aws

管理員指南

AWS Client VPN

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

AWS Client VPN: 管理員指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 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 2
使用 Client VPN 3
Client VPN 的定價 4
規則和最佳實務 5
網路和頻寬需求 5
子網路和 VPC 組態 6
身分驗證和安全性 6
連線和 DNS 需求 7
限制 7
Client VPN 的運作方式 8
案例和範例 9
用戶端身分驗證 18
Active Directory 身分驗證 19
交互身分驗證 20
單一登入 (SAML 2.0 型聯合身分驗證) 25
客戶端授權 30
安全群組 30
以網路為基礎的授權 30
建立端點安全群組規則 31
連線授權 31
需求和考量事項 32
Lambda 界面 32
使用用戶端連線處理常式進行姿勢評估 34
啟用用戶端連線處理常式 34
服務連結角色 35
監控連線授權失敗 35
分割通道 Client VPN 35
分割隧道的優點 36
路由傳送考量 36
啟用分割通道 36
連線日誌記錄 37
連線日誌項目 37

擴展考量 39
Client VPN 入門 41
先決條件 42
步驟 1：選擇您的端點類型 42
步驟 2：產生伺服器和用戶端憑證和金鑰 42
步驟 3：建立 Client VPN 端點 42
步驟 4：關聯目標網路 44
步驟 5：新增 VPC 的授權規則 44
步驟 6：提供網際網路的存取權 45
步驟 7：驗證安全群組需求 46
步驟 8：下載 Client VPN 端點組態檔案 46
步驟 9：連線至 Client VPN 端點 47
使用 Client VPN 48
自助式入口網站存取 49
授權規則 49
重點 50
範例方案 50
新增授權規則 60
移除授權規則 61
檢視授權規則 61
用戶端憑證撤銷清單 62
產生用戶端憑證撤銷清單 62
匯入用戶端憑證撤銷清單 64
匯出用戶端憑證撤銷清單 65
用戶端連線 65
查看用戶端連線 65
終止用戶端連線 66
用戶端登入橫幅 66
橫幅建立 67
設定現有端點的用戶端登入橫幅 67
停用端點的用戶端登入橫幅 67
修改現有的橫幅文字 68
檢視目前設定的登入橫幅 68
用戶端路由強制執行 69
要求 69
路由衝突 70

考量事項 70
啟用用戶端路由強制執行 71
停用用戶端路由強制執行 72
疑難排解 IPv6 用戶端路由強制執行 72
端點 73
建立 Client VPN 端點的需求 74
IP 地址類型 74
端點修改 75
建立端點 77
檢視 端點 82
修改端點 82
刪除端點 85
連線日誌 85
啟用新 端點的連線日誌記錄 86
啟用現有 端點的連線日誌記錄 87
檢視連線日誌 87
關閉連線日誌記錄 88
用戶端組態檔案匯出 88
匯出用戶端組態檔 89
為交互身分驗證新增用戶端憑證和金鑰資訊 90
路由 91
在 Client VPN 端點上使用分割通道的考量事項 91
建立端點路由 92
檢視端點路由 92
刪除端點路由 93
目標網路 93
建立目標網路的需求 93
將目標網路與端點建立關聯 94
將安全群組套用到目標網路 95
檢視目標網路 96
取消目標網路與端點的關聯 96
VPN 工作階段持續時間上限 96
在建立端點期間設定 VPN 工作階段上限 97
檢視目前 VPN 工作階段持續時間上限 97
修改 VPN 工作階段持續時間上限 98
傳輸閘道與 Client VPN 整合 98

概觀 99
優勢 99
Transit Gateway 整合的運作方式 100
先決條件 100
建立 Transit Gateway Client VPN 端點 101
管理路由 104
設定授權 105
管理可用區域 106
跨帳戶傳輸閘道存取 107
考量和限制 107
安全 109
資料保護 109
傳輸中加密 110
網際網路流量隱私權 110
身分與存取管理 111
目標對象 111
使用身分驗證 111
使用政策管理存取權 113
AWS Client VPN 如何使用 IAM 114
身分型政策範例 118
疑難排解 120
使用服務連結角色 121
恢復能力 124
提供高可用性的多個目標網路 124
基礎設施安全性 125
最佳實務 125
IPv6 考量因素 126
IPv6 支援的關鍵元件 126
IPv6 用戶端 CIDR 指派 127
相容性要求 127
DNS 支援 127
限制 127
IPv6 的用戶端路由強制執行 127
IPv6 洩漏預防 （舊版資訊） 128
監控 Client VPN 130
CloudWatch 指標 130

檢視 CloudWatch 指標 133
配額 134
Client VPN 配額 134
使用者和群組配額 135
一般考量 135
疑難排解 136
無法解析 Client VPN 端點 DNS 名稱 136
流量不會在子網路之間分割 137
Active Directory 群組的授權規則未如預期般運作 138
用戶端無法存取對等 VPC、Amazon S3 或網際網路 139
對等 VPC、Amazon S3 或網際網路的存取斷斷續續 142
用戶端軟體傳回 TLS 錯誤 142
用戶端軟體傳回使用者名稱和密碼錯誤 — Active Directory 身分驗證 143
用戶端軟體會傳回使用者名稱和密碼錯誤 — 聯合身分驗證 144
用戶端無法連線 — 交互身分驗證 144
用戶端傳回的登入資料超過大小上限錯誤 — 聯合身分驗證 145
用戶端不會開啟瀏覽器 — 聯合身分驗證 145
用戶端未傳回任何可用的連接埠錯誤 — 聯合身分驗證 146
由於 IP 不相符而終止 VPN 連線 146
將流量路由到 LAN 無法如預期般運作 146
驗證端點的頻寬限制 147
Client VPN 通道連線 147
網路連線先決條件 148
檢查 Client VPN 端點狀態 148
驗證用戶端連線 149
驗證用戶端身分驗證 149
檢查授權規則 149
驗證 Client VPN 路由 150
驗證安全群組和網路 ACLs 150
測試用戶端連線 151
診斷用戶端裝置 151
故障診斷 DNS 解析 152
對效能進行故障診斷 152
監控 Client VPN 指標 153
檢查 Client VPN 日誌 153
常見問題與解決方案 153

文件歷史紀錄 155
..... clvii

什麼是 AWS Client VPN？

AWS Client VPN 是一種受管的用戶端型 VPN 服務，可讓您安全地存取內部部署網路中的 AWS 資源和資源。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。

主題

- Client VPN 的功能
- Client VPN 的元件
- 使用 Client VPN
- Client VPN 的定價
- 使用 的規則和最佳實務 AWS Client VPN

Client VPN 的功能

Client VPN 提供以下特色和功能：

- 安全連線 — 透過 OpenVPN 用戶端從任何位置建立加密的 TLS 連線，以確保資料隱私權和完整性。
- 受管服務 — 透過完整的 AWS 管理，免除部署和維護第三方遠端存取 VPN 解決方案的操作負擔。
- 高可用性和彈性 — 動態擴展以適應連接到 AWS 和內部部署資源的各種使用者數量，而無需手動介入。
- 身分驗證 — 支援多種身分驗證方法，包括 Active Directory 整合、聯合身分驗證和憑證型身分驗證，以實現靈活的身分管理。
- 精細控制 — 透過可在 Active Directory 群組層級設定的網路型存取規則和安全群組型存取控制，實作精確的安全控制。
- 易於使用 — 透過單一 VPN 通道提供對 AWS 和內部部署資源的統一存取，簡化最終使用者體驗。
- 可管理性 — 透過詳細的連線日誌和即時管理功能提供全面的可見性，包括在必要時監控和終止作用中用戶端連線的能力。
- 深度整合 — 與現有的 AWS 服務無縫整合，包括 AWS Directory Service 和 Amazon VPC，增強您雲端基礎設施的連線能力。
- 彈性網路架構 — 同時支援 VPC 子網路關聯和直接傳輸閘道附件。如需詳細資訊，請參閱傳輸閘道與 Client VPN 整合。
- IPv6 支援 — 啟用 Client VPN 端點的完整 IPv6 連線，支援 VPCs中 IPv6 資源的連線，以及來自 IPv6 網路上用戶端的連線，以滿足現代聯網需求。

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。它是所有用户端 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。您可以關聯 VPC 子網路或直接連接至 AWS Transit Gateway。如需 Transit Gateway 整合的詳細資訊，請參閱 傳輸閘道與 Client VPN 整合。

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。對於 IPv4 流量，您可以選擇用戶端 CIDR 範圍，例如 `10.2.0.0/16`。對於 IPv6 流量， AWS Client VPN 會自動指派用戶端 CIDR 範圍。

用戶端 VPN 連接埠

AWS Client VPN 支援 TCP 和 UDP 的連接埠 443 和 1194。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。對於 IPv4 流量，會套用來源網路位址轉譯 (SNAT)，其中來自用戶端 CIDR 範圍的來源 IP 地址會轉譯為 Client VPN 網路介面 IP 地址。對於 IPv6 流量，不會套用 SNAT，從而增強對連線使用者的 IP 地址的可見性。

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。自助式入口網站是一項全球服務，由下列區域中的服務堆疊提供支援：美國東部（維吉尼亞北部）、亞太區域（東京）、歐洲（愛爾蘭）和 AWS GovCloud (US-West)。

端點 IP 地址類型

Client VPN 端點的 IP 地址類型，可以是 IPv4、IPv6 或雙堆疊 (IPv4 和 IPv6)。

流量 IP 地址類型

流經 Client VPN 端點的流量 IP 地址類型，可以是 IPv4、IPv6 或雙堆疊 (IPv4 和 IPv6)。這會決定每個端點的內部流量類型（透過 VPN 連線通道的實際承載或原始流量）、用戶端 CIDR 範圍、子網路關聯、路由和規則。

使用 Client VPN

您可以透過以下任何方式來使用 Client VPN：

AWS 管理主控台

主控台為 Client VPN 提供 Web 型使用者界面。

主控台為 Client VPN 提供兩種設定方法的 Web 型使用者介面：

- 快速入門設定：使用 AWS 建議的預設值簡化端點建立
- 標準設定：完全控制所有組態選項

如果您已註冊 AWS 帳戶，您可以登入 Amazon VPC 主控台，然後在導覽窗格中選取 Client VPN。

AWS Command Line Interface (AWS CLI)

AWS CLI 可讓您直接存取 Client VPN 公有 APIs。Windows、macOS 和 Linux 都提供支援。如需入門的詳細資訊 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 Amazon EC2 命令列參考的 EC2 一節。 Amazon EC2

AWS Tools for Windows PowerShell

AWS 為在 PowerShell 環境中編寫指令碼的人員提供廣泛的 AWS 產品命令。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)。使用 IPv6 或雙堆疊端點無需額外費用；它們的收費費率與 IPv4 端點相同。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

如果您啟用 Client VPN 端點的連線日誌記錄，則必須在帳戶中建立 CloudWatch Logs 日誌群組。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 Paid tier (付費層級) 下，選擇 Logs (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 端點與目標網路相關聯，該網路是 VPC 中的子網路。如果此 VPC 具有網際網路閘道，我們會將彈性 IP 地址與 Client VPN 彈性網路介面 (ENIs建立關聯。這些彈性 IP 地址會以使用中的公有 IPv4 地址收費。如需詳細資訊，請參閱 VPC 定價頁面上的公有 IPv4 地址索引標籤。

> **Note**
>
> Client VPN 端點在與具有網際網路閘道的 VPC 子網路相關聯時需要彈性 IP 地址，因為這些 EIPs可為 VPN 用戶端啟用直接網際網路連線。透過 Client VPN 端點連線時，他們需要公有 IP 地址才能與網際網路資源通訊。彈性 IPs提供一致的公開端點來實現此目的。這些 EIPs會連接到 Client VPN 彈性網路介面 (ENIs)，對於為 VPN 用戶端維持穩定、安全的網際網路存取，同時確保適當的流量路由至關重要。由於這些彈性 IP 地址已配置並主動用於 Client VPN 服務，

會依照其配置和相關聯 EIPs 的標準定價模式，將它們 AWS 做為使用中的公有 IPv4 地址收費。

使用 的規則和最佳實務 AWS Client VPN

下列各節說明使用 的規則和最佳實務 AWS Client VPN：

主題

- 網路和頻寬需求
- 子網路和 VPC 組態
- 身分驗證和安全性
- 連線和 DNS 需求
- 限制

網路和頻寬需求

- AWS Client VPN 是一種全受管服務，可自動擴展以適應額外的使用者連線和頻寬需求。每個使用者連線的最大基準頻寬為 50 Mbps。

  您透過 Client VPN 端點連線的實際頻寬可能會因多種因素而有所不同。這些因素包括封包大小、流量合成 (TCP/UDP 混合）、中繼網路上的網路政策 （成形或限流）、網際網路條件、應用程式特定需求，以及並行使用者連線的總數。如果您達到最大頻寬限制，您可以透過 AWS Support 請求增加頻寬。
- 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，就無法變更用戶端 CIDR 範圍。
- Client VPN 支援 IPv4、IPv6 和雙堆疊 (IPv4 和 IPv6) 流量。如需 IPv6 支援的詳細資訊，請參閱 的 IPv6 考量 AWS Client VPN。
- • 來源 IP 地址會轉譯為 Client VPN 端點的 IP 地址。

  - 來自用戶端的原始來源連接埠號碼保持不變。
- Client VPN 只有在並行使用者連線到相同的目標時，才會執行連接埠地址轉譯 (PAT)。連接埠轉譯是自動且必要的，可透過相同的 VPN 端點支援多個同時連線。
  - 對於來源 IP 轉譯，來源 IP 地址會轉譯為 Client VPN 的 IP 地址。
  - 對於單一用戶端連線的來源連接埠轉譯，原始來源連接埠號碼可能保持不變。
  - 對於連接到相同目的地（相同目標 IP 地址和連接埠）的多個用戶端的來源連接埠轉譯，Client VPN 會執行連接埠轉譯，以確保唯一連線。

  例如，當兩個用戶端，用戶端 1 和用戶端 2，透過 Client VPN 端點連線到相同的目的地伺服器和連接埠：
  - 用戶端 1 的原始連接埠，例如9999，可能翻譯為不同的連接埠，例如連接埠 4306。
  - 用戶端 2 的原始連接埠 - 例如 9999 - 可能會轉譯為唯一的連接埠不同的格式用戶端 1 - 例如連接埠 63922。
- 對於 IPv6 流量，Client VPN 不會執行網路位址轉譯 (NAT)。這可增強對連線使用者的 IPv6 地址的可見性。

子網路和 VPC 組態

- 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。
- 對於 IPv6 或雙堆疊流量，關聯的子網路必須具有 IPv6 或雙堆疊 CIDR 範圍。
- 對於雙堆疊端點，您無法為每個可用區域建立多個子網路的關聯。

身分驗證和安全性

- 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。
- 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
```

- AWS Client VPN 中使用的憑證必須遵循 RFC 5280：網際網路 X.509 公有金鑰基礎設施憑證和憑證撤銷清單 (CRL) 設定檔，包括備註第 4.2 節中指定的憑證延伸。
- 具有特殊字元的使用者名稱可能會導致連線錯誤。

- 使用者名稱長度上限為 1024 個位元組。使用者名稱較長的連線將被拒絕。

連線和 DNS 需求

- 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，您也會在 CloudTrail 日誌中看到 Client VPN 網路界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。
- Client VPN 服務需要用戶端連線的 IP 地址符合 Client VPN 端點 DNS 名稱解析的 IP。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 名稱解析的實際 IP 地址，則此設定無法使用最近 AWS 提供的用戶端。新增此規則是為了減輕伺服器 IP 攻擊，如此處所述：TunnelCrack。
- 您可以使用 AWS 提供的用戶端連線到多個並行 DNS 工作階段。不過，若要讓名稱解析正常運作，所有連線的 DNS 伺服器都應有同步記錄。
- Client VPN 服務要求用戶端裝置的本機區域網路 (LAN) IP 地址範圍在下列標準私有 IP 地址範圍內：`10.0.0.0/8`、`192.168.0.0/16`、 `172.16.0.0/12`或 `169.254.0.0/16`。如果偵測到用戶端 LAN 地址範圍超出上述範圍，則 Client VPN 端點會自動將 OpenVPN 指令 "redirect-gateway block-local" 推送至用戶端，強制將所有 LAN 流量傳入 VPN。因此，如果您在 VPN 連線期間需要 LAN 存取，建議您為 LAN 使用上面列出的傳統地址範圍。強制執行此規則是為了降低本機網路攻擊的機會，如下所述：TunnelCrack。
- 在 Windows 中，使用完整通道端點時，無論端點的 IP 地址類型為何 (IPv4 IPv6 或雙堆疊），都會強制所有 DNS 流量通過通道。若要讓 DNS 正常運作，必須在通道內設定和連線 DNS 伺服器。

限制

- 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。
- 如果有多個使用者已登入作業系統，則無法從電腦建立 VPN 連線。
- IPv6 用戶端不支援Client-to-client通訊。如果 IPv6 用戶端嘗試與其他 IPv6 用戶端通訊，則會捨棄流量。
- IPv6 和雙堆疊端點需要使用者裝置和網際網路服務提供者 (ISPs) 支援對應的 IP 組態。

AWS Client VPN 運作方式

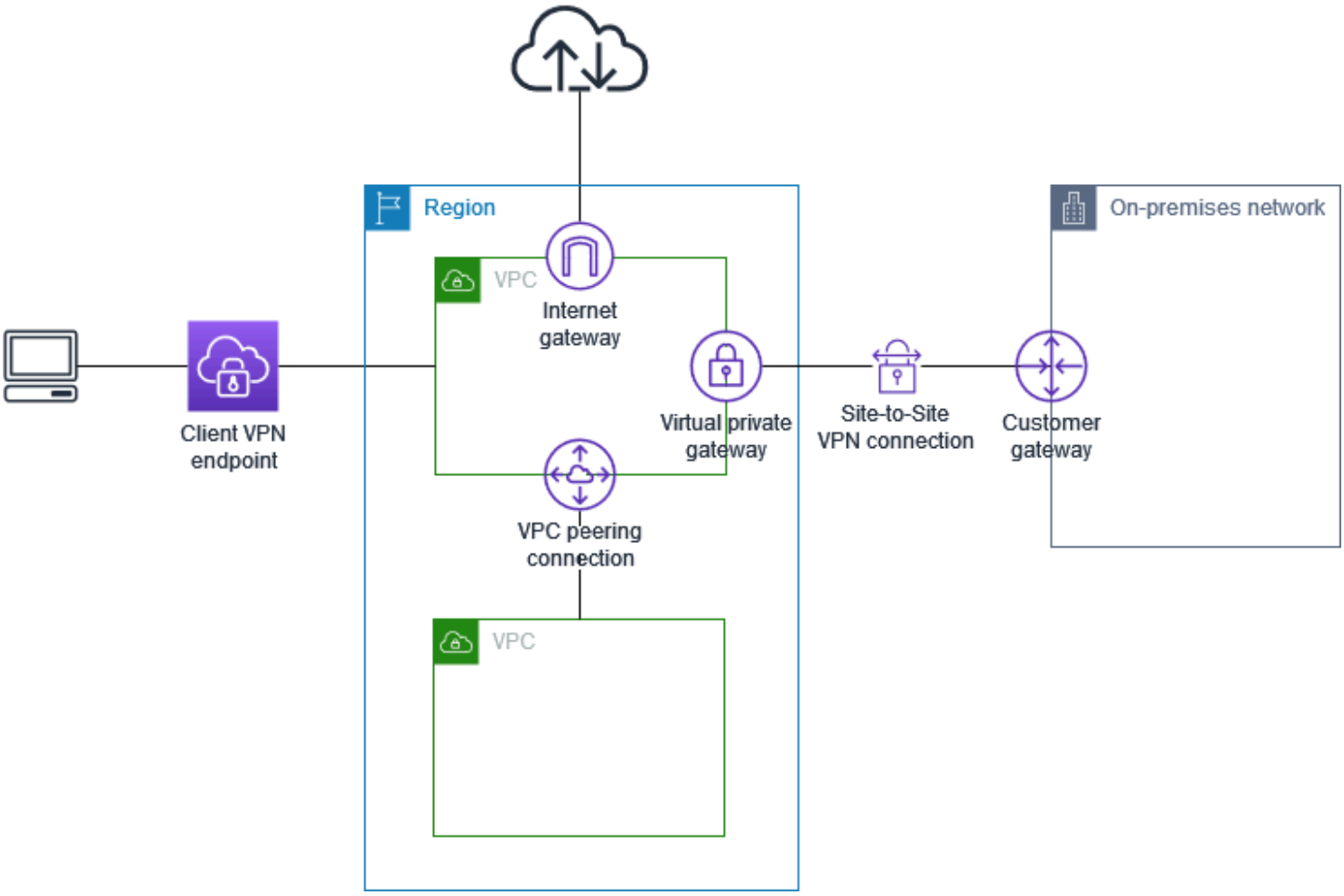
使用 時 AWS Client VPN，有兩種類型的使用者角色會與 Client VPN 端點互動：管理員和用戶端。

Client VPN 支援 IPv4、IPv6 和雙堆疊 (IPv4 和 IPv6) 連線。您可以建立使用 IPv4、IPv6 或兩者的端點，讓您連線到 VPCs中的 IPv6 資源，或從 IPv6 網路的用戶端連線。此彈性可協助已實作或正在轉換至 IPv6 基礎設施的組織。

管理員負責安裝和設定服務。這包括建立 Client VPN 端點、關聯目標網路、設定授權規則，以及設定其他路由（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，請參閱開始使用 AWS Client VPN。

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 AWS，他們也可以存取 中的其他資源、內部部署網路或其他用戶端。如需連線至 Client VPN 端點以建立 VPN 工作階段的詳細資訊，請參閱《 使用者指南》中的入門。 AWS Client VPN

下圖說明基本的 Client VPN 架構。



Client VPN 的案例和範例

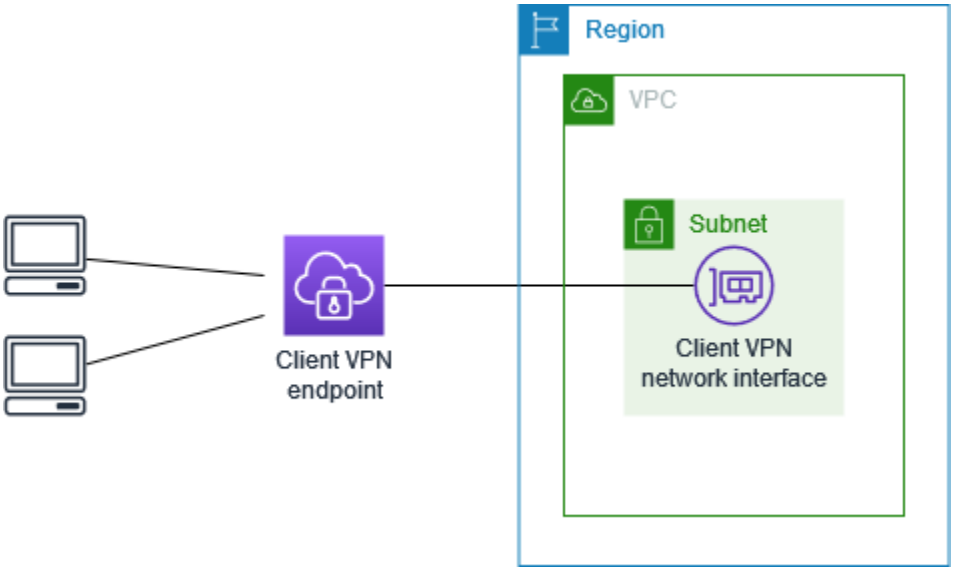
AWS Client VPN 是全受管遠端存取 VPN 解決方案，可讓您用來允許用戶端安全存取 AWS 和內部部署網路內的資源。設定存取的方式有多種選項。本節提供範例來示範為您的用戶端建立和設定 Client VPN 存取。

案例

- the section called “存取 VPC”
- the section called “存取對等 VPC”
- the section called “存取內部部署網路”
- the section called “存取網際網路”
- the section called “用戶端對用戶端的存取權限”
- the section called “限制存取您的網路”

使用 Client VPN 存取 VPC

此案例的 AWS Client VPN 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 使用 的規則和最佳實務 AWS Client VPN 檢閱 Client VPN 端點的規則和限制。

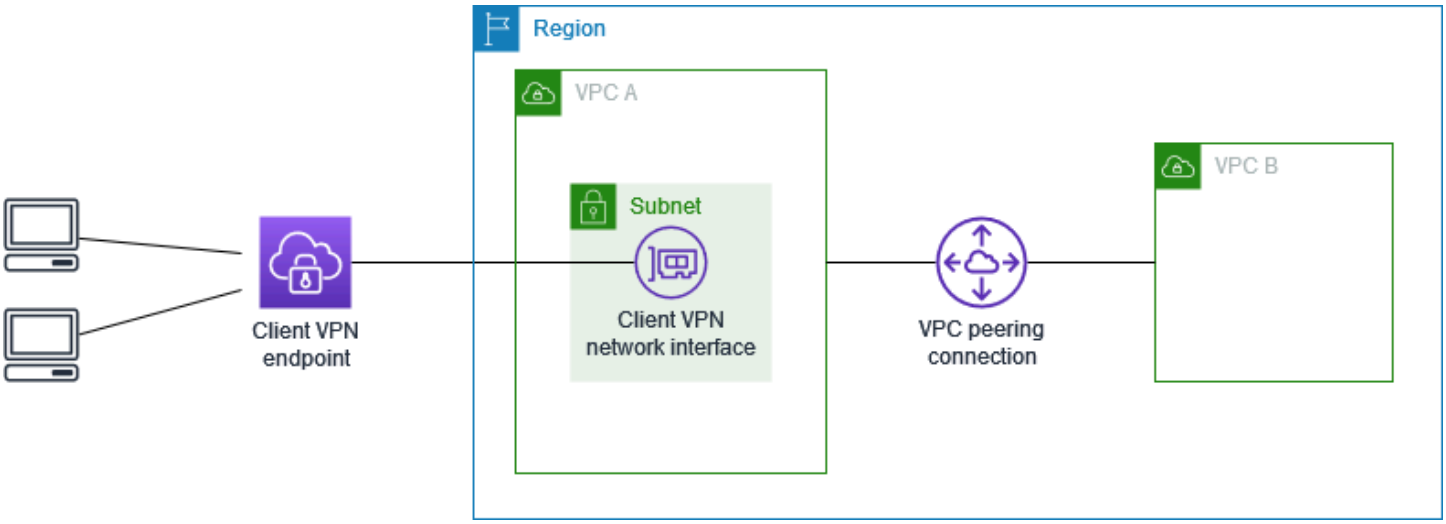
實作此組態

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AWS Client VPN端點中所述的步驟。
2. 將子網路與 Client VPN 端點建立關聯。若要執行此作業，請執行將目標網路與 AWS Client VPN 端點建立關聯中所述的步驟，然後選擇您稍早所識別的子網路和 VPC。
3. 新增授權規則讓用戶端存取 VPC。若要執行此作業，請執行新增授權規則中所述的步驟；並對於目的地網路，輸入 VPC 的 IPv4 CIDR 範圍。
4. 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。如需詳細資訊，請參閱安全群組。

使用 Client VPN 存取對等 VPC

此案例的 AWS Client VPN 組態包含與其他 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 內的資源，以及與其對等的其他 VPCs（例如 VPC B），建議您使用此組態。

> **Note**
>
> 只有在 Client VPN 端點設定為分割通道模式時，才需要允許存取對等 VPC （概述於網路圖表）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 使用 的規則和最佳實務 AWS Client VPN 檢閱 Client VPN 端點的規則和限制。

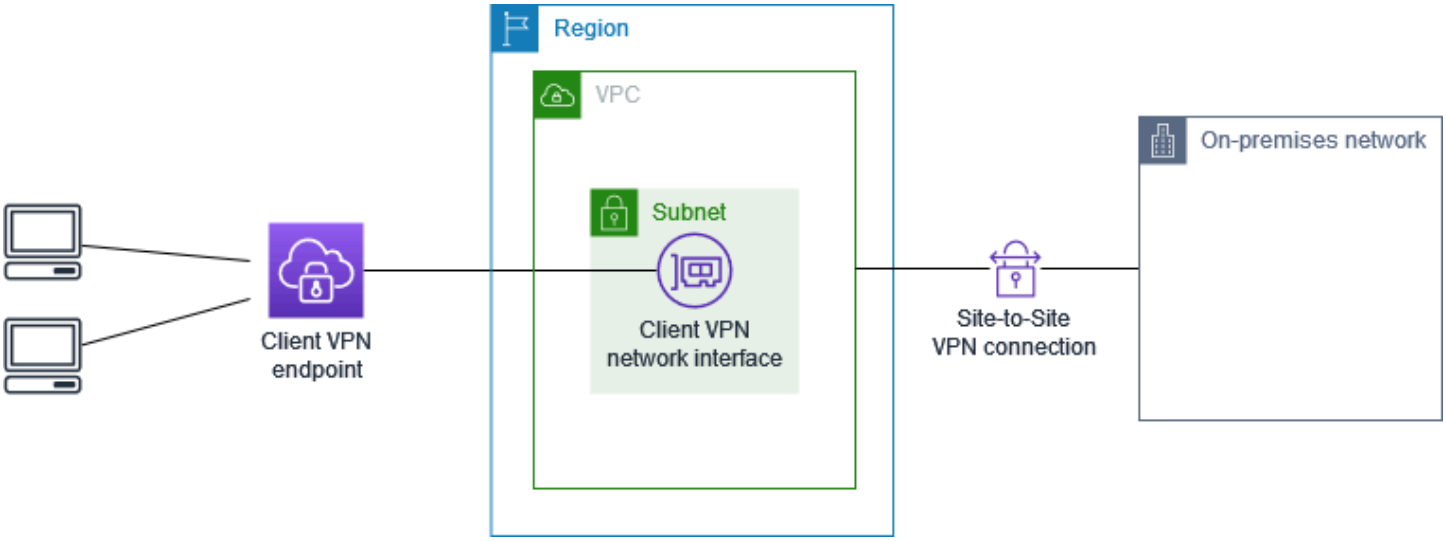
實作此組態

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AWS 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 將目標網路與 AWS Client VPN 端點建立關聯 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，請執行新增授權規則中所述的步驟。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 AWS Client VPN 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，請執行新增授權規則中所述的步驟。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 Client VPN 存取內部部署網路

此案例的 AWS Client VPN 組態僅包含對內部部署網路的存取。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 使用 的規則和最佳實務 AWS Client VPN 檢閱 Client VPN 端點的規則和限制。

實作此組態

1. 啟用 VPC 與您自己的內部部署網路之間透過 an AWS Site-to-Site VPN 連線的通訊。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。

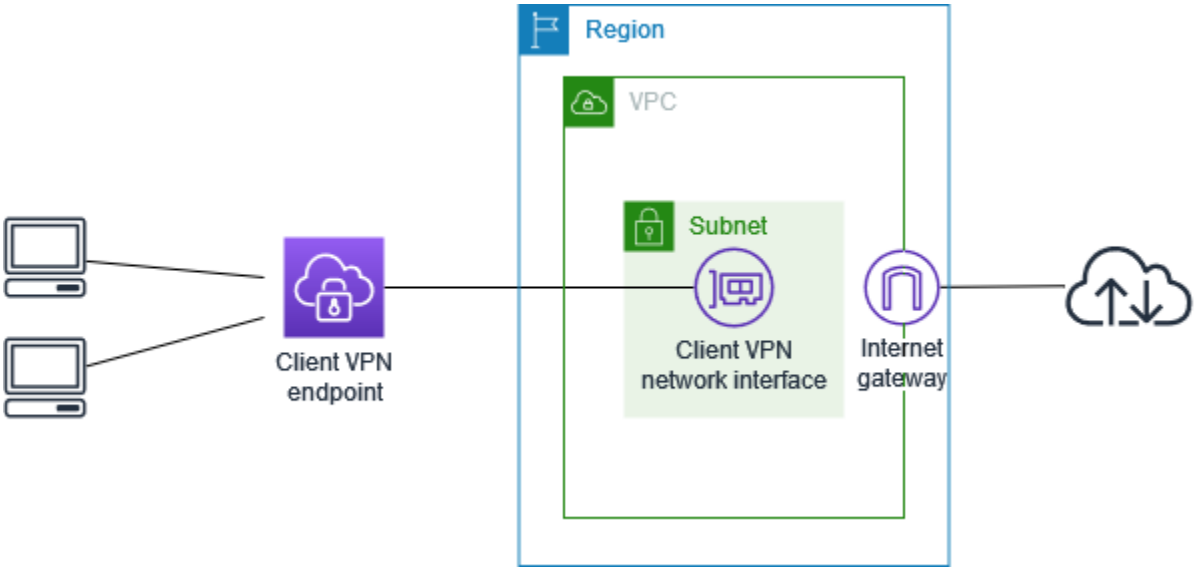
   > **Note**
   >
   > 或者，您可以使用 VPC 與內部部署網路之間的 Direct Connect 連線來實作此案例。如需詳細資訊，請參閱「Direct Connect 使用者指南」。

2. 測試您在上一個步驟中建立的 AWS Site-to-Site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AWS 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，請執行將目標網路與 AWS Client VPN 端點建立關聯中所述的步驟，然後選取 VPC 和子網路。
5. 新增允許存取 AWS Site-to-Site連接的路由。若要執行此操作，請執行中所述的步驟建立 AWS Client VPN 端點路由；對於路由目的地，輸入 AWS Site-to-Site連線的 IPv4 CIDR 範圍，對於目標 VPC 子網路 ID，請選取您與 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連接。若要這樣做，請執行中所述的步驟將授權規則新增至 AWS Client VPN 端點；對於目的地網路，輸入 AWS Site-to-Site連接 IPv4 CIDR 範圍。

使用 用戶端 VPC 存取網際網路

此案例的 AWS Client VPN 組態包含單一目標 VPC 和網際網路的存取。如果您需要讓用戶端存取單一目標 VPC 內的資源，並允許存取網際網路，建議您使用此組態。

如果您已完成 開始使用 AWS Client VPN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 使用 的規則和最佳實務 AWS Client VPN 檢閱 Client VPN 端點的規則和限制。

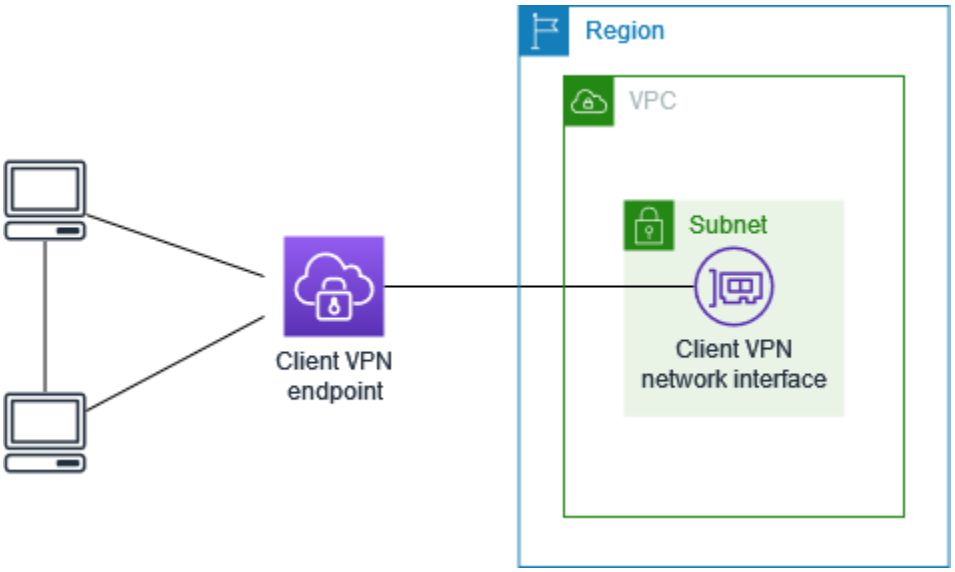
實作此組態

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AWS 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，請執行將目標網路與 AWS Client VPN 端點建立關聯中所述的步驟，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，請執行新增授權規則中所述的步驟；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 AWS Client VPN 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，請執行新增授權規則中所述的步驟；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 用戶端 VPC 取得用戶端對用戶端的存取權限

此案例的 AWS Client VPN 組態可讓用戶端存取單一 VPC，並讓用戶端將流量路由至彼此。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 使用 的規則和最佳實務 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AWS 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，請執行將目標網路與 AWS Client VPN 端點建立關聯中所述的步驟，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 AWS Client VPN 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，請執行新增授權規則中所述的步驟。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，請執行新增授權規則中所述的步驟。在要啟用的目的地網路中，輸入用戶端的 CIDR 範圍。

使用 Client VPN 限制存取您的網路

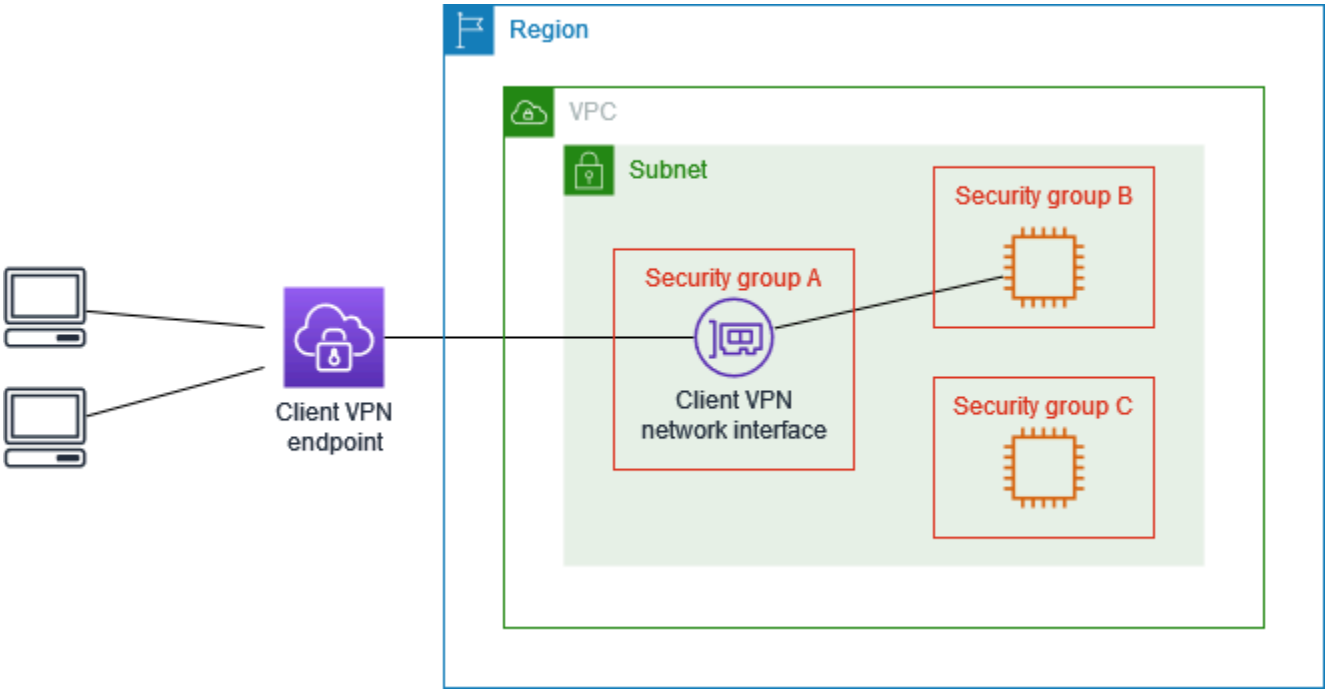
您可以設定 AWS Client VPN 端點以限制對 VPC 中特定資源的存取。針對使用者類型身分驗證，您也可以根據存取 Client VPN 端點的使用者群組，將存取限制在一部分的網路。

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 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. 設定 Directory Service 或 IdP 中的使用者和群組。如需詳細資訊，請參閱下列主題：
   - Client VPN 中的 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 AWS Client VPN 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和用戶端憑證和金鑰。如需更多詳細資訊，請參閱 中的相互身分驗證 AWS Client VPN。
2. 建立 Client VPN 端點。如需更多詳細資訊，請參閱 建立AWS 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。如需詳細資訊，請參閱新增授權規則。

中的用戶端身分驗證 AWS Client VPN

用戶端身分驗證會在進入 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 型聯合身分驗證) (以使用者為基礎)

您可以單獨使用上述其中一種方法，也可以將交互身分驗證與使用者型方法結合使用，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，無論您使用的身分驗證類型為何。如需建立和佈建伺服器憑證的詳細資訊，請參閱中的相互身分驗證 AWS Client VPN中的步驟。
> - 如果您使用交互身分驗證和使用者型身分驗證的組合，則必須使用這兩種方法在 VPN 中正確驗證。

Client VPN 中的 Active Directory 身分驗證

Client VPN 透過與 整合，提供 Active Directory 支援 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 Directory Service時，Client VPN 可以連線至佈建於 AWS 或內部部署網路中的現有 Active Directory。這可讓您使用現有的用戶端身分驗證基礎設施。如果您使用內部部署 Active Directory，但沒有現有的 AWS Managed Microsoft AD，則必須設定 Active Directory Connector (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。

中的相互身分驗證 AWS Client VPN

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 端點時指定它。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。

AWS Client VPN 中使用的憑證必須遵循 RFC 5280：網際網路 X.509 公有金鑰基礎設施憑證和憑證撤銷清單 (CRL) 設定檔，包括備註第 4.2 節中指定的憑證延伸。

> **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。
> 更新與 Client VPN 服務搭配使用的憑證時，無論是透過 ACM 自動輪換、手動匯入新憑證，還是中繼資料更新至 IAM Identity Center，Client VPN 服務都會使用較新的憑證自動更新 theClient VPN 端點。這是一個自動化程序，最多可能需要 5 小時。

任務

- 啟用 的交互身分驗證 AWS Client VPN
- 為 續約您的伺服器憑證 AWS Client VPN

啟用 的交互身分驗證 AWS Client VPN

您可以在 Linux/MacOS 或 Windows 的 Client VPN 中啟用交互身分驗證。

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。

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。

為 續約您的伺服器憑證 AWS Client VPN

您可以續約並重新匯入已過期的 Client VPN 伺服器憑證。根據您正在使用的 OpenVPN easy-rsa 版本，程序會有所不同。如需詳細資訊，請參閱 Easy-RSA 3 憑證續約和撤銷文件。

續約您的伺服器憑證

1. 執行下列其中一項操作：
   - Easy-RSA 3.1.x 版
     - 執行憑證更新命令。

       ```
       $ ./easyrsa renew server nopass
       ```
   - Easy-RSA 3.2.x 版
     a. 執行 expire 命令。

        ```
        $ ./easyrsa expire server
        ```
     b. 簽署新的憑證。

        ```
        $ ./easyrsa --san=DNS:server 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 \
   ```

```
    --certificate-arn
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Client VPN 中的單一登入 — SAML 2.0 型聯合身分驗證

AWS Client VPN 支援 Client VPN 端點的聯合身分與安全性聲明標記語言 2.0 (SAML 2.0)。您可以使用支援 SAML 2.0 的身分提供者 (IdP)，來建立集中式使用者身分。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。

主題

- 為 啟用 SAML AWS Client VPN
- 身分驗證工作流程
- SAML 型聯合身分驗證的需求和考量
- SAML 型 IdP 組態資源

為 啟用 SAML AWS Client VPN

您可以完成下列步驟，為 Client VPN 的單一登入啟用 SAML。或者，如果您為 Client VPN 端點啟用了自助入口網站，請指示您的使用者前往自助入口網站，以取得組態檔案和 AWS 提供的用戶端。如需詳細資訊，請參閱AWS Client VPN 存取自助式入口網站。

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，以與 AWS Client VPN現有應用程式搭配使用。
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。

   此簽署的 XML 文件用於建立 AWS 和 IdP 之間的信任關係。
4. 在與 Client VPN 端點相同的 AWS 帳戶中建立 IAM SAML 身分提供者。

   IAM SAML 身分提供者會使用 IdP 產生的中繼資料文件，定義組織的 IdP 以 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。

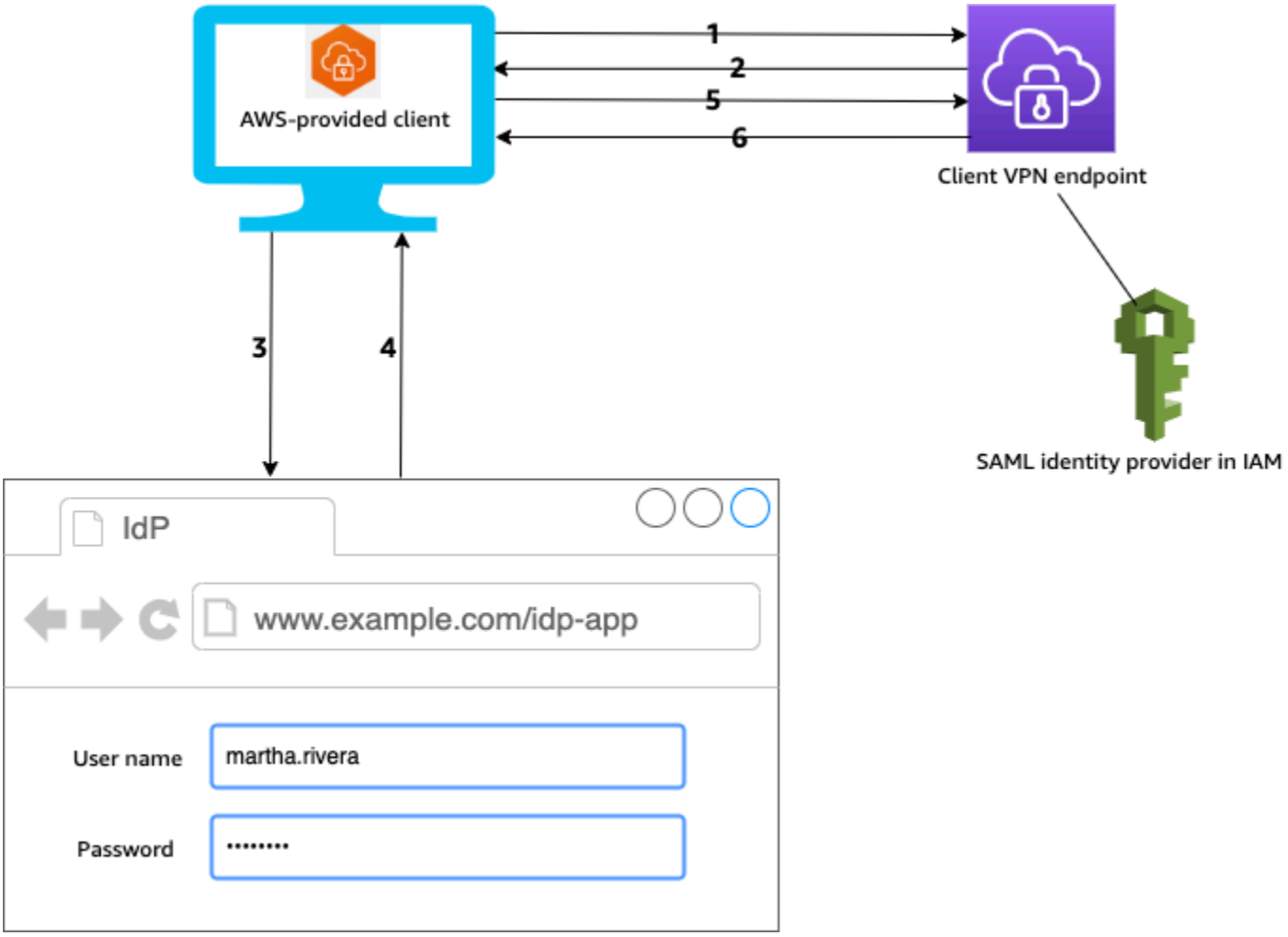
5. 建立 Client VPN 端點。

   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AWS 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。

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 提供的用戶端會在使用者的裝置上開啟新的瀏覽器視窗。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 聲明傳送至 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。
- SAML 聲明和回應必須簽署。
- AWS Client VPN 僅支援 SAML 聲明中的「AudienceRestriction」和「NotBefore 和 NotOnOrAfter」條件。
- SAML 回應的支援大小上限為 128 KB。
- AWS Client VPN 不提供已簽章的身分驗證請求。
- 不支援 SAML 單一登出。使用者可以透過中斷與 AWS 所提供用戶端的連線來登出，或者您可以終止連線。
- 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 提供的用戶端連線。
- 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的裝置上保留 TCP 連接埠 35001 以進行 SAML 回應。
- 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 請求傳送至 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。
- 使用者名稱 (`NameID`) 長度上限為 1024 個位元組。使用者名稱較長的連線將被拒絕。
- 與 Client VPN 服務搭配使用的憑證更新時，無論是透過 ACM 自動輪換、手動匯入新憑證，還是中繼資料更新至 IAM Identity Center，Client VPN 服務都會使用較新的憑證自動更新 Client VPN 端點。這是一個自動化程序，最多可能需要 5 小時。

SAML 型 IdP 組態資源

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

IdP	資源
Okta	使用 SAML 驗證 AWS Client VPN 使用者
Microsoft Entra ID （先前稱為 Azure Active Directory)	如需詳細資訊，請參閱 Microsoft 文件網站上的教學課程：Microsoft Entra 單一登入 (SSO) 與 AWS ClientVPN 整合。
JumpCloud	與 整合 AWS Client VPN
AWS IAM Identity Center	搭配 使用 IAM Identity Center AWS Client VPN 進行身分驗證和授權

建立應用程式的服務提供者資訊

若要使用上表中未列出的 IdP 建立 SAML 型應用程式，請使用以下資訊來設定 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	Description
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 AWS Client VPN 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 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 應用程式為標準和 GovCloud 區域進行驗證，則可同時新增這兩個 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。

中的用戶端授權 AWS Client VPN

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 在 中將安全群組套用至目標網路 AWS Client VPN。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。

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 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。如需詳細資訊，請參閱AWS Client VPN 授權規則。

任務

- 建立 AWS Client VPN 端點安全群組規則

建立 AWS Client VPN 端點安全群組規則

當您將子網路與 Client VPN 建立關聯時所套用 VPC 的預設安全群組可能會限制來自您想要允許的預設安全群組流量的流量，同時允許您不希望的流量。使用下列步驟建立 Client VPN 端點安全群組規則，以允許或限制與資源或應用程式相關聯之端點安全群組的流量。如需安全群組規則的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 的安全群組。

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)。

中的連線授權 AWS Client VPN

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 `AWSClientVPN-` 前綴開頭。
- 支援合格的 Lambda 函數。
- Lambda 函數必須與 Client VPN 端點位於相同的 AWS 區域和相同的 AWS 帳戶。
- 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 AWS Client VPN 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，則必須針對 Windows 使用 1.2.6 版或更新版本，針對 macOS 使用 1.2.4 版或更新版本。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 — 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。如果在執行 Lambda 函數期間發生失敗 （ 例如，由於限流 ），Client VPN 服務會將下列預設訊息傳回給用戶端。

```
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進行姿勢評估

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，並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AWS Client VPN端點及修改 AWS Client VPN 端點。

服務連結角色

AWS Client VPN 會在您的帳戶中自動建立稱為 AWSServiceRoleForClientVPNConnections 的服務連結角色。連線到 Client VPN 端點時，角色具有呼叫 Lambda 函數的許可。如需詳細資訊，請參閱使用的服務連結角色 AWS Client VPN。

監控連線授權失敗

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 檢視 AWS Client VPN 用戶端連線。

使用用戶端連線處理常式評估狀態時，您也可以在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 AWS Client VPN 端點的連線記錄。

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：

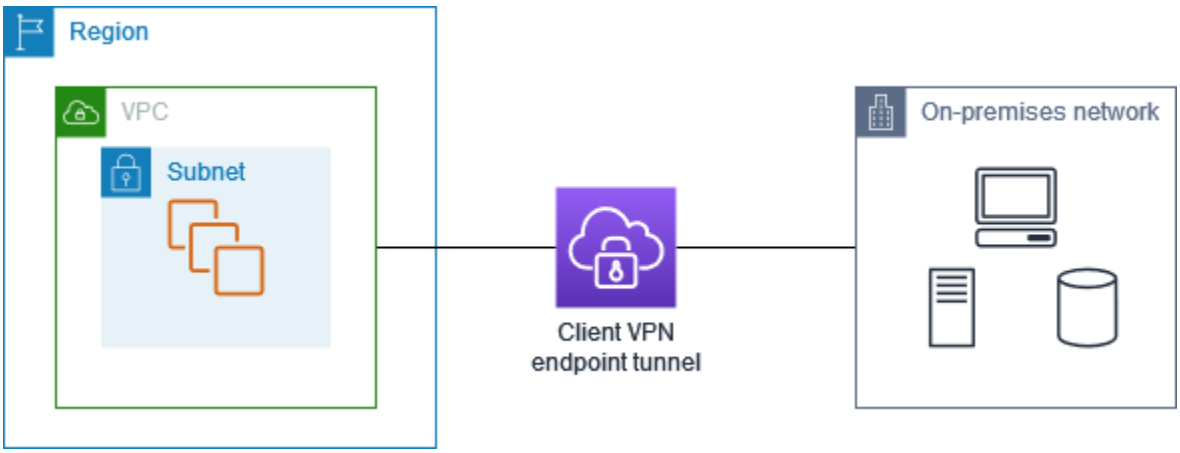
- `client-connect-failed` – 防止建立連線的 Lambda 函數。
- `client-connect-handler-timed-out` – Lambda 函數已逾時。
- `client-connect-handler-other-execution-error` – Lambda 函數發生未預期的錯誤。
- `client-connect-handler-throttled` – 經過調節的 Lambda 函數。
- `client-connect-handler-invalid-response` – 傳回無效回應的 Lambda 函數。
- `client-connect-handler-service-error` – 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 AWS 目的地流量周遊 VPN 通道，以最佳化來自用戶端的流量路由。
- 您可以減少傳出流量的量 AWS，進而降低資料傳輸成本。

路由傳送考量

- 當您啟用分割通道模式時，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的路由表。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，將 0.0.0.0/0 路由新增至 Client VPN 端點的路由表，可能會導致連線中斷，不建議這麼做

- 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。

啟用分割通道

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AWS Client VPN端點
- 修改 AWS Client VPN 端點

AWS Client VPN 端點的連線記錄

連線記錄是 的一項功能 AWS Client VPN ，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，可擷取連線事件的相關資訊，例如用戶端（最終使用者）何時連線、嘗試連線或中斷與 Client VPN 端點的連線。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。

連線記錄適用於所有 AWS Client VPN 可用 的 區域。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AWS Client VPN 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量，以及您的 Client VPN 端點是否可以視需要擴展以滿足其他需求。

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，您無法變更用戶端 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，子網路關聯的數目也取決於 AWS 區域中可用的可用區域數目。

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 使用 的規則和最佳實務 AWS Client VPN。

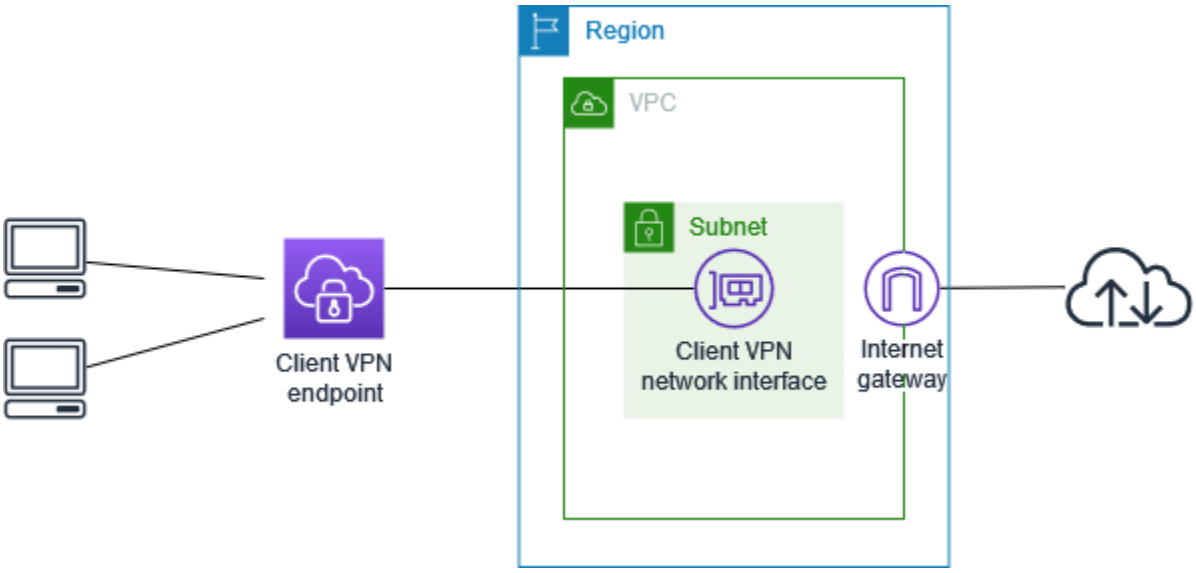
如需 Client VPN 端點配額的詳細資訊，請參閱 AWS Client VPN 配額。

開始使用 AWS Client VPN

在本教學課程中，您將建立執行下列動作的 AWS 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

- 先決條件
- 步驟 1：選擇您的端點類型
- 步驟 2：產生伺服器和用戶端憑證和金鑰
- 步驟 3：建立 Client VPN 端點
- 步驟 4：關聯目標網路
- 步驟 5：新增 VPC 的授權規則
- 步驟 6：提供網際網路的存取權
- 步驟 7：驗證安全群組需求
- 步驟 8：下載 Client VPN 端點組態檔案
- 步驟 9：連線至 Client VPN 端點

先決條件

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：選擇您的端點類型

Client VPN 支援兩種端點類型：適用於單一 VPC 存取的 VPC 子網路關聯，以及適用於多 VPC 和混合網路案例的 Transit Gateway 關聯。本教學課程涵蓋 VPC 相關端點。如需 Transit Gateway 端點，請參閱 傳輸閘道與 Client VPN 整合。

步驟 2：產生伺服器和用戶端憑證和金鑰

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，伺服器憑證需要匯入 AWS Certificate Manager (ACM)，並在您建立 Client VPN 端點時指定。將客户端憑證匯入 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和用户端憑證及金鑰，然後將它們匯入 ACM 中的詳細步驟，請參閱中的相互身分驗證 AWS Client VPN。

> **Note**
>
> 伺服器憑證必須在您要建立 Client VPN 端點的相同 AWS 區域中佈建或匯入至 AWS Certificate Manager (ACM)。

步驟 3：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。它是所有用户端 VPN 工作階段的終止點。

建立 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)，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。

   > **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。用户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，您無法變更用戶端地址範圍。

5. 針對伺服器憑證 ARN，選取您在步驟 2 中產生的伺服器憑證 ARN。
6. 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户端憑證均可用於進行身分驗證。
7. (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。

8. 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AWS Client VPN端點。

步驟 4：關聯目標網路

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

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)。
4. 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 5：新增 VPC 的授權規則

若要讓客户端存取 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 6：提供網際網路的存取權

您可以提供連接到 VPC 的其他網路的存取權，例如 AWS 服務、對等 VPCs、內部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 7：驗證安全群組需求

在本教學課程中，步驟 3 中的 Client VPN 端點建立期間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 8：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 用户端應用程式。

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 (下載用户端組態)。
4. 找到步驟 2 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AWS Client VPN 端點組態檔案匯出。

步驟 9：連線至 Client VPN 端點

您可以使用 AWS 提供的用戶端或其他 OpenVPN 型用戶端應用程式，以及您剛建立的組態檔案，連線至 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

下列主題說明使用 Client VPN 所需的主要管理任務：

- 存取自助式入口網站 — 設定 Client VPN 自助式入口網站的存取權，以便用戶端可以自行下載 Client VPN 端點組態檔案。如需存取自助式入口網站的資訊，請參閱 the section called “自助式入口網站存取”。
- 授權規則 — 新增授權規則以控制用戶端對指定網路的存取。如需新增授權規則的詳細資訊，請參閱 the section called “授權規則”。
- 用戶端憑證撤銷清單 — 使用用戶端憑證撤銷清單撤銷對 Client VPN 端點的存取。如需用戶端憑證撤銷清單的資訊，請參閱 the section called “用戶端憑證撤銷清單”。
- 用戶端連線 — 檢視或終止 Client VPN 端點的用戶端連線。如需有關檢視或終止用戶端連線的資訊，請參閱 the section called “用戶端連線”。
- 用戶端登入橫幅 — 建立 VPN 工作階段時，在 Client VPN 桌面應用程式上新增文字橫幅。您可以使用文字橫幅來滿足您的法規和合規需求。如需登入橫幅的資訊，請參閱 the section called “用戶端登入橫幅”。
- 用戶端路由強制執行 — 在透過 VPN 連線的裝置上強制執行管理員定義的路由。如需用戶端路由強制執行的詳細資訊，請參閱 the section called “用戶端路由強制執行”。
- Client VPN 端點 — 設定 Client VPN 端點以管理和控制所有 VPN 工作階段。如需設定端點的資訊，請參閱 the section called “端點”。
- 連線日誌 — 為新的或現有的 Client VPN 端點啟用連線記錄，以開始擷取連線日誌。如需連線記錄的資訊，請參閱 the section called “連線日誌”。
- 用戶端組態檔案匯出 — 設定 Client VPN 用戶端建立 VPN 連線所需的用戶端組態檔案。設定檔案之後，請下載（匯出）檔案以分發給用戶端。如需匯出用戶端組態檔案的詳細資訊，請參閱 the section called “用戶端組態檔案匯出”。
- 路由 — 為每個 Client VPN 路由設定授權規則，以指定哪些用戶端可存取目的地網路。如需設定授權規則的資訊，請參閱 the section called “授權規則”
- 目標網路 — 關聯 VPC 子網路或直接連接至 AWS Transit Gateway，讓用戶端能夠連線並建立 VPN 連線。如需目標網路的相關資訊，請參閱 the section called “目標網路”。如需 Transit Gateway 整合的詳細資訊，請參閱 the section called “傳輸閘道與 Client VPN 整合”。
- 最長 VPN 工作階段持續時間 — 設定最長 VPN 工作階段持續時間的選項，以符合您的安全和合規要求。如需 VPN 工作階段持續時間上限的相關資訊，請參閱 the section called “VPN 工作階段持續時間上限”。

AWS Client VPN 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 所提供用戶端的最新版本。

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。
- 自助式入口網站中可用的組態檔案與您使用 Amazon VPC 主控台或 匯出的組態檔案相同 AWS CLI。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>*。

您也可以在 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。

AWS Client VPN 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 故障診斷 AWS Client VPN：Active Directory 群組的授權規則未如預期運作和路由優先順序以取得更多詳細資訊。

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。

主題

- Client VPN 授權規則的範例案例
- 將授權規則新增至 AWS Client VPN 端點
- 從 AWS Client VPN 端點移除授權規則
- 檢視 AWS Client VPN 授權規則

Client VPN 授權規則的範例案例

本節說明授權規則的運作方式 AWS Client VPN。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。

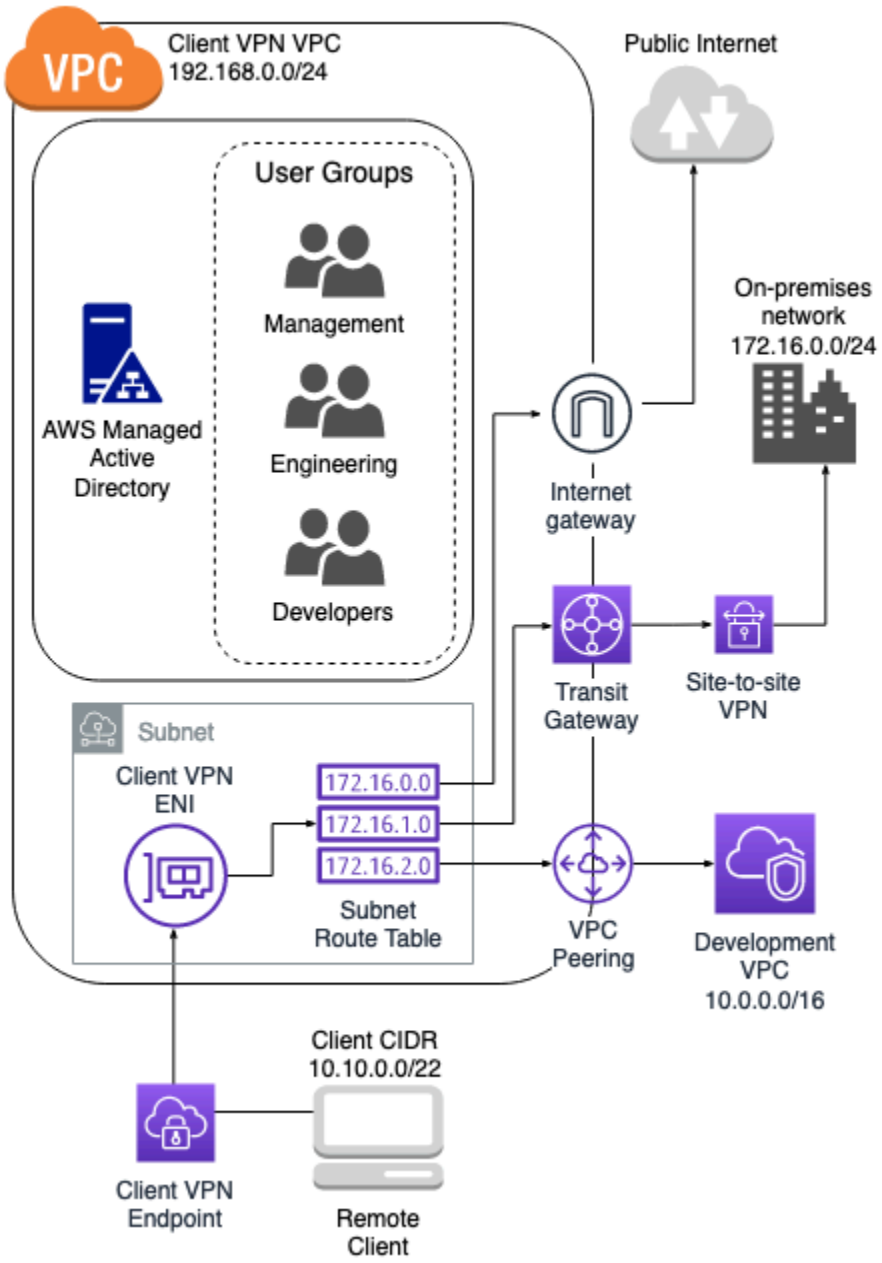
案例

- the section called “範例架構”
- the section called “存取單一目的地”
- the section called “使用任何目的地 (0.0.0.0/0) CIDR”
- the section called “較長的 IP 字首比對”
- the section called “重疊 CIDR（相同群組）”

- the section called “其他 0.0.0.0/0 規則”
- the section called “新增 192.168.0.0/24 的規則”
- the section called “SAML 聯合身分驗證”
- the section called “所有使用者群組的存取權”

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。



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
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。

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
	S-xxxxx15	False	10.0.0.0/16

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			
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。

較長的 IP 字首比對

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
	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任何目的地			
提供管理員群組存取開發 VPC 中的單一主機	S-xxxxx16	False	10.0.2.119/32

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。

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
	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任何目的地			
提供管理員群組存取開發 VPC 中的單一主機	S-xxxxx16	False	10.0.2.119/32
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。

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

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	10.0.2.119/32
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。

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

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	10.0.2.119/32
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。

SAML 聯合身分驗證

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	工程設計	False	172.16.0.0/24
提供開發群組存取開發 VPC	開發人員	False	10.0.0.0/16
提供管理員群組存取 Client VPN VPC	管理員	False	192.168.0.0/24

產生行為

- 使用「工程」群組屬性透過 SAML 驗證的使用者只能存取 172.16.0.0/24。
- 使用「開發人員」群組屬性透過 SAML 驗證的使用者只能存取 10.0.0.0/16。
- 使用「Managers」群組屬性透過 SAML 驗證的使用者只能存取 192.168.0.0/24。
- 所有其他流量都會由 Client VPN 端點捨棄。

> **Note**
>
> 使用 SAML 聯合身分驗證時，群組 ID 欄位會對應至識別使用者群組成員資格的 SAML 屬性值。此屬性是在 SAML 身分提供者中設定，並在身分驗證期間傳遞給 Client VPN。

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
提供管理員群組存取開發 VPC 中的單一主機	S-xxxxx16	False	10.0.2.119/32
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。

將授權規則新增至 AWS Client VPN 端點

您可以使用 新增授權規則，以授予或限制對 Client VPN 端點的存取 AWS 管理主控台。您可以使用 Amazon VPC 主控台或使用命令列或 API 將授權規則新增至 Client VPN 端點。

使用 將授權規則新增至 Client VPN 端點 AWS 管理主控台

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 AWS Client VPN 端點移除授權規則

您可以使用 主控台和 移除特定 Client VPN 端點的授權規則 AWS CLI。

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. 選取新增授權規則的 Client VPN 端點，然後選擇授權規則。
4. 選取要刪除的授權規則，選擇移除授權規則，然後再次選擇移除授權規則以確認刪除。

移除授權規則 (AWS CLI)

使用 revoke-client-vpn-ingress 命令。

檢視 AWS Client VPN 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。

AWS Client VPN 用戶端憑證撤銷清單

Client VPN 用戶端憑證撤銷清單用於撤銷對特定用戶端憑證之 Client VPN 端點的存取權。您可以產生撤銷清單或匯入現有的清單。您也可以匯出撤銷清單檔案的目前清單。在 Linux/macOS 或 Windows 上使用 OpenVPN 軟體來產生清單。匯入和匯出可以使用 Amazon VPC 主控台或使用 AWS CLI 來完成。

如需有關產生伺服器和用戶端憑證及金鑰的詳細資訊，請參閱中的相互身分驗證 AWS Client VPN

> **Note**
>
> 如果用戶端憑證撤銷清單已過期，您就無法連線至 Client VPN 端點。您需要建立新的 ，並將其匯入 Client VPN 端點。

您只能將有限數量的項目新增至用戶端憑證撤銷清單。如需可新增至撤銷清單的項目數量詳細資訊，請參閱 Client VPN 配額。

任務

- 產生 AWS Client VPN 用戶端憑證撤銷清單
- 匯入 AWS Client VPN 用戶端憑證撤銷清單
- 匯出 AWS Client VPN 用戶端憑證撤銷清單

產生 AWS Client VPN 用戶端憑證撤銷清單

您可以在 Linux/macOS 或 Windows 作業系統上產生 Client VPN 憑證撤銷清單。撤銷清單用於撤銷對特定憑證之 Client VPN 端點的存取權。如需用戶端憑證撤銷清單的詳細資訊，請參閱 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. 登入託管用於產生憑證之 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yes時輸入 。

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 檔案以啟動 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yes時輸入 。
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 AWS Client VPN 用戶端憑證撤銷清單

您必須擁有要匯入的 Client VPN 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 AWS Client VPN 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 AWS Client VPN 用戶端憑證撤銷清單

您可以使用 主控台和 匯出 Client VPN 用戶端憑證撤銷清單 AWS CLI。

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。

AWS Client VPN 用戶端連線

AWS Client VPN 連線是用戶端針對特定 Client VPN 端點建立的作用中 VPN 工作階段，以及該端點在過去 60 分鐘內終止的連線。用戶端成功連線到 Client VPN 端點時，即表示已建立連線。終止工作階段會結束用戶端與 Client VPN 端點的連線。

您可以檢視和終止 Client VPN 連線。檢視連線資訊會傳回資訊，例如從用戶端 CIDR 區塊範圍指派的 IP 地址、端點 ID 和時間戳記。終止工作階段會結束與端點的指定 VPN 連線。您可以使用 Amazon VPC 主控台或 AWS CLI 檢視和終止工作階段。如果您無法連線至端點，且根據錯誤，請參閱 疑難排解 以取得解決問題的步驟。

任務

- 檢視 AWS Client VPN 用戶端連線
- 終止 AWS Client VPN 用戶端連線

檢視 AWS Client VPN 用戶端連線

您可以使用 Amazon VPC 主控台或 CLI 檢視作用中的 AWS Client VPN 連線。

檢視 Client VPN 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。

檢視 Client VPN 用戶端連線 (AWS CLI)

使用 describe-client-vpn-connections 命令。

終止 AWS Client VPN 用戶端連線

您可以使用 Amazon VPC 主控台或 CLI 終止 Client VPN AWS 用戶端連線。

終止 Client VPN 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. 選取用戶端連線的 Client VPN 端點，然後選擇連線。
4. 選取要終止的連線，選擇終止連線，然後再次選擇終止連線以確認終止。

終止 Client VPN 用戶端連線 (AWS CLI)

使用 terminate-client-vpn-connections 命令。

AWS Client VPN 用戶端登入橫幅

AWS Client VPN 提供在建立 VPN 工作階段時，在 AWS 提供的 Client VPN 桌面應用程式上顯示文字橫幅的選項。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。

橫幅建立

最初會在建立 Client VPN 端點期間建立和啟用登入橫幅。如需在建立 Client VPN 端點期間啟用用戶端登入橫幅的步驟，請參閱 建立AWS Client VPN端點。

任務

- 設定現有 AWS Client VPN 端點的用戶端登入橫幅
- 停用現有 AWS Client VPN 端點的用戶端登入橫幅
- 修改 AWS Client VPN 端點上現有的橫幅文字
- 檢視目前設定的 AWS Client VPN 登入橫幅

設定現有 AWS 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. 針對用戶端登入橫幅文字，輸入在建立 VPN 工作階段時，將在 AWS 所提供用戶端上橫幅中顯示的文字。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 AWS 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 AWS Client VPN 端點上現有的橫幅文字

使用下列步驟修改 Client VPN 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. 對於用戶端登入橫幅文字，在建立 VPN 工作階段時，將現有文字取代為要在 AWS 所提供用戶端的橫幅中顯示的新文字。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。

檢視目前設定的 AWS Client VPN 登入橫幅

使用下列步驟來檢視目前設定的 Client VPN 用戶端登入橫幅。

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。

AWS Client VPN 用戶端路由強制執行

Client Route Enforcement 有助於在透過 VPN 連線的裝置上強制執行管理員定義的路由。此功能可確保來自連線用戶端的網路流量不會不小心傳送到 VPN 通道之外，以協助改善您的安全狀態。

Client Route Enforcement 會監控連線裝置的主要路由表，並根據用戶端 VPN 端點中設定的網路路由，確保傳出網路流量流向 VPN 通道。這包括在偵測到與 VPN 通道衝突的路由時修改裝置上的路由表。用戶端路由強制執行同時支援 IPv4 和 IPv6 地址系列。

要求

Client Route Enforcement 僅適用於下列 AWS 提供的 Client VPN 版本：

- Windows 5.2.0 版或更新版本 (IPv4 支援)
- macOS 5.2.0 版或更新版本 (IPv4 支援)
- Ubuntu 5.2.0 版或更新版本 (IPv4 支援)
- Windows 5.3.0 版或更新版本 (IPv6 支援)
- macOS 5.3.0 版或更新版本 (IPv6 支援)
- Ubuntu 5.3.0 版或更新版本 (IPv6 支援)

對於雙堆疊端點，用戶端路由強制執行設定會同時套用至 IPv4 和 IPv6 堆疊。您只能為一個堆疊啟用用戶端路由強制執行。

路由衝突

當用戶端連線至 VPN 時，會在用戶端的本機路由表和端點的網路路由之間進行比較。如果兩個路由表項目之間的網路重疊，則會發生路由衝突。重疊網路的範例如下：

- `172.31.0.0/16`
- `172.31.1.0/24`

在此範例中，這些 CIDR 區塊構成路由衝突。例如，`172.31.0.0/16` 可能是 VPN 通道 CIDR。由於 `172.31.1.0/24` 具有較長的字首，因此更為具體，因此通常會優先考慮並可能將 `172.31.1.0/24` IP 範圍內的 VPN 流量重新導向至另一個目的地。這可能會導致意外的路由行為。不過，啟用用戶端路由強制執行時，會移除後者 CIDR。使用此功能時，應考慮潛在的路由衝突。

完整通道 VPN 連接會透過 VPN 連接引導所有網路流量。因此，如果啟用 Client Route Enforcement 功能，連線至 VPN 的裝置將無法存取本機網路 (LAN) 資源。如果需要本機 LAN 存取，請考慮使用分割通道模式，而非完整通道模式。如需分割通道的詳細資訊，請參閱 分割通道 Client VPN。

考量事項

啟用用戶端路由強制執行之前，應考慮以下資訊。

- 在連線時，如果偵測到路由衝突，此功能會更新用戶端的路由表，將流量導向 VPN 通道。建立連線之前已存在且由此功能刪除的路由將會還原。
- 此功能僅在主要路由表上強制執行，不適用於其他路由機制。例如，強制執行不會套用至下列項目：
  - 政策型路由
  - 介面範圍路由
- Client Route Enforcement 會在 VPN 通道開啟時保護它。通道中斷連線後或用戶端重新連線時，不會提供任何保護。

OpenVPN 指令對雲端路由強制執行的影響

OpenVPN 組態檔案中的某些自訂指令與 Client Route Enforcement 有特定的互動：

- `route` 指令
  - 將路由新增至 VPN 閘道時。例如，將路由新增至 VPN `192.168.100.0 255.255.255.0` 閘道。

新增至 VPN 閘道的路由會受到用戶端路由強制執行的監控，類似於任何其他 VPN 路由。其中的任何衝突路由都會被偵測並移除。

- 新增路由至非 VPN 閘道時。例如，新增路由 `192.168.200.0 255.255.255.0 net_gateway`。

  新增至非 VPN 閘道的路由會因繞過 VPN 通道而從用戶端路由強制執行中排除。其中允許衝突路由。在此範例中，用戶端路由強制執行會將路由上方排除在監控之外。

- 與 IPv4 路由類似，新增至 VPN 閘道的 IPv6 路由會受到用戶端路由強制執行的監控，而新增至非 VPN 閘道的路由會排除在監控之外。

忽略的路由

用戶端路由強制執行會忽略下列 IPv4 網路的路由：

- `127.0.0.0/8` — 預留給本機主機
- `169.254.0.0/16` — 預留給 link-local 地址
- `224.0.0.0/4` — 預留給多點傳送
- `255.255.255.255/32` — 預留廣播

用戶端路由強制執行會忽略下列 IPv6 網路的路由：

- `::1/128` — 預留給迴路
- `fe80::/10` — 預留給 link-local 地址
- `ff00::/8` — 預留給多點傳送

主題

- 啟用 AWS Client VPN 端點的用戶端路由強制執行
- 從 AWS Client VPN 端點停用用戶端路由強制執行
- 疑難排解 IPv6 用戶端路由強制執行

啟用 AWS Client VPN 端點的用戶端路由強制執行

您可以使用 主控台或 在現有的 Client VPN 端點上啟用 Client Route Enforcement AWS CLI。

使用主控台啟用用戶端路由強制執行

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. 選擇您要修改的 Client VPN 端點，選擇動作，然後選擇修改 Client VPN 端點。
4. 向下捲動頁面到 Other parameters (其他參數) 區段。
5. 開啟用戶端路由強制執行。
6. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

使用 啟用用戶端路由強制執行 AWS CLI)

- 使用 modify-client-vpn-endpoint 命令。

從 AWS Client VPN 端點停用用戶端路由強制執行

您可以使用 主控台或 在 Client VPN 端點上停用 Client Route Enforcement AWS CLI。

使用主控台停用用戶端路由強制執行

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. 選擇您要修改的 Client VPN 端點，選擇動作，然後選擇修改 Client VPN 端點。
4. 向下捲動頁面到 Other parameters (其他參數) 區段。
5. 關閉用戶端路由強制執行。
6. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

使用 停用用戶端路由強制執行 AWS CLI

- 使用 modify-client-vpn-endpoint 命令。

疑難排解 IPv6 用戶端路由強制執行

如果您遇到 IPv6 用戶端路由強制執行的問題，請考慮下列疑難排解步驟：

驗證用戶端版本

確保您使用的是 AWS VPN Client 5.3.0 版或更新版本，這是 IPv6 Client Route Enforcement 支援的必要項目。

檢查端點組態

確認端點已啟用用戶端路由強制執行，並已針對 IPv6 或雙堆疊流量進行設定。

檢查用戶端日誌

檢閱 AWS VPN 用戶端日誌是否有任何與 IPv6 用戶端路由強制執行相關的錯誤訊息。尋找包含「IPv6」和「用戶端路由強制執行」或「CRM」的項目。

檢查路由表

為您的作業系統使用適當的命令來檢視 IPv6 路由表：

- Windows：`netsh interface ipv6 show route`
- macOS：`netstat -rn -f inet6`
- Linux：`ip -6 route`

檢查是否有衝突的路由

尋找可能與 VPN 路由衝突的任何 IPv6 路由。請特別注意具有相同目的地但不同閘道的路由。

驗證 ISP IPv6 支援

確保您的網際網路服務提供者 (ISP) 正確支援 IPv6。

如果您在嘗試這些疑難排解步驟後仍遇到 IPv6 用戶端路由強制執行的問題，請聯絡 AWS Support 以取得進一步協助。

AWS Client VPN 端點

所有 AWS Client VPN 工作階段都會與 Client VPN 端點建立通訊。您可以管理 Client VPN 端點，以建立、修改、檢視和刪除具有該端點的用戶端 VPN 工作階段。您可以使用 Amazon VPC 主控台或使用 CLI 來 AWS 建立和修改端點。

建立 Client VPN 端點的需求

> **Important**
>
> Client VPN 端點必須在佈建預期目標網路的相同 AWS 帳戶中建立。您還需要產生伺服器憑證，並視需要產生用戶端憑證。如需詳細資訊，請參閱中的用戶端身分驗證 AWS Client VPN。

開始之前，請務必備妥下列項目：

- 檢閱使用 的規則和最佳實務 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，請參閱中的用戶端身分驗證 AWS Client VPN。

IP 地址類型

AWS Client VPN 支援端點連線和流量路由的IPv4-only, IPv6-only 和雙堆疊組態。下列指引可協助您根據您的用戶端裝置功能、網路基礎設施和應用程式需求，選取適當的 IP 地址類型。

端點地址類型

端點地址類型會決定您的 Client VPN 端點支援哪些 IP 通訊協定進行用戶端連線。此設定無法在建立端點後變更。

在以下情況下選擇IPv4-only：

- 您的用戶端裝置僅支援 IPv4 VPN 連線
- 您的安全工具已針對 IPv4 流量檢查進行最佳化

在以下情況下選擇IPv6-only：

- 所有用戶端裝置完全支援 IPv6 連線
- 您位於 IPv4 地址耗盡的網路中

在下列情況下選擇雙堆疊：

- 您混合了具有不同 IP 功能的用戶端裝置

- 您正在逐漸從 IPv4 轉換到 IPv6

流量 IP 地址類型

流量 IP 地址類型控制 Client VPN 如何在用戶端和 VPC 資源之間路由流量，而不受端點支援的通訊協定影響。

在下列情況下，將流量路由為 IPv4：

- VPC 中的目標應用程式僅支援 IPv4
- 您有複雜的 IPv4 安全群組和網路 ACLs
- 您正在連線至舊版系統

在下列情況下，將流量路由為 IPv6：

- 您的 VPC 基礎設施主要是 IPv6
- 您想要面向未來的網路架構
- 您已為 IPv6 建置現代應用程式

端點修改

> **Note**
>
> 使用快速入門設定建立的 Client VPN 端點可以使用與標準設定建立的端點相同的程序進行修改。無論建立期間使用的設定方法為何，所有組態選項都可使用。

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
- 啟用或停用工作階段逾時時自動重新連線
- 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

任務

- 建立AWS Client VPN端點
- 檢視 AWS Client VPN 端點
- 修改 AWS Client VPN 端點
- 刪除 AWS Client VPN 端點

建立AWS Client VPN端點

建立AWS Client VPN端點，讓您的用戶端能夠使用 Amazon VPC 主控台或 建立 VPN 工作階段AWS CLI。Client VPN 在初始建立期間支援端點類型 （分割通道和完整通道） 與流量類型 (IPv4、IPv6 和雙堆疊） 的所有組合。

建立端點之前，請先熟悉需求。如需詳細資訊，請參閱the section called “建立 Client VPN 端點的需求”。

使用主控台建立 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)，然後選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。
3. 在「選擇設定方法」下，選取下列其中一項：
   - Quickstart - 使用 AWS 建議的預設值建立端點
   - 標準 - 手動設定端點的所有設定

快速入門設定：

1. 對於「選擇設定方法」，選取快速入門。
2. 對於「用戶端 IPv4 CIDR」，輸入要從中指派用戶端 IP 地址的 IP 地址範圍。AWS 建議使用 /22 CIDR 區塊 （例如 10.0.0.0/22)。
3. 對於「VPC」，選取要與 Client VPN 端點建立關聯的 VPC。
4. 針對「子網路」，選取 VPC 中的一或多個子網路。這些子網路將用於目標網路關聯。
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。
6. 選擇「建立 Client VPN 端點」。

AWS 會自動建立下列資源：

- 允許所有使用者存取 VPC CIDR 的授權規則
- 與所選 VPC 子網路的目標網路關聯
- VPC CIDR 的路由表項目

建立端點之後，您可以從端點詳細資訊頁面下載用戶端組態檔案，並將其與用戶端憑證和金鑰一起分發給您的使用者。

標準設定：

1. 對於「選擇設定方法」，選取標準。
2. (選用) 提供 Client VPN 端點的名稱標籤和說明。
3. 針對端點 IP 地址類型，選擇端點的 IP 地址類型：
   - IPv4：端點使用外部 VPN 通道流量的 IPv4 地址。
   - IPv6：端點使用外部 VPN 通道流量的 IPv6 地址。
   - 雙堆疊：端點會將 IPv4 和 IPv6 地址用於外部 VPN 通道流量。
4. 針對流量 IP 地址類型，選擇流經端點的流量 IP 地址類型：
   - IPv4：端點僅支援 IPv4 流量。
   - IPv6：端點僅支援 IPv6 流量。
   - 雙堆疊：端點支援 IPv4 和 IPv6 流量。
5. 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`。如果您為流量 IP 地址類型選取 IPv4 或雙堆疊，則此為必要項目。

> **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。用户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，您無法變更用戶端地址範圍。
> - 當您選取 IPv6 做為端點 IP 地址類型時，用戶端 IPv4 CIDR 欄位會停用。Client VPN 端點會從關聯的子網路配置用戶端 IPv6 地址，而且您可以在建立端點之後關聯子網路。

> **Note**
>
> 對於 IPv6 流量，您不需要指定用戶端 CIDR 範圍。Amazon 會自動為用戶端指派 IPv6 CIDR 範圍。

6. 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**
>
> 在您建立 Client VPN 端點的區域中，伺服器憑證必須位於AWS Certificate Manager(ACM) 中。憑證可以使用 ACM 佈建，也可以匯入至 ACM。
> 如需佈建憑證或將憑證匯入 ACM 的步驟，請參閱AWS Certificate Manager《 使用者指南》中的AWS Certificate Manager憑證。

7. 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，請選取使用交互驗證，然後在用戶端憑證 ARN 中指定佈建於AWS Certificate Manager(ACM) 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。

8. (選用) 對於 Connection logging (連線日誌記錄)，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 (啟用用户端連線的日誌詳細資訊)。針對 CloudWatch Logs log group name (CloudWatch Logs 日誌群組名稱)，請輸入要使用的日誌群組名稱。針對 CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱)，請輸入要使用的日誌串流名稱，或將此選項留白，讓我們為您建立日誌串流。
9. (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。

10. (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，請針對 DNS 伺服器 1 IP 地址和 DNS 伺服器 2 IP 地址，指定要使用的 DNS 伺服器的 IPv4 地址。對於 IPv6 或雙堆疊端點，您也可以指定 DNS Server IPv6 1 和 DNS Server IPv6 2 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。

11. (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。

12. (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。
13. (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。
14. (選用) 對於 VPN port (VPN 連接埠)，請選擇 VPN 連接埠號碼。預設為 443。
15. (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)。
16. (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。
17. （選用）對於工作階段逾時時中斷連線，選擇是否要在達到工作階段時間上限時終止工作階段。選擇此選項需要使用者在工作階段逾時時手動重新連線至端點，否則 Client VPN 會自動嘗試重新連線。
18. (選用) 指定是否啟用用戶端登入橫幅文字。開啟 Enable client login banner (啟用用户端登入橫幅)。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。
19. 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 型用戶端應用程式來連線至 Client VPN 端點。如需詳細資訊，請參閱「AWS Client VPN使用者指南」。

使用 建立 Client VPN 端點AWS CLI

使用 create-client-vpn-endpoint 命令。

建立 IPv4 端點的範例：

```
aws ec2 create-client-vpn-endpoint \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

建立 IPv6 端點的範例：

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "ipv6" \
  --traffic-ip-address-type "ipv6" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

建立雙堆疊端點的範例：

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "dual-stack" \
```

```
  --traffic-ip-address-type "dual-stack" \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

檢視 AWS Client VPN 端點

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

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。

修改 AWS Client VPN 端點

您可以使用 Amazon VPC 主控台或 修改 Client VPN 端點 AWS CLI。如需有關您可以修改之 Client VPN 欄位的詳細資訊，請參閱 the section called “端點修改”。

限制

修改端點時適用下列限制

- 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。
- 您可以將現有的 IPv4 端點修改為端點 IP 和流量 IP 類型的雙堆疊。如果端點 IP 和流量 IP 只需要 IPv6-only，則必須建立新的端點。
- Client VPN 不支援在建立後修改端點類型 (IPv4、IPv6、雙堆疊） 或流量類型 (IPv4、IPv6、雙堆疊）。
- 不支援修改具有端點類型和流量類型之特定組合的 Client VPN。您無法變更為任何其他組合。必須刪除端點，並使用所需的組態重新建立。
- 不支援 IPv6 流量的Client-to-client通訊。

修改 Client VPN 端點

您可以使用 主控台或 修改 Client VPN 端點 AWS CLI。

使用主控台修改 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. 對於端點 IP 地址類型，您可以將現有的 IPv4 端點修改為雙堆疊。此選項僅適用於 IPv4 端點。
6. 對於流量 IP 地址類型，您可以將現有的 IPv4 端點修改為雙堆疊。此選項僅適用於 IPv4 端點。
7. 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**
   >
   > 在您建立 Client VPN 端點的區域中，伺服器憑證必須位於 AWS Certificate Manager (ACM) 中。憑證可以使用 ACM 佈建，也可以匯入至 ACM。

8. 指定是否使用 Amazon CloudWatch Logs 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)。針對 CloudWatch Logs log group name (CloudWatch Logs 日誌群組

名稱)，請選取要使用的日誌群組名稱。對於 CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱)，請選取要使用的日誌串流名稱，或將此選項留白，讓我們為您建立日誌串流。

- 若要停用用户端連線的日誌記錄，請關閉 Enable log details on client connections (啟用用户端連線的日誌詳細資訊)。

9. 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 (啟用用户端連線處理常式)。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。
10. 開啟或關閉 Enable DNS servers (啟用 DNS 伺服器)。若要使用自訂 DNS 伺服器，請針對 DNS 伺服器 1 IP 地址和 DNS 伺服器 2 IP 地址，指定要使用的 DNS 伺服器的 IPv4 地址。對於 IPv6 或雙堆疊端點，您也可以指定 DNS Server IPv6 1 和 DNS Server IPv6 2 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。

11. 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。
12. 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。
13. 對於 VPN port (VPN 連接埠)，請選擇 VPN 連接埠號碼。預設為 443。
14. 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. 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. 針對工作階段逾時時中斷連線，選擇是否要在達到工作階段時間上限時終止工作階段。選擇此選項需要使用者在工作階段逾時時手動重新連線至端點，否則 Client VPN 會自動嘗試重新連線。
17. 開啟或關閉 Enable client login banner (啟用用户端登入橫幅)。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。
18. 選擇 Modify Client VPN Endpoint (修改 Client VPN 端點)。

使用 修改 Client VPN 端點 AWS CLI

使用 modify-client-vpn-endpoint 命令。

將 IPv4 端點修改為雙堆疊的範例：

```
aws ec2 modify-client-vpn-endpoint \
  --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
  --client-cidr-block "172.31.0.0/16"
```

刪除 AWS 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。

AWS Client VPN 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。連線日誌會顯示 Client VPN 端點的日誌事件序列。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。然後，連線記錄會記錄以下資訊：用戶端連線請求、用戶端連線結果（成功或失敗）、連線結果失敗的原因，以及來自端點的用戶端終止時間。

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。

可以使用 Amazon VPC 主控台或 AWS CLI 建立 Client VPN 連線日誌。

任務

- 啟用新 AWS Client VPN 端點的連線記錄
- 啟用現有 AWS Client VPN 端點的連線記錄
- 檢視 AWS Client VPN 連線日誌
- 關閉 AWS Client VPN 連線記錄

啟用新 AWS Client VPN 端點的連線記錄

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AWS 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 啟用新 Client VPN 端點的連線記錄 AWS CLI

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 AWS Client VPN 端點的連線記錄

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 啟用現有 Client VPN 端點的連線記錄 AWS CLI

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 AWS Client VPN 連線日誌

您可以使用 CloudWatch Logs 主控台檢視 Client VPN 連線日誌。

使用主控台檢視連線日誌

1. 透過 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 AWS Client VPN 連線記錄

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 關閉連線記錄 AWS CLI

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

AWS Client VPN 端點組態檔案匯出

AWS Client VPN 端點組態檔案是用戶端 （使用者） 用來與 Client VPN 端點建立 VPN 連線的檔案。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，如果您為 Client VPN 端點

啟用自助式入口網站，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AWS Client VPN 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。

任務

- 匯出 AWS Client VPN 用戶端組態檔案
- 為交互身分驗證新增 AWS Client VPN 用戶端憑證和金鑰資訊

匯出 AWS Client VPN 用戶端組態檔案

您可以使用 主控台或 匯出 Client VPN 用戶端組態 AWS CLI。

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 命令，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
```

為交互身分驗證新增 AWS Client VPN 用戶端憑證和金鑰資訊

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-0011abcabcabcabc1.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
```

AWS Client VPN 路由

每個 AWS Client VPN 端點都有一個路由表，描述可用的目的地網路路由。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，如此處所述故障診斷 AWS Client VPN：對對等 VPC、Amazon S3 或網際網路的存取是間歇性的。每個關聯的子網路應該有一組相同的路由。

在 Client VPN 端點上使用分割通道的考量事項

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。

任務

- 建立 AWS Client VPN 端點路由

- 檢視 AWS Client VPN 端點路由
- 刪除 AWS Client VPN 端點路由

建立 AWS Client VPN 端點路由

當您建立 Client VPN 端點路由時，您可以指定應如何導向目的地網路的流量。

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 AWS Client VPN 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 AWS Client VPN 端點路由

您只能刪除手動新增的 Client VPN 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。

AWS Client VPN 目標網路

目標網路是 VPC 中的子網路。 AWS Client VPN 端點必須至少有一個目標網路，才能讓用戶端與其連線並建立 VPN 連線。

如需您可以設定之存取類型的詳細資訊（例如，讓您的用戶端存取網際網路），請參閱 Client VPN 的案例和範例。

Client VPN 目標網路需求

建立目標網路時，適用下列規則：

- 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。如需詳細資訊，請參閱修改 AWS 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。

任務

- 將目標網路與 AWS Client VPN 端點建立關聯
- 在 中將安全群組套用至目標網路 AWS Client VPN
- 檢視 AWS Client VPN 目標網路
- 取消目標網路與 AWS Client VPN 端點的關聯

將目標網路與 AWS Client VPN 端點建立關聯

您可以使用 Amazon VPC 主控台或 CLI，將一或多個目標網路 （子網路） 與 Client VPN AWS 端點建立關聯。將目標網路與 Client VPN 端點建立關聯之前，請先熟悉需求。請參閱 建立目標網路的需求。

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。

在 中將安全群組套用至目標網路 AWS Client VPN

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。如需詳細資訊，請參閱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。

檢視 AWS Client VPN 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 檢視目標網路 AWS CLI

使用 describe-client-vpn-target-networks 命令。

取消目標網路與 AWS 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。

AWS Client VPN VPN 工作階段持續時間逾時上限

AWS Client VPN 針對最長 VPN 工作階段持續時間提供數個選項，這是用戶端連線至 Client VPN 端點所允許的最長時間。您可以設定較短的 VPN 工作階段持續時間上限，以協助滿足安全和合規要求。根據預設，VPN 工作階段最長持續時間為 24 小時。設定工作階段持續時間上限後，您就可以控制達到該

逾時時該工作階段會發生的情況。工作階段逾時中斷連線選項可讓您終止工作階段，或自動嘗試重新連線至端點。終止工作階段可讓您透過強制執行最長 VPN 工作階段持續時間，進一步控制端點安全性。如果工作階段設定為在達到最長時間時終止，使用者將需要重新連線並提供其身分驗證憑證，才能重新建立 VPN 連線。

當工作階段逾時中斷連線設定為自動重新連線，並達到工作階段時間上限時，

- 在快取的使用者登入資料 (Active Directory) 或憑證型身分驗證 （ 相互身分驗證 ） 的情況下，會自動建立新的工作階段。若要完全中斷連線而不自動重新連線，這些使用者應該手動中斷連線。
- 在聯合身分驗證 (SAML) 的情況下，不會自動建立新的工作階段。這些使用者必須在工作階段逾時過期後再次驗證，才能重新建立 VPN 連線。

> **Note**
>
> - 當最大 VPN 工作階段持續時間值從其目前值減少時，任何連接至端點且時間超過新設定持續時間的作用中 VPN 工作階段都會中斷連線。
> - 變更工作階段逾時中斷連線選項會將新設定套用至任何目前開啟的工作階段。
> - Client VPN 會強制執行每個連線的工作階段持續時間上限。如果連線中斷並啟動新連線，則新連線的工作階段持續時間計時器上限會重設。

在建立 AWS Client VPN 端點期間設定 VPN 工作階段上限

VPN 工作階段的持續時間是在建立 Client VPN 端點期間設定。如需建立 Client VPN 端點和設定最大工作階段持續時間的步驟，建立AWS Client VPN端點請參閱 。

任務

- 檢視 AWS Client VPN 目前的 VPN 工作階段持續時間上限
- 修改 AWS Client VPN 工作階段持續時間上限和逾時行為

檢視 AWS Client VPN 目前的 VPN 工作階段持續時間上限

使用下列步驟來檢視目前的 Client VPN 最長 VPN 工作階段持續時間。

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. 檢視工作階段逾時小時數旁的目前 VPN 工作階段持續時間上限，以及是否啟用或停用逾時時中斷連線。

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 AWS Client VPN 工作階段持續時間上限和逾時行為

使用下列步驟修改現有的 Client VPN 最長 VPN 工作階段持續時間，並變更工作階段逾時行為的中斷連線。

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. 針對工作階段逾時時中斷連線，選擇是否要在達到工作階段逾時上限時中斷連線工作階段。根據預設，這會在您第一次修改端點時關閉。
6. 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。

傳輸閘道與 Client VPN 整合

您可以將 Client VPN 端點原生連接至 Transit Gateway，以安全地遠端存取多個 VPCs、內部部署網路，以及連接到 Transit Gateway 的其他資源。這不需要為每個 VPC 建立單獨的 VPN 端點，或管理透過中繼 VPCs複雜路由。

主題

- 概觀
- 優勢
- Transit Gateway 整合的運作方式
- 先決條件
- 建立 Transit Gateway Client VPN 端點
- 管理路由
- 設定授權
- 管理可用區域
- 跨帳戶傳輸閘道存取
- 考量和限制

概觀

當您將 Transit Gateway 與 Client VPN 端點建立關聯時，如果 Client VPN 端點中設定了適當的路由和授權規則，連線的 VPN 用戶端可以存取連線至 Transit Gateway 的所有資源。

Transit Gateway 相關端點會保留用戶端來源 IP 地址。來源網路地址轉譯 (SNAT) 不會套用，這可增強用戶端流量的可見性。

> **Important**
>
> 您無法在單一 Client VPN 端點中混合 VPC 子網路關聯和 Transit Gateway 關聯。在建立端點時選擇一個關聯類型。

優勢

與 Client VPN 整合的 Transit Gateway 提供下列優點：

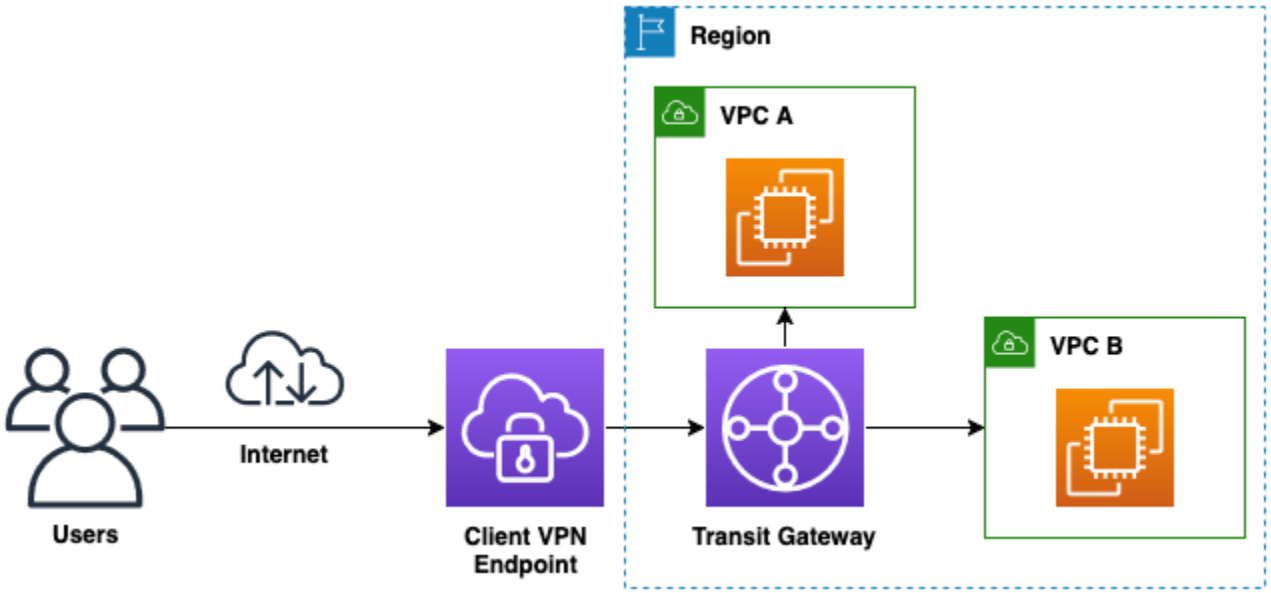
- 簡化管理 — 消除每個 VPC 個別 VPN 端點的需求。不需要僅為 VPN 終止建立中繼 VPCs。
- 集中式路由 — 利用 Transit Gateway 作為中央路由中樞。簡化整個網路的路由管理。
- 增強可見性 — 保留用戶端來源 IP 地址 （無 SNAT)。提供 Client VPN 的流程日誌支援。
- 可擴展性 — 輕鬆將新的 VPCs 新增至您的 Transit Gateway，您可以透過 Client VPN 存取。擴展以支援大型遠端人力資源和業務單位。

- 集中式安全 — 在所有連線網路中實作一致的安全政策。維護完整的稽核線索。

Transit Gateway 整合的運作方式

以下說明 Client VPN 如何與 Transit Gateway 搭配使用：

1. 建立端點 — 您可以建立 Client VPN 端點並指定 Transit Gateway ID。
2. 附件建立 — AWS `client-vpn` 自動為端點建立 類型的 Transit Gateway 附件。
3. 可用區域選擇 — 您可以指定要使用的可用區域，或自動 AWS 選取 2 個可用區域。
4. 路由組態 — 您可以將路由新增至 Client VPN 端點路由表，以透過 Transit Gateway 將用戶端流量導向目的地網路。
5. 用戶端連線流程 — 當用戶端連線時，流量會透過 Client VPN 端點從用戶端流向 Transit Gateway，然後流向根據 Transit Gateway 路由表的目的地網路。



先決條件

建立 Transit Gateway 相關 Client VPN 端點之前，請確認下列需求。

傳輸閘道需求

- 與 Client VPN 端點位於相同區域中的現有 Transit Gateway。
- 對於跨帳戶存取，傳輸閘道必須透過 與您的帳戶共用 AWS Resource Access Manager。

- Transit Gateway 必須指派 IPv4 CIDR 區塊。如果您打算使用 IPv6 或雙堆疊組態，請同時指派 IPv6 CIDR 區塊。

網路需求

- 用戶端 CIDR 範圍不得與連接到 Transit Gateway 的 VPCs CIDR 範圍重疊。
- 您選取的可用區域必須由 Transit Gateway 支援。
- 傳回路由必須在 VPC 路由表中設定，將目的地為用戶端 CIDR 範圍的流量導向 Transit Gateway。

憑證需求

- 在與 Client VPN 端點相同區域中佈建的伺服器憑證 AWS Certificate Manager (ACM)。
- 如果您使用交互身分驗證，則會在 ACM 中佈建用戶端憑證。

建立 Transit Gateway Client VPN 端點

您可以使用 主控台或 建立與 Transit Gateway 相關聯的 Client VPN 端點 AWS CLI。

建立 Transit Gateway 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)，然後選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。
3. （選用）針對名稱標籤和描述，輸入端點的名稱和描述。
4. 針對流量 IP 地址類型，選擇下列其中一項：
   - IPv4 — 指定用戶端 IPv4 CIDR 範圍（例如 `10.0.0.0/22`）。
   - IPv6 — AWS 自動指派用戶端 IPv6 CIDR 範圍。
   - 雙堆疊 — 指定用戶端 IPv4 CIDR 範圍。 AWS 會自動指派用戶端 IPv6 CIDR 範圍。
5. 對於伺服器憑證 ARN，請為在 ACM 中佈建的 TLS 憑證指定 ARN。
6. 選擇您的身分驗證方法。如需詳細資訊，請參閱中的用戶端身分驗證 AWS Client VPN。
7. （選用）對於連線記錄，開啟在用戶端連線上啟用日誌詳細資訊，並指定 CloudWatch Logs 日誌群組和日誌串流。
8. 針對網路基礎設施，選擇傳輸閘道。
9. 對於傳輸閘道 ID，從下拉式清單中選取傳輸閘道。
10. （選用）針對可用區域，選取最多 5 個可用區域。如果您未選取可用區域， AWS 會自動選取 2。

11. （選用）設定其他設定，例如 DNS 伺服器、傳輸通訊協定、分割通道、VPN 連接埠、工作階段逾時和登入橫幅。
12. 選擇 Create Client VPN Endpoint (建立 Client VPN 端點)。

> **Note**
>
> 建立之後，端點狀態為 `pending-associate`。Transit Gateway 附件會自動建立。用戶端可以在附件可用後進行連線。

建立 Transit Gateway Client VPN 端點 (AWS CLI)

使用 create-client-vpn-endpoint 命令搭配 `--transit-gateway-id` 參數。

下列範例會建立具有特定可用區域的 Client VPN 端點：

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone-list us-east-1a us-east-1b us-east-1c
```

輸出範例：

```
{
    "ClientVpnEndpointId": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE",
    "Status": {
        "Code": "pending-associate"
    },
    "DnsName": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE.prod.clientvpn.us-
east-1.amazonaws.com"
}
```

若要讓 AWS 自動選取 2 個可用區域，請省略 `--availability-zone-list` 參數：

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE
```

驗證 Transit Gateway 連接

建立端點之後，請確認已建立 Transit Gateway 附件。

驗證 Transit Gateway 連接（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 Transit Gateway Attachments (傳輸閘道連接)。
3. 尋找資源類型 = `client-vpn`且資源 ID 符合您 Client VPN 端點 ID 的附件。
4. 確認狀態為 `available`。

驗證 Transit Gateway 連接 (AWS CLI)

使用 describe-transit-gateway-attachments 命令。

```
aws ec2 describe-transit-gateway-attachments \
    --filters Name=transit-gateway-id,Values=tgw-0a1b2c3d4e5f6EXAMPLE Name=resource-
type,Values=client-vpn
```

若要檢視端點的 Transit Gateway 組態，請使用 describe-client-vpn-endpoints 命令：

```
aws ec2 describe-client-vpn-endpoints \
    --client-vpn-endpoint-ids cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

輸出包含具有傳輸閘道 ID 和相關聯可用區域的`TransitGatewayConfiguration`物件。

管理路由

> **Important**
>
> 對於 Transit Gateway 相關端點，您在建立路由時不會指定目標子網路 ID。流量會自動透過 Transit Gateway 附件導向。

新增路由（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 Client VPN 端點，選擇路由表，然後選擇建立路由。
4. 對於路由目的地，輸入目的地 CIDR 範圍（例如，`10.1.0.0/16`VPC 或`0.0.0.0/0`所有流量）。
5. （選用）針對描述，輸入路由的描述。
6. 選擇 Create route (建立路由)。

新增路由 (AWS CLI)

使用 create-client-vpn-route 命令，而不使用 `--target-vpc-subnet-id` 參數。

```
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

若要新增多個路由，請為每個目的地 CIDR 範圍執行 命令：

```
# Route to VPC 1
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16

# Route to VPC 2
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.2.0.0/16
```

```
# Route to on-premises network
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 192.168.0.0/16
```

刪除路由（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 Client VPN 端點，選擇路由表，選取路由，然後選擇刪除路由。
4. 選擇刪除路由以確認。

刪除路由 (AWS CLI)

使用 delete-client-vpn-route 命令。

```
aws ec2 delete-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

設定授權

> **Important**
>
> Transit Gateway 相關 Client VPN 端點不支援安全群組型授權。您必須使用網路型授權規則來控制用戶端存取。

新增授權規則（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 Client VPN 端點，選擇授權規則，然後選擇新增授權規則。
4. 若要讓目的地網路啟用存取，請輸入目的地 CIDR 範圍（例如 `10.1.0.0/16`)。
5. 針對授予存取權，請選擇下列其中一項：
   - 允許存取所有使用者 — 所有已驗證的用戶端都可以存取目的地網路。

- 允許特定存取群組中的使用者存取 — 在存取群組 ID 中輸入 Active Directory 群組 SID 或 IdP 群組名稱。

6. 選擇 Add authorization rule (新增授權規則)。

新增授權規則 (AWS CLI)

使用 authorize-client-vpn-ingress 命令。

下列範例授權所有使用者存取10.1.0.0/16網路：

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
    --authorize-all-groups
```

下列範例授權特定的 Active Directory 群組：

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
    --access-group-id S-1-2-34-1234567890-1234567890-1234567890-1234
```

管理可用區域

您可以在建立後修改 Transit Gateway 相關 Client VPN 端點的可用區域。

新增單一可用區域 (AWS CLI)

使用 associate-client-vpn-target-network 命令搭配 `--availability-zone` 參數。

```
aws ec2 associate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone us-east-1c
```

移除單一可用區域 (AWS CLI)

首先，使用 describe-client-vpn-target-networks 命令來尋找可用區域的關聯 ID。

```
aws ec2 describe-client-vpn-target-networks \
```

```
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

然後使用 disassociate-client-vpn-target-network 命令搭配關聯 ID。

```
aws ec2 disassociate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --association-id cvpn-assoc-0a1b2c3d4e5f6EXAMPLE
```

跨帳戶傳輸閘道存取

您可以建立與不同 AWS 帳戶擁有的 Transit Gateway 相關聯的 Client VPN 端點。若要這樣做，傳輸閘道擁有者必須透過您的帳戶共用傳輸閘道 AWS Resource Access Manager。

先決條件

- Transit Gateway 擁有者帳戶 — 現有的 Transit Gateway 和在其中建立資源共用的許可 AWS Resource Access Manager。
- Client VPN 端點帳戶 — 建立 Client VPN 端點並接受 AWS Resource Access Manager 資源共用的許可。

在 Client VPN 端點帳戶中，使用 accept-resource-share-invitation 命令在 AWS Resource Access Manager 主控台中接受資源共用。接受共用後，當您建立 Client VPN 端點時，傳輸閘道 ID 下拉式清單中會顯示傳輸閘道。

考量和限制

當您使用 Transit Gateway 與 Client VPN 整合時，請考慮下列事項：

- 關聯限制
  - 您無法在單一端點中混合 VPC 子網路關聯和 Transit Gateway 關聯。
  - 每個端點只能使用一種關聯類型。
- 安全群組
  - Transit Gateway 端點不支援安全群組型授權。
  - 僅使用網路型授權規則。
- 路由管理
  - 不支援來自 Transit Gateway 的自動路由傳播。
  - 您必須手動定義目的地網路的路由。

- CIDR 重疊
  - Client VPN CIDR 區塊不應與其他 Transit Gateway 附件或 Transit Gateway CIDR 區塊重疊。
  - Transit Gateway 不支援跨連接的 VPCs 重疊 CIDR 範圍。
- 區域限制
  - Client VPN 端點和 Transit Gateway 必須位於相同的 AWS 區域。
  - Client VPN 不支援跨區域傳輸閘道對等互連。
- 可用區域
  - 每個端點最多可以指定 5 個可用區域。
  - 如果未指定， AWS 會自動指派 2 個可用區域。
  - Client VPN 和 Transit Gateway 必須同時支援所有指定的可用區域。
- 傳回路由
  - 連接到 Transit Gateway VPCs 必須設定傳回路由，以將目的地為 Client VPN CIDR 的流量路由回 Transit Gateway。
  - 如果沒有適當的傳回路由，VPN 用戶端無法存取 VPCs中的資源。
    - 對於 IPv4：Client VPN CIDR 在端點建立時已知。
    - 對於 IPv6：您必須描述 Transit Gateway 路由表，以判斷指派給 Client VPN 端點的 IPv6 CIDR 範圍 （與 Client VPN 端點相關聯的 Transit Gateway Route Table 中最大的 CIDR 範圍），因為 IPv6 用戶端 CIDR 範圍會自動指派 AWS Client VPN。
- 連線和流程日誌
  - 您可以啟用傳輸閘道流量日誌，以擷取進出傳輸閘道之 IP 流量的相關資訊。您可以啟用 Client VPN 連線日誌，以擷取 Client VPN 連線事件的相關資訊。
  - 您可以比較 Transit Gateway 流量日誌事件中的用戶端 IP 和時間戳記與 Client VPN 連線日誌中的相同用戶端 IP 和期間，將 Transit Gateway 流量日誌事件與 Client VPN 連線關聯。
- 網際網路連線
  - 若要透過具有 Transit Gateway 的 Client VPN 存取網際網路，而不需要分割通道，連接的 VPC 必須已設定 NAT。
    - 針對 IPv4：設定 NAT 閘道以公有 IPs地址取代 Client VPN 用戶端 IP。
    - 對於 IPv6：請參閱使用 IPv6 的集中式網際網路傳出流量。

中的安全性 AWS Client VPN

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。作為AWS 合規計劃的一部分，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計劃 AWS Client VPN，請參閱合規AWS 計劃的 服務範圍合規。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

AWS Client VPN 是 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。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Client VPN 資源。

主題

- 中的資料保護 AWS Client VPN
- 的身分和存取管理 AWS Client VPN
- 中的彈性 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 AWS Client VPN

中的資料保護 AWS Client VPN

共同責任模型適用於 AWS Client VPN AWS 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。 如需歐洲資料保護的相關資訊，請參閱「一般資料保護法規 (GDPR) 中心」。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Client VPN 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 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，從任何位置提供安全連線。

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 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 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)

的身分和存取管理 AWS Client VPN

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可以控制誰能進行身分驗證 (已登入) 和獲得授權 (具有許可) 而得以使用 Client VPN 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS Client VPN 如何使用 IAM
- 的身分型政策範例 AWS Client VPN
- 對 AWS Client VPN 身分和存取進行故障診斷
- 使用 的服務連結角色 AWS Client VPN

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 AWS Client VPN 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 AWS Client VPN 如何使用 IAM)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 的身分型政策範例 AWS Client VPN)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須驗證為 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和 資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是您企業目錄、Web 身分提供者的使用者，或是 AWS 服務 使用身分來源的憑證 Directory Service 存取的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。

- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS Client VPN 如何使用 IAM

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
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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 的身分型政策範例 AWS Client VPN。

Client VPN 內的資源型政策

支援資源型政策：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。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

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內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 Client VPN 動作清單，請參閱《服務授權參考》中的 AWS Client VPN 定義的動作。

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 的身分型政策範例 AWS Client VPN。

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內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看 Client VPN 資源類型及其 ARNs的清單，請參閱服務授權參考中的 AWS Client VPN 定義的資源。若要了解您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 的身分型政策範例 AWS Client VPN。

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內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 Client VPN 條件金鑰清單，請參閱《服務授權參考》中的 AWS Client VPN 的條件金鑰。若要了解您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 的身分型政策範例 AWS Client VPN。

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)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

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》中的使用 ABAC 授權定義許可。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

臨時登入資料提供 AWS 資源的短期存取權，並在您使用聯合或切換角色時自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

Client VPN 的跨服務委託人許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。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。

Client VPN 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

的身分型政策範例 AWS Client VPN

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。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。

如需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 (主控台)。

如需有關 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 ARNs 格式，請參閱《服務授權參考》中的 AWS Client VPN 的動作、資源和條件索引鍵。

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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作

AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

對 AWS Client VPN 身分和存取進行故障診斷

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
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 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 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

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

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 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 沒有將角色傳遞給服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 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 如何使用 IAM。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

使用 的服務連結角色 AWS Client VPN

AWS Client VPN use 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。服務連結角色是由 Client VPN 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

主題

- 使用 的角色 AWS Client VPN
- 在 Client VPN 中使用 角色進行連線授權；

使用 的角色 AWS Client VPN

AWS Client VPN use 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。服務連結角色是由 Client VPN 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 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，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。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。

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`

此服務連結角色使用受管政策 ClientVPNServiceRolePolicy。若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 ClientVPNServiceRolePolicy。

建立 Client VPN 的服務連結角色

您不需要手動建立服務連結角色，當您使用 AWS CLI、 或 AWS API 在帳戶中建立第一個 Client VPN AWS 管理主控台端點時，Client VPN 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 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描述。

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。

在 Client VPN 中使用 角色進行連線授權；

AWS Client VPN use 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。服務連結角色是由 Client VPN 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 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，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。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。

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

您不需要手動建立服務連結角色，當您使用 AWS CLI、 或 AWS API 在帳戶中建立第一個 Client VPN AWS 管理主控台端點時，Client VPN 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描述。

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。

中的彈性 AWS Client VPN

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施之外， AWS Client VPN 還提供 功能，以協助支援您的資料彈性和備份需求。

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。

中的基礎設施安全AWS Client VPN

AWS用戶端 VPN 是受管服務，受到AWS全球網路安全的保護。如需AWS安全服務以及 如何AWS保護基礎設施的相關資訊，請參閱AWS雲端安全。若要使用基礎設施安全的最佳實務來設計您的AWS環境，請參閱安全支柱AWS Well-Architected Framework 中的基礎設施保護。

您可以使用AWS發佈的 API 呼叫，透過網路存取 Client VPN。使用者端必須支援下列專案：

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

的安全最佳實務 AWS Client VPN

AWS Client VPN 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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。如需詳細資訊，請參閱用戶端憑證撤銷清單。

工作階段逾時時中斷連線

達到 Client VPN 工作階段時間上限時中斷連線工作階段，強制執行 VPN 工作階段持續時間上限。如需詳細資訊，請參閱VPN 工作階段持續時間上限。

監控工具

使用監控工具來追蹤 Client VPN 端點的可用性和效能。如需詳細資訊，請參閱監控 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。如需詳細資訊，請參閱的身分和存取管理 AWS Client VPN。

使用 AWS 提供的 VPN 用戶端

使用 AWS 提供的用戶端 AWS Client VPN，可從AWS Client VPN 下載頁面取得。

使用匯出的用戶端組態

使用從 AWS Client VPN 端點匯出的用戶端組態檔案。如需詳細資訊，請參閱匯出用戶端組態檔。請勿修改組態檔案中的密碼或 TLS 設定。 AWS Client VPN 端點僅支援下列演算法：

- TLS 1.3： TLS_AES_256_GCM_SHA384和 TLS_AES_128_GCM_SHA256
- TLS 1.2：TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384、TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384、 TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256和 TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
- 資料管道： AES-256-GCM

的 IPv6 考量 AWS Client VPN

Client VPN 現在支援原生 IPv6 連線與現有的 IPv4 功能。您可以建立IPv6-only, IPv4-only 或雙堆疊 (IPv4 和 IPv6) 端點，以符合您的聯網需求。

IPv6 支援的關鍵元件

在 Client VPN 中使用 IPv6 時，有兩個金鑰組態參數：

端點 IP 地址類型

此參數定義端點管理 IP 類型，這會決定為端點佈建的 EC2 執行個體類型。此 IP 類型用於管理外部 VPN 通道流量 （透過公有網際網路在 OpenVPN 用戶端和伺服器之間流動的加密流量）。

流量 IP 地址類型

此參數定義流經 VPN 通道的流量類型。此 IP 類型用於管理每個端點的內部加密流量 （實際承載）、用戶端 CIDR 範圍、子網路關聯、路由和規則。

IPv6 用戶端 CIDR 指派

對於 IPv6 用戶端 CIDR，您不需要指定 CIDR 區塊。Amazon 會自動為 IPv6 用戶端指派 CIDR 範圍。此自動指派可為 IPv6 通道流量啟用無 SNATing，從而增強對連線使用者的 IPv6 地址的可見性。

相容性要求

IPv6 和雙堆疊端點取決於使用者裝置和網際網路服務提供者 (ISPs)：

- 執行 CVPN 用戶端的使用者裝置必須支援必要的 IP 組態，如以下相容性資料表所示。
- ISPs支援必要的 IP 組態，連線才能正常運作。
- 對於 IPv6 或雙堆疊流量，相關聯的 VPC 子網路必須具有 IPv6 或雙堆疊 CIDR 範圍。

DNS 支援

所有類型的端點都支援 DNS - IPv4, IPv6 和雙堆疊。對於 IPv6 端點，您可以使用 `--dns-server-ipv6` 參數設定 IPv6 DNS 伺服器。服務和用戶端都支援 AAAA DNS 記錄。

限制

以下是 IPv6 的限制：

- IPv6 用戶端不支援Client-to-client(C2C) 通訊。如果 IPv6 用戶端嘗試與其他 IPv6 用戶端通訊，則會捨棄流量。

IPv6 的用戶端路由強制執行

Client VPN 現在支援 IPv6 流量的用戶端路由強制執行。此功能有助於確保來自連線用戶端的 IPv6 網路流量遵循管理員定義的路由，且不會不小心傳送至 VPN 通道外部。

IPv6 用戶端路由強制執行支援的關鍵層面：

- 現有的`ClientRouteEnforcementOptions.enforced`旗標會同時為 IPv4 和 IPv6 堆疊啟用 CRE。
- IPv6 用戶端路由強制執行會排除特定 IPv6 範圍，以維護重要的 IPv6 功能：
  - `::1/128` — 預留給迴路
  - `fe80::/10` — 預留給 link-local 地址

- ff00::/8 — 預留給多點傳送
- IPv6 用戶端路由強制執行適用於 Windows、macOS 和 Ubuntu 上的 AWS VPN 用戶端 5.3.0 版和更新版本。

如需 CRE 的詳細資訊，包括如何啟用和設定，請參閱 the section called “用戶端路由強制執行”。

IPv6 洩漏預防 （ 舊版資訊 ）

對於不使用原生 IPv6 支援的舊組態，您可能仍然需要防止 IPv6 洩漏。當 IPv4 和 IPv6 都啟用並連接到 VPN 時，IPv6 洩漏可能會發生，但 VPN 不會將 IPv6 流量路由到其通道。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」裝置路由， 的第二個參數`ifconfig-ipv6`將用作 的路由目標`--route-ipv6`。

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。還有一些公開可用的工具。

監控 AWS Client VPN

監控是維護 AWS Client VPN 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。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

AWS 即時監控您的 AWS 資源和您在 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀板表，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

擷取由您的帳戶或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。CloudTrail 會記錄所有 Client VPN 動作，並記錄在《Amazon EC2 API 參考》中。

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AWS Client VPN 端點的連線記錄和《Amazon CloudWatch Logs 使用者指南》。

主題

- 的 Amazon CloudWatch 指標 AWS Client VPN

的 Amazon CloudWatch 指標 AWS Client VPN

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

指標	說明
ActiveConnectionsCount	Client VPN 端點的作用中連線數目。

指標	說明
	單位：Count
AuthenticationFailures	Client VPN 端點的身分驗證失敗次數。 單位：Count
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：Count
IdpCertDaysToExpiry	在 Client VPN 端點上設定的身分提供者 (IdP) 憑證過期前的天數。只有使用 SAML 型聯合身分驗證設定的端點才會報告此指標。 單位：天
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：Count
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	說明
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：Count
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。 單位：Count
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：Count
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：Count
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：Count
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：Count

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)。

如需更多資訊，請參閱 Amazon CloudWatch 使用者指南。

任務

- 在 Amazon CloudWatch 中檢視 Client VPN 端點指標

在 Amazon CloudWatch 中檢視 Client VPN 端點指標

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。

使用 檢視指標 AWS CLI

在命令提示中，使用下列命令來列出可用於 Client VPN 的指標。

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

AWS Client VPN 配額

AWS 您的帳戶具有下列配額，先前稱為與 Client VPN 端點相關的限制。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	200 對於雙堆疊端點，此限制會在 IPv4 和 IPv6 路由之間共用。	是
每個區域的 Client VPN 端點	5	是
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。 • 1 – 7,000 • 2 – 36,500 • 3 – 66,500 • 4 – 96,500 • 5 – 126,000 對於雙堆疊端點，此限制會在 IPv4 和 IPv6 連線之間共用。	是
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

名稱	預設	可調整
每個 Client VPN 目標網路關聯的路由數	100 對於雙堆疊端點，此限制會在 IPv4 和 IPv6 路由之間共用。	是

† 操作包含：

- 關聯或取消關聯子網路
- 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 身分驗證 AWS Directory Service 的資源相同的帳戶。
- 如果您使用 SAML 型聯合身分驗證來驗證使用者，則 Client VPN 端點必須與您建立的 IAM SAML 身分提供者屬於相同的帳戶，以定義 AWS IdP 信任關係。IAM SAML 身分提供者可以在相同 AWS 帳戶中的多個 Client VPN 端點之間共用。

故障診斷 AWS Client VPN

下列各節可協助您針對 Client VPN 端點可能遇到的問題進行疑難排解。

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

- 故障診斷 AWS Client VPN：無法解析 Client VPN 端點 DNS 名稱
- 故障診斷 AWS Client VPN：未在子網路之間分割流量
- 故障診斷 AWS Client VPN：Active Directory 群組的授權規則未如預期運作
- 故障診斷 AWS Client VPN：用戶端無法存取對等 VPC、Amazon S3 或網際網路
- 故障診斷 AWS Client VPN：對對等 VPC、Amazon S3 或網際網路的存取是間歇性的
- 故障診斷 AWS Client VPN：嘗試連線至 Client VPN 時，用戶端軟體會傳回 TLS 錯誤
- 故障診斷 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — Active Directory 身分驗證
- 故障診斷 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — 聯合身分驗證
- 故障診斷 AWS Client VPN：用戶端無法連線 — 交互身分驗證
- 故障診斷 AWS Client VPN：用戶端傳回的憑證超過 Client VPN 中的大小上限錯誤 — 聯合身分驗證
- 故障診斷 AWS Client VPN：用戶端不會開啟端點的瀏覽器 — 聯合身分驗證
- 故障診斷 AWS Client VPN：用戶端未傳回任何可用的連接埠錯誤 — 聯合身分驗證
- 故障診斷 AWS Client VPN：因 IP 不相符而終止連線
- 故障診斷 AWS Client VPN：將流量路由到 LAN 無法如預期運作
- 故障診斷 AWS Client VPN：驗證 Client VPN 端點的頻寬限制
- 故障診斷 AWS Client VPN：VPC 的通道連線問題

故障診斷 AWS Client VPN：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`

故障診斷 AWS Client VPN：未在子網路之間分割流量

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。

故障診斷 AWS Client VPN：Active Directory 群組的授權規則未如預期運作

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。

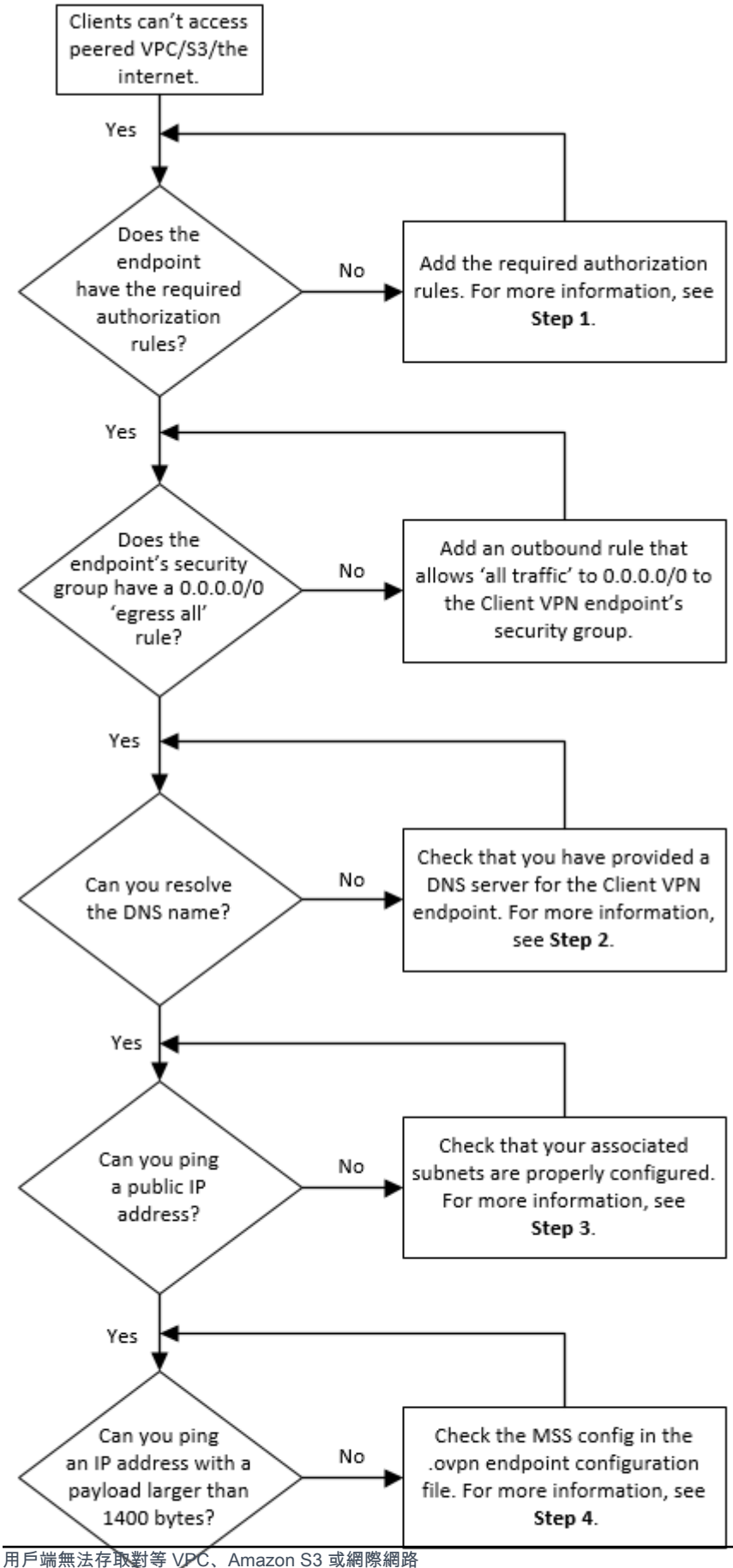
故障診斷 AWS Client VPN：用戶端無法存取對等 VPC、Amazon S3 或網際網路

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。


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

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
   ```

故障診斷 AWS Client VPN：對對等 VPC、Amazon S3 或網際網路的存取是間歇性的

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

故障診斷 AWS Client VPN：嘗試連線至 Client VPN 時，用戶端軟體會傳回 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AWS Client VPN 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 CLI AWS 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户端憑證及金鑰，然後將它們匯入 ACM 中的詳細步驟，請參閱中的相互身分驗證 AWS Client VPN。

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。

故障診斷 AWS Client VPN：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AWS Client VPN 端點組態檔案匯出。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。

故障診斷 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — 聯合身分驗證

問題

嘗試使用聯合身分驗證的使用者名稱和密碼登入，並收到錯誤「收到的登入資料不正確。請聯絡您的 IT 管理員。」

原因

此錯誤可能是因為 IdP 的 SAML 回應中沒有包含至少一個屬性。

解決方案

確定 IdP 的 SAML 回應中至少包含一個屬性。如需詳細資訊，請參閱「SAML 型 IdP 組態資源」。

故障診斷 AWS Client VPN：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AWS Client VPN 端點組態檔案匯出。

故障診斷 AWS Client VPN：用戶端傳回的憑證超過 Client VPN 中的大小上限錯誤 — 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。

故障診斷 AWS Client VPN：用戶端不會開啟端點的瀏覽器 — 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，將其匯入至 AWS 提供的用戶端，然後再次嘗試連線。

故障診斷 AWS Client VPN：用戶端未傳回任何可用的連接埠錯誤 — 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 來完成身分驗證。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。

故障診斷 AWS Client VPN：因 IP 不相符而終止連線

問題

VPN 連線已終止，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連線的 IP 地址符合支援 Client VPN 端點的 VPN 伺服器的 IP。如需詳細資訊，請參閱使用 的規則和最佳實務 AWS Client VPN。

解決方案

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

故障診斷 AWS Client VPN：將流量路由到 LAN 無法如預期運作

問題

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

原因

如果偵測到用戶端 LAN 地址範圍超出上述標準範圍，則 Client VPN 端點會自動將 OpenVPN 指令 "redirect-gateway block-local" 推送至用戶端，強制所有 LAN 流量進入 VPN。如需詳細資訊，請參閱使用 的規則和最佳實務 AWS Client VPN。

解決方案

如果您在 VPN 連接期間需要 LAN 存取，建議您為 LAN 使用上面列出的傳統地址範圍。

故障診斷 AWS Client VPN：驗證 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。每個使用者連線支援 10 Mbps 的最小頻寬。

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
```

故障診斷 AWS Client VPN：VPC 的通道連線問題

當您的 AWS Client VPN 連線遇到連線問題時，請遵循此系統疑難排解方法來識別並解決問題。本節提供step-by-step程序，以診斷遠端用戶端與 Amazon VPC 資源之間的常見 Client VPN 連線問題。

主題

- 網路連線先決條件
- 檢查 Client VPN 端點狀態
- 驗證用戶端連線
- 驗證用戶端身分驗證
- 檢查授權規則
- 驗證 Client VPN 路由
- 驗證安全群組和網路 ACLs
- 測試用戶端連線
- 診斷用戶端裝置
- 故障診斷 DNS 解析
- 對效能進行故障診斷
- 監控 Client VPN 指標
- 檢查 Client VPN 日誌
- 常見問題與解決方案

網路連線先決條件

在對 Client VPN 連線進行故障診斷之前，請確認這些網路先決條件：

- 確保 Client VPN 端點子網路具有網際網路連線能力（透過網際網路閘道或 NAT 閘道）。
- 確認 Client VPN 端點與不同可用區域中的子網路相關聯，以獲得高可用性。
- 檢查 VPC 是否有足夠的 IP 地址空間，且不與用戶端 CIDR 區塊衝突。
- 確認目標子網路具有適當的路由表關聯。

檢查 Client VPN 端點狀態

首先，確認您的 Client VPN 端點處於正確狀態：

1. 使用 AWS CLI 檢查 Client VPN 端點狀態：

```
aws ec2 describe-client-vpn-endpoints --region your-region
```

2. 在輸出中尋找端點狀態。狀態應為 `available`。
3. 確認端點具有相關聯的目標網路（子網路）。
4. 如果狀態不是 `available`，請檢查可能表示組態問題的任何錯誤訊息或擱置狀態。

驗證用戶端連線

檢查用戶端連線至 Client VPN 端點的狀態：

1. 檢查作用中的用戶端連線：

```
aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id
 --region your-region
```

2. 檢閱連線狀態和輸出中的任何錯誤訊息。
3. 檢查用戶端身分驗證日誌是否有失敗的身分驗證嘗試。
4. 確認用戶端正在從設定的用戶端 CIDR 區塊接收 IP 地址。

> **Note**
>
> 如果用戶端無法連線，問題可能是身分驗證組態、授權規則或網路連線。

驗證用戶端身分驗證

身分驗證問題是 Client VPN 連線問題的常見原因：

- 對於交互身分驗證，請確保用戶端憑證有效且未過期。
- 針對 Active Directory 身分驗證，驗證使用者登入資料和網域連線。
- 對於以 SAML 為基礎的聯合身分驗證，請檢查 IdP 組態和使用者許可。
- 檢閱 CloudWatch 中的身分驗證日誌，以取得詳細的錯誤資訊。
- 確認端點上設定的身分驗證方法符合用戶端組態。

檢查授權規則

授權規則控制用戶端可存取的網路資源：

1. 列出目前的授權規則：

```
aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. 確認用戶端需要存取的目標網路存在規則。
3. 檢查規則是否指定正確的 Active Directory 群組（如果使用 AD 身分驗證）。
4. 確保授權規則處於 `active` 狀態。

驗證 Client VPN 路由

適當的路由組態對於 Client VPN 連線至關重要：

1. 檢查 Client VPN 端點路由：

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. 驗證用戶端需要存取的目標網路是否有路由。
3. 檢查 Amazon VPC 路由表，以確保傳回流量可以到達 Client VPN 端點：

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-region
```

4. 確認已正確設定目標網路關聯。

驗證安全群組和網路 ACLs

安全群組和網路 ACLs可以封鎖 Client VPN 流量：

1. 檢查目標 EC2 執行個體的安全群組：

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxxx --region your-region
```

2. 驗證傳入規則允許來自 Client VPN CIDR 區塊的流量：
   - Client VPN CIDR 的 SSH（連接埠 22)： `10.0.0.0/16`
   - 來自 Client VPN CIDR 的 HTTP（連接埠 80)： `10.0.0.0/16`

- 來自 Client VPN CIDR 的 HTTPS（連接埠 443）：`10.0.0.0/16`
- 視需要自訂應用程式連接埠

3. 對於 Client VPN 端點安全群組（如果適用），請確保它允許：
   - 從 0.0.0.0/0 的 UDP 連接埠 443 (OpenVPN)
   - 所有傳出至 VPC CIDR 區塊的流量
4. 檢查網路 ACLs是否未封鎖流量。網路 ACLs 是無狀態的，因此必須設定傳入和傳出規則。
5. 驗證您嘗試傳送之特定流量的傳入和傳出規則。

測試用戶端連線

測試從 Client VPN 用戶端到 Amazon VPC 資源的連線：

1. 從連線的 Client VPN 用戶端，測試與 Amazon VPC 資源的連線：

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. 測試特定應用程式連線：

```
telnet vpc-resource-ip port
```

3. 如果使用私有 DNS 名稱，請驗證 DNS 解析：

```
nslookup private-dns-name
```

4. 如果啟用分割通道，則測試網際網路資源的連線能力。

診斷用戶端裝置

在用戶端裝置上執行這些檢查：

1. 確認用戶端組態檔案 (.ovpn) 包含正確的設定：
   - 正確的伺服器端點 URL
   - 有效的用戶端憑證和私有金鑰
   - 適當的身分驗證方法組態

2. 檢查用戶端日誌是否有連線錯誤：
   - Windows：事件檢視器 → 應用程式和服務日誌 → OpenVPN
   - macOS：主控台應用程式，搜尋「Tunnelblick」或「OpenVPN」
   - Linux： `/var/log/openvpn/`或系統化日誌
3. 從用戶端測試基本網路連線：

```
ping 8.8.8.8
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

故障診斷 DNS 解析

DNS 問題可能會阻止使用私有 DNS 名稱存取資源：

1. 檢查是否已在 Client VPN 端點中設定 DNS 伺服器：

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --
query 'ClientVpnEndpoints[0].DnsServers'
```

2. 從用戶端測試 DNS 解析：

```
nslookup private-resource.internal
dig private-resource.internal
```

3. 如果使用自訂 DNS 解析，請驗證 Route 53 Resolver 規則。
4. 檢查安全群組是否允許從 Client VPN CIDR 到 DNS 伺服器的 DNS 流量 (UDP/TCP 連接埠 53)。

對效能進行故障診斷

解決 Client VPN 連線的效能問題：

- 使用 CloudWatch 指標監控傳入/傳出位元組的頻寬使用率。
- 使用用戶端的持續 ping 測試來檢查封包遺失。
- 確認 Client VPN 端點未達到連線限制。
- 考慮使用多個 Client VPN 端點進行負載分佈。
- 使用不同的用戶端位置進行測試，以識別區域效能問題。

監控 Client VPN 指標

使用 CloudWatch 監控 Client VPN 端點指標：

1. 檢查作用中連線指標：

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name ActiveConnectionsCount \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Average
```

2. 檢閱身分驗證失敗指標：

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name AuthenticationFailures \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Sum
```

3. 檢閱其他可用的指標，例如輸入和輸出位元組和封包。

檢查 Client VPN 日誌

Client VPN 連線日誌提供有關連線嘗試和錯誤的詳細資訊：

- 如果尚未設定，請啟用 Client VPN 連線記錄。
- 檢閱 CloudWatch 日誌是否有連線嘗試、身分驗證失敗和授權錯誤。
- 尋找指出連線問題根本原因的特定錯誤代碼和訊息。
- 檢查失敗連線中可能表示組態問題的模式。

常見問題與解決方案

可能影響 Client VPN 連線的常見問題：

身分驗證失敗

用戶端憑證過期或無效，或 Active Directory 憑證不正確。驗證身分驗證組態和登入資料有效性。

缺少授權規則

由於授權規則遺失或不正確，用戶端無法存取目標網路。為所需的網路新增適當的授權規則。

分割通道問題

由於通道組態分割，流量路由不正確。視需要檢閱和調整分割通道設定。

用戶端 IP 集區耗盡

用戶端 CIDR 區塊中沒有可用的 IP 地址。展開用戶端 CIDR 範圍或中斷連接未使用的用戶端。

MTU 問題

由於 MTU 大小限制，大型封包正在捨棄。嘗試將 MTU 設定為 1436 位元組，或在用戶端裝置上啟用路徑 MTU 探索。

DNS 解析問題

用戶端無法解析私有 DNS 名稱。驗證 DNS 伺服器組態，並確保透過安全群組允許 DNS 流量。

重疊 IP 範圍

用戶端 CIDR 區塊與本機網路範圍衝突。檢查並解決用戶端 CIDR 和本機網路之間任何重疊的 IP 地址範圍。

TLS 交握失敗

TLS 交涉期間連線失敗。檢查憑證有效性、確保正確的密碼套件，並確認已正確設定用戶端和伺服器憑證。

路由傳播延遲

用戶端無法立即使用新的路由。變更 Client VPN 路由後，請等待 1-2 分鐘進行路由傳播。

連線中斷/不穩定

頻繁中斷連線或連線不穩定。檢查用戶端裝置上的網路擁塞、防火牆干擾或電源管理設定。

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
IPv6 支援	Client VPN 現在可啟用 Client VPN 端點的完整 IPv6 連線，支援 VPCs中和 IPv6 網路上用戶端對 IPv6 資源的連線。	2025 年 8 月 25 日
用戶端路由強制執行功能	新增用戶端路由強制執行功能。	2025 年 4 月 20 日
Client VPN 配額增加	將每個 Client VPN 端點配額的授權規則從 50 提高到 200。	2025 年 3 月 13 日
在工作階段逾時時支援中斷連線	工作階段逾時現在支援在達到工作階段持續時間上限時中斷連線。	2025 年 1 月 13 日
增加的配額	每個 Client VPN 端點的授權規則配額和每個 Client VPN 端點的路由配額分別從 50 和 10 增加到 100。	2024 年 12 月 19 日
授權規則範例	新增授權規則的範例案例。	2022 年 9 月 15 日
VPN 工作階段最長持續時間	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
用戶端登入橫幅	您可以在建立 VPN 工作階段以滿足法規和合規需求時，在 AWS 提供的 Client VPN 桌面應用程式上啟用文字橫幅。	2022 年 1 月 20 日

用戶端連線處理器	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
自助式入口網站	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
用戶端對用戶端的存取權限	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
SAML 2.0 型同盟驗證	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
在建立期間指定安全群組	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
可設定的 VPN 連接埠	您可以為 AWS Client VPN 端點指定支援的 VPN 連接埠號碼。	2020 年 1 月 16 日
支援 Multi-Factor Authentication (MFA)	如果您的 Active Directory 已啟用 MFA，則您的 AWS Client VPN 端點支援 MFA。	2019 年 9 月 30 日
支援分割通道	您可以在 AWS Client VPN 端點上啟用分割通道。	2019 年 7 月 24 日
初始版本	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。