aws

用户指南

AWS Client VPN

AWS Client VPN: 用户指南

Table of Contents

什么是 AWS Client VPN？

AWS Client VPN 是一种基于客户端的托管式 VPN 服务，让您能够安全地访问 AWS 资源和本地网络中的资源。

本指南提供的步骤介绍了如何使用设备上的客户端应用程序，建立与 Client VPN 端点的 VPN 连接。

Client VPN 组件

以下是使用 AWS Client VPN 的关键组件。

- Client VPN 端点：您的 Client VPN 管理员在 AWS 中创建并配置 Client VPN 端点。您的管理员控制当您建立 VPN 连接时，您可以访问哪些网络和资源。
- VPN 客户端应用程序：用于连接到 Client VPN 端点并建立安全 VPN 连接的软件应用程序。
- Client VPN 端点配置文件：Client VPN 管理员向您提供的配置文件。此文件包括有关 Client VPN 端点以及建立 VPN 连接所需证书的信息。您将此文件加载到选择的 VPN 客户端应用程序中。AWS 提供的客户端允许您连接五个并发会话，每个会话都使用由 Client VPN 管理员提供的独立配置文件。有关并发会话的更多信息，请参阅支持并发连接。

用于配置 Client VPN 的其他资源

如果您是 Client VPN 管理员，请参阅 AWS Client VPN 管理员指南，了解有关创建和配置 Client VPN 端点的更多信息。

开始使用 AWS Client VPN

在可以建立 VPN 会话之前，您的 Client VPN 管理员必须创建并配置一个 Client VPN 端点。您的管理员控制当您访问建立 VPN 会话时您可以访问哪些网络和资源。然后，您可以使用 VPN 客户端应用程序连接到 Client VPN 端点并建立安全的 VPN 连接。

如果您是需要创建 Client VPN 端点的管理员，请参阅 AWS Client VPN 管理员指南。

主题

使用 Client VPN 的先决条件

要建立 VPN 连接，您必须满足以下条件：

- 可以访问 Internet
- 受支持的设备
- 受支持的 Windows、macOS 或 Linux 版本。
- 以下浏览器之一（对于使用基于 SAML 的联合身份验证（单点登录）的 Client VPN 端点）：
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

步骤 1：获取 VPN 客户端应用程序

您可以使用 AWS 提供的客户端或其他基于 OpenVPN 的客户端应用程序连接到 Client VPN 端点并建立 VPN 连接。

可以通过以下两种方法之一下载 Client VPN 应用程序，具体取决于管理员是否已为该应用程序创建端点配置文件：

- 如果管理员未设置端点配置文件，请从 AWS Client VPN 下载中下载并安装客户端。下载并安装应用程序后，继续执行the section called “步骤 2：获取 Client VPN 端点配置文件”，从您的管理员处获取端点配置文件。如果您要连接多个配置文件，则每个配置文件都需要一个配置文件。
- 如果您的管理员已预先配置端点配置文件，则可以从自助服务门户下载 Client VPN 应用程序以及配置文件。有关从自助服务门户下载客户端和配置文件的步骤，请参阅the section called “下载 Client VPN”。下载并安装应用程序和文件后，转至the section called “步骤 2：连接到 VPN”。

或者，在您要从中建立 VPN 连接的设备上下载并安装 OpenVPN 客户端应用程序。

步骤 2：获取 Client VPN 端点配置文件

从您的管理员处获取 Client VPN 端点配置文件。配置文件包括有关 Client VPN 端点以及建立 VPN 连接所需的证书的信息。

或者，如果您的 Client VPN 管理员已为 Client VPN 终端节点配置了自助服务门户，则可以自己下载 AWS 所提供客户端的最新版本和最新版本的 Client VPN 端点配置文件。有关更多信息，请参阅 从自助服务门户下载 AWS Client VPN。

步骤 2：连接到 VPN

将 Client VPN 端点配置文件导入 AWS 提供的客户端或您的 OpenVPN 客户端应用程序，然后连接到 VPN。有关连接到 VPN 的步骤，包括为 AWS 所提供的客户端导入一个或多个终端节点配置文件，请参阅以下主题：

- 使用 AWS 提供的客户端连接到 AWS Client VPN 终端节点
- Connect 到 AWS Client VPN 使用 OpenVPN 客户端的终端节点

对于使用 Active Directory 身份验证的 Client VPN 端点，系统将提示您输入用户名和密码。如果已为目录启用 Multi-Factor Authentication (MFA)，系统还会提示您输入 MFA 码。

对于使用基于 SAML 的联合身份验证（单点登录）的 Client VPN 端点， AWS 提供的客户端会在您的计算机上打开浏览器窗口。系统将提示您输入公司凭证，然后才能连接到 Client VPN 端点。

从自助服务门户下载 AWS Client VPN

自助服务门户是一个网页，您可以通过该网页下载 AWS 提供的客户端的最新版本和 Client VPN 端点配置文件的最新版本。如果您的 Client VPN 端点管理员已预先配置 Client VPN 客户端的一个或多个配置文件，则可以从此门户下载并安装该 Client VPN 应用程序以及这些配置文件。

> **Note**
>
> 如果您是管理员并且希望配置自助服务门户，请参阅《AWS Client VPN 管理员指南》中的 Client VPN 端点。

开始之前，您必须拥有要下载的每个 Client VPN 端点的 ID。您的 Client VPN 端点管理员可以向您提供此 ID，或者提供包含此 ID 的自助服务门户 URL。对于多个端点连接，您需要有要连接的每个配置文件的端点 ID。

访问自助服务门户

1. 通过 https://self-service.clientvpn.amazonaws.com/ 转到自助服务门户，或使用管理员提供给您的 URL。
2. 如果需要，请输入 Client VPN 端点的 ID，例如 `cvpn-endpoint-0123456abcd123456`。选择 Next (下一步)。
3. 输入您的用户名和密码，然后选择登录。这与用于连接到 Client VPN 端点的用户名和密码相同。
4. 在自助服务门户中，您可以执行以下操作：
   - 下载 Client VPN 端点的客户端配置文件的最新版本。如果要连接到多个端点，则需要下载每个端点的配置文件。
   - 下载 AWS 提供的适用于您的平台的客户端的最新版本。
5. 对要为其创建连接配置文件的每个端点配置文件重复这些步骤。

使用 AWS 提供的客户端连接到 AWS Client VPN 终端节点

你可以使用 AWS 提供的客户端连接到客户端 VPN 端点，Windows、macOS 和 Ubuntu 都支持该客户端。 AWS 提供的客户端还支持多达五个并发连接以及 OpenVPN 指令。

主题

安全性

在所 AWS 提供的客户端中，安全性是重中之重。我们会定期发布补丁以改善应用程序的安全状况。与其他 OpenVPN 客户端相比，AWS 提供的客户端包含多项独特的安全功能，包括 SAML 身份验证、客户端路由强制执行和设备设置监控。

虽然 AWS 提供的客户端旨在缓解因配置错误或受损的网络环境而产生的威胁，但它不负责修改环境或从源头消除外部威胁。所 AWS 提供的客户依靠客户来维护安全且配置良好的环境。这包括：

- 防止本地用户未经授权的修改或滥用
- 将管理权限限制为可信用户
- 维护 up-to-date安全补丁

Support 支持使用 AWS 提供的客户端进行并发连接

AWS 提供的客户端允许连接到多个并发会话。如果您需要访问多个 AWS 环境中的资源并且这些资源有不同的终端节点，这会很有用。例如，您可能需要访问环境中的数据库，该数据库所在的端点与您当前连接的端点不同，但您又不想断开当前的连接。要使您 AWS 提供的客户端能够连接到当前会话，请下载管理员为每个端点创建的配置文件，然后为每个文件创建连接配置文件。然后，使用 AWS 提供的客户端，您可以连接到多个会话，而无需与当前打开的任何会话断开连接。仅 AWS 提供的客户端支持此功能。有关连接到并发会话的步骤，请参阅以下内容：

- 使用 AWS 提供的适用于 Windows 的客户端 Connect
- 使用 AWS 提供的适用于 macOS 的客户端 Connect
- 使用 AWS 提供的适用于 Linux 的客户端 Connect

当连接到多个端点时，Client VPN 会进行检查以确保与其他打开的端点连接没有冲突。例如，是否有两个会话的 CIDR 数据块或路由策略发生冲突；或者，您是否已经使用全隧道连接进行连接。如果检查发现冲突，则不会建立连接，除非您执行以下任一操作：一是选择一个与当前已打开连接无冲突的其他连接，二是断开导致冲突的当前已打开会话。

允许进行并发 DNS 连接。届时将应用其中一个启用 DNS 的连接的 DNS 服务器。在重新连接期间，系统可能会提示您进行身份验证，具体取决于 DNS 服务器。

> **Note**
>
> 允许的最大并行会话数是五个。

OpenVPN 指令

AWS 提供的客户端支持以下 OpenVPN 指令。有关这些指令的更多信息，请参阅 OpenVPN 网站中的文档。

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- block-outside-dns
- ca
- cert
- cipher
- 客户端
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option

- ifconfig-ipv6
- inactive
- keepalive
- 键
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- ping-exit
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- 远程
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- 路由
- route-ipv6
- server-poll-timeout
- static-challenge
- tap-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN 适用于 Windows

这些部分介绍如何使用 AWS 提供的适用于 Windows x64 和 Windows Arm64 系统的客户端建立 VPN 连接。您可以通过 AWS 客户端 VPN 下载来下载并安装客户端。 AWS 提供的客户端不支持自动更新。

要求

AWS 提供的客户端同时支持 Windows x64 和 Arm64 系统。对于每种操作系统，以下条件必须满足：

Windows Arm64 操作系统

- Windows 11（64 位操作系统，Arm64 处理器）
- .NET 框架 4.8.1 或更高版本

> **Note**
>
> 此应用程序包括使用 Arm64 模拟的后台进程。Windows 11 Arm64 设备完全支持并默认启用此功能，可确保流畅运行，无需任何其他设置。有关更多信息，请参阅 How emulation works on Arm。

Windows x64 操作系统

- Windows 11（64 位操作系统，x64 处理器）
- .NET Framework 4.7.2 或更高版本

> **Note**
>
> 对于 Windows x64 和 Arm64 操作系统，即使用 SAML-based 联合身份验证（单点登录）的客户端 VPN 端点，客户端会在您的计算机上保留 TCP 端口 8096-8115。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

主题

连接到 AWS Client VPN 用一个 AWS 提供适用于 Windows 的客户端

在开始之前，请您务必阅读要求。在以下步骤中， AWS 提供的客户端也称为AWS VPN 客户端。

要使用连接 AWS 为基于 Windows x64 的系统或 Window Arm64-based s 系统提供的客户端：

1. 打开 AWS VPN 客户端应用程序。
2. 选择文件、管理配置文件。
3. 选择添加配置文件。
4. 对于显示名称，输入配置文件的名称。
5. 对于 VPN 配置文件，浏览到并选择您从 Client VPN 管理员那里收到的配置文件，然后选择添加配置文件。
6. 如果要创建多个连接，请对要添加的每个配置文件重复添加配置文件步骤。您可以根据需要添加任意数量的配置文件，但最多只能有五个打开的连接。
7. 在 AWS VPN 客户端窗口中，选择要连接的配置文件，然后选择 C onnect。如果已将客户端 VPN 终端节点配置为使用基于凭证的身份验证，系统将提示您输入用户名和密码。对要启动的每个配置文件连接重复此步骤，最多可连接五个并发端点。

   > **Note**
   >
   > 如果您连接的任何配置文件与当前打开的会话发生冲突，则您将无法建立连接。要么选择新的连接，要么断开导致冲突的会话连接。

8. 要查看连接的统计信息，请在 AWS VPN 客户端窗口中选择连接，选择显示详细信息，然后选择要查看其详细信息的连接。
9. 要断开连接，请在 AWS VPN 客户端窗口中选择一个连接，然后选择断开连接。如果您有多个打开的连接，则必须分别关闭每个连接。或者，选择 Windows 任务栏上的客户端图标，然后选择断开连接。

端点安全软件兼容性

企业端点安全产品，例如基于主机的防火墙、端点检测和响应 (EDR) 代理以及防病毒软件，有时会干扰 AWS Client VPN 连接。如果您在使用 AWS 提供的适用于 Windows 的客户端时遇到连接问题，则可能需要在终端安全软件中配置排除项。

AWS Client VPN 可执行路径

AWS 提供的 Windows 客户端安装以下关键可执行文件。在配置防火墙规则、应用程序许可名单或端点安全策略时，您可能需要这些路径。

VPN 客户端应用程序

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

OpenVPN 流程

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

这是建立和维护 VPN 隧道连接的核心过程。

Windows 服务

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

网络要求

AWS 提供的客户端需要对 Client VPN 端点进行出站网络访问才能建立 VPN 连接。确保您的防火墙或端点安全软件允许从`acvc-openvpn.exe`进程到您的 Client VPN 端点上配置的端口和协议的出站流量。

配置端点安全排除项

如果您的终端安全产品干扰了 AWS 提供的客户端连接，请与您的安全管理员一起查看以下排除类别：

Process-based 排除

将中列出的可执行文件the section called “AWS Client VPN 可执行路径”添加到您的端点安全产品的进程允许列表或排除列表中。

Network-based 排除

允许从该`acvc-openvpn.exe`进程到您的 Client VPN 端点的端口和协议的出站流量。

Path-based 排除

将 AWS 提供的客户端安装目录排除在实时扫描或行为分析之外：

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

Important

由于产品版本和配置之间存在差异，特定第三方端点安全产品的规范性配置说明不在 AWS 文档的范围之内。有关为特定产品配置排除项的详细说明，请参阅您的端点安全供应商的文档。

AWS Client VPN 适用于 Windows 的发行说明

下表包含基于 Windows x64 和基于 Windows ARM64 的系统的当前和先前版本的 AWS Client VPN 发行说明和下载链接。

Note

我们继续为每个版本提供可用性和安全性修复。强烈建议您为每一种平台使用最新版本。以前的版本可能会受到可用性 and/or 安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	日期	下载链接和 SHA256
5.3.4 (x64 和 Arm64)	• 次要错误修复和增强功能 • 改善安全状况	2026年3月27日	• 下载 Windows x64 版本 5.3.4 sha256：81 a5c510162 4c5f74de8 afdcb816f 03ea8ff9e

版本	更改	日期	下载链接和 SHA256
			a8ff9e8c6 a5eaa8890 a95779a95 779a94dbe41 • 下载 Windows Arm64 版本 5.3.4 sha256：34 10282ebb0 24e64812a 63668b301 17657d470 ed4c51f05 e96fc812b 887b887d887d

版本	更改	日期	下载链接和 SHA256
5.3.3 (x64 和 Arm64)	• 修复了 5.3.2 版中的连接故障	2026年2月28日	• 下载 Windows x64 版本 5.3.3 sha256：bbaebb977b270add6497c941505fed5913b58056e980e3721707337dc056ac86 • 下载 Windows Arm64 版本 5.3.3 sha256：c30b6d0121a5070643fdbebc27e7fdbebc27e7f9569d574a5698631480becb5cb9631480becb9631480becb963963fde

版本	更改	日期	下载链接和 SHA256
5.3.2 (x64 和 Arm64)	• 次要错误修复和增强功能。 • 改进了安保状况。	2026 年 2 月 17 日	• 下载 Windows x64 版本 5.3.2 sha256：dd 1e4fb6718 ddbf13a5a ee5421757 61bf8ed85 4290c5429 0c576a488 b98173a0a 0ccf92 • 下载 Windows Arm64 版本 5.3.2 sha256：d2 d18d91ca9 ef53cc557 434db18ef 5d0002ef5 d0002e782 5a998f2d7 39eac443b 034af00

版本	更改	日期	下载链接和 SHA256
5.3.1（x64 和 Arm64）	次要错误修复和增强功能。	2025 年 9 月 30 日	• 下载 Windows x64 版本 5.3.1 sha256：b71ddbc78230630963acf3ebba7afeb6e52599843091ff589aed6afce4c9eb06 • 下载 Windows Arm64 版本 5.3.1 sha256：e691bdb0bdcb55b3da36f4fb2e5198f20f1878dc22a00bf55bc660999698500b

版本	更改	日期	下载链接和 SHA256
5.3.0（Arı 64）	对基于 Windows ARM64 的操作系统的新 AWS Client VPN 支持。 此版本包括来自 Windows（x64）5.3.0 版的所有更新。	2025 年 8 月 26 日	下载 Windows Arm64 版本 5.3.0 sha256：3f 1be6b487a f8307dafb b0f7737cd 597cf71dc 64dcd3177 5aeeebf91 d04b8dce
5.3.0	• 次要增强功能。 • 增加了对 IPv6 连接的支持	2025 年 8 月 14 日	下载 Windows x64 版本 5.3.0 sha256： e3cf1aff6e1 4d79aa443 78229a3a0 602a9e9c2 a0c6d0d05 5df901440 b6d1454a
5.2.2	改进了安保状况。	2025 年 6 月 2 日	下载版本 5.2.2 sha256：f2 7cb0eed7c 9c5354caa 5d7e37595 eefbb048d 7481bf698 b2e5fb653 b667c190

版本	更改	日期	下载链接和 SHA256
5.2.1	• 增加了对 `ping-exit` OpenVPN 标志的支持。 • 更新了 OpenSSL 库。 • 次要错误修复和增强功能。	2025 年 4 月 21 日	不再受支持。
5.2.0	• 次要增强功能。 • 增加了对客户端路由强制执行的支持。	2025 年 4 月 8 日	不再受支持。
5.1.0	• 修复了导致 AWS Client VPN 版本 5.0.x 在非活动超时断开连接后自动重新连接到 VPN 的问题。 • 次要错误修复和增强功能。	2025 年 3 月 17 日	不再受支持。
5.0.2	• 修复了并发连接的 DNS 问题。 • 修复了安装新 TAP 适配器时的偶然性问题。	2025 年 2 月 24 日	不再受支持。
5.0.1	修复了导致 Windows 客户端版本 5.0.0 上偶然出现 VPN 连接错误的问题。	2025 年 1 月 30 日	不再受支持。
5.0.0	• 增加了对并发连接的支持。 • 更新了 TAP 驱动程序版本。 • 更新了图形用户界面。 • 次要错误修复和增强功能	2025 年 1 月 21 日	不再受支持。
4.1.0	次要错误修复和增强功能。	2024 年 11 月 12 日	不再受支持。

版本	更改	日期	下载链接和 SHA256
4.0.0	次要增强功能。	2024 年 9 月 25 日	下载版本 4.0.0 sha256：65 32f911385 ec8fac149 4d0847c8f 90a999b3b d7380844e 2ea4318e9 db4a2ebc
3.14.2	增加了对 `mssfix` OpenVPN 标志的支持。	2024 年 9 月 4 日	下载版本 3.14.2 sha256：c1 71639d7e0 7e5fd4899 8cf76f74e 6e49e5cbe 3356c6264 a67b4a9bf 473b5f5d
3.14.1	次要错误修复和增强功能。	2024 年 8 月 22 日	下载版本 3.14.1 sha256：f7 43a7b4bc8 2daa4b803 c29943905 29997bb57 a4bb54d1f 5195ab288 27283335

版本	更改	日期	下载链接和 SHA256
3.14.0	• 增加了对 `tap-sleep` OpenVPN 标志的支持。 • 更新了 OpenVPN 和 OpenSSL 库。	2024 年 8 月 12 日	下载版本 3.14.0 sha256：812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516
3.13.0	更新了 OpenVPN 和 OpenSSL 库。	2024 年 7 月 29 日	下载版本 3.13.0 sha256：c9cc896e81a74411840951e349eed9384507c53337fb703c5ec64d522c29388b
3.12.1	修复了 Windows 客户端版本 3.12.0 无法为某些用户建立 VPN 连接的问题。	2024 年 7 月 18 日	下载版本 3.12.1 sha256：5ed34aee6c03aa281e625acdbed272896c67046364a9e5846ca697e05dbfec08

版本	更改	日期	下载链接和 SHA256
3.12.0	• 当局域网范围发生更改时自动重新建立连接。 • 去除了与 SAML 端点连接时的自动应用程序焦点。	2024 年 5 月 21 日	不再受支持
3.11.2	自版本 123 起，解决了基于 Chromium 的浏览器的 SAML 身份验证问题。	2024 年 4 月 11 日	下载版本 3.11.2 sha256：8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc
3.11.1	• 修复了缓冲区溢出操作，该操作可能允许本地操作者以提升的权限执行任意命令。 • 改进了安保状况。	2024 年 2 月 16 日	下载版本 3.11.1 sha256：fb67b60aa8370197958a11ea6f57d5bc0512279560b52a857ae34cb321eaefd0

版本	更改	日期	下载链接和 SHA256
3.11.0	• 修复了由 Windows 引起的连接问题 VMs。 • 修复了某些 LAN 配置的连接问题。 • 改进了可访问性。	2023 年 12 月 6 日	下载版本 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9
3.10.0	• 修复了在客户端网络中 NAT64 启用时的连接问题。 • 修复了在客户端计算机上安装 Hyper-V 网络适配器时的连接问题。 • 次要错误修复和增强功能。	2023 年 8 月 24 日	下载版本 3.10.0 sha256：d4 6721aad40 ccb816f16 3e406c366 ff03b1120 abbb43a20 607e06d3b 1fa8667f
3.9.0	改进了安保状况。	2023 年 8 月 3 日	下载版本 3.9.0 sha256：de 9a3800ea2 349155540 bd32bbae4 72404c636 d8d8267a0 e1fb2173a 8aae21ed
3.8.0	改进了安保状况。	2023 年 7 月 15 日	不再受支持
3.7.0	回滚了版本 3.6.0 中的更改。	2023 年 7 月 15 日	不再受支持

版本	更改	日期	下载链接和 SHA256
3.6.0	改进了安保状况。	2023 年 7 月 14 日	不再受支持
3.5.0	次要错误修复和增强功能。	2023 年 4 月 3 日	不再受支持
3.4.0	回滚了版本 3.3.0 中的更改。	2023 年 3 月 28 日	不再受支持
3.3.0	次要错误修复和增强功能。	2023 年 3 月 17 日	不再受支持
3.2.0	• 添加了对“verify-x509-name”OpenVPN 标志的支持。 • 自动检测客户端的更新版本何时可用。 • 添加了在新的客户端版本可用时自动安装这些版本的功能。	2023 年 1 月 23 日	不再受支持
3.1.0	改进了安保状况。	2022 年 5 月 23 日	不再受支持
3.0.0	• 增加了对 Windows 11 的支持。 • 修复了 TAP Windows 驱动程序命名导致其他驱动程序名称受到影响的问题。 • 修复了使用联合身份验证时不显示横幅消息的问题。 • 修复了横幅文字显示以支持更长文本。 • 增强了安保状况。	2022 年 3 月 3 日	不再受支持
2.0.0	• 增加了支持在新连接建立之后显示横幅文本。 • 取消了使用与 echo 有关的拉取筛选条件（即 pull-filter * echo）的功能 • 次要错误修复和增强功能。	2022 年 1 月 20 日	不再受支持
1.3.7	• 修复了在某些情况下出现的联合身份验证连接尝试问题。 • 次要错误修复和增强功能。	2021 年 11 月 8 日	不再受支持

版本	更改	日期	下载链接和 SHA256
1.3.6	• 增加了对 OpenVPN 标志的支持：connect-retry-max、开发者类型、keepalive、ping、ping 重启、ping 重启、pull、rcvbuf、。 server-poll-timeout • 次要错误修复和增强功能。	2021 年 9 月 20 日	不再受支持
1.3.5	添加了删除大型窗口日志文件的补丁。	2021 年 8 月 16 日	不再受支持
1.3.4	• 添加了对 OpenVPN 标志的支持：dhcp 选项。 • 次要错误修复和增强功能。	2021 年 8 月 4 日	不再受支持
1.3.3	• 增加了对以下 OpenVPN 标记的支持：非活跃、下拉筛选、路由。 • 修复了导致应用程序在断开连接或退出时崩溃的问题。 • 修复了带反斜杠的 Active Directory 用户名的问题。 • 修复了在应用程序外部操作配置文件列表时应用程序崩溃的问题。 • 次要错误修复和增强功能。	2021 年 7 月 1 日	不再受支持
1.3.2	• 配置防 IPv6 漏功能后，添加防漏功能。 • 修复了在使用 Connection（连接）下的 Show Details（显示详细信息）选项时潜在的崩溃。	2021 年 5 月 12 日	不再受支持

版本	更改	日期	下载链接和 SHA256
1.3.1	• 新增了对具有相同主题的多个客户端证书的支持。过期的证书将被忽略。 • 修复了本地日志保留以减少磁盘使用。 • 新增了对“route-ipv6”OpenVPN 指令的支持。 • 次要错误修复和增强功能。	2021 年 4 月 5 日	不再受支持
1.3.0	添加了诸如错误报告、发送诊断日志和分析等支持特征。	2021 年 3 月 8 日	不再受支持
1.2.7	• 添加了对 cryptoapicert OpenVPN 指令的支持。 • 修复了连接之间的旧路由。 • 次要错误修复和增强功能。	2021 年 2 月 25 日	不再受支持
1.2.6	次要错误修复和增强功能。	2020 年 10 月 26 日	不再受支持
1.2.5	• 添加了对 OpenVPN 配置中注释的支持。 • 添加了 TLS 握手错误的错误消息。	2020 年 10 月 8 日	不再受支持
1.2.4	次要错误修复和增强功能。	2020 年 9 月 1 日	不再受支持
1.2.3	回滚版本 1.2.2 中的更改。	2020 年 8 月 20 日	不再受支持
1.2.1	次要错误修复和增强功能。	2020 年 7 月 1 日	不再受支持
1.2.0	• 增加了对基于 SAML 2.0 的联合身份验证的支持。 • 对 Windows 7 平台的支持已弃用。	2020 年 5 月 19 日	不再受支持
1.1.1	次要错误修复和增强功能。	2020 年 4 月 21 日	不再受支持

版本	更改	日期	下载链接和 SHA256
1.1.0	• 增加了对 OpenVPN 静态咨询重复功能的支持，以隐藏或显示用户界面中显示的文本。 • 次要错误修复和增强功能。	2020 年 3 月 9 日	不再受支持
1.0.0	首次发布。	2020 年 2 月 4 日	不再受支持

AWS Client VPN适用于 macOS

以下各节介绍如何使用AWS提供的适用于 macOS 的客户端建立 VPN 连接。您可以通过 AWS客户端 VPN 下载来下载并安装客户端。AWS提供的客户端不支持自动更新。

要求

要使用AWS提供的适用于 macOS 的客户端，需要满足以下条件：

- macOS Sonoma (14.0)、Sequoia (15.0) 或 Tahoe (26.0)
- 兼容 x86_64 或处理器 ARM64 。
- 对于使用基于 SAML 的联合身份验证（单点登录）的 Client VPN 端点，客户端会在您的计算机上保留 TCP 端口 8096-8115。

主题

- 连接到 AWS Client VPN 用 AWS 为 macOS 提供了客户端
- AWS Client VPN 适用于 macOS 的发行说明

连接到 AWS Client VPN 用 AWS 为 macOS 提供了客户端

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

此外，请您务必阅读要求。在以下步骤中， AWS 提供的客户端也称为AWS VPN 客户端。

要使用 “连接” AWS 为 macOS 提供了客户端

1. 打开 AWS VPN 客户端应用程序。
2. 选择文件、管理配置文件。
3. 选择添加配置文件。
4. 对于显示名称，输入配置文件的名称。
5. 对于 VPN 配置文件，浏览到并选择您从 Client VPN 管理员那里收到的配置文件，然后选择添加配置文件。
6. 如果要创建多个连接，请对要添加的每个配置文件重复添加配置文件步骤。您可以根据需要添加任意数量的配置文件，但最多只能有五个打开的连接。
7. 在 AWS VPN 客户端窗口中，选择要连接的配置文件，然后选择 C onnect。如果已将客户端 VPN 终端节点配置为使用基于凭证的身份验证，系统将提示您输入用户名和密码。对要启动的每个配置文件连接重复此步骤，最多可连接五个并发端点。

   > **Note**
   >
   > 如果您连接的任何配置文件与当前打开的会话发生冲突，则您将无法建立连接。要么选择新的连接，要么断开导致冲突的会话连接。

8. 要查看连接的统计信息，请在 AWS VPN 客户端窗口中选择连接，选择显示详细信息，然后选择要查看其详细信息的连接。
9. 要断开连接，请在 AWS VPN 客户端窗口中选择一个连接，然后选择断开连接。如果您有多个打开的连接，则必须分别关闭每个连接。

AWS Client VPN 适用于 macOS 的发行说明

下表包含适用于 macOS 的当前和先前版本 AWS Client VPN 的发行说明和下载链接。

> **Note**
>
> 我们继续为每个版本提供可用性和安全性修复。强烈建议您为每一种平台使用最新版本。以前的版本可能会受到可用性 and/or 安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	日期	下载链接
5.3.5	• 次要错误修复和增强功能 • 改善安全状况 • 在 Future 的更新中为 ARM-based Mac 用户启用了自动升级到本机 ARM64 客户端的功能，无需从 Rosetta 翻译层下运行的 Intel-based 客户端进行手动迁移	2026 年 5 月 14 日	• 下载 macOS ARM64 版本 5.3.5 sha256：048c9011b7cea43720cb92d7c2fe064c8d853b391ee499408736cba5d9111652 • 下载 macOS x64 版本 5.3.5 sha256：64a84f529a09b2ee9756dd8f5ee193b9624b3239bcd76d9f20411a72d1f93887c
5.3.4	• 移除了 ARM 机器上的英特尔兼容层 (Rosetta) 要求 • 次要错误修复和增强功能	2026 年 2 月 17 日	不再受支持。
5.3.3	• 次要错误修复和增强功能。 • 改进了安保状况。	2025年12月26日	不再受支持。
5.3.2	• 增加了对 Apple Silicon 架构的原生支持和新的 macOS ARM64 安装程序。 • 次要错误修复和增强功能。	2025 年 10 月 27 日	不再受支持。
5.3.1	• 次要错误修复和增强功能。	2025 年 9 月 9 日	不再受支持。
5.3.0	• 次要增强功能。 • 增加了对 IPv6 连接的支持。	2025 年 8 月 14 日	不再受支持。
5.2.1	• 增加了对 ping-exit OpenVPN 标志的支持。	2025 年 6 月 18 日	不再受支持。

版本	更改	日期	下载链接
	• 更新了 OpenSSL 库。 • 改进了安保状况。 • 次要错误修复和增强功能。		
5.2.0	• 次要增强功能。 • 增加了对客户端路由强制执行的支持。	2025 年 4 月 8 日	不再受支持。
5.1.0	• 修复了导致 AWS Client VPN 版本 5.0.x 在非活动超时断开连接后自动重新连接到 VPN 的问题。 • 修复了无法 AWS Client VPN 为带有 Windows-style 行尾的配置文件建立 VPN 连接的问题。 • 次要错误修复和增强功能。	2025 年 3 月 17 日	不再受支持。
5.0.3	次要错误修复和增强功能。	2025 年 3 月 6 日	不再受支持。
5.0.2	修复了在选择连接时会导致偶然性错误的问题。	2025 年 2 月 17 日	不再受支持。
5.0.1	修复了导致客户端版本 5.0.0 无法为名称包含空格的配置文件建立 VPN 连接的问题。	2025 年 1 月 22 日	不再受支持。
5.0.0	• 增加了对并发连接的支持。 • 更新了图形用户界面。 • 次要错误修复和增强功能。	2025 年 1 月 21 日	不再受支持。
4.1.0	次要错误修复和增强功能。	2024 年 11 月 12 日	不再受支持。
4.0.0	次要增强功能。	2024 年 9 月 25 日	不再受支持。

版本	更改	日期	下载链接
3.12.1	增加了对 `mssfix` OpenVPN 标志的支持。	2024 年 9 月 4 日	不再受支持。
3.12.0	• 增加了对 `tap-sleep` OpenVPN 标志的支持。 • 更新了 OpenVPN 和 OpenSSL 库。	2024 年 8 月 12 日	不再受支持。
3.11.0	• 更新了 OpenVPN 和 OpenSSL 库。	2024 年 7 月 29 日	不再受支持。
3.10.0	• 当局域网范围发生更改时自动重新建立连接。 • 修复了网络切换期间的 DNS 还原问题。 • 去除了与 SAML 端点连接时的自动应用程序焦点。	2024 年 5 月 21 日	不再受支持。
3.9.2	• 解决了 123 版以来的 Chromium-based浏览器的 SAML 身份验证问题。 • 增加了对 macOS Sonoma 的支持。停止对 macOS Big Sur 的支持。 • 改进了安保状况。	2024 年 4 月 11 日	不再受支持。
3.9.1	• 修复了缓冲区溢出操作，该操作可能允许本地操作者以提升的权限执行任意命令。 • 修复了应用程序更新下载进度条。 • 改进了安保状况。	2024 年 2 月 16 日	不再受支持。
3.9.0	• 修复了某些 LAN 配置的连接问题。 • 改进了可访问性。	2023 年 12 月 6 日	不再受支持。

版本	更改	日期	下载链接
3.8.0	• 修复了在客户端网络中启用 NAT64 时的连接问题。 • 次要错误修复和增强功能。	2023 年 8 月 24 日	不再受支持。
3.7.0	• 改进了安保状况。	2023 年 8 月 3 日	不再受支持。
3.6.0	• 改进了安保状况。	2023 年 7 月 15 日	不再受支持。
3.5.0	• 回滚了版本 3.4.0 中的更改。	2023 年 7 月 15 日	不再受支持。
3.4.0	• 改进了安保状况。	2023 年 7 月 14 日	不再受支持。
3.3.0	• 增加了对 macOS Ventura（13.0）的支持。 • 次要错误修复和增强功能。	2023 年 4 月 27 日	不再受支持。
3.2.0	• 添加了对“verify-x509-name”OpenVPN 标志的支持。 • 自动检测客户端的更新版本何时可用。 • 添加了在新的客户端版本可用时自动安装这些版本的功能。	2023 年 1 月 23 日	不再受支持。
3.1.0	• 增加了对 macOS Monterey 的支持。 • 修复了驱动器类型检测的问题。 • 改进了安保状况。	2022 年 5 月 23 日	不再受支持。
3.0.0	• 修复了使用联合身份验证时不显示横幅消息的问题。 • 修复了横幅文字显示以支持更长文本。 • 增强了安保状况。	2022 年 3 月 3 日	不再受支持。

版本	更改	日期	下载链接
2.0.0	• 增加了支持在新连接建立之后显示横幅文本。 • 取消了使用与 echo 有关的拉取筛选条件（即 pull-filter * echo）的功能 • 次要错误修复和增强功能。	2022 年 1 月 20 日	不再受支持。
1.4.0	• 添加了连接期间的 DNS 服务器监控。如果设置与 VPN 设置不匹配，则会重新配置它们。 • 修复了在某些情况下出现的联合身份验证连接尝试问题。 • 次要错误修复和增强功能。	2021 年 11 月 9 日	不再受支持。
1.3.5	• 增加了对以下 OpenVPN 标志的支持：connect-retry-max、dev-type、keepalive、ping、ping-restart、pull、rcvbuf、server-poll-timeout。 • 次要错误修复和增强功能。	2021 年 9 月 20 日	不再受支持。
1.3.4	• 添加了对 OpenVPN 标志的支持：dhcp 选项。 • 次要错误修复和增强功能。	2021 年 8 月 4 日	不再受支持。

版本	更改	日期	下载链接
1.3.3	• 增加了对以下 OpenVPN 标记的支持：非活跃、下拉筛选、路由。 • 修复了配置文件名包含空格或 Unicode 的问题。 • 修复了导致应用程序在断开连接或退出时崩溃的问题。 • 修复了带反斜杠的 Active Directory 用户名的问题。 • 修复了在应用程序外部操作配置文件列表时应用程序崩溃的问题。 • 次要错误修复和增强功能。	2021 年 7 月 1 日	不再受支持。
1.3.2	• 配置时添加 IPv6 泄漏防护功能。 • 修复了在使用 Connection（连接）下的 Show Details（显示详细信息）选项时潜在的崩溃。 • 添加守护程序日志轮换。	2021 年 5 月 12 日	不再受支持。
1.3.1	• 新增了对 macOS Big Sur（10.16）的支持。 • 修复了删除由其他应用程序配置的 DNS 设置的问题。 • 修复了在使用无效证书进行双向身份验证时导致连接问题的问题。 • 新增了对“route-ipv6”OpenVPN 指令的支持。 • 次要错误修复和增强功能。	2021 年 4 月 5 日	不再受支持。
1.3.0	添加了诸如错误报告、发送诊断日志和分析等支持特征。	2021 年 3 月 8 日	不再受支持。
1.2.5	次要错误修复和增强功能。	2021 年 2 月 25 日	不再受支持。

版本	更改	日期	下载链接
1.2.4	次要错误修复和增强功能。	2020 年 10 月 26 日	不再受支持。
1.2.3	• 添加了对 OpenVPN 配置中注释的支持。 • 添加了 TLS 握手错误的错误消息。 • 修正了一个影响部分用户的卸载错误。	2020 年 10 月 8 日	不再受支持。
1.2.2	次要错误修复和增强功能。	2020 年 8 月 12 日	不再受支持。
1.2.1	• 添加了对卸载应用程序的支持。 • 次要错误修复和增强功能。	2020 年 7 月 1 日	不再受支持。
1.2.0	• 增加了对基于 SAML 2.0 的联合身份验证的支持。 • 增加了对 macOS Catalina（10.15）的支持。	2020 年 5 月 19 日	不再受支持。
1.1.2	次要错误修复和增强功能。	2020 年 4 月 21 日	不再受支持。
1.1.1	• 修复了 DNS 无法解析的问题。 • 修复了因连接较长而导致的应用程序崩溃问题。 • 修复了 MFA 问题。	2020 年 4 月 2 日	不再受支持。
1.1.0	• 增加了对 macOS DNS 配置的支持。 • 增加了对 OpenVPN 静态咨询重复功能的支持，以隐藏或显示用户界面中显示的文本。 • 次要错误修复和增强功能。	2020 年 3 月 9 日	不再受支持。
1.0.0	首次发布。	2020 年 2 月 4 日	不再受支持。

AWS Client VPN 适用于Linux

这些部分介绍安装所 AWS 提供的 Linux 客户端，然后使用 AWS 提供的客户端建立 VPN 连接。 AWS 提供的 Linux 客户端不支持自动更新。有关最新更新和下载内容，请参阅the section called “发行说明”。

使用连接到 Client VPN 的要求 AWS 为 Linux 提供了客户端

要使用 AWS 提供的适用于 Linux 的客户端，需要满足以下条件：

- Ubuntu 22.04 LTS (AMD64)、Ubuntu 24.04 LTS（仅限 AMD64）或 Ubuntu 26.04 LTS（仅限 AMD64）

对于使用 SAML-based 联合身份验证（单点登录）的 Client VPN 端点，客户端会在您的计算机上保留 TCP 端口 8096-8115。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

主题

- 安装提供的 AWS Client VPN 适用于 Linux 的
- Connect 连接到提供的 AWS Client VPN 适用于Linux
- AWS Client VPN 适用于 Linux 的发行说明

安装提供的 AWS Client VPN 适用于 Linux 的

有多种方法可用于安装所 AWS 提供的 Linux 客户端。从以下选项中选择一种方法。在开始之前，请您务必阅读要求。

选项 1：通过程序包存储库安装

1. 将 AWS VPN 客户端公钥添加到您的 Ubuntu 操作系统。

```
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. 使用以下命令将存储库添加到您的 Ubuntu 操作系统（版本 22.04 及更高版本）：

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

3. 使用以下命令更新系统上的存储库。

```
sudo apt-get update
```

4. 使用以下命令安装所 AWS 提供的 Linux 客户端。

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

选项 2：使用 .deb 程序包文件安装

1. 通过 AWS Client VPN 下载或使用以下命令下载 .deb 文件。

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

2. 使用该dpkg实用程序安装 AWS 所提供的 Linux 客户端。

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

选项 3 – 通过 Ubuntu 软件中心安装 .deb 程序包

1. 通过 AWS Client VPN 下载下载 .deb 程序包文件。
2. 下载 .deb 程序包文件后，通过 Ubuntu 软件中心安装程序包。按照 Ubuntu Wiki 上所述的步骤，通过 Ubuntu 软件中心安装独立的 .deb 程序包。

Connect 连接到提供的 AWS Client VPN 适用于Linux

在以下步骤中， AWS 提供的客户端也称为AWS VPN 客户端。

要使用连接 AWS 为 Linux 提供了客户端

1. 打开 AWS VPN 客户端应用程序。
2. 选择文件、管理配置文件。
3. 选择添加配置文件。

4. 对于显示名称，输入配置文件的名称。
5. 对于 VPN 配置文件，浏览到您从客户端 VPN 管理员那里收到的配置文件。选择 Open。
6. 选择 Add Profile (添加配置文件)。
7. 如果要创建多个连接，请对要添加的每个配置文件重复添加配置文件步骤。您可以根据需要添加任意数量的配置文件，但最多只能有五个打开的连接。
8. 在 AWS VPN 客户端窗口中，选择要连接的配置文件，然后选择 C onnect。如果已将客户端 VPN 终端节点配置为使用基于凭证的身份验证，系统将提示您输入用户名和密码。对要启动的每个配置文件连接重复此步骤，最多可连接五个并发端点。

> **Note**
>
> 如果您连接的任何配置文件与当前打开的会话发生冲突，则您将无法建立连接。要么选择新的连接，要么断开导致冲突的会话连接。

9. 要查看连接的统计信息，请在 AWS VPN 客户端窗口中选择连接，选择显示详细信息，然后选择要查看其详细信息的连接。
10. 要断开连接，请在 AWS VPN 客户端窗口中选择一个连接，然后选择断开连接。如果您有多个打开的连接，则必须分别关闭每个连接。

AWS Client VPN 适用于 Linux 的发行说明

下表包含适用于Linux的当前和先前版本 AWS Client VPN 的发行说明和下载链接。

> **Note**
>
> 我们继续为每个版本提供可用性和安全性修复。强烈建议您为每一种平台使用最新版本。以前的版本可能会受到可用性 and/or 安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	日期	下载链接
5.3.3	• 次要错误修复和增强功能 • 改善安全状况	2026年5月18日	下载版本 5.3.3 sha256：d0096c934b36122c245d

版本	更改	日期	下载链接
			8c2243d41 46cdac671 25c7421c4 e1e6ad430 eb3adfcf
5.3.2	• 次要错误修复和增强功能。 • 改进了安保状况。	2025 年 12 月 17 日	下载版本 5.3.2 sha256：89 e4b9f2c9f 7def37167 f5f137f4ff9c6c5246 fd6e0a724 4b70c196a 17683569
5.3.1	• 次要增强功能。	2025 年 9 月 25 日	下载版本 5.3.1 sha256：4a 426cc2263 82748d683 a49463404 47dab87ec 42583977d 9488ee45d 11cdcec0

版本	更改	日期	下载链接
5.3.0	• 次要增强功能。 • 增加了对 IPv6 连接的支持。	2025 年 8 月 14 日	下载版本 5.3.0 sha256：31 edb55f12d cd68a7a4c a9b6233dd beebcd37e 01f87655a 520cc7e75 42bbfcb4
5.2.0	• 次要增强功能。 • 增加了对客户端路由强制执行的支持。	2025 年 4 月 8 日	下载版本 5.2.0 sha256：ef 7189f085d b30ef0c52 1adcdfec8 92075cb00 5c8e0014f dbcc59021 8509891f
5.1.0	• 修复了导致 AWS Client VPN 版本 5.0.x 在非活动超时断开连接后自动重新连接到 VPN 的问题。 • 次要错误修复和增强功能。	2025 年 3 月 17 日	下载版本 5.1.0 sha256：14 f26c05b11 b0cc484b0 8a8f8d207 39de3d815 c268db3bb a9ac70c0e 766b70ba

版本	更改	日期	下载链接
5.0.0	• 增加了对多个并发连接的支持。 • 更新了图形用户界面。 • 次要错误修复和增强功能。	2025 年 1 月 21 日	下载版本 5.0.0 sha256：645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c
4.1.0	• 增加了对 Ubuntu 22.04 和 24.04 的支持。 • 错误修复。	2024 年 11 月 12 日	下载版本 4.1.0 sha256：334d00222458fbfe9dade16c99fe97e9ebcbd51fff017d0d6b1d1b764e7af472
4.0.0	次要增强功能。	2024 年 9 月 25 日	下载版本 4.0.0 sha256：c2632718742 17d79783f cca182025 ace27ddbf 8f9661b56 df48843fa 17922686

版本	更改	日期	下载链接
3.15.1	增加了对 `mssfix` OpenVPN 标志的支持。	2024 年 9 月 4 日	下载版本 3.15.1 sha256：ffb65c0bc93e8d611cbce2deb6b82f600e6434e4d03c6b44c53d61a2efcaadc2
3.15.0	• 增加了对 `tap-sleep` OpenVPN 标志的支持。 • 更新了 OpenVPN 和 OpenSSL 库。	2024 年 8 月 12 日	下载版本 3.15.0 sha256：5cf3eb08de96821b0ad3d0c93174b2e308041d5490a3edb772dfd89a6d89d012
3.14.0	• 更新了 OpenVPN 和 OpenSSL 库。	2024 年 7 月 29 日	下载版本 3.14.0 sha256：bd2b401a1ede6057d725a13c77ef92147a79e0c5e0020d379e44f319b5334f60

版本	更改	日期	下载链接
3.13.0	• 当局域网范围发生更改时自动重新建立连接。	2024 年 5 月 21 日	下载版本 3.13.0 sha256：e89f3bb7fc24c148e3044b807774fcfe05e7eae9e551863a38a2dcd7e0ac05f1
3.12.2	• 解决了 123 版以来的 Chromium-based 浏览器的 SAML 身份验证问题。	2024 年 4 月 11 日	下载版本 3.12.2 sha256：f7178c33797740bd596a14cbe7b6f5f58fb79d17af79f88bd8801353a7571a7d
3.12.1	• 修复了缓冲区溢出操作，该操作可能允许本地操作者以提升的权限执行任意命令。 • 改进了安保状况。	2024 年 2 月 16 日	下载版本 3.12.1 sha256：547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0

版本	更改	日期	下载链接
3.12.0	• 修复了某些 LAN 配置的连接问题。	2023 年 12 月 19 日	下载版本 3.12.0 sha256：9b 73987309f 1dca1960a 322c5dd86 eec1568ed 270bfd25f 78cc430e3 b5f85cc1
3.11.0	• 针对“修复了某些 LAN 配置的连接问题”的回滚。 • 改进了可访问性。	2023 年 12 月 6 日	下载版本 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	• 修复了某些 LAN 配置的连接问题。 • 改进了可访问性。	2023 年 12 月 6 日	下载版本 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51

版本	更改	日期	下载链接
3.9.0	• 修复了在客户端网络中启用 NAT64 时的连接问题。 • 次要错误修复和增强功能。	2023 年 8 月 24 日	下载版本 3.9.0 sha256：6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454
3.8.0	• 改进了安保状况。	2023 年 8 月 3 日	下载版本 3.8.0 sha256：5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	• 改进了安保状况。	2023 年 7 月 15 日	不再受支持
3.6.0	• 回滚了版本 3.5.0 中的更改。	2023 年 7 月 15 日	不再受支持
3.5.0	• 改进了安保状况。	2023 年 7 月 14 日	不再受支持
3.4.0	• 添加了对“verify-x509-name”OpenVPN 标志的支持。	2023 年 2 月 14 日	不再受支持
3.1.0	• 修复了驱动器类型检测的问题。 • 改进了安保状况。	2022 年 5 月 23 日	不再受支持

版本	更改	日期	下载链接
3.0.0	• 修复了使用联合身份验证时不显示横幅消息的问题。 • 修复了横幅文本显示以支持更长文本和特定字符序列。 • 增强了安保状况。	2022 年 3 月 3 日	不再受支持。
2.0.0	• 增加了支持在新连接建立之后显示横幅文本。 • 取消了使用与 echo 有关的拉取筛选条件（即 pull-filter * echo）的功能 • 次要错误修复和增强功能。	2022 年 1 月 20 日	不再受支持。
1.0.3	• 修复了在某些情况下出现的联合身份验证连接尝试问题。 • 次要错误修复和增强功能。	2021 年 11 月 8 日	不再受支持。
1.0.2	• 增加了对以下 OpenVPN 标志的支持：connect-retry-max、dev-type、keepalive、ping、ping-restart、pull、rcvbuf、server-poll-timeout。 • 次要错误修复和增强功能。	2021 年 9 月 28 日	不再受支持。
1.0.1	• 启用了从 Ubuntu 应用程序栏退出的选项。 • 增加了对以下 OpenVPN 标记的支持：非活跃、下拉筛选、路由。 • 次要错误修复和增强功能。	2021 年 8 月 4 日	不再受支持。
1.0.0	首次发布。	2021 年 6 月 11 日	不再受支持。

Connect 到 AWS Client VPN 使用 OpenVPN 客户端的终端节点

可以使用常见的 OpenVPN 客户端应用程序与 Client VPN 端点建立连接。以下操作系统支持 Client VPN：

- Windows

  使用 Windows 证书存储区中的证书和私钥。生成证书和密钥后，您可以使用 OpenVPN GUI AWS 客户端应用程序或 OpenVPN GUI Connect 客户端建立客户端连接。有关创建证书和密钥的步骤，请参阅在 Windows 上使用证书建立 VPN 连接。

- macOS

  使用适用于 Mac OS-based Tunnelblick 或 Client VPN 的配置文件建立 VPN AWS 连接。有关更多信息，请参阅 在 macOS 上建立 VPN 连接。

- Linux

  在 Linux 上使用 OpenVPN - 网络管理器界面或 OpenVPN 应用程序建立 VPN 连接。要使用 OpenVPN - 网络管理器界面，首先需要安装网络管理器模块（如果尚未安装）。有关更多信息，请参阅 在 Linux 上建立 VPN 连接。

- Android 和 iOS

  在 Android 或 iOS 设备上使用 OpenVPN 客户端应用程序建立 VPN 连接。有关更多信息，请参阅 在 Android 和 iOS 上建立 Client VPN 连接。

> **Important**
>
> 如果已将 Client VPN 端点配置为使用SAML-based 联合身份验证，则无法使用 OpenVPN-based VPN 客户端连接到客户端 VPN 端点。这包括任何 ARM-based 架构。如果您使用的是带有 ARM 处理器的设备（例如 Apple Silicon Mac 或 ARM-based Windows 设备），则必须在 AWS 提供的客户端上使用 SAML-based VPN 端点，而不是 OpenVPN 客户端。

客户端应用程序

- Connect 到 AWS Client VPN 使用 Windows 客户端应用程序的终端节点
- Connect 到 AWS Client VPN 使用 macOS 客户端应用程序的端点

- Connect 到 AWS Client VPN 使用 OpenVPN 客户端应用程序的终端节点
- AWS Client VPN 安卓和 iOS 应用程序上的连接

Connect 到 AWS Client VPN 使用 Windows 客户端应用程序的终端节点

这些部分介绍如何使用 VPN 客户端建立 Windows-based VPN 连接。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

有关问题排查信息，请参阅问题排查 AWS 客户端 VPN 与 Windows-based 客户端的连接。

> **Important**
>
> 如果已将 Client VPN 端点配置为使用SAML-based 联合身份验证，则无法使用 OpenVPN-based VPN 客户端连接到客户端 VPN 端点。这包括任何 ARM-based 架构。如果您使用的是带有 ARM 处理器的设备（例如 Apple Silicon Mac 或 ARM-based Windows 设备），则必须在 AWS 提供的客户端上使用 SAML-based VPN 端点，而不是 OpenVPN 客户端。

任务

- 使用证书并建立 AWS Windows 上的 Client VPN 连接

使用证书并建立 AWS Windows 上的 Client VPN 连接

您可以将 OpenVPN 客户端配置为使用 Windows 证书系统存储区中的证书和私钥。当您使用智能卡作为 Client VPN 连接的一部分时，此选项非常有用。有关 OpenVPN 客户端 cryptoapicert 选项的信息，请参阅 OpenVPN 网站上的 OpenVPN 参考手册。

> **Note**
>
> 证书必须存储在本地计算机上。

使用证书并建立连接

1. 创建一个包含客户端证书和私钥的 .pfx 文件。
2. 将 .pfx 文件导入本地计算机上的个人证书存储区。有关详细信息，请参阅 Microsoft 网站上的如何使用 MMC 管理单元查看证书。
3. 验证您的帐户是否有权读取本地计算机的证书。您可以使用 Microsoft 管理控制台修改权限。有关详细信息，请参阅 Microsoft 网站上的查看本地计算机证书存储区的权限。
4. 更新 OpenVPN 配置文件并使用证书主题或证书指纹指定证书。

   以下是通过主题来指定证书的示例。

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

   以下是通过指纹来指定证书的示例。您可以使用 Microsoft 管理控制台查找指纹。有关详细信息，请参阅 Microsoft 网站上的如何检索证书的指纹。

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

5. 完成配置后，通过执行以下操作，使用 OpenVPN 建立 VPN 连接：

   - 使用 OpenVPN GUI 客户端应用程序
     1. 启动 OpenVPN 客户端应用程序。
     2. 在 Windows 任务栏上，选择Show/Hide 图标。 Right-clickOpenVPN GUI，然后选择 “导入文件”。
     3. 在“打开”对话框中，选择从您的 Client VPN 管理员处收到的配置文件，然后选择打开。
     4. 在 Windows 任务栏上，选择Show/Hide 图标。 Right-clickOpenVPN GUI，然后选择 Connect。

   - 使用 OpenVPN GUI Connect 客户端
     1. 启动 OpenVPN 应用程序，然后依次选择导入、从本地文件...。
     2. 导航到您从 VPN 管理员处收到的配置文件，然后选择 Open (打开)。

Connect 到 AWS Client VPN 使用 macOS 客户端应用程序的端点

这些部分介绍如何使用 mac VPN 客户端、Tunnelblick 或 Client OS-based VPN 建立 VPN AWS 连接。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

有关问题排查信息，请参阅问题排查 AWS 客户端 VPN 与 macOS 客户端的连接。

> **Important**
>
> 如果已将 Client VPN 端点配置为使用SAML-based 联合身份验证，则无法使用 OpenVPN-based VPN 客户端连接到客户端 VPN 端点。这包括任何 ARM-based 架构。如果您使用的是带有 ARM 处理器的设备（例如 Apple Silicon Mac 或 ARM-based Windows 设备），则必须在 AWS 提供的客户端上使用 SAML-based VPN 端点，而不是 OpenVPN 客户端。

主题

建立一个 AWS Client VPN 在 macOS 上进行连接

您可以在 macOS 计算机上使用 Tunnelblick 客户端应用程序建立 VPN 连接。

> **Note**
>
> 有关用于 macOS 的 Tunnelblick 客户端应用程序的更多信息，请参阅 Tunnelblick 网站上的 Tunnelblick 文档。

使用 Tunnelblick 建立 VPN 连接

1. 启动 Tunnelblick 客户端应用程序，然后选择 I have configuration files (我拥有配置文件)。
2. 将您从 VPN 管理员处收到的配置文件拖放到 Configurations (配置) 面板中。
3. 在 Configurations (配置) 面板中选择此配置文件，然后选择 Connect (连接)。

要建立 VPN 连接，请使用以下方法 AWS Client VPN。

1. 启动 OpenVPN 应用程序，然后依次选择导入和从本地文件...。
2. 导航到您从 VPN 管理员处收到的配置文件，然后选择 Open (打开)。

Connect 到 AWS Client VPN 使用 OpenVPN 客户端应用程序的终端节点

以下各节介绍如何使用“OpenVPN - 网络管理器”或 OpenVPN 建立 VPN 连接。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

有关问题排查信息，请参阅问题排查 AWS 客户端 VPN 与 Linux-based 客户端的连接。

> **Important**
>
> 如果已将 Client VPN 端点配置为使用SAML-based 联合身份验证，则无法使用 OpenVPN-based VPN 客户端连接到客户端 VPN 端点。这包括任何 ARM-based 架构。如果您使用的是带有 ARM 处理器的设备（例如 Apple Silicon Mac 或 ARM-based Windows 设备），则必须在 AWS 提供的客户端上使用 SAML-based VPN 端点，而不是 OpenVPN 客户端。

主题

建立一个 AWS Client VPN Linux 上的连接

使用 Ubuntu 计算机上的网络管理器 GUI 或 OpenVPN 应用程序建立 VPN 连接。

使用“OpenVPN - 网络管理器”建立 VPN 连接

1. 使用以下命令安装网络管理器模块。

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

2. 依次转到 Settings (设置) 和 Network (网络)。
3. 选择 VPN 旁边的加号（ + ），然后选择从文件导入...。
4. 导航到您从 VPN 管理员处收到的配置文件，然后选择 Open (打开)。
5. 在 Add VPN (添加 VPN) 窗口中，选择 Add (添加)。
6. 通过启用您添加的 VPN 配置文件旁边的开关来启动连接。

使用 OpenVPN 建立 VPN 连接

1. 使用以下命令安装 OpenVPN。

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

2. 通过加载您从 VPN 管理员处收到的配置文件来启动连接。

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

AWS Client VPN 安卓和 iOS 应用程序上的连接

Important

如果已将 Client VPN 端点配置为使用SAML-based 联合身份验证，则无法使用 OpenVPN-based VPN 客户端连接到客户端 VPN 端点。这包括任何 ARM-based 架构。如果您使用的是带有 ARM 处理器的设备（例如 Apple Silicon Mac 或 ARM-based Windows 设备），则必须在 AWS 提供的客户端上使用 SAML-based VPN 端点，而不是 OpenVPN 客户端。

以下信息说明如何在 Android 或 iOS 移动设备上使用 OpenVPN 客户端应用程序建立 VPN 连接。用于 Android 和 iOS 的步骤是相同的。

Note

有关下载和使用适用于 iOS 或 Android 的 OpenVPN 客户端应用程序的更多信息，请参阅 OpenVPN 网站上的 OpenVPN Connect 用户指南。

在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。如果要同时连接到多个配置文件，则需要为每个配置文件提供一个配置文件。

要建立连接，请启动 OpenVPN 客户端应用程序，然后导入您从 Client VPN 管理员那里收到的文件。

问题排查 AWS 客户端 VPN 连接

使用以下主题排查您在使用客户端应用程序连接到 Client VPN 端点时可能遇到的问题。

主题

由管理员排查 Client VPN 端点问题

本指南中的一些步骤可以由您执行。其他步骤必须由您的 Client VPN 管理员在 Client VPN 端点本身上执行。以下部分说明您需要联系管理员的情况。

有关排查 Client VPN 端点问题的其他信息，请参阅《AWS Client VPN 管理员指南》中的排查 Client VPN 问题。

将诊断日志发送到 AWS 支持 在 AWS 提供的客户端

如果您在使用 AWS 提供的客户端时遇到问题，需要联系 AWS 支持 以帮助进行故障排除，则 AWS 提供的客户端可以选择将诊断日志发送到 AWS 支持。该选项在 Windows、macOS 和 Linux 客户端应用程序中都可用。

在发送文件之前，您必须同意 AWS 支持 允许访问您的诊断日志。在您同意后，我们会向您提供一个参考号， AWS 支持 以便他们可以立即访问文件。

发送诊断日志

在以下步骤中， AWS 提供的客户端也称为AWS VPN 客户端。

要使用发送诊断日志 AWS 提供适用于 Windows 的客户端

1. 打开 AWS VPN 客户端应用程序。

2. 选择帮助，发送诊断日志。
3. 在发送诊断日志窗口中，选择是。
4. 在发送诊断日志窗口中，请执行以下操作之一：
   - 要将参考编号复制到剪贴板，请选择 Yes (是)，然后选择 OK (确定)。
   - 要手动跟踪参考编号，请选择否。

   当您联系时 AWS 支持，您需要向他们提供参考号。

要使用发送诊断日志 AWS 为 macOS 提供了客户端

1. 打开 AWS VPN 客户端应用程序。
2. 选择帮助，发送诊断日志。
3. 在发送诊断日志窗口中，选择是。
4. 记下确认窗口中的参考编号，然后选择确定。

   当您联系时 AWS 支持，您需要向他们提供参考号。

要使用发送诊断日志 AWS 为 Ubuntu 提供了客户端

1. 打开 AWS VPN 客户端应用程序。
2. 选择帮助，发送诊断日志。
3. 在发送诊断日志窗口中，选择 Send (发送)。
4. 记下确认窗口中的参考编号。可以选择将信息复制到剪贴板。

   当您联系时 AWS 支持，您需要向他们提供参考号。

问题排查 AWS 客户端 VPN 与 Windows-based 客户端的连接

以下各节包含有关您在使用 Windows-based 客户端连接到 Client VPN 端点时可能遇到的问题的信息。

AWS 提供的客户端事件日志

AWS 提供的客户端会创建事件日志并将其存储在您计算机上的以下位置。

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

提供以下日志类型：

- 应用程序日志：包含有关应用程序的信息。这些日志的前缀为“aws_vpn_client_”。
- OpenVPN 日志：包含有关 OpenVPN 进程的信息。这些日志的前缀是“ovpn_aws_vpn_client_”。

AWS 提供的客户端使用 Windows 服务执行根目录操作。Windows 服务日志存储在计算机的以下位置。

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

故障排除主题

- 客户端无法连接
- 客户端无法连接，并显示 “无 TAP-Windows 适配器” 日志消息
- 客户端卡在重新连接状态
- VPN 连接进程意外退出
- 应用程序无法启动
- 客户端无法创建配置文件
- VPN 断开连接并显示弹出消息
- 使用 Windows 10 或 11 的 Dell PC 上出现客户端崩溃问题
- OpenVPN GUI
- OpenVPN 连接客户端
- 无法解析 DNS
- 缺少 PKI 别名

客户端无法连接

问题

AWS 提供的客户端无法连接到 Client VPN 端点。

原因

出现此问题的原因可能是以下原因之一：

- 计算机上已有另一个 OpenVPN 进程在运行，这会阻止客户端连接。
- 您的配置（.ovpn）文件无效。

解决方案

确保您的计算机上是否运行其他 OpenVPN 应用程序。如果在运行这些应用程序，请停止或退出这些进程，然后再次尝试连接到客户端 VPN 终端节点。检查 OpenVPN 日志中的错误，并要求客户端 VPN 管理员验证以下信息：

- 配置文件包含正确的客户端密钥和证书。有关更多信息，请参阅 AWS Client VPN 管理员指南中的导出客户端配置。
- CRL 仍然有效。有关更多信息，请参阅 AWS Client VPN 管理员指南中的客户端无法连接到客户端 VPN 终端节点。

客户端无法连接，并显示 “无 TAP-Windows 适配器” 日志消息

问题

AWS 提供的客户端无法连接到 Client VPN 端点，应用程序日志中会显示以下错误消息：“此系统上没有 TAP-Windows 适配器。您应该能够通过 TAP-Windows 转到 “开始”-> “所有程序”-> “实用程序”-TAP-Windows > “添加新的 TAP-Windows 虚拟以太网适配器” 来创建适配器。

解决方案

您可以通过采取以下一项或多项操作来修复此问题：

- 重新启动 TAP-Windows 适配器。
- 重新安装 TAP-Windows 驱动程序。
- 创建新的 TAP-Windows 适配器。

客户端卡在重新连接状态

问题

AWS 提供的客户端正在尝试连接到 Client VPN 端点，但处于重新连接状态。

原因

出现此问题的原因可能是以下原因之一：

- 您的计算机未连接到 Internet。
- DNS 主机名不会解析为 IP 地址。
- OpenVPN 进程无限期地尝试连接到终端节点。

解决方案

验证您的计算机已连接到 Internet。要求客户端 VPN 管理员验证配置文件中的 `remote` 指令是否解析为有效的 IP 地址。也可以在 VPN 客户端窗口中选择 “断开连接” 来断开 AWS VPN 会话，然后重试连接。

VPN 连接进程意外退出

问题

连接到 Client VPN 端点时，客户端意外退出。

原因

TAP-Windows 未安装在您的计算机上。运行客户端需要此软件。

解决方案

重新运行 AWS 提供的客户端安装程序以安装所有必需的依赖项。

应用程序无法启动

问题

在 Windows 7 上，当你尝试打开 AWS 提供的客户端时，它不会启动。

原因

计算机上未安装 .NET Framework 4.7.2 或更高版本。这是运行客户端所需的。

解决方案

重新运行 AWS 提供的客户端安装程序以安装所有必需的依赖项。

客户端无法创建配置文件

问题

在您尝试使用 AWS 提供的客户端创建配置文件时收到了以下错误。

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

原因

如果 Client VPN 端点使用双向身份验证，则配置（.ovpn）文件未包含客户端证书和密钥。

解决方案

确保您的客户端 VPN 管理员将客户端证书和密钥添加到配置文件中。有关更多信息，请参阅 AWS Client VPN 管理员指南中的导出客户端配置。

VPN 断开连接并显示弹出消息

问题

VPN 断开连接并弹出消息，指出：“由于您的设备所连接的本地网络的地址空间已更改，因此即将终止 VPN 连接。请建立新的 VPN 连接。”

原因

TAP-Windows 适配器不包含所需的描述。

解决方案

如果下面的`Description`字段不匹配，请先移除 TAP-Windows 适配器，然后重新运行 AWS 提供的客户端安装程序以安装所有必需的依赖项。

```
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
```

使用 Windows 10 或 11 的 Dell PC 上出现客户端崩溃问题

问题

在运行 Windows 10 或 11 的某些 Dell PC（台式机和笔记本电脑）上，当您浏览文件系统以导入 VPN 配置文件时，可能会出现客户端崩溃的问题。如果出现此问题，您将在 AWS 提供的客户端的日志中看到如下消息：

```
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中的戴尔备份和恢复系统可能会导致与 AWS 提供的客户机发生冲突，尤其是与以下三个DLL发生冲突：

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

解决方案

为避免出现此问题，请首先确保您的客户机与所 AWS 提供客户端的最新版本保持同步。转到 AWS Client VPN 下载，如果有更新的版本，则升级到最新版本。

此外请执行下面的任意一项操作：

- 如果您使用的是 Dell Backup and Recovery 应用程序，请确保该应用程序已经更新。一篇 Dell 论坛帖子表示该问题已在该应用程序的较新版本中得到解决。

- 如果您使用的不是 Dell Backup and Recovery 应用程序，如果遇到此问题，仍需采取一些措施。如果您不想升级应用程序，则可以删除或重命名 DLL 文件。但请注意，这将导致 Dell Backup and Recovery 应用程序无法完整运行。

删除或重命名 DLL 文件

1. 打开 Windows 资源管理器并浏览到 Dell Backup and Recovery 的安装位置。该应用程序通常安装在以下位置，但有时您可能需要使用搜索功能。

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

2. 从安装目录中手动删除以下 DLL 文件，或将其重命名。这两种操作都将避免加载它们。

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

   您可以通过在文件名末尾添加 “.bak” 来重命名文件，例如，。DBROverlayIconBackuped.dll.bak

OpenVPN GUI

在 Windows 10 家庭版（64 位）和 Windows Server 2016（64 位） 上，测试了 11.10.0.0 和 11.11.0.0 版本的 OpenVPN GUI 软件的以下故障排查信息。

配置文件存储在计算机的以下位置。

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

连接日志存储在计算机的以下位置。

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

OpenVPN 连接客户端

在 Windows 10 家庭版（64 位）和 Windows Server 2016（64 位） 上，测试了 2.6.0.100 和 2.7.1.101 版本的 OpenVPN Connect 客户端软件的以下故障排查信息。

配置文件存储在计算机的以下位置。

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

连接日志存储在计算机的以下位置。

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

无法解析 DNS

问题

连接失败并显示以下错误。

```
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

无法解析 DNS 名称。客户端必须在 DNS 名称前附加一个随机字符串，以防止 DNS 缓存；但是，某些客户端不这样做。

解决方案

请参阅 AWS Client VPN 管理员指南中的无法解析客户端 VPN 终端节点 DNS 名称的解决方案。

缺少 PKI 别名

问题

与不使用双向身份验证的 Client VPN 端点的连接失败，并出现以下错误。

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

原因

OpenVPN Connect 客户端软件有一个已知问题，它尝试使用双向身份验证进行身份验证。如果配置文件不包含客户端密钥和证书，则身份验证将失败。

解决方案

在 Client VPN 配置文件中指定随机客户端密钥和证书，然后将新配置导入 OpenVPN Connect 客户端软件。或者，使用不同的客户端，例如 OpenVPN GUI 客户端 (v11.12.0.0) 或 Viscosity 客户端 (v.1.7.14)。

问题排查 AWS 客户端 VPN 与 macOS 客户端的连接

以下部分包含有关使用 macOS 客户端时可能遇到的日志记录和问题的信息。请确保您正在运行这些客户端的最新版本。

AWS 提供的客户端事件日志

AWS 提供的客户端会创建事件日志并将其存储在您计算机上的以下位置。

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

提供以下日志类型：

- 应用程序日志：包含有关应用程序的信息。这些日志的前缀为“aws_vpn_client_”。
- OpenVPN 日志：包含有关 OpenVPN 进程的信息。这些日志的前缀是“ovpn_aws_vpn_client_”。

AWS 提供的客户端使用客户端守护程序来执行 root 操作。守护程序日志存储在计算机的以下位置。

```
/var/log/AWSVPNClient/AcvcHelperErrLog.txt
/var/log/AWSVPNClient/AcvcHelperOutLog.txt
```

AWS 提供的客户端将配置文件存储在您计算机上的以下位置。

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

故障排除主题

- 客户端无法连接
- 客户端卡在重新连接状态
- 客户端无法创建配置文件
- 需要具备助手工具错误
- Tunnelblick
- 未找到密码算法 “AES-256-GCM”

- 连接停止响应并重置
- 扩展密钥用法 (EKU)
- 过期的证书
- OpenVPN
- 无法解析 DNS

客户端无法连接

问题

AWS 提供的客户端无法连接到 Client VPN 端点。

原因

出现此问题的原因可能是以下原因之一：

- 计算机上已有另一个 OpenVPN 进程在运行，这会阻止客户端连接。
- 您的配置（.ovpn）文件无效。

解决方案

确保您的计算机上是否运行其他 OpenVPN 应用程序。如果在运行这些应用程序，请停止或退出这些进程，然后再次尝试连接到客户端 VPN 终端节点。检查 OpenVPN 日志中的错误，并要求客户端 VPN 管理员验证以下信息：

- 配置文件包含正确的客户端密钥和证书。有关更多信息，请参阅 AWS Client VPN 管理员指南中的导出客户端配置。
- CRL 仍然有效。有关更多信息，请参阅 AWS Client VPN 管理员指南中的客户端无法连接到客户端 VPN 终端节点。

客户端卡在重新连接状态

问题

AWS 提供的客户端正在尝试连接到 Client VPN 端点，但处于重新连接状态。

原因

出现此问题的原因可能是以下原因之一：

- 您的计算机未连接到 Internet。
- DNS 主机名不会解析为 IP 地址。
- OpenVPN 进程无限期地尝试连接到终端节点。

解决方案

验证您的计算机已连接到 Internet。要求客户端 VPN 管理员验证配置文件中的 `remote` 指令是否解析为有效的 IP 地址。也可以在 VPN 客户端窗口中选择 “断开连接” 来断开 AWS VPN 会话，然后重试连接。

客户端无法创建配置文件

问题

在您尝试使用 AWS 提供的客户端创建配置文件时收到了以下错误。

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

原因

如果 Client VPN 端点使用双向身份验证，则配置（.ovpn）文件未包含客户端证书和密钥。

解决方案

确保您的客户端 VPN 管理员将客户端证书和密钥添加到配置文件中。有关更多信息，请参阅 AWS Client VPN 管理员指南中的导出客户端配置。

需要具备助手工具错误

问题

在尝试连接 VPN 时，遇到以下错误。

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

解决方案

请参阅以下关于 re AWS : Post 的文章。AWS VPN Client - 需要助手工具错误

Tunnelblick

在 macOS High Sierra 10.13.6 上测试了 Tunnelblick 软件版本 3.7.8（build 5180）的以下故障排查信息。

私有配置的配置文件存储在计算机的以下位置。

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

共享配置的配置文件存储在计算机的以下位置。

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

连接日志存储在计算机的以下位置。

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

要增加日志详细程度，请打开 Tunnelblick 应用程序，选择 Settings (设置)，然后调整 VPN log level (VPN 日志级别) 的值。

未找到密码算法 “AES-256-GCM”

问题

连接失败，并在日志中返回以下错误。

```
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

该应用程序使用的OpenVPN版本不支持密码算法。 AES-256-GCM

解决方案

通过执行以下操作来选择兼容的 OpenVPN 版本：

1. 打开 Tunnelblick 应用程序。
2. 选择设置。

3. 对于 OpenVPN version (OpenVPN 版本)，请选择 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - OpenSSL 版本为 v1.0.2q)。

连接停止响应并重置

问题

连接失败，并在日志中返回以下错误。

```
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

客户端证书已吊销。连接在尝试进行身份验证后停止响应，并最终从服务器端重置。

解决方案

请求 Client VPN 管理员提供新的配置文件。

扩展密钥用法 (EKU)

问题

连接失败，并在日志中返回以下错误。

```
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

服务器身份验证成功。但是，客户端身份验证失败，因为客户端证书已为服务器身份验证启用了扩展密钥用法 (EKU) 字段。

解决方案

确保您使用的是正确的客户端证书和密钥。如有必要，请与您的 Client VPN 管理员进行验证。如果使用服务器证书而不是客户端证书连接到 Client VPN 端点，则可能会发生此错误。

过期的证书

问题

服务器身份验证成功，但客户端身份验证失败，并显示以下错误。

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

原因

客户端证书有效性已过期。

解决方案

请求 Client VPN 管理员提供新的客户端证书。

OpenVPN

在 macOS High Sierra 10.13.6 上测试了 OpenVPN Connect 客户端版本 2.7.1.100 的以下故障排查信息。

配置文件存储在计算机的以下位置。

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

连接日志存储在计算机的以下位置。

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

无法解析 DNS

问题

连接失败并显示以下错误。

```
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

OpenVPN Connect 无法解析 Client VPN DNS 名称。

解决方案

请参阅 AWS Client VPN 管理员指南中的无法解析客户端 VPN 终端节点 DNS 名称的解决方案。

问题排查 AWS 客户端 VPN 与 Linux-based 客户端的连接

以下各节包含有关日志记录以及您在使用 Linux-based 客户端时可能遇到的问题的信息。请确保您正在运行这些客户端的最新版本。

主题

- AWS 提供的客户端事件日志
- DNS 查询转到默认名称服务器
- OpenVPN（命令行）
- 通过 Network Manager 建立 OpenVPN (GUI)

AWS 提供的客户端事件日志

AWS 提供的客户端将日志文件和配置文件存储在系统的以下位置：

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

AWS 提供的客户端守护程序进程将日志文件存储在系统的以下位置：

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

例如，您可以检查以下日志文件以查找 DNS up/down 脚本中导致连接失败的错误：

- `/var/log/aws-vpn-client/configure-dns-up.log`
- `/var/log/aws-vpn-client/configure-dns-down.log`

DNS 查询转到默认名称服务器

问题

在某些情况下，建立 VPN 连接后，DNS 查询仍会转到默认系统名称服务器，而不是为 ClientVPN 端点配置的名称服务器。

原因

客户端与 systemd-resolved 交互，后者是 Linux 系统上提供的一项服务，也是 DNS 管理的核心组件之一。它用于配置从 Client VPN 端点推送的 DNS 服务器。出现问题的原因是 systemd-resolved 未为 Client VPN 端点提供的 DNS 服务器设置最高优先级。相反，它将服务器附加到在本地系统上配置的现有 DNS 服务器列表中。因此，原始 DNS 服务器可能仍具有最高优先级，因此可用于解析 DNS 查询。

解决方案

1. 在 OpenVPN 配置文件的第一行中添加以下指令，以确保所有 DNS 查询都发送到 VPN 隧道。

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

2. 使用 systemd-resolved 提供的存根解析程序。要确保这一点，请通过在系统上运行以下命令将符号链接 `/etc/resolv.conf` 链接到 `/run/systemd/resolve/stub-resolv.conf`。

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

3. （可选）如果您不想要 systemd-resolved 代理 DNS 查询，而是希望查询直接发送到真正的 DNS 名称服务器，则将符号链接 `/etc/resolv.conf` 链接到 `/run/systemd/resolve/resolv.conf`。

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

   您可能希望执行此操作以绕过 systemd-resolved 配置，例如 DNS 应答缓存、每接口 DNS 配置、DNSSec 实施等。当您需要在连接到 VPN 时使用私有记录覆盖公共 DNS 记录时，此选项特别有用。例如，您的私有 VPC 中可能有一个带有 www.example.com 记录的私有 DNS 解析程序，该记录可解析为私有 IP。此选项可用于覆盖 www.example.com 的公共记录，该记录可解析为公有 IP。

OpenVPN（命令行）

问题

连接无法正常工作，因为 DNS 解析不起作用。

原因

Client VPN 端点上未配置 DNS 服务器，或者客户端软件未遵循该服务器。

解决方案

使用以下步骤检查 DNS 服务器是否已配置并正常工作。

1. 确保日志中存在 DNS 服务器条目。在以下示例中，在最后一行中返回 DNS 服务器 `192.168.0.2`（在 Client VPN 端点中配置）。

   ```
   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
   ```

   如果未指定 DNS 服务器，请要求 Client VPN 管理员修改 Client VPN 端点，并确保已为 Client VPN 端点指定了 DNS 服务器（例如 VPC DNS 服务器）。有关更多信息，请参阅 AWS Client VPN 管理员指南中的 Client VPN 端点。
2. 通过运行以下命令确保已安装 `resolvconf` 软件包。

```
sudo apt list resolvconf
```

输出应返回以下内容。

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

如果未安装，请使用以下命令进行安装。

```
sudo apt install resolvconf
```

3. 在文本编辑器中打开 Client VPN 配置文件（.ovpn 文件）并添加以下行。

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

检查日志以验证是否已调用 `resolvconf` 脚本。日志应包含类似于以下内容的行。

```
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
```

通过 Network Manager 建立 OpenVPN (GUI)

问题

使用 Network Manager OpenVPN 客户端时，连接失败并显示以下错误。

```
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

未遵守 `remote-random-hostname` 标志，并且客户端无法使用 `network-manager-gnome` 软件包进行连接。

解决方案

请参阅 AWS Client VPN 管理员指南中的无法解析客户端 VPN 终端节点 DNS 名称的解决方案。

常见故障排除 AWS Client VPN 问题

以下是您在使用客户端连接到 Client VPN 端点时可能遇到的常见问题。

TLS 密钥协商失败

问题

TLS 协商失败并显示以下错误。

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

原因

出现此问题的原因可能是以下原因之一：

- 防火墙规则阻止 UDP 或 TCP 流量。
- 您在配置 (.ovpn) 文件中使用的客户端密钥和证书不正确。
- 客户端证书吊销列表 (CRL) 已过期。

解决方案

查看计算机上的防火墙规则是否阻止端口 443 或 1194 上的入站或出站 TCP 或 UDP 流量。请 Client VPN 管理员验证以下信息：

- Client VPN 端点的防火墙规则未阻止端口 443 或 1194 上的 TCP 或 UDP 流量。
- 配置文件包含正确的客户端密钥和证书。有关更多信息，请参阅 AWS Client VPN 管理员指南中的导出客户端配置。
- CRL 仍然有效。有关更多信息，请参阅 AWS Client VPN 管理员指南中的客户端无法连接到客户端 VPN 终端节点。

文档历史记录

下表描述了《 AWS Client VPN 用户指南》的更新。

变更	说明	日期
AWS 为 Ubuntu 提供的客户端 (5.3.3) 已发布	请参阅发行说明了解详细信息。	2026年5月18日
AWS 为 macOS 提供客户端 (5.3.5) ARM64 和 x64 已发布	请参阅发行说明了解详细信息。	2026 年 5 月 14 日
AWS 已发布适用于 Windows ARM64 和 x64 的客户端 (5.3.4)	请参阅发行说明了解详细信息。	2026 年 3 月 26 日
AWS 已发布适用于 Windows ARM64 和 x64 的客户端 (5.3.3)	请参阅发行说明了解详细信息。	2026年2月28日
AWS 为 macOS 提供客户端 (5.3.4) ARM64 和 x64 已发布	请参阅发行说明了解详细信息。	2026 年 2 月 17 日
AWS 已发布适用于 Windows ARM64 和 x64 的客户端 (5.3.2)	请参阅发行说明了解详细信息。	2026 年 2 月 17 日
AWS 为 macOS 提供客户端 (5.3.3) ARM64 和 x64 已发布	请参阅发行说明了解详细信息。	2025年12月26日
AWS 为 Ubuntu 提供的客户端 (5.3.2) 已发布	请参阅发行说明了解详细信息。	2025 年 12 月 17 日
AWS 已发布适用于 macOS x64 的客户端 (5.3.2)	请参阅发行说明了解详细信息。	2025 年 10 月 27 日
AWS 为 macOS ARM64 系统提供的客户端 (5.3.2) 已发布	现在增加了对 macOS ARM64-based 操作系统的支持。其中包括专为 macOS ARM64 系统	2025 年 10 月 27 日

	下载的新 AWS Client VPN 版本 5.3.2。请参阅 Client VPN for macOS Requirements 了解更多详情，参阅 AWS Client VPN for macOS release notes 获取下载链接。	
AWS 提供的适用于 Windows x64 的客户端 (5.3.1) 和 Arm64 已发布	请参阅发行说明了解详细信息。	2025 年 9 月 30 日
AWS 提供的 macOS 客户端现在支持 Tahoe (26.0)	请参阅“要求”部分了解详情。	2025 年 9 月 25 日
AWS 为 Ubuntu 提供的客户端 (5.3.1) 已发布	请参阅发行说明了解详细信息。	2025 年 9 月 25 日
AWS 已发布适用于 macOS 的客户端 (5.3.1)	请参阅发行说明了解详细信息。	2025 年 9 月 9 日
AWS 为 Windows Arm64 系统提供的客户端 (5.3.0) 已发布	现在增加了对 Windows Arm64-based 操作系统的支持。其中包括专为 Windows Arm64 系统下载的新 AWS Client VPN 版本 5.3.0。请参阅 Client VPN for Windows Requirements 了解更多详情，参阅 AWS Client VPN for Windows release notes 获取下载链接。	2025 年 8 月 26 日
AWS 已发布适用于 macOS 的客户端 (5.3.0)	请参阅发行说明了解详细信息。	2025 年 8 月 14 日
AWS 提供的适用于 Windows 的客户端 (5.3.0) 已发布	请参阅发行说明了解详细信息。	2025 年 8 月 14 日
AWS 为 Ubuntu 提供的客户端 (5.3.0) 已发布	请参阅发行说明了解详细信息。	2025 年 8 月 14 日

AWS 已发布适用于 macOS 的客户端 (5.2.1)	请参阅发行说明了解详细信息。	2025 年 6 月 18 日
AWS 提供的适用于 Windows 的客户端 (5.2.2) 已发布	请参阅发行说明了解详细信息。	2025 年 6 月 2 日
AWS 提供的适用于 Windows 的客户端 (5.2.1) 已发布	请参阅发行说明了解详细信息。	2025 年 4 月 21 日
AWS 已发布适用于 macOS 的客户端 (5.2.0)	请参阅发行说明了解详细信息。	2025 年 4 月 8 日
AWS 提供的适用于 Windows 的客户端 (5.2.0) 已发布	请参阅发行说明了解详细信息。	2025 年 4 月 8 日
AWS 为 Ubuntu 提供的客户端 (5.2.0) 已发布	请参阅发行说明了解详细信息。	2025 年 4 月 8 日
AWS 已发布适用于 macOS 的客户端 (5.1.0)	请参阅发行说明了解详细信息。	2025 年 3 月 17 日
AWS 提供的适用于 Windows 的客户端 (5.1.0) 已发布	请参阅发行说明了解详细信息。	2025 年 3 月 17 日
AWS 为 Ubuntu 提供的客户端 (5.1.0) 已发布	请参阅发行说明了解详细信息。	2025 年 3 月 17 日
移除了对 macOS Monterey 的支持并增加了对 macOS Sonoma（14.0）的支持	请参阅 Client VPN for macOS Requirements 了解详情。	2025 年 3 月 12 日
移除了对 Ubuntu 18.0.4（LTS）和 Ubuntu 20.04 LTS（仅限 AMD64）的支持	请参阅 Client VPN for Linux Requirements 了解详情。	2025 年 3 月 12 日
AWS 已发布适用于 macOS 的客户端 (5.0.3)	请参阅发行说明了解详细信息。	2025 年 3 月 6 日
AWS 已发布适用于 Windows 的客户端 (5.0.2)	请参阅发行说明了解详细信息。	2025 年 2 月 24 日

AWS 已发布适用于 macOS 的客户端 (5.0.2)	请参阅发行说明了解详细信息。	2025 年 2 月 17 日
AWS 提供的适用于 Windows 的客户端 (5.0.1) 已发布	请参阅发行说明了解详细信息。	2025 年 1 月 30 日
AWS 已发布适用于 macOS 的客户端 (5.0.1)	请参阅发行说明了解详细信息。	2025 年 1 月 22 日
AWS 提供的客户端现在最多支持五个并发连接	有关详细信息，请参阅 Support 支持使用 AWS 提供的客户端进行并发连接。	2025 年 1 月 21 日
AWS 已发布适用于 macOS 的客户端 (5.0.0)	请参阅发行说明了解详细信息。	2025 年 1 月 21 日
AWS 提供的适用于 Windows 的客户端 (5.0.0) 已发布	请参阅发行说明了解详细信息。	2025 年 1 月 21 日
AWS 为 Ubuntu 提供的客户端 (5.0.0) 已发布	请参阅发行说明了解详细信息。	2024 年 11 月 12 日
AWS 已发布适用于 macOS 的客户端 (4.1.0)	请参阅发行说明了解详细信息。	2024 年 11 月 12 日
AWS 提供的适用于 Windows 的客户端 (4.1.0) 已发布	请参阅发行说明了解详细信息。	2024 年 11 月 12 日
AWS 为 Ubuntu 提供的客户端 (4.1.0) 已发布	请参阅发行说明了解详细信息。	2024 年 11 月 12 日
AWS 已发布适用于 macOS 的客户端 (4.0.0)	请参阅发行说明了解详细信息。	2024 年 9 月 25 日
AWS 提供的适用于 Windows 的客户端 (4.0.0) 已发布	请参阅发行说明了解详细信息。	2024 年 9 月 25 日
AWS 为 Ubuntu 提供的客户端 (4.0.0) 已发布	请参阅发行说明了解详细信息。	2024 年 9 月 25 日

AWS 为 Ubuntu 提供的客户端 (3.15.1) 已发布	请参阅发行说明了解详细信息。	2024 年 9 月 4 日
AWS 提供的适用于 Windows 的客户端 (3.14.2) 已发布	请参阅发行说明了解详细信息。	2024 年 9 月 4 日
AWS 已发布适用于 macOS 的客户端 (3.12.1)	请参阅发行说明了解详细信息。	2024 年 9 月 4 日
AWS 提供的适用于 Windows 的客户端 (3.14.1) 已发布	请参阅发行说明了解详细信息。	2024 年 8 月 22 日
AWS 为 Ubuntu 提供的客户端 (3.15.0) 已发布	请参阅发行说明了解详细信息。	2024 年 8 月 12 日
AWS 提供的适用于 Windows 的客户端 (3.14.0) 已发布	请参阅发行说明了解详细信息。	2024 年 8 月 12 日
AWS 已发布适用于 macOS 的客户端 (3.12.0)	请参阅发行说明了解详细信息。	2024 年 8 月 12 日
AWS 为 Ubuntu 提供的客户端 (3.14.0) 已发布	请参阅发行说明了解详细信息。	2024 年 7 月 29 日
AWS 提供的适用于 Windows 的客户端 (3.13.0) 已发布	请参阅发行说明了解详细信息。	2024 年 7 月 29 日
AWS 已发布适用于 macOS 的客户端 (3.11.0)	请参阅发行说明了解详细信息。	2024 年 7 月 29 日
AWS 提供的适用于 Windows 的客户端 (3.12.1) 已发布	请参阅发行说明了解详细信息。	2024 年 7 月 18 日
AWS 为 Ubuntu 提供的客户端 (3.13.0) 已发布	请参阅发行说明了解详细信息。	2024 年 5 月 21 日
AWS 提供的适用于 Windows 的客户端 (3.12.0) 已发布	请参阅发行说明了解详细信息。	2024 年 5 月 21 日

AWS 已发布适用于 macOS 的客户端 (3.10.0)	请参阅发行说明了解详细信息。	2024 年 5 月 21 日
AWS 已发布适用于 macOS 的客户端 (3.9.2)	请参阅发行说明了解详细信息。	2024 年 4 月 11 日
AWS 为 Ubuntu 提供的客户端 (3.12.2) 已发布	请参阅发行说明了解详细信息。	2024 年 4 月 11 日
AWS 提供的适用于 Windows 的客户端 (3.11.2) 已发布	请参阅发行说明了解详细信息。	2024 年 4 月 11 日
AWS 已发布适用于 macOS 的客户端 (3.9.1)	请参阅发行说明了解详细信息。	2024 年 2 月 16 日
AWS 为 Ubuntu 提供的客户端 (3.12.1) 已发布	请参阅发行说明了解详细信息。	2024 年 2 月 16 日
AWS 提供的适用于 Windows 的客户端 (3.11.1) 已发布	请参阅发行说明了解详细信息。	2024 年 2 月 16 日
AWS 为 Ubuntu 提供的客户端 (3.12.0) 已发布	请参阅发行说明了解详细信息。	2023 年 12 月 19 日
AWS 已发布适用于 macOS 的客户端 (3.9.0)	请参阅发行说明了解详细信息。	2023 年 12 月 6 日
AWS 提供的适用于 Windows 的客户端 (3.11.0) 已发布	请参阅发行说明了解详细信息。	2023 年 12 月 6 日
AWS 为 Ubuntu 提供的客户端 (3.11.0) 已发布	请参阅发行说明了解详细信息。	2023 年 12 月 6 日
AWS 为 Ubuntu 提供的客户端 (3.10.0) 已发布	请参阅发行说明了解详细信息。	2023 年 12 月 6 日
AWS 为 Ubuntu 提供的客户端 (3.9.0) 已发布	请参阅发行说明了解详细信息。	2023 年 8 月 24 日

AWS 已发布适用于 macOS 的客户端 (3.8.0)	请参阅发行说明了解详细信息。	2023 年 8 月 24 日
AWS 提供的适用于 Windows 的客户端 (3.10.0) 已发布	请参阅发行说明了解详细信息。	2023 年 8 月 24 日
AWS 提供的适用于 Windows 的客户端 (3.9.0) 已发布	请参阅发行说明了解详细信息。	2023 年 8 月 3 日
AWS 为 Ubuntu 提供的客户端 (3.8.0) 已发布	请参阅发行说明了解详细信息。	2023 年 8 月 3 日
AWS 已发布适用于 macOS 的客户端 (3.7.0)	请参阅发行说明了解详细信息。	2023 年 8 月 3 日
AWS 提供的适用于 Windows 的客户端 (3.8.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 提供的适用于 Windows 的客户端 (3.7.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 为 Ubuntu 提供的客户端 (3.7.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 已发布适用于 macOS 的客户端 (3.6.0)	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 为 Ubuntu 提供的客户端 (3.6.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 已发布适用于 macOS 的客户端 (3.5.0)	请参阅发行说明了解详细信息。	2023 年 7 月 15 日
AWS 提供的适用于 Windows 的客户端 (3.6.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 14 日
AWS 为 Ubuntu 提供的客户端 (3.5.0) 已发布	请参阅发行说明了解详细信息。	2023 年 7 月 14 日

AWS 已发布适用于 macOS 的客户端 (3.4.0)	请参阅发行说明了解详细信息。	2023 年 7 月 14 日
AWS 已发布适用于 macOS 的客户端 (3.3.0)	请参阅发行说明了解详细信息。	2023 年 4 月 27 日
AWS 提供的适用于 Windows 的客户端 (3.5.0) 已发布	请参阅发行说明了解详细信息。	2023 年 4 月 3 日
AWS 提供的适用于 Windows 的客户端 (3.4.0) 已发布	请参阅发行说明了解详细信息。	2023 年 3 月 28 日
AWS 提供的适用于 Windows 的客户端 (3.3.0) 已发布	请参阅发行说明了解详细信息。	2023 年 3 月 17 日
AWS 为 Ubuntu 提供的客户端 (3.4.0) 已发布	请参阅发行说明了解详细信息。	2023 年 2 月 14 日
AWS 已发布适用于 macOS 的客户端 (3.2.0)	请参阅发行说明了解详细信息。	2023 年 1 月 23 日
AWS 提供的适用于 Windows 的客户端 (3.2.0) 已发布	请参阅发行说明了解详细信息。	2023 年 1 月 23 日
AWS 已发布适用于 macOS 的客户端 (3.1.0)	请参阅发行说明了解详细信息。	2022 年 5 月 23 日
AWS 提供的适用于 Windows 的客户端 (3.1.0) 已发布	请参阅发行说明了解详细信息。	2022 年 5 月 23 日
AWS 为 Ubuntu 提供的客户端 (3.1.0) 已发布	请参阅发行说明了解详细信息。	2022 年 5 月 23 日
AWS 已发布适用于 macOS 的客户端 (3.0.0)	请参阅发行说明了解详细信息。	2022 年 3 月 3 日
AWS 提供的适用于 Windows 的客户端 (3.0.0) 已发布	请参阅发行说明了解详细信息。	2022 年 3 月 3 日

AWS 为 Ubuntu 提供的客户端 (3.0.0) 已发布	请参阅发行说明了解详细信息。	2022 年 3 月 3 日
AWS 已发布适用于 macOS 的客户端 (2.0.0)	请参阅发行说明了解详细信息。	2022 年 1 月 20 日
AWS 提供的适用于 Windows 的客户端 (2.0.0) 已发布	请参阅发行说明了解详细信息。	2022 年 1 月 20 日
AWS 为 Ubuntu 提供的客户端 (2.0.0) 已发布	请参阅发行说明了解详细信息。	2022 年 1 月 20 日
AWS 已发布适用于 macOS 的客户端 (1.4.0)	请参阅发行说明了解详细信息。	2021 年 11 月 9 日
AWS 提供的 Windows 客户端 (1.3.7) 已发布	请参阅发行说明了解详细信息。	2021 年 11 月 8 日
AWS 为 Ubuntu 提供的客户端 (1.0.3) 已发布	请参阅发行说明了解详细信息。	2021 年 11 月 8 日
AWS 为 Ubuntu 提供的客户端 (1.0.2) 已发布	请参阅发行说明了解详细信息。	2021 年 9 月 28 日
AWS 已发布适用于 Windows (1.3.6) 和 macOS (1.3.5) 的客户端	请参阅发行说明了解详细信息。	2021 年 9 月 20 日
AWS 为 Ubuntu 18.04 LTS 和 Ubuntu 20.04 LTS 提供了客户端	你可以在 Ubuntu 18.04 L AWS TS 和 Ubuntu 20.04 LTS 上使用提供的客户端。	2021 年 6 月 11 日
支持使用 Windows 证书系统存储区中证书的 OpenVPN	您可以使用支持 Windows 证书系统存储区中证书的 OpenVPN。	2021 年 2 月 25 日
Self-service 传送门	您可以访问自助服务门户以获取最新 AWS 提供的客户端和配置文件。	2020 年 10 月 29 日

AWS 提供的客户	您可以使用 AWS 提供的客户端连接到 Client VPN 端点。	2020 年 2 月 4 日
初始版本	此版本引入了 AWS Client VPN。	2018 年 12 月 18 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。