使用者指南

AWS 客戶 VPN

AWS 客戶 VPN: 使用者指南

Table of Contents

什麼是 AWS 客戶VPN？

AWS Client VPN 是受管用戶端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。

本指南提供使用裝置上的用戶端應用程式建立與 Client VPN 端點之間的VPN連線的步驟。

用戶端VPN元件

以下是使用 AWS 客戶端的關鍵組件VPN。

- 用戶端VPN端點 — 您的用戶端VPN管理員會在中建立並設定用戶VPN端端點。 AWS您的管理員控制當您建立VPN連線時，您可以存取哪些網路和資源。
- VPN用戶端應用程式 — 您用來連線到 Client VPN 端點並建立安全VPN連線的軟體應用程式。
- 用戶VPN端端點組態檔案 — 用戶端VPN管理員提供給您的組態檔案。此檔案包含用戶VPN端端點的相關資訊，以及建立VPN連線所需的憑證。您將此檔案載入您選擇的用VPN戶端應用程式。

設定用戶端的其他資源 VPN

如果您是用戶端VPN管理員，請參閱《AWS Client VPN 管理手冊》，以取得有關建立和設定 Client VPN 端點的詳細資訊。

開始使用 AWS Client VPN

您的用戶端VPN管理員必須先建立並設定 Client VPN 端點，才能建立VPN工作階段。您的管理員控制當您建立VPN工作階段時，您可以存取哪些網路和資源。然後，您可以使用用VPN戶端應用程式連線到 Client VPN 端點並建立安全VPN連線。

如果您是需要建立用戶VPN端端點的管理員，請參閱《AWS Client VPN 管理員指南》。

主題

使用用戶端的先決條 VPN

若要建立VPN連線，您必須具備下列條件：

- 存取網際網路
- 支援的裝置
- 對SAML於使用聯合驗證 (單一登入) 的用戶VPN端端點，請使用下列其中一種瀏覽器：
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

步驟 1：取得用VPN戶端應用程式

您可以VPN連線到 Client VPN 端點，並使用 AWS 提供的用戶端或其他開放式用戶端應用程VPN式建立連線。

所 AWS 提供的客戶端支持視窗, macOS, Ubuntu 18.04LTS, 和 Ubuntu 20. LTS 04.

視管理員是否為VPN應用程式建立端點組態檔案而定，您可以透過下列兩種方法之一下載用戶端應用程式：

- 如果您的管理員未設定端點組態檔案，請從「用戶端下載」下VPN載並安裝AWS 用戶端。下載並安裝應用程式後，請繼續the section called “步驟 2：取得用戶端VPN端點設定檔”向管理員取得端點組態檔案。
- 如果您的管理員已預先設定端點組態檔案，您可以從自助入口網站下載 Client VPN 應用程式及組態檔案。如需從自助入口網站下載用戶端和組態檔案的步驟，請參閱the section called “下載用戶端VPN”。下載並安裝應用程式和檔案後，移至the section called “步驟 3：Connect 到 VPN”。

或者，您也可以在要建立VPN連線的裝置上下載並安裝 Open 用VPN戶端應用程式。

步驟 2：取得用戶端VPN端點設定檔

您可以從系統管理員取得用戶VPN端端點設定檔案。組態檔案包含用戶VPN端端點的相關資訊，以及建立VPN連線所需的憑證。

或者，如果您的用戶端VPN管理員已為 Client VPN 端點設定自助入口網站，您可以自行下載所 AWS 提供用戶端的最新版本和最新版本的 Client VPN 端點設定檔案。如需詳細資訊，請參閱AWS Client VPN 從自助服務入口網站下載。

步驟 3：Connect 到 VPN

將用戶VPN端端點組態設定檔匯入 AWS 提供的用戶端或您的開啟用VPN戶端應用程式，然後連線到 VPN. 如需連線到的步驟VPN，包括匯入端點組態檔案，請參閱下列主題：

- 使用提供的用戶VPN端 Connect 到用 AWS 戶端端點
- 使用開放式用戶VPN端 Connect 到用VPN戶端端點

對於使用 Active Directory 驗證的用戶VPN端端點，系統會提示您輸入使用者名稱和密碼。如果目錄已啟用多因素驗證 (MFA)，系統也會提示您輸入驗證MFA碼。

對SAML於使用聯合驗證 (單一登入) 的用戶VPN端端點， AWS 提供的用戶端會在您的電腦上開啟瀏覽器視窗。系統會提示您輸入公司認證，然後才能連線到 Client VPN 端點。

AWS Client VPN 從自助服務入口網站下載

自助入口網站是一個網頁，可讓您下載最新版本的 AWS 用戶端和用戶VPN端端點設定檔的最新版本。如果您的 Client VPN 端點管理員已預先設定用戶端用戶VPN端的組態檔案，您可以從此入口網站下載並安裝該VPN用戶端應用程式以及設定檔。

> **Note**
>
> 如果您是系統管理員，且想要設定自助入口網站，請參閱《AWS Client VPN 管理員指南》中的用戶VPN端端點。

開始之前，您必須具有用戶VPN端端點的 ID。您的用戶VPN端端點管理員可以為您提供 ID，也可以為您提供包含 ID URL 的自助入口網站。

存取自助式入口網站

1. 前往 https://self-service.clientvpn.amazonaws.com/ 的自助服務入口網站，或使URL用管理員提供給您的服務。
2. 如有必要，請輸入用戶端VPN端點的 ID，例如`cvpn-endpoint-0123456abcd123456`。選擇 Next (下一步)。
3. 輸入您的使用者名稱和密碼，然後選擇 Sign in (登入)。這與您用來連線至用戶VPN端端點的使用者名稱和密碼相同。
4. 在自助式入口網站中，您可以執行下列動作：
   - 下載用戶端端點的最新版本用戶VPN端組態檔案。
   - 為您的平台下載 AWS 所提供的客戶端的最新版本。

使用提供的用戶VPN端 Connect 到用 AWS 戶端端點

您可以使用 AWS 提供的用戶VPN端連線到用戶端端點。所 AWS 提供的客戶端支持視窗, macOS, Ubuntu 18.04LTS, 和 Ubuntu 20. LTS 04.

用戶端

- AWS Client VPN 適用於視窗
- AWS Client VPN 適用於 macOS
- AWS Client VPN 對於 Linux

開放式VPN指令

AWS 提供的客戶端支持以下 Open VPN 指令：

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- 用戶端
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive
- 金鑰

- nobind
- persist-key
- persist-tun
- ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- 路由
- route-ipv6
- server-poll-timeout
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN 適用於視窗

這些章節說明如何使用 AWS 提供的 Windows 用戶端建立VPN連線。您可以在用戶端下載時下VPN載並安裝AWS 用戶端。 AWS 提供的用戶端不支援自動更新。

要求

若要使用 Windows AWS 提供的用戶端，必須具備下列條件：

- 視窗 10 或視窗 11（64 位操作系統，x64 處理器）
- 。 NET框架 4.7.2 或更高版本

用戶端會在您的電腦上保留TCP連接埠 8096。對SAML於使用聯合驗證 (單一登入) 的用戶VPN端端點，用戶端會保留TCP連接埠 35001。

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

主題

- VPN使用 AWS 提供的 Windows 用戶端連 Connect 到用戶端
- AWS Client VPN 適用於視窗版本說明

VPN使用 AWS 提供的 Windows 用戶端連 Connect 到用戶端

開始之前，請務必先詳閱需求。在下列步驟中， AWS 提供的AWS VPN 用戶端也稱為「用戶端」。

若要使用 AWS 提供的視窗用戶端進行連線

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。
5. 針對「VPN組態檔案」，瀏覽至您從用戶端VPN管理員收到的組態檔案，然後選擇「新增設定檔」。
6. 在 AWS VPN Client 視窗中，確定已選取您的設定檔，然後選擇 Connect (連接)。如果 Client VPN 端點已設定為使用憑證型驗證，系統會提示您輸入使用者名稱和密碼。
7. 若要檢視連線的統計資料，請選擇 Connection (連線)、Show Details (顯示詳細資料)。
8. 若要中斷連接，請在 AWS VPN Client 視窗中選擇 Disconnect (中斷連接)。或者，選擇 Windows 工作列上的用戶端圖示，然後選擇 Disconnect (中斷連接)。

AWS Client VPN 適用於視窗版本說明

下表包含 Windows 目前和舊版的 AWS Client VPN 版本說明和下載連結。

> **Note**
>
> 我們會繼續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版可能受到可用性和/或安全性問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載鏈接和 SHA256
3.14.0	• 增加了對`tap-sleep` 打開標VPN誌的支持。 • 更新了「打開」VPN 和「打開」SSL 庫。	2024年8月12日	下載版本 SHA256：812fb2f6d263288c664d598f6bd70e3f601d11dcbe63b281b0a96b96354516
3.13.0	更新了「打開」VPN 和「打開」SSL 庫。	2024年7月29日	下載版本 SHA256：C9cc896e81a7a7a4507c53337fb5ec64c64d5ec64d522c29388b
3.12.1	修正 Windows 用戶端 3.12.0 版無法為某些使用者建立VPN連線的問題。	2024年7月18日	下載版本 SHA256：5ed34e6c03A281e625acdA696c670364a9e5846CA697e05DB
3.12.0	• 區域網路範圍變更時自動重新連線。	2024年5月21 日	不再支援

版本	改變	日期	下載鏈接和 SHA256
	• 移除與端點連線時的自動應用程式焦SAML點。		
3.11.2	解決了自 123 版以來基於 Chromium 的瀏覽器的SAML身份驗證問題。	2024年4月11日	下載版本 SHA256：八八八八八八八八八八八八八八八八八 f8a6d4d4b cd8f8fc7cc
3.11.1	• 修正緩衝區溢位動作，此動作可能允許本機 actor 以提升的權限執行任意命令。 • 改善安全狀態。	2024年2月16日	下載版本 SHA256：fb 67b60A837 0197958a1 1e6f5BC05 12279560b 52a857ae3 4cb321EF0
3.11.0	• 修正視窗造成的連線問題VMs。 • 已修正某些LAN組態的連線問題。 • 已改善存取性。	2023 年 12 月 6 日	下載 3.11.0 版 sha256：9b 6b7def99d 76c59a97b 067b6a73b dc6ee1c6b 89a206328 6f542e96b 32df5ae9

版本	改變	日期	下載鏈接和 SHA256
3.10.0	• 修正在用戶端網路中啟用時NAT64的連線問題。 • 修正用戶端機器上安裝 Hyper-V 網路介面卡時的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	下載 3.10.0 版 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	改善安全狀態。	2023 年 8 月 3 日	下載 3.9.0 版 sha256：de 9a3800ea2 349155540 bd32bbae4 72404c636 d8d8267a0 e1fb2173a 8aae21ed
3.8.0	改善安全狀態。	2023 年 7 月 15 日	不再支援
3.7.0	已復原 3.6.0 版的變更。	2023 年 7 月 15 日	不再支援
3.6.0	改善安全狀態。	2023 年 7 月 14 日	不再支援
3.5.0	次要錯誤修正與增強功能。	2023 年 4 月 3 日	不再支援
3.4.0	已復原 3.3.0 版的變更。	2023 年 3 月 28 日	不再支援
3.3.0	次要錯誤修正與增強功能。	2023 年 3 月 17 日	不再支援

版本	改變	日期	下載鏈接和 SHA256
3.2.0	• 增加了對「驗證 x509 名稱」打開標誌的支持。VPN • 當用戶端更新版本可用時會自動偵測。 • 加入了新客戶端版本可用時自動安裝的功能。	2023 年 1 月 23 日	不再支援
3.1.0	改善安全狀態。	2022 年 5 月 23 日	不再支援
3.0.0	• 加入了 Windows 11 支援。 • 修復了 TAP Windows 驅動程序命名導致其他驅動程序名稱受到影響。 • 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字的橫幅文字顯示。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援
1.3.7	• 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 8 日	不再支援
1.3.6	• 增加了對打開VPN標誌的支持：connect-retry-max，開發類型，保持活動，ping，乒乓重啟，拉，rcvbuf，。server-poll-timeout • 次要錯誤修正與增強功能。	2021 年 9 月 20 日	不再支援
1.3.5	刪除大型視窗日誌的修補程式。	2021 年 8 月 16 日	不再支援

版本	改變	日期	下載鏈接和 SHA256
1.3.4	• 增加了對打開VPN標誌的支持：dhCP 選項。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援
1.3.3	• 增加了對打開VPN標誌的支持：非活動，拉過濾器，路由。 • 修正導致應用程式在中斷連線或結束時當機的問題。 • 修正含反斜線的 Active Directory 使用者名稱相關問題。 • 修正在應用程式外操作設定檔清單時的應用程式當機問題。 • 次要錯誤修正與強化功能。	2021 年 7 月 1 日	不再支援
1.3.2	• 在配置時添加IPv6洩漏預防。 • 修正使用 Connection (連線)下的 Show Details (顯示詳細資料) 選項時可能發生的當機問題	2021 年 5 月 12 日	不再支援
1.3.1	• 新增了對具有相同主體的多個用戶端憑證的支援。過期的憑證將會被忽略。 • 修正了本機日誌保留，以減少磁碟使用量。 • 增加了對「路由 IPv6」開放VPN指令的支持。 • 次要錯誤修正與增強功能。	2021 年 4 月 5 日	不再支援
1.3.0	新增了支援功能，如錯誤報告、傳送診斷日誌和分析。	2021 年 3 月 8 日	不再支援

版本	改變	日期	下載鏈接和 SHA256
1.2.7	• 增加了對加密技術 Open 指令的支援。VPN • 修正了連線之間的過時路由。 • 次要錯誤修正與強化功能。	2021 年 2 月 25 日	不再支援
1.2.6	次要錯誤修正與強化功能。	2020 年 10 月 26 日	不再支援
1.2.5	• 在「開啟」VPN 組態中新增了對註解的支援。 • 新增TLS交握錯誤的錯誤訊息。	2020 年 10 月 8 日	不再支援
1.2.4	次要錯誤修正與強化功能。	2020 年 9 月 1 日	不再支援
1.2.3	轉返在 1.2.2 版本中的變更。	2020 年 8 月 20 日	不再支援
1.2.1	次要錯誤修正與強化功能。	2020 年 7 月 1 日	不再支援
1.2.0	• 增加了對基於 SAML2.0 的聯合身份驗證的支持。 • 已取代對 Windows 7 平台的支援。	2020 年 5 月 19 日	不再支援
1.1.1	次要錯誤修正與強化功能。	2020 年 4 月 21 日	不再支援
1.1.0	• 增加了對開放VPN靜態挑戰 echo 功能的支持，以隱藏或顯示在用戶界面中顯示的文本。 • 次要錯誤修正與增強功能。	2020 年 3 月 9 日	不再支援
1.0.0	初始版本。	2020 年 2 月 4 日	不再支援

AWS Client VPN 適用於 macOS

這些章節說明如何使用 AWS 提供的 macOS 用戶端建立VPN連線。您可以在用戶端下載時下VPN載並安裝AWS 用戶端。 AWS 提供的用戶端不支援自動更新。

要求

若要使用 AWS 提供的 macOS 用戶端，需要下列項目：

- macOS 蒙特雷 (12.0), 文圖拉 (13.0), 或索諾瑪 (14.0).
- 相容的 x86_64 處理器。
- 用戶端會在您的電腦上保留TCP連接埠 8096。
- 對SAML於使用聯合驗證 (單一登入) 的用戶VPN端端點，用戶端會保留TCP連接埠 35001。

> **Note**
>
> 如果您使用的是配備蘋果矽處理器的 Mac，則需要安裝 Rosetta 2 才能運行客戶端軟件。如需進一步的詳細資訊，請參閱 Apple 網站上的「關於 Rosetta 翻譯環境」。

主題

- VPN使用 AWS 提供的 macOS 用戶端連 Connect 至用戶端
- AWS Client VPN 適用於 macOS 版本說明

VPN使用 AWS 提供的 macOS 用戶端連 Connect 至用戶端

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

同樣的，請務必先詳閱需求。在以下步驟中， AWS 提供的AWS VPN 用戶端也稱為「用戶端」。

若要使用 AWS 提供的 macOS 用戶端進行連線

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。

5. 對於「VPN組態檔案」，瀏覽至您從用戶端VPN管理員收到的組態檔案。選擇 Open (開啟)。
6. 選擇 Add Profile (新增設定檔)。
7. 在 AWS VPN Client 視窗中，確定已選取您的設定檔，然後選擇 Connect (連接)。如果 Client VPN 端點已設定為使用憑證型驗證，系統會提示您輸入使用者名稱和密碼。
8. 若要檢視連線的統計資料，請選擇 Connection (連線)、Show Details (顯示詳細資料)。
9. 若要中斷連接，請在 AWS VPN Client 視窗中選擇 Disconnect (中斷連接)。或者，選擇功能表列上的用戶端圖示，然後選擇「中斷連線 < your-profile-name >」。

AWS Client VPN 適用於 macOS 版本說明

下表包含適用於 macOS 的目前和先前版本的 AWS Client VPN 版本說明和下載連結。

> **Note**
>
> 我們持續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版可能受到可用性和/或安全性問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載連結
3.12.0	• 增加了對`tap-sleep` 打開標VPN誌的支持。 • 更新了「打開」VPN 和「打開」SSL 庫。	2024年8月12日	下載 3.12.0 版 SHA256：37 de7736e19 da380b034 1f722271e2f5aca8 的方法三十八乙太網路 366d9e4b13
3.11.0	• 更新了「打開」VPN 和「打開」SSL 庫。	2024年7月29日	下載 3.11.0 版 SHA256：44 b5e6f8478 8bf45ddb7 7871d743e 159755585

版本	改變	日期	下載連結
			06221b8CA E81732848F
3.10.0	• 區域網路範圍變更時自動重新連線。 • 修DNS復了網絡切換期間的恢復問題。 • 移除與端點連線時的自動應用程式焦SAML點。	2024年5月21 日	下載 3.10.0 版 SHA256：28bf26fa134 b01FF1270 3CF59F4ad4ad7d
3.9.2	• 解決了自 123 版以來基於 Chromium 的瀏覽器的SAML身份驗證問題。 • 增加了對 macOS 索諾瑪的支持。棄用對 macOS 大蘇爾的支持。 • 改善安全狀態。	2024年4月11日	下載版本 3.9.2 SHA256：37 4467d991e 8953b50e5 b985cda80 a0A0ea27f b5d5f23cf 16c556a15 68b0d480
3.9.1	• 修正緩衝區溢位動作，此動作可能允許本機 actor 以提升的權限執行任意命令。(• 固定應用程序更新下載進度條。 • 改善安全狀態。	2024年2月16日	下載版本 3.9.1 SHA256：9b ba4b27a63 5e7503870 3e2CF4cd8 14A753061 79Fac8e50 0e2C7af4e8e971

版本	改變	日期	下載連結
3.9.0	• 已修正某些LAN組態的連線問題。 • 已改善存取性。	2023 年 12 月 6 日	下載 3.9.0 版 sha256：f0f6a5579fe943157745 2e8aac072 41c36cb34 c2b3f028d fdd07f41d00ff80d8
3.8.0	• 修正在用戶端網路中啟用時NAT64的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	下載 3.8.0 版 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	• 改善安全狀態。	2023 年 8 月 3 日	下載 3.7.0 版 sha256：4a34b25b482 33b02d610 7638a3868 f7e419a84 d20bb4989 f7b394aae 9a9de00a
3.6.0	• 改善安全狀態。	2023 年 7 月 15 日	不再支援
3.5.0	• 已復原 3.4.0 版的變更。	2023 年 7 月 15 日	不再支援
3.4.0	• 改善安全狀態。	2023 年 7 月 14 日	不再支援

版本	改變	日期	下載連結
3.3.0	• 已新增對 macOS Ventura (13.0) 的支援。 • 次要錯誤修正與增強功能。	2023 年 4 月 27 日	不再支援
3.2.0	• 增加了對「驗證 x509 名稱」打開標誌的支持。VPN • 當用戶端更新版本可用時會自動偵測。 • 加入了新客戶端版本可用時自動安裝的功能。	2023 年 1 月 23 日	不再支援
3.1.0	• 新增對 macOS Monterey 的支援。 • 修復了磁碟機類型偵測的問題。 • 改善安全狀態。	2022 年 5 月 23 日	不再支援
3.0.0	• 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字的橫幅文字顯示。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援。
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援。
1.4.0	• 連接期間添加了DNS服務器監控。如果設定不符合設定，將會重新VPN設定。 • 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 9 日	不再支援。

版本	改變	日期	下載連結
1.3.5	• 增加了對打開VPN標誌的支持：connect-retry-max，開發類型，保持活動，ping，乒乓重啟，拉，rcvbuf，。server-poll-timeout • 次要錯誤修正與增強功能。	2021 年 9 月 20 日	不再支援。
1.3.4	• 增加了對打開VPN標誌的支持：dhCP選項。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援。
1.3.3	• 增加了對打開VPN標誌的支持：非活動，拉過濾器，路由。 • 修正含空格或 Unicode 的組態檔案名稱相關問題。 • 修正導致應用程式在中斷連線或結束時當機的問題。 • 修正含反斜線的 Active Directory 使用者名稱相關問題。 • 修正在應用程式外操作設定檔清單時的應用程式當機問題。 • 次要錯誤修正與強化功能。	2021 年 7 月 1 日	不再支援。
1.3.2	• 在配置時添加IPv6洩漏預防。 • 修正使用 Connection (連線)下的 Show Details (顯示詳細資料) 選項時可能發生的當機問題 • 新增 daemon 日誌輪替。	2021 年 5 月 12 日	不再支援。

版本	改變	日期	下載連結
1.3.1	• 新增了對 macOS Big Sur (10.16) 的支援。 • 已修正移除其他應用程式所DNS設定之設定的問題。 • 修正了使用非有效憑證進行相互驗證導致連線問題的問題。 • 增加了對「路由 IPv6」開放VPN指令的支持。 • 次要錯誤修正與增強功能。	2021 年 4 月 5 日	不再支援。
1.3.0	新增了支援功能，如錯誤報告、傳送診斷日誌和分析。	2021 年 3 月 8 日	不再支援。
1.2.5	次要錯誤修正與強化功能。	2021 年 2 月 25 日	不再支援。
1.2.4	次要錯誤修正與強化功能。	2020 年 10 月 26 日	不再支援。
1.2.3	• 在「開啟」VPN 組態中新增了對註解的支援。 • 新增TLS交握錯誤的錯誤訊息。 • 修正了影響部分使用者的解除安裝錯誤。	2020 年 10 月 8 日	不再支援。
1.2.2	次要錯誤修正與強化功能。	2020 年 8 月 12 日	不再支援。
1.2.1	• 新增解除安裝應用程式的支援。 • 次要錯誤修正與強化功能。	2020 年 7 月 1 日	不再支援。
1.2.0	• 增加了對基於 SAML2.0 的聯合身份驗證的支持。 • 新增了對 macOS Catalina (10.15) 的支援。	2020 年 5 月 19 日	不再支援。
1.1.2	次要錯誤修正與強化功能。	2020 年 4 月 21 日	不再支援。

版本	改變	日期	下載連結
1.1.1	• 修正DNS了沒有解決的問題。 • 修正因連線較長所造成的應用程式當機問題。 • 修正了一個MFA問題。	2020 年 4 月 2 日	不再支援。
1.1.0	• 增加了對 macOS DNS 配置的支持。 • 增加了對開放VPN靜態挑戰 echo 功能的支持，以隱藏或顯示在用戶界面中顯示的文本。 • 次要錯誤修正與增強功能。	2020 年 3 月 9 日	不再支援。
1.0.0	初始版本。	2020 年 2 月 4 日	不再支援。

AWS Client VPN 對於 Linux

這些部分描述了為 Linux 安裝 AWS 提供的客戶端，然後使用 AWS 提供的客戶端建立VPN連接。提 AWS 供的 Linux 用戶端不支援自動更新。如需最新的更新和下載，請參閱the section called “版本備註”。

使用提供的 Linux 用戶端VPN連線至 AWS 用戶端的需求

要使用提 AWS 供的 Linux 客戶端，需要以下內容：

- Ubuntu 18.04 LTS 或 (只有LTS) AMD64

用戶端會在您的電腦上保留TCP連接埠 8096。對SAML於使用聯合驗證 (單一登入) 的用戶VPN端端點，用戶端會保留TCP連接埠 35001。

開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

主題

- 安裝提 AWS 供的 Linux 用戶端
- Connect 到提 AWS 供的 Linux 用戶端

- AWS Client VPN 適用於 Linux 版本說明

安裝提 AWS 供的 Linux 用戶端

有多種方法可用於安裝 Linux AWS 所提供的用戶端。請使用下列其中一種方法。開始之前，請務必先詳閱需求。

選項 1：透過套件儲存庫安裝

1. 將AWSVPN用戶端公開金鑰新增至您的 Ubuntu 作業系統。

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. 根據您的 Ubuntu 版本，使用適用的命令將儲存庫新增您的 Ubuntu 作業系統：

   Ubuntu 18.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

   Ubuntu 20.04

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

3. 使用下列命令更新系統上的儲存庫。

```
sudo apt-get update
```

4. 使用下面的命令來安裝 Linux AWS 提供的客戶端。

```
sudo apt-get install awsvpnclient
```

選項 2：使用 .deb 套件檔案進行安裝

1. 從用AWS 戶端下載或使用下列命令下VPN載 .deb 檔案。

```
curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
 awsvpnclient_amd64.deb
```

2. 使用公用程式安裝 AWS 提供的 Linux dpkg 用戶端。

```
sudo dpkg -i awsvpnclient_amd64.deb
```

選項 3 — 使用 Ubuntu Software Center 安裝 .deb 套件

1. 從AWS 用戶端VPN下載下載 .deb 套件檔案。
2. 下載 .deb 套件檔案後，使用 Ubuntu Software Center 安裝套件。遵循使用 Ubuntu Software Center 從獨立 .deb 套件安裝的步驟，如 Ubuntu Wiki 所述。

Connect 到提 AWS 供的 Linux 用戶端

在以下步驟中， AWS 提供的AWS VPN 用戶端也稱為「用戶端」。

若要使用 AWS 提供的 Linux 用戶端進行連線

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。
5. 對於「VPN組態檔案」，瀏覽至您從用戶端VPN管理員收到的組態檔案。選擇 Open (開啟)。
6. 選擇 Add Profile (新增設定檔)。
7. 在 AWS VPN Client 視窗中，確定已選取您的設定檔，然後選擇 Connect (連接)。如果 Client VPN 端點已設定為使用憑證型驗證，系統會提示您輸入使用者名稱和密碼。
8. 若要檢視連線的統計資料，請選擇 Connection (連線)、Show Details (顯示詳細資料)。
9. 若要中斷連接，請在 AWS VPN Client 視窗中選擇 Disconnect (中斷連接)。

AWS Client VPN 適用於 Linux 版本說明

下表包含目前和舊版 Linux 的 AWS Client VPN 版本說明和下載連結。

> **Note**
>
> 我們會繼續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版本可能受到可用性和/或安全性問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載連結
3.15.0	• 增加了對`tap-sleep` 打開標VPN誌的支持。 • 更新了打開VPN和打開SSL庫。	2024年8月12日	下載版本 SHA256：5cf3eb08de96821b0ad3d0d0C9174b2e308041d5490a3edb72dfd89a6d89d012
3.14.0	• 更新了打開VPN和打開SSL庫。	2024年7月29日	下載版本 SHA256：bd2b401a1a1E1E1E1E419d7a7a79e0a20d379e44f319b5334f60
3.13.0	• 區域網路範圍變更時自動重新連線。	2024年5月21 日	下載版本 SHA256：e89f3bb7fc24c148e3044b807774fffff05e7e9e551863a2dcd7e0ac05f1

版本	改變	日期	下載連結
3.12.2	• 解決了自 123 版以來基於 Chromium 的瀏覽器的SAML身份驗證問題。	2024年4月11日	下載版本 SHA256：f7178c33777740b596a14cbe7b6f5f58fb79f79f88bd8801353a757a7a7d
3.12.1	• 修正緩衝區溢位動作，此動作可能允許本機 actor 以提升的權限執行任意命令。 • 改善安全狀態。	2024年2月16日	下載版本 SHA256：547c4FFD3e35c54db8e0b792aed9f31A600e558af4f0c2f5cf31d0
3.12.0	• 已修正某些LAN組態的連線問題。	2023 年 12 月 19 日	下載 3.12.0 版 sha256:9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1

版本	改變	日期	下載連結
3.11.0	• 回滾「修復了某些LAN配置的連接問題」。 • 已改善存取性。	2023 年 12 月 6 日	下載 3.11.0 版 sha256：86c0fa1bf1c971940828 35a739ec7f1c87e540 194955f414a35c679b 94538970
3.10.0	• 已修正某些LAN組態的連線問題。 • 已改善存取性。	2023 年 12 月 6 日	下載 3.10.0 版 sha256：e7450b2490f 3b96ab7d589a8000d8 38d9fd2adcdd72ae80 666c4c0d900687e51
3.9.0	• 修正在用戶端網路中啟用時NAT64的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	下載 3.9.0 版 sha256: 6cde9cfff82754119e 6a68464d4bb350da3c b3e1ebf9140dacf24e 4fd2197454

版本	改變	日期	下載連結
3.8.0	• 改善安全狀態。	2023 年 8 月 3 日	下載 3.8.0 版 sha256：5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• 改善安全狀態。	2023 年 7 月 15 日	不再支援
3.6.0	• 已復原 3.5.0 版的變更。	2023 年 7 月 15 日	不再支援
3.5.0	• 改善安全狀態。	2023 年 7 月 14 日	不再支援
3.4.0	• 增加了對「驗證 x509 名稱」打開標誌的支持。VPN	2023 年 2 月 14 日	不再支援
3.1.0	• 修復了磁碟機類型偵測的問題。 • 改善安全狀態。	2022 年 5 月 23 日	不再支援
3.0.0	• 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字和特定字元序列的橫幅文字顯示問題。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援。
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援。

版本	改變	日期	下載連結
1.0.3	• 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 8 日	不再支援。
1.0.2	• 增加了對打開VPN標誌的支持：connect-retry-max，開發類型，保持活動，ping，乒乓重啟，拉，rcvbuf，。server-poll-timeout • 次要錯誤修正與增強功能。	2021 年 9 月 28 日	不再支援。
1.0.1	• 啟用選項從 Ubuntu 應用程式欄退出。 • 增加了對打開VPN標誌的支持：非活動，拉過濾器，路由。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援。
1.0.0	初始版本。	2021 年 6 月 11 日	不再支援。

使用開放式用戶VPN端 Connect 到用VPN戶端端點

您可以使用常見的開放式用戶VPN端應用程式連線到用VPN戶端端點。

> **Important**
>
> 如果用戶端VPN端點已設定為使用SAML型聯合驗證，則無法使用開放VPN式用VPN戶端連線到用戶VPN端端點。

用戶端應用程式

- 使用 Windows 用戶VPN端應用程式 Connect 到用戶端端點
- 使用 Android 或 iOS 用戶VPN端應用程式 Connect 線到用VPN戶端端點
- 使用 macOS 用戶VPN端應用程式 Connect 至用戶端端點
- 使用開放式用戶VPN端應用程式 Connect 線到用VPN戶端端點

使用 Windows 用戶VPN端應用程式 Connect 到用戶端端點

這些章節說明如何使用以 Windows 為基礎的用VPN戶端建立VPN連線。

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

如需故障診斷資訊，請參閱疑難排解用戶VPN端與 Windows 用戶端的連線。

> **Important**
>
> 如果用戶端VPN端點已設定為使用SAML型聯合驗證，則無法使用開放VPN式用VPN戶端連線到用戶VPN端端點。

任務

- 在開啟狀態下使用 Windows 憑證系統存放區中的憑證 VPN
- 使用「開啟」VPN GUI
- 使用開啟 VPN Connect 用戶端

在開啟狀態下使用 Windows 憑證系統存放區中的憑證 VPN

您可以將開啟用VPN戶端設定為使用 Windows 憑證系統存放區中的憑證和私密金鑰。當您使用智慧卡做為用戶端VPN連線的一部分時，此選項非常有用。如需「開啟VPN用戶端密碼應用程式」選項的相關資訊，請參閱開啟網站VPN上開啟的參考手冊。VPN

> **Note**
>
> 憑證必須存放在本機電腦上。

若要使用「開啟」中的加密資料應用程式選項 VPN

1. 建立包含用戶端憑證和私密金鑰的 .pfx 檔案。
2. 將 .pfx 檔案匯入您的本機電腦上的個人憑證存放區。如需詳細資訊，請參閱 HOW TO：使用 Microsoft 網站上的MMC嵌入式管理單元檢視憑證。
3. 驗證您的帳戶具有讀取本機電腦憑證的權限。您可以使用 Microsoft 管理主控台來修改權限。如需詳細資訊，請參閱 Microsoft Technet 網站上的 Rights to see the local computer certificates store。
4. 更新開啟VPN組態檔案，並使用憑證主體或憑證指紋來指定憑證。

   以下是使用主體指定憑證的範例。

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   以下是使用指紋指定憑證的範例。您可以使用 Microsoft 管理主控台尋找指紋。如需詳細資訊，請參閱 Microsoft TechNet 網站上的 How to: Retrieve the Thumbprint of a Certificate。

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```

完成組態後，您可以使用「開啟」(Open) VPN 來建立連線。

使用「開啟」VPN GUI

下列程序顯示如何使用 Windows 電腦上的開啟用VPNGUI戶端應用程式來建立VPN連線。

> **Note**
>
> 如需開啟用VPN戶端應用程式的相關資訊，請參閱開啟VPN網站上的社群下載。

若要建立VPN連線

1. 啟動開啟用VPN戶端應用程式。
2. 在 Windows 工作列上，選擇 [顯示/隱藏圖示]。以滑鼠右鍵按一下 [開啟] VPNGUI，然後選擇 [匯
3. 在 [開啟舊檔] 對話方塊中，選取您從用戶端VPN管理員接收的組態檔案，然後選擇 [開啟]。
4. 在 Windows 工作列上，選擇 [顯示/隱藏圖示]。以滑鼠右鍵按一下 [開啟] VPNGUI，然 Connect 選擇

使用開啟 VPN Connect 用戶端

下列程序顯示如何使用 Windows 電腦上的開啟 VPN Connect VPN 線用戶端應用程式來建立連線。

> **Note**
>
> 如需詳細資訊，請參閱開啟VPN網站上的使用 Windows 連線到存取伺服器。

若要建立VPN連線

1. 啟動開啟 VPN Connect 用戶端應用程式。
2. 在 Windows 工作列上，選擇 [顯示/隱藏圖示]。在 [開啟] 上按一下滑鼠右鍵VPN，然後選擇 [
3. 選擇「從檔案匯入」，然後選取您從用戶端VPN管理員收到的組態檔案。
4. 若要開始連線，請選擇連線設定檔。

使用 Android 或 iOS 用戶VPN端應用程式 Connect 線到用VPN戶端端點

> **Important**
>
> 如果用戶端VPN端點已設定為使用SAML型聯合驗證，則無法使用開放VPN式用VPN戶端連線到用戶VPN端端點。

下列資訊顯示如何使用 Android 或 iOS 行動裝置上的開啟用VPN戶端應用程式建立VPN連線。適用於 Android 和 iOS 的步驟相同。

> **Note**
>
> 如需有關下載及使用 iOS 或 Android 開啟用VPN戶端應用程式的詳細資訊，請參閱開啟VPN網站上的開放 VPN Connect 使用手冊。

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

若要建立連線，請啟動開啟用VPN戶端應用程式，然後匯入您從用戶端VPN管理員那裡收到的檔案。

使用 macOS 用戶VPN端應用程式 Connect 至用戶端端點

這些章節說明如何使用以 Mac 為基礎VPN的用戶端建立VPN連線。

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

如需故障診斷資訊，請參閱疑難排解用戶VPN端與 macOS 用戶端。

> **Important**
>
> 如果用戶端VPN端點已設定為使用SAML型聯合驗證，則無法使用開放VPN式用VPN戶端連線到用戶VPN端端點。

主題

- 啟動隧道通道以建立連接 AWS Client VPN
- 使用開啟 Connect 用戶 AWS Client VPN 端 VPN Connect 到端點

啟動隧道通道以建立連接 AWS Client VPN

下列程序顯示如何使用 macOS 電腦上的通道用戶端應用程式建立VPN連線。

> **Note**
>
> 如需適用於 macOS 的 Tunnelblick 用戶端應用程式的詳細資訊，請參閱 Tunnelblick 網站上的 Tunnelblick 文件。

若要建立VPN連線

1. 啟動 Tunnelblick 用戶端應用程式，然後選擇我有組態檔案。
2. 將您從VPN管理員那裡收到的組態檔案拖放到「組態」面板中。
3. 在組態面板中選取組態檔案，然後選擇連接。

使用開啟 Connect 用戶 AWS Client VPN 端 VPN Connect 到端點

下列程序顯示如何使用 macOS 電腦上的「開啟 VPN Connect VPN 線用戶端」應用程式建立連線。

> **Note**
>
> 如需詳細資訊，請參閱「開啟」VPN 網站上的使用 macOS 連線至存取伺服器。

若要建立VPN連線

1. 啟動開啟VPN應用程式，然後選擇匯入，從本機檔案... 。
2. 瀏覽至您從VPN管理員那裡收到的組態檔案，然後選擇 [開啟]。

使用開放式用戶VPN端應用程式 Connect 線到用VPN戶端端點

這些章節說明如何使用開放VPN式用VPN戶端建立VPN連線。

在開始之前，請確定您的用戶端VPN管理員已建立 Client VPN 端點，並為您提供用戶VPN端端點組態設定檔。

如需故障診斷資訊，請參閱疑難排解用戶VPN端與 Linux 用戶端的連線。

> **Important**
>
> 如果用戶端VPN端點已設定為使用SAML型聯合驗證，則無法使用開放VPN式用VPN戶端連線到用戶VPN端端點。

主題

AWS Client VPN 使用 [開啟] VPN-[網路管理員] 建立連線

下列程序顯示如何透過 Ubuntu 電腦GUI上的網路管理員使用「開啟」VPN 應用程式建立VPN連線。

若要建立VPN連線

1. 使用以下命令安裝網路管理員模組。

   ```
   sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
   ```

2. 移至 Settings (設定)、Network (網路)。
3. 選擇旁邊的加號 (+) VPN，然後選擇從檔案匯入... 。
4. 瀏覽至您從VPN管理員那裡收到的組態檔案，然後選擇 [開啟]。
5. 在「新增 VPN」視窗中，選擇「新增」。
6. 啟用新增VPN設定檔旁邊的切換開關，以啟動連線。

AWS Client VPN 使用「開啟」建立連線 VPN

下列程序顯示如何使用 Ubuntu 電腦上的「開啟」VPN 應用程式建立VPN連線。

若要建立VPN連線

1. VPN使用下列命令安裝開啟。

```
sudo apt-get install openvpn
```

2. 載入您從VPN管理員那裡收到的組態檔案，以啟動連線。

```
sudo openvpn --config /path/to/config/file
```

疑難排解用戶端VPN連線

使用下列主題疑難排解使用用戶端應用程式連線到 Client VPN 端點時可能遇到的問題。

主題

管理員的用戶VPN端端點疑難

您可執行本指南中的某些步驟。其他步驟必須由您的用戶端VPN管理員在用戶VPN端端點本身上執行。下列各節可讓您知道何時需要聯絡系統管理員。

如需疑難排解用戶VPN端端點問題的其他資訊，請參閱《AWS Client VPN 管理員指南》VPN中的疑難排解

將診斷記錄傳送到 AWS Support 提 AWS 供的用戶端

如果您使用所 AWS 提供的用戶端發生問題，而且需 AWS Support 要連絡以協助疑難排解， AWS 提供的用戶端可以選擇將診斷記錄檔傳送至 AWS Support。此選項可在 Windows、macOS 和 Linux 用戶端應用程式上使用。

在傳送檔案之前，您必須同意允許存 AWS Support 取診斷記錄檔。在您同意之後，我們會為您提供參考編號，以 AWS Support 便他們可以立即存取檔案。

傳送診斷日誌

在以下步驟中， AWS 提供的AWS VPN 用戶端也稱為「用戶端」。

使用 AWS 提供的 Windows 用戶端傳送診斷記錄

1. 開啟 AWS VPN Client 應用程式。

2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Yes (是)。
4. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，執行以下其中一個操作：

   - 若要將參考編號複製到剪貼簿，請選擇 Yes (是)，然後選擇 OK (確定)。
   - 若要手動追蹤參考編號，請選擇 No (否)。

   聯絡時 AWS Support，您需要向他們提供參考編號。

使用 AWS 提供的 macOS 用戶端傳送診斷記錄

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Yes (是)。
4. 請記下確認視窗中的參考編號，然後選擇 OK (確定)。

   聯絡時 AWS Support，您需要向他們提供參考編號。

若要使用 AWS 提供的 Ubuntu 用戶端傳送診斷記錄

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Send (傳送)。
4. 請記下確認視窗中的參考編號。您可以選擇將信息複製到剪貼板。

   聯絡時 AWS Support，您需要向他們提供參考編號。

疑難排解用戶VPN端與 Windows 用戶端的連線

下列各節包含使用 Windows 用戶端連線到用戶VPN端端點時可能遇到之問題的相關資訊。

主題

AWS 提供的客戶

AWS 提供的用戶端會建立事件記錄檔，並將它們儲存在您電腦上的下列位置。

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

以下是可用的日誌類型：

- 應用程式日誌：包含應用程式的相關資訊。這些日誌的字首會加上 'aws_vpn_client_'。
- 開啟VPN記錄：包含開啟VPN處理程序的相關資訊。這些日誌的字首會加上 'ovpn_aws_vpn_client_'。

AWS 提供的用戶端會使用 Windows 服務來執行根作業。Windows 服務日誌儲存在電腦的下列位置。

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

主題

用戶端無法連線

問題

AWS 提供的用戶端無法連線到用戶端VPN端點。

原因

導致此問題的原因可能為下列其中一項：

- 另一個「開啟」VPN 處理程序已在您的電腦上執行，這會阻止用戶端連線。
- 您的組態 (.ovpn) 檔案無效。

解決方案

檢查您的計算機上是否有其他打開的VPN應用程序正在運行。如果存在，請停止或結束這些程序，然後再次嘗試連線到 Client VPN 端點。檢查「開啟VPN記錄檔」是否有錯誤，並要求用戶端VPN管理員驗證下列資訊：

- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- 這仍然CRL是有效的。如需詳細資訊，請參閱《AWS Client VPN 管理手冊》中的用戶VPN端無法 Connect 到用戶端端點。

用戶端無法使用「無 TAP-Windows 介面卡」記錄檔訊息連線

問題

AWS 提供的用戶端無法連線到用戶VPN端端點，應用程式記錄檔中會出現下列錯誤訊息：「此系統上沒有 TAP-Windows 介面卡。您應該可以通過轉到開始 TAP-> 所有程序-> Windows-> 實用程序-> 添加新的 TAP-Windows 虛擬以太網適配器「創建一個 TAP-Windows 適配器。

解決方案

您可以採取下列其中一個或多個動作來解決此問題：

- 重新啟動 TAP-視窗介面卡。
- 重新安裝 TAP-視窗驅動程式。
- 創建一個新的 TAP-視窗適配器。

用戶端卡在重新連接狀態

問題

AWS 提供的用戶端嘗試連線到 Client VPN 端點，但處於重新連線狀態。

原因

導致此問題的原因可能為下列其中一項：

- 您的電腦未連線到網際網路。
- 主DNS機名稱未解析為 IP 位址。
- 開啟VPN處理序無限期地嘗試連線到端點。

解決方案

確定您的電腦已連線至網際網路。請您的用戶端VPN管理員確認組態檔中的`remote`指示詞是否解析為有效的 IP 位址。您也可以選擇「 AWS VPN用戶端」視窗中的「中斷連線」來中斷VPN工作階段的連線，然後再嘗試連線

VPN連線程序意外結束

問題

連線至用戶VPN端端點時，用戶端會意外結束。

原因

TAP-視窗未安裝在您的電腦上。需要此軟體才能執行用戶端。

解決方案

重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

應用程式無法啟動

問題

在 Windows 7 上，當您嘗試開啟 AWS 提供的用戶端時，不會啟動該用戶端。

原因

。 NET您的計算機上未安裝框架 4.7.2 或更高版本。這是執行用戶端的必要項目。

解決方案

重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

用戶端無法建立設定檔

問題

當您使用 AWS 提供的用戶端嘗試建立描述檔時，發生下列錯誤。

```
The config should have either cert and key or auth-user-pass specified.
```

原因

如果用戶端VPN端點使用相互驗證，則組態 (.ovpn) 檔案不包含用戶端憑證和金鑰。

解決方案

確定您的用戶端VPN管理員已將用戶端憑證和金鑰新增至組態檔案。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。

戴爾PCs使用視窗 10 或 11 時會發生用戶端當機

問題

在執行 Windows 10 或 11 的特定 Dell PCs (桌上型電腦和筆記型電腦) 上，當您瀏覽檔案系統匯入VPN組態檔時，可能會發生當機。如果發生這個問題，您會在 AWS 提供的用戶端的記錄檔中看到類似下列的訊息：

```
System.AccessViolationException: Attempted to read or write protected memory. This is
 often an indication that other memory is corrupt.
   at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
 Int32 flags, IntPtr& db)
   at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
 connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
   at System.Data.SQLite.SQLiteConnection.Open()
   at
 STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
 newConnection)
   at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
 targetSettings)
   at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

原因

Windows 10 和 11 中的戴爾 Backup 和恢復系統可能會導致與 AWS 提供的客戶端發生衝突，尤其是以下三種情況DLLs：

- DBRShellExtension.dll

- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.dll

解決方案

若要避免此問題，請先確定您的用戶端是最新版本的 AWS 所提供用戶端。移至 [用AWS 戶端VPN下載]，如果有更新的版本可用，請升級至最新版本。

此外，請執行下列作業：

- 如果您使用的是 Dell Backup and Recovery 應用程式，請務必使用最新版。一篇 Dell 論壇文章聲明此問題已在較新版的應用程式中解決。
- 如果您沒有使用 Dell Backup and Recovery 應用程式，如果您遇到此問題，仍需採取一些動作。如果您不想升級應用程式，也可以刪除或重新命名DLL檔案。但是，請注意，這會使得 Dell Backup and Recovery 應用程式難以順暢運作。

刪除或重命名DLL文件

1. 前往 Windows 檔案總管並瀏覽到 Dell Backup and Recovery 的安裝位置。此應用程式通常會安裝在下列位置，但您可能需要搜尋才能找出來。

   ```
   C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
   ```

2. 從安裝目錄手動刪除下列DLL檔案，或重新命名它們。任何一項動作皆會使這些檔案無法載入。

   - DBRShellExtension.dll
   - DBROverlayIconBackuped.dll
   - DBROverlayIconNotBackuped.dll

   您可以通過在文件名的末尾添加「.bak」來重命名文件，例如 .dll.bak。DBROverlayIconBackuped

VPN與彈出消息斷開連接

問題

與彈出消息VPN斷開連接，說：「連接正在終止，因為您的設備VPN連接到的本地網絡的地址空間已更改。請建立一個新的VPN連接。」

原因

TAP-Windows 介面卡不包含必要的描述。

解決方案

如果下面的Description欄位不相符，請先移除 TAP-Windows 介面卡，然後重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

打開 VPN GUI

下列疑難排解資訊已在 Windows 10 家用版 (64 位元) 和視窗伺服器 2016 年 (64 位元) 上的開啟VPNGUI軟體 11.10.0.0 和 11.11.0.0 版上測試。

組態檔案儲存在電腦的下列位置。

```
C:\Users\User\OpenVPN\config
```

連線日誌儲存在電腦的下列位置。

```
C:\Users\User\OpenVPN\log
```

開啟VPN連線用戶端

下列疑難排解資訊已在 Windows 10 家用版 (64 位元) 和視窗伺服器 2016 年 (64 位元) 上的開啟 VPN Connect 用戶端軟體 2.6.0.100 和 2.7.1.101 版上進行測試。

組態檔案儲存在電腦的下列位置。

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

連線日誌儲存在電腦的下列位置。

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

無法解決 DNS

問題

連線失敗，並出現下列錯誤。

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

原因

無法解析DNS名稱。用戶端必須在DNS名稱前面加上隨機字串，以防止DNS快取；但是，有些用戶端不會這麼做。

解決方案

請參閱《AWS Client VPN 管理員指南》中的「無法解析用戶VPN端端點DNS名稱」的解決方案。

缺少PKI別名

問題

與不使用相互驗證的用戶VPN端端點的連線會失敗，並出現下列錯誤。

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

原因

開啟 VPN Connect 用戶端軟體有一個已知的問題，即嘗試使用相互驗證進行驗證。如果組態檔案不包含用戶端金鑰和憑證，身分驗證會失敗。

解決方案

在用戶端VPN組態檔案中指定隨機的用戶端金鑰和憑證，然後將新的組態匯入開啟 VPN Connect 用戶端軟體。或者，使用不同的用戶端，例如開啟用VPNGUI戶端 (v11.12.0.0) 或黏度用戶端 (v.1.7.14)。

疑難排解用戶VPN端與 macOS 用戶端

以下各節針對記錄和您使用 macOS 用戶端時可能遇到的問題提供了相關資訊。請確定您執行的是這些用戶端的最新版本。

主題

AWS 提供的客戶

AWS 提供的用戶端會建立事件記錄檔，並將它們儲存在您電腦上的下列位置。

```
/Users/username/.config/AWSVPNClient/logs
```

以下是可用的日誌類型：

- 應用程式日誌：包含應用程式的相關資訊。這些日誌的字首會加上 'aws_vpn_client_'。
- 開啟VPN記錄：包含開啟VPN處理程序的相關資訊。這些日誌的字首會加上 'ovpn_aws_vpn_client_'。

AWS 提供的客戶端使用客戶端守護進程來執行根操作。協助程式日誌儲存在電腦的下列位置。

```
/tmp/AcvcHelperErrLog.txt
/tmp/AcvcHelperOutLog.txt
```

AWS 提供的用戶端會將組態檔案儲存在您電腦上的下列位置。

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

主題

- 輔助工具是必需的錯誤

用戶端無法連線

問題

AWS 提供的用戶端無法連線到用戶端VPN端點。

原因

導致此問題的原因可能為下列其中一項：

- 另一個「開啟」VPN 處理程序已在您的電腦上執行，這會阻止用戶端連線。
- 您的組態 (.ovpn) 檔案無效。

解決方案

檢查您的計算機上是否有其他打開的VPN應用程序正在運行。如果存在，請停止或結束這些程序，然後再次嘗試連線到 Client VPN 端點。檢查「開啟VPN記錄檔」是否有錯誤，並要求用戶端VPN管理員驗證下列資訊：

- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- 這仍然CRL是有效的。如需詳細資訊，請參閱《AWS Client VPN 管理手冊》中的用戶VPN端無法 Connect 到用戶端端點。

用戶端卡在重新連接狀態

問題

AWS 提供的用戶端嘗試連線到 Client VPN 端點，但處於重新連線狀態。

原因

導致此問題的原因可能為下列其中一項：

- 您的電腦未連線到網際網路。
- 主DNS機名稱未解析為 IP 位址。

- 開啟VPN處理序無限期地嘗試連線到端點。

解決方案

確定您的電腦已連線至網際網路。請您的用戶端VPN管理員確認組態檔中的remote指示詞是否解析為有效的 IP 位址。您也可以選擇「 AWS VPN用戶端」視窗中的「中斷連線」來中斷VPN工作階段的連線，然後再嘗試連線

用戶端無法建立設定檔

問題

當您使用 AWS 提供的用戶端嘗試建立描述檔時，發生下列錯誤。

```
The config should have either cert and key or auth-user-pass specified.
```

原因

如果用戶端VPN端點使用相互驗證，則組態 (.ovpn) 檔案不包含用戶端憑證和金鑰。

解決方案

確定您的用戶端VPN管理員已將用戶端憑證和金鑰新增至組態檔案。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。

輔助工具是必需的錯誤

問題

當您嘗試連線時，您收到下列錯誤VPN。

```
AWS VPN Client Helper Tool is required to establish the connection.
```

解決方案

請參閱以下關於 AWS Re: POST 的文章。AWSVPN客戶端-輔助工具是必需的錯誤

Tunnelblick

下列故障診斷資訊已在 macOS High Sierra 10.13.6 版的 Tunnelblick 軟體 3.7.8 版 (組建 5180) 上經過測試。

私有組態的組態檔案儲存在電腦的下列位置。

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

共用組態的組態檔儲存在電腦的下列位置。

```
/Library/Application Support/Tunnelblick/Shared
```

連線日誌儲存在電腦的下列位置。

```
/Library/Application Support/Tunnelblick/Logs
```

若要提高記錄詳細程度，請開啟 Tunnelblick 應用程式，選擇 [設定]，然後調整記錄檔層級的值。VPN

找不到密碼演算法 'AES-256-GCM'

問題

連線失敗，並在日誌中傳回下列錯誤。

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

原因

該應用程序正在使用不支持密碼算法 AES -256-的 Open VPN 版本。GCM

解決方案

通過執行以下操作選擇兼容的 Open VPN 版本：

1. 開啟 Tunnelblick 應用程式。
2. 選擇設定。
3. 對於打開VPN版本，選擇 2.4.6-打開SSL版本是 v 1.0.2q。

連線停止回應並重設

問題

連線失敗，並在日誌中傳回下列錯誤。

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

原因

用戶端憑證已被撤銷。嘗試驗證後，連線會停止回應，並最終從伺服器端重設。

解決方案

向用戶端VPN管理員要求新的組態檔案。

延伸金鑰用法 (EKU)

問題

連線失敗，並在日誌中傳回下列錯誤。

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

原因

伺服器身分驗證成功。不過，用戶端驗證失敗，因為用戶端憑證已啟用伺服器驗證的延伸金鑰用法 (EKU) 欄位。

解決方案

請確定您使用的是正確的用戶端憑證和金鑰。如有必要，請向您的用戶端VPN管理員確認。如果您使用的是伺服器憑證，而不是用戶端憑證連線到 Client VPN 端點，則可能會發生此錯誤。

過期的憑證

問題

伺服器驗證成功，但用戶端身分驗證失敗，並顯示下列錯誤。

```
WARNING: “Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
 process restarting”
```

原因

用戶端憑證有效性已過期。

解決方案

向用戶端VPN管理員要求新的用戶端憑證。

打開 VPN

下列疑難排解資訊已在 macOS 海伊塞拉利昂 10.13.6 上的開放 VPN Connect 用戶端軟體 2.7.1.100 版進行測試。

組態檔案儲存在電腦的下列位置。

```
/Library/Application Support/OpenVPN/profile
```

連線日誌儲存在電腦的下列位置。

```
Library/Application Support/OpenVPN/log/connection_name.log
```

無法解決 DNS

問題

連線失敗，並出現下列錯誤。

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

原因

開啟 VPN Connect 無法解析用戶端VPNDNS名稱。

解決方案

請參閱《AWS Client VPN 管理員指南》中的「無法解析用戶VPN端端點DNS名稱」的解決方案。

疑難排解用戶VPN端與 Linux 用戶端的連線

以下各節針對記錄和您使用 Linux 用戶端時可能遇到的問題提供了相關資訊。請確定您執行的是這些用戶端的最新版本。

主題

- AWS 提供的客戶
- 開啟 VPN (指令行)
- VPN透過網路管理員開啟 (GUI)

AWS 提供的客戶

AWS 提供的用戶端會將記錄檔和組態檔儲存在系統上的下列位置：

```
/home/username/.config/AWSVPNClient/
```

AWS 提供的用戶端常駐程式處理程序會將記錄檔儲存在系統上的下列位置：

```
/var/log/aws-vpn-client/username/
```

問題

在建立VPN連線之後的某些情況下，DNS查詢仍會移至預設的系統名稱伺服器，而不是為 Client 端點設定的名稱伺服器。VPN

原因

用戶端與系統解析的互動，Linux 系統上可用的一項服務，作為管理的核心部分。DNS它是用來設定從用戶VPN端端點推送的DNS伺服器。之所以發生這個問題，是因為系統已解決並未將最高優先順序設定為用戶端端VPN點所提供的DNS伺服器。相反地，它會將伺服器附加到本機系統上設定的現有DNS伺服器清單。因此，原始DNS伺服器可能仍然具有最高的優先順序，因此可用於解析DNS查詢。

解決方案

1. 在 Open VPN 配置文件的第一行添加以下指令，以確保所有DNS查詢都發送到VPN隧道。

   ```
   dhcp-option DOMAIN-ROUTE .
   ```

2. 使用 systemd-resolved 提供的虛設常式解析程式。方法是在系統上執行下列命令，建立 `/etc/resolv.conf` 至 `/run/systemd/resolve/stub-resolv.conf` 的符號連結。

   ```
   sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
   ```

3. （可選）如果您不希望系統解析為代理DNS查詢，而是希望將查詢直接發送到實際DNS名稱服務器，則將符號鏈接改為。`/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

   ```
   sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

   您可能想要執行此程序以略過系統解析的組態，例如DNS回答快取、每個介面DNS配置、DNSSec強制執行等。當您需要在連接到私人記錄時覆寫公用DNS記錄時，此選項特別有用VPN。例如，您的私人解析器可能有一個私人DNS解析器，其中包VPC含 www.example.com 的記錄，該記錄可解析為私有 IP。此選項可用來覆寫可解析為公有 IP 的 www.example.com 公有記錄。

開啟 VPN (指令行)

問題

連線無法正常運作，因為DNS解析度不起作用。

原因

DNS伺服器未在用戶VPN端端點上設定，或者用戶端軟體未承受此伺服器。

解決方案

請使用下列步驟來檢查DNS伺服器是否已設定並正常運作。

1. 確定記錄檔中有DNS伺服器項目。在下列範例中，最後一行傳回DNS伺服器 192.168.0.2 (在 Client VPN 端點中設定)。

   ```
   Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
   WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
    'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
   gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
    10.0.0.98 255.255.255.224,peer-id 0
   ```

   如果沒有指定DNS伺服器，請要求用戶端VPN管理員修改 Client VPN 端點，並確定已為 Client 端 VPN點指定VPCDNS伺服器（例如伺服器）。DNS如需詳細資訊，請參閱《AWS Client VPN 管理手冊》中的用戶VPN端端點。
2. 請執行下列命令，確定已安裝 resolvconf 套件。

   ```
   sudo apt list resolvconf
   ```

   輸出應該會傳回以下內容。

   ```
   Listing... Done
   resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
   ```

   如果未安裝，請使用以下命令安裝它。

   ```
   sudo apt install resolvconf
   ```
3. 在文字編輯器中開啟用戶端VPN組態檔案 (.ovpn 檔案)，然後新增下列幾行。

   ```
   script-security 2
   up /etc/openvpn/update-resolv-conf
   down /etc/openvpn/update-resolv-conf
   ```

   檢查日誌以確認 resolvconf 指令碼是否已被叫用。日誌應該包含類似下列的行。

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

VPN透過網路管理員開啟 (GUI)

問題

使用網路管理員開啟用VPN戶端時，連線失敗，並出現下列錯誤。

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

原因

`remote-random-hostname` 旗標不會生效，且用戶端無法使用 `network-manager-gnome` 套件進行連線。

解決方案

請參閱《AWS Client VPN 管理員指南》中的「無法解析用戶VPN端端點DNS名稱」的解決方案。

疑難排解常見用戶端 VPN

以下是使用用戶端連線至用戶VPN端端點時可能會遇到的常見問題。

TLS金鑰交涉失敗

問題

TLS交涉失敗，並出現以下錯誤。

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

原因

導致此問題的原因可能為下列其中一項：

- 防火牆規則正在封鎖UDP或TCP流量。
- 您在組態 (.ovpn) 檔案中使用了不正確的用戶端金鑰和憑證。
- 用戶端憑證撤銷清單 (CRL) 已過期。

解決方案

檢查電腦上的防火牆規則是否封鎖了通訊埠 443 或 1194 的輸入TCP或輸出或UDP流量。請您的用戶端VPN管理員確認下列資訊：

- 用戶VPN端端點的防火牆規則不會封鎖TCP或UDP通訊埠 443 或 1194 上的流量。
- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- 這仍然CRL是有效的。如需詳細資訊，請參閱《AWS Client VPN 管理手冊》中的用戶VPN端無法 Connect 到用戶端端點。

文件歷史紀錄

下表說明《VPN用 AWS 戶端使用手冊》更新。

變更	描述	日期
AWS 提供的客戶端（3.15.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2024年8月12日
AWS 提供的客戶端（3.14.0）用於窗口發布	請參閱版本備註取得詳細資訊。	2024年8月12日
AWS 提供客戶端 (3.12.0) 為 macOS 發布	請參閱版本備註取得詳細資訊。	2024年8月12日
AWS 提供的客戶端（3.14.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2024年7月29日
AWS 提供的客戶端（3.13.0）的窗口發布	請參閱版本備註取得詳細資訊。	2024年7月29日
AWS 提供的客戶端（3.11.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2024年7月29日
AWS 提供的客戶端（3.12.1）為視窗發布	請參閱版本備註取得詳細資訊。	2024年7月18日
AWS 提供的客戶端（3.13.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2024年5月21 日
AWS 提供的客戶端（3.12.0）的窗口發布	請參閱版本備註取得詳細資訊。	2024年5月21 日
AWS 提供的客戶端（3.10.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2024年5月21 日
AWS 提供客戶端（3.9.2）為 macOS 發布	請參閱版本備註取得詳細資訊。	2024年4月11日

AWS 提供的客戶端（3.12.2）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2024年4月11日
AWS 提供的客戶端（3.11.2）為窗口發布	請參閱版本備註取得詳細資訊。	2024年4月11日
AWS 提供客戶端（3.9.1）為 macOS 發布	請參閱版本備註取得詳細資訊。	2024年2月16日
AWS 提供的客戶端（3.12.1）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2024年2月16日
AWS 提供的用戶端 (3.11.1) 適用於視窗已發行	請參閱版本備註取得詳細資訊。	2024年2月16日
AWS 提供的客戶端（3.12.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 12 月 19 日
AWS 提供客戶端（3.9.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 提供的客戶端（3.11.0）為窗口發布	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 提供的客戶端（3.11.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 提供的客戶端（3.10.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 提供客戶端（3.9.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日
AWS 提供的客戶端（3.8.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日
AWS 提供的客戶端（3.10.0）的窗口發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日

AWS 提供客戶端（3.9.0）為窗口發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 提供的客戶端（3.8.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 提供的客戶端（3.7.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 提供的客戶端（3.8.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供的客戶端（3.7.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供的客戶端（3.7.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供客戶端（3.6.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供客戶端（3.6.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供的客戶端（3.5.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 提供的客戶端（3.6.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS 提供的客戶端（3.5.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS 提供的客戶端（3.4.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS 提供客戶端（3.3.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 4 月 27 日

AWS 提供的客戶端（3.5.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 4 月 3 日
AWS 提供的客戶端（3.4.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 3 月 28 日
AWS 提供的客戶端（3.3.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 3 月 17 日
AWS 提供的客戶端（3.4.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2023 年 2 月 14 日
AWS 提供客戶端（3.2.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2023 年 1 月 23 日
AWS 提供的客戶端（3.2.0）為視窗發布	請參閱版本備註取得詳細資訊。	2023 年 1 月 23 日
AWS 提供客戶端（3.1.0）的 macOS 發布	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日
AWS 提供客戶端（3.1.0）為視窗發布	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日
AWS 提供客戶端（3.1.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日
AWS 提供的客戶端（3.0.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 提供的客戶端（3.0.0）為窗口發布	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 提供的客戶端（3.0.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 提供的客戶端（2.0.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日

AWS 提供的客戶端（2.0.0）為窗口發布	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日
AWS 提供的客戶端（2.0.0）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日
AWS 提供的客戶端（1.4.0）為 macOS 發布	請參閱版本備註取得詳細資訊。	2021 年 11 月 9 日
AWS 提供客戶端視窗（1.3.7）發布	請參閱版本備註取得詳細資訊。	2021 年 11 月 8 日
AWS 提供的客戶端（1.0.3）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2021 年 11 月 8 日
AWS 提供的客戶端（1.0.2）為 Ubuntu 發布	請參閱版本備註取得詳細資訊。	2021 年 9 月 28 日
AWS 提供客戶端視窗（1.3.6）和 macOS（1.3.5）發布	請參閱版本備註取得詳細資訊。	2021 年 9 月 20 日
AWS 提供客戶端為 Ubuntu 18.04 LTS 和 Ubuntu 20. LTS 04 發布	您可以在 Ubuntu 18.04 LTS 和 Ubuntu 20.04 上使用 AWS提供的客戶端。LTS	2021 年 6 月 11 日
Support VPN 使用 Windows 憑證系統存放區中的憑證開啟	您可以使用 Windows 憑證系統存放VPN區中的憑證開啟。	2021 年 2 月 25 日
自助式入口網站	您可以存取自助入口網站，以取得最新 AWS 提供的用戶端和設定檔。	2020 年 10 月 29 日
AWS 提供的客戶	您可以使用提 AWS 供的用戶端連線到用戶端VPN端點。	2020 年 2 月 4 日
初始版本	此版本介紹了 AWS 客戶端 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。