管理員指南

AWS Client VPN

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

AWS Client VPN: 管理員指南

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

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

Table of Contents

什麼是 AWS Client VPN？

AWS Client VPN 是一項受管理的用戶端VPN服務，可讓您安全地存取內部部署網路中的資 AWS 源和資源。使用 ClientVPN，您可以使用開放VPN式用VPN戶端從任何位置存取您的資源。

主題

客戶的特點 VPN

用戶端VPN提供下列特性和功能：

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

用戶端的元件 VPN

以下是客戶端的關鍵概念VPN：

用戶端VPN端點

Client VPN 端點是您建立和設定以啟用和管理用戶端VPN工作階段的資源。這是所有用戶端VPN工作階段的終止點。

目標網路

目標網路是您與用戶VPN端端點建立關聯的網路。來自的子網路VPC是目標網路。將子網路與 Client VPN 端點建立關聯可讓您建立VPN工作階段。您可以將多個子網路與用戶VPN端端點建立關聯，以取得高可用性。所有子網路必須來自相同VPC的子網路。每個子網路必須屬於不同的可用區域。

路由

每個 Client VPN 端點都有一個路由表格，說明可用的目的地網路路由。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

連線到用戶端端點以建立VPN工作階段的終VPN端使用者。使用者需要下載開啟的用VPN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。每個與用戶VPN端端點的連線都會從用戶端CIDR範圍指派一個唯一的 IP 位址。您可以選擇用戶端CIDR範圍，例如，`10.2.0.0/16`。

客戶端端VPN口

AWS Client VPN 同TCP時支援和的連接埠 443 和 1194。UDP預設值為連接埠 443。

用戶端VPN網路介面

當您將子網路與 Client VPN 端點建立關聯時，我們會在該子VPN網路中建立用戶端網路介面。從用戶端端點傳送VPC到的流量會透過用戶VPN端VPN網路介面傳送。接著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 位址會轉譯為用戶端VPN網路介面 IP 位址。

連線日誌記錄

您可以啟用用戶VPN端端點的連線記錄，以記錄連線事件。您可以使用此資訊執行鑑識、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 提供自助入口網站做為網頁，供使用者下載最新版的AWSVPN桌面用戶端和最新版本的用戶VPN端端點設定檔，其中包含連線到其端點所需的設定。用戶端VPN端點管理員可以啟用或停用 Client VPN 端點的自助入口網站。自助入口網站是以下區域的服務堆疊支援的全球服務：美國東部 (維吉尼亞北部)、亞太區域 (東京)、歐洲 (愛爾蘭) 及 AWS GovCloud (美國西部)。

使用用戶端 VPN

您可以透過下列任何一種方式與用戶端VPN合作：

AWS Management Console

主控台為用戶端提供網頁式使用者介面VPN。如果您已註冊 AWS 帳戶，則可以登入 Amazon VPC 主控台並在導覽窗格VPN中選取用戶端。

AWS Command Line Interface (AWS CLI)

提 AWS CLI 供對用戶端VPN公用的直接存取APIs。Windows、macOS 和 Linux 都提供支援。若要取得有關入門的更多資訊 AWS CLI，請參閱《AWS Command Line Interface 使用者指南》。若要取得有關用戶端指令的更多資訊VPN，請參閱《AWS CLI 命令參考》。

AWS Tools for Windows PowerShell

AWS 為在PowerShell 環境中編寫指令碼的使用者提供廣泛的 AWS 產品組合的命令。如需 AWS Tools for Windows PowerShell入門的詳細資訊，請參閱 AWS Tools for Windows PowerShell 使用者指南。如需用戶端指令程式的相關資訊VPN，請參閱AWS Tools for Windows PowerShell 指令程式參考。

查詢 API

用戶端VPNHTTPS查詢可API讓您以程式設計方式存取用戶端VPN和 AWS.「HTTPS查詢」API 可讓您直接向服務發出HTTPS要求。使用時 HTTPSAPI，您必須包含程式碼，才能使用您的認證進行數位簽署要求。如需詳細資訊，請參閱 AWS Client VPN 動作。

客戶定價 VPN

每個端點關聯和每個VPN連線每小時都會向您收費。如需詳細資訊，請參閱 AWS Client VPN 定價。

您需要支付從 Amazon 傳輸到互聯網EC2的數據費用。如需詳細資訊，請參閱 Amazon EC2 隨需定價期限的資料傳輸。

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

如果您為用戶端端點啟用用戶VPN端連線處理常式，則必須建立並叫用 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。

用戶VPN端端點與目標網路相關聯，目標網路是VPC. 如果VPC有網 Internet Gateway，我們會將彈性 IP 位址與用戶端VPN彈性網路介面 (ENIs) 建立關聯。這些彈性 IP 位址會以使用中的公用位IPv4址計費。如需詳細資訊，請參閱定VPC價頁面上的 [公用IPv4位址] 索引標籤。

使用規則和最佳做法 AWS Client VPN

以下是使用的規則和最佳實踐 AWS Client VPN

- 每個使用者連線支援最低 10 Mbps 的頻寬。每個使用者連線的最大頻寬取決於要與用戶VPN端端點建立的連線數目。
- 用戶端CIDR範圍不能與相關子網路所VPC在的本機CIDR或任何手動新增至 Client VPN 端點路由表格的路由重疊。
- 用戶端CIDR範圍的區塊大小必須至少為 /22，且不得大於 /12。
- 用戶端CIDR範圍中的一部分位址用於支援用戶VPN端端點的可用性模型，而且無法指派給用戶端。因此，我們建議您指派一個CIDR區塊，其中包含的 IP 位址數目是啟用您計劃在 Client VPN 端點上支援的最大並行連線數目所需的兩倍。
- 建立用戶端端點之後，就無法變更用戶VPN端CIDR範圍。
- 與用戶VPN端端點相關聯的子網路必須位於相同VPC的子網路中。
- 您無法將來自相同可用區域的多個子網路與用戶VPN端端點建立關聯。
- 用戶端VPN端點不支援專用租用中的子網路關聯VPC。
- 用戶端僅VPN支援IPv4流量。IPv6的注意事項 AWS Client VPN如需詳細資訊，請參閱IPv6。
- 客戶VPN不符合聯邦資訊處理標準 (FIPS) 規範。
- 使用交互身分驗證進行身分驗證的用戶端無法使用自助式入口網站。
- 我們不建議使用 IP 位址連線到用戶VPN端端點。由於 Client VPN 是受管理的服務，因此您偶爾會看到DNS名稱解析的 IP 位址中的變更。此外，您會在 CloudTrail 記錄檔中看到用戶端VPN網路介面已刪除並重新建立。建議您使用提供的DNS名稱連線至用戶VPN端端點。
- 使用 AWS Client VPN 桌面應用程式時，目前不支援 IP 轉送。其他用戶端支援 IP 轉送。
- 用戶端VPN不支援中的多區域複寫 AWS Managed Microsoft AD。用戶端VPN端點必須與 AWS Managed Microsoft AD 資源位於相同的區域。

- 如果您的 Active Directory 停用了多因素驗證 (MFA)，使用者密碼就無法使用下列格式。

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- 如果有多個用戶登錄到操作系統，則無法從計算機建立VPN連接。
- 用戶端VPN服務要求用戶端所連線的 IP 位址與用戶VPN端端點DNS名稱解析為的 IP 相符。換句話說，如果您為 Client VPN 端點設定自訂DNS記錄，然後將流量轉寄到端點DNS名稱解析為的實際 IP 位址，則此設定將無法使用最近 AWS 提供的用戶端運作。新增此規則是為了緩解伺服器 IP 攻擊，如下所述：TunnelCrack。
- 用戶端VPN服務要求用戶端裝置的區域網路 (LAN) IP 位址範圍必須在下列標準私有 IP 位址範圍內：`10.0.0.0/8``172.16.0.0/12``192.168.0.0/16`、、或`169.254.0.0/16`。如果偵測到用戶端LAN位址範圍超出上述範圍，用戶VPN端端點會自動將 Open VPN 指令「重新導向閘道區塊本機」推送到用戶端，將所有LAN流量強制進入. VPN 因此，如果您在VPN連接過程中需要LAN訪問，建議您使用上面列出的常規地址範圍LAN。強制執行此規則以減輕本機網路攻擊的可能性，如下所述：TunnelCrack。

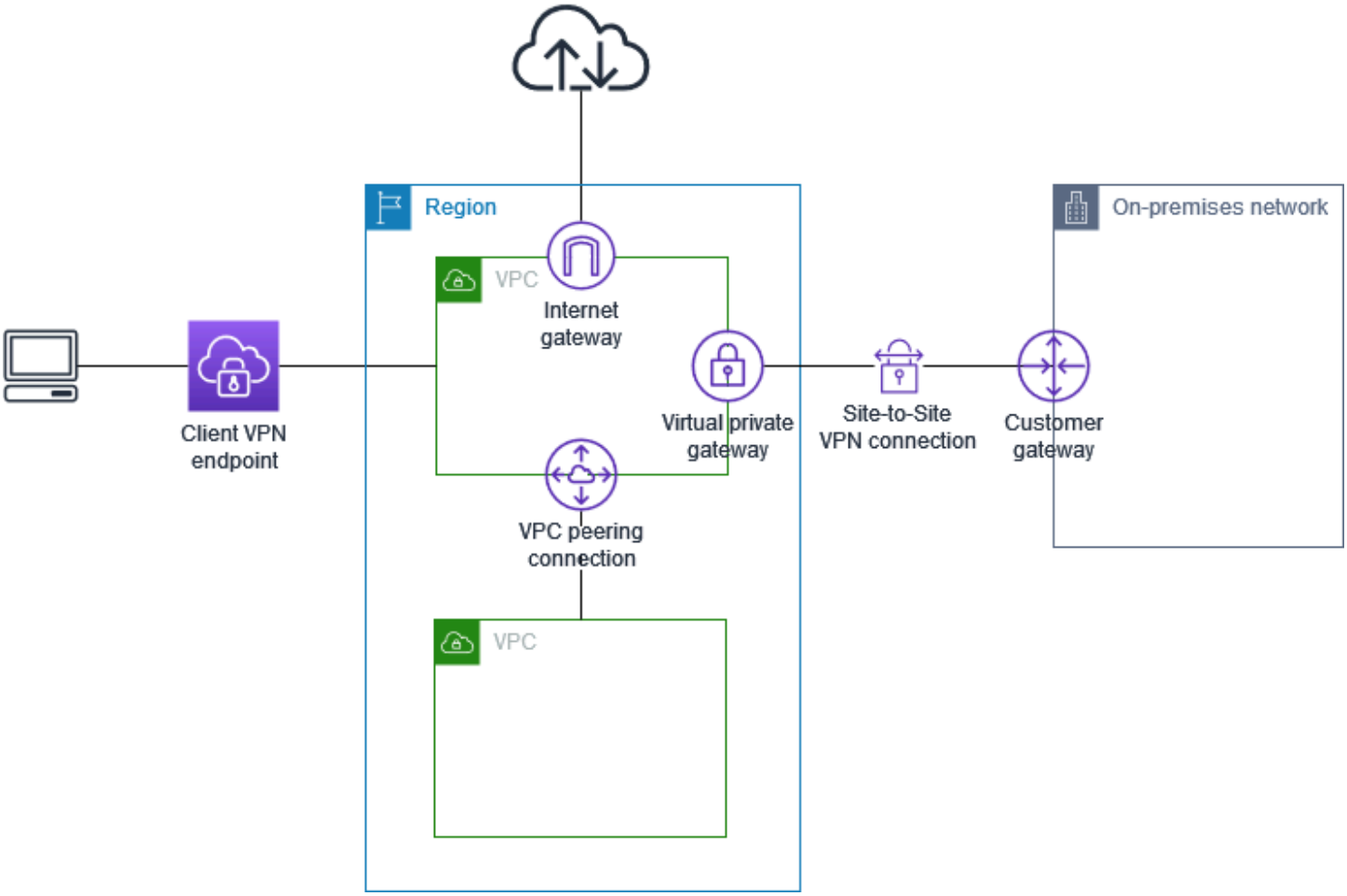
如何 AWS Client VPN 工作

使用時 AWS Client VPN，與用戶端端點互動的使用者角色有兩種類型：管理員和用戶VPN端。

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)。設定並設定 Client VPN 端點之後，管理員會下載 Client VPN 端點組態設定檔案，並將其散發給需要存取權的用戶端。用戶端VPN端點組態檔案包含用戶VPN端端點的DNS名稱和建立VPN工作階段所需的驗證資訊。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。這是連線至用戶VPN端端點以建立VPN工作階段的人員。用戶端VPN會使用開VPN放式用戶VPN端應用程式，從其本機電腦或行動裝置建立工作階段。建立VPN工作階段之後，他們就可以安全地存取關聯子網路所VPC在的資源。如果已設定所需的路由和授權規則 AWS，他們也可以存取內部部署網路或其他用戶端中的其他資源。如需有關連線到 Client VPN 端點以建立VPN工作階段的詳細資訊，請參閱AWS Client VPN 使用指南中的入門。

下圖說明基本的用戶端VPN架構。



用戶端的案例和範例 VPN

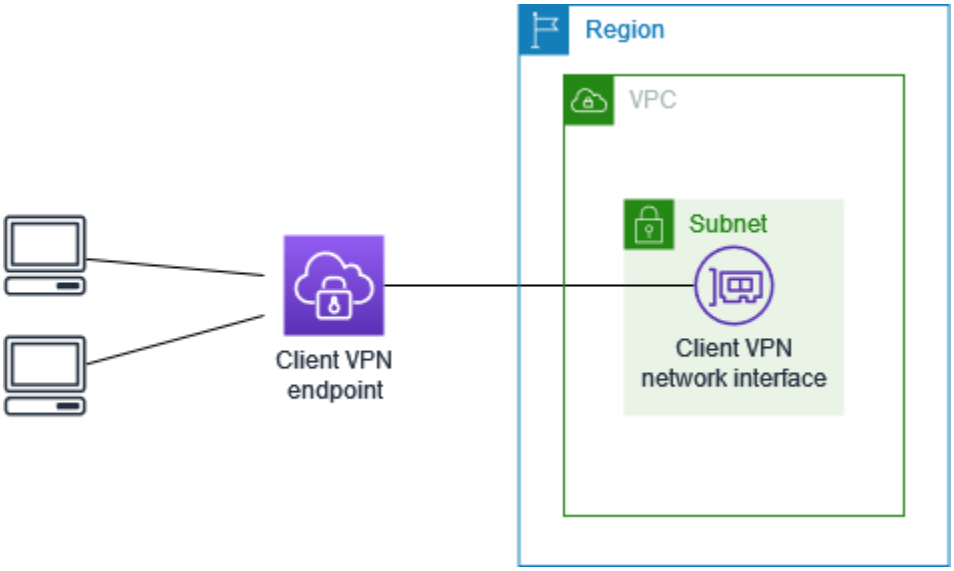
AWS Client VPN 是一種完全受管的遠端存取VPN解決方案，可讓用戶端安全地存取內部部署網路 AWS 和內部部署網路內的資源。如何設定存取權限，有多個選項。本節提供建立和設定用戶端VPN存取用戶端的範例。

案例

- the section called “存取一個 VPC”
- the section called “訪問對等 VPC”
- the section called “存取內部部署網路”
- the section called “存取網際網路”
- the section called “C lient-to-client 訪問權限”
- the section called “限制存取您的網路”

VPC使用客戶端訪問 VPN

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VPC只能存取單一資源，我們建議您使用此設定。



開始之前，請執行以下動作：

- 建立或識別至少VPC具有一個子網路。識別中的子網路VPC以與用戶VPN端端點建立關聯，並記下其IPv4CIDR範圍。
- 為不與重疊CIDR的用戶端 IP 位址識別適當的範圍VPCCIDR。

- 檢閱中用戶VPN端端點的規則和限制使用規則和最佳做法 AWS Client VPN。

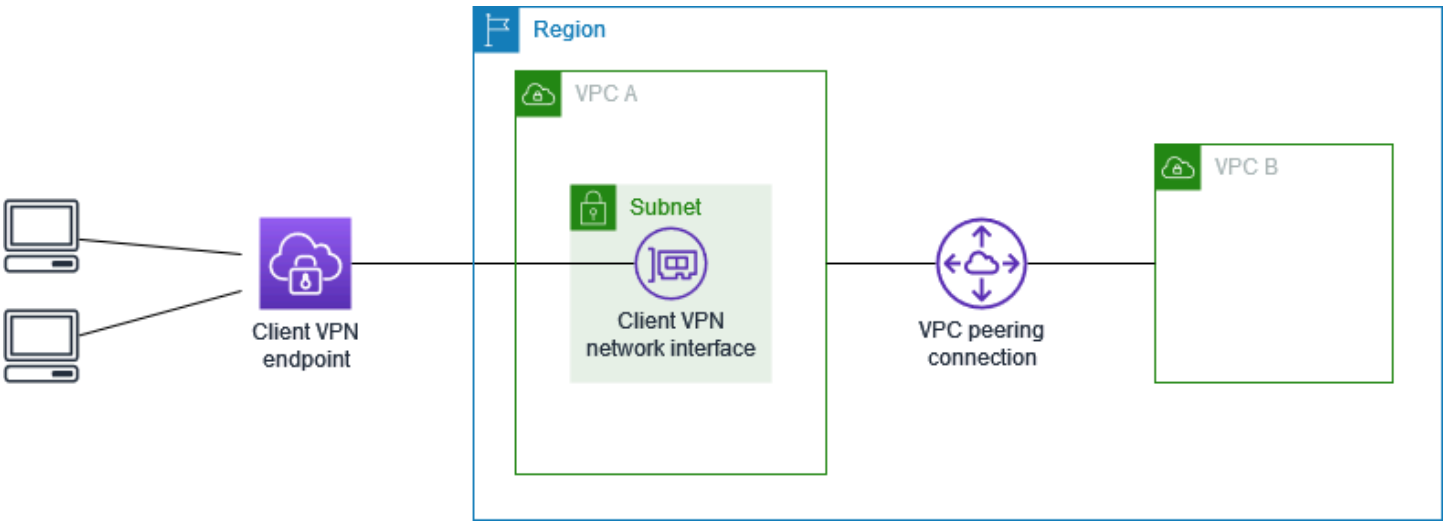
實作此組態

1. 在相同的區域中建立用戶VPN端端點VPC。若要執行此作業，請執行建立 AWS Client VPN 端點中所述的步驟。
2. 將子網路與用戶VPN端端點建立關聯。若要這麼做，請執行中所述的步驟，將目標網路與 AWS Client VPN 端點建立關聯然後選取子網路和VPC您先前所識別的子網路。
3. 新增授權規則，讓用戶端存取VPC. 若要執行此操作，請執行中所述的步驟新增授權規則，對於目的地網路，請輸入的IPv4CIDR範圍VPC。
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。

VPC使用客戶端訪問對等 VPN

此案例的 AWS Client VPN 組態包括與其他 VPC (VPCVPCB) 對等的目標 VPC (A)。如果您需要讓用戶端存取目標內的資源，以VPC及與目標對等的其他資源 (例如 VPC B) VPCs 的存取權，我們建議您使用此設定。

> **Note**
>
> 只有在用戶VPN端端點設定為分割通道模式時，才需要允許存取對等 VPC (如網路圖表之後所述) 的程序。在完整通道模式中，依預設允許存取對等。VPC



開始之前，請執行以下動作：

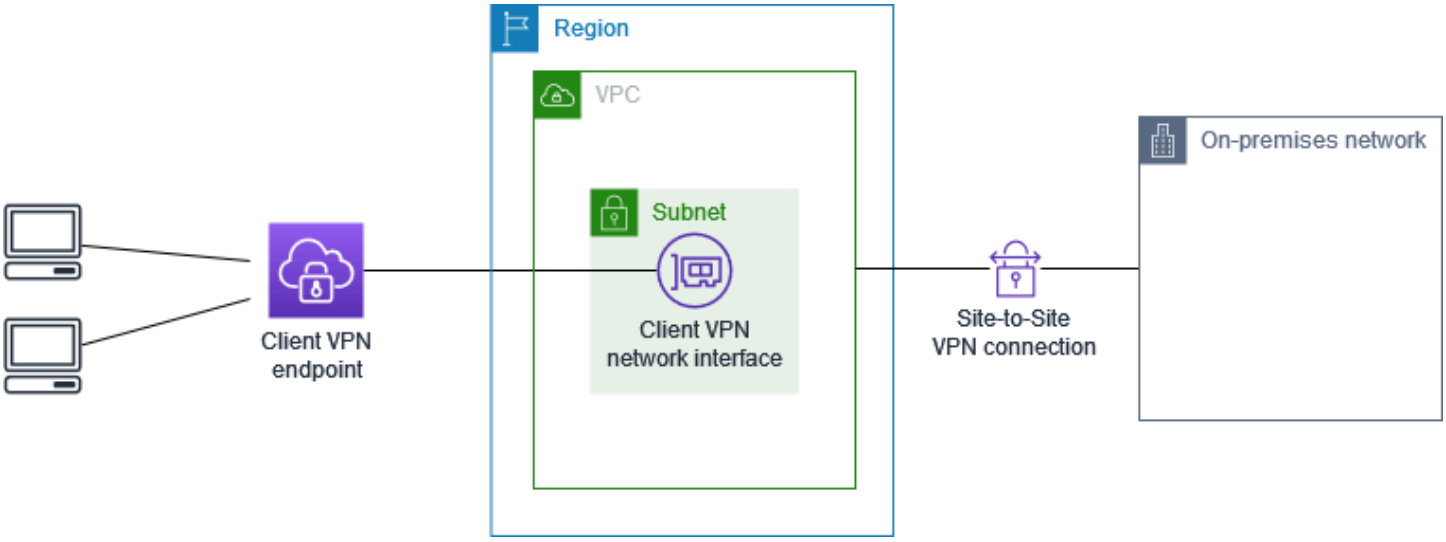
- 建立或識別至少VPC具有一個子網路。識別中的子網路VPC以與用戶VPN端端點建立關聯，並記下其IPv4CIDR範圍。
- 為不與重疊CIDR的用戶端 IP 位址識別適當的範圍VPCCIDR。
- 檢閱中用戶VPN端端點的規則和限制使用規則和最佳做法 AWS Client VPN。

實作此組態

1. 建立之間的VPC對等連接。VPCs請依照 Amazon 對等互連指南中建立和接受VPC對等連線中的步驟進行操VPC作。確認 A 中的執行VPC個體可以使用對等連線與 VPC B 中的執行個體進行通訊。
2. 在與目標相同的區域中建立用戶VPN端端點VPC。在圖中，這是 VPC A。執行中所述的步驟建立 AWS Client VPN 端點。
3. 將您識別的子網路與您建立的用戶VPN端端點建立關聯。若要這樣做，請執行中所述的步驟將目標網路與 AWS Client VPN 端點建立關聯，選取VPC和子網路。根據預設，我們會將的預設安全性群組VPC與 Client VPN 端點產生關聯。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，讓用戶端可存取目標VPC。若要執行此作業，請執行新增授權規則中所述的步驟。對於要啟用的目標網路，請輸入的IPv4CIDR範圍VPC。
5. 新增路由，將流量引導至對等。VPC在圖表中，這是 VPC B。若要這麼做，請執行中所述的步驟建立 AWS Client VPN 端點路由。在「路線目的地」中，輸入對等的IPv4CIDR範圍。VPC針對目標VPC子網路 ID，選取您與用戶VPN端端點相關聯的子網路。
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，輸入對等的IPv4CIDR範圍。VPC
7. 將規則新增至 VPC A 和 B 中執行VPC個體的安全群組，以允許來自在步驟 3 中套用 Client VPN 端點之安全群組的流量。如需詳細資訊，請參閱安全群組。

使用用戶端存取內部部署網路 VPN

此案例的 AWS Client VPN 組態僅包含內部部署網路的存取權。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VPC具有一個子網路。識別中的子網路VPC以與用戶VPN端端點建立關聯，並記下其IPv4CIDR範圍。
- 為不與重疊CIDR的用戶端 IP 位址識別適當的範圍VPCCIDR。
- 檢閱中用戶VPN端端點的規則和限制使用規則和最佳做法 AWS Client VPN。

實作此組態

1. 透過 AWS 站台對VPN站台連線，啟用VPC與您自己的內部部署網路之間的通訊。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，您可以使用您VPC與內部部署網路之間的 AWS Direct Connect 連線來實作此案例。如需詳細資訊，請參閱《AWS Direct Connect 使用者指南》https://docs.aws.amazon.com/directconnect/latest/UserGuide/。

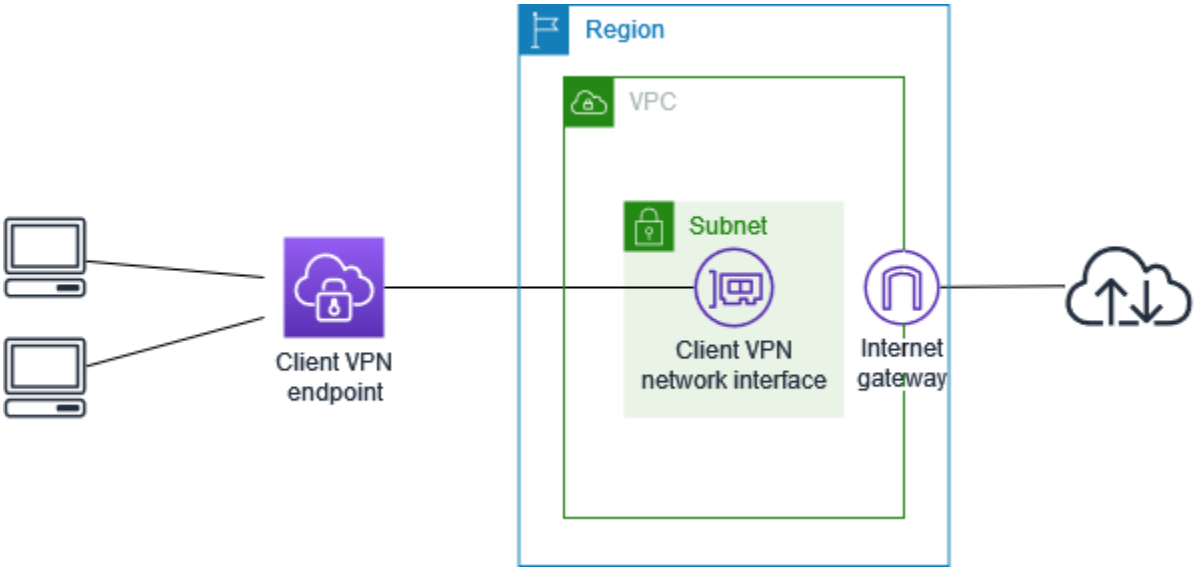
2. 測試您在上一個步驟中建立的 AWS 站台對站台VPN連線。若要這麼做，請執行「AWS Site-to-Site VPN 使用者指南」中測試站台間VPN連線中所述的步驟。如果VPN連線如預期般運作，請繼續執行下一個步驟。
3. 在相同的區域中建立用戶VPN端端點VPC。若要執行此作業，請執行建立 AWS Client VPN 端點中所述的步驟。

4. 將您先前識別的子網路與用戶VPN端端點建立關聯。若要這麼做，請執行中所述的步驟，將目標網路與 AWS Client VPN 端點建立關聯然後選取VPC和子網路。
5. 新增允許存取 AWS 站台間連VPN線的路由。若要這樣做，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，請輸入站 AWS 台對站台VPN連線的IPv4CIDR範圍，並針對目標VPC子網路 ID，選取與用戶端端VPN點相關聯的子網路。
6. 新增授權規則，讓用戶端存取站 AWS 台對站台連線VPN。若要執行此操作，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，請輸入站 AWS 台對站台VPN連線IPv4CIDR範圍。

使用用戶端存取網際網路 VPN

此案例的 AWS Client VPN 組態包括單一目標VPC和網際網路的存取權。如果您需要讓用戶端存取單一目標內的資源，VPC並允許存取網際網路，我們建議您使用此設定。

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：

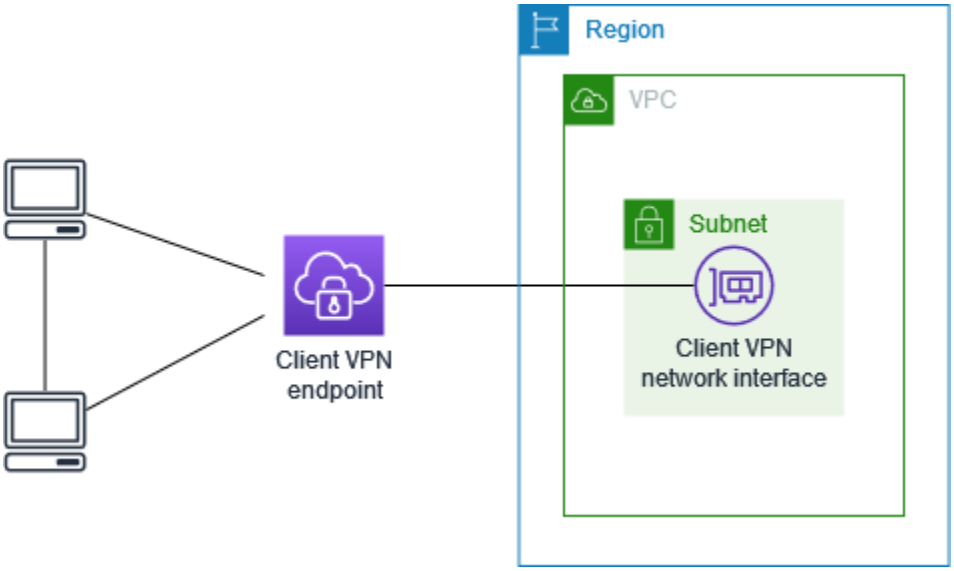
- 建立或識別至少VPC具有一個子網路。識別中的子網路VPC以與用戶VPN端端點建立關聯，並記下其IPv4CIDR範圍。
- 為不與重疊CIDR的用戶端 IP 位址識別適當的範圍VPCCIDR。
- 檢閱中用戶VPN端端點的規則和限制使用規則和最佳做法 AWS Client VPN。

實作此組態

1. 請確定您將用於 Client VPN 端點的安全性群組允許輸出流量到網際網路。若要這麼做，請新增允許流量和流量為 0.0.0.0/0 的輸出規則。HTTP HTTPS
2. 創建一個互聯網網關並將其附加到您的VPC. 如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立和連接 Internet Gateway。
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主控台中，選擇 [子網路]，選取要與用戶VPN端端點建立關聯的子網路，選擇 [路由表]，然後選擇路由表格識別碼。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. 在相同的區域中建立用戶VPN端端點VPC。若要執行此作業，請執行建立 AWS Client VPN 端點中所述的步驟。
5. 將您先前識別的子網路與用戶VPN端端點建立關聯。若要這麼做，請執行中所述的步驟，將目標網路與 AWS Client VPN 端點建立關聯然後選取VPC和子網路。
6. 新增授權規則，讓用戶端存取VPC. 若要執行此操作，請執行中所述的步驟新增授權規則；若要啟用目的地網路，請輸入的IPv4CIDR範圍VPC。
7. 新增路由以允許流向網際網路的流量。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，請輸入`0.0.0.0/0`，然後針對目標VPC子網路 ID，選取與用戶VPN端端點相關聯的子網路。
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. 確保您中資源的安全群組具VPC有允許從與 Client VPN 端點關聯的安全性群組進行存取的規則。這可讓您的用戶端存取VPC.

使用客戶端lient-to-client 訪問 C VPN

此案例的 AWS Client VPN 組態可讓用戶端存取單一資料VPC，並讓用戶端彼此路由傳送流量。如果連線到相同用戶端端點的用戶VPN端也需要彼此通訊，建議使用此設定。當用戶端連線到用戶端端點時，用戶端可以使用從用戶端CIDR範圍指派給用戶VPN端的唯一 IP 位址彼此通訊。



開始之前，請執行以下動作：

- 建立或識別至少VPC具有一個子網路。識別中的子網路VPC以與用戶VPN端端點建立關聯，並記下其IPv4CIDR範圍。
- 為不與重疊CIDR的用戶端 IP 位址識別適當的範圍VPCCIDR。
- 檢閱中用戶VPN端端點的規則和限制使用規則和最佳做法 AWS Client VPN。

> **Note**
>
> 在這個案例中，不支援使用 Active Directory 群組或SAML以網路為基礎的 IdP 群組的授權規則。

實作此組態

1. 在相同的區域中建立用戶VPN端端點VPC。若要執行此作業，請執行建立 AWS Client VPN 端點中所述的步驟。
2. 將您先前識別的子網路與用戶VPN端端點建立關聯。若要這麼做，請執行中所述的步驟，將目標網路與 AWS Client VPN 端點建立關聯然後選取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。對於路由目的地，請輸入用戶端CIDR範圍，然後指定做為目標VPC子網路 ID `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。對於要啟用的目標網路，請輸入的IPv4CIDR範圍VPC。

5. 新增授權規則，讓用戶端可存取用戶端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。對於要啟用的目標網路，請輸入用戶端CIDR範圍。

使用用戶端限制存取您的網路 VPN

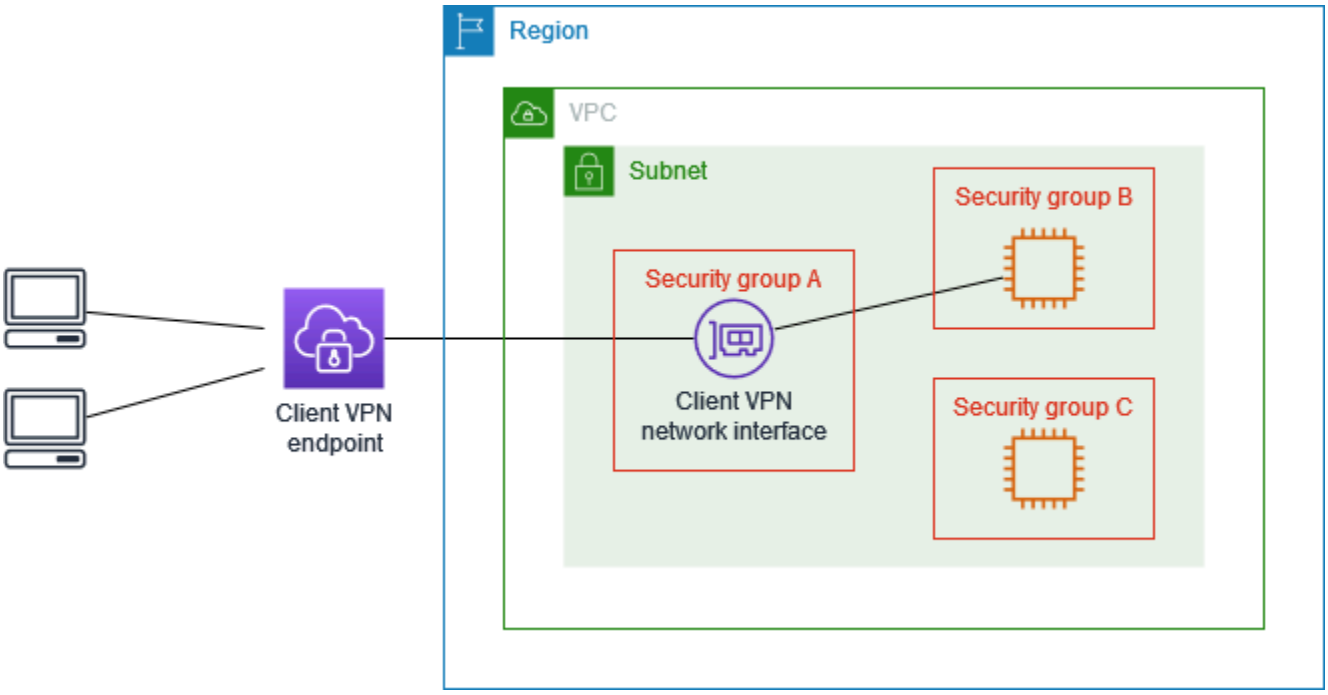
您可以將 AWS Client VPN 端點配置為限制對VPC. 對於以使用者為基礎的驗證，您也可以根據存取 Client VPN 端點的使用者群組限制對網路某些部分的存取。

使用安全群組限制存取

您可以新增或移除參照已套用至目標網路關聯 (Client VPN 安全性群組) 之安全性群組規則的安全性群組規則，來授與或拒絕對您VPC的特定資源的存取。此組態闡明VPC使用客戶端訪問 VPN 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 安全性群組之流量的規則。

在下圖中，安全性群組 A 是用戶端VPN安全性群組、安全性群組 B 與EC2執行個體相關聯，而安全性群組 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。



在開始之前，請檢查用戶端VPN安全性群組是否與VPC. 如果您新增或移除參照 Client VPN 安全性群組的規則，您也可能會授與或拒絕其他相關資源的存取權。為了防止這種情況發生，請使用專門為與 Client VPN 端點搭配使用而建立的安全性群組。

建立安全群組規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
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 [來源] 中，選擇 [自訂]，然後輸入或選擇用戶端VPN安全性群組的識別碼。
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。如果有規則允許來自 Client VPN 安全性群組的流量，請將其刪除。

檢查安全群組規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
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「來源」是用戶端VPN安全性群組的規則，請選擇 「編輯規則」，然後為該規則選擇「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 端點設定為以使用者為基礎的驗證，您可以授與特定使用者群組存取網路特定部分的存取權。若要執行此動作，請執行下列步驟。

1. 在 AWS Directory Service 或您的 IdP 中設定使用者和群組。如需詳細資訊，請參閱下列主題：
   - 客戶端中的活動目錄驗證 VPN
   - SAML以聯合認證為基礎的需求和考量

2. 為 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 端點設定為相互驗證，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。如果要讓特定的使用者群組存取網路的特定部分，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。如需詳細資訊，請參閱中的相互認證 AWS Client VPN。
2. 建立用戶端VPN端點。如需詳細資訊，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，您可以建立授與整個網路存取權的授權規則。如需詳細資訊，請參閱新增授權規則。

用戶端驗證 AWS Client VPN

用戶端驗證是在進入 AWS 雲端的第一個點實作。它是用來判斷是否允許用戶端連線到用戶端VPN端點。如果驗證成功，用戶端會連線到 Client VPN 端點並建立VPN工作階段。如果驗證失敗，則會拒絕連線，且用戶端無法建立工作VPN階段。

用戶端VPN提供下列類型的用戶端驗證：

- 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以使用者為基礎) (以使用者為基礎)

您可以單獨使用上述方法之一，也可以將相互驗證與以使用者為基礎的方法結合使用，如下所示：

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

> **Important**
>
> 若要建立 Client VPN 端點，您必須在中佈建伺服器憑證 AWS Certificate Manager，而不論您使用的驗證類型為何。如需建立和佈建伺服器憑證的詳細資訊，請參閱中的相互認證 AWS Client VPN中的步驟。

客戶端中的活動目錄驗證 VPN

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

用戶端VPN支援多重要素驗證 (MFA)，當它為 AWS 受管理的 Microsoft AD 或 AD Connector 啟用。如果MFA已啟動，用戶端必須在連線到 Client VPN 端點時輸入使用者名稱、密MFA碼和代碼。如需啟用的詳細資訊MFA，請參閱AWS Directory Service 《管理指南》中的 < 啟用 AWS 受管理 Microsoft AD 的多重要素驗證 > 和 < 啟用 AD Connector 的多重要素驗證 >。

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。

中的相互認證 AWS Client VPN

透過相互驗證，Client VPN 會使用憑證在用戶端與伺服器之間執行驗證。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 端點時，伺服器會使用用戶端憑證來驗證用戶VPN端。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)，並在建立用戶VPN端端點時指定憑證。當您將伺服器憑證上傳至時ACM，您也會指定憑證授權單位 (CA)。只有當用戶端憑證的 CA 與伺服器憑證的 CA 不同ACM時，您才需要將用戶端憑證上傳至。若要取得有關的更多資訊ACM，請參閱AWS Certificate Manager 使用者指南。

您可以為每個要連線到 Client 端點的用戶端建立個別的用戶VPN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。在此情況下，當您建立 Client VPN 端點時，您可以指定用戶端憑證ARN的伺服器憑證，前提是用戶端憑證已由與伺服器憑證相同的 CA 發行。

> **Note**
>
> 用戶VPN端端點僅支援 1024 位元和 2048 位元金RSA鑰大小。此外，用戶端憑證必須在「主旨」欄位中具有 CN 屬性。
> 當與用戶端VPN服務搭配使用的憑證更新時，無論是透過ACM自動循環、手動匯入新憑證，還是將中繼資料更新至 IAM Identity Center，用戶端VPN服務都會使用較新的憑證自動更新用戶VPN端端點。此自動化程序最多可能需要 24 小時。

任務

- 啟用相互驗證 AWS Client VPN
- 更新您的伺服器憑證 AWS Client VPN

啟用相互驗證 AWS Client VPN

您可以在「用戶端 MacOS VPN 中啟用相互驗證。

Linux/macOS

下列程序使用 Open easy VPN rsa 來產生伺服器和用戶端憑證和金鑰，然後將伺服器憑證和金鑰上傳至。ACM如需詳細資訊，請參閱 Easy-RSA 3 快速入門導覽課程README。

要生成服務器和客戶端證書和密鑰並將其上傳到 ACM

1. 克隆打開易於 VPN rsa 回購到您的本地計算機並導航到該`easy-rsa/easyrsa3`文件夾。

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

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

2. 初始化新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。請務必將它們上傳到您打算建立用戶VPN端端點的相同區域。下列命令使用 AWS CLI 上傳憑證。若要改用ACM主控台上傳憑證，請參閱使用AWS Certificate Manager 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到ACM。如果伺服器和用戶端憑證是由相同的憑證授權單位 (CA) 發行的，您可以在建立 Client 端點時同時ARN針對伺服器和用戶VPN端使用伺服器憑證。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，並使用它來產生伺服器和用戶端憑證和金鑰。

生成服務器和客戶端證書和密鑰並將其上傳到 ACM

1. 開啟簡易RSA版本頁面，並下載適用於您 Windows 版本的ZIP檔案並將其解壓縮。
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簡易 RSA 3 殼層。

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

4. 初始化新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. 退出簡易 RSA 3 外殼。

```
# 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。請務必將它們上傳到您打算建立用戶VPN端端點的相同區域。下列命令使用 AWS CLI 來上傳憑證。若要改用ACM主控台上傳憑證，請參閱使用AWS Certificate Manager 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到ACM。如果伺服器和用戶端憑證是由相同的憑證授權單位 (CA) 發行的，您可以在建立 Client 端點時同時ARN針對伺服器和用戶VPN端使用伺服器憑證。在上述步驟中，已使用相同的 CA 來建立這兩個憑證。然而，系統為了完整性，會包含上傳用戶端憑證的步驟。

更新您的伺服器憑證 AWS Client VPN

您可以更新並重新匯入已過期的 Client VPN 伺服器憑證。根據您使用的 Open VPN Easy-rsa 版本，程序會有所不同。有關更多詳細信息，請參閱 Easy-RSA 3 證書更新和撤銷文檔。

若要更新您的伺服器憑證

1. 執行下列其中一項作業：
   - 簡易RSA版本 3.1.x 中
     - 執行憑證更新命令。

       ```
       $ ./easyrsa renew server nopass
       ```
   - 簡單的-RSA 版本 3.2.x
     a. 運行過期命令。

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

b. 簽署新憑證。

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

2. 建立自訂資料夾，將新檔案複製到該資料夾中，然後導覽至該資料夾。

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

3. 將新檔案匯入到ACM。請務必將它們匯入到與用戶VPN端端點相同的區域。

```
$ 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
```

用戶端中的單一登入 — SAML 以 2.0 為基礎的同盟驗證 VPN

AWS Client VPN 針對用戶VPN端端點支援與安全宣告標記語言 2.0 (SAML2.0) 的身分識別聯合。您可以使用支援 SAML 2.0 的身分識別提供者 (IdPs) 來建立集中式使用者身分識別。然後，您可以將用戶VPN端端點設定為使用SAML基礎的聯合驗證，並將其與 IdP 建立關聯。然後，使用者使用其集中式認證連線到 Client VPN 端點。

主題

啟SAML用 AWS Client VPN

若要讓您的SAML基礎 IdP 與用戶VPN端端點搭配使用，您必須執行下列動作。

1. 在您選擇的 IdP 中建立SAML基於應用程式以搭配使用 AWS Client VPN，或使用現有的應用程式。
2. 設定 IdP 與 建立信任關係 AWS如需資源，請參閱 SAML基於 IdP 組態資源。
3. 在 IdP 中產生並下載聯合中繼資料文件，以將您的組織描述為 IdP。

   此已簽署的XML文件可用來建立與 IdP 之間 AWS 的信任關係。
4. 在與用戶VPN端端點相同的 AWS 帳戶中建立IAMSAML身分識別提供者。

   IAMSAML身分識別提供者會使用 IdP 產生的中繼資料文件，將組織的 IdP 定義為 AWS 信任關係。如需詳細資訊，請參閱IAM使用指南中的建立IAMSAML身分識別提供者。如果您稍後在 IdP 中更新應用程式設定，請產生新的中繼資料文件並更新您的IAMSAML身分識別提供者。

   > **Note**
   > 您不需要建立IAM角色即可使用IAMSAML身分識別提供者。

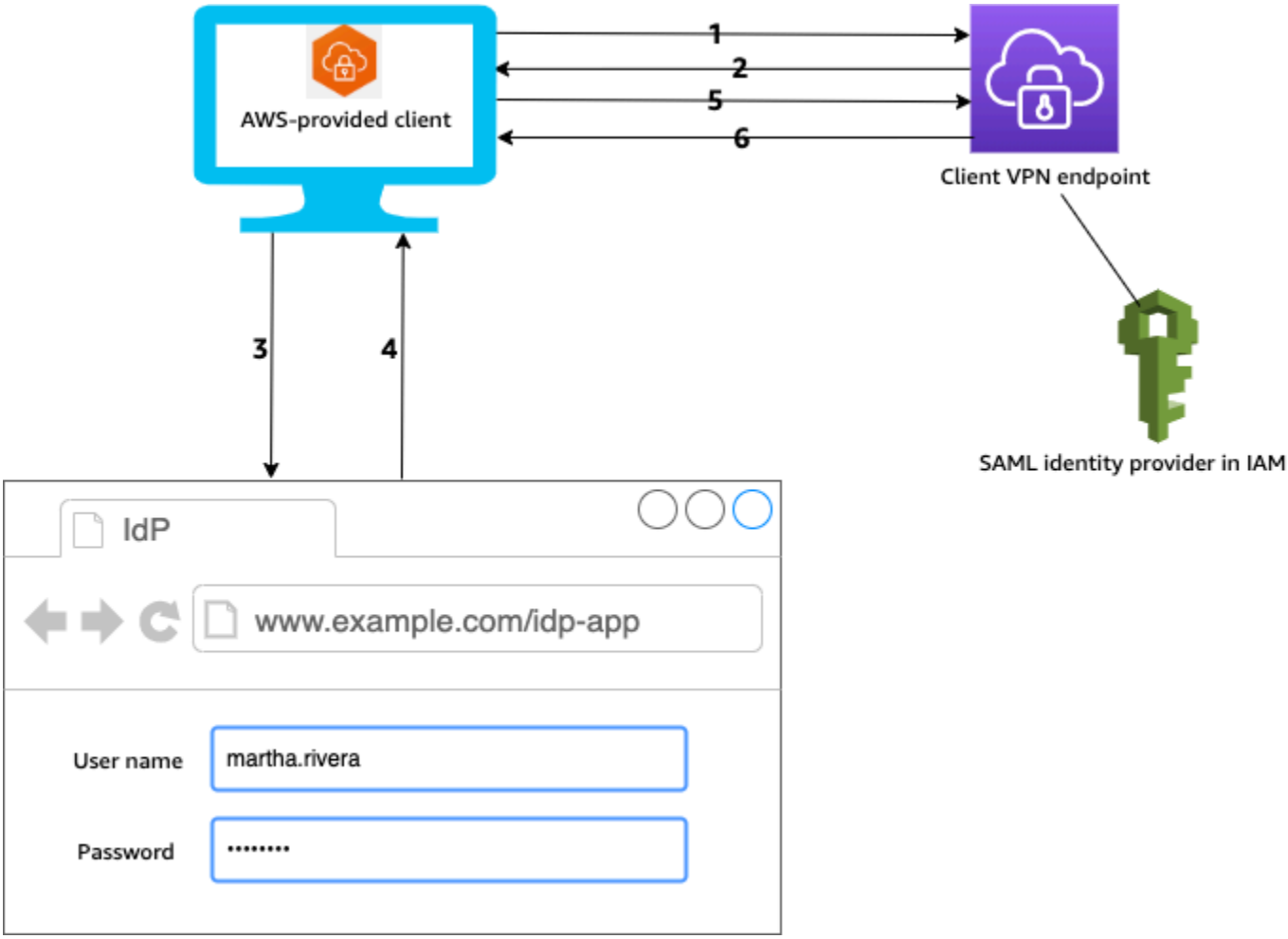
5. 建立用戶端VPN端點。

   指定同盟驗證作為驗證類型，然後指定您建立的IAMSAML身分識別提供者。如需詳細資訊，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。指示您的使用者下載所AWS 提供的用戶端的最新版本，並使用它載入組態檔案並連線到 Client VPN 端點。

   或者，如果您為 Client VPN 端點啟用了自助入口網站，請指示使用者前往自助入口網站以取得設定檔和 AWS 提供的用戶端。如需詳細資訊，請參閱AWS Client VPN 存取自助入口網站。

身分驗證工作流程

下圖提供使用聯合驗證之用SAML戶VPN端端點的驗證工作流程概觀。建立並設定用戶VPN端端點時，請指定IAMSAML身分識別提供者。



1. 使用者會在其裝置上開啟 AWS 所提供的用戶端，並啟動與 Client VPN 端點的連線。
2. 用戶端VPN端點會根據IAMSAML身分識別提供者中提供的資訊，將 IdP URL 和驗證要求傳回給用戶端。
3. AWS 提供的客戶端在用戶的設備上打開一個新的瀏覽器窗口。瀏覽器向 IdP 發出請求並顯示登入頁面。
4. 使用者在登入頁面上輸入其認證，IdP 會將已簽署的SAML宣告傳回給用戶端。
5. AWS 提供的客戶端將SAML斷言發送到客戶VPN端端點。
6. 用戶端VPN端點會驗證宣告，並允許或拒絕使用者存取。

SAML以聯合認證為基礎的需求和考量

以下是以聯合認證為SAML基礎的需求和考量事項。

- 如需在 IdP 中設定使用者和群組的SAML配額和規則，請參閱使用者和群組配額。

- SAML斷言和SAML文件必須簽署。
- AWS Client VPN 僅支援SAML宣告中的 "" NotBefore 和 NotOnOrAfter "和" 條件。AudienceRestriction
- 支援的SAML回應大小上限為 128 KB。
- AWS Client VPN 不提供已簽署的驗證要求。
- SAML不支援單一登出。使用者可以從 AWS 提供的用戶端中斷連線來登出，或者您也可以終止連線。
- 用戶端VPN端點僅支援單一 IdP。
- 在您的 IdP 中啟用多因素驗證 (MFA) 時，支援該驗證 ()。
- 使用者必須使用 AWS 提供的用戶端連線至用戶端VPN端點。您必須使用版本 1.2.0 或更新的版本。如需詳細資訊，請參閱使用AWS 提供的用戶端進行 Connect。
- 以下瀏覽器支援 IdP 身分驗證：Apple Safari，Google Chrome，Microsoft Edge 和 Mozilla Firefox。
- AWS 提供的用戶端會在使用者裝置上保留TCP連接埠 35001 以供SAML回應。
- 如果IAMSAML身分識別提供者的中繼資料文件更新為不正確或惡意URL，這可能會對使用者造成驗證問題，或導致網路釣魚攻擊。因此，建議您使用 AWS CloudTrail 來監視對IAMSAML身分識別提供者進行的更新。如需詳細資訊，請參閱IAM使用者指南 AWS CloudTrail中的記錄IAM和 AWS STS 通話。
- AWS Client VPN 透過HTTP重新導向繫結傳送 AuthN 要求至 IdP。因此，IdP 應該支援HTTP重新導向繫結，並且應該出現在 IdP 的中繼資料文件中。
- 對於SAML斷言，您必須使用`NameID`屬性的電子郵件地址格式。

SAML基於 IdP 組態資源

下表列出了我們 IdPs 已測試與搭配使用的SAML基礎 AWS Client VPN，以及可協助您設定 IdP 的資源。

IdP	資源
Okta	驗證 AWS Client VPN 使用者 SAML
Microsoft Azure Active Directory	如需詳細資訊，請參閱 Microsoft 文件網站VPN上的教學課程：Azure 作用中目錄單一登入 (SSO) 與 AWS 用戶端整合。

IdP	資源
JumpCloud	單次登入 (SSO) AWS Client VPN
AWS IAM Identity Center	使用IAM身分識別中心 AWS Client VPN 進行驗證和授權

建立應用程式的服務提供者資訊

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

- 斷言消費者服務（ACS）URL：`http://127.0.0.1:35001`
- 觀眾URI：`urn:amazon:webservices:clientvpn`

IdP 的SAML回應中必須包含至少一個屬性。範例屬性如下。

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

> **Note**
>
> 該`memberOf`屬性是使用活動目錄或 SAML IdP 基於組的授權規則所必需的。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

如果您為用戶VPN端端點啟用自助入口網站，則使用者會使用其SAML基於 IdP 認證的入口網站登入入口網站。

如果您的 IdP 支持多個斷言消費者服務（ACS）URLs，請將以下內容添加ACSURL到您的應用程序中。

```
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ACSURL改用下列指令。如果您使用相同的應用IDP程式來驗證標準和 GovCloud 區域，您可以同時新增這兩個應用程式URLs。

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

如果您的 IdP 不支援多個 ACSURLs，請執行下列動作：

1. 在 IdP 中建立其他SAML基於應用程式，並指定以下ACSURL內容。

   ```
   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. 在與用戶VPN端端點相同的 AWS 帳戶中建立IAMSAML身分識別提供者。如需詳細資訊，請參閱IAM使用指南中的建立IAMSAML身分識別提供者。

   > **Note**
   >
   > 除了為主應用程式建立的IAMSAML身分識別提供者之外，您還要建立此身分識別提供者。

4. 建立用戶端VPN端點，並指定您建立的兩個IAMSAML身分識別提供者。

用戶端授權 AWS Client VPN

客戶端VPN支持兩種類型的客戶端授權：安全組和基於網絡的授權（使用授權規則）。

安全群組

建立用戶VPN端端點時，您可以從特定的安全群組指定VPC要套用到用戶端VPN端點。當您將子網路與 Client VPN 端點建立關聯時，我們會自動套用VPC的預設安全性群組。您可以在建立用戶VPN端端點之後變更安全群組。如需詳細資訊，請參閱將安全群組套用至中的目標網路 AWS Client VPN。安全群組與用戶端VPN網路介面相關聯。

您可以在中啟VPN用用戶端使用者存取您的應用程式，方法是將規則新增至應用程式的安全性群組，以允許來自已套用至關聯的安全性群組的流量。VPC

相反地，您可以透過不指定套用至關聯的安全性群組，或移除參照 Client 端點安全性群組的規則，來限制用戶VPN端VPN使用者的存取。您需要的安全性群組規則也可能取決於您要設定的VPN存取權類型。如需詳細資訊，請參閱用戶端的案例和範例 VPN。

如需有關安全群組的詳細資訊，請參閱 Amazon VPC 使用者指南VPC中的適用於您的安全群組。

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，您可以設定允許存取的作用中目錄群組或SAML以基礎為基礎的 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 或以聯合SAML為基礎的驗證，或者想要對所有使用者開放存取權，您可以指定授與所有用戶端存取權的規則。如需詳細資訊，請參閱 AWS Client VPN 授權規則。

任務

- 建立 AWS Client VPN 端點安全性群組規則

建立 AWS Client VPN 端點安全性群組規則

建立用戶端VPN規則，允許來自用戶VPN端端點安全性群組的流量。

新增允許來自用戶VPN端端點安全性群組之流量的規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
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. 針對類型，選擇所有流量。或者，您也可以限制對特定類型流量的存取，例如SSH。

   針對來源，指定與用戶VPN端端點之目標網路 (子網路) 相關聯的安全性群組識別碼。
6. 選擇儲存規則。

連線授權 AWS Client VPN

您可以為用戶端端點設定用戶VPN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用戶端VPN服務驗證裝置和使用者之後執行。

要為客戶端端點配置客戶VPN端連接處理程序，請創建一個將設備，用戶和連接屬性作為輸入的 AWS Lambda 函數，並將決定返回給客戶端VPN服務以允許或拒絕新連接。您可以在用戶VPN端端點中指定 Lambda 函數。當裝置連線到您的用戶端VPN端點時，用戶端VPN服務會代表您叫用 Lambda 函數。只有 Lambda 函數授權的連線才能連線到用戶端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 函數必須與用戶VPN端端點位於相同的 AWS 區域，且 AWS 帳戶必須相同。
- Lambda 函數會在 30 秒後逾時。此值無法變更。
- 會以同步方式呼叫 Lambda 函數。在驗證設備和使用者身分後、評估授權規則前呼叫。
- 如果針對新連線叫用 Lambda 函數，且用戶端VPN服務未從函數取得預期的回應，則用戶端VPN服務會拒絕連線要求。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，與用戶VPN端端點的現有連線不會受到影響。您可以終止現有的連線，然後指示用戶端建立新的連線。如需詳細資訊，請參閱終止用 AWS Client VPN 戶端連線。
- 如果用戶端使用 AWS 提供的用戶端連線至用戶端VPN端點，則必須為 Windows 使用 1.2.6 或更新版本，而 macOS 則必須使用 1.2.4 或更新版本。如需詳細資訊，請參閱使用 AWS 提供的用戶端連線。

Lambda 界面

Lambda 函數會從用戶端VPN服務取得裝置屬性、使用者屬性和連線屬性做為輸入。然後，它必須將決定傳回給用戶端VPN服務是否允許或拒絕連線。

請求結構描述

Lambda 函數接受一個包含以下字段作為輸入的 JSON blob。

```
{
    "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`— 用戶端與用戶端端點之間的用戶VPN端連線識別碼。
- `endpoint-id`— 用戶VPN端端點的識別碼。
- `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。對於SAML基於聯合的身份驗證，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。當用戶端連線到用戶端端點時，以及VPN用戶端執行 Windows 平台時，「開啟」用戶VPN端組態中出現`--push-peer-info`指示詞時，用戶端VPN服務會提供值。
- `public-ip` – 要連線裝置的公有 IP 地址。
- `client-openvpn-version`— 用戶端正在使用的「開啟」VPN 版本。
- `aws-client-version`— 用 AWS 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。對於SAML以聯合為基礎的驗證，這將是身分識別提供者 (IdP) 群組的清單。若要交互身分驗證，此欄位為空白。
- `schema-version` – 結構描述版本。預設值為 v3。

回應結構描述

Lambda 函數必須傳回下列欄位。

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v3"
}
```

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

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

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

您可以在相同區域中的多個用戶VPN端端點使用相同的 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狀態評估

您可以使用用戶端連線處理常式，將 Client VPN 端點與現有裝置管理解決方案整合，以評估連線裝置的狀態符合性。若要讓 Lambda 函數當做裝置授權處理常式運作，請為用戶VPN端端點使用相互驗證。為將連線到 Client 端點的每個用戶端 (裝置) 建立唯一的用戶VPN端憑證和金鑰。Lambda 函數可以使用用戶端憑證的唯一一般名稱 (從 Client VPN 服務傳遞) 來識別裝置，並從裝置管理解決方案擷取其狀態符合性狀態。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，您可以評估用戶端VPN服務傳遞至 Lambda 函數的`platform`和`platform-version`欄位。

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

啟用用戶端連線處理程式

若要啟用用戶端連線處理常式，請建立或修改用戶VPN端端點，並指定 Lambda 函數的 Amazon 資源名稱 (ARN)。如需詳細資訊，請參閱 建立 AWS Client VPN 端點 和 修改端 AWS Client VPN 點。

服務連結角色

AWS Client VPN 會在您的AWSServiceRoleForClientVPNConnections帳戶中自動建立服務連結角色。當與用戶VPN端端點建立連線時，角色具有叫用 Lambda 函數的權限。如需詳細資訊，請參閱使用服務連結角色 AWS Client VPN。

監視連線授權失敗

您可以檢視與用戶VPN端端點之連線的連線授權狀態。如需詳細資訊，請參閱檢視 AWS Client VPN 用戶端連線。

使用用戶端連線處理常式進行狀態評估時，您也可以在連線記錄檔中檢視連線到 Client VPN 端點之裝置的狀態符合性狀態。如需詳細資訊，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：

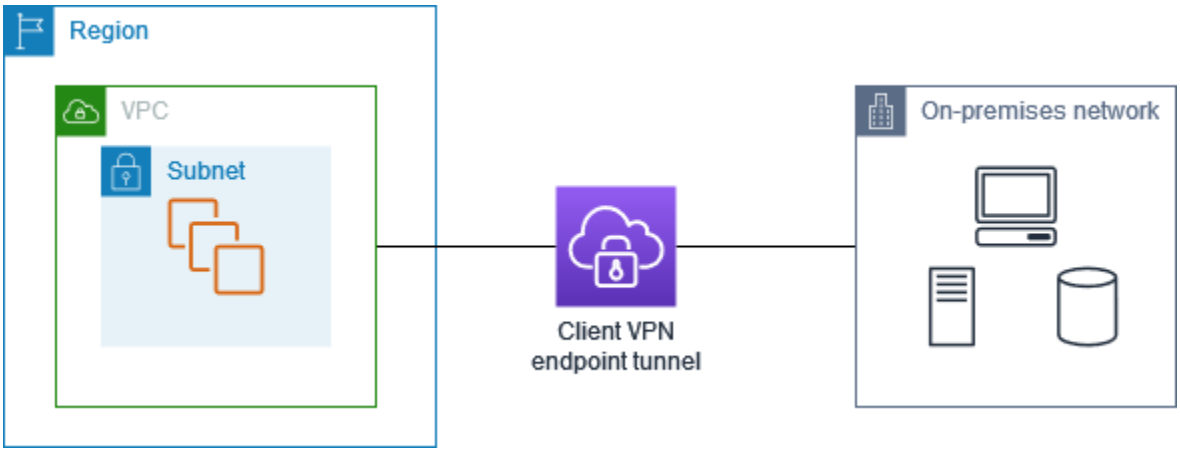
- `client-connect-failed` – 防止建立連線的 Lambda 函數。
- `client-connect-handler-timed-out` – Lambda 函數已逾時。
- `client-connect-handler-other-execution-error` – Lambda 函數發生未預期的錯誤。
- `client-connect-handler-throttled` – 經過調節的 Lambda 函數。
- `client-connect-handler-invalid-response` – 傳回無效回應的 Lambda 函數。
- `client-connect-handler-service-error`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

用戶端端點上的分割通道 VPN

根據預設，當您擁有 Client 端點時，來自用戶VPN端的所有流量都會透過 Client 通VPN道路由傳送。當您在用戶端端點上啟用分割通道時，我們會將用戶VPN端VPN端點路由資料表上的路由推送至連線至用戶VPN端端點的裝置。這可確保只有目的地到網路的流量符合來自 Client VPN 端點路由表之路由資料表的路由才會透過 Client 通VPN道路由傳送。

當您不希望所有使用者流量都透過 Client VPN 端點路由時，可以使用分割通道用戶VPN端端點。

在下列範例中，會在用戶端端VPN點上啟用分割通道。只有傳送至 VPC (`172.31.0.0/16`) 的流量才會透過用戶端通VPN道路由傳送。目的地為內部部署資源的流量不會透過 Client 通VPN道路由傳送。



分割隧道的優點

用戶VPN端端點上的分割通道具有下列優點：

- 您可以只讓 AWS 目標流量穿越通VPN道，藉此最佳化來自用戶端的流量路由。
- 您可以減少傳出流量 AWS，從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，用戶VPN端端點的路由資料表中的所有路由都會在建立VPN連線時新增至用戶端的路由資料表。此作業與預設行為不同，預設行為會使用項目覆寫用戶端的路由表格，`0.0.0.0/0`以路由傳送所有流量。VPN

> **Note**
>
> 使用分割通道模式時，不建議將`0.0.0.0/0`路由新增至 Client VPN 端點的路由資料表。

- 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用戶端端VPN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
- 修改端 AWS Client VPN 點

AWS Client VPN 端點的連線記錄

連線記錄是一項功能 AWS Client VPN ，可讓您擷取用戶VPN端端點的連線記錄檔。

連線記錄檔包含擷取連線事件相關資訊的連線記錄項目，例如用戶端 (一般使用者) 連線、嘗試連線或與 Client VPN 端點中斷連線時。您可以使用此資訊來執行鑑識、分析 Client VPN 端點的使用方式，或偵錯連線問題。

連線記錄可在所有可用的區域中 AWS Client VPN 使用。連線記錄會發佈至您帳戶中的 CloudWatch 記錄檔記錄群組。

> **Note**
>
> 不會記錄失敗的相互驗證嘗試。

連線日誌項目

連線記錄項目是索引鍵值配對的JSON格式化 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`— 建立連線的用戶VPN端端點識別碼。
- `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`— 從用戶端端點的用戶端IPv4CIDR範圍配置的用戶VPN端 IP 位址。
- `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「」和「connection-start-timeconnection-end-time」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 連線記錄。

用戶端VPN擴展考量

建立 Client VPN 端點時，請考慮您打算支援的同時VPN連線數目上限。您應該考慮當前支持的客戶數量，以及您的客戶VPN端端點是否可以根據需要擴展以滿足其他需求。

下列因素會影響用戶VPN端端點可支援的同時VPN連線數目上限：

用戶端CIDR範圍大小

建立用戶VPN端端點時，必須指定用戶端CIDR範圍，即介於 /12 和 /22 網路遮罩之間的IPv4CIDR區塊。每個與用戶VPN端端點的VPN連線都會從用戶端CIDR範圍指派一個唯一的 IP 位址。用戶端CIDR範圍中的一部分位址也會用來支援用戶VPN端端點的可用性模型，而且無法指派給用戶端。建立用戶端端點之後，就無法變更用戶VPN端CIDR範圍。

一般而言，我們建議您指定一個用戶端CIDR範圍，其中包含的 IP 位址數量是您打算在 Client VPN 端點上支援的兩倍 (因此同時連線)。

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與用戶VPN端端點的VPN工作階段。您可以將多個子網路與 Client VPN 端點建立關聯，以獲得高可用性，並啟用額外的連線容量。

以下是根據用戶VPN端端點的子網路關聯數目，支援的並行VPN連線數目。

子網路關聯	支援的連線數量
1	7,000
2	36,500

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

您無法將來自相同可用區域的多個子網路與用戶VPN端端點建立關聯。因此，子網路關聯的數目也取決於區域中可用的可用區 AWS 域數目。

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

如果您不確定 Client VPN 端點的預期VPN連線數目為何，建議您指定大小/16CIDR區塊或更大的大小。

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，請參閱使用規則和最佳做法 AWS Client VPN。

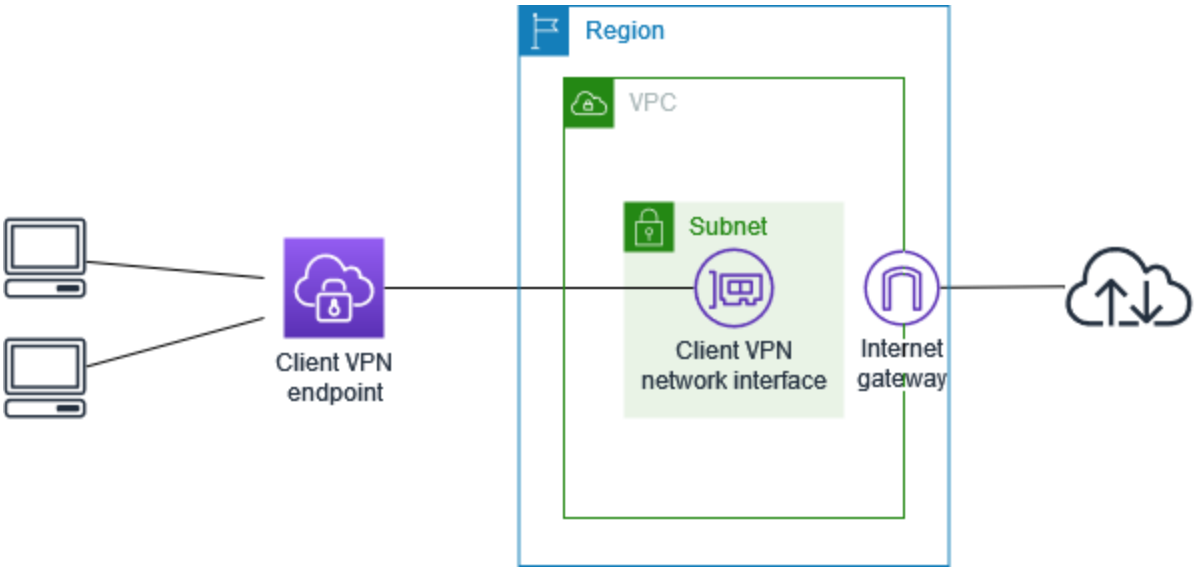
如需 Client VPN 端點配額的詳細資訊，請參閱AWS Client VPN 配額。

開始使用 AWS Client VPN

在本教學課程中，您將建立執行下列作業的 AWS Client VPN 端點：

- 為所有用戶端提供單一的存取權VPC。
- 提供所有用戶端存取網際網路。
- 使用交互身分驗證。

下圖顯示完成本教學課程之後，您VPC和 Client VPN 端點的配置。



步驟

- 必要條件
- 步驟 1：產生伺服器和用戶端憑證及金鑰
- 步驟 2：建立用戶端VPN端點
- 步驟 3：建立目標網路關聯
- 步驟 4：新增授權規則 VPC
- 步驟 5：提供對網際網路的存取權限
- 步驟 6：驗證安全群組要求
- 步驟 7：下載用戶端VPN端點設定檔
- 步驟 8：Connect 至用戶端VPN端點

必要條件

開始本教學課程之前，請確定您有：

- 使用用戶VPN端端點所需的權限。
- 將憑證導入 AWS Certificate Manager的許可。
- VPC具有至少一個子網路和一個網際網路閘道的 A。與子網路相關聯的路由表必須具有通往網際網路閘道的路由。

步驟 1：產生伺服器和用戶端憑證及金鑰

此教學課程使用交互身分驗證。使用相互驗證時，用戶端VPN會使用憑證在用戶端和用戶VPN端端點之間執行驗證。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，伺服器憑證必須匯入 AWS Certificate Manager (ACM)，並在建立用戶VPN端端點時指定。將用戶端憑證匯入至ACM是選擇性的。

如果您還沒有要用於此目的的的憑證，可以使用 Open VPN Easy-rsa 公用程式來建立這些憑證。有關使用 Open VPN Easy-rsa 實用程序生成服務器和客戶端證書和密鑰的詳細步驟，並將ACM其導入到請參閱。中的相互認證 AWS Client VPN

> **Note**
>
> 伺服器憑證必須在您建立用戶VPN端端點的相同 AWS 區域中佈建或匯入 AWS Certificate Manager (ACM)。

步驟 2：建立用戶端VPN端點

Client VPN 端點是您建立和設定以啟用和管理用戶端VPN工作階段的資源。這是所有用戶端VPN工作階段的終止點。

建立用戶VPN端端點

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶VPN端端點」，然後選擇「建立用戶端VPN端點」。
3. (選擇性) 提供用戶VPN端端點的名稱標記和說明。
4. 對於用戶端 IPv4 CIDR，請以CIDR標記指定 IP 位址範圍，以從中指派用戶端 IP 位址。

> **Note**
>
> 位址範圍不能與目標網路位址範圍、VPC位址範圍或任何將與 Client VPN 端點關聯的路由重疊。用戶端位址範圍必須至少為 /22 且不大於 /12 CIDR 區塊大小。建立用戶端端點之後，就無法變更用戶VPN端位址範圍。

5. 對於伺服器憑證 ARN，請選取您在步驟 1 中產生ARN的伺服器憑證。
6. 在 [驗證選項] 底下，選擇 [使用相互驗證]ARN，然後針對 [用ARN戶端憑證] 選取要用作用戶端憑證的憑證。

   如果伺服器和用戶端憑證由相同的憑證授權單位 (CA) 簽署，您可以選擇同時ARN為用戶端和伺服器憑證指定伺服器憑證。在這種情況下，與伺服器憑證對應的任何客戶端憑證均可用於進行身分驗證。
7. (選擇性) 指定要使用哪些DNS伺服器進行DNS解析。若要使用自訂DNS伺服器，請對於DNS伺服器 1 IP 位址和DNS伺服器 2 IP 位址，指定要使用的DNS伺服器 IP 位址。若要使用VPCDNS伺服器，請針對DNS伺服器 1 IP 位址或DNS伺服器 2 IP 位址指定 IP 位址，然後新增VPCDNS伺服器 IP 位址。

   > **Note**
   >
   > 確認用戶端可以連線到DNS伺服器。
8. 保留其餘的預設設定，然後選擇「建立用戶VPN端端點」。

建立用戶VPN端端點之後，其狀態為`pending-associate`。用戶端只能在您至少關聯一個目標網路之後建立VPN連線。

如需可為用戶VPN端端點指定之選項的詳細資訊，請參閱建立 AWS Client VPN 端點。

步驟 3：建立目標網路關聯

如果要允許用戶端建立VPN工作階段，請將目標網路與 Client VPN 端點建立關聯。目標網路是VPC.

將目標網路與用戶VPN端端點建立關聯

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。

3. 選取您在上述程序中建立的用戶VPN端端點，然後選擇 [目標網路關聯]、[關聯目標網路]。
4. 對於 VPC，選擇VPC子網路所在的位置。
5. 對於 「選擇要關聯的子網路」，請選擇要與用戶VPN端端點建立關聯的子網路。
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整個網路。VPC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用戶VPN端端點建立關聯時，會發生下列情況：

- 用戶VPN端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VPC前，無法存取中的任何資源。
- 的本機路由會自動新增至「用戶VPN端」端點路由表。VPC
- 用戶VPN端端點會自動套用VPC的預設安全性群組。

步驟 4：新增授權規則 VPC

若要讓用戶端存取VPC，必須有通往用戶VPN端端點的路由資料表VPC中的路由和授權規則。路由已經在上一個步驟中自動新增。在本教學課程中，我們想要授與所有使用者存取VPC.

若要新增授權規則 VPC

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要新增授權規則的用戶VPN端端點。選擇 Authorization rules (授權規則)，然後選擇 Add authorization rule (新增授權規則)。
4. 若要啟用存取CIDR的目標網路，請輸入您要允許存取的網路。例如，若要允許存取整個VPC，請指定的IPv4CIDR區塊VPC。
5. 在授與存取權限中，選擇允許所有使用者存取權限。
6. (選用) 對於 Description (描述)，輸入授權規則的簡短描述。
7. 選擇 Add authorization rule (新增授權規則)。

步驟 5：提供對網際網路的存取權限

您可以提供對連接到的其他網路的存取權VPC，例如 AWS 服務、對等VPCs、內部部署網路和網際網路。對於每個其他網路，您可以在用戶VPN端端點的路由表中新增路由到網路，並設定授權規則以提供用戶端存取權。

在本教程中，我們希望授予所有用戶訪問互聯網以及VPC. 您已設定存取權限VPC，因此此此步驟適用於存取網際網路。

提供對網際網路的存取

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

步驟 6：驗證安全群組要求

在此教學課程中，在步驟 2 中建立用戶VPN端端點期間未指定任何安全群組。這表示當目標網路相關聯時，的預設安全性群組會自動套用至用戶VPN端端點。VPC因此，的預設安全性群組現在VPC應該與用戶VPN端端點相關聯。

驗證下列安全群組要求

- 與您要路由傳送流量的子網路相關聯的安全性群組 (在此例中為預設VPC安全性群組) 允許輸出流量至網際網路。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。
- 您中資源的安全性群組VPC具有允許從套用至 Client VPN 端點的安全性群組存取的規則 (在此情況下為預設VPC安全性群組)。這可讓您的用戶端存取VPC.

如需詳細資訊，請參閱安全群組。

步驟 7：下載用戶端VPN端點設定檔

下一個步驟是下載並準備用戶VPN端端點組態檔案。組態檔案包含用戶VPN端端點詳細資料和建立VPN連線所需的憑證資訊。您可以將此檔案提供給需要連線到用戶VPN端端點的使用者。最終用戶使用該文件來配置他們的VPN客戶端應用程序。

下載並準備用戶VPN端端點設定檔

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您在此教學課程中建立的用戶VPN端端點，然後選擇「下載用戶端組態」。
4. 找出步驟 1 中產生的用戶端憑證和金鑰。客戶端證書和密鑰可以在克隆的 Open VPN Easy-rsa 存儲庫中的以下位置找到：
   - 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. 使用偏好的文字編輯器開啟用戶VPN端端點設定檔案。將 `<cert></cert>` 和 `<key></key>` 標籤新增至檔案中。將用户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. 儲存並關閉用戶端VPN端點設定檔。
7. 將用戶VPN端端點設定檔分發給您的使用者。

如需有關用戶VPN端端點設定檔的詳細資訊，請參閱AWS Client VPN 端點組態檔案匯出。

步驟 8：Connect 至用戶端VPN端點

您可以使用 AWS 提供的用戶VPN端或其他開放式用戶端應用程VPN式以及您剛建立的組態檔案來連線到 Client 端點。如需詳細資訊，請參閱《AWS Client VPN 使用者指南》。

使用 AWS Client VPN

下列主題說明使用用戶端所需的主要管理工作VPN：

- 存取自助入口網站 — 設定對用戶端自VPN助入口網站的存取權，以便用戶端可以自行下載 Client VPN 端點組態檔案。如需存取自助入口網站的相關資訊，請參閱the section called “自助式入口網站”。
- 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 端VPN點的存取權。如需有關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 — 檢視或終止用戶端與用戶端端點的用戶VPN端連線。如需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，在用戶端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。如需有關登入橫幅的資訊，請參閱the section called “客戶登錄橫幅”。
- 用戶端VPN端點 — 將用戶端VPN端點設定為管理和控制所有VPN工作階段。如需有關設定端點的資訊，請參閱the section called “端點”。
- 連線記錄檔 — 啟動新用戶端或現有用戶VPN端端點的連線記錄，以開始擷取連線記錄檔。如需有關連線記錄的資訊，請參閱the section called “連線日誌”。
- 用戶端組態檔案匯出 — 設定用戶端用VPN戶端建立VPN連線所需的用戶端組態檔案。設定檔案後，請下載 (匯出) 檔案，以便散佈至用戶端。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 — 設定每個 Client VPN 路由的授權規則，以指定哪些用戶端可以存取目的地網路。如需有關配置授權規則的資訊，請參閱 the section called “授權規則”
- 目標網路 — 將目標網路與用戶VPN端端點建立關聯，以便讓用戶端連線至該端點並建立VPN連線。如需有關目標網路的資訊，請參閱the section called “目標網路”。
- VPN工作階段持續時間上限 — 設定最長VPN工作階段持續時間的選項，以符合您的安全性和合 有關VPN工作階段持續時間上限的資訊，請參閱 the section called “VPN工作階段期間上”

AWS Client VPN 存取自助入口網站

如果您為 Client VPN 端點啟用了自助入口網站，則可以為您的客戶提供自助入口網站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 端點設定檔案，然後下載 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。
- 自助服務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。
- 您必須為 Client 端點啟用自助入口網站選項，否則用戶VPN端將無法存取入口網站。如果未啟用此選項，您可以修改 Client VPN 端點以啟用它。

啟用自助入口網站選項之後，請提供您的客戶下列其中一項URLs：

- `https://self-service.clientvpn.amazonaws.com/`

  如果用戶端使用此功能存取入口網站URL，則必須先輸入用戶端VPN端點的 ID，才能登入。
- `https://self-service.clientvpn.amazonaws.com/endpoints/`*`<endpoint-id>`*

  Replace (取代) *`<endpoint-id>`* 在前面URL帶有您的客戶VPN端點的 ID，例如，`cvpn-endpoint-0123456abcd123456`.

您也可以在describe-client-vpn-endpoints AWS CLI 命令的輸出中檢視自助入口網站的。URL或者，您也可以在 Amazon VPC 主控台「用戶VPN端端點」頁面的「詳細資料」索引標籤中找到。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將授權規則新增至用戶VPN端端點 AWS CLI。

> **Note**
>
> 客戶端在評估授權規則時VPN使用最長的前綴匹配。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的疑難排解主題疑難排解 AWS Client VPN：使用中目錄群組的授權規則未如預期般運作和路由優先順序。

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。
- 會`0.0.0.0/0`CIDR以特殊情況的方式處理。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可以將其視為「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

用戶端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。

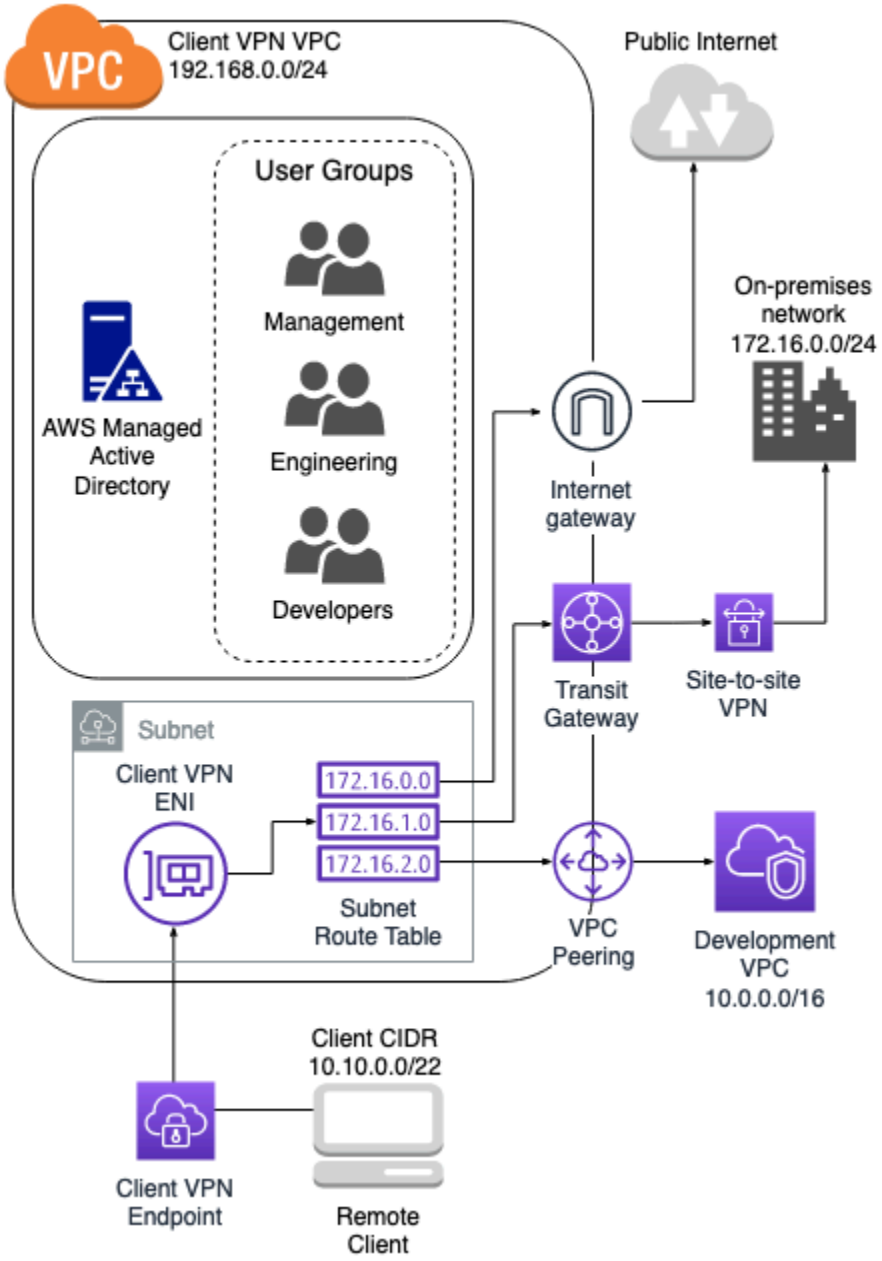
案例

- 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 “更長的 IP 前綴匹配”

- the section called “重疊 CIDR (相同群組)”
- the section called “額外 0.0.0/0 規則”
- the section called “為 192.168.0.0/24 新增一個規則”
- 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用戶端 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`。
- 用戶VPN端端點會捨棄所有其他流量。

> **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 `10.0.0/16`。

> **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。

更長的 IP 前綴匹配

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中的單一主機 VPC	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用網際網路`192.168.0.0/24`，以及開發中的單一主機 (`10.0.2.119/32`)VPC，但無法存取`172.16.0.0/24`或開發中的任何剩餘主機VPC。

> **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中的單一主機 VPC	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`。

額外 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中的單一主機 VPC	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`。

為 192.168.0.0/24 新增一個規則

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中的單一主機 VPC	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用戶端 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。

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中的單一主機 VPC	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用戶端 VPN VPC	S-xxxxx16	False	192.168.0.0/24
	N/A	True	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
提供所有群組的存取權			

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

您可以使用將授權規則新增至用戶VPN端端點 AWS Management Console。

若要使用將授權規則新增至用戶VPN端端點 AWS Management Console

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要新增授權規則的用戶VPN端端點，選擇「授權規則」，然後選擇「新增授權規則」。
4. 若要啟用存取的目的地網路，請以CIDR符號輸入您要使用者存取的網路 IP 位址 (例如，您的CIDR區塊VPC)。
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 群組的安全性識別碼 (SID)，或以基礎為SAML基礎的身分識別提供者 (IdP) 中定義之群組的 ID/ 名稱。
     - (使用中目錄) 若要取得SID，您可以使用 Microsoft PowerShell 取得ADGroup指令程式，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以聯合為基礎的驗證) 群組 ID/Name 應該符合宣告中傳回的群組屬性資訊。SAML

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)

使用指authorize-client-vpn-ingress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用戶VPN端端點的授權規則 AWS CLI。

要刪除授權規則（控制台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要新增授權規則的用戶VPN端端點，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。

若要移除授權規則 (AWS CLI)

使用指revoke-client-vpn-ingress令。

檢視 AWS Client VPN 授權規則

您可以使用主控台和檢視特定用戶VPN端端點的授權規則 AWS CLI。

檢視授權規則 (主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要檢視其授權規則的用戶VPN端端點，然後選擇授權規則。

檢視授權規則 (AWS CLI)

使用 describe-client-vpn-authorization-規則命令。

AWS Client VPN 用戶端憑證撤銷清單

用戶端用VPN戶端憑證撤銷清單可用來撤銷特定用戶端憑證之 Client VPN 端點的存取權。您可以生成撤銷列表以及導入或現有列表，或將當前列表導出一個撤銷列表文件。產生清單是使用開啟VPN軟體在 Linxu/macOS 或視窗上執行的。匯入和匯出可以使用 Amazon VPC 主控台或使用 AWS CLI.

> **Note**
>
> 如需有關產生伺服器和用戶端憑證及金鑰的詳細資訊，請參閱中的相互認證 AWS Client VPN

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之項目數的詳細資訊，請參閱用戶端VPN配額。

任務

- 產生用 AWS Client VPN 戶端憑證撤銷清單
- 匯入用 AWS Client VPN 戶端憑證撤銷清單
- 匯出用 AWS Client VPN 戶端憑證撤銷清單

產生用 AWS Client VPN 戶端憑證撤銷清單

Linux/macOS

在下列程序中，您會使用 Open easy VPN rsa 命令列公用程式產生用戶端憑證撤銷清單。

若要使用 O VPN pen easyrsa 產生用戶端憑證撤銷清單

1. 登入主控用於產生憑證之 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 Open VPN 軟體產生用戶端撤銷清單。它假設您遵循使用 Open VPN 軟體產生用戶端和伺服器憑證和金鑰的步驟。

使用簡易RSA版本 3.x.x 產生用戶端憑證撤銷清單

1. 打開命令提示符並導航到 Easy RSA -3.x.x 目錄，該目錄將取決於它在系統上的安裝位置。

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

2. 運行該EasyRSA-Start.bat文件以啟動簡單的RSA外殼。

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

3. 在簡易RSA殼層中，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
```

使用舊版簡RSA易產生用戶端憑證撤銷清單

1. 開啟命令提示字元並瀏覽至「開啟」VPN 目錄。

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

2. 執行 vars.bat 檔案。

```
C:\> vars
```

3. 撤銷用戶端憑證並產生用戶端撤銷清單。

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

匯入用 AWS Client VPN 戶端憑證撤銷清單

您必須具有要匯入的 VPN Client 用戶端憑證撤銷清單檔案。如需有關產生用戶端憑證撤銷清單的詳細資訊，請參閱產生用 AWS Client VPN 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. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要為其匯入用戶VPN端憑證撤銷清單的用戶端端點。
4. 選擇動作，然後選擇匯入用戶端憑證CRL。
5. 在憑證撤銷清單中，輸入用戶端憑證撤銷清單檔案的內容，然後選擇匯入用戶端憑證。CRL

匯入用戶端憑證撤銷清單 (AWS CLI)

使用 import-client-vpn-client-certificate-revocation-list 指令。

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

匯出用 AWS Client VPN 戶端憑證撤銷清單

您可以使用主控台和匯出用VPN戶端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. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要為其匯出用戶VPN端憑證撤銷清單的用戶端端點。
4. 選擇「動作」，選擇「匯出用戶端憑證」CRL，然後選擇「匯出用戶端 CRL

匯出用戶端憑證撤銷 (AWS CLI)

使用 export-client-vpn-client-certificate-revocation-list 指令。

AWS Client VPN 用戶端連線

AWS Client VPN 連線是由用戶端建立至特定 Client VPN 端點的作用中VPN工作階段，以及該端點過去 60 分鐘內終止的連線。當用戶端成功連線到用戶VPN端端點時，便會建立連線。終止工作階段會結束該用戶端與用戶VPN端端點的連線。

您可以檢視和終止用戶端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 位址、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。檢視和終止工作階段可以使用 Amazon VPC 主控台或. AWS CLI 如果您無法連線到端點，並且視錯誤而定，請參疑難排解閱以取得解決問題的步驟。

任務

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

檢視 AWS Client VPN 用戶端連線

您可以使VPN用 Amazon 主VPC控台或 AWS CLI.

檢視用戶端用VPN戶端連線（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要檢視其用戶VPN端連線的用戶端端點。
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。

檢視用戶端用VPN戶端連線 (AWS CLI)

使用指describe-client-vpn-connections令。

終止用 AWS Client VPN 戶端連線

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

終止用戶端用戶VPN端連線（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取用戶VPN端所連線的用戶端端點，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。

終止用戶端用VPN戶端連線 (AWS CLI)

使用指terminate-client-vpn-connections令。

AWS Client VPN 客戶登錄橫幅

AWS Client VPN 提供在建立VPN工作階段時，在提 AWS 供的用戶端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。最多可以使用 1400 UTF -8 個編碼字符。

> **Note**
>
> 啟用用戶端登入橫幅後，它只會顯示在新建立的VPN工作階段中。現有VPN工作階段不會中斷，但是當重新建立現有工作階段時，標題會顯示出來。

如需用戶端桌面應用程式的詳細資訊，請參閱AWS Client VPN 使用指南中AWS所提供用戶端的版本說明。

橫幅建立

登入橫幅最初會建立並在建立用戶VPN端端點期間啟用。如需在建立 Client 端點期間啟用用戶VPN端登入橫幅的步驟，請參閱建立 AWS Client VPN 端點。

任務

- 為現有端點設定用戶 AWS Client VPN 端登入橫幅

- 停用現有端點的用戶 AWS Client VPN 端登入橫幅
- 修改 AWS Client VPN 端點上的現有橫幅文字
- 檢視目前設定的 AWS Client VPN 登入橫幅

為現有端點設定用戶 AWS Client VPN 端登入橫幅

使用下列步驟設定現有用戶端端點的用戶VPN端登入橫幅。

在用戶端VPN端點（主控台）上啟用用戶端登入橫幅

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要修改的用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端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 (啟用用户端登入橫幅)。
6. 對于「客戶端」登錄標題文本，請輸入在 AWS 提供客戶端的標題中顯示的文本。VPN僅使用 UTF -8 個編碼字元，最多允許 1400 個字元。
7. 選擇修改用戶VPN端端點。

在用戶端端點上啟用用戶VPN端登入橫幅 (AWS CLI)

使用指modify-client-vpn-endpoint令。

停用現有端點的用戶 AWS Client VPN 端登入橫幅

使用下列步驟停用現有 Client 端點的用戶VPN端登入橫幅。

停用用戶端VPN端點（主控台）上的用戶端登入橫幅

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要修改的用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端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. 選擇修改用戶VPN端端點。

停用用戶端端點上的用戶VPN端登入橫幅 (AWS CLI)

使用指modify-client-vpn-endpoint令。

修改 AWS Client VPN 端點上的現有橫幅文字

使用下列步驟修改用戶端用戶VPN端登入橫幅上的現有文字。

修改用戶VPN端端點 (主控台) 上的現有橫幅文字

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要修改的用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端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. 對于客戶端登錄標題文本，請用新文本替換現有文本，這些文本在提供的客戶端建立時顯示在 AWS 提供的客戶VPN端的標題中。僅使用 UTF -8 個編碼字元，最多 1400 個字元。
6. 選擇修改用戶VPN端端點。

修改用戶端端點上的用戶VPN端登入橫幅 (AWS CLI)

使用指modify-client-vpn-endpoint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用戶端用VPN戶端登入橫幅。

檢視用戶VPN端端點 (主控台) 的目前登入橫幅

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要檢視的用戶VPN端端點。
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。

檢視用戶VPN端端點目前設定的登入橫幅 (AWS CLI)

使用指describe-client-vpn-endpoints令。

AWS Client VPN 端點

所有 AWS Client VPN 工作階段都會與用戶VPN端端點建立通訊。您可以管理 Client VPN 端點，以建立、修改、檢視和刪除與該端點的用戶端VPN工作階段。您可以使用 Amazon 主VPC控台或使用 AWS CLI.

建立用戶VPN端端點的需求

> **Important**
>
> 必須在佈建預期目標網路的相同 AWS 帳戶中建立用戶VPN端端點。您還需要生成服務器證書，並在需要時生成客戶端證書。如需詳細資訊，請參閱用戶端驗證 AWS Client VPN。

開始之前，請務必備妥下列項目：

- 檢閱使用規則和最佳做法 AWS Client VPN中的規則和限制。
- 產生伺服器憑證，並視需要取得用戶端憑證。如需詳細資訊，請參閱用戶端驗證 AWS Client VPN。

端點修改

建立用戶端VPN之後，您可以修改下列任何設定：

- 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
- 伺DNS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與安全性群組關聯
- 端VPN口號
- 自助式入口網站選項

- VPN工作階段持續時間上
- 啟用或停用用戶端登入橫幅文字
- 用戶端登入橫幅文字

> **Note**
>
> 對用戶VPN端端點所做的修改，包括憑證撤銷清單 (CRL) 變更，在 Client VPN 服務接受要求後最多 4 小時內會生效。
> 建立用戶端端點之後，您就無法修改用戶端IPv4CIDR範圍、驗證選項、用戶VPN端憑證或傳輸通訊協定。

當您修改用戶VPN端端點上的下列任何參數時，連線會重設：

- 伺服器憑證
- 伺DNS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
- 端VPN口號

任務

- 建立 AWS Client VPN 端點
- 檢視 AWS Client VPN 端點
- 修改端 AWS Client VPN 點
- 刪除端 AWS Client VPN 點

建立 AWS Client VPN 端點

建立用戶VPN端端點，讓您的VPN客戶能夠使用 Amazon VPC 主控台或 AWS CLI.

在建立端點之前，請先熟悉需求。如需端點需求的詳細資訊，請參閱the section called “建立用戶VPN端端點的需求”。

建立用戶VPN端端點（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶VPN端端點」，然後選擇「建立用戶端VPN端點」。
3. (選擇性) 提供用戶VPN端端點的名稱標記和說明。
4. 對於用戶端 IPv4 CIDR，請以CIDR標記指定 IP 位址範圍，以從中指派用戶端 IP 位址。例如：`10.0.0.0/22`。

   > **Note**
   > 位址範圍不能與目標網路位址範圍、VPC位址範圍或將與 Client VPN 端點關聯的任何路由重疊。用戶端位址範圍必須至少為 /22 且不大於 /12 CIDR 區塊大小。建立用戶端端點之後，就無法變更用戶VPN端位址範圍。

5. 對於伺服器憑證 ARN，ARN請指定伺服器要使用的TLS憑證。用戶端會使用伺服器憑證來驗證正在連線的用戶VPN端端點。

   > **Note**
   > 伺服器憑證必須出現在您要建立用戶VPN端端點的區域 AWS Certificate Manager (ACM) 中。憑證可以使用佈建ACM或匯入ACM。

6. 指定建立VPN連線時用來驗證用戶端的驗證方法。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。
     - 聯合驗證：選擇此選項以進行SAML以聯合認證為基礎。

       對於SAML提供者 ARN，請指定IAMSAML身分識別提供者ARN的。

       (選擇性) 若為自助服務SAML提供者 ARN，請指定ARN您為支援自助入口網站而建立的IAMSAML身分識別提供者 (如果適用)。
   - 若要使用相互憑證驗證，請選取 [使用相互驗證]ARN，然後針對 [用戶端憑證]，指定 AWS Certificate Manager (ACM) 中佈建的用戶端憑證。ARN

> **Note**
>
> 如果伺服器和用戶端憑證已由相同的憑證授權單位 (CA) 發行，您可以同時ARN針對伺服器和用戶端使用伺服器憑證。如果用戶端憑證是由不同的 CA 核發，則ARN應指定用戶端憑證。

7. (選擇性) 對於連線記錄，請指定是否使用 Amazon Lo CloudWatch gs 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)。在記CloudWatch 錄檔記錄群組名稱中，輸入要使用的記錄群組名稱。對於CloudWatch 記錄檔資料流名稱，請輸入要使用的記錄串流名稱，或將此選項保留空白，讓我們為您建立記錄資料流。
8. （選擇性）對於用戶端 Connect 線處理常式，開啟啟用用戶端連線處理常式以執行允許或拒絕新連線到 Client VPN 端點的自訂程式碼。對於用戶端 Connect 線處理常式 ARN，請指定 Lambda 函數的 Amazon 資源名稱 (ARN)，該函數包含允許或拒絕連線的邏輯。
9. (選擇性) 指定要使用哪些DNS伺服器進行DNS解析。若要使用自訂DNS伺服器，請對於DNS伺服器 1 IP 位址和DNS伺服器 2 IP 位址，指定要使用的DNS伺服器 IP 位址。若要使用VPCDNS伺服器，請針對DNS伺服器 1 IP 位址或DNS伺服器 2 IP 位址指定 IP 位址，然後新增VPCDNS伺服器 IP 位址。

> **Note**
>
> 確認用戶端可以連線到DNS伺服器。

10. (選擇性) 根據預設，用戶VPN端端點會使用UDP傳輸通訊協定。若要改用TCP傳輸通訊協定，請針對「傳輸通訊協定」選取TCP。

> **Note**
>
> UDP通常提供比TCP. 建立用戶VPN端端點之後，就無法變更傳輸通訊協定。

11. (選擇性) 若要讓端點成為分割通道用戶VPN端端點，請開啟啟用分割通道。根據預設，用戶VPN端端點上的分割通道為停用狀態。
12. (選擇性) 對於 VPCID，請選擇VPC要與用戶VPN端端點建立關聯。在 VPC「安全群組」中IDs，選擇要套用至用戶VPN端端點的一或多個安全群組。
13. (選擇性) 對於VPN連接埠，請選擇VPN連接埠號碼。預設為 443。
14. (選擇性) 若要URL為用戶端產生自助入口網站，請開啟啟用自助入口網站。

15. (選擇性) 對於工作階段逾時時數，請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)，或保留預設值為 24 小時。
16. (選用) 指定是否啟用用戶端登入橫幅文字。開啟 Enable client login banner (啟用用户端登入橫幅)。對于「客戶端」登錄標題文本，請輸入在AWS提供客戶端的標題中顯示的文本。VPNUTF僅限 -8 個編碼字元。最多 1400 個字元。
17. 選擇建立用戶VPN端端點。

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

- 用戶VPN端端點的初始狀態為`pending-associate`。只有在您關聯第一個目標網路後，用戶VPN端才能連線到用戶端端點。
- 建立授權規則，以指定哪些用戶端具有網路的存取權。
- 下載並準備用戶VPN端端點設定檔案，以便散發給您的用戶端。
- 指示您的用戶端使用 AWS 提供的用戶端或其他開放VPN式用戶端應用程式連線到 Client VPN 端點。如需詳細資訊，請參閱《AWS Client VPN 使用者指南》https://docs.aws.amazon.com/vpn/latest/clientvpn-user/。

建立用戶端VPN端點 (AWS CLI)

使用指create-client-vpn-endpoint令。

檢視 AWS Client VPN 端點

您可以使VPN用 Amazon 主VPC控台或 AWS CLI.

檢視用戶端VPN端點（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要檢視的用戶VPN端端點。
4. 使用「詳細資料」、「目標網路關聯」、「安全群組」、「授權規則」、「路由」表、「連線」和「標籤」標籤來檢視有關現有用戶VPN端

   您可以使用篩選條件來協助縮小搜尋範圍。

檢視用戶端VPN端點 (AWS CLI)

使用指describe-client-vpn-endpoints令。

修改端 AWS Client VPN 點

您可以使VPN用 Amazon 主VPC控台或 AWS CLI. 有關「客戶端」字段（您可以修改的VPN字段）的更多內容，敬請參閱the section called “端點修改”。

> **Note**
>
> 對用戶VPN端端點所做的修改，包括憑證撤銷清單 (CRL) 變更，在 Client VPN 服務接受要求後最多 4 小時內會生效。
> 建立用戶端端點之後，您就無法修改用戶端IPv4CIDR範圍、驗證選項、用戶VPN端憑證或傳輸通訊協定。

修改用戶VPN端端點（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要修改的用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端VPN端點」。
4. 在「說明」中，輸入用戶VPN端端點的簡短說明。
5. 對於伺服器憑證 ARN，ARN請指定伺服器要使用的TLS憑證。用戶端會使用伺服器憑證來驗證正在連線的用戶VPN端端點。

   > **Note**
   >
   > 伺服器憑證必須出現在您要建立用戶VPN端端點的區域 AWS Certificate Manager (ACM) 中。憑證可以使用佈建ACM或匯入ACM。

6. 指定是否使用 Amazon CloudWatch 日誌記錄有關用戶端連線的資料。對於 Enable log details on client connections (啟用用戶端連線的日誌詳細資訊)，請執行以下其中一項：

   - 若要啟用用户端連線的日誌記錄，請開啟 Enable log details on client connections (啟用用户端連線的日誌詳細資訊)。在記CloudWatch錄檔記錄群組名稱中，選取要使用的記錄群組名稱。對於CloudWatch 記錄檔資料流名稱，請選取要使用的記錄串流名稱，或將此選項保留空白，讓我們為您建立記錄資料流。
   - 若要停用用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)。

7. 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)。對於用戶端 Connect 線處理常式 ARN，請指定 Lambda 函數的 Amazon 資源名稱 (ARN)，該函數包含允許或拒絕連線的邏輯。
8. 開啟或關閉「啟用DNS伺服器」。若要使用自訂DNS伺服器，請對於DNS伺服器 1 IP 位址和DNS伺服器 2 IP 位址，指定要使用的DNS伺服器 IP 位址。若要使用VPCDNS伺服器，請針對DNS伺服器 1 IP 位址或DNS伺服器 2 IP 位址指定 IP 位址，然後新增VPCDNS伺服器 IP 位址。

> **Note**
>
> 確認用戶端可以連線到DNS伺服器。

9. 開啟或關閉 Enable split-tunnel (啟用分割通道)。依預設，VPN端點上的分割通道處於關閉狀態。
10. 對於 VPCID，請選擇VPC要與用戶VPN端端點建立關聯。在 VPC「安全群組」中IDs，選擇要套用至用戶VPN端端點的一或多個安全群組。
11. 對於VPN連接埠，請選擇VPN連接埠號碼。預設為 443。
12. 若要URL為用戶端產生自助入口網站，請開啟啟用自助入口網站。
13. 對於工作階段逾時時數，請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)，或保留預設值為 24 小時。
14. 開啟或關閉 Enable client login banner (啟用用户端登入橫幅)。如果您想使用客戶端登錄標題，那么請輸入在AWS提供客戶端的標題中顯示的VPN文本。UTF僅限 -8 個編碼字元。最多 1400 個字元。
15. 選擇修改用戶VPN端端點。

修改用戶端VPN端點 (AWS CLI)

使用指modify-client-vpn-endpoint令。

刪除端 AWS Client VPN 點

您必須先取消所有目標網路的關聯，才能刪除用戶VPN端端點。當您刪除 Client VPN 端點時，其狀態會變更為，`deleting`且用戶端無法再連線到該端點。

您可以使用主控台或刪除用戶VPN端端點 AWS CLI。

刪除用戶VPN端端點（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要刪除的用戶VPN端端點。選擇「處理行動」，「刪除用戶VPN端
4. 在確認視窗中輸入 delete (刪除)，然後選擇 Delete (刪除)。

刪除用戶端VPN端點 (AWS CLI)

使用指delete-client-vpn-endpoint令。

AWS Client VPN 連線記錄

您可以為新的或現有的用戶VPN端端點啟動連線記錄，並開始擷取連線記錄檔。連線記錄檔會顯示用戶VPN端端點的記錄事件順序。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。如果您未指定記錄資料流，Client VPN 服務會為您建立一個記錄資料流。連線記錄會記錄下列資訊：用戶端連線要求、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，您的帳戶中必須有一個 CloudWatch 記錄日誌群組。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的使用日誌群組和日誌串流。使用 CloudWatch 記錄需支付費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

用戶端VPN連線日誌可以使用 Amazon VPC 主控台或 AWS CLI.

任務

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

啟用新 AWS Client VPN 端點的連線日誌記錄

當您使用主控台或命令列建立新的用戶VPN端端點時，可以啟用連線記錄。

使用主控台啟用新用戶VPN端端點的連線記錄

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇「用戶VPN端端點」，然後選擇「建立用戶端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. 在記CloudWatch 錄檔記錄群組名稱中，選擇 CloudWatch 記錄檔記錄群組的名稱。
6. (選擇性) 對於CloudWatch 記錄記錄資料流名稱，請選擇 CloudWatch 記錄檔記錄串流的名稱。
7. 選擇建立用戶VPN端端點。

使用啟用新用戶VPN端端點的連線記錄 AWS CLI

使用指create-client-vpn-endpoint令，並指定`--connection-log-options`參數。您可以使用JSON格式指定連線記錄資訊，如下列範例所示。

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

啟用現有 AWS Client VPN 端點的連線日誌記錄

您可以使用主控台或命令列啟用現有用戶VPN端端點的連線記錄。

使用主控台啟用現有用戶VPN端端點的連線記錄

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端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. 在記CloudWatch 錄檔記錄群組名稱中，選擇 CloudWatch 記錄檔記錄群組的名稱。
6. (選擇性) 對於CloudWatch 記錄記錄資料流名稱，請選擇 CloudWatch 記錄檔記錄串流的名稱。

7. 選擇修改用戶VPN端端點。

使用啟用現有用戶VPN端端點的連線記錄 AWS CLI

使用指modify-client-vpn-endpoint令並指定`--connection-log-options`參數。您可以使用JSON格式指定連線記錄資訊，如下列範例所示。

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

檢視 AWS Client VPN 連線記錄

您可以使用記錄主控台檢視用戶端VPN連線 CloudWatch 記錄檔。

使用主控台檢視連線日誌

1. 在開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
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. 選取用戶VPN端端點的記錄資料流。

> **Note**
>
> 「時間戳記」欄會顯示連線記錄發佈至 CloudWatch 記錄的時間，而不是連線的時間。

如需有關搜尋日誌資料的詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南中的使用篩選模式搜尋日誌資料。

關閉 AWS Client VPN 連線記錄

您可以使用主控台或命令列關閉用戶VPN端端點的連線記錄。當您關閉連線記錄時，不會刪除記錄檔中 CloudWatch 現有的連線記錄。

使用主控台關閉連線日誌記錄

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端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. 選擇修改用戶VPN端端點。

若要使用關閉連線記錄 AWS CLI

使用指modify-client-vpn-endpoint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）用來建立與用戶VPN端端點之間的VPN連線的檔案。您必須下載 (匯出) 此檔案，並將其散佈給所有需要存取的用戶端VPN。或者，如果您為 Client 端點啟用了自助入口網站，用戶VPN端可以登入入口網站並自行下載設定檔。如需詳細資訊，請參閱AWS Client VPN 存取自助入口網站。

如果您的 Client VPN 端點使用相互驗證，則必須將用戶端憑證和用戶端私密金鑰新增至您下載的 .ovpn 組態檔案。新增資訊之後，用戶端可以將 .ovpn 檔案匯入開啟VPN用戶端軟體。

> **Important**
>
> 如果您未將用戶端憑證和用戶端私密金鑰資訊新增至檔案，使用相互驗證進行驗證的用戶端將無法連線到 Client VPN 端點。

依預設，開啟用VPN戶端組態中的「remote-random-hostname」選項會啟用萬用字元DNS。由於DNS已啟用萬用字元，因此用戶端不會快取端點的 IP 位址，而且您將無法 Ping 端點的DNS名稱。

如果您的用戶VPN端端點使用 Active Directory 驗證，而且在發佈用戶端設定檔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分發給用戶端。用戶端無法使用先前的組態設定檔連線到用戶端VPN端點。

任務

- 匯出用 AWS Client VPN 戶端組態檔

- 新增用 AWS Client VPN 戶端憑證和金鑰資訊以進行相互驗證

匯出用 AWS Client VPN 戶端組態檔

您可以使用主控台或匯出用VPN戶端用戶端組態 AWS CLI。

匯出用戶端組態 (主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要為其下載用戶VPN端組態的用戶端端點，然後選擇「下載用戶端組態設定」。

匯出用戶端組態 (AWS CLI)

使用 export-client-vpn-client-configuration 指令並指定輸出檔案名稱。

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

新增用 AWS Client VPN 戶端憑證和金鑰資訊以進行相互驗證

如果您的用戶VPN端端點使用相互驗證，則必須將用戶端憑證和用戶端私密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用戶VPN端端點設定檔一起散發給用戶端。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。Replace (取代) */path/* 與客戶端證書和密鑰的位置（該位置相對於連接到端點的客戶端）。

```
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。

如果您為將連線到 Client 端點的每個使用者產生個別的用戶VPN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用戶端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 路線

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的地網路。

當您將來自的子網路VPC與 Client VPN 端點產生關聯時，的路VPC由會自動新增至用戶端VPN端點的路由表。若要啟用其他網路的存取權，例如對等VPCs、內部部署網路、區域網路 (以讓用戶端彼此通訊) 或網際網路，您必須手動將路由新增至 Client VPN 端點的路由表。

> **Note**
>
> 如果要將多個子網路與 Client VPN 端點相關聯，則應確定為每個子網路建立路由，如此處所述。疑難排解 AWS Client VPN：對VPC等式、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。

在用戶端端點上使用分割通道的考量 VPN

當您在用戶端端點上使用分割通道時，用戶VPN端VPN路由資料表中的所有路由都會新增至用戶端路由資料表建立時。VPN如果您在建立之VPN後新增路由，您必須重設連線，以便將新路由傳送至用戶端。

我們建議您在修改 Client 端點路由表之前，先列出用戶VPN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

建立 Client VPN 端點路由時，您可以指定如何導向目標網路的流量。

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VPN用主控台和 AWS CLI.

建立用戶VPN端端點路由（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要新增路由的用戶VPN端端點，選擇「路由表」，然後選擇「建立路由」。
4. 對於「路由目的地」，請指定目的地網路的IPv4CIDR範圍。例如：
   - 若要為用戶VPN端端點新增路由，請輸入VPC的IPv4CIDR範圍。VPC
   - 若要新增網際網路存取的路由，請輸入 `0.0.0.0/0`

- 若要為對等加入路線VPC，請輸入對等VPC的IPv4CIDR範圍。
- 若要新增內部部署網路的路由，請輸入站 AWS 台對站台VPN連線的IPv4CIDR範圍。

5. 對於目標網路關聯的子網路 ID，請選取與用戶VPN端端點相關聯的子網路。

   或者，如果您要為本機 Client VPN 端點網路新增路由，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)。

建立用戶VPN端端點路由 (AWS CLI)

使用指create-client-vpn-route令。

檢視 AWS Client VPN 端點路由

您可以使用主控台或檢視特定用戶VPN端端點的路由 AWS CLI。

檢視用戶端VPN端點路由（主控台）

1. 在導覽窗格中，選擇「用戶端VPN端點」。
2. 選取要檢視其路由的用戶VPN端端點，然後選擇「路由」表格。

檢視用戶端VPN端點路由 (AWS CLI)

使用指describe-client-vpn-routes令。

刪除 AWS Client VPN 端點路由

您只能刪除手動新增的用戶端VPN路由。您無法刪除將子網路與 Client VPN 端點產生關聯時自動新增的路由。若要刪除自動新增的路由，您必須取消啟動其建立的子網路與 Client VPN 端點的關聯。

您可以使用主控台或從用戶VPN端端點刪除路由 AWS CLI。

刪除用戶VPN端端點路由（主控台）

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要從中刪除路由的用戶VPN端端點，然後選擇「路由」表格。
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)。

刪除用戶VPN端端點路由 (AWS CLI)

使用指delete-client-vpn-route令。

AWS Client VPN 目標網路

目標網路是VPC. AWS Client VPN 端點必須至少有一個目標網路，才能讓用戶端連線至該網路並建立VPN連線。

如需有關可設定的存取類型 (例如讓用戶端存取網際網路) 的詳細資訊，請參閱用戶端的案例和範例VPN。

用戶端VPN目標網路需求

建立目標網路時，會套用下列規則：

- 子網路必須具有至少包含 /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區塊不能與用戶端端點的用戶VPN端CIDR範圍重疊。
- 如果您將多個子網路與用戶VPN端端點建立關聯，則每個子網路都必須位於不同的可用區域中。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。
- 如果您在建立用戶VPN端端點VPC時指定了，則子網路必須位於相同的位置VPC。如果您尚未VPC與用戶VPN端端點建立關聯，則可以選擇任何子網路中的任何子網路VPC。

  所有其他子網路關聯必須來自相同的VPC。若要關聯來自其他子網路的子網路VPC，您必須先修改用戶端VPN端點，然後變更與其VPC相關聯的端點。如需詳細資訊，請參閱修改端 AWS Client VPN 點。

當您將子網路與 Client VPN 端點建立關聯時，我們會自動將佈建關聯子網路的本機路由新增至用戶端VPN端點的路由表。VPC

> **Note**
>
> 在您的目標網路建立關聯之後，當您新增或移除附加CIDRs至連結的其他網路時VPC，必須執行下列其中一項作業，以更新 Client VPN 端點路由表的本機路由：
>
> - 取消用戶VPN端端點與目標網路的關聯，然後將用戶VPN端端點與目標網路建立關聯。
> - 手動將路由新增至用戶端端點路由表，或從用戶VPN端端點路由表移除路由。

將第一個子網路與 Client VPN 端點建立關聯後，用戶端VPN端點的狀態會從變更`pending-associate`為，`available`而且用戶端也能夠建立VPN連線。

任務

- 將目標網路與 AWS Client VPN 端點建立關聯
- 將安全群組套用至中的目標網路 AWS Client VPN
- 檢視 AWS Client VPN 目標網路
- 取消目標網路與端點的關聯 AWS Client VPN

將目標網路與 AWS Client VPN 端點建立關聯

您可以使用 Amazon VPC 主控台或將一或多個目標網路 (子網路) 與用戶VPN端端點建立關聯。 AWS CLI在將目標網路與 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。

將目標網路與用戶VPN端端點 (主控台) 建立關聯

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要與目標網路建立關聯的用戶VPN端端點，選擇「目標網路關聯」，然後選擇「關聯目標網路」。
4. 對於 VPC，選擇VPC子網路所在的位置。如果您在建立 Client VPN 端點VPC時指定了，或者您有先前的子網路關聯，則它必須相同VPC。
5. 對於 「選擇要關聯的子網路」，請選擇要與用戶VPN端端點建立關聯的子網路。
6. 選擇 Associate target network (關聯目標網路)。

將目標網路與用戶VPN端端點建立關聯 (AWS CLI)

使用 associate-client-vpn-target-網絡命令。

將安全群組套用至中的目標網路 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子網路所VPC在的預設安全性群組。如需詳細資訊，請參閱安全群組。

您可以變更用戶VPN端端點的安全群組。您需要的安全性群組規則取決於您要設定的VPN存取類型。如需詳細資訊，請參閱用戶端的案例和範例 VPN。

將安全群組套用到目標網路 (主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取要套用安全群組的用戶VPN端端點。
4. 選擇 Security Groups (安全群組)，然後選擇 Apply Security Group (套用安全群組)。
5. 從「安全性群組」中選取適當的安全性群組IDs。
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 指令。

檢視 AWS Client VPN 目標網路

您可以使用主控台或檢視與用戶VPN端端點相關聯的目標 AWS CLI。

檢視目標網路 (主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取適當的用戶端VPN端點並選擇「目標網路關聯」。

使用檢視目標網路 AWS CLI

使用 describe-client-vpn-target-網路指令。

取消目標網路與端點的關聯 AWS Client VPN

取消目標網路的關聯時，會刪除手動新增至 Client VPN 端點之路由表的任何路由，以及建立目標網路關聯時自動建立的路由 (的區域路由VPC)。如果您取消所有目標網路與用戶VPN端端點的關聯，用戶端將無法再建立VPN連線。

取消目標網路與用戶VPN端端點 (主控台) 的關聯

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取與目標網路相關聯的用戶VPN端端點，然後選擇「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)。

取消目標網路與用戶VPN端端點的關聯 ()AWS CLI

使用 disassociate-client-vpn-target-網絡命令。

AWS Client VPN VPN工作階段期間上

AWS Client VPN 提供數個VPN工作階段持續時間上限的選項，也就是用戶端連線到用戶VPN端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，以符合安全性和合規性需求 依預設，VPN工作階段持續時間上限為 24 小時。

> **Note**
>
> 當工VPN作VPN階段持續時間上限值從其目前的值減少時，連線到端點時間範圍超過新設定持續時間的任何作用中工作階段都會中斷連線。將需要啟動新的工作階段。

如需用戶端桌面應用程式工作階段持續時間的詳細資訊，請參閱《AWS Client VPN 使用指南》中AWS提供用戶端的版本

設定 AWS Client VPN 端點建立期間的VPN工作階段上限

VPN工作階段的持續時間是在建立用戶VPN端端點期間設定的。如建立 AWS Client VPN 端點需建立 Client VPN 端點和設定工作階段持續時間上限的步驟，請參閱。

任務

- 檢視 AWS Client VPN 目前的最長VPN工作階段
- 修改 AWS Client VPN 工作階段持續時間上

檢視 AWS Client VPN 目前的最長VPN工作階段

使用下列步驟來檢視目前的用戶端VPN工作階段持續時間上VPN限。

檢視用戶VPN端端點 (主控台) 目前的VPN工作階段持續時間上限

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要檢視的用戶VPN端端點。
4. 請確認選取了 Details (詳細資訊) 索引標籤。
5. 檢視VPN工作階段逾時小時旁的目前階段作業持續時間上限。

檢視用戶VPN端端點目前的VPN工作階段持續時間上限 (AWS CLI)

使用指describe-client-vpn-endpoints令。

修改 AWS Client VPN 工作階段持續時間上

使用下列步驟修改現有的用戶端VPN工作階段持續時間上VPN限。

修改用戶VPN端端點（主控台）的現有VPN工作階段持續時間上限

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇「用戶端VPN端點」。
3. 選取您要修改的用戶VPN端端點，選擇「處理行動」，然後選擇「修改用戶端VPN端點」。
4. 對於工作階段逾時時數，請選擇所需的VPN工作階段持續時間上限 (小時)
5. 選擇修改用戶VPN端端點。

修改用戶VPN端端點的現有VPN工作階段持續時間上限 (AWS CLI)

使用指modify-client-vpn-endpoint令。

中的安全性 AWS Client VPN

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Client VPN，請參閱合規計劃的AWS服務範圍範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您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 中安全性的詳細資訊VPC，請參閱 Amazon VPC 使用者指南中的安全性。

本文檔可幫助您了解如何在使用客戶端時應用共同的責任模型VPN。下列主題說明如何設定 Client VPN 以符合您的安全性和合規性目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Client VPN 資源的服務。

主題

資料保護 AWS Client VPN

AWS 共同責任模型適用於 AWS 客戶中的資料保護VPN。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

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

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，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。這包括當您使用主控台、API、VPN或 AWS 服務 使用用戶端或其他用戶端時 AWS SDKs。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

傳輸中加密

AWS Client VPN 使用傳輸層安全性 (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VPC和其他網路。如需詳細資訊和範例，請參閱 用戶端的案例和範例 VPN。

限制對網路的存取

您可以將 Client VPN 端點設定為限制對VPC. 對於以使用者為基礎的驗證，您也可以根據存取 Client VPN 端點的使用者群組來限制對網路某些部分的存取。如需詳細資訊，請參閱使用用戶端限制存取您的網路 VPN。

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。它是用來判斷是否允許用戶端連線到用戶端VPN端點。如果驗證成功，用戶端會連線到 Client VPN 端點並建立VPN工作階段。如果驗證失敗，則會拒絕連線，且用戶端無法建立工作VPN階段。

用戶端VPN提供下列類型的用戶端驗證：

- 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以使用者為基礎) (以使用者為基礎)

的身分識別與存取管理 AWS Client VPN

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (具有權限) 使用 Client VPN 資源。IAM是一種您 AWS 服務 可以使用，無需額外費用。

主題

物件

根據您在客戶端中執行的工作，使用方式 AWS Identity and Access Management （IAM）會有所不同VPN。

服務使用者 — 如果您使用 Client VPN 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多用戶端VPN功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在用戶端中存取某個功能VPN，請參閱疑難排解 AWS Client VPN 身分和存取。

服務管理員 — 如果您負責公司的客戶端VPN資源，則可能擁有對客戶端的完整訪問權限VPN。決定您的服務使用者應該存取哪些 Client VPN 功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM與客戶搭配使用VPN，請參閱如何 AWS Client VPN 使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理 Client 存取權的詳細資訊VPN。若要檢視可在中使用的以用戶端VPN身分識別為基礎的原則範例IAM，請參閱。AWS Client VPN的身分型政策範例

使用身分驗證

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

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

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

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

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

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

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

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資

源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

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

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

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

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

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

如何 AWS Client VPN 使用 IAM

在您用IAM來管理用戶端的存取權之前VPN，請先瞭解哪些IAM功能可搭配 Client 使用VPN。

IAM您可以搭配用 AWS 戶端使用的功能 VPN

IAM特徵	用戶端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

IAM特徵	用戶端VPN支援
ACLs	否
ABAC(策略中的標籤)	否
暫時性憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要取得用戶端VPN和其他 AWS 服務如何搭配大部分IAM功能運作的高階檢視，請參閱IAM使用者指南IAM中的使用AWS 服務。

用戶端的身分識別原則 VPN

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

用戶端的身分識別原則範例 VPN

若要檢視以用戶端VPN身分識別為基礎的原則範例，請參閱。AWS Client VPN的身分型政策範例

用戶端內的資源型政策 VPN

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定

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

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

用戶端政策處理行動 VPN

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看用戶端VPN動作清單，請參閱服務授權參考VPN中由 AWS Client 定義的處理行動。

VPN用戶端中的政策處理行動會在處理行動前使用下列前置詞

```
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"
         ]
```

若要檢視以用戶端VPN身分識別為基礎的原則範例，請參閱。AWS Client VPN的身分型政策範例

用戶端的政策資源 VPN

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

若要查看 Client VPN 資源類型及其清單ARNs，請參閱服務授權參考VPN中由 AWS Client 定義的資源。若要瞭解您可以針對每個資源指定ARN哪些動作，請參閱AWS 用戶端定義的動作VPN。

若要檢視以用戶端VPN身分識別為基礎的原則範例，請參閱。AWS Client VPN的身分型政策範例

用戶端的政策條件金鑰 VPN

支援服務特定政策條件金鑰：是

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

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

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

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看用戶端VPN條件金鑰清單，請參閱服務授權參考VPN中AWS 用戶端的條件金鑰。若要瞭解可以使用條件索引鍵的動作和資源，請參閱用AWS 戶端定義的動作VPN。

若要檢視以用戶端VPN身分識別為基礎的原則範例，請參閱。AWS Client VPN的身分型政策範例

ACLs在用戶端 VPN

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與客戶 VPN

支援 ABAC (策略中的標籤): 否

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

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。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

透過用戶端使用臨時認證 VPN

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

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

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

用戶端的跨服務主體權限 VPN

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

用戶端的服務角色 VPN

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
> 變更服務角色的權限可能會中斷用戶端VPN功能。只有當用戶端VPN提供指引時，才編輯服務角色。

用戶端的服務連結角色 VPN

支援服務連結角色：是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇 Yes (是) 連結，以檢視該服務的服務連結角色文件。

AWS Client VPN的身分型政策範例

根據預設，使用者和角色沒有建立或修改用戶端VPN資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需有關 Client 定義的動作和資源類型的詳細資訊VPN，包括每種資源類型的格式，請參閱服務授權參考VPN中 AWS 用戶端的動作、資源和條件索引鍵。ARNs

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

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 Client VPN 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer 會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。

- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

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

```
}
```

疑難排解 AWS Client VPN 身分和存取

使用下列資訊可協助您診斷及修正使用 Client VPN 和時可能會遇到的常見問題IAM。

主題

我沒有在客戶端中執行操作的權限 VPN

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。

當使用`mateojackson`IAM者嘗試使用主控台來檢視虛構*`my-example-widget`*資源的詳細資料，但沒有虛構的`ec2:`*`GetWidget`*權限時，就會發生下列範例錯誤。

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

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

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

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行`iam:PassRole`動作的錯誤訊息，您必須更新原則，才能將角色傳遞給用戶端VPN。

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

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

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

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

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

我想允許我以外的人訪問我 AWS 帳戶 的客戶端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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解用戶端是否VPN支援這些功能，請參閱如何 AWS Client VPN 使用 IAM。
- 若要瞭解如何提供您所擁有資 AWS 帳戶 源的存取權，請參閱《IAM使用指南》中的〈提供存取權給您 AWS 帳戶 所擁有的其他IAM使用者〉。
- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過聯合身分識別提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

使用服務連結角色 AWS Client VPN

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至用戶端VPN的唯一IAM角色類型。服務連結角色由 Client 預先定義，VPN並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

主題

- 使用角色 AWS Client VPN
- 在客戶端中使用角色進行連接授權VPN;

使用角色 AWS Client VPN

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至用戶端VPN的唯一IAM角色類型。服務連結角色由 Client 預先定義，VPN並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您VPN更輕鬆地設定用戶端，因為您不需要手動新增必要的權限。用戶端會VPN定義其服務連結角色的權限，除非另有定義，否則只有 Client VPN 可以擔任其角色。定義的權限包括信任原則和權限原則，而且該權限原則無法附加至任何其他IAM實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 Client VPN 資源，因為您無法意外移除存取資源的權限。

如需支援服務連結角色之其他服務的相關資訊，請參閱使用的AWS 服務，IAM並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

用戶端的服務連結角色權限 VPN

VPN用戶端使用名為的服務連結角色 AWSServiceRoleForClientVPN— 允許用戶端VPN建立和管理與您的VPN連線相關的資源。

服AWSServiceRoleForClientVPN務連結角色會信任下列服務擔任該角色：

- `clientvpn.amazonaws.com`

名為 C 的角色權限原則lientVPNServiceRolePolicy可讓VPN用戶端對指定的資源完成下列動作：

- 動作：`Resource: "*"` 上的 `ec2:CreateNetworkInterface`
- 動作：`Resource: "*"` 上的 `ec2:CreateNetworkInterfacePermission`
- 動作：`Resource: "*"` 上的 `ec2:DescribeSecurityGroups`
- 動作：`Resource: "*"` 上的 `ec2:DescribeVpcs`
- 動作：`Resource: "*"` 上的 `ec2:DescribeSubnets`
- 動作：`Resource: "*"` 上的 `ec2:DescribeInternetGateways`
- 動作：`Resource: "*"` 上的 `ec2:ModifyNetworkInterfaceAttribute`
- 動作：`Resource: "*"` 上的 `ec2:DeleteNetworkInterface`
- 動作：`Resource: "*"` 上的 `ec2:DescribeAccountAttributes`

- 動作：Resource: "*" 上的 ds:AuthorizeApplication
- 動作：Resource: "*" 上的 ds:DescribeDirectories
- 動作：Resource: "*" 上的 ds:GetDirectoryLimits
- 動作：Resource: "*" 上的 ds:UnauthorizeApplication
- 動作：Resource: "*" 上的 logs:DescribeLogStreams
- 動作：Resource: "*" 上的 logs:CreateLogStream
- 動作：Resource: "*" 上的 logs:PutLogEvents
- 動作：Resource: "*" 上的 logs:DescribeLogGroups
- 動作：Resource: "*" 上的 acm:GetCertificate
- 動作：Resource: "*" 上的 acm:DescribeCertificate
- 動作：Resource: "*" 上的 iam:GetSAMLProvider
- 動作：Resource: "*" 上的 lambda:GetFunctionConfiguration

您必須設定權限，才能允許IAM實體 (例如使用者、群組或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱IAM使用指南中的服務連結角色權限。

為用戶端建立服務連結角色 VPN

您不需要手動建立一個服務連結角色。當您使用 AWS Management Console、或在帳戶中建立第一個用戶VPN端端點時 AWS CLI AWS API，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。

編輯用戶端的服務連結角色 VPN

用戶端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。但是，您可以使用編輯角色的描述IAM。如需詳細資訊，請參閱IAM使用指南中的編輯服務連結角色。

刪除用戶端的服務連結角色 VPN

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

您必須先刪除相關的用戶端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IAMCLI、或刪除服務連結角色。IAM API如需詳細資訊，請參閱IAM使用指南中的刪除服務連結角色。

用戶端VPN服務連結角色的支援區域

用戶端VPN支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

在客戶端中使用角色進行連接授權VPN;

AWS Client VPN 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至用戶端VPN的唯一IAM角色類型。服務連結角色由 Client 預先定義，VPN並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您VPN更輕鬆地設定用戶端，因為您不需要手動新增必要的權限。用戶端會VPN定義其服務連結角色的權限，除非另有定義，否則只有 Client VPN 可以擔任其角色。定義的權限包括信任原則和權限原則，而且該權限原則無法附加至任何其他IAM實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 Client VPN 資源，因為您無法意外移除存取資源的權限。

如需支援服務連結角色之其他服務的相關資訊，請參閱使用的AWS 服務，IAM並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

用戶端的服務連結角色權限 VPN

VPN用戶端會針對用戶端連線使用名為 AWSServiceRoleForClientVPNConnections— 服務連結角色的服務VPN連結角色。

服 AWSServiceRoleForClientVPNConnections 務連結角色會信任下列服務擔任該角色：

- `clientvpn-connections.amazonaws.com`

名為 C 的角色權限原則lientVPNServiceConnectionsRolePolicy 可讓VPN用戶端對指定的資源完成下列動作：

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

您必須設定權限，才能允許IAM實體 (例如使用者、群組或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱IAM使用指南中的服務連結角色權限。

為用戶端建立服務連結角色 VPN

您不需要手動建立一個服務連結角色。當您使用 AWS Management Console、或在帳戶中建立第一個用戶VPN端端點時 AWS CLI AWS API，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。

編輯用戶端的服務連結角色 VPN

用戶端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。但是，您可以使用編輯角色的描述IAM。如需詳細資訊，請參閱IAM使用指南中的編輯服務連結角色。

刪除用戶端的服務連結角色 VPN

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

您必須先刪除相關的用戶端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IAMCLI、或刪除服務連結角色。IAM API如需詳細資訊，請參閱IAM使用指南中的刪除服務連結角色。

用戶端VPN服務連結角色的支援區域

用戶端VPN支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

韌性在 AWS Client VPN

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構之外，還 AWS Client VPN 提供可協助支援資料復原和備份需求的功能。

提供高可用性的多個目標網路

您可以將目標網路與用戶VPN端端點建立關聯，以便讓用戶端建立VPN工作階段。目標網路是您的VPC. 與用戶VPN端端點關聯的每個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用戶VPN端端點建立關聯，以取得高可用性。

基礎結構安全 AWS Client VPN

作為託管服務， AWS 用戶端VPN受到 AWS 全球網路安全性的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

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

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

安全性最佳做法 AWS Client VPN

AWS Client VPN 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。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AWS Client VPN 授權規則。

Security groups (安全群組)

使用安全性群組來控制使用者可以在VPC. 如需詳細資訊，請參閱安全群組。

用戶端憑證撤銷清單

使用用戶端憑證撤銷清單來撤銷對特定用戶端憑證之 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AWS Client VPN 用戶端憑證撤銷清單。

監控工具

使用監控工具追蹤用戶VPN端端點的可用性和效能。如需詳細資訊，請參閱監控 AWS Client VPN。

身分與存取管理

管理用戶端資VPN源的存取，並APIsIAM針對您的使用IAM者和IAM角色使用原則。如需詳細資訊，請參閱的身分識別與存取管理 AWS Client VPN。

IPv6的注意事項 AWS Client VPN

目前用戶端VPN服務不支援透過IPv6通VPN道路由傳送流量。但是，在某些情況下，應將IPv6交通路由到VPN隧道，以防止IPv6洩漏。IPv6當啟用IPv4並且IPv6連接到時，可能會發生洩漏VPN，但VPN不會將IPv6流量路由到其隧道。在這種情況下，當連接到IPv6已啟用的目的IPv6地時，您實際上仍然與您提供的ISP. 這會洩露你的真實IPv6地址。下面的說明解釋如何將IPv6交通路由到VPN隧道。

以下IPv6相關指令應該添加到客戶端VPN配置文件中，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`將本機通道裝置IPv6位址設定為，`fd15:53b6:dead::2`並將遠VPN端端點IPv6位址設定為`fd15:53b6:dead::1`。

下一個命令，`route-ipv6 2000::/4`將路由IPv6地址從`2000:0000:0000:0000:0000:0000:0000:00002fff: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，組態會將所有目前配置的IPv6流量路由至VPN連線。

驗證

您的組織可能有自己的測試。基本驗證是設置完整的隧道VPN連接，然後使用該IPv6地址將 ping6 運行到IPv6服務器。伺服器的IPv6位址應在指`route-ipv6`令所指定的範圍內。這個 ping 測試應該會失敗。但是，如果 future 將IPv6支援新增至 Client VPN 服務，這可能會變更。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

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS Client VPN 重要組成部分。您可以使用下列功能來監控用戶VPN端端點、分析流量病毒碼，以及疑難排解 Client VPN 端點的問題。

Amazon CloudWatch

即時監控您的 AWS 資源和執行 AWS 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 CloudWatch 追蹤 Amazon EC2 執行個體的CPU使用情況或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWS CloudTrail

擷取您帳戶或代表您的 AWS 帳戶發出的API呼叫和相關事件，並將日誌檔傳送到您指定的 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 位址，以及呼叫發生的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。

Amazon CloudWatch 日誌

可讓您監控對 AWS Client VPN 端點進行的連線嘗試。您可以檢視用戶端連VPN線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 記錄檔資料流來記錄連線詳細資料。如需詳細資訊，請參閱AWS Client VPN 端點的連線記錄和 Amazon CloudWatch 日誌使用者指南。

主題

Amazon CloudWatch 指標 AWS Client VPN

AWS Client VPN CloudWatch 針對您的用戶VPN端端點，將下列指標發佈到 Amazon。指標 CloudWatch 每五分鐘發佈一次到 Amazon。

指標	描述
ActiveConnectionsCount	與用戶VPN端端點的作用中連線數目。

指標	描述
	單位：計數
AuthenticationFailures	用戶VPN端端點的驗證失敗數目。 單位：計數
CrlDaysToExpiry	直到在用戶VPN端端點上設定的憑證撤銷清單 (CRL) 到期的天數。 單位：天
EgressBytes	從用戶VPN端端點傳送的位元組數目。 單位：位元組
EgressPackets	從用戶VPN端端點傳送的封包數目。 單位：計數
IngressBytes	用戶VPN端端點接收的位元組數目。 單位：位元組
IngressPackets	用戶VPN端端點接收的封包數目。 單位：計數
SelfServicePortalClientConfigurationDownloads	從自助入口網站下載用戶VPN端端點組態檔案的數目。 單位：計數

AWS Client VPN 針對您的用戶VPN端端點發佈下列狀況評估指標。

指標	描述
ClientConnectHandlerTimeouts	呼叫用戶端連線處理常式以連線至用戶端端點的逾時數目。VPN

指標	描述
	單位：計數
ClientConnectHandlerInvalidResponses	用戶端連線處理常式針對用戶VPN端端點的連線所傳回的無效回應數目。 單位：計數
ClientConnectHandlerOtherExecutionErrors	執行用戶端連線處理常式以連線至用戶VPN端端點時發生未預期的錯誤數目。 單位：計數
ClientConnectHandlerThrottlingErrors	呼叫用戶端連線處理常式以連線至用戶端端點時的節流錯誤數目。VPN 單位：計數
ClientConnectHandlerDeniedConnections	用戶端連線處理常式拒絕連線至用戶VPN端端點的連線數目。 單位：計數
ClientConnectHandlerFailedServiceErrors	執行用戶端連線處理常式以連線至用戶端端點時發生的服務VPN端錯誤數目。 單位：計數

您可以依端點篩選用戶端VPN端點的指標。

CloudWatch 可讓您擷取有關這些資料點的統計資料，做為一組排序的時間序列資料 (稱為指標)。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，如果指標超出您認為可接受的範圍，您可以建立 CloudWatch 警示來監控指定的指標並啟動動作 (例如傳送通知至電子郵件地址)。

如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

任務

- 在 Amazon 中檢視用戶VPN端端點指標 CloudWatch

在 Amazon 中檢視用戶VPN端端點指標 CloudWatch

您可以按如下方式檢視用戶端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. 在開啟 CloudWatch 主控台https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇 指標。
3. 在「所有測量結果」底下，選擇從屬端VPN測量結果
4. 若要檢視指標，請選取 by endpoint (依照端點區分) 的指標維度。

若要使用檢視量度 AWS CLI

在命令提示字元中，使用下列命令列出用戶端可用的測量結果 VPN

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

AWS CloudTrail 記錄 AWS Client VPN

AWS Client VPN 與服務整合 AWS CloudTrail，可提供用戶端中使用者、角色或服務所採取之動作記錄的 AWS 服務VPN。 CloudTrail 捕獲客戶端的所有API調用VPN作為事件。擷取的呼叫包括來自用戶端VPN主控台的呼叫，以及對用戶端VPNAPI作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail事件到 Amazon S3 儲存貯體，包括用戶端的事件VPN。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail 來判斷向 Client 發出的要求VPN、要求的 IP 位址、要求者、提出時間以及其他詳細資訊。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail 使用者指南。

用戶端VPN資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當用戶端中發生活動時VPN，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需帳戶中持續記錄事件 (包括客 AWS 戶的事件)VPN，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

所有用戶端VPN動作均由 Amazon EC2 API 參考記錄 CloudTrail 並記錄在此。例如，呼叫`CreateClientVpnEndpoint``AssociateClientVpnTargetNetwork`、和`AuthorizeClientVpnIngress`動作會在 CloudTrail 記錄檔中產生項目。

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

- 要求是使用 root 或 AWS Identity and Access Management (IAM) 使用者認證進行。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail userIdentity 元素。

瞭解用戶端VPN記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌文件不是公共API調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

有關更多信息，請參閱 Amazon EC2API參考 AWS CloudTrail中的記錄 AmazonEBS，Amazon 和 Amazon VPC API 呼叫。EC2

AWS Client VPN 配額

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

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

用戶端VPN配額

名稱	預設	可調整
每個客戶VPN端點的授權規則	50	是
各區域的用戶VPN端端點	5	是
每個用戶VPN端端點同時連線	此值取決於每個端點的子網路關聯數量。 • 一至二萬 • 2 – 36,500 • 3 – 66,500 • 4 – 96,500 • 5 – 126,000	是
每個用戶VPN端端點的並行作業 †	10	否
用戶端端點的用戶端憑證撤銷清單中的項目VPN	20,000	否
每個用戶VPN端點的路由	10	是

† 操作包含：

- 關聯或取消關聯子網路
- 建立或刪除路由

- 建立或刪除傳入和傳出規則
- 建立或刪除安全群組

使用者和群組配額

當您設定使用中目錄或SAML基於 IdP 的使用者和群組時，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

使用用戶VPN端端點時，請考慮下列事項：

- 如果您使用 Active Directory 來驗證使用者，則用戶端VPN端點必須屬於與用於 Active Directory 驗證的 AWS Directory Service 資源相同的帳號。
- 如果您使用SAML基於聯合認證來驗證使用者，則 Client VPN 端點必須與您建立的IAMSAML身分識別提供者屬於相同的帳戶，以定義要 AWS 信任關係的 IdP。IAMSAML身分識別提供者可以在同一 AWS 帳號中的多個用戶VPN端端點之間共用。

疑難排 AWS Client VPN

下列各節可協助您疑難排解用戶VPN端端點可能遇到的問題。

如需疑難排解用戶端用來連線到用戶端的開放VPN式軟體的詳細資訊VPN，請參閱使用指南中的疑難排解用AWS Client VPN 戶端VPN連線。

常見問題

- 疑難排解 AWS Client VPN：無法解析用戶端VPN端點DNS名稱
- 疑難排解 AWS Client VPN：流量未在子網路之間分割
- 疑難排解 AWS Client VPN：使用中目錄群組的授權規則未如預期般運作
- 疑難排解 AWS Client VPN：用戶端無法存取對等式VPC、Amazon S3 或網際網路
- 疑難排解 AWS Client VPN：對VPC等式、Amazon S3 或網際網路的存取是間歇性的
- 疑難排解 AWS Client VPN：用戶端軟體在嘗試連線到用戶端時傳回TLS錯誤 VPN
- 疑難排解 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — Active Directory 驗證
- 疑難排解 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — 聯合驗證
- 疑難排解 AWS Client VPN：用戶端無法連線 — 相互驗證
- 疑難排解 AWS Client VPN：用戶端傳回認證超過用戶端 VPN — 聯合驗證中的認證大小上限錯誤
- 疑難排解 AWS Client VPN：用戶端未開啟端點的瀏覽器 — 聯合驗證
- 疑難排解 AWS Client VPN：用戶端沒有傳回可用的連接埠錯誤 — 聯合驗證
- 疑難排解 AWS Client VPN：連線因 IP 不相符而終止
- 疑難排解 AWS Client VPN：將流量路由至LAN未如預期運作
- 疑難排解 AWS Client VPN：確認用戶VPN端端點的頻寬限制

疑難排解 AWS Client VPN：無法解析用戶端VPN端點DNS名稱

問題

我無法解析用戶VPN端端點的DNS名稱。

原因

用戶VPN端端點組態檔案包含一個名為的參數`remote-random-hostname`。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此參數，因此不會在名稱前面加上必要的隨機字串。DNS

解決方案

使用偏好的文字編輯器開啟用戶VPN端端點設定檔案。找到指定 Client VPN 端點DNS名稱的行，並在其前面加上隨機字串，使其格式為 *random_string.displayed_DNS_name*。 例如：

- 原始DNS名稱：`cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- 修改後的DNS名稱：`asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

疑難排解 AWS Client VPN：流量未在子網路之間分割

問題

我嘗試在兩個子網路之間分割網路流量。私有流量應透過私有子網路路由，而網際網路流量應透過公有子網路路由。但是，即使我已將兩個路由添加到客戶VPN端端點路由表，也只使用一個路由。

原因

您可以將多個子網路與一個 Client VPN 端點產生關聯，但是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，Client VPN 不會讓您選擇性地分割與用戶VPN端端點相關聯的子網路之間的流量。

用戶VPN端會根據DNS循環配置資源演算法連線到用戶端端點。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VPN端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。

疑難排解 AWS Client VPN：使用中目錄群組的授權規則未如預期般運作

問題

我已為我的 Active Directory 群組設定授權規則，但它們並未如預期般運作。我已經添加了授權規則`0.0.0.0/0`來授權所有網絡的流量，但是特定目的地的流量仍然失敗CIDRs。

原因

授權規則會在網路上建立索引CIDRs。授權規則必須將特定網路的存取權授與 Active Directory 群組CIDRs。`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。

客戶端在評估授權規則時VPN使用最長的前綴匹配。有關更多詳細信息，請參閱 Amazon VPC 用戶指南中的路線優先級。

解決方案

確認您已建立明確授與特定網路的 Active Directory 群組存取權的授權規則CIDRs。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。

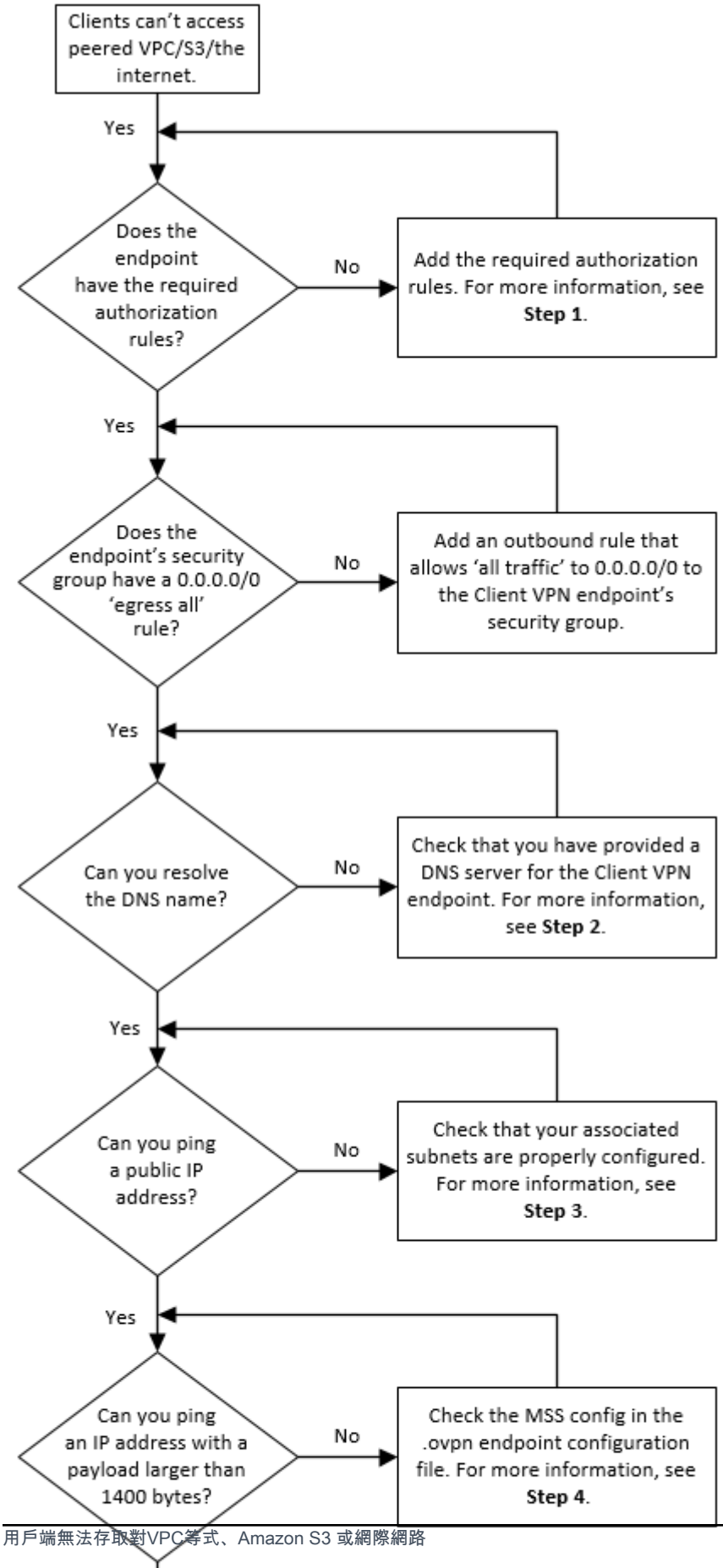
疑難排解 AWS Client VPN：用戶端無法存取對等式VPC、Amazon S3 或網際網路

問題

我已正確設定我的用戶VPN端端點路由，但我的客戶無法存取對VPC等、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VPC等和 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VPC等，請針對的IPv4CIDR範圍新增授權規則。VPC

   若要存取 S3，請指定 Amazon S3 端點的 IP 地址。
2. 檢查您是否能夠解析名DNS稱。

   如果您無法解析DNS名稱，請確認您已為用戶VPN端端點指定DNS伺服器。如果您管理自己的DNS伺服器，請指定其 IP 位址。確認DNS伺服器是否可從存取VPC。

   如果您不確定要為DNS伺服器指定VPCDNS哪個 IP 位址，請在. VPC
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，請確定相關子網路的路由表具有以網際網路閘道或閘道為目標的預設路由。NAT 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。

   如果您無法到達對VPC等，請確認相關子網路的路由表具有對等的路由項目。VPC

   如果您無法連線到 Amazon S3，請確認相關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 Ping 承載大於 1400 位元組的 IP 位址，請使用偏好的文字編輯器開啟用戶VPN端端點`.ovpn`設定檔案，然後新增下列項目。

   ```
   mssfix 1328
   ```

疑難排解 AWS Client VPN：對VPC等式、Amazon S3 或網際網路的存取是間歇性的

問題

我在連線至對VPC等、Amazon S3 或網際網路時出現間歇性連線問題，但是存取關聯的子網路不受影響。我需要中斷連接並重新連接以解決連接問題。

原因

用戶VPN端會根據DNS循環配置資源演算法連線到用戶端端點。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VPN端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VPN端端點有三個關聯的子網路 (子網路 A、B 和 C)，而且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

疑難排解 AWS Client VPN：用戶端軟體在嘗試連線到用戶端時傳回TLS錯誤 VPN

問題

我曾經能夠VPN成功地將客戶端連接到客戶端，但現在，VPN基於打開的客戶端在嘗試連接時返回以下錯誤之一：

```
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。在驗證階段，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「開啟」SSL 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，您必須建立新的憑證並將其匯入 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：

用於用戶VPN端端點的伺服器憑證已過期。

解決方案 2：

在 AWS Certificate Manager 主控台或使用檢查伺服器憑證的狀態 AWS CLI。如果伺服器憑證已過期，請建立新憑證並上傳至ACM。有關使用 Open VPN Easy-rsa 實用程序生成服務器和客戶端證書和密鑰的詳細步驟，並將ACM其導入到請參閱。中的相互認證 AWS Client VPN

或者，用戶端用來連線到用戶端的開放VPN式軟體可能有問題VPN。如需疑難排解開放VPN式軟體的詳細資訊，請參閱AWS Client VPN 使用指南中的疑難排解用戶端VPN連線。

疑難排解 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — Active Directory 驗證

問題

我為我的客戶VPN端端點使用 Active Directory 身份驗證，並且曾經能夠將我的客戶端VPN成功連接到客戶端。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 驗證，並且在分發用戶端組態檔之後啟用了多重要素驗證 (MFA)，則檔案不會包含提示使用者輸入其MFA程式碼的必要資訊。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。在不使用用戶VPN端端點的情況下測試 Active Directory 的MFA組態，以確認MFA是否正常運作。

疑難排解 AWS Client VPN：用戶端軟體傳回使用者名稱和密碼錯誤 — 聯合驗證

問題

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

原因

此錯誤可能是由於 IdP 的SAML回應中包含至少一個屬性所致。

解決方案

確保 IdP 的SAML回應中包含至少一個屬性。如需詳細資訊，請參閱「SAML基於 IdP 組態資源」。

疑難排解 AWS Client VPN：用戶端無法連線 — 相互驗證

問題

我為我的用戶VPN端端點使用相互身份驗證。用戶端收到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。

疑難排解 AWS Client VPN：用戶端傳回認證超過用戶端 VPN — 聯合驗證中的認證大小上限錯誤

問題

我為我的用戶VPN端端點使用聯合身份驗證。當用戶端在SAML基礎識別提供者 (IdP) 瀏覽器視窗中輸入其使用者名稱和密碼時，會收到認證超過支援大小上限的錯誤訊息。

原因

IdP 傳SAML回的回應超過支援的大小上限。如需詳細資訊，請參閱SAML以聯合認證為基礎的需求和考量。

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。

疑難排解 AWS Client VPN：用戶端未開啟端點的瀏覽器 — 聯合驗證

問題

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

原因

提供給用戶端的組態檔案不包含 `auth-federate` 旗標。

解決方案

匯出最新的組態檔案，將其匯入 AWS 提供的用戶端，然後再次嘗試連線。

疑難排解 AWS Client VPN：用戶端沒有傳回可用的連接埠錯誤 — 聯合驗證

問題

我為我的用戶VPN端端點使用聯合身份驗證。當用戶端嘗試連線到端點時，用戶端軟體會傳回下列錯誤：

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

原因

AWS 提供的用戶端需要使用TCP連接埠 35001 才能完成驗證。如需詳細資訊，請參閱SAML以聯合認證為基礎的需求和考量。

解決方案

確認用戶端的裝置未封鎖TCP通訊埠 35001，或是將其用於其他程序。

疑難排解 AWS Client VPN：連線因 IP 不相符而終止

問題

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

原因

AWS 提供的用戶端要求其所連線的 IP 位址與支援用戶VPN端端點之VPN伺服器的 IP 相符。如需詳細資訊，請參閱使用規則和最佳做法 AWS Client VPN。

解決方案

確認 AWS 提供的用戶端和用戶VPN端端點之間沒有 DNS Proxy。

疑難排解 AWS Client VPN：將流量路由至LAN未如預期運作

問題

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

原因

如果偵測到用戶端LAN位址範圍超出上述標準範圍，用戶VPN端端點會自動將 Open VPN 指令「重新導向閘道區塊本機」推送到用戶端，將所有LAN流量強制進入. VPN 如需詳細資訊，請參閱使用規則和最佳做法 AWS Client VPN。

解決方案

如果您在VPN連接過程中需要LAN訪問，建議您使用上面列出的常規地址範圍LAN。

疑難排解 AWS Client VPN：確認用戶VPN端端點的頻寬限制

問題

我需要驗證用戶VPN端端點的頻寬限制。

原因

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

解決方案

執行下列命令以驗證頻寬。

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

在用戶端上：

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

VPN用戶端使用者指南的文件記錄

下表說明《 AWS Client VPN 管理手冊》的更新。

變更	描述	日期
授權規則範例	新增授權規則的範例案例。	2022 年 9 月 15 日
VPN工作階段最長期	您可以設定較短的VPN工作階段持續時間上限，以符合安全性和合規性需求	2022 年 1 月 20 日
用戶端登入橫幅	當建立VPN工作階段以符合法規和合規需求時，您可以在 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 端點啟用用戶VPN端連線處理常式，以執行授權新連線的自訂邏輯。	2020 年 11 月 4 日
自助式入口網站	您可以在客戶VPN端點上為客戶啟用自助服務門戶。	2020 年 10 月 29 日
C lient-to-client 存取	您可以讓連線到用戶VPN端端點的用戶端彼此連線。	2020 年 9 月 29 日
SAML以 2.0 為基礎的同盟驗證	您可以使用 SAML 2.0 型聯合驗證來驗證用VPN戶端使用者。	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
可配置的VPN端	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

Support 多重要素驗證 () MFA	MFA如果您的活動目錄已啟用該 AWS Client VPN 端點，則支持該端點。	2019 年 9 月 30 日
支援分割通道	您可以在端點上啟用分割通道。 AWS Client VPN	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。