讓用戶端透過 Client VPN 端點連線到您的 VPC 和其他網路。如需詳細資訊和範例，請參閱[AWS Client VPN 的案例和範例](#)。

### 限制對網路的存取

您可以設定您的 Client VPN 端點，限制對 VPC 中特定資源的存取。針對使用者類型身分驗證，您也可以根據存取 Client VPN 端點的使用者群組，將存取限制在一部分的網路。如需更多詳細資訊，請參閱[使用 AWS Client VPN 限制存取您的網路](#)。

### 對用戶端進行身分驗證

身分驗證是在 AWS 雲端的第一個進入點實作。其會用於決定是否允許用戶端連線到 Client VPN 端點。如果身分驗證成功，則用戶端會連線到 Client VPN 端點並建立 VPN 工作階段。如果身分驗證失敗，則拒絕連線，並防止用戶端建立 VPN 工作階段。

Client VPN 提供下列類型的用戶端身分驗證：

- [Active Directory 身分驗證](#) (以使用者為基礎)
- [交互身分驗證](#) (以憑證為基礎)
- [單一登入 \(SAML 型同盟驗證\)](#) (以使用者為基礎)

## AWS Client VPN 的身分識別與存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員可以控制誰能進行身分驗證 (已登入) 和獲得授權 (具有許可) 而得以使用 Client VPN 資源。IAM 是您可以使用的 AWS 服務，無需額外付費。

### 主題

- [物件](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Client VPN 如何與 IAM 搭配使用](#)
- [Client VPN 的身分識別型原則範例 AWS](#)
- [疑難排解 AWS Client VPN 身分和存取](#)
- [在 Client VPN 使用服務連結角色](#)

### 物件

根據您在 Client VPN 中執行的工作而定，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 – 如果您使用 Client VPN 執行任務，管理員會為您提供所需的憑證和許可。當您使用更多 Client VPN 功能來執行工作時，您可能會需要額外的許可。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。若您無法存取 Client VPN 中的某項功能，請參閱 [疑難排解 AWS Client VPN 身分和存取](#)。

服務管理員 – 如果您負責公司內的 Client VPN 資源，您可能具備 Client VPN 的完整存取權限。您的任務是判斷服務使用者應該存取哪些 Client VPN 功能及資源。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。若要進一步了解貴公司可搭配 Client VPN 使用 IAM 的方式，請參閱 [AWS Client VPN 如何與 IAM 搭配使用](#)。

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 Client VPN 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的範例 Client VPN 身分型政策，請參閱 [Client VPN 的身分識別型原則範例 AWS](#)。

## 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。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》AWS 帳戶中 [的如何登入](#) 您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便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

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

## 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 的詳細資訊，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詳細資訊，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 — 如需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 (信任的主體) 存取您帳戶的資源。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角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。

- 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。如需詳細資訊，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](#)。
- 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。如需詳細資訊，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](#)。

如需了解是否要使用 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 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詳細資訊，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。如需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) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

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

## 其他政策類型

AWS 支援其他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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 [IAM 實體許可界限](#)。

- 服務控制策略 ( 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 帳戶的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 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 Organizations 和 SCP 的詳細資訊，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。如需詳細資訊，請參閱 IAM 使用者指南中的 [工作階段政策](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。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](#)。

## AWS Client VPN 如何與 IAM 搭配使用

在您使用 IAM 管理 Client VPN 的存取權限之前，請了解有哪些 IAM 功能可搭配 Client VPN 使用。

您可以搭配 AWS Client VPN 使用的 IAM 功能

IAM 功能	Client VPN 支援
<a href="#">身分型政策</a>	是
<a href="#">資源型政策</a>	否
<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>	否

IAM 功能	Client VPN 支援
<a href="#">臨時憑證</a>	是
<a href="#">主體許可</a>	是
<a href="#">服務角色</a>	是
<a href="#">服務連結角色</a>	是

若要深入瞭解 Client VPN 和其他 AWS 服務如何搭配大多數 IAM 功能運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的[AWS 服務](#)。

## 適用於 Client VPN 的身分型政策

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](#)。

## Client VPN 的身分型政策範例

若要檢視 Client VPN 身分型政策範例，請參閱[Client VPN 的身分識別型原則範例 AWS](#)。

## Client VPN 內的資源型政策

支援以資源基礎的政策	否
------------	---

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

如需啟用跨帳戶存取權，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。當主體和資源位於不同時 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 中的跨帳戶資源存取](#)。

## Client VPN 的政策動作

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。

若要查看 Client VPN 動作清單，請參閱服務授權參考資料中的 [AWS Client VPN 定義的處理行動](#)。

Client VPN 中的政策動作會在動作之前使用以下字首：

```
ec2
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"  
]
```

若要檢視 Client VPN 身分型政策的範例，請參閱 [Client VPN 的身分識別型原則範例 AWS](#)。

## Client VPN 的政策資源

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": "*"
```

若要查看 Client VPN 資源類型及其 ARN 的清單，請參閱服務授權參考資料中的 [AWS Client VPN 定義的資源](#)。若要瞭解可以使用哪些動作指定每個資源的 ARN，請參閱 [AWS Client VPN 定義的動作](#)。

若要檢視 Client VPN 身分型政策範例，請參閱 [Client VPN 的身分識別型原則範例 AWS](#)。

## Client VPN 的條件索引鍵

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。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，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](#)。

若要查看 Client VPN 條件金鑰清單，請參閱服務授權參考資料中的 [AWS Client VPN 條件金鑰](#)。若要瞭解可以使用條件金鑰的動作和資源，請參閱 [AWS Client VPN 定義的動作](#)。

若要檢視 Client VPN 身分型政策範例，請參閱 [Client VPN 的身分識別型原則範例 AWS](#)。

## Client VPN 中的 ACL

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。

## ABAC 搭配 Client VPN

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

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。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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 \(ABAC\)](#)。

## 將臨時憑證與 Client VPN 搭配使用

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，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

## Client VPN 的跨服務委託人許可

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》](#)。

## Client VPN 的服務角色

支援服務角色 是

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。如需詳細資訊，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](#)。

### Warning

變更服務角色的許可有可能會讓 Client VPN 功能出現故障。只有在 Client VPN 提供指引時，才能編輯服務角色。

## Client VPN 的服務連結角色

支援服務連結角色 是

服務連結角色是一種連結至 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。

如需建立或管理服务連結角色的詳細資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

## Client VPN 的身分識別型原則範例 AWS

根據預設，使用者和角色不具備建立或修改 Client VPN 資源的許可。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](#)。

如需 Client VPN 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的[AWS Client VPN 的動作、資源和條件金鑰](#)。

### 主題

- [政策最佳實務](#)
- [允許使用者檢視他們自己的許可](#)

## 政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Client VPN 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的 AWS 受管理原則。它們可用在您的 AWS 帳戶。建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的[AWS 受管政策](#)或[任務職能的AWS 受管政策](#)。



- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM Access Analyzer 政策驗證](#)。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

## 允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
```

```
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
```

## 疑難排解 AWS Client VPN 身分和存取

請使用以下資訊來協助您診斷和修正使用 Client VPN 和 IAM 時發生的常見問題。

### 主題

- [我未獲授權，不得在 Client VPN 中執行動作](#)
- [我沒有授權執行 iam : PassRole](#)
- [我想允許我以外的人訪 AWS 帳戶 問我的 Client VPN 資源](#)

### 我未獲授權，不得在 Client VPN 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在 mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 *ec2:GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 *ec2:GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

## 我沒有授權執行 iam : PassRole

如果您收到錯誤，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，以允許您將角色傳遞給 Client VPN。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 Client VPN 中執行動作時，發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

## 我想允許我以外的人訪 AWS 帳戶 問我的 Client VPN 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Client VPN 是否支援這些功能，請參閱 [AWS Client VPN 如何與 IAM 搭配使用](#)。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 [《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限](#)。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 [IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 [IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 [IAM 使用者指南中的 IAM 中的跨帳戶資源存取](#)。

## 在 Client VPN 使用服務連結角色

AWS Client VPN 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Client VPN 的一種特殊 IAM 角色類型。服務連結角色由 Client VPN 預先定義，並包含該服務代您呼叫其他 AWS 服務所需的所有許可。

### 主題

- [使用 Client VPN 角色](#)
- [使用角色進行連線授權](#)

## 使用 Client VPN 角色

AWS Client VPN 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Client VPN 的一種特殊 IAM 角色類型。服務連結角色由 Client VPN 預先定義，並包含該服務代您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 Client VPN 更為簡單，因為您不必手動新增必要的許可。Client VPN 定義其服務連結角色的許可，除非另有定義，否則僅有 Client VPN 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。如此可保護您 Client VPN 的資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務資訊，請參閱 [《可搭配 IAM 運作的 AWS 服務》](#)，尋找 Service-linked roles (服務連結角色) 欄中顯示為 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

### Client VPN 的服務連結角色許可

Client VPN 會使用名為 AWSServiceRoleForClientVPN 的服務連結角色 – 允許 Client VPN 建立和管理與 VPN 連結相關的資源。

AWSServiceRoleForClientVPN 服務連結角色信任下列服務來擔任此角色：

- `clientvpn.amazonaws.com`

名為 ClientVPNServiceRolePolicy 的角色許可政策允許 Client VPN 對指定資源完成下列動作：

- 動作：Resource: "\*" 上的 `ec2:CreateNetworkInterface`

- 動作 : Resource: "\*" 上的 ec2:CreateNetworkInterfacePermission
- 動作 : Resource: "\*" 上的 ec2:DescribeSecurityGroups
- 動作 : Resource: "\*" 上的 ec2:DescribeVpcs
- 動作 : Resource: "\*" 上的 ec2:DescribeSubnets
- 動作 : Resource: "\*" 上的 ec2:DescribeInternetGateways
- 動作 : Resource: "\*" 上的 ec2:ModifyNetworkInterfaceAttribute
- 動作 : Resource: "\*" 上的 ec2>DeleteNetworkInterface
- 動作 : Resource: "\*" 上的 ec2:DescribeAccountAttributes
- 動作 : Resource: "\*" 上的 ds:AuthorizeApplication
- 動作 : Resource: "\*" 上的 ds:DescribeDirectories
- 動作 : Resource: "\*" 上的 ds:GetDirectoryLimits
- 動作 : Resource: "\*" 上的 ds:UnauthorizeApplication
- 動作 : Resource: "\*" 上的 logs:DescribeLogStreams
- 動作 : Resource: "\*" 上的 logs>CreateLogStream
- 動作 : Resource: "\*" 上的 logs:PutLogEvents
- 動作 : Resource: "\*" 上的 logs:DescribeLogGroups
- 動作 : Resource: "\*" 上的 acm:GetCertificate
- 動作 : Resource: "\*" 上的 acm:DescribeCertificate
- 動作 : Resource: "\*" 上的 iam:GetSAMLProvider
- 動作 : Resource: "\*" 上的 lambda:GetFunctionConfiguration

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[服務連結角色許可](#)。

### 建立 Client VPN 服務連結角色

您不需要手動建立一個服務連結角色。當您使用 AWS Management Console、AWS CLI 或 AWS API 在帳戶中建立第一個 Client VPN 端點時，Client VPN 即會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您在帳戶中建立第一個 Client VPN 端點時，Client VPN 會再次為您建立角色。

## 編輯 Client VPN 的服務連結角色

Client VPN 不允許您編輯 `AWSServiceRoleForClientVPN` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

## 刪除 Client VPN 的服務連結角色

如果您不再需要使用 Client VPN，建議您刪除 `AWSServiceRoleForClientVPN` 服務連結角色。

您必須先刪除相關的 Client VPN 資源。這可確保避免您不小心移除資源的存取許可。

使用 IAM 主控台、IAM CLI 或 IAM API 刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

## Client VPN 服務連結角色的支援區域

Client VPN 在所有提供該服務的區域中支援使用服務連結角色。如需詳細資訊，請參閱[AWS 區域與端點](#)。

## 使用角色進行連線授權

AWS Client VPN 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Client VPN 的一種特殊 IAM 角色類型。服務連結角色由 Client VPN 預先定義，並包含該服務代您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 Client VPN 更為簡單，因為您不必手動新增必要的許可。Client VPN 定義其服務連結角色的許可，除非另有定義，否則僅有 Client VPN 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。如此可保護您 Client VPN 的資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務資訊，請參閱[《可搭配 IAM 運作的 AWS 服務》](#)，尋找 Service-linked roles (服務連結角色) 欄中顯示為 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

## Client VPN 的服務連結角色許可

Client VPN 會使用名為 `AWSServiceRoleForClientVPN` 的服務連結角色 — Client VPN 連線的服務連結角色。

AWSServiceRoleForClientVPNConnections 服務連結角色信任下列服務來擔任該角色：

- `clientvpn-connections.amazonaws.com`

名為 ClientVPNServiceConnectionsRolePolicy 的角色許可政策允許 Client VPN 對指定資源完成下列動作：

- 動作：`arn:aws:lambda:*:*:function:AWSClientVPN-*` 上的 `lambda:InvokeFunction`

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[服務連結角色許可](#)。

### 建立 Client VPN 的服務連結角色

您不需要手動建立一個服務連結角色。當您使用 AWS Management Console、AWS CLI 或 AWS API 在帳戶中建立第一個 Client VPN 端點時，Client VPN 即會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您在帳戶中建立第一個 Client VPN 端點時，Client VPN 會再次為您建立服務連結角色。

### 編輯 Client VPN 的服務連結角色

Client VPN 不允許您編輯 AWSServiceRoleForClientVPNConnections 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

### 刪除 Client VPN 的服務連結角色

如果您不再需要使用 Client VPN，建議您刪除 AWSServiceRoleForClientVPNConnections 服務連結角色。

您必須先刪除相關的 Client VPN 資源。這可確保避免您不小心移除資源的存取許可。

使用 IAM 主控台、IAM CLI 或 IAM API 刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

### Client VPN 服務連結角色的支援區域

Client VPN 在所有提供該服務的區域中支援使用服務連結角色。如需詳細資訊，請參閱 [AWS 區域與端點](#)。

## AWS Client VPN 中的恢復能力

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援聯網功能相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域與可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施外，AWS Client VPN 還提供支援資料復原和備份需求的多項功能。

### 提供高可用性的多個目標網路

您可以將目標網路與 Client VPN 端點建立關聯，以讓用戶端建立 VPN 工作階段。目標網路是您 VPC 中的子網路。每個您與 Client VPN 端點建立關聯的子網路，都必須屬於不同的可用區域。您可以將多個子網路與 Client VPN 端點建立關聯，以獲得高可用性。

## AWS Client VPN 中的基礎設施安全

AWS Client VPN 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 [AWS 雲端安全](#)。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的 [基礎設施保護](#)。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 Client VPN。用戶端必須支援下列項目：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密 (PFS) 的密碼套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

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

## AWS Client VPN 的安全最佳實務

在您開發和實作自己的安全政策時，可考慮使用 AWS Client VPN 提供的多種安全功能。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。



## 授權規則

使用授權規則以限制可以存取您網路的使用者。如需更多詳細資訊，請參閱 [授權規則](#)。

## Security groups (安全群組)

使用安全群組以控制使用者可在您 VPC 中存取的資源。如需更多詳細資訊，請參閱 [安全群組](#)。

## 用戶端憑證撤銷清單

您可以使用用戶端憑證撤銷清單來撤銷特定用戶端憑證對 Client VPN 端點的存取權。例如，當使用者離職後。如需更多詳細資訊，請參閱 [用戶端憑證撤銷清單](#)。

## 監控工具

使用監控工具來追蹤 Client VPN 端點的可用性和效能。如需更多詳細資訊，請參閱 [監控 AWS Client VPN](#)。

## 身分與存取管理

使用 IAM 使用者和 IAM 角色的 IAM 政策來管理對 Client VPN 資源和 API 的存取。如需更多詳細資訊，請參閱 [AWS Client VPN 的身分識別與存取管理](#)。

# AWS Client VPN 的 IPv6 考量因素

目前 Client VPN 服務不支援透過 VPN 通道路由 IPv6 流量。不過，在某些情況下，IPv6 流量應該被路由至 VPN 通道，以防止 IPv6 洩漏。當 IPv4 和 IPv6 同時啟用並連線至 VPN 時，就可能發生 IPv6 洩漏，但 VPN 不會將 IPv6 流量路由至其通道。在這種情況下，連線至啟用 IPv6 的目的地時，您實際上仍然與 ISP 提供的 IPv6 位址連線。這會洩漏您的真實 IPv6 地址。以下說明會解釋如何將 IPv6 流量路由到 VPN 通道。

下列 IPv6 相關指示詞應新增至 Client VPN 設定檔，以防止 IPv6 洩漏：

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

範例可能是：

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

在此範例中，`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` 會將本機通道裝置 IPv6 地址設定為 `fd15:53b6:dead::2` 和遠端 VPN 端點 IPv6 地址設定為 `fd15:53b6:dead::1`。

下一個命令，`route-ipv6 2000::/4` 將 IPv6 地址從 `2000:0000:0000:0000:0000:0000:0000:0000` 路由至 `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` VPN 連接。

#### Note

例如，對於 Windows 中的「TAP」設備路由，`ifconfig-ipv6` 的第二個參數將被用作 `--route-ipv6` 的路由目標。

Organizations 應該設定 `ifconfig-ipv6` 本身的兩個參數，並且可以使用 `100::/64` (從 `0100:0000:0000:0000:0000:0000:0000:0000` 至 `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) 或 `fc00::/7` (從 `fc00:0000:0000:0000:0000:0000:0000:0000` 至 `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`) 中的地址。`100::/64` 是「僅捨棄地址區塊」，而 `fc00::/7` 是唯一本地。

另一個範例是：

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

在此範例中，設定會將目前配置的所有 IPv6 流量路由至 VPN 連接。

## 驗證

您的組織可能有自己的測試。基本驗證是設定完整通道 VPN 連接，然後使用 IPv6 地址將 `ping6` 執行至 IPv6 伺服器。伺服器的 IPv6 地址應該在 `route-ipv6` 命令指定的範圍內。這個 ping 測試應該會失敗。不過，如果 IPv6 支援在未來新增至 Client VPN 服務，這可能會改變。如果 ping 成功，而且您可以在以完整通道模式連線時存取公有站點，則您可能需要進一步的疑難排解。您也可以透過使用一些公開可用的工具進行測試，如 [ipleak.org](https://ipleak.org)。

# 監控 AWS Client VPN

監控是相當重要的部分，其能維護 AWS Client VPN 和其他 AWS 解決方案的可靠性、可用性及效能。您可以使用下列功能來監控您的 Client VPN 端點、分析流量模式，以及針對 Client VPN 端點的問題進行故障診斷。

## Amazon CloudWatch

即時監控您的 AWS 資源和您在 AWS 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀表板，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

## AWS CloudTrail

擷取您 AWS 帳戶發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Simple Storage Service (Amazon S3) 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 [《AWS CloudTrail 使用者指南》](#)。

## Amazon CloudWatch Logs

可讓您監控對 AWS Client VPN 端點進行的連線嘗試。您可以檢視 Client VPN 連接的連線嘗試和連線重設。對於連線嘗試，您可以看到成功和失敗的連線嘗試。您可以指定 CloudWatch Logs 日誌串流記錄連線詳細資訊。如需詳細資訊，請參閱 [連線日誌記錄](#) 和 [《Amazon CloudWatch Logs 使用者指南》](#)。

## AWS Client VPN 的 CloudWatch 指標

AWS Client VPN 會將下列指標發佈到您 Client VPN 端點的 Amazon CloudWatch。每五分鐘就會將指標發佈到 Amazon CloudWatch。

指標	描述
ActiveConnectionsCount	Client VPN 端點的作用中連線數目。  單位：計數
AuthenticationFailures	Client VPN 端點的身分驗證失敗次數。

指標	描述
	單位：計數
CrldaysToExpiry	Client VPN 端點上所設定憑證撤銷清單 (CRL) 到期之前的天數。  單位：天
EgressBytes	從 Client VPN 端點傳送的位元組數目。  單位：位元組
EgressPackets	從 Client VPN 端點傳送的封包數目。  單位：計數
IngressBytes	Client VPN 端點接收到的位元組數目。  單位：位元組
IngressPackets	Client VPN 端點接收到的封包數目。  單位：計數
SelfServicePortalClientConfigurationDownloads	從自助式入口網站下載 Client VPN 端點組態檔案的次數。  單位：計數

AWS Client VPN 會發佈 Client VPN 端點的下列[狀態評估](#)指標。

指標	描述
ClientConnectHandlerTimeouts	叫用 Client VPN 端點連線的用戶端連線處理常式之逾時數量。  單位：計數
ClientConnectHandlerInvalidResponses	Client VPN 端點連線的用戶端連線處理常式傳回之無效回應數量。

指標	描述
	單位：計數
ClientConnectHandlerOtherExecutionErrors	執行 Client VPN 端點連線的用戶端連線處理常式時之未預期錯誤數量。  單位：計數
ClientConnectHandlerThrottlingErrors	叫用 Client VPN 端點連線的用戶端連線處理常式之調節錯誤數量。  單位：計數
ClientConnectHandlerDeniedConnections	Client VPN 端點連線的用戶端連線處理常式拒絕之連線數量。  單位：計數
ClientConnectHandlerFailedServiceErrors	執行 Client VPN 端點連線的用戶端連線處理常式時之服務端錯誤數量。  單位：計數

您可以依端點篩選 Client VPN 端點的指標。

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)。

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

## 檢視 CloudWatch 指標

您可以依照下列步驟來檢視 Client VPN 端點的指標。

## 使用 CloudWatch 主控台檢視指標

指標會先依服務命名空間分組，再依各命名空間內不同的維度組合分類。

1. 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. 在 All metrics (所有指標) 下，選擇 ClientVPN 指標命名空間。
4. 若要檢視指標，請選取 by endpoint (依照端點區分) 的指標維度。

若要使用 AWS CLI 來檢視指標

在命令提示中，使用下列命令來列出可用於 Client VPN 的指標。

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

## AWS Client VPN 的 CloudTrail 日誌

AWS Client VPN 是與 AWS CloudTrail 整合的一項服務，可提供由使用者、角色或 AWS 服務在 Client VPN 中所採取動作的記錄。CloudTrail 會將 Client VPN 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Client VPN 主控台的呼叫，以及對 Client VPN API 操作發出的程式碼呼叫。如果您建立線索，就可以將 CloudTrail 事件持續交付到 Amazon S3 儲存貯體，包括 Client VPN 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台內的 Event history (事件歷史記錄) 檢視最新事件。使用 CloudTrail 收集的資訊，判斷對 Client VPN 提出的請求、請求 IP 位址、申請者，提出請求的時間，以及其他詳細資訊。

如需有關 CloudTrail 的詳細資訊，請參閱 [AWS CloudTrail 使用者指南](#)。

## CloudTrail 中的 Client VPN 資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。Client VPN 中發生活動時，系統便會將該活動與其他 AWS 服務活動一同記錄在 Event history (事件歷史記錄) 中的 CloudTrail 事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱 [使用 CloudTrail 事件歷史記錄檢視事件](#)。

若要持續記錄您 AWS 帳戶中正在進行的事件 (包括 Client VPN 的事件)，請建立線索。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的

Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收來自多個區域的 CloudTrail 日誌檔案](#)，以及[接收來自多個帳戶的 CloudTrail 日誌檔案](#)。

CloudTrail 會記錄所有 Client VPN 動作，並記錄在《[Amazon EC2 API 參考](#)》中。例如，對 CreateClientVpnEndpoint、AssociateClientVpnTargetNetwork 以及 AuthorizeClientVpnIngress 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 了解 Client VPN 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

如需詳細資訊，請參閱《[Amazon EC2 API 參考](#)》中的[使用 AWS CloudTrail 記錄 Amazon EC2、Amazon EBS 及 Amazon VPC API 呼叫的日誌](#)。

## AWS Client VPN 配額

您的 AWS 帳戶具有下列與 Client VPN 端點相關的配額 (先前稱為限制)。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。

若要為可調整配額請求增加配額上限，請在 Adjustable (可調整) 直欄中選擇 Yes (是)。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的[請求提高配額](#)。

### Client VPN 配額

名稱	預設	可調整
每個 Client VPN 端點的授權規則	50	<a href="#">是</a>
每個區域的 Client VPN 端點	5	<a href="#">是</a>
每個 Client VPN 端點的並行用戶端連線	此值取決於每個端點的子網路關聯數量。 <ul style="list-style-type: none"> <li>一至二萬</li> <li>2 – 36,500</li> <li>3 – 66,500</li> <li>4 – 96,500</li> <li>5 – 126,000</li> </ul>	<a href="#">是</a>
每個 Client VPN 端點的並行操作 †	10	否
Client VPN 端點之用戶端憑證撤銷清單中的項目	20,000	否
每個 Client VPN 端點的路由	10	<a href="#">是</a>

† 操作包含：

- 關聯或取消關聯子網路
- 建立或刪除路由
- 建立或刪除傳入和傳出規則



- 建立或刪除安全群組

## 使用者和群組配額

當您為 Active Directory 或 SAML 型 IdP 設定使用者和群組時，系統會套用下列配額：

- 使用者最多可以屬於 200 個群組。我們忽略第 200 組之後的任何群組。
- 群組 ID 的長度上限為 255 個字元。
- 名稱 ID 的長度上限為 255 個字元。我們會截斷第 255 個字元之後的字元。

## 一般考量

使用 Client VPN 端點時，請考慮下列事項：

- 如果您使用 Active Directory 來驗證使用者，則 Client VPN 端點必須屬於與用於 Active Directory 驗證的 AWS Directory Service 資源相同的帳號。
- 如果您使用以 SAML 為基礎的聯合身分驗證來驗證使用者，則 Client VPN 端點必須與您為定義 IDP 對信任關係而建立的 IAM SAML 身分識別提供者所屬的帳戶相同。AWS IAM SAML 身分識別提供者可以在同一 AWS 帳戶中的多個 Client VPN 端點之間共用。

# 疑難排解 AWS Client VPN

以下主題可協助您對 Client VPN 端點可能發生的問題進行故障診斷。

如需有關疑難排解用戶端用來連線到 Client VPN 之 OpenVPN 型軟體的更多資訊，請參閱《AWS Client VPN 使用者指南》中的[對您的 Client VPN 連接進行故障診斷](#)。

## 常見問題

- [無法解析 Client VPN 端點 DNS 名稱](#)
- [流量不會在子網路之間分割](#)
- [Active Directory 群組的授權規則未如預期般運作](#)
- [用戶端無法存取對等 VPC、Amazon S3 或網際網路](#)
- [對等 VPC、Amazon S3 或網際網路的存取斷斷續續](#)
- [用戶端軟體傳回 TLS 錯誤](#)
- [用戶端軟體傳回使用者名稱和密碼錯誤 \(Active Directory 身分驗證\)](#)
- [用戶端軟體傳回使用者名稱和密碼錯誤 \(聯合驗證\)](#)
- [用戶端無法連線 \(交互身分驗證\)](#)
- [用戶端傳回的登入資料超過大小上限錯誤 \(聯合身分驗證\)](#)
- [用戶端無法開啟瀏覽器 \(聯合身分驗證\)](#)
- [用戶端傳回沒有可用的連接埠錯誤 \(聯合身分驗證\)](#)
- [VPN 連接由於 IP 不匹配而終止](#)
- [將流量路由到 LAN 無法如預期般運作](#)
- [確認 Client VPN 端點的頻寬限制](#)

## 無法解析 Client VPN 端點 DNS 名稱

### 問題

我無法解析 Client VPN 端點的 DNS 名稱。

### 原因

Client VPN 端點組態檔案包含一個名為 `remote-random-hostname` 的參數。此參數會強制用戶端在 DNS 名稱前面加上隨機字串，以防止 DNS 快取。有些用戶端無法辨識這個參數，因此它們不會在 DNS 名稱前面加上必要的隨機字串。

## 解決方案

使用您偏好的文字編輯器開啟 Client VPN 端點組態檔案。找出指定 Client VPN 端點 DNS 名稱的行，並在前面加上隨機字串，使格式成為 *random\_string.displayed\_DNS\_name*。例如：

- 原始 DNS 名稱：cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com
- 修改過的 DNS 名稱：asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com

## 流量不會在子網路之間分割

### 問題

我嘗試在兩個子網路之間分割網路流量。私有流量應透過私有子網路路由，而網際網路流量應透過公有子網路路由。但是，即使我已將兩個路由都新增到 Client VPN 端點路由表中，仍只使用一個路由。

### 原因

您可以將多個子網路與用戶端 VPN 端點產生關聯，但每個可用區域只能關聯一個子網路。多個子網路關聯的目的是為用戶端提供高可用性和可用區域備援。不過，用戶端 VPN 不會讓您選擇性地分割與用戶端 VPN 端點相關聯的子網路之間的流量。

用戶端會根據 DNS 循環配置資源演算法連線到用戶端 VPN 端點。這表示其流量可以在建立連線時透過任何關聯的子網路路由傳送。因此，如果用戶端登陸在沒有必要路由項目的關聯子網路上，可能會遇到連線問題。

例如，假設您設定下列子網路關聯和路由：

- 子網路關聯
  - 關聯 1：子網路 A (us-east-1a)
  - 關聯 2：子網路 B (us-east-1b)
- 路由
  - 路由 1：10.0.0.0/16 路由到子網路 A
  - 路由 2：172.31.0.0/16 路由到子網路 B

在此範例中，連線時登陸子網路 A 的用戶端無法存取路由 2，而連線時登陸子網路 B 的用戶端無法存取路由 1。

## 解決方案

確認用戶端 VPN 端點與每個關聯網路的目標具有相同的路由項目。這可確保用戶端能夠存取所有路由，而不論其流量是透過哪個子網路路由傳送。

# Active Directory 群組的授權規則未如預期般運作

## 問題

我已為我的 Active Directory 群組設定授權規則，但它們並未如預期般運作。我新增了 0.0.0.0/0 的授權規則來授權所有網路的流量，但是特定目的地 CIDR 的流量仍然失敗。

## 原因

授權規則在網路 CIDR 上編製索引。授權規則必須授與 Active Directory 群組對特定網路 CIDR 的存取權。0.0.0.0/0 的授權規則會視為特殊情況來處理，因此不論建立授權規則的順序為何，都會最後才評估。

例如，假設您以下列順序建立五個授權規則：

- 規則 1：群組 1 可存取 10.1.0.0/16
- 規則 2：群組 1 可存取 0.0.0.0/0
- 規則 3：群組 2 可存取 0.0.0.0/0
- 規則 4：群組 3 可存取 0.0.0.0/0
- 規則 5：群組 2 可存取 172.131.0.0/16

在此範例中，最後評估規則 2、規則 3 和規則 4。群組 1 僅具有 10.1.0.0/16 的存取權，而群組 2 僅具有 172.131.0.0/16 的存取權。群組 3 沒有 10.1.0.0/16 或 172.131.0.0/16 的存取權，但它可以存取所有其他網路。如果您移除規則 1 和 5，則所有三個群組都可以存取所有網路。

評估授權規則時，Client VPN 會使用最長字首比對。請參閱 Amazon VPC 使用者指南中的[路由優先順序](#)以取得更多詳細資訊。

## 解決方案

確認您是否建立明確授與 Active Directory 群組存取特定網路 CIDR 的授權規則。如果您新增 0.0.0.0/0 的授權規則，請記住此規則將最後評估，而前面的授權規則可能會限制其授與存取權的網路。

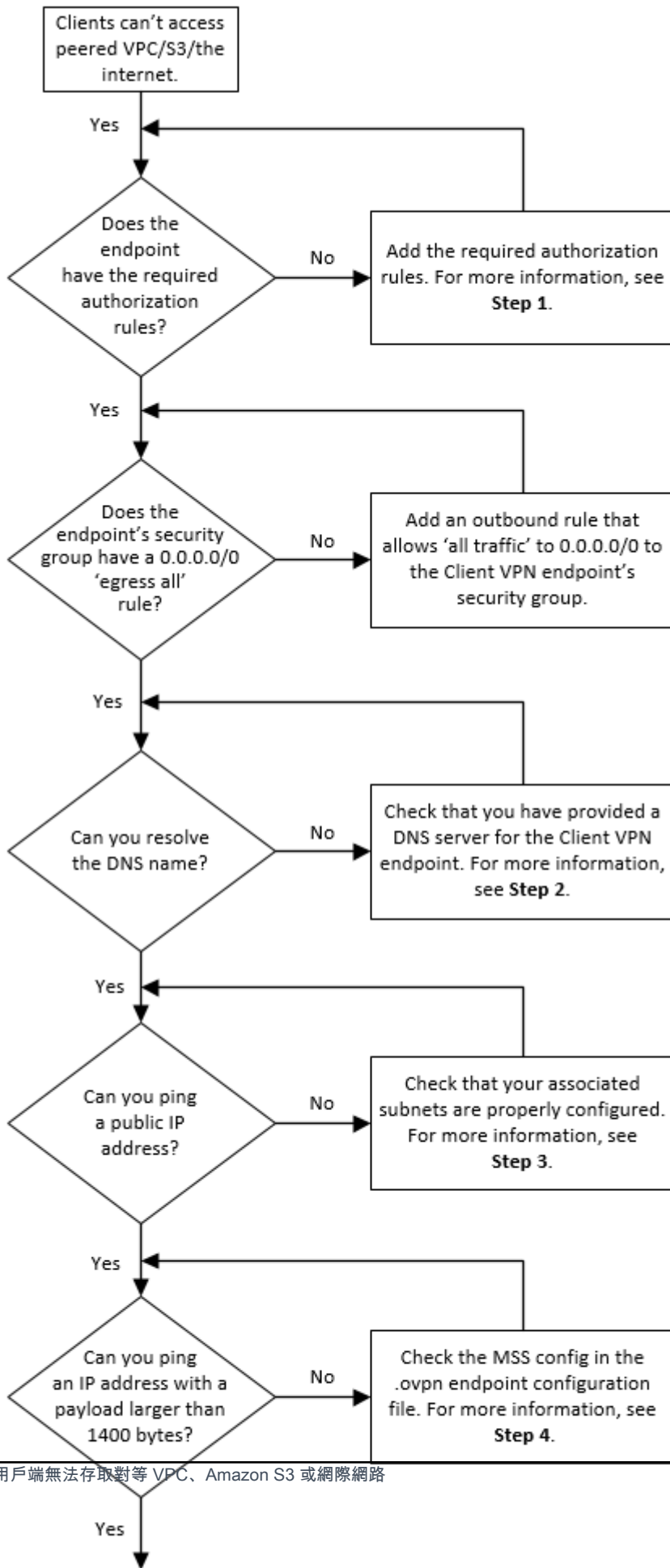
# 用戶端無法存取對等 VPC、Amazon S3 或網際網路

## 問題

我已經正確設定 Client VPN 端點路由，但用戶端卻無法存取對等 VPC、Amazon S3 或網際網路。

## 解決方案

下列流程圖包含診斷網際網路、對等 VPC 和 Amazon S3 連線問題的步驟。



1. 若要存取網際網路，請新增 `0.0.0.0/0` 的授權規則。

若要存取對等 VPC，請為 VPC 的 IPv4 CIDR 範圍新增授權規則。

若要存取 S3，請指定 Amazon S3 端點的 IP 地址。

2. 請檢查您是否能夠解析 DNS 名稱。

如果您無法解析 DNS 名稱，請確認已為 Client VPN 端點指定 DNS 伺服器。如果您管理自己的 DNS 伺服器，請指定其 IP 地址。確認 DNS 伺服器可從 VPC 存取。

如果不確定要為 DNS 伺服器指定哪個 IP 地址，請在 VPC 中的 `.2` IP 地址指定 VPC DNS 解析程式。

3. 對於網際網路存取，請檢查您是否能夠 ping 公用 IP 地址或公用網站，例如 `amazon.com`。如果您沒有收到回應，請確定關聯子網路的路由表具有預設路由，其以網際網路閘道或 NAT 閘道為目標。如果預設路由已存在，請確認關聯的子網路沒有會封鎖傳入和傳出流量的網路存取控制清單規則。

如果您無法連上對等 VPC，請確認關聯子網路的路由表具有對等 VPC 的路由項目。

如果您無法連線到 Amazon S3，請確認關聯子網路的路由表具有閘道 VPC 端點的路由項目。

4. 檢查您是否可以使用大於 1400 位元組的承載 ping 公有 IP 地址。請使用以下其中一個命令：

- Windows

```
C:\> ping 8.8.8.8 -l 1480 -f
```

- Linux

```
$ ping -s 1480 8.8.8.8 -M do
```

如果您無法使用 1400 位元組以上的承載對 IP 地址執行 ping 命令，請使用您偏好的文字編輯器開啟 Client VPN 端點 `.ovpn` 組態檔案，然後新增下列項目。

```
mssfix 1328
```

## 對等 VPC、Amazon S3 或網際網路的存取斷斷續續

### 問題

連線到對等 VPC、Amazon S3 或網際網路時，我的連線斷斷續續，但關聯子網路的存取不受影響。我需要中斷連接並重新連接以解決連接問題。

### 原因

用戶端會根據 DNS 循環配置資源演算法連線到用戶端 VPN 端點。這表示其流量可以在建立連線時透過任何關聯的子網路路由傳送。因此，如果用戶端登陸在沒有必要路由項目的關聯子網路上，可能會遇到連線問題。

### 解決方案

確認用戶端 VPN 端點與每個關聯網路的目標具有相同的路由項目。這可確保用戶端能夠存取所有路由，而不論其流量是透過哪個關聯的子網路。

例如，假設您的用戶端 VPN 端點有三個關聯的子網路 (子網路 A、B 和 C)，而您想要為用戶端啟用網際網路存取。若要這樣做，您必須新增三個 `0.0.0.0/0` 路由 - 每個各以一個關聯子網路為目標：

- 路由 1：`0.0.0.0/0` 用於子網路 A
- 路由 2：`0.0.0.0/0` 用於子網路 B
- 路由 3：`0.0.0.0/0` 用於子網路 C

## 用戶端軟體傳回 TLS 錯誤

### 問題

我的用戶端以前可以成功連線到 Client VPN，但現在 OpenVPN 型用戶端在嘗試連線時會傳回以下錯誤之一：

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

可能的原因 1：



如果您使用交互式身分驗證並匯入用戶端憑證撤銷清單，則用戶端憑證撤銷清單可能已過期。在身分驗證階段期間，Client VPN 端點會根據您匯入的用戶端憑證撤銷清單來檢查用戶端憑證。如果用戶端憑證撤銷清單已過期，您就無法連線到 Client VPN 端點。

#### 解決方案 1：

使用 OpenSSL 工具檢查用戶端憑證撤銷清單的到期日。

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

輸出會顯示到期日期和時間。如果用戶端憑證撤銷清單已過期，您必須建立新的清單並將其匯入 Client VPN 端點。如需詳細資訊，請參閱 [用戶端憑證撤銷清單](#)。

#### 可能的原因 2：

用於 Client VPN 端點的伺服器憑證已過期。

#### 解決方案 2：

在 AWS Certificate Manager 主控台或使用 AWS CLI 檢查伺服器憑證的狀態。如果伺服器憑證已過期，建立新憑證並上傳至 ACM。有關使用 [OpenVPN easy-rsa 實用程序](#) 產生伺服器和用戶端憑證及金鑰，然後將它們匯入 ACM 中的詳細步驟，請參閱 [交互身分驗證](#)。

或者，可能是用戶端用來連線到 Client VPN 的 OpenVPN 型軟體有問題。如需對 OpenVPN 型軟體進行故障診斷的更多資訊，請參閱《AWS Client VPN Client VPN 使用者指南》中的 [對您的 Client VPN 連接進行故障診斷](#)。

## 用戶端軟體傳回使用者名稱和密碼錯誤 (Active Directory 身分驗證)

### 問題

我的 Client VPN 端點使用 Active Directory 身分驗證，以前能夠成功連線到 Client VPN。但是現在，用戶端取得無效的使用者名稱和密碼錯誤。

### 可能原因

如果您使用 Active Directory 身分驗證，且在分發用戶端組態檔案之後啟用多重要素驗證 (MFA)，則檔案不包含提示使用者輸入其 MFA 代碼的必要資訊。系統會提示使用者只輸入其使用者名稱和密碼，且身分驗證失敗。

### 解決方案

下載新的用戶端組態檔案，並將它分發到您的用戶端。確認新檔案是否包含下列程式碼行。

```
static-challenge "Enter MFA code " 1
```

如需詳細資訊，請參閱 [匯出和設定用戶端組態檔](#)。測試您 Active Directory 的 MFA 組態，而不使用 Client VPN 端點確認 MFA 是否如預期運作。

## 用戶端軟體傳回使用者名稱和密碼錯誤 (聯合驗證)

### 問題

嘗試使用聯合身份驗證使用用戶名和密碼登錄，並收到錯誤「收到的憑據不正確。請聯絡您的 IT 管理員。」

### 原因

此錯誤的原因可能是由於 IdP 的 SAML 回應中包含至少一個屬性。

### 解決方案

請確定 IdP 的 SAML 回應中包含至少一個屬性。如需更多資訊，請參閱 [SAML 型 IdP 組態資源](#)。

## 用戶端無法連線 (交互身分驗證)

### 問題

我在 Client VPN 端點使用交互身分驗證。用戶端取得 TLS 金鑰交涉失敗錯誤和逾時錯誤。

### 可能原因

提供給用戶端的組態檔案不包含用戶端憑證和用戶端私有金鑰，或是憑證和金鑰不正確。

### 解決方案

確定組態檔案包含正確的用戶端憑證和金鑰。如有必要，請修正組態檔案並將其重新分發給您的用戶端。如需詳細資訊，請參閱 [匯出和設定用戶端組態檔](#)。

## 用戶端傳回的登入資料超過大小上限錯誤 (聯合身分驗證)

### 問題

我在 Client VPN 端點使用聯合身分驗證。當用戶端在 SAML 型身分提供者 (IdP) 瀏覽器視窗中輸入其使用者名稱和密碼時，會收到登入資料超過支援大小上限的錯誤。

### 原因

IdP 傳回的 SAML 回應超過支援的大小上限。如需詳細資訊，請參閱 [SAML 型聯合身分驗證的需求和考量](#)。

### 解決方案

請嘗試減少 IdP 中使用者所屬的群組數目，然後再試一次連線。

## 用戶端無法開啟瀏覽器 (聯合身分驗證)

### 問題

我在 Client VPN 端點使用聯合身分驗證。當用戶端嘗試連線到端點時，用戶端軟體不會開啟瀏覽器視窗，而是顯示使用者名稱和密碼快顯視窗。

### 原因

提供給用戶端的組態檔案不包含 `auth-federate` 旗標。

### 解決方案

[匯出最新的組態檔案](#)，將其匯入 AWS 提供的用戶端，然後再次嘗試連線。

## 用戶端傳回沒有可用的連接埠錯誤 (聯合身分驗證)

### 問題

我在 Client VPN 端點使用聯合身分驗證。當用戶端嘗試連線到端點時，用戶端軟體會傳回下列錯誤：

```
The authentication flow could not be initiated. There are no available ports.
```

### 原因

AWS 提供的用戶端需要使用 TCP 連接埠 35001 才能完成驗證。如需詳細資訊，請參閱 [SAML 型聯合身分驗證的需求和考量](#)。

### 解決方案

請確認用戶端的裝置未封鎖 TCP 連接埠 35001，或將它用於不同的程序。

## VPN 連接由於 IP 不匹配而終止

### 問題

VPN 連線終止，用戶端軟體會傳回下列錯誤："The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."

### 原因

AWS 提供的用戶端要求其所連線的 IP 位址與支援 Client VPN 端點的 VPN 伺服器 IP 相符。如需詳細資訊，請參閱 [規則和最佳做法 AWS Client VPN](#)。

### 解決方案

確認 AWS 提供的用戶端和 Client VPN 端點之間沒有 DNS 代理。

## 將流量路由到 LAN 無法如預期般運作

### 問題

當 LAN IP 位址範圍不在下列標準私有 IP 位址範圍內時，嘗試將流量路由到區域網路 (LAN) 無法如預期般運作：10.0.0.0/8、172.16.0.0/12、192.168.0.0/16、或 169.254.0.0/16。

### 原因

如果偵測到用戶端區域網路位址範圍超出上述標準範圍，Client VPN 端點會自動將 OpenVPN 指令「重新導向閘道區塊本機」推送到用戶端，強制將所有 LAN 流量進入 VPN。如需詳細資訊，請參閱 [規則和最佳做法 AWS Client VPN](#)。

### 解決方案

如果您在 VPN 連線期間需要 LAN 存取，建議您針對 LAN 使用上述的傳統位址範圍。

## 確認 Client VPN 端點的頻寬限制

### 問題

我需要確認 Client VPN 端點的頻寬限制。

### 原因

輸送量取決於多個因素，例如來自您位置的連線容量，以及電腦上 Client VPN 桌面應用程式和 VPC 端點之間的網路延遲。每個使用者連線也有 10 Mbps 的頻寬限制。

### 解決方案

執行下列命令以驗證頻寬。

```
sudo iperf3 -s -V
```

在用戶端上：

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

# Client VPN 使用者指南的文件歷程記錄

下表說明《AWS Client VPN 管理員指南》的更新。

變更	描述	日期
<a href="#">授權規則範例</a>	新增授權規則的範例案例。	2022 年 9 月 15 日
<a href="#">VPN 工作階段最長持續時間</a>	您可以設定較短的 VPN 工作階段持續時間上限來滿足安全性與合規的要求。	2022 年 1 月 20 日
<a href="#">用戶端登入橫幅</a>	您可以在 AWS 提供的 Client VPN 桌面應用程式上啟用文字橫幅 (當系統建立了 VPN 工作階段時) 以滿足法規與合規需求。	2022 年 1 月 20 日
<a href="#">用戶端連線處理器</a>	您可以為 Client VPN 端點啟用用戶端連線處理器，以執行可授權新連線的自訂邏輯。	2020 年 11 月 4 日
<a href="#">自助式入口網站</a>	您可以在 Client VPN 端點上為您的用戶端啟用自助式入口網站。	2020 年 10 月 29 日
<a href="#">用戶端對用戶端的存取權限</a>	您可以讓連線到 Client VPN 端點的用戶端互相連線。	2020 年 9 月 29 日
<a href="#">SAML 2.0 型同盟驗證</a>	您可以使用 SAML 2.0 型聯合身分驗證來驗證 Client VPN 使用者。	2020 年 5 月 19 日
<a href="#">在建立期間指定安全群組</a>	您可以在建立 AWS Client VPN 端點時指定 VPC 和安全群組。	2020 年 3 月 5 日

---

<a href="#">可設定的 VPN 連接埠</a>	您可以為 AWS Client VPN 端點指定支援的 VPN 連接埠編號。	2020 年 1 月 16 日
<a href="#">支援 Multi-Factor Authentication (MFA)</a>	如果已為 Active Directory 啟用 MFA，則您的 AWS Client VPN 端點支援 MFA。	2019 年 9 月 30 日
<a href="#">支援分割通道</a>	您可以在 AWS Client VPN 端點上啟用分割通道。	2019 年 7 月 24 日
<a href="#">初始版本</a>	此版本推出 AWS Client VPN。	2018 年 12 月 18 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。