用户指南

AWS 客户端 VPN

AWS 客户端 VPN: 用户指南

Table of Contents

什么是 AWS 客户VPN？

AWS Client VPN 是一项基于客户端的托管VPN服务，可让您安全地访问本地网络中的 AWS 资源和资源。

本指南提供了使用设备上的客户端应用程序与客户端VPN终端节点建立VPN连接的步骤。

客户机VPN组件

以下是使用 AWS 客户端的关键组件VPN。

- 客户端VPN终端节点-您的客户端VPN管理员在中创建和配置客户端VPN终端节点。 AWS您的管理员控制您在建立VPN连接时可以访问哪些网络和资源。
- VPN客户端应用程序-用于连接到客户端VPN端点并建立安全VPN连接的软件应用程序。
- 客户端VPN端点配置文件-由您的客户端VPN管理员提供给您的配置文件。该文件包含有关客户端VPN端点和建立VPN连接所需的证书的信息。您将此文件加载到您选择的VPN客户端应用程序中。

用于配置客户端的其他资源 VPN

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

开始使用 AWS Client VPN

在建立会VPN话之前，您的客户端VPN管理员必须创建和配置客户端VPN终端节点。您的管理员控制您在建立VPN会话时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客户端VPN终端节点并建立安全VPN连接。

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

主题

使用客户端的先决条件 VPN

要建立VPN连接，必须具备以下条件：

- 可以访问 Internet
- 受支持的设备
- 对于使用SAML基于联合身份验证（单点登录）的客户端VPN终端节点，请使用以下浏览器之一：
  - 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VPN基于开放的客户端应用程序连接到客户端VPN终端节点并建立VPN连接。

Windows、macOS、Ubuntu 18.04 和 Ubuntu 20.04 LTS 支持所 AWS 提供的客户端。LTS

您可以通过以下两种方法之一下载客户端VPN应用程序，具体取决于管理员是否为该应用程序创建了端点配置文件：

- 如果您的管理员未设置端点配置文件，请从 “客户端下载” 中下载并安装AWS 客户端VPN。下载并安装应用程序后，the section called “步骤 2：获取客户端VPN端点配置文件”继续从管理员那里获取端点配置文件。
- 如果您的管理员已经预先配置了端点配置文件，则可以从自助服务门户下载客户端VPN应用程序和配置文件。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 “下载客户端 VPN”。下载并安装应用程序和文件后，请转至the section called “第 3 步：Connect 连接到 VPN”。

或者，在要建立VPN连接的设备上下载并安装开放VPN客户端应用程序。

步骤 2：获取客户端VPN端点配置文件

您可以从管理员那里获得客户端VPN终端节点配置文件。配置文件包含有关客户端VPN端点的信息以及建立VPN连接所需的证书。

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

第 3 步：Connect 连接到 VPN

将客户端VPN端点配置文件导入所 AWS 提供的客户端或您的 Open VPN 客户端应用程序，然后连接到VPN。有关连接的步骤（包括导入端点配置文件），请参阅以下主题：VPN

- 使用 AWS 提供的客户端连接到 AWS Client VPN 终端节点
- 使用 Open VPN 客户端连接到 AWS Client VPN 端点

对于使用 Active Directory 身份验证的客户端VPN终端，系统将提示您输入用户名和密码。如果已为目录启用多重身份验证 (MFA)，系统还会提示您输入验证MFA码。

对于使用SAML基于联合身份验证（单点登录）的客户端VPN端点，所 AWS 提供的客户端会在您的计算机上打开浏览器窗口。在连接到客户端VPN终端节点之前，系统会提示您输入公司凭证。

AWS Client VPN 从自助服务门户下载

自助服务门户是一个网页，允许您下载所 AWS 提供客户端的最新版本和最新版本的客户端VPN端点配置文件。如果您的客户端VPN终端管理员已预先配置了客户端VPN客户端的配置文件，则可以从此门户下载并安装该客户端VPN应用程序以及配置文件。

> **Note**
>
> 如果您是管理员并且想要配置自助服务门户，请参阅《AWS Client VPN 管理员指南》中的客户端VPN终端节点。

在开始之前，您必须拥有客户端VPN终端节点的 ID。您的客户端VPN终端节点管理员可以向您提供 ID，也可以为您提供包含URL该 ID 的自助服务门户。

访问自助服务门户

1. 前往自助服务门户 https://self-service.clientvpn.amazonaws.com/，或使用管理员提供给您的自助服务门户。URL
2. 如果需要，请输入客户端VPN终端节点的 ID，例如`cvpn-endpoint-0123456abcd123456`。选择下一步。
3. 输入您的用户名和密码，然后选择登录。这与您用于连接到客户端VPN终端节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：
   - 下载客户端VPN终端节点的最新版本的客户端配置文件。
   - 为您的平台下载所 AWS 提供的客户端的最新版本。

使用 AWS 提供的客户端连接到 AWS Client VPN 终端节点

您可以使用 AWS 提供的客户端连接到客户端VPN终端节点。Windows、macOS、Ubuntu 18.04 和 Ubuntu 20.04 LTS 支持所 AWS 提供的客户端。LTS

客户端

- AWS Client VPN 适用于 Windows
- AWS Client VPN 适用于 macOS
- AWS Client VPN 适用于Linux

打开VPN指令

AWS 提供的客户端支持以下 Open VPN 指令。有关这些指令的更多信息，请参阅 Ope n VPN 网站上的文档。

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

- 键
- nobind
- persist-key
- persist-tun
- ping
- 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
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN 适用于 Windows

以下各节介绍如何使用 AWS 提供的适用于 Windows 的客户端建立VPN连接。您可以在客户端下载处下载并安装AWS 客户端VPN。 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 Windows 的客户端，需要满足以下条件：

- Windows 10 或 Windows 11（64 位操作系统，x64 处理器）
- 。 NET框架 4.7.2 或更高版本

客户端在您的计算机上保留TCP端口 8096。对于使用SAML基于联合身份验证（单点登录）的客户端VPN端点，客户端会保留TCP端口 35001。

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

主题

- AWS Client VPN 使用 AWS 提供的适用于 Windows 的客户端 Connect
- AWS Client VPN 适用于 Windows 的发行说明

AWS Client VPN 使用 AWS 提供的适用于 Windows 的客户端 Connect

在开始之前，请您务必阅读要求。在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 Windows 的客户端进行连接

1. 打开 AWS VPN 客户端应用程序。
2. 选择 File (文件)、Manage Profiles (管理配置文件)。
3. 选择 Add Profile (添加配置文件)。
4. 对于 Display name (显示名称)，输入配置文件的名称。
5. 在 “VPN配置文件” 中，浏览并选择从客户机VPN管理员那里收到的配置文件，然后选择 “添加配置文件”。
6. 在 AWS VPN Client 窗口中，确保选择了您的配置文件，然后选择 Connect（连接）。如果已将客户端VPN终端节点配置为使用基于凭据的身份验证，则系统将提示您输入用户名和密码。
7. 要查看连接的统计信息，请选择 Connection (连接)、Show Details (显示详细信息)。
8. 要断开连接，请在 AWS VPN Client (VPN 客户端) 窗口中选择 Disconnect (断开连接)。或者，选择 Windows 任务栏上的客户端图标，然后选择 Disconnect (断开连接)。

AWS Client VPN 适用于 Windows 的发行说明

下表包含适用于Windows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补丁。我们强烈建议您在每个平台上使用最新版本。以前的版本可能会受到可用性和/或安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	Date	下载链接和 SHA256
4.0.0	次要增强。	2024年9月25日	下载版本 4.0.0 sha256：6532f911385ec8fac1494d0847c847c8f90a999b3bd7380844e2ea4318e9e9db4db4a2ebc
3.14.2	添加了对 O `mssfix` pen VPN 标志的支持。	2024 年 9 月 4 日	下载版本 3.14.2 sha256：c171639d7e07e5fd48998cf76f76f74e6e6e49e5cbe3356c6264a67b4a9bf473bf473b5f5d
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：f743a7b4bc82daa4b803

版本	更改	Date	下载链接和 SHA256
			c29943905 29997bb57 a4b54d1f5195 ab28827283335
3.14.0	• 添加了对 O `tap-sleep` pen VPN 标志的支持。 • 更新了打开库VPN和打开SSL库。	2024 年 8 月 12 日	下载版本 3.14.0 sha256：81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96b0a96b9 6b96b96354516
3.13.0	更新了打开库VPN和打开SSL库。	2024 年 7 月 29 日	下载版本 3.13.0 sha256：c9 cc896e81a 744118409 51e349eed 9384507c5 3337fb703 c5ec64d52 2c29388b

版本	更改	Date	下载链接和 SHA256
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 sha256：5ed34aee6c03aa281e625acdbed272896c67046364a9a9e5846ca697e05e05dbfec08
3.12.0	• 局域网范围发生变化时自动重新连接。 • 移除了与SAML端点连接时的应用程序自动焦点。	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 sha256：8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bcd8fe42cb9ef8bc294e7e72f365c7cc

版本	更改	Date	下载链接和 SHA256
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
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: 9b6b7def99d76c59a97b067b6a73bdc6ee1c6b89a2063286f542e96b32df5ae9
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：d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f

版本	更改	Date	下载链接和 SHA256
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
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” 打开标志的支持。VPN • 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

版本	更改	Date	下载链接和 SHA256
3.0.0	• 增加了对 Windows 11 的支持。 • 修复了 TAP Windows 驱动程序命名会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
1.3.6	• 增加了对 Open VPN flags 的支持：connect-retry-max、dev-type、keepalive、ping、ping restart、p ull、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	• 增加了对 Open fla VPN g：dhcp 选项的支持。 • 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	Date	下载链接和 SHA256
1.3.3	• 增加了对打开VPN标志的支持：非活动、拉取过滤器、路线。 • 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
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。 • 添加了对 “路由-ipv6” 打开VPN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功能。	2021 年 3 月 8 日	不再受支持
1.2.7	• 增加了对 cryptoapicert Open 指令的支持。VPN • 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

版本	更改	Date	下载链接和 SHA256
1.2.5	• 在 “打开” VPN 配置中添加了对评论的支持。 • 为TLS握手错误添加了错误消息。	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SAML基于 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
1.1.0	• 增加了对打开VPN静态挑战回声功能的支持，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。您可以在客户端下载处下载并安装AWS 客户端VPN。 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 Monterey（12.0）、Ventura（13.0）或索诺玛（14.0）。
- 与 x86_64 处理器兼容。
- 客户端在您的计算机上保留TCP端口 8096。

- 对于使用SAML基于联合身份验证（单点登录）的客户端VPN端点，客户端会保留TCP端口 35001。

> **Note**
>
> 如果您使用的是搭载 Apple 硅处理器的 Mac，则需要安装 Rosetta 2 才能运行客户端软件。有关更多详细信息，请参阅 Apple 网站上的 “关于罗塞塔翻译环境”。

主题

- AWS Client VPN 使用 AWS 提供的适用于 macOS 的客户端 Connect
- AWS Client VPN 适用于 macOS 的发行说明

AWS Client VPN 使用 AWS 提供的适用于 macOS 的客户端 Connect

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

此外，请您务必阅读要求。在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 macOS 的客户端进行连接

1. 打开 AWS VPN 客户端应用程序。
2. 选择 File (文件)、Manage Profiles (管理配置文件)。
3. 选择 Add Profile (添加配置文件)。
4. 对于 Display name (显示名称)，输入配置文件的名称。
5. 对于VPN配置文件，浏览到您从客户机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. 在 AWS VPN Client (VPN 客户端) 窗口中，确保选择了您的配置文件，然后选择 Connect (连接)。如果已将客户端VPN终端节点配置为使用基于凭据的身份验证，则系统将提示您输入用户名和密码。
8. 要查看连接的统计信息，请选择 Connection (连接)、Show Details (显示详细信息)。
9. 要断开连接，请在 AWS VPN Client 窗口中选择 Disconnect（断开连接）。或者，在菜单栏上选择客户端图标，然后选择断开连接 < your-profile-name >。

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**
>
> 我们将继续为每个版本提供可用性和安全性补丁。我们强烈建议您在每个平台上使用最新版本。以前的版本可能会受到可用性和/或安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	日期	下载链接
4.0.0	次要增强。	2024年9月25日	下载版本 4.0.0 sha256：ad 574475a80 b614499c9 7ae75612e f1ff905bb 4aa1b5f71 09420e80b f95aef942 0e80bf95a ef95aefcbd
3.12.1	添加了对 O `mssfix` pen VPN 标志的支持。	2024 年 9 月 4 日	下载版本 3.12.1 sha256：a5 c31d3e0e8 bf8937682 805c9fff7 682805c9f ff76ca920 5875e009e 9e949ad1b 0532f449cee47

版本	更改	日期	下载链接
3.12.0	• 添加了对 O `tap-sleep` pen VPN 标志的支持。 • 更新了打开库VPN和打开SSL库。	2024 年 8 月 12 日	下载版本 3.12.0 sha256：37 de7736e19 da380b034 1f72271e2 f5aca8fae ae33ac18e cedafd366d9e4b13
3.11.0	• 更新了打开库VPN和打开SSL库。	2024 年 7 月 29 日	下载版本 3.11.0 sha256：44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f
3.10.0	• 局域网范围发生变化时自动重新连接。 • DNS修复了网络切换期间的恢复问题。 • 移除了与SAML端点连接时的应用程序自动焦点。	2024 年 5 月 21 日	下载版本 3.10.0 sha256：28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4add4404e 84404e84287dd

版本	更改	日期	下载链接
3.9.2	• 自版本 123 起，解决了基于 Chromium 的浏览器的SAML身份验证问题。 • 增加了对 macOS 索诺玛的支持。弃用对 macOS Big Sur 的支持。 • 改进了安保状况。	2024 年 4 月 11 日	下载版本 3.9.2 sha256：374467d991e8953b5032e5b985cda80a0ea27fb5d5f23cf16c556a1568b0d480
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	下载版本 3.9.1 sha256：9bba4b27a635e75038703e2cd4cd814aa75306179fac8e500e2c7af4e8e8e8e8e899e971
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	下载版本 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8

版本	更改	日期	下载链接
3.8.0	• 修复了在客户端网络中NAT64启用时的连接问题。 • 次要错误修复和增强功能。	2023 年 8 月 24 日	下载版本 3.8.0 sha256：d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• 改进了安保状况。	2023 年 8 月 3 日	下载版本 3.7.0 sha256：4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a
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

版本	更改	日期	下载链接
3.2.0	• 添加了对 “verify-x509-name” 打开标志的支持。VPN • 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。
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。如果设置与设置不匹配VPN，则将对其进行重新配置。 • 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 Open VPN flags 的支持：connect-retry-max、dev-type、keepalive、ping、ping restart、p ull、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。

版本	更改	日期	下载链接
1.3.4	• 增加了对 Open fla VPN g：dhcp 选项的支持。 • 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	• 增加了对打开VPN标志的支持：非活动、拉取过滤器、路线。 • 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。 • 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。 • 修复了移除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。 • 添加了对 “路由-ipv6” 开放VPN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。

版本	更改	日期	下载链接
1.3.0	添加了诸如错误报告、发送诊断日志和分析等支持功能。	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。
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	• 在 “打开” VPN 配置中添加了对评论的支持。 • 为TLS握手错误添加了错误消息。 • 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SAML基于 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DNS了无法解决的问题。 • 修复了因连接较长而导致的应用程序崩溃问题。 • 修复了一个MFA问题。	2020 年 4 月 2 日	不再受支持。
1.1.0	• 增加了对 macOS 配置DNS的支持。 • 增加了对打开VPN静态挑战回声功能的支持，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。

版本	更改	日期	下载链接
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 提供的适用于 Linux 的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 “发布说明”。

使用 AWS 提供的适用于 Linux VPN 的客户端连接到客户端的要求

要使用 AWS 提供的适用于 Linux 的客户端，需要满足以下条件：

- Ubuntu 18.04 LTS 或 Ubuntu 20.04（仅限）LTSAMD64

客户端在您的计算机上保留TCP端口 8096。对于使用SAML基于联合身份验证（单VPN点登录）的客户端终端，客户端会保留TCP端口 35001。

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

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 的
- 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：通过软件包存储库安装

1. 将AWSVPN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. 使用适用命令将存储库添加到您的 Ubuntu 操作系统，具体取决于您的 Ubuntu 版本：

   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 软件包文件进行安装

1. 从AWS 客户端下载或使用以下命令VPN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. 从AWS 客户端VPN下载中下载.deb 软件包文件。

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 的

在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 Linux 的客户端进行连接

1. 打开 AWS VPN 客户端应用程序。
2. 选择 File (文件)、Manage Profiles (管理配置文件)。
3. 选择 Add Profile (添加配置文件)。
4. 对于 Display name (显示名称)，输入配置文件的名称。
5. 对于VPN配置文件，浏览到您从客户机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. 在 AWS VPN Client 窗口中，确保选择了您的配置文件，然后选择 Connect（连接）。如果已将客户端VPN终端节点配置为使用基于凭据的身份验证，则系统将提示您输入用户名和密码。
8. 要查看连接的统计信息，请选择 Connection (连接)、Show Details (显示详细信息)。
9. 要断开连接，请在 AWS VPN Client 窗口中选择 Disconnect（断开连接）。

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补丁。我们强烈建议您在每个平台上使用最新版本。以前的版本可能会受到可用性和/或安全问题的影响。请参阅发行说明了解详细信息。

版本	更改	日期	下载链接
4.0.0	次要增强。	2024年9月25日	下载版本 4.0.0 sha256：c2632718742

版本	更改	日期	下载链接
			17d79783f ca182025a ce27ddbf8 f9661b56d f48843fa17922686
3.15.1	添加了对 O `mssfix` pen VPN 标志的支持。	2024 年 9 月 4 日	下载版本 3.15.1 sha256：ff b65c0bc93 e8d611cbc e2cbce2de b6b82f600 e6434e4d0 3c6b44c53 d61a2efcaadc2
3.15.0	• 添加了对 O `tap-sleep` pen VPN 标志的支持。 • 更新了打开库VPN和打开SSL库。	2024 年 8 月 12 日	下载版本 3.15.0 sha256：5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6dfd89a6d89d012

版本	更改	日期	下载链接
3.14.0	• 更新了打开库VPN和打开SSL库。	2024 年 7 月 29 日	下载版本 3.14.0 sha256：bd 2b401a1ed e6057d725 a13c77ef9 2147a79e0 c5e0020d3 79e44f319 b5334f60
3.13.0	• 局域网范围发生变化时自动重新连接。	2024 年 5 月 21 日	下载版本 3.13.0 sha256：e8 9f3bb7fc2 4c148e304 4b804b807 774fcfe05 e7eae9e55 1863a38a2 dcd7e0ac05f1
3.12.2	• 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 3.12.2 sha256：f7 178c33797 740bd596a 14cbe7b6f 5f58fb79d 17af79f88 bd8801353 a75a7571a 7d753a7571a7d

版本	更改	日期	下载链接
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
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 sha256：9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1
3.11.0	• 回滚 “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: 86c0fa1bf1c97194082835a739ec7f1c87e540194955f414a35c679b94538970

版本	更改	日期	下载链接
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
3.9.0	• 修复了在客户端网络中NAT64启用时的连接问题。 • 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 : 6cde9cfff82 754119e6a 68464d4bb 350da3cb3 e1ebf9140 dacf24e4f d2197454
3.8.0	• 改进了安保状况。	2023 年 8 月 3 日	下载版本 3.8.0 sha256 : 5f e479236cc 0a1940ba3 7fe168e55 1096f8dae 4c68d4556 0a164e41e dea3e5bd
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

版本	更改	日期	下载链接
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” 打开标志的支持。VPN	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
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 Open VPN flags 的支持：connect-retry-max、dev-type、keepalive、ping、ping restart、p ull、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。

版本	更改	日期	下载链接
1.0.1	• 启用了从 Ubuntu 应用程序栏退出的选项。 • 增加了对打开VPN标志的支持：非活动、拉取过滤器、路线。 • 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。

使用 Open VPN 客户端连接到 AWS Client VPN 端点

您可以使用常见的 Open VPN 客户端应用程序与客户端VPN端点建立连接。以下操作系统支持客户端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 Open AWS 客户端应用程序或 Open VPN GUI Connect 客户端建立客户端VPNGUI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。

- Android 和 iOS

  在 Android 或 iOS 设备上使用开放VPN客户端应用程序建立VPN连接。有关更多信息，请参阅安卓和 iOS 上的客户端VPN连接。

- macOS

  使用基于 macOS 的 Tunnelblick 或客户端的配置文件建立VPN连接。 AWS VPN有关更多信息，请参阅 在 macOS 上建立VPN连接。

- Linux

  使用 Ope n VPN-网络管理器界面或 Open VPN 应用程序在 Linux 上建立VPN连接。要使用 Open VPN-Network Manager 界面，您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。

> **Important**
>
> 如果已将客户端VPN终端节点配置为使用SAML基于开放的联合身份验证，则无法使用VPN基于开放的VPN客户端连接到客户端VPN终端节点。

客户端应用程序

- 使用 Windows 客户端应用程序连接到 AWS Client VPN 端点
- AWS Client VPN 安卓和 iOS 应用程序上的连接
- 使用 macOS 客户端应用程序连接到 AWS Client VPN 终端节点
- 使用 Open VPN 客户端应用程序连接到 AWS Client VPN 端点

使用 Windows 客户端应用程序连接到 AWS Client VPN 端点

以下各节介绍如何使用基于 Windows VPN 的客户端建立VPN连接。

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

有关故障排除信息，请参阅排除 AWS 客户端与基于 Windows 的客户端的VPN连接故障。

> **Important**
>
> 如果已将客户端VPN终端节点配置为使用SAML基于开放的联合身份验证，则无法使用VPN基于开放的VPN客户端连接到客户端VPN终端节点。

任务

- 在 Windows 上使用证书并建立 AWS 客户端VPN连接

在 Windows 上使用证书并建立 AWS 客户端VPN连接

您可以将 Open VPN 客户端配置为使用 Windows 证书系统存储区中的证书和私钥。当您将智能卡用作客户端VPN连接的一部分时，此选项非常有用。有关开放VPN客户端 cryptoapicert 选项的信息，请参阅 Open VPN 网站上的“打开参考手册”。VPN

> **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。有关更多信息，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 Technet 网站上的查看本地计算机证书存储区的权限。
4. 更新 Open VPN 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 Technet 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，使用 Open 通过执行以下任一操作VPN来建立VPN连接：

- 使用 Open VPN GUI 客户端应用程序
  1. 启动 Open VPN 客户端应用程序。
  2. 在 Windows 任务栏上，选择 “显示/隐藏图标”。右键单击 “打开” VPNGUI，然后选择 “导入文件”。
  3. 在 “打开” 对话框中，选择从客户机VPN管理员那里收到的配置文件，然后选择 “打开”。
  4. 在 Windows 任务栏上，选择 “显示/隐藏图标”。右键单击 “打开” VPNGUI，然后选择 “连接”。

- 使用 Open VPN GUI Connect 客户端
  1. 启动 “打开” VPN 应用程序，然后选择 “导入”、“从本地文件...” 。
  2. 导航到您从VPN管理员那里收到的配置文件，然后选择打开。

AWS Client VPN 安卓和 iOS 应用程序上的连接

> **Important**
>
> 如果已将客户端VPN终端节点配置为使用SAML基于开放的联合身份验证，则无法使用VPN基于开放的VPN客户端连接到客户端VPN终端节点。

以下信息显示了如何在 Android 或 iOS 移动设备上使用开放VPN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 Open VPN Connect 应用程序的更多信息，请参阅 Ope n VPN 网站上的 Open VPN Connect 用户指南。

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

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

使用 macOS 客户端应用程序连接到 AWS Client VPN 终端节点

这些部分介绍如何使用基于 macOS 的VPN客户端、Tunnelblick 或客户端建立VPN连接。 AWS VPN

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

有关故障排除信息，请参阅排除 AWS 客户端与 macOS 客户端的VPN连接故障。

> **Important**
>
> 如果已将客户端VPN终端节点配置为使用SAML基于开放的联合身份验证，则无法使用VPN基于开放的VPN客户端连接到客户端VPN终端节点。

主题

- 在 macOS 上建立 AWS Client VPN 连接

在 macOS 上建立 AWS Client VPN 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 Tun VPN nelblick 建立连接

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管理员那里收到的配置文件拖放到 “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)。

使用 AWS 客户端建立VPN连接VPN。

1. 启动 “打开” VPN 应用程序，然后选择 “导入”、“从本地文件...” 。
2. 导航到您从VPN管理员那里收到的配置文件，然后选择打开。

使用 Open VPN 客户端应用程序连接到 AWS Client VPN 端点

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

在开始之前，请确保您的客户端VPN管理员已创建客户端VPN终端节点并向您提供了客户端VPN终端节点配置文件。

有关故障排除信息，请参阅排除 AWS 客户端与基于 Linux 的客户端的VPN连接故障。

> **Important**
>
> 如果已将客户端VPN终端节点配置为使用SAML基于开放的联合身份验证，则无法使用VPN基于开放的VPN客户端连接到客户端VPN终端节点。

主题

- 在 Linux 上建立 AWS Client VPN 连接

在 Linux 上建立 AWS Client VPN 连接

使用 Ubuntu 计算机GUI上的网络管理器或 Open VPN 应用程序建立VPN连接。

使用 Open VPN-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. 选择旁边的加号 (+) VPN，然后选择从文件导入... 。
4. 导航到您从VPN管理员那里收到的配置文件，然后选择打开。
5. 在 VPN “添加” 窗口中，选择 “添加”。
6. 启用您添加的VPN配置文件旁边的切换开关，即可开始连接。

使用 Open 建立VPN连接 VPN

1. VPN使用以下命令安装 Open。

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

2. 通过加载从VPN管理员那里收到的配置文件来启动连接。

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

排除 AWS 客户端VPN连接故障

使用以下主题来解决在使用客户端应用程序连接到客户端VPN终端节点时可能遇到的问题。

主题

管理员的客户端VPN端点疑难解答

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

有关解决客户端VPN端点问题的更多信息，请参阅《AWS Client VPN 管理员指南》VPN中的客户端故障排除。

在 AWS 提供的客户端 AWS Support 中将诊断日志发送到

如果您在使用 AWS 提供的客户端时遇到问题，需要联系 AWS Support 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 Support。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 Support 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 Support 以便他们可以立即访问文件。

发送诊断日志

在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 Windows 的客户端发送诊断日志

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。

   联系时 AWS Support，您需要向他们提供参考号。

使用 AWS 提供的适用于 macOS 的客户端发送诊断日志

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。

   联系时 AWS Support，您需要向他们提供参考号。

使用 AWS 提供的 Ubuntu 客户端发送诊断日志

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。您可以选择将信息复制到剪贴板。

   联系时 AWS Support，您需要向他们提供参考号。

排除 AWS 客户端与基于 Windows 的客户端的VPN连接故障

以下各节包含有关您在使用基于 Windows 的客户端连接到客户端端VPN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_”。
- 打开VPN日志：包含有关打开VPN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 “没有 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
- PCs使用Windows 10或11的戴尔系统会发生客户机崩溃
- 打开 VPN GUI
- 打开VPN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客户端VPN端点。

原因

出现此问题的原因可能是以下原因之一：

- 另一个 Open VPN 进程已在您的计算机上运行，这会阻止客户端连接。
- 您的配置 (.ovpn) 文件无效。

解决方案

检查您的计算机上是否有其他 Open VPN 应用程序在运行。如果有，请停止或退出这些进程，然后尝试再次连接到客户端VPN终端节点。查看 Open VPN 日志中是否有错误，并请您的客户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。
- 那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端点。

客户端无法连接 “没有 TAP Windows 适配器” 日志消息

问题

AWS 提供的客户端无法连接到客户端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。你应该能够通过转到 “开始”-> “所有程序” TAP-> “-Windows”-> “实用程序” TAP-> “添加新的-Windows 虚拟以太网适配器” 来创建 TAP-Windows 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。
- 创建一个新的 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客户端VPN终端节点，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主机名无法解析为 IP 地址。
- Open VPN 进程正在无限期地尝试连接到端点。

解决方案

验证您的计算机已连接到 Internet。请您的客户端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。您也可以通过在 “ AWS VPN客户端” 窗口中选择 “断开连接” 来断开VPN会话连接，然后再次尝试连接。

VPN连接进程意外退出

问题

连接到客户端VPN端点时，客户端意外退出。

原因

TAP-您的计算机上未安装 Windows。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

。 NET您的计算机上未安装 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

如果客户端VPN端点使用相互身份验证，则配置 (.ovpn) 文件不包含客户端证书和密钥。

解决方案

确保您的客户VPN管理员将客户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断开连接时会弹出一条消息，上面写着：“由于您的设备所VPN连接的本地网络的地址空间已更改，连接正在终止。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
```

PCs使用Windows 10或11的戴尔系统会发生客户机崩溃

问题

在某些运行Windows 10或11的戴尔PCs（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，可能会发生崩溃。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Dell Backup和Recovery系统可能会导致与 AWS 提供的客户机发生冲突，尤其是与以下三个客户机发生冲突DLLs：

- DBRShellExtension.ll
- DBROverlayIconBackuped.ll
- DBROverlayIconNotBackuped.ll

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 客户端VPN下载，如果有更新的版本可用，请升级到最新版本。

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，也可以删除或重命名这些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，或对其进行重命名。这两种操作都将避免加载它们。

   - DBRShellExtension.ll
   - DBROverlayIconBackuped.ll
   - DBROverlayIconNotBackuped.ll

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

打开 VPN GUI

以下故障排除信息已在 Windows 10 Home（64 位）和 Windows Server 2016（64 位）的 Open VPN GUI 软件版本 11.10.0.0 和 11.11.0.0 上进行了测试。

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
```

打开VPN连接客户端

以下故障排除信息已在 Windows 10 Home（64 位）和 Windows Server 2016（64 位）上的 Open VPN Connect Client 软件版本 2.6.0.100 和 2.7.1.101 上进行了测试。

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

无法解析该DNS名称。为了防止DNS缓存，客户端必须在DNS名称前面添加一个随机字符串；但是，有些客户端不这样做。

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端点DNS名称” 的解决方案。

缺少PKI别名

问题

与不使用相互身份验证的客户端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

Open VPN Connect Client 软件存在一个已知问题，即它尝试使用相互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

在客户机VPN配置文件中随机指定客户端密钥和证书，然后将新配置导入 Open VPN Connect Client 软件中。或者，使用其他客户端，例如开放客户VPNGUI端 (v11.12.0.0) 或粘度客户端 (v.1.7.14)。

排除 AWS 客户端与 macOS 客户端的VPN连接故障

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_”。
- 打开VPN日志：包含有关打开VPN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。

```
/tmp/AcvcHelperErrLog.txt
/tmp/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
- 需要帮助工具错误
- 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
- 打开 VPN
- 无法解决 DNS

客户端无法连接

问题

AWS 提供的客户端无法连接到客户端VPN端点。

原因

出现此问题的原因可能是以下原因之一：

- 另一个 Open VPN 进程已在您的计算机上运行，这会阻止客户端连接。
- 您的配置 (.ovpn) 文件无效。

解决方案

检查您的计算机上是否有其他 Open VPN 应用程序在运行。如果有，请停止或退出这些进程，然后尝试再次连接到客户端VPN终端节点。查看 Open VPN 日志中是否有错误，并请您的客户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。
- 那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端点。

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客户端VPN终端节点，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主机名无法解析为 IP 地址。
- Open VPN 进程正在无限期地尝试连接到端点。

解决方案

验证您的计算机已连接到 Internet。请您的客户端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。您也可以通过在 “ AWS VPN客户端” 窗口中选择 “断开连接” 来断开VPN会话连接，然后再次尝试连接。

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

如果客户端VPN端点使用相互身份验证，则配置 (.ovpn) 文件不包含客户端证书和密钥。

解决方案

确保您的客户VPN管理员将客户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。

需要帮助工具错误

问题

尝试连接时出现以下错误VPN。

```
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。AWSVPN客户端-需要帮助工具错误

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
```

要增加日志的详细程度，请打开 Tunnelblick 应用程序，选择设置，然后调整日志级别的值。VPN

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

该应用程序使用的开放VPN版本不支持密码算法 AES -256-。GCM

解决方案

通过执行以下操作选择兼容的 Open VPN 版本：

1. 打开 Tunnelblick 应用程序。
2. 选择设置。
3. 对于开放VPN版本，请选择 2.4.6-开放SSL版本为 v 1.0.2q。

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

向您的客户机VPN管理员申请新的配置文件。

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，由于客户端证书为服务器身份验证启用了扩展密钥用法 (EKU) 字段，因此客户端身份验证失败。

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，请向您的客户VPN管理员进行验证。如果您使用服务器证书而不是客户端证书连接到客户端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

向您的客户VPN管理员申请新的客户证书。

打开 VPN

以下故障排除信息已在 macOS High Sierra 10.13.6 上的 Open Conn VPN ect Client 软件版本 2.7.1.100 上进行了测试。

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
```

无法解决 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

Open VPN Connect 无法解析客户机VPNDNS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端点DNS名称” 的解决方案。

排除 AWS 客户端与基于 Linux 的客户端的VPN连接故障

以下部分包含有关使用基于 Linux 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。

主题

- AWS 提供的客户端事件日志
- DNS查询转到默认域名服务器
- 打开VPN（命令行）
- VPN通过网络管理器打开 (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导致连接失败的向DNS上/向下脚本中的错误：

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

DNS查询转到默认域名服务器

问题

在某些情况下，建立VPN连接后，DNS查询仍将转到默认的系统域名服务器，而不是为客户端终端节点配置的域名服务器。VPN

原因

客户端与 systemd- resolved（一种在 Linux 系统上可用的服务）进行交互，后者是管理的中心部分。DNS它用于配置从客户端VPN端点推送的DNS服务器。之所以出现问题，是因为 systemd-resolved 没有为客户端端VPN点提供的DNS服务器设置最高优先级。相反，它会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，因此可以用来解析DNS查询。

解决方案

1. 在 Open VPN 配置文件的第一行添加以下指令，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）如果您不希望 systemd 解析为代理DNS查询，而是希望将查询直接发送到真实DNS域名服务器，请改为使用符号链接到。`/etc/resolv.conf` `/run/systemd/resolve/resolv.conf`

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

您可能需要执行此步骤以绕过系统解析的配置，例如用于DNS答案缓存、每接口DNS配置、DNSSec强制执行等。当您需要在连接时用私有记录覆盖公共DNS记录时，此选项特别有用VPN。例如，你的私有解析器可能有一个私有DNS解析器，里面有一个 www.example.com 的记录，该记录可以解析为私VPC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。

打开VPN（命令行）

问题

由于DNS分辨率不起作用，连接无法正常运行。

原因

DNS服务器未在客户端VPN端点上配置，或者客户端软件不支持该服务器。

解决方案

使用以下步骤检查DNS服务器是否已配置且运行正常。

1. 确保日志中存在DNS服务器条目。在以下示例中，DNS服务器192.168.0.2（在客户端VPN端点中配置）在最后一行返回。

```
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，请要求您的客户端VPN管理员修改客户端VPN终端节点，并确保已为客户端VPN终端节点指定DNSVPCDNS服务器（例如服务器）。有关更多信息，请参阅《AWS Client VPN 管理员指南》中的客户端VPN终端节点。
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客户端VPN配置文件（.ovpn 文件），然后添加以下几行。

```
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
```

VPN通过网络管理器打开 (GUI)

问题

使用 Network Manager Open VPN 客户端时，连接失败并出现以下错误。

```
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端点DNS名称” 的解决方案。

解决常见的 AWS 客户机VPN问题

以下是您在使用客户端连接到客户端VPN终端节点时可能遇到的常见问题。

TLS密钥协商失败

问题

TLS协商失败并出现以下错误。

```
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：

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

解决方案

检查计算机上的防火墙规则是否阻止了端口 443 或 1194 上的入站TCP或出站UDP流量。请您的客户VPN管理员验证以下信息：

- 客户端VPN端点的防火墙规则不会阻止端口 443 TCP 或 1194 上的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。
- 那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端点。

文档历史记录

下表介绍了《 AWS 客户端VPN用户指南》的更新。

变更	说明	日期
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 提供了客户端 LTS	你可以在 Ubuntu 18.04 和 Ubuntu 20.04 LTS 上使用 AWS提供的客户端。LTS	2021 年 6 月 11 日
VPN使用 Windows 证书系统存储区中的证书支持 Open	你可以使用 Op VPN en 和 Windows 证书系统商店中的证书。	2021 年 2 月 25 日
自助服务门户	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客户端VPN终端节点。	2020 年 2 月 4 日
初始版本	此版本引入了 AWS 客户端 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。