AWS Client VPN

管理員指南

AWS Client VPN: 管理員指南

Table of Contents

什麼是 AWS Client VPN？

AWS Client VPN 是以用戶端為基礎的受管 VPN 服務，能讓您安全地存取您的 AWS 資源，以及您的現場部署網路中的資源。透過 用戶端 VPN，您可以從任何地方使用以 OpenVPN 為基礎的 VPN 用戶端存取您的資源。

內容

用戶端 VPN 的功能

用戶端 VPN 提供以下特色和功能：

- 安全連線 — 支援從任何地方使用 OpenVPN 用戶端建立安全的 TLS 連線。
- 受管服務 — 它是受管服務，免去部署和管理第三方遠端存取 VPN 解決方案的操作負擔。
- 高可用性又有彈性 — 隨著連接到您的 AWS 資源和內部部署資源的使用者人數而自動擴展。
- Authentication (身份驗證)：支援使用 Active Directory、同盟驗證和以憑證為基礎的身份驗證進行用戶端身份驗證。
- 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 — 可讓您使用單一 VPN 通道存取您的 AWS 資源與現場部署資源。
- 可管理性 — 可讓您查看連線日誌，其中提供用戶端連線嘗試的詳細資訊。您也可以管理作用中用戶端連線，允許您終止作用中用戶端連線。
- 深度整合 — 與現有的 AWS 服務整合，包括 AWS Directory Service 和 Amazon VPC。

用戶端 VPN 的元件

以下是 用戶端 VPN 的重要概念：

用戶端 VPN 端點

用戶端 VPN 端點是您為了啟用和管理用戶端 VPN 工作階段而建立和設定的資源。此資源是所有用戶端 VPN 工作階段的終點。

目標網路

目標網路是與 用戶端 VPN 端點相關聯的網路。始於 VPC 的子網路是目標網路。將子網路與 用戶端 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關聯至 用戶端 VPN 端點，以獲得高可用性。所有子網路必須來自相同的 VPC。每個子網路必須屬於不同的可用區域。

路由

每個 用戶端 VPN 端點都有路由表來描述可用的目的地網路路由。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

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

用戶端 CIDR 範圍

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

用戶端 VPN 連接埠

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

用戶端 VPN 網路界面

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

連線日誌記錄

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

使用 用戶端 VPN

您可以透過以下任何方式來使用 用戶端 VPN：

Amazon VPC 主控台

Amazon VPC 主控台為 用戶端 VPN 提供 Web 型使用者界面。如果您已註冊 AWS 帳戶，您可以登入 Amazon VPC 主控台，然後在導覽窗格中選擇 用戶端 VPN。

AWS Command Line Interface (CLI)

AWS CLI 可讓您直接存取 用戶端 VPN 公有 API。Windows、macOS 和 Linux 都提供支援。如需 AWS CLI 入門的詳細資訊，請參閱 AWS Command Line Interface 使用者指南。如需 用戶端 VPN 命令的詳細資訊，請參閱 AWS CLI Command Reference。

適用於 Windows PowerShell 的 AWS 工具

對於在 PowerShell 環境中編寫指令碼的使用者，AWS 提供許多 AWS 產品的命令。如需 適用於 Windows PowerShell 的 AWS 工具 入門的詳細資訊，請參閱 適用於 Windows PowerShell 的 AWS 工具 使用者指南。如需 用戶端 VPN Cmdlet 的詳細資訊，請參閱 適用於 Windows PowerShell 的 AWS 工具 Cmdlet 參考。

查詢 API

用戶端 VPN HTTPS 查詢 API 可讓您以程式設計方式存取 用戶端 VPN 和 AWS。HTTPS 查詢 API 可讓您直接向該服務發出 HTTPS 請求。當您使用 HTTPS API 時，必須包含程式碼來使用您的登入資料以數位簽署請求。如需詳細資訊，請參閱 用戶端 VPN API 參考。

用戶端 VPN 的限制和規則

用戶端 VPN 具有下列規則和限制：

- 用戶端 CIDR 範圍與相關聯子網路所在的 VPC 的本機 CIDR 不可重疊，或與手動新增到 用戶端 VPN 端點路由表的任何路由不可重疊。
- 用戶端 CIDR 範圍必須有至少為 /22 且不可大於 /12 的區塊大小。
- 用戶端 CIDR 範圍中的一部分地址用於支援 用戶端 VPN 端點的可用性模型，而且無法指派給用戶端。因此，建議您指派 CIDR 區塊，其中包含您計劃在 用戶端 VPN 端點上支援同時連線數目上限所需 IP 地址數目兩倍的 IP 地址數目。
- 建立 用戶端 VPN 端點之後，就無法變更用戶端 CIDR 範圍。
- 與 用戶端 VPN 端點相關聯的子網路必須位於同一個 VPC 中。
- 您不能將來自相同可用區域的多個子網路與一個 用戶端 VPN 端點建立關聯。
- 用戶端 VPN 端點不支援專用租用 VPC 中的子網路關聯。
- 用戶端 VPN 僅支援 IPv4 流量。
- 用戶端 VPN 不符合健康保險流通與責任法案 (HIPAA) 或聯邦資訊處理標準 (FIPS)。
- 如果您的 Active Directory 停用 Multi-Factor Authentication (MFA)，則使用者密碼不能使用下列格式。

```
SCRV1:<base64_encoded_string>:<base64_encoded_string>
```

用戶端 VPN 的定價

我們依照每個 用戶端 VPN 端點的每個作用中關聯，按小時計費。按小時的比例分配來計費。

我們依照每個用戶端 VPN 連線，按小時計費。按小時的比例分配來計費。

如需詳細資訊，請參閱 AWS Client VPN 定價。

如果您啟用 用戶端 VPN 端點的連線日誌記錄，則必須在帳戶中建立 CloudWatch Logs 日誌群組。使用日誌群組需支付費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

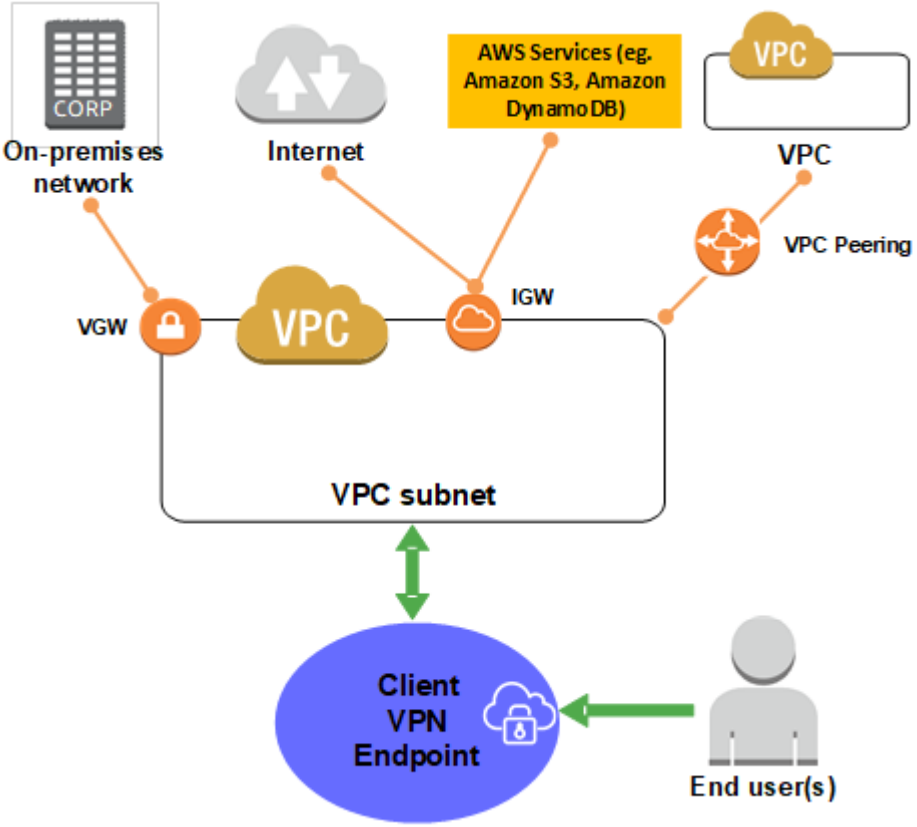
AWS Client VPN 的運作方式

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

管理員負責安裝和設定服務。這包括建立 用戶端 VPN 端點、將目標網路相關聯、設定授權規則，以及設定額外的路由 (如果需要)。在安裝和設定 用戶端 VPN 端點後，管理員會下載 用戶端 VPN 端點組態檔案，並分發給需要存取的用戶端。用戶端 VPN 端點組態檔案包含 用戶端 VPN 端點的 DNS 名稱，以及建立 VPN 工作階段所需的身份驗證資訊。如需有關設定此服務的詳細資訊，請參閱用戶端 VPN 入門 (p. 26)。

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

下圖說明基本的 用戶端 VPN 架構。



用戶端身份驗證和授權

用戶端 VPN 提供身份驗證和授權功能。

內容

身分驗證

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

用戶端 VPN 提供下列類型的用戶端身份驗證：

- Active Directory 身份驗證 (p. 5) (以使用者為基礎)
- 交互身份驗證 (p. 5) (以憑證為基礎)
- 單一登入 (SAML 型同盟驗證) (p. 8) (以使用者為基礎)

您可以使用下列其中一項或組合：

- 交互身份驗證和同盟驗證
- 交互身份驗證和 Active Directory 身份驗證

> Important
>
> 若要建立 用戶端 VPN 端點，無論使用何種身份驗證類型，您都必須在 AWS Certificate Manager 中佈建伺服器憑證。如需建立和佈建伺服器憑證的詳細資訊，請參閱交互身份驗證 (p. 5)中的步驟。

Active Directory 身份驗證

用戶端 VPN 與 AWS Directory Service 整合，以提供 Active Directory 支援。透過 Active Directory 身份驗證，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 連接到佈建在 AWS 或現場部署網路中的 Active Directory。這可讓您使用現有的用戶端身份驗證基礎設施。如果您使用內部部署 Active Directory，但沒有現有的 AWS Managed Microsoft AD，則必須設定 Active Directory Connector (AD Connector)。您可以使用一個 Active Directory 伺服器來驗證使用者。如需 Active Directory 整合的詳細資訊，請參閱 AWS Directory Service Administration Guide。

為 AWS 受管 Microsoft AD 或 AD Connector 啟用 Multi-Factor Authentication (MFA) 時，用戶端 VPN 支援 Multi-Factor Authentication (MFA)。如果啟用 MFA，用戶端必須在連線到 用戶端 VPN 端點時輸入使用者名稱、密碼和 MFA 代碼。如需啟用 MFA 的詳細資訊，請參閱AWS Directory Service Administration Guide中的為 AWS 受管 Microsoft AD 啟用 Multi-Factor Authentication和為 AD Connector 啟用 Multi-Factor Authentication。

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 (p. 51)。

交互身份驗證

透過交互身份驗證，用戶端 VPN 使用憑證在用戶端和伺服器之間執行身份驗證。憑證為憑證授權機構 (CA) 發出的數位形式身分證明。當用戶端嘗試連接到 用戶端 VPN 端點時，伺服器會使用用戶端憑證來驗證用戶端。

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

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

用戶端 VPN 端點僅支援 1024 位元和 2048 位元 RSA 金鑰大小。

Linux/macOS

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

產生伺服器和用戶端憑證及金鑰並上傳到 ACM

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

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

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

2. 初始化新的 PKI 環境。

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

3. 建置新的憑證授權機構 (CA)。

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

依照提示建置 CA。

4. 產生伺服器憑證和金鑰。

```
$ ./easyrsa 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. 上傳伺服器憑證和金鑰，以及用戶端憑證和金鑰至 ACM。下列命令使用 AWS CLI。

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

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

若要使用 ACM 主控台上傳憑證，請參閱AWS Certificate Manager 使用者指南中的匯入憑證。

Note

務必在您想要建立 用戶端 VPN 端點的同一區域中上傳憑證和金鑰。
只有當用戶端憑證的 CA 和伺服器憑證的 CA 不同時，您才需要將用戶端憑證上傳到 ACM。在上述步驟中，用戶端憑證使用與伺服器憑證相同的 CA，但為了完整起見，此處會包含用戶端憑證的上傳步驟。

Windows

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

產生伺服器和用戶端憑證及金鑰並上傳到 ACM

1. 前往 OpenVPN Community Downloads (OpenVPN 社群下載) 頁面，並下載適用您 Windows 版本的 Windows 安裝程式。
2. 執行安裝程式。在 OpenVPN 安裝精靈的第一頁中，選擇 Next (下一步)。
3. 在 License Agreement (授權合約) 頁面上，選擇 I Agree (我同意)。
4. 在 Choose Components (選擇元件) 頁面上，選擇 EasyRSA 2 Certificate Management Scripts (EasyRSA 2 憑證管理指令碼)。選擇 Next (下一步)，然後選擇 Install (安裝)。
5. 選擇 Next (下一步)，然後選擇 Finish (完成) 以完成安裝。
6. 以管理員身分打開命令提示，導覽至 OpenVPN 目錄，然後執行 `init-config`。

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

```
C:\> init-config
```

7. 使用記事本開啟 `vars.bat` 檔案。

```
C:\> notepad vars.bat
```

8. 在該檔案中，執行下列動作並儲存變更。
   - 針對 `set KEY_SIZE`，請將值變更為 `2048`。
   - 提供下列參數的值。請勿將任何值保留空白。
     - KEY_COUNTRY
     - KEY_PROVINCE
     - KEY_CITY
     - KEY_ORG
     - KEY_EMAIL
9. 在命令列中，執行 `vars.bat` 檔案，然後執行 `clean-all`。

```
C:\> vars
```

```
C:\> clean-all
```

10. 建置新的憑證授權機構 (CA)。

```
C:\> build-ca
```

依照提示建置 CA。您可以保留所有欄位的預設值。如果您願意，您可以將 Common Name (一般名稱) 變更為伺服器的網域名稱，例如 `server.example.com`。

11. 產生伺服器憑證和金鑰。

```
C:\> build-key-server server
```

依照提示產生憑證和金鑰。除了 Common Name (一般名稱) 以外，您可以保留所有欄位的預設值。針對此欄位，您必須以網域名稱格式指定伺服器網域。例如，`server.example.com`。

當系統提示您簽署憑證時，請在這兩個提示都輸入 `y`。

12. 產生用戶端憑證和金鑰。

```
C:\> build-key client
```

依照提示產生憑證和金鑰。除了 Common Name (一般名稱) 以外，您可以保留所有欄位的預設值。針對此欄位，您必須以網域名稱格式指定用戶端網域。例如，`client.example.com`。

當系統提示您簽署憑證時，請在這兩個提示都輸入 `y`。

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。

13. 上傳伺服器憑證和金鑰，以及用戶端憑證和金鑰至 ACM。下列命令使用 AWS CLI。

```
C:\> aws acm import-certificate --certificate fileb://"C:\Program Files\OpenVPN
\easy-rsa\keys\server.crt" --private-key fileb://"C:\Program Files\OpenVPN\easy-
rsa\keys\server.key" --certificate-chain fileb://"C:\Program Files\OpenVPN\easy-rsa
\keys\ca.crt" --region region
```

```
C:\> aws acm import-certificate --certificate fileb://"C:\Program Files\OpenVPN
\easy-rsa\keys\client.crt" --private-key fileb://"C:\Program Files\OpenVPN\easy-
rsa\keys\client.key" --certificate-chain fileb://"C:\Program Files\OpenVPN\easy-rsa
\keys\ca.crt"  --region region
```

若要使用 ACM 主控台上傳憑證，請參閱AWS Certificate Manager 使用者指南中的匯入憑證。

Note

務必在您想要建立 用戶端 VPN 端點的同一區域中上傳憑證和金鑰。
只有當用戶端憑證的 CA 和伺服器憑證的 CA 不同時，您才需要將用戶端憑證上傳到 ACM。在上述步驟中，用戶端憑證使用與伺服器憑證相同的 CA，但為了完整起見，此處會包含用戶端憑證的上傳步驟。

單一登入 (SAML 2.0 型同盟驗證)

AWS Client VPN 支援具有適用於 用戶端 VPN 端點之安全性聲明標記語言 2.0 (SAML 2.0) 的聯合身份。您可以使用支援 SAML 2.0 的身分提供者 (IdP)，來建立集中式使用者身分。然後，您可以將 用戶端 VPN 端點設定為使用 SAML 型同盟驗證，並將其與 IdP 建立關聯。然後，使用者使用其集中式登入資料連線至 用戶端 VPN 端點。

若要讓以 SAML 型的 IdP 能夠與 用戶端 VPN 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 型應用程式，以與 AWS Client VPN 搭配使用或使用現有應用程式。
2. 設定 IdP 與 AWS 建立信任關係。如需資源，請參閱 SAML 型 IdP 組態資源 (p. 11)。
3. 在 IdP 中產生並下載聯合中繼資料文件，以將您的組織描述為 IdP。此簽署的 XML 文件用於建立 AWS 和 IdP 之間的信任關係。

4. 在與 用戶端 VPN 端點相同的 AWS 帳戶中建立 IAM SAML 身分提供者。IAM SAML 身分提供者會使用 IdP 產生的中繼資料文件，來定義組織的 IdP 對 AWS 的信任關係。如需詳細資訊，請參閱 IAM 使用者指南 的建立 IAM SAML 身分提供者。如果您稍後更新 IdP 中的應用程式組態，請產生新的中繼資料文件並更新 IAM SAML 身分提供者。

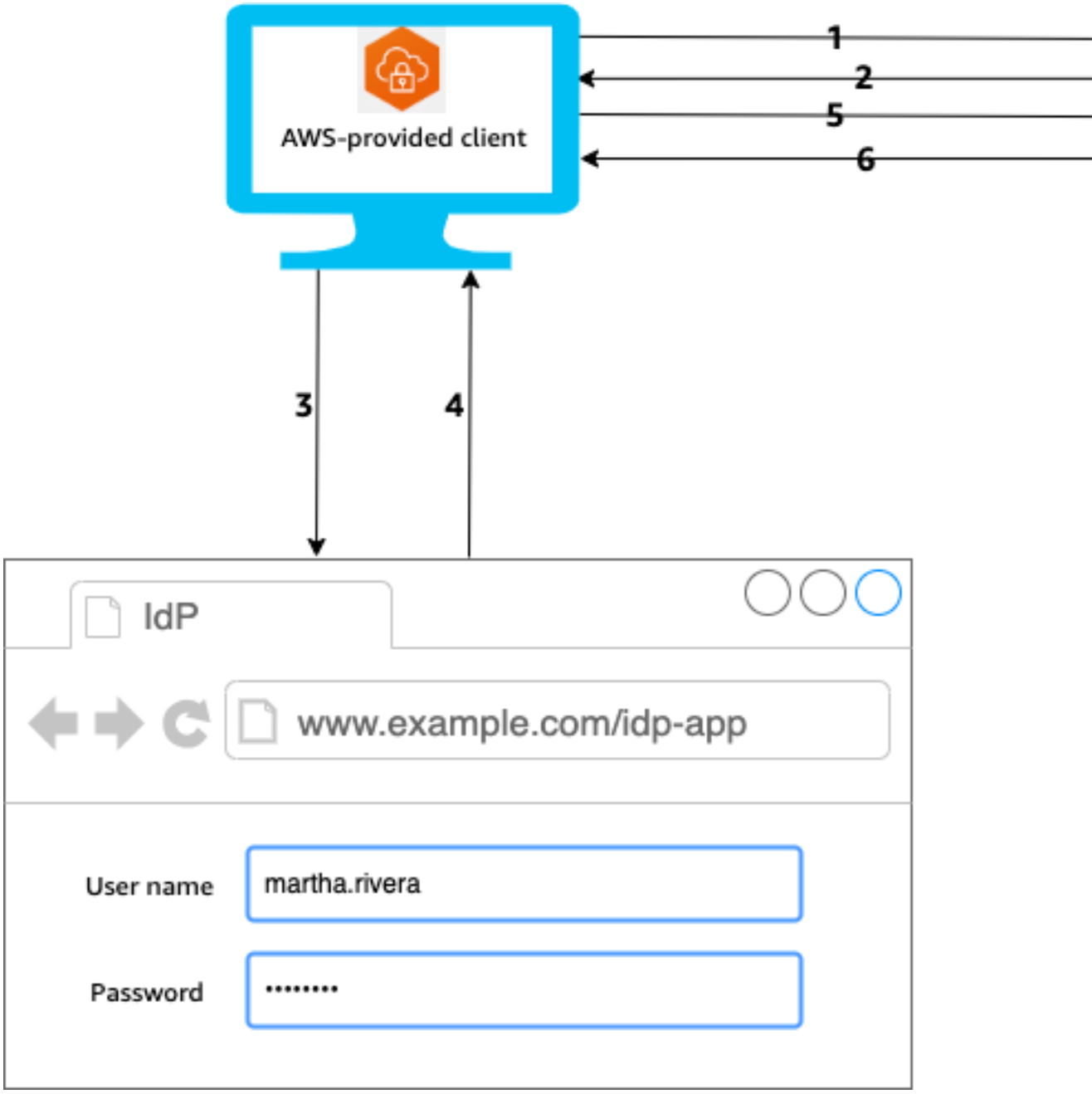
   Note

   您不需要建立 IAM 角色即可使用 IAM SAML 身分提供者。

5. 建立 用戶端 VPN 端點。指定同盟驗證做為身份驗證類型，並指定您建立的 IAM SAML 身分提供者。如需詳細資訊，請參閱 建立 用戶端 VPN 端點 (p. 31)。
6. 匯出用戶端組態檔案 (p. 33)，並將其分配到您的使用者。指示使用者下載最新版本的 AWS 提供的用戶端，並使用它來載入組態檔並連線到 用戶端 VPN 端點。

驗證工作流程

下圖提供驗證工作流程概觀，適用於使用 SAML 型同盟驗證的 用戶端 VPN 端點。建立和設定 用戶端 VPN 端點時，請指定 IAM SAML 身分提供者。



1. 使用者會在其裝置上開啟 AWS 提供的用戶端，並將與 用戶端 VPN 端點的連線初始化。
2. 用戶端 VPN 端點會根據 IAM SAML 身分提供者中提供的資訊，將 IdP URL 和身份驗證請求傳回用戶端。
3. AWS 提供的用戶端 會在使用者的裝置上開啟新的瀏覽器視窗。瀏覽器向 IdP 發出請求並顯示登入頁面。
4. 使用者在登入頁面上輸入登入資料，且 IdP 會將簽署的 SAML 聲明傳回給用戶端。
5. AWS 提供的用戶端 將 SAML 聲明傳送至 用戶端 VPN 端點。
6. 用戶端 VPN 端點會驗證聲明，並允許或拒絕對使用者的存取。

SAML 型同盟驗證的需求和考量

以下是 SAML 型同盟驗證的需求和考量。

- 如需在 SAML 型 IdP 中設定使用者和群組的配額和規則，請參閱使用者和群組配額 (p. 51)。
- SAML 回應必須經過簽署和解除加密。
- SAML 回應的支援大小上限為 128 KB。
- AWS Client VPN 不會提供簽署的身份驗證請求。
- 不支援 SAML 單一登出。使用者可以透過中斷與 AWS 提供的用戶端 的連線來登出，或者您可以終止連線 (p. 43)。
- 用戶端 VPN 端點僅支援單一 IdP。
- 在 IdP 中啟用 Multi-factor authentication (MFA) 時，即支援 Multi-factor authentication (MFA)。
- 使用者必須使用 AWS 提供的用戶端 來連線至 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 進行連線。
- 以下瀏覽器支援 IdP 身份驗證：Apple Safari，Google Chrome，Microsoft Edge 和 Mozilla Firefox。
- AWS 提供的用戶端 會在使用者裝置上保留 TCP 連接埠 35001，以供 SAML 回應使用。
- 如果使用不正確或惡意的 URL 更新 IAM SAML 身分提供者的中繼資料文件，這可能會導致使用者身份驗證問題，或導致網路釣魚攻擊。因此，我們建議您使用 AWS CloudTrail 監視對 IAM SAML 身分提供者所做的更新。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 AWS CloudTrail 記錄 IAM 和 AWS STS 呼叫。
- AWS Client VPN 透過 HTTP 重新導向繫結向 IdP 傳送 AuthN 請求。因此，IdP 應該支援 HTTP 重新導向繫結，而且它應該存在於 IdP 的中繼資料文件中。
- 針對 SAML 聲明，您必須使用 `NameID` 屬性的電子郵件地址格式。

SAML 型 IdP 組態資源

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

IdP	資源
Okta	使用 SAML 驗證 AWS Client VPN 使用者

建立應用程式的服務提供者資訊

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

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

以下是必要屬性。

屬性	描述
`NameID`	使用者的電子郵件地址。
`FirstName`	使用者的名字。
`LastName`	使用者的姓氏。

屬性	描述
memberOf	使用者所屬的一或多個群組。

屬性區分大小寫，且必須完全按照指定進行設定。

授權

用戶端 VPN 支援兩種類型的授權：安全群組和以網路為基礎的授權 (使用授權規則)。

安全群組

建立 用戶端 VPN 端點時，您可以從特定 VPC 指定要套用至 用戶端 VPN 端點的安全群組。當您將子網路與用戶端 VPN 端點建立關聯時，我們會自動套用 VPC 的預設安全群組。您可以在建立 用戶端 VPN 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到目標網路 (p. 36)。安全群組與 用戶端 VPN 網路界面關聯。

您可以新增規則到應用程式的安全群組以允許套用到關聯的安全群組所傳來的流量，讓 用戶端 VPN 使用者可以存取 VPC 中的應用程式。

新增允許來自 用戶端 VPN 端點安全群組的流量的規則

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 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性群組，然後選擇動作、編輯傳入規則。
4. 選擇 Add rule (新增規則)。
5. 針對 Type (類型)，選擇 All traffic (所有流量)。或者，您可以限制存取特定類型的流量，例如 SSH。

   在來源中，指定與 用戶端 VPN 端點的目標網路 (子網路) 相關聯的安全性群組識別碼。
6. 選擇 Save rules (儲存規則)。

相反地，您可以藉由不指定套用至關聯的安全性群組，或移除參照 用戶端 VPN 端點安全性群組的規則，來限制 用戶端 VPN 使用者的存取。您需要的安全群組規則也可能取決於您要設定的 VPN 存取種類。如需詳細資訊，請參閱案例和範例 (p. 16)。

如需安全群組的詳細資訊，請參閱Amazon VPC 使用者指南中的 VPC 的安全群組。

以網路為基礎的授權

以網路為基礎的授權是使用授權規則來實作。對於您想要啟用存取的每個網路，您必須設定授權規則來限制有存取權的使用者。對於指定的網路，請設定允許存取的 Active Directory 群組或 SAML 型 IdP 群組。只有屬於指定群組的使用者，才可以存取指定的網路。如果您不是使用 Active Directory 或 SAML 型同盟驗證，或是您希望開放所有使用者的存取權，您可以指定規則來將存取權授與給所有用戶端。如需更多詳細資訊，請參閱 授權規則 (p. 37)。

AWS Client VPN 端點上的分割通道

根據預設，當您擁有 AWS Client VPN 端點時，所有用戶端流量都會透過 AWS Client VPN 通道路由傳送。當您在 AWS Client VPN 端點上啟用分割通道，我們會將 AWS Client VPN 端點路由表上的路由推送到連接到 AWS Client VPN 的裝置。這可確保只有網路目的地符合 AWS Client VPN 端點路由表中路由的流量，才會透過 用戶端 VPN 通道路由傳送。

當您不希望所有使用者流量透過 AWS Client VPN 端點路由傳送時，可以使用分割通道 AWS Client VPN 端點。

AWS Client VPN 端點上的分割通道優點

AWS Client VPN 端點上的分割通道可提供下列優點：

- 有了分割通道，客戶可透過只讓 AWS 的流量周遊 VPN 通道，優化客端來的流量路由。
- 客戶也能透過優化流量，減少來自 AWS 的傳出流量，因而減少資料傳輸成本。

分割通道 AWS Client VPN 端點路由考量

當您在 AWS Client VPN 端點上啟用分割通道，建立 VPN 時，AWS Client VPN 路由表中的所有路由都會新增至用戶端路由表。此操作不同於預設 AWS Client VPN 端點操作，它會以項目 0.0.0.0/0 覆寫用戶端路由表，以透過 VPN 路由傳送所有流量。

連線日誌記錄

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

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

可在所有可用 AWS Client VPN 的區域中使用連線日誌記錄。連線日誌會發佈至您帳戶中的 CloudWatch Logs 日誌群組。

連線日誌項目

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

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

連線日誌項目包含下列金鑰：

- connection-log-type — 連線日誌項目 (connection-attempt 或 connection-reset) 的類型。
- connection-attempt-status — 連線要求的狀態 (successful、failed、waiting-for-assertion 或 NA)。
- connection-reset-status — 連線重設事件 (NA 或 assertion-received) 的狀態。
- connection-attempt-failure-reason — 連線失敗的原因 (如果適用)。
- connection-id — 連線的 ID。
- client-vpn-endpoint-id — 建立連線之 用戶端 VPN 端點的 ID。
- transport-protocol — 用於連線的傳輸通訊協定。
- connection-start-time — 連線的開始時間。
- connection-last-update-time — 連線的上次更新時間。此值在日誌中會定期更新。
- client-ip — 從用戶端 IPv4 CIDR 範圍配置給 用戶端 VPN 端點的用戶端 IP 地址。
- common-name — 憑證型身份驗證所使用之憑證的一般名稱。
- device-type — 最終使用者用於連線的裝置類型。
- 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) 位元組數目。此值在日誌中會定期更新。
- egress-bytes — 連線的輸出 (傳出) 位元組數目。此值在日誌中會定期更新。
- ingress-packets — 連線的輸入 (傳入) 封包數目。此值在日誌中會定期更新。
- egress-packets — 連線的輸出 (傳出) 封包數目。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。

如需啟用連線日誌記錄的詳細資訊，請參閱 使用連線日誌 (p. 43)。

使用 用戶端 VPN 的服務連結角色

AWS Client VPN 使用服務連結角色，以取得代表您呼叫其他 AWS 服務所需的許可。如需詳細資訊，請參閱 IAM 使用者指南中的使用服務連結角色。

用戶端 VPN 的服務連結角色許可

AWS Client VPN 使用名為 AWSServiceRoleForClientVPN 的服務連結角色，當您使用 用戶端 VPN 端點時，代表您呼叫以下動作：

- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeInternetGateways
- ec2:ModifyNetworkInterfaceAttribute
- ec2:DeleteNetworkInterface
- ec2:DescribeAccountAttributes
- ds:AuthorizeApplication
- ds:DescribeDirectories
- ds:GetDirectoryLimits
- ds:ListAuthorizedApplications

- `ds:UnauthorizeApplication`
- `logs:DescribeLogStreams`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogGroups`
- `acm:GetCertificate`
- `acm:DescribeCertificate`

AWSServiceRoleForClientVPN 服務連結角色信任 clientvpn.amazonaws.com 委託人來擔任角色。

為 用戶端 VPN 建立服務連結角色

您不需要手動建立 AWSServiceRoleForClientVPN 角色。當您在帳戶中建立第一個 用戶端 VPN 端點時，用戶端 VPN 會為您建立此角色。

為了讓 用戶端 VPN 代表您建立服務連結角色，您必須具有必要的許可。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

編輯 用戶端 VPN 的服務連結角色

用戶端 VPN 不允許您編輯 AWSServiceRoleForClientVPN 服務連結角色。

刪除 用戶端 VPN 的服務連結角色

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

您必須先刪除相關的 用戶端 VPN 資源，才能刪除 AWSServiceRoleForClientVPN 服務連結角色。這可確保避免您不小心移除資源的存取許可。

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForClientVPN 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的刪除服務連結角色。

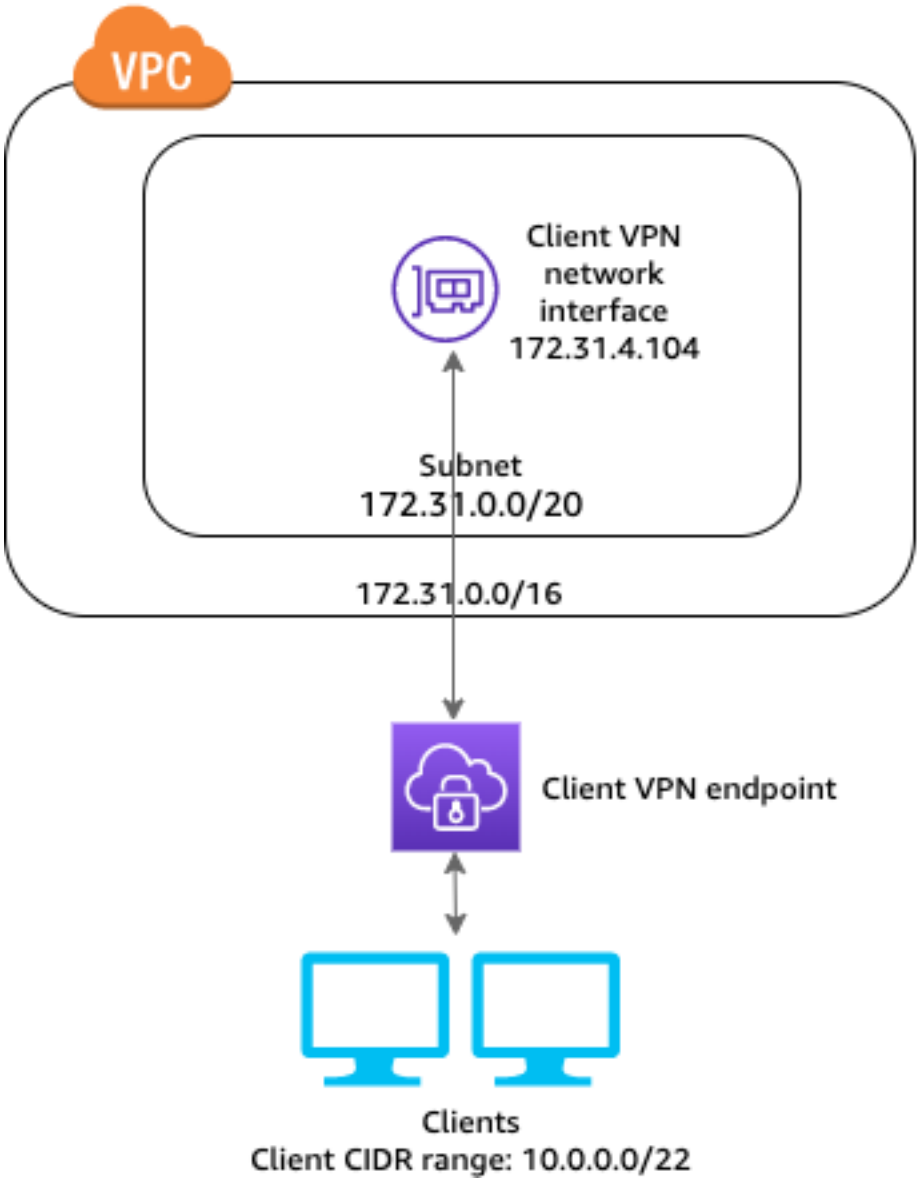
案例和範例

本節提供範例來示範為您的用戶端建立和設定 用戶端 VPN 存取。

內容

存取 VPC

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



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別要與 用戶端 VPN 端點相關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 和子網路。
- 識別與 VPC CIDR 不重疊的用戶端 IP 位址適當的 CIDR 範圍。
- 於 用戶端 VPN 的限制和規則 (p. 2) 檢閱 用戶端 VPN 端點的規則和限制。

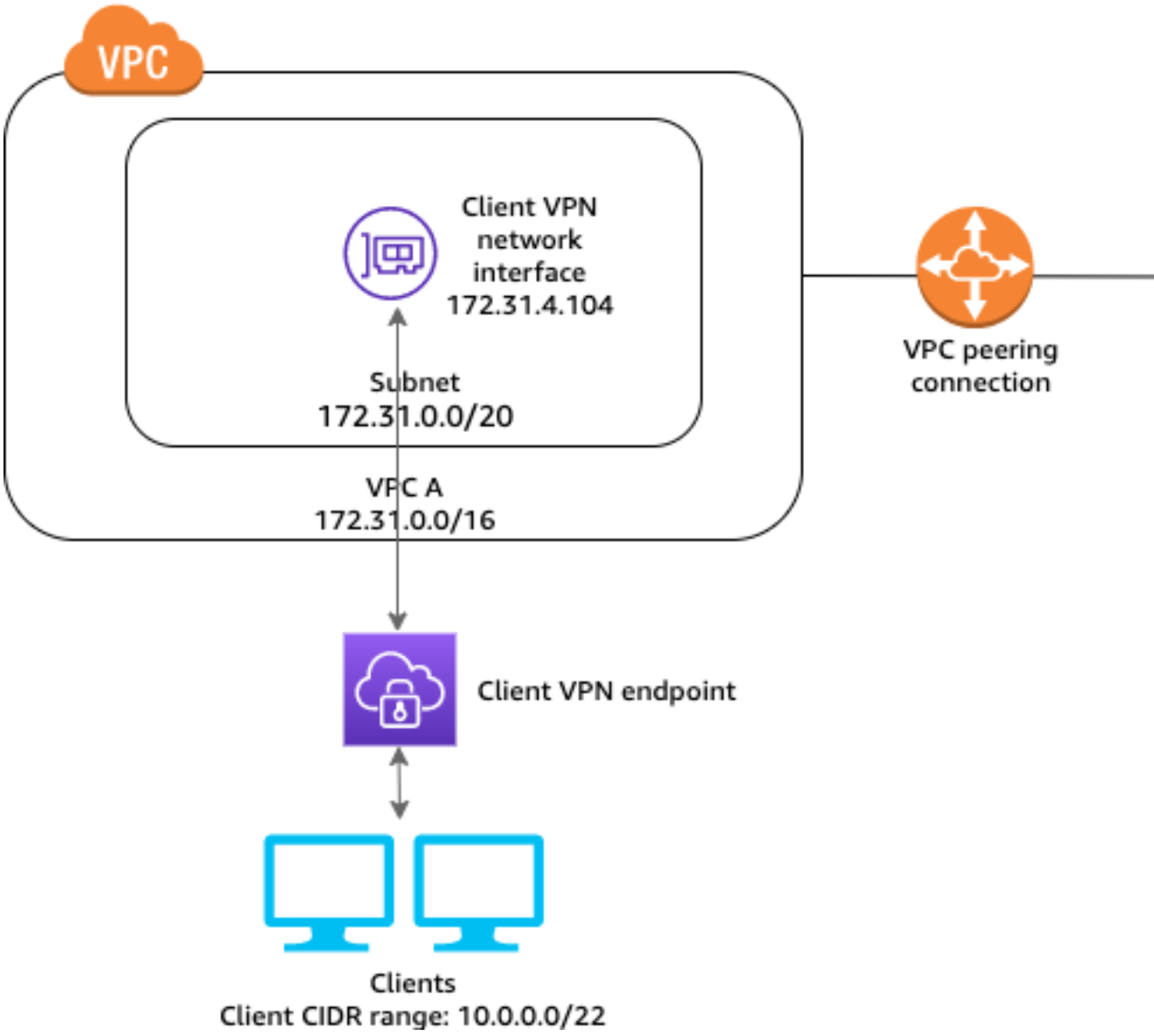
實作此組態

1. 在與 VPC 相同的區域中建立 用戶端 VPN 端點。若要這樣做，請執行建立 用戶端 VPN 端點 (p. 31)中所述的步驟。
2. 將子網路與 用戶端 VPN 端點建立關聯。若要這樣做，請執行將目標網路與 用戶端 VPN 端點建立關聯 (p. 36)中所述的步驟，然後選擇您稍早所識別的子網路和 VPC。

3. 新增授權規則讓用戶端存取 VPC。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟；對於 Destination network (目的地網路)，輸入 VPC 的 IPv4 CIDR 範圍。
4. 將規則新增至資源的安全性群組，以允許來自步驟 2 中套用至子網路關聯的安全性群組的流量。如需更多詳細資訊，請參閱 安全群組 (p. 12)。

存取對等 VPC

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



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別要與 用戶端 VPN 端點相關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 和子網路。
- 識別與 VPC CIDR 不重疊的用戶端 IP 位址適當的 CIDR 範圍。

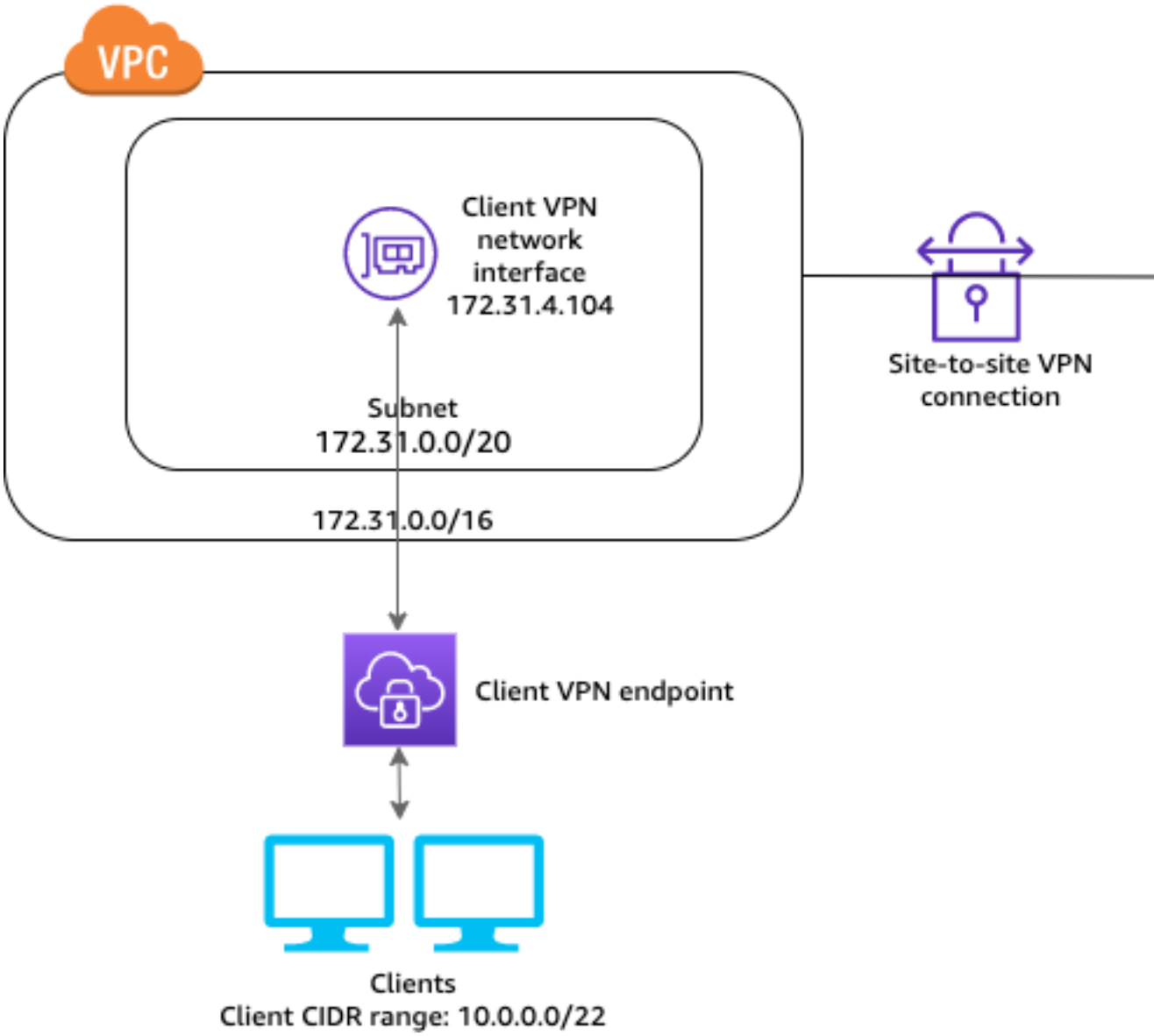
- 於 用戶端 VPN 的限制和規則 (p. 2) 檢閱 用戶端 VPN 端點的規則和限制。

實作此組態

1. 在 VPC 之間建立 VPC 對等連線。遵循Amazon VPC Peering Guide中的建立和接受 VPC 對等連線的步驟。
2. 測試 VPC 對等連線。確認任一 VPC 中的執行個體可彼此通訊，有如位於相同網路中一樣。如果對等連線的運作符合預期，請繼續下一個步驟。
3. 在與目標 VPC 相同的區域中建立 用戶端 VPN 端點。在上述範例中，這是 VPC A。請執行中建立 用戶端 VPN 端點 (p. 31)所述的步驟。
4. 將您稍早所識別的子網路與您建立的 用戶端 VPN 端點建立關聯。若要這樣做，請執行將目標網路與 用戶端 VPN 端點建立關聯 (p. 36)中所述的步驟，然後選擇子網路和 VPC。
5. 新增授權規則讓用戶端存取目標 VPC。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟，對於Destination network to enable (要啟用的目的地網路)，輸入 VPC 的 IPv4 CIDR 範圍。
6. 新增路由將流量引導至對等 VPC。在先前的範例中，這是 VPC B。若要這樣做，請執行建立端點路由 (p. 39)中所述的步驟；對於 Route destination (路由目的地)，輸入對等 VPC 的 IPv4 CIDR 範圍，對於 Target VPC Subnet ID (目標 VPC 子網路 ID)，選擇與 用戶端 VPN 端點相關聯的子網路。
7. 新增授權規則讓用戶端存取對等 VPC。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟；對於 Destination network (目的地網路)，輸入對等 VPC 的 IPv4 CIDR 範圍。
8. 將規則新增至 VPC A 和 VPC B 中的資源安全群組，以允許來自步驟 2 中套用至子網路關聯的安全群組的流量。如需更多詳細資訊，請參閱 安全群組 (p. 12)。

存取內部部署網路

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



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別要與 用戶端 VPN 端點相關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 和子網路。
- 識別與 VPC CIDR 不重疊的用戶端 IP 位址適當的 CIDR 範圍。
- 於 用戶端 VPN 的限制和規則 (p. 2) 檢閱 用戶端 VPN 端點的規則和限制。

實作此組態

1. 允許 VPC 和您自己的現場部署網路之間透過 AWS Site-to-Site VPN 連線進行通訊。若要執行此動作，請執行AWS Site-to-Site VPN 使用者指南中入門所述的步驟。

   Note

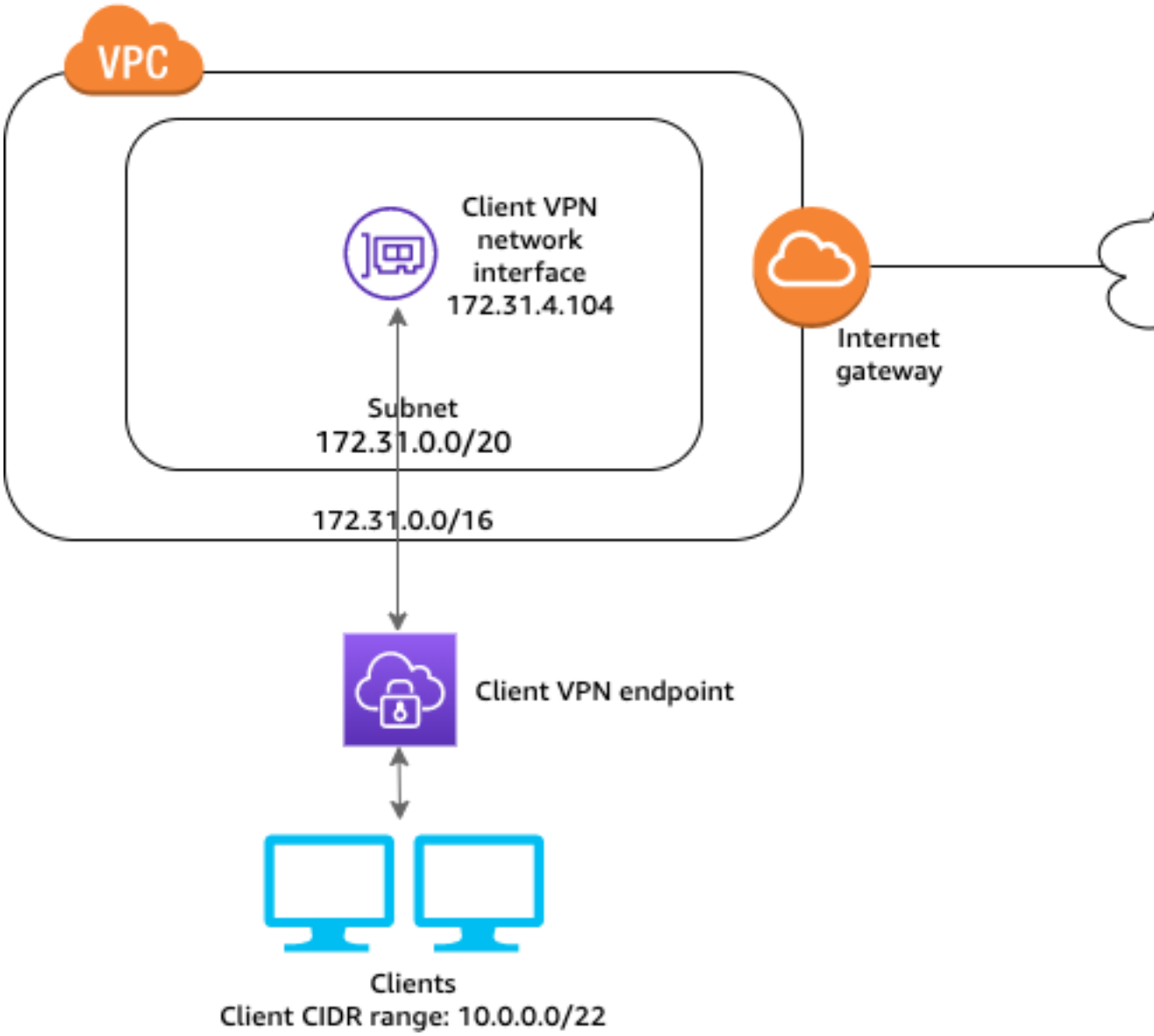
   或者，您可以使用 VPC 與內部部署網路之間的 AWS Direct Connect 連線來實作此案例。如需詳細資訊，請參閱 AWS Direct Connect 使用者指南.

2. 測試您在上一個步驟建立的 AWS Site-to-Site VPN 連線。若要這樣做，請執行AWS Site-to-Site VPN 使用者指南中的測試 站台對站台 VPN 連接所述的步驟。如果 VPN 連接的運作符合預期，請繼續下一個步驟。
3. 在與 VPC 相同的區域中建立 用戶端 VPN 端點。若要這樣做，請執行建立 用戶端 VPN 端點 (p. 31)中所述的步驟。
4. 將您稍早所識別的子網路與 用戶端 VPN 端點建立關聯。若要這樣做，請執行將目標網路與 用戶端 VPN 端點建立關聯 (p. 36)中所述的步驟，然後選擇 VPC 和子網路。
5. 新增路由以允許存取 AWS Site-to-Site VPN 連線。若要這樣做，請執行建立端點路由 (p. 39)中所述的步驟；對於 Route destination (路由目的地)，輸入 AWS Site-to-Site VPN 連線的 IPv4 CIDR 範圍，對於 Target VPC Subnet ID (目標 VPC 子網路 ID)，選擇與 用戶端 VPN 端點相關聯的子網路。
6. 新增授權規則讓用戶端存取 AWS Site-to-Site VPN 連線。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟；對於 Destination network (目的地網路)，輸入 AWS Site-to-Site VPN 連線 IPv4 CIDR 範圍。

存取網際網路

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

如果您已完成用戶端 VPN 入門 (p. 26)教學課程，則您已實作此案例。



開始之前，請執行以下動作：

- 建立或識別至少具有一個子網路的 VPC。識別要與 用戶端 VPN 端點相關聯的 VPC 中的子網路，並記下其 IPv4 CIDR 範圍。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 和子網路。
- 識別與 VPC CIDR 不重疊的用戶端 IP 位址適當的 CIDR 範圍。
- 於 用戶端 VPN 的限制和規則 (p. 2) 檢閱 用戶端 VPN 端點的規則和限制。

實作此組態

1. 確定您將用於 用戶端 VPN 端點的安全群組允許進出網際網路的傳入與傳出流量。若要這樣做，請新增允許 HTTP 和 HTTPS 流量進出 0.0.0.0/0 的傳入與傳出流量規則。
2. 建立網際網路閘道，並將它連接至您的 VPC。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立和連接網際網路閘道。

3. 將網際網路閘道的路由新增到其路由表，以公開您的子網路。在 VPC 主控台，選擇 Subnets (子網路)，選取要與 用戶端 VPN 端點相關聯的子網路，選擇 Route Table (路由表)，然後選擇路由表 ID。選擇 Actions (動作)，選擇 Edit routes (編輯路由)，然後選擇 Add route (新增路由)。對於 Destination (目的地)，輸入 `0.0.0.0/0`，對於 Target (目標)，選擇上一個步驟中的網際網路閘道。
4. 在與 VPC 相同的區域中建立 用戶端 VPN 端點。若要這樣做，請執行建立 用戶端 VPN 端點 (p. 31)中所述的步驟。
5. 將您稍早所識別的子網路與 用戶端 VPN 端點建立關聯。若要這樣做，請執行將目標網路與 用戶端 VPN 端點建立關聯 (p. 36)中所述的步驟，然後選擇 VPC 和子網路。
6. 新增授權規則讓用戶端存取 VPC。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟；對於 Destination network to enable (要啟用的目的地網路)，輸入 VPC 的 IPv4 CIDR 範圍。
7. 新增路由以允許流向網際網路的流量。若要這樣做，請執行建立端點路由 (p. 39)中所述的步驟；對於 Route destination (路由目的地)，輸入 `0.0.0.0/0`，對於 Target VPC Subnet ID (目標 VPC 子網路 ID)，選擇與 用戶端 VPN 相關聯的子網路。
8. 新增授權規則讓用戶端存取網際網路。若要這樣做，請執行將授權規則新增到 用戶端 VPN 端點 (p. 38)中所述的步驟；對於 Destination network (目的地網路)，輸入 `0.0.0.0/0`。
9. 確定步驟 5 中子網路關聯的安全性群組具有允許網際網路存取的輸出規則 (目的地是 `0.0.0.0/0`)。

限制存取您的網路

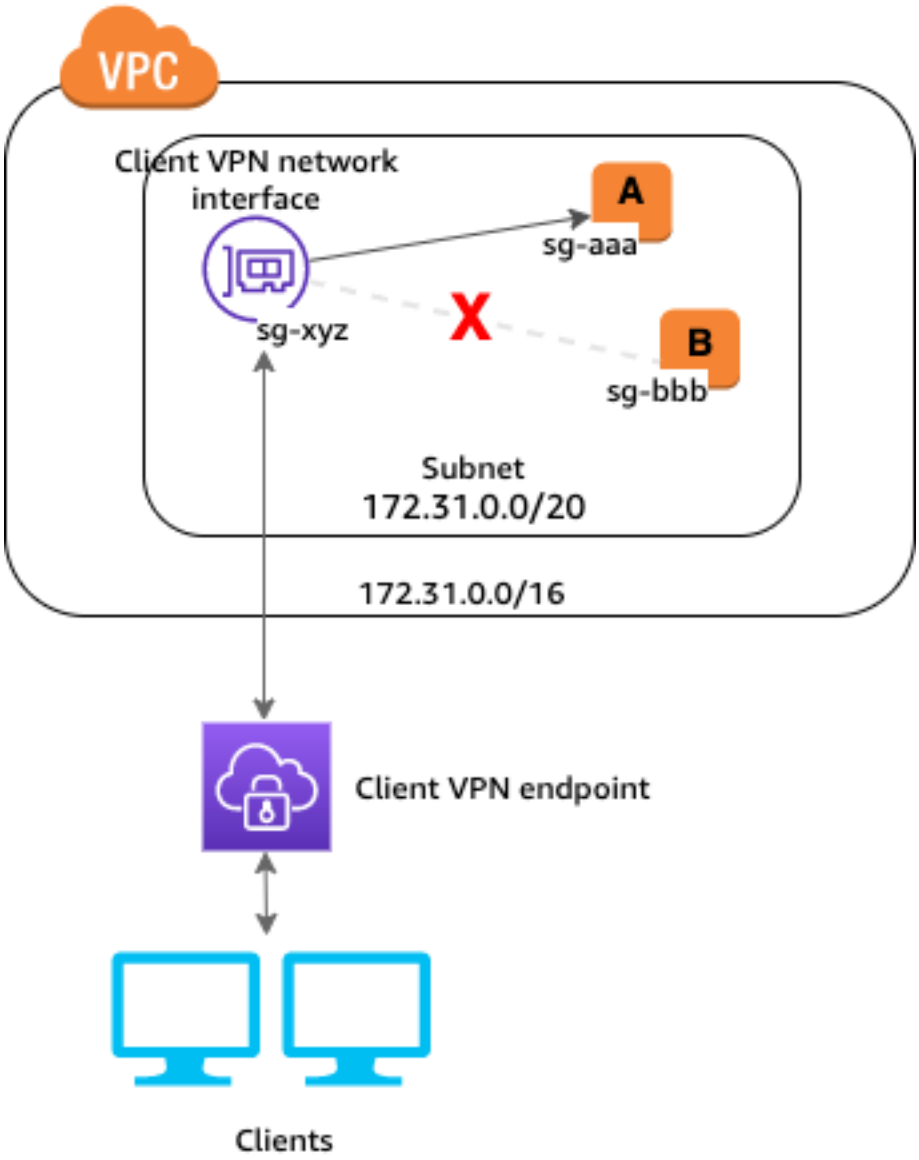
您可以設定 用戶端 VPN 端點，以限制對 VPC 中特定資源的存取。對於以使用者為基礎的驗證，您也可以根據存取 用戶端 VPN 端點的使用者群組，限制對網路部分的存取。

使用安全性群組限制存取

您可以透過新增或移除參考套用至目標網路關聯之安全群組 (用戶端 VPN 安全群組) 的安全群組規則，來授與或拒絕 VPC 中特定資源的存取權。此組態闡明存取 VPC (p. 16) 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性群組。然後，建立允許來自 用戶端 VPN 安全性群組的流量的規則。

在下列範例中，`sg-xyz` 是 用戶端 VPN 安全群組、安全群組 `sg-aaa` 會與執行個體 A 相關聯，以及安全群組 `sg-bbb` 會與執行個體 B 相關聯。您可以新增規則至 `sg-aaa` 以允許從 `sg-xyz` 存取，因此用戶端可以在執行個體 A。安全群組 `sg-bbb` 沒有允許從 `sg-xyz` 或 用戶端 VPN 網路介面存取的規則。用戶端無法存取執行個體 B 中的資源。



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

建立安全群組規則

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

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

檢查安全群組規則

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

根據使用者群組限制存取

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

1. 在 AWS Directory Service 或您的 IdP 中設定使用者和群組。如需詳細資訊，請參閱下列主題：
   - Active Directory 身份驗證 (p. 5)
   - SAML 型同盟驗證的需求和考量 (p. 11)
2. 為您的 用戶端 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 授權規則 (p. 37)。

如果您的 用戶端 VPN 端點設定為進行交互驗證，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。若要讓特定使用者群組存取您的網路的特定部分，您可以建立多個 用戶端 VPN 端點。例如，對於存取您網路的每個使用者群組，請執行下列動作：

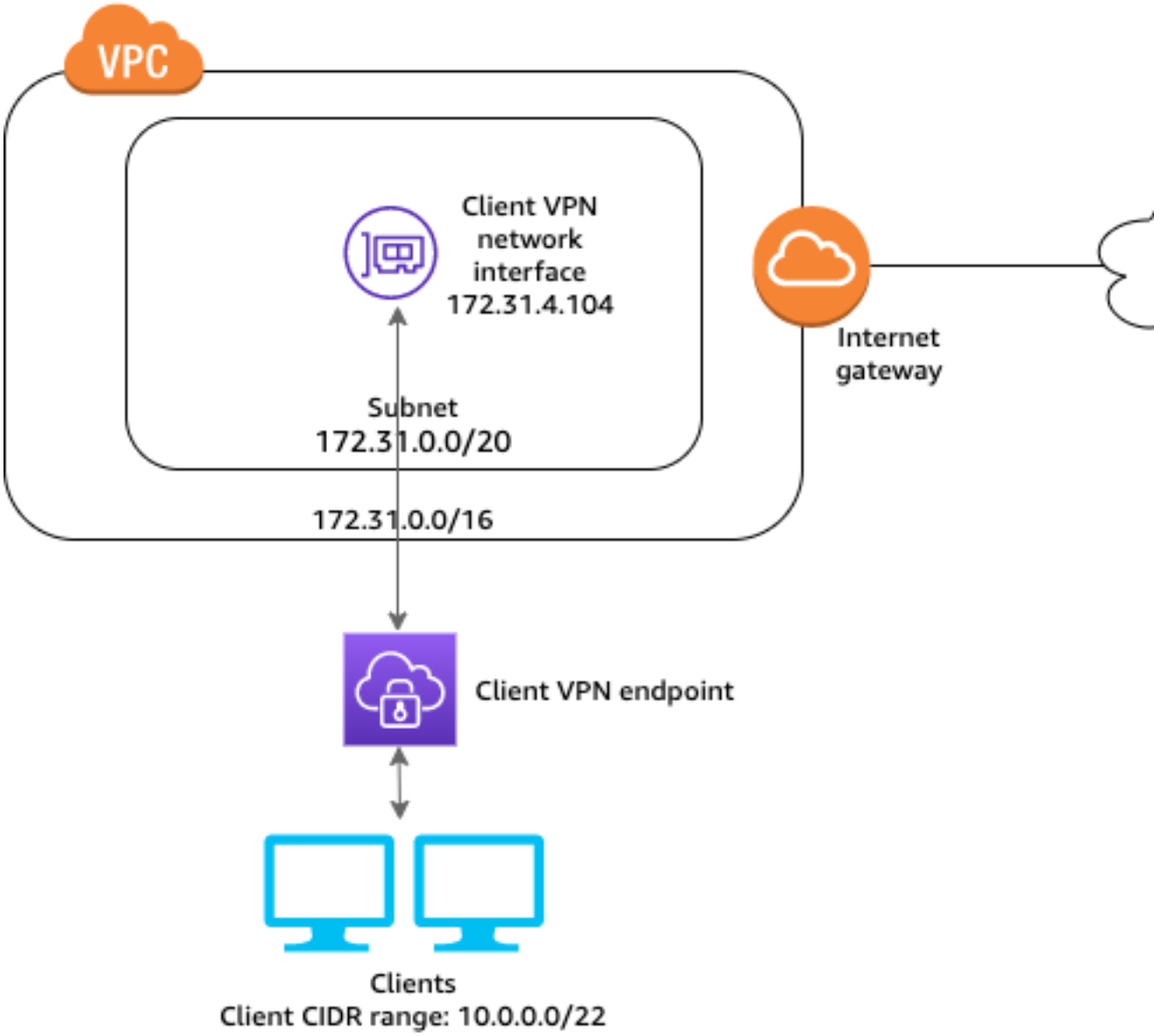
1. 為該使用者群組建立一組伺服器和用戶端憑證和金鑰。如需更多詳細資訊，請參閱 交互身份驗證 (p. 5)。
2. 建立 用戶端 VPN 端點。如需詳細資訊，請參閱 建立 用戶端 VPN 端點 (p. 31)。
3. 建立授權規則，授與全部或部分網路的存取權。例如，對於系統管理員所使用的 用戶端 VPN 端點，您可以建立授權規則來授與整個網路的存取權。如需詳細資訊，請參閱 將授權規則新增到 用戶端 VPN 端點 (p. 38)。

用戶端 VPN 入門

以下任務協助您熟悉 用戶端 VPN。在此教學課程中，您將建立一個會執行下列動作的 用戶端 VPN 端點：

- 提供所有用戶端對單一 VPC 的存取權。
- 提供所有用戶端存取網際網路。
- 使用交互身份驗證 (p. 5)。

以下圖表顯示完成此教學課程後，您的 VPC 和 用戶端 VPN 端點的組態。



步驟

- 先決條件 (p. 27)

先決條件

若要完成此入門教學課程，您需要以下項目：

- 使用 用戶端 VPN 端點所需的許可。
- 具有至少一個子網路和一個網際網路閘道的 VPC。與子網路相關聯的路由表必須具有通往網際網路閘道的路由。

步驟 1：產生伺服器和用戶端憑證及金鑰

此教學課程使用交互身分驗證。透過交互身份驗證，用戶端 VPN 使用憑證在用戶端和伺服器之間執行身份驗證。

如需產生伺服器和用戶端憑證及金鑰的詳細步驟，請參閱交互身份驗證 (p. 5)。

步驟 2：建立 用戶端 VPN 端點

當您建立 用戶端 VPN 端點時，您需要建立 VPN 建構，供用戶端連接以建立 VPN 連接。

建立 用戶端 VPN 端點

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)，然後選擇 Create 用戶端 VPN Endpoint (建立 用戶端 VPN 端點)。
3. (選用) 提供 用戶端 VPN 端點的名稱和說明。
4. 對於 Client IPv4 CIDR (用戶端 IPv4 CIDR)，以 CIDR 標記法指定 IP 地址範圍，以從中指派用戶端 IP 地址。例如，`10.0.0.0/22`。

   Note

   IP 地址範圍不可以與目標網路或任何將與 用戶端 VPN 端點相關聯的路由重疊。用戶端 CIDR 範圍必須有 /12 和 /22 之間的區塊大小，而且與 VPC CIDR 或路由表中的任何其他路由不重疊。建立 用戶端 VPN 端點後，您無法變更用戶端 CIDR。
5. 對於 Server certificate ARN (伺服器憑證 ARN)，指定要由伺服器使用的 TLS 憑證的 ARN。用戶端使用伺服器憑證來驗證它們所連接的 用戶端 VPN 端點。

   Note

   伺服器憑證必須佈建在 AWS Certificate Manager (ACM)。
6. 指定當用戶端建立 VPN 連接時，用來驗證用戶端的身分驗證方法。在此教學課程中，選擇使用交互驗證，然後針對用戶端憑證 ARN，指定您在步驟 1 (p. 27) 中產生之用戶端憑證的 ARN。
7. 對於您要記錄用戶端連線的詳細資訊嗎？，請選擇否。

8. 保留其他預設設定，並選擇建立 用戶端 VPN 端點。

如需建立 用戶端 VPN 端點時可以指定的其他選項的詳細資訊，請參閱 建立 用戶端 VPN 端點 (p. 31)。

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

步驟 3：為用戶端啟用 VPN 連接

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

將子網路與 用戶端 VPN 端點建立關聯

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選擇要與子網路建立關聯的 用戶端 VPN 端點，然後選擇 Associations (關聯)、Associate (建立關聯)。
4. 對於 VPC，選擇子網路所在的 VPC。如果您在建立 用戶端 VPN 端點時指定了 VPC，這必須是相同的 VPC。
5. 對於 Subnet to associate (要相關聯的子網路)，選擇要與 用戶端 VPN 端點建立關聯的子網路。
6. 選擇 Associate (建立關聯)。

   Note

   如果授權規則允許，一個子網路關聯就足以讓用戶端存取 VPC 的整個網路。您可以關聯其他子網路，以在其中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 用戶端 VPN 端點建立關聯時，會發生下列情況：

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

步驟 4：授權用戶端存取網路

若要授權用戶端存取相關聯的子網路所在的 VPC，您必須建立授權規則。授權規則指定哪些用戶端有權存取 VPC。在本教學課程中，我們將存取權授與所有使用者。

將授權規則新增至目標網路

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選擇要新增授權規則的 用戶端 VPN 端點，選擇 Authorization (授權)，然後選擇 Authorize Ingress (授權輸入)。
4. 若要啟用目的地網路，請輸入您要允許存取之網路的 CIDR。例如，若要允許存取整個 VPC，請指定 VPC 的 IPv4 CIDR 區塊。
5. 在授與存取權限中，選擇允許所有使用者存取權限。
6. 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)。

8. 確定 VPC 中資源的安全性群組具有允許從子網路關聯 (p. 28)的安全性群組存取的規則。這可讓您的用戶端存取 VPC 中的資源。如需詳細資訊，請參閱安全群組 (p. 12)。

步驟 5：(選用) 允許存取其他網路

您可以允許存取連接到 VPC 的其他網路，例如 AWS 服務、對等 VPC 和現場部署網路。對於每個額外的網路，您必須新增網路的路由，並設定授權規則將存取權給予用戶端。

在本教學課程中，我們新增網際網路的路由 (`0.0.0.0/0`)，並新增授權規則將存取權授與所有使用者。

啟用網際網路存取

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要新增路由的 用戶端 VPN 端點，選擇 Route Table (路由表)，然後選擇 Create Route (建立路由)。
4. 對於 Route destination (路由目的地)，輸入 `0.0.0.0/0`。對於 Target VPC Subnet ID (目標 VPC 子網路 ID)，指定路由傳送流量所經過的子網路的 ID。
5. 選擇 Create Route (建立路由)。
6. 選擇授權，然後選擇授權輸入。
7. 若要啟用目的地網路，請輸入 `0.0.0.0/0`，然後選擇允許所有使用者存取。
8. 選擇 Add authorization rule (新增授權規則)。
9. 確定與您路由流量所經過的子網路相關聯的安全群組允許進出網際網路的傳入與傳出流量。若要這樣做，請新增傳入和傳出規則，以允許往返於 `0.0.0.0/0` 的網際網路流量。

步驟 6：下載 用戶端 VPN 端點組態檔案

最後一個步驟是下載和準備 用戶端 VPN 端點組態檔案。組態檔案包含 用戶端 VPN 端點，以及建立 VPN 連接所需的憑證資訊。您必須提供此檔案給需要連接 用戶端 VPN 端點來建立 VPN 連接的用戶端。用戶端將這個檔案上傳到其 VPN 用戶端應用程式。

下載和準備 用戶端 VPN 端點組態檔案

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取 用戶端 VPN 端點，然後選擇下載用戶端設定。
4. 找出步驟 1 (p. 27) 中產生的用戶端憑證和金鑰。在複製的 OpenVPN easy-rsa 儲存庫的下列位置中，可以找到用戶端憑證和金鑰：
   - 用戶端憑證 — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - 用戶端金鑰 — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. 使用您偏好的文字編輯器開啟 用戶端 VPN 端點組態檔，並在 `<cert></cert>` 標籤與 `<key></key>` 標籤之間私密金鑰的內容之間新增用戶端憑證的內容。

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

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

6. 在 用戶端 VPN 端點 DNS 名稱前加上隨機字串。找出指定 用戶端 VPN 端點 DNS 名稱的行，並在其前面加上隨機字串，讓格式成為 *random_string.displayed_DNS_name*。例如：
   - 原始 DNS 名稱：`cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
   - 修改過的 DNS 名稱：`asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
7. 儲存並關閉 用戶端 VPN 端點組態檔案。
8. 將 用戶端 VPN 端點組態檔案分發給您的用戶端。

如需 用戶端 VPN 端點組態檔案的詳細資訊，請參閱 匯出和設定用戶端組態檔 (p. 33)。

步驟 7：連接至 用戶端 VPN 端點

您可以使用 AWS 提供的用戶端 或其他 OpenVPN 型用戶端應用程式連接到 用戶端 VPN 端點。如需詳細資訊，請參閱AWS Client VPN 使用者指南。

使用 用戶端 VPN

您可以透過 Amazon VPC 主控台或 AWS CLI 來使用 用戶端 VPN。

內容

用戶端 VPN 端點

所有用戶端 VPN 工作階段都以 用戶端 VPN 端點為終點。請設定 用戶端 VPN 端點來管理和控制所有用戶端 VPN 工作階段。

內容

建立 用戶端 VPN 端點

建立 用戶端 VPN 端點，讓您的用戶端建立 VPN 工作階段。

用戶端 VPN 必須在佈建所需目標網路的同一個 AWS 帳戶中建立。

必要條件

開始之前，請務必備妥下列項目：

- 檢閱用戶端 VPN 的限制和規則 (p. 2)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。如需更多詳細資訊，請參閱 身分驗證 (p. 5)。

建立 用戶端 VPN 端點 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)，然後選擇 Create 用戶端 VPN Endpoint (建立 用戶端 VPN 端點)。
3. (選用) 對於 Description (描述)，輸入 用戶端 VPN 端點的簡短描述。
4. 對於 Client IPv4 CIDR (用戶端 IPv4 CIDR)，以 CIDR 標記法指定 IP 地址範圍，以從中指派用戶端 IP 地址。
5. 對於 Server certificate ARN (伺服器憑證 ARN)，指定要由伺服器使用的 TLS 憑證的 ARN。用戶端使用伺服器憑證來驗證它們所連接的 用戶端 VPN 端點。

Note

伺服器憑證必須佈建在 AWS Certificate Manager (ACM)。

6. 指定當用戶端建立 VPN 連接時，用來驗證用戶端的身分驗證方法。您至少必須選取一個身份驗證方法。

   - 若要使用使用者型身份驗證，請選取 Use user-based authentication (使用使用者型身份驗證)，然後選擇下列其中一項：
     - Active Directory authentication (Active Directory 身份驗證)：為 Active Directory 身份驗證選擇此選項。針對 Directory ID (目錄 ID)，指定要使用的 Active Directory ID。
     - Federated authentication (同盟驗證)：為 SAML 型同盟驗證選擇此選項。若為 SAML provider ARN (SAML 提供者 ARN)，請指定 IAM SAML 身分提供者的 ARN。
   - 若要使用交互憑證驗證，請選取 Use mutual authentication (使用交互身分驗證)，然後對於 Client certificate ARN (用戶端憑證 ARN)，指定於 AWS Certificate Manager (ACM) 中佈建的用戶端憑證 ARN。

     Note

     如果用戶端憑證是由發行伺服器憑證的同一家憑證授權機構 (發行者) 所發行，則您可以繼續使用伺服器憑證 ARN 作為用戶端憑證 ARN。如果已為使用相同 CA 的每個使用者產生個別用戶端憑證和金鑰做為伺服器憑證，則可以使用伺服器憑證 ARN。

7. 指定是否使用 Amazon CloudWatch Logs 來記錄用戶端連線的相關資料。對於 Do you want to log the details on client connections? (您想要記錄用戶端連線的詳細資訊嗎？)，請執行以下其中一項：

   - 若要啟用用戶端連線的日誌記錄，請選擇 Yes (是)。針對 CloudWatch Logs log group name (CloudWatch Logs 日誌群組名稱)，請輸入要使用的日誌群組名稱。針對 CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱)，請輸入要使用的日誌串流名稱，或將此選項留白，讓我們為您建立日誌串流。
   - 若要停用用戶端連線的日誌記錄，請選擇 No (否)。

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

   Note

   請確定用戶端可以觸達 DNS 伺服器。

9. (選用) 若要讓端點成為分割通道 VPN 端點，請選取 Enable split-tunnel (啟用分割通道)。

   根據預設，VPN 端點上的分割通道會停用。

10. (選用) 在預設情況下，用戶端 VPN 伺服器使用 `UDP` 傳輸通訊協定。若要改用 `TCP` 傳輸通訊協定，對於 Transport Protocol (傳輸通訊協定)，請選擇 TCP。

    Note

    UDP 的效能通常比 TCP 更好。您無法在建立 用戶端 VPN 端點之後變更傳輸通訊協定。

11. (選用) 對於 VPC ID，請選擇要與 用戶端 VPN 端點關聯的 VPC。對於 Security Group IDs (安全群組識別碼)，請選擇一或多個要套用至 用戶端 VPN 端點的 VPC 安全群組。
12. (選用) 對於 VPN port (VPN 連接埠)，請選擇 VPN 連接埠號碼。預設為 443。
13. 選擇 Create 用戶端 VPN Endpoint (建立 用戶端 VPN 端點)。

建立 用戶端 VPN 端點之後，請執行下列動作以完成組態並讓用戶端連線：

- 用戶端 VPN 端點的最初狀態是 `pending-associate`。只有在您將第一個目標網路 (p. 36)相關聯之後，用戶端才能連線到 用戶端 VPN 端點。

- 建立授權規則 (p. 37)，以指定哪些用戶端具有網路的存取權。
- 下載並準備 用戶端 VPN 端點組態檔 (p. 33)，以散發給您的用戶端。
- 指示您的用戶端使用 AWS 提供的用戶端 或其他 OpenVPN 型用戶端應用程式連線到 用戶端 VPN 端點。如需詳細資訊，請參閱AWS Client VPN 使用者指南。

建立 用戶端 VPN 端點 (AWS CLI)

使用 create-client-vpn-endpoint 命令。

修改 用戶端 VPN 端點

建立 用戶端 VPN 之後，您可以修改下列任一設定：

- 描述
- 伺服器憑證
- 用戶端連線日誌記錄選項
- DNS 伺服器
- 分割通道選項
- VPC 和安全群組關聯
- VPN 連接埠號碼

在建立 用戶端 VPN 端點之後，您無法修改用戶端 IPv4 CIDR 範圍、身份驗證選項或傳輸通訊協定。

您可以使用主控台或 AWS CLI 來修改 用戶端 VPN 端點。

修改 用戶端 VPN 端點 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要修改的 用戶端 VPN 端點，選擇 Actions (動作)，然後選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。
4. 進行必要的變更，然後選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。

修改 用戶端 VPN 端點 (AWS CLI)

使用 modify-client-vpn-endpoint 命令。

匯出和設定用戶端組態檔

用戶端 VPN 端點組態檔案是供用戶端 (使用者) 用來與 用戶端 VPN 端點建立 VPN 連接的檔案。您必須下載 (匯出) 此檔案，並分發給所有需要存取 VPN 的用戶端。

如果您的 用戶端 VPN 端點使用交互身份驗證，您必須將用戶端憑證和用戶端私有金鑰新增至您下載的 .ovpn 組態檔案 (p. 34)。在您新增資訊之後，用戶端可以將 .ovpn 檔案匯入到 OpenVPN 用戶端軟體。

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

在預設情況下，OpenVPN 用戶端組態中的 “--remote-random-hostname” 選項支援萬用字元 DNS。由於萬用字元 DNS 已啟用，用戶端不會快取端點的 IP 地址，而您將無法以 Ping 偵測端點的 DNS 名稱。

如果您的 用戶端 VPN 端點使用 Active Directory 身份驗證，且在分發用戶端組態檔案之後，您在目錄上啟用 Multi-Factor Authentication (MFA)，則必須下載新檔案並將其重新分發至用戶端。用戶端無法使用先前的組態檔案來連線到 用戶端 VPN 端點。

匯出用戶端組態檔

您可以使用主控台或 AWS CLI 來匯出用戶端組態。

匯出用戶端組態 (主控台)

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

匯出用戶端組態 (AWS CLI)

使用 export-client-vpn-client-configuration 命令，並指定輸出檔案名稱。

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

新增用戶端憑證和金鑰資訊 (交互身份驗證)

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

新增用戶端憑證和金鑰資訊 (交互身份驗證)

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 用戶端 VPN 端點組態檔案一起分發給用戶端。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。以用戶端憑證和金鑰的位置取代 */path/* (位置是相對於連線至端點的用戶端)。

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

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

如果您為將連線至 用戶端 VPN 端點的每個使用者產生個別的用戶端憑證和金鑰，請針對每個使用者重複此步驟。

以下是 用戶端 VPN 組態檔案的格式範例，其中包含用戶端憑證和金鑰。

```
client
dev tun
proto udp
remote asdf.cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
persist-key
persist-tun
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
```

檢視 用戶端 VPN 端點

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

使用主控台來檢視 用戶端 VPN 端點

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選擇要檢視的 用戶端 VPN 端點。
4. 使用索引標籤來檢視相關聯的目標網路、授權規則、路由和用戶端連接。

使用 AWS CLI 來檢視 用戶端 VPN 端點

使用 describe-client-vpn-endpoints 命令。

刪除 用戶端 VPN 端點

當您刪除 用戶端 VPN 端點時，它的狀態會變更為 `deleting`，而且用戶端無法再連接它。您必須取消所有相關聯目標網路的關聯，才能刪除 用戶端 VPN 端點。

您可以使用主控台或 AWS CLI 來刪除 用戶端 VPN 端點。

刪除 用戶端 VPN 端點 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要刪除的 用戶端 VPN 端點，選擇 Actions (動作)，選擇 Delete 用戶端 VPN Endpoint (刪除 用戶端 VPN 端點)，然後選擇 Yes, Delete (是，刪除)。

刪除 用戶端 VPN 端點 (AWS CLI)

使用 delete-client-vpn-endpoint 命令。

目標網路

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

如需您可以設定之存取類型的詳細資訊 (例如讓用戶端存取網際網路)，請參閱 案例和範例 (p. 16)。

內容

將目標網路與 用戶端 VPN 端點建立關聯

您可以將一或多個目標網路 (子網路) 關聯至 用戶端 VPN 端點。

適用的規定如下：

- 子網路必須具有至少 /27 位元遮罩的 CIDR 區塊，例如 10.0.0.0/27。子網路也必須至少有 8 個可用的 IP 地址。
- 子網路的 CIDR 區塊不可與 用戶端 VPN 端點的用戶端 CIDR 範圍重疊。
- 如果您將多個子網路關聯至 用戶端 VPN 端點，則每個子網路必須位於不同的可用區域。我們建議您與至少兩個子網路建立關聯，來提供可用區域備援。
- 如果您在建立 用戶端 VPN 端點時指定了 VPC，則子網路必須位於相同的 VPC 中。如果您尚未將 VPC 與 用戶端 VPN 端點建立關聯，您可選擇任何 VPC 中的任何子網路。

  所有其他子網路關聯都必須來自相同的 VPC。若要從不同的 VPC 建立子網路關聯，您必須先修改 用戶端 VPN 端點並變更與其相關聯的 VPC。如需詳細資訊，請參閱修改 用戶端 VPN 端點 (p. 33)。

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

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

將目標網路與 用戶端 VPN 端點建立關聯 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要與目標網路建立關聯的 用戶端 VPN 端點，選擇 Associations (關聯)，然後選擇 Associate (建立關聯)。
4. 對於 VPC，選擇子網路所在的 VPC。如果您在建立 用戶端 VPN 端點時指定了 VPC，或者您有先前的子網路關聯，則它必須是相同的 VPC。
5. 對於 Subnet to associate (要相關聯的子網路)，選擇要與 用戶端 VPN 端點建立關聯的子網路。
6. 選擇 Associate (建立關聯)。

將目標網路與 用戶端 VPN 端點建立關聯 (AWS CLI)

使用 associate-client-vpn-target-network 命令。

將安全群組套用到目標網路

建立 用戶端 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 用戶端 VPN 端點建立關聯時，我們會自動套用相關聯子網路所在的 VPC 的預設安全群組。如需詳細資訊，請參閱安全群組 (p. 12)。

您可以變更 用戶端 VPN 端點的安全群組。您需要的安全群組規則，取決於您要設定的 VPN 存取種類。如需詳細資訊，請參閱案例和範例 (p. 16)。

將安全群組套用到目標網路 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要套用安全群組的 用戶端 VPN 端點。
4. 選擇 Security Groups (安全群組)，選取目前的安全群組，然後選擇 Apply Security Groups (套用安全群組)。
5. 在清單中選取新的安全群組，然後選擇 Apply Security Groups (套用安全群組)。

將安全群組套用到目標網路 (AWS CLI)

使用 apply-security-groups-to-client-vpn-target-network 命令。

取消目標網路與 用戶端 VPN 端點的關聯

如果您取消所有目標網路與 用戶端 VPN 端點的關聯，用戶端就無法再建立 VPN 連接。當您取消子網路的關聯時，我們會移除形成關聯時所自動建立的路由。

取消目標網路與 用戶端 VPN 端點的關聯 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取目標網路相關聯的 用戶端 VPN 端點，然後選擇 Associations (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 Yes, Disassociate (是，取消關聯)。

取消目標網路與 用戶端 VPN 端點的關聯 (AWS CLI)

使用 disassociate-client-vpn-target-network 命令。

檢視目標網路

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

檢視目標網路 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取 用戶端 VPN 端點，然後選擇 Associations (關聯)。

使用 AWS CLI 來檢視目標網路

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

授權規則

授權規則做為授與存取網路的防火牆規則。您要授與存取的每個網路都應該有授權規則。

內容

將授權規則新增到 用戶端 VPN 端點

透過新增授權規則，您可以授與特定的用戶端存取指定的網路。

您可以使用主控台和 AWS CLI 將授權規則新增到 用戶端 VPN 端點。

將授權規則新增到 用戶端 VPN 端點 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選擇要新增授權規則的 用戶端 VPN 端點，選擇 Authorization (授權)，然後選擇 Authorize ingress (授權輸入)。
4. 對於 Destination network (目的地網路)，請以 CIDR 標記法輸入您希望使用者存取的網路 IP 地址 (例如 VPC 的 CIDR 區塊)。
5. 指定允許哪些用戶端存取指定的網路。對於 For grant access to (將存取權授與)，請執行以下其中一項：

   - 若准許所有用戶端存取，請選擇 Allow access to all users (允許所有使用者存取)。
   - 若要限制特定用戶端的存取權，請選擇 Allow access to users in a specific access group (允許特定存取群組中使用者的存取權)，然後在 Access group ID (存取群組 ID) 中，輸入要授與存取權的群組 ID。例如，Active Directory 群組的安全性識別符 (SID)，或在 SAML 型身分提供者 (IdP) 中定義的群組 ID/名稱。

   Note

   (Active Directory) 若要取得 SID，您可以使用 Microsoft Powershell Get-ADGroup cmdlet，例如：

   ```
   Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
   ```

   或者，開啟 Active Directory 使用者和電腦工具，檢視群組的內容，移至「屬性編輯器」索引標籤，然後取得 `objectSID` 的值。如有必要，請先選擇檢視、進階功能以啟用「屬性編輯器」標籤。

   Note

   (SAML 型同盟驗證) 群組 ID/名稱應與 SAML 聲明中傳回的群組屬性資訊相符。
6. 對於 Description (描述)，輸入授權規則的簡短描述。
7. 選擇 Add authorization rule (新增授權規則)。

將授權規則新增到 用戶端 VPN 端點 (AWS CLI)

使用 authorize-client-vpn-ingress 命令。

從 用戶端 VPN 端點移除授權規則

透過刪除授權規則，您可以移除對指定網路的存取權。

您可以使用主控台和 AWS CLI 從 用戶端 VPN 端點移除授權規則。

從 用戶端 VPN 端點移除授權規則 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取已新增授權規則的 用戶端 VPN 端點，然後選擇 Authorization (授權)。
4. 選取要刪除的授權規則，選擇 Revoke ingress (撤銷輸入)，然後選擇 Revoke ingress (撤銷輸入)。

從 用戶端 VPN 端點移除授權規則 (AWS CLI)

使用 revoke-client-vpn-ingress 命令。

檢視授權規則

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

檢視授權規則 (主控台)

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

檢視授權規則 (AWS CLI)

使用 describe-client-vpn-authorization-rules 命令。

路由

每個 用戶端 VPN 端點都有路由表來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 用戶端 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。

當您將始於 VPC 的子網路與 用戶端 VPN 端點建立關聯時，VPC 的路由會自動新增到 用戶端 VPN 端點的路由表。若要允許存取其他網路，例如對等 VPC、內部部署網路和網際網路，您必須手動將路由新增到 用戶端 VPN 端點的路由表。

內容

AWS Client VPN 端點上分割通道的考量

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

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

建立端點路由

當您建立路由時，請指定如何引導目的地網路的流量。

若要允許用戶端存取網際網路，請新增目的地 `0.0.0.0/0` 路由。

您可以使用主控台和 AWS CLI 將路由新增到 用戶端 VPN 端點。

建立 用戶端 VPN 端點路由 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取要新增路由的 用戶端 VPN 端點，選擇 Route Table (路由表)，然後選擇 Create Route (建立路由)。
4. 對於 Route destination (路由目的地)，指定目的地網路的 IPv4 CIDR 範圍。例如：
   - 若要新增網際網路存取的路由，請輸入 `0.0.0.0/0`
   - 若要新增對等端 VPC 的路由，請輸入對等端 VPC 的 IPv4 CIDR 範圍。
   - 若要新增內部部署網路的路由，請輸入 AWS Site-to-Site VPN 連線的 IPv4 CIDR 範圍。
5. 對於 Target VPC Subnet ID (目標 VPC 子網路 ID)，選擇與 用戶端 VPN 端點相關聯的子網路。
6. 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 用戶端 VPN 端點路由 (AWS CLI)

使用 create-client-vpn-route 命令。

檢視端點路由

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

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 Endpoints (用戶端 VPN 端點)。
2. 選取要檢視路由的 用戶端 VPN 端點，然後選擇 Route Table (路由表)。

檢視 用戶端 VPN 端點路由 (AWS CLI)

使用 describe-client-vpn-routes 命令。

刪除端點路由

只能刪除您手動新增的路由。無法刪除您將子網路與 用戶端 VPN 端點建立關聯時所自動新增的路由。若要刪除自動新增的路由，您必須將始於 用戶端 VPN 端點來建立的子網路取消關聯。

您可以使用主控台或 AWS CLI 來刪除出自 用戶端 VPN 端點的路由。

刪除 用戶端 VPN 端點路由 (主控台)

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

刪除 用戶端 VPN 端點路由 (AWS CLI)

使用 delete-client-vpn-route 命令。

用戶端憑證撤銷清單

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

Note

如需有關產生伺服器和用戶端憑證及金鑰的詳細資訊，請參閱交互身份驗證 (p. 5)

內容

產生用戶端憑證撤銷清單

Linux/macOS

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

使用 OpenVPN easy-rsa 產生用戶端憑證撤銷清單

1. 將 OpenVPN easy-rsa 儲存庫複製到本機電腦。

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

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 client_certificate_name
$ ./easyrsa gen-crl
```

出現提示時，輸入 `yes`。

Windows

下列程序會使用 OpenVPN 軟體來產生用戶端撤銷清單。它假設您遵循使用 OpenVPN 軟體的步驟 (p. 5)來產生用戶端和伺服器憑證和金鑰。

產生用戶端憑證撤銷清單

1. 開啟命令提示，然後導覽至 OpenVPN 目錄。

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

2. 執行 `vars.bat` 檔案。

```
C:\> vars
```

3. 撤銷用戶端憑證並產生用戶端撤銷清單。

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

匯入用戶端憑證撤銷清單

您必須有可匯入的用戶端憑證撤銷清單檔案。如需有關產生用戶端憑證撤銷清單的詳細資訊，請參閱產生用戶端憑證撤銷清單 (p. 41)。

您可以使用主控台和 AWS CLI 來匯入用戶端憑證撤銷清單。

匯入用戶端憑證撤銷清單 (主控台)

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

匯入用戶端憑證撤銷清單 (AWS CLI)

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

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

匯出用戶端憑證撤銷清單

您可以使用主控台和 AWS CLI 來匯出用戶端憑證撤銷清單。

匯出用戶端憑證撤銷清單 (主控台)

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

匯出用戶端憑證撤銷 (AWS CLI)

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

用戶端連線

連線是用戶端已建立的 VPN 工作階段。用戶端成功連接到 用戶端 VPN 端點時，就表示已建立連線。

內容

- 終止用戶端連線 (p. 43)

查看用戶端連線

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

查看用戶端連線 (主控台)

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

查看用戶端連線 (AWS CLI)

使用 describe-client-vpn-connections 命令。

終止用戶端連線

當您終止用戶端連線時，VPN 工作階段會結束。

您可以使用主控台和 AWS CLI 來終止用戶端連線。

終止用戶端連線 (主控台)

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取用戶端連接的 用戶端 VPN 端點，然後選擇 Connections (連線)。
4. 選取要終止的連線，選擇 Terminate Connection (終止連線)，然後選擇 Terminate Connection (終止連線)。

終止用戶端連線 (AWS CLI)

使用 terminate-client-vpn-connections 命令。

使用連線日誌

您可以啟用新端點或現有 用戶端 VPN 端點的連線日誌，並開始擷取連線日誌。

在開始之前，您的帳戶中必須有一個 CloudWatch Logs 日誌群組。如需詳細資訊，請參閱 Amazon CloudWatch Logs User Guide 中的使用日誌群組和日誌串流。使用 CloudWatch Logs 需支付費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

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

啟用新 用戶端 VPN 端點的連線日誌記錄

當您使用主控台或命令列建立新 用戶端 VPN 端點時，可以啟用連線日誌記錄。

使用主控台啟用新 用戶端 VPN 端點的連線日誌記錄

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)，然後選擇 Create 用戶端 VPN Endpoint (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。如需關於選項的詳細資訊，請參閱 建立 用戶端 VPN 端點 (p. 31)。
4. 對於 Do you want to log the details on client connections? (您要記錄用戶端連線的詳細資訊嗎？)，請選擇 Yes (是)。
5. 對於 CloudWatch Logs log group name (CloudWatch Logs 日誌群組名稱)，請選擇 CloudWatch Logs 日誌群組的名稱。
6. (選用) 對於 CloudWatch Logs log stream name (CloudWatch Logs 日誌串流名稱)，請選擇 CloudWatch Logs 日誌串流的名稱。
7. 選擇 Create Client VPN Endpoint (建立用戶端 VPN 端點)。

使用 AWS CLI 啟用新 用戶端 VPN 端點的連線日誌記錄

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

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

啟用現有 用戶端 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 用戶端 VPN 端點的連線日誌記錄。

使用主控台啟用現有 用戶端 VPN 端點的連線日誌記錄

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取 用戶端 VPN 端點，選擇 Actions (動作)，然後選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。
4. 對於 Connection Logging (連線記錄日誌)，請選擇 Yes (是)，然後執行下列動作：
   - 對於 CloudWatch Log Group (CloudWatch 日誌群組)，請選擇 CloudWatch Logs 日誌群組的名稱。
   - (選用) 對於 CloudWatch Log Stream (CloudWatch 日誌串流)，請選擇 CloudWatch Logs 日誌串流的名稱。
5. 選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。

使用 AWS CLI 啟用現有 用戶端 VPN 端點的連線日誌記錄

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

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

檢視連線日誌

您可以使用 CloudWatch Logs 主控台檢視連線日誌。

使用主控台檢視連線日誌

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

   Note

   Timestamp (時間戳記) 欄會顯示連線日誌發佈到 CloudWatch Logs 的時間，而非連線時間。

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

停用連線日誌記錄

您可以使用主控台或命令列停用 用戶端 VPN 端點的連線日誌記錄。當您停用連線日誌記錄時，CloudWatch Logs 不會刪除現有的連線日誌。

使用主控台來停用連線日誌記錄

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中選擇 用戶端 VPN Endpoints (用戶端 VPN 端點)。
3. 選取 用戶端 VPN 端點，選擇 Actions (動作)，然後選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。
4. 針對 Connection Logging (連線日誌記錄)，選擇 No (否)。
5. 選擇 Modify 用戶端 VPN Endpoint (修改 用戶端 VPN 端點)。

使用 AWS CLI 停用連線日誌記錄

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

用戶端 VPN 的 Identity and Access Management

AWS 使用安全登入資料來識別您並授予您對 AWS 資源的存取權。您可以使用 AWS Identity and Access Management (IAM) 的功能，來允許其他使用者、服務和應用程式完整地或有所限制地使用您的 AWS 資源，而不共用您的安全登入資料。

預設情況下，IAM 使用者沒有可建立、檢視或修改 AWS 資源的許可。若要允許 IAM 使用者存取資源 (例如用戶端 VPN 端點) 和執行任務，您必須建立 IAM 政策。此政策必須准許 IAM 使用者使用他們所需的特定資源和 API 動作。然後，將政策連接到 IAM 使用者所屬的 IAM 使用者或群組。將政策連接至使用者或使用者群組時，此政策會允許或拒絕使用者對特定資源執行特定任務。

例如，下列政策會啟用唯讀存取權。使用者可以檢視 用戶端 VPN 端點及其元件，但無法建立、修改或刪除它們。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeClientVpnEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

您也可以使用資源層級許可來限制使用者在呼叫 用戶端 VPN 動作時可以使用的資源。例如，下列政策允許使用者使用 用戶端 VPN 端點，但僅限具有標籤 `purpose=test` 的 用戶端 VPN 端點。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteClientVpnEndpoint",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:CreateClientVpnRoute",
                "ec2:DeleteClientVpnRoute",
                "ec2:RevokeClientVpnIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
```

```
                }
            }
        }
    ]
}
```

如需 IAM 的詳細資訊，請參閱 IAM 使用者指南。如需 Amazon EC2 動作清單，包括 用戶端 VPN 動作，請參閱IAM 使用者指南中的Amazon EC2 的動作、資源與條件鍵。

如需連接至 用戶端 VPN 端點的身份驗證和授權的詳細資訊，請參閱用戶端身份驗證和授權 (p. 4)。

監控 用戶端 VPN

監控是維護 AWS Client VPN 與其他 AWS 解決方案之可靠性、可用性和效能的重要手段。您可以使用以下功能來監控 用戶端 VPN 端點、分析流量模式，以及排除 用戶端 VPN 端點的問題。

Amazon CloudWatch

即時監控您的 AWS 資源和您在 AWS 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀表板和設定通知您的警示，或在特定指標達到您指定的閾值時採取動作。例如，您可以使用 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWS CloudTrail

擷取由您的 AWS 帳戶或代表它所發出的 API 呼叫和相關事件，並將日誌檔案傳送至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 AWS CloudTrail User Guide。

Amazon CloudWatch Logs

可讓您監控對 AWS Client VPN 端點進行的連線嘗試。您可以檢視 用戶端 VPN 連接的連線嘗試和連線重設。對於連線嘗試，您可以看到成功和失敗的連線嘗試。您可以指定 CloudWatch Logs 日誌串流記錄連線詳細資訊。如需詳細資訊，請參閱 Amazon CloudWatch Logs User Guide。

Amazon CloudWatch

AWS Client VPN 會將下列指標發佈至您 用戶端 VPN 端點的 Amazon CloudWatch。指標每五分鐘發佈一次到 Amazon CloudWatch。

指標	描述
ActiveConnectionsCount	連至 用戶端 VPN 端點的作用中連線數目。 單位：計數
AuthenticationFailures	用戶端 VPN 端點的身份驗證失敗次數。 單位：計數
EgressBytes	用戶端 VPN 端點傳送的位元組數量。 單位：位元組
EgressPackets	從 用戶端 VPN 端點傳送的封包數目。 單位：計數
IngressBytes	用戶端 VPN 端點接收的位元組數量。 單位：位元組
IngressPackets	用戶端 VPN 端點接收的封包數量。 單位：計數

您可以依端點篩選 用戶端 VPN 端點的指標。

CloudWatch 可讓您以一組有序的時間序列資料來擷取這些資料點的相關統計資料，也就是指標。將指標視為要監控的變數，而資料點是該變數在一段時間內的值。每個資料點都有相關聯的時間戳記和可選的測量單位。

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

如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWS CloudTrail

AWS Client VPN 是與 AWS CloudTrail 整合的一種服務，可提供由使用者、角色或 AWS 服務在 用戶端 VPN 中所採取動作的記錄。CloudTrail 會將 用戶端 VPN 的所有 API 呼叫當做事件擷取。擷取的呼叫包括從 用戶端 VPN 主控台進行的呼叫，以及針對 用戶端 VPN API 操作的程式碼呼叫。如果您建立追蹤，就可以持續傳送 CloudTrail 事件至 Amazon S3 儲存貯體，包括 用戶端 VPN 的事件。如果您不設定追蹤，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。使用由 CloudTrail 收集的資訊，以判斷對 用戶端 VPN 提出的請求、發出請求 IP 地址、請求者、提出請求的時間，以及其他詳細資訊。

如需 CloudTrail 的詳細資訊，請參閱 AWS CloudTrail User Guide。

CloudTrail 中的 用戶端 VPN 資訊

當您建立帳戶時，系統會在您的 AWS 帳戶中啟用 CloudTrail。當 用戶端 VPN 中發生活動時，該活動會記錄在 CloudTrail 事件中，其他 AWS 服務事件則記錄於 Event history (事件歷史記錄)。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

若要持續記錄 AWS 帳戶中的事件 (包括 用戶端 VPN 的事件)，請建立追蹤。追蹤記錄可讓 CloudTrail 將日誌檔案交付到 Amazon S3 儲存貯體。依預設，當您在主控台建立追蹤時，該追蹤會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有 用戶端 VPN 動作由 CloudTrail 記錄，並記載於 Amazon EC2 API Reference中。例如，對 `CreateClientVpnEndpoint`、`AssociateClientVpnTargetNetwork` 及 `AuthorizeClientVpnIngress` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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

- 該請求是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全登入資料。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 用戶端 VPN 日誌檔項目

追蹤記錄是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。事件代表從任何來源的單一請求，並包含有關請求的動作、動作的日期和時

間、請求參數等資訊。CloudTrail 日誌檔不是公有 API 呼叫的排序堆疊追蹤記錄，因此不會現以任何特定順序顯示。

AWS Client VPN 配額

您的 AWS 帳戶具有下列與 用戶端 VPN 端點相關的配額。您可以對一部分配額請求提高限制。

用戶端 VPN 配額

- 每個區域的 用戶端 VPN 端點數量：5
- 每個 用戶端 VPN 端點的授權規則數量：50
- 每個 用戶端 VPN 端點的路由數量：10
- 每個 用戶端 VPN 端點的並行用戶端連線數：2000
- 每個 用戶端 VPN 端點的並行操作數目：10

  這些操作包含：
  - 關聯或取消關聯子網路
  - 建立或刪除路由
  - 建立或刪除傳入和傳出規則
  - 建立或刪除安全群組

使用者和群組配額

當您為使用中的目錄或 SAML 型 IdP 設定使用者和群組時，系統會套用下列配額：

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

一般考量

使用 用戶端 VPN 端點時，請考慮下列事項：

- 如果您使用 Active Directory 身份驗證使用者，則 用戶端 VPN 端點必須與 Active Directory 驗證所用 AWS Directory Service 資源屬於相同的帳戶。
- 如果您使用 SAML 型同盟驗證來驗證使用者身分，則 用戶端 VPN 端點必須與您建立之 IAM SAML 身分提供者屬於相同的帳戶，以定義 IdP 對 AWS 的信任關係。IAM SAML 身分提供者可以在相同 AWS 帳戶中的多個 用戶端 VPN 端點之間共用。

對 用戶端 VPN 進行故障診斷

以下主題可協助您對 用戶端 VPN 端點可能發生的問題進行故障診斷。

如需有關故障診斷用戶端用來連接至 用戶端 VPN 之 OpenVPN 軟體的詳細資訊，請參閱AWS Client VPN 使用者指南中的對您的 用戶端 VPN 連接進行故障診斷。

常見問題

無法解析 用戶端 VPN 端點 DNS 名稱

問題

我無法解析 用戶端 VPN 端點的 DNS 名稱。

原因

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

解決方案

使用您偏好的文字編輯器開啟 用戶端 VPN 端點組態檔案。找出指定 用戶端 VPN 端點 DNS 名稱的行，並在其前面加上隨機字串，讓格式成為 *`random_string.displayed_DNS_name`*。例如：

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

流量不會在子網路之間分割

問題

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

原因

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

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

例如，假設您設定下列子網路關聯和路由：

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

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

解決方案

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

Active Directory 群組的授權規則未如預期般運作

問題

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

原因

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

例如，假設您以下列順序建立三個授權規則：

- 規則 1：群組 1 可存取 `10.1.0.0/16`
- 規則 2：群組 1、群組 2 和群組 3 可存取 `0.0.0.0/0`
- 規則 3：群組 2 可存取 `172.131.0.0/16`

在此範例中，規則 2 將於最後評估。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 3，則所有三個群組都可以存取所有網路。

此外，評估授權規則時，用戶端 VPN 會使用最長字首比對。

解決方案

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

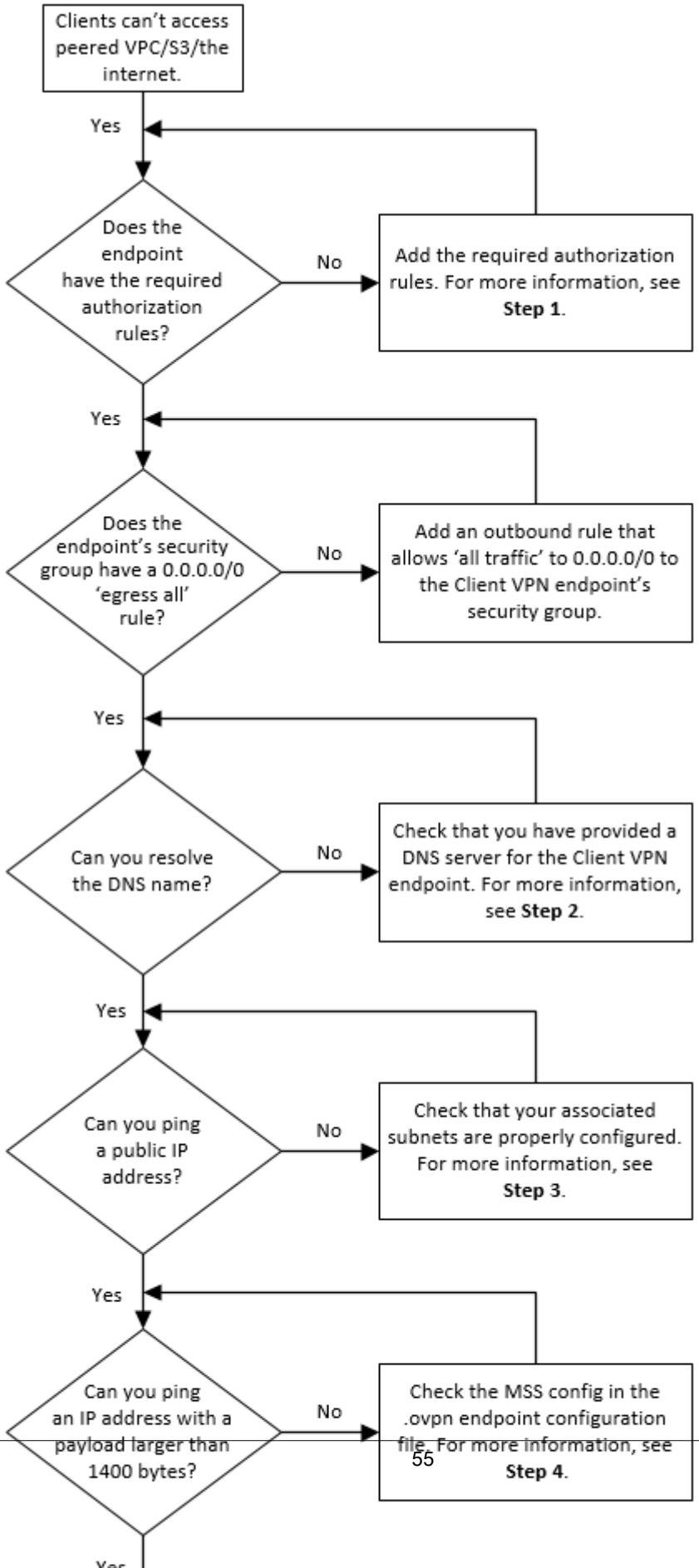
用戶端無法存取對等 VPC、Amazon S3 或網際網路

問題

我已經正確設定 用戶端 VPN 端點路由，但我的用戶端無法存取對等 VPC、Amazon S3 或網際網路。

解決方案

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


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

1. 若要存取網際網路，請新增 `0.0.0.0/0` 的授權規則。

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

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

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

   如果不確定要為 DNS 伺服器指定哪個 IP 位址，請在 VPC 中的 .2 IP 位址指定 VPC DNS 解析程式。
3. 對於網際網路存取，請檢查您是否能夠 ping 公用 IP 位址或公用網站，例如 `amazon.com`。如果您沒有收到回應，請確定關聯子網路的路由表具有預設路由，其以網際網路閘道或 NAT 閘道為目標。如果預設路由已存在，請確認關聯的子網路沒有會封鎖傳入和傳出流量的網路存取控制清單規則。

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

   如果您無法連上 Amazon S3，請確認關聯子網路的路由表具有閘道 VPC 端點的路由項目。
4. 檢查您是否可以使用大於 1400 位元組的承載 ping 公有 IP 地址。請使用下列其中一個命令：

   - Windows

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

   - Linux

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

   如果您無法使用大於 1400 位元組的承載 ping IP 地址，請使用您偏好的文字編輯器開啟 用戶端 VPN 端點 `.ovpn` 組態檔案，然後新增下列項目。

   ```
   mssfix 1328
   ```

對等 VPC、Amazon S3 或網際網路的存取斷斷續續

問題

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

原因

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

解決方案

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

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

- 路由 1：`0.0.0.0/0` 用於子網路 A

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

用戶端軟體傳回 TLS 錯誤

問題

我曾經能夠成功地將我的用戶端連接到 用戶端 VPN，但現在基於 OpenVPN 的用戶端在嘗試連接時返回以下錯誤：

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

可能原因

如果您使用交互身份驗證並匯入用戶端憑證撤銷清單，則用戶端憑證撤銷清單可能已過期。在身份驗證階段期間，用戶端 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，您就無法連接到 用戶端 VPN 端點。

或者，用戶端用來連線到 用戶端 VPN 的 OpenVPN 型軟體可能發生問題。

解決方案

使用 OpenSSL 工具檢查用戶端憑證撤銷清單的到期日。

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

輸出會顯示到期日期和時間。如果用戶端憑證撤銷清單已過期，您必須建立新的清單並將其匯入 用戶端 VPN 端點。如需詳細資訊，請參閱用戶端憑證撤銷清單 (p. 41)。

如需有關故障診斷 OpenVPN 型軟體的詳細資訊，請參閱AWS Client VPN 使用者指南中的對您的 用戶端 VPN 連接進行故障診斷。

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

問題

我的 用戶端 VPN 端點使用 Active Directory 身份驗證，以前能夠成功地將我的用戶端連接到 用戶端 VPN。但是現在，用戶端取得無效的使用者名稱和密碼錯誤。

可能原因

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

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
```

如需更多詳細資訊，請參閱 匯出和設定用戶端組態檔 (p. 33)。測試您的 Active Directory 的 MFA 組態，而不使用 用戶端 VPN 端點來確認 MFA 是否如預期般運作。

用戶端無法連線 (交互身份驗證)

問題

我的 用戶端 VPN 端點使用交互身份驗證。用戶端取得 TLS 金鑰交涉失敗錯誤和逾時錯誤。

可能原因

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

解決方案

確定組態檔案包含正確的用戶端憑證和金鑰。如有必要，請修正組態檔案並將其重新分發給您的用戶端。如需更多詳細資訊，請參閱 匯出和設定用戶端組態檔 (p. 33)。

用戶端傳回的登入資料超過大小上限錯誤 (同盟驗證)

問題

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

原因

IdP 傳回的 SAML 回應超過支援的大小上限。如需更多詳細資訊，請參閱 SAML 型同盟驗證的需求和考量 (p. 11)。

解決方案

請嘗試減少 IdP 中使用者所屬的群組數目，然後再試一次連線。

用戶端無法開啟瀏覽器 (同盟驗證)

問題

我將同盟驗證用於 用戶端 VPN 端點。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 (p. 33)、將它匯入到 AWS 提供的用戶端，然後再試一次連線。

用戶端傳回沒有可用的連接埠錯誤 (同盟驗證)

問題

我將同盟驗證用於 用戶端 VPN 端點。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 才能完成身份驗證。如需詳細資訊，請參閱 SAML 型同盟驗證的需求和考量 (p. 11)。

解決方案

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

文件歷史記錄

下表說明《AWS Client VPN 管理員指南》的更新。

update-history-change	update-history-description	update-history-date
SAML 2.0 型同盟驗證	您可以使用 SAML 2.0 型同盟驗證來驗證 用戶端 VPN 使用者。	May 19, 2020
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。	March 5, 2020
可設定的 VPN 連接埠	您可以為 AWS Client VPN 端點指定支援的 VPN 連接埠號碼。	January 16, 2020
支援 Multi-Factor Authentication (MFA)	如果已為 Active Directory 啟用 MFA，則您的 AWS Client VPN 端點支援 MFA。	September 30, 2019
支援分割通道	您可以在 AWS Client VPN 端點上啟用分割通道。	July 24, 2019
初始版本 (p. 60)	此版本推出 AWS Client VPN。	December 18, 2018