aws

用户指南

AWS Client VPN

AWS Client VPN: 用户指南

Table of Contents

AWS 客户端 VPN 是什么？

AWS 客户端 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，建立与客户端 VPN 终端节点的 VPN 连接。

组件

以下是使用 AWS 客户端 VPN 的关键组件。

- 客户端 VPN 终端节点 – 您的客户端 VPN 管理员在 AWS 中创建并配置客户端 VPN 终端节点。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 – 用于连接到客户端 VPN 终端节点并建立安全 VPN 连接的软件应用程序。
- 客户端 VPN 终端节点配置文件 – 客户端 VPN 管理员向您提供的配置文件。文件包括有关客户端 VPN 终端节点以及建立 VPN 连接所需的证书的信息。您将此文件加载到选择的 VPN 客户端应用程序中。

其他资源

如果您是客户端 VPN 管理员，请参阅 AWS Client VPN 管理员指南，以了解有关创建并配置客户端 VPN 终端节点的更多信息。

客户端 VPN 入门

在可以建立 VPN 会话之前，您的客户端 VPN 管理员必须创建并配置一个客户端 VPN 终端节点。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客户端 VPN 终端节点并建立安全的 VPN 连接。

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

主题

Prerequisites

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
- 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）的客户端 VPN 终端节点）：
  - 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客户端 VPN 终端节点并建立 VPN 连接。

AWS 提供的客户端适用于 Windows、macOS、Ubuntu 18.04 LTS 和 Ubuntu 20.04 LTS。您可以通过 AWS 客户端 VPN 下载来下载客户端。

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：获取客户端 VPN 终端节点配置文件

您必须从您的管理员处获取客户端 VPN 终端节点配置文件。配置文件包括有关客户端 VPN 终端节点以及建立 VPN 连接所需的证书的信息。

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，则您可以自行下载 AWS 提供的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，请参阅使用自助服务门户。

步骤 2：连接到 VPN

将客户端 VPN 终端节点配置文件导入到 AWS 提供的客户端或您的 OpenVPN 客户端应用程序中，然后连接到 VPN。有关连接到 VPN 的步骤，请参阅以下主题：

- 使用 AWS 提供的客户端进行连接
- 使用 OpenVPN 客户端进行连接

对于使用 Active Directory 身份验证的客户端 VPN 终端节点，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）的客户端 VPN 终端节点，AWS 提供的客户端将在计算机上打开一个浏览器窗口。系统将提示您输入公司凭证，然后才能连接到客户端 VPN 终端节点。

使用自助服务门户

您的客户端 VPN 终端节点管理员可以为客户端 VPN 终端节点配置自助服务门户。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客户端 VPN 终端节点配置文件的最新版本。有关配置自助服务门户的更多信息，请参阅 AWS Client VPN 管理员指南中的客户端 VPN 终端节点。

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 或包含 ID 的自助服务门户 URL。

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，请输入客户端 VPN 终端节点的 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 终端节点的客户端配置文件的最新版本。
   - 下载 AWS 提供的适用于您的平台的客户端的最新版本。

使用 AWS 提供的客户端进行连接

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

客户

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

OpenVPN 指令

AWS 提供的客户端支持以下 OpenVPN 指令：

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- 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

以下过程说明如何使用 AWS 提供的适用于 Windows 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。

内容

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

客户端保留您计算机上的 TCP 端口 8096。对于使用基于 SAML 的联合身份验证（单点登录）的客户端 VPN 终端节点，客户端保留 TCP 端口 35001。

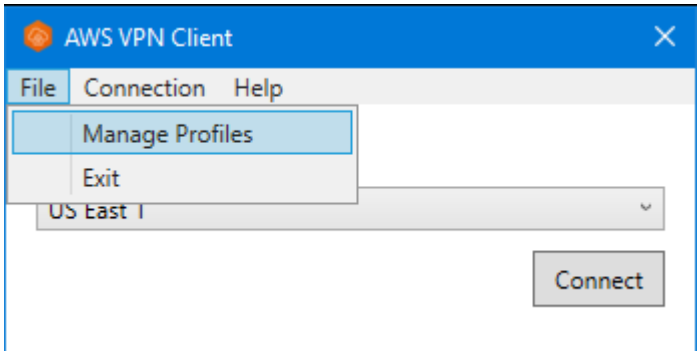
在开始之前，请确保您的客户端 VPN 管理员已经创建了客户端 VPN 终端节点，并为您提供了客户端 VPN 终端节点配置文件。

连接

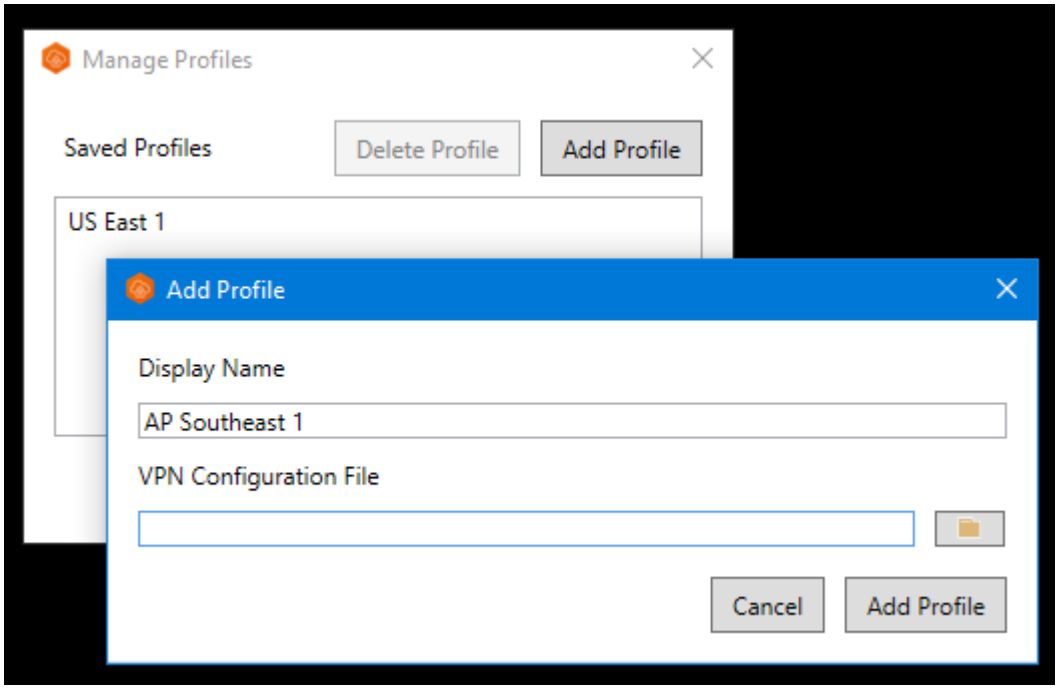
在开始之前，请您务必阅读要求。在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 Windows 的客户端进行连接

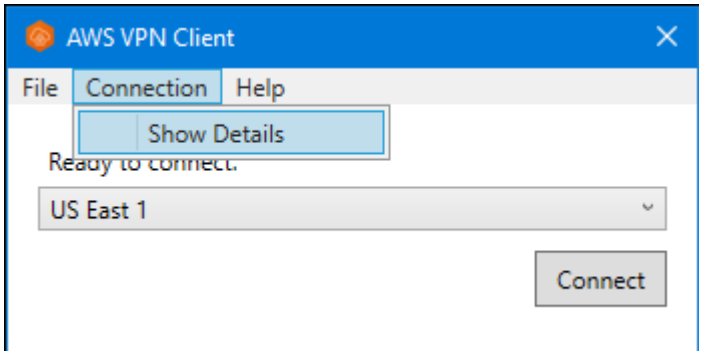
1. 打开 AWS VPN 客户端应用程序。
2. 选择 File (文件)、Manage Profiles (管理配置文件)。



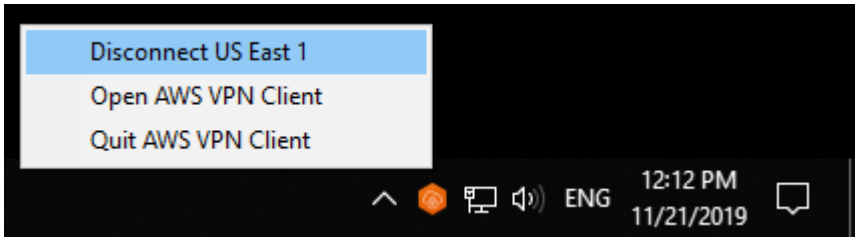
3. 选择 Add Profile (添加配置文件)。



4. 对于 Display name (显示名称)，输入配置文件的名称。
5. 对于 VPN 配置文件，浏览到并选择您从客户端 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 (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证的身份验证，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)。



发布说明

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。

版本	更改	Date	下载链接和 SHA256
3.11.1	• 改进了安保状况。	2024年2月16日	下载版本 3.11.1 sha256：fb 67b60aa83 70197958a 11ea6f57d 5bc051227 9560b52a8 57ae34cb3 21eaefd0
3.11.0	• 修复了由 Windows 虚拟机导致的连接问题。 • 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启用 NAT64 时的连接问题。	2023 年 8 月 24 日	下载版本 3.10.0 sha256：d4 6721aad40

版本	更改	Date	下载链接和 SHA256
	• 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。		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
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

版本	更改	Date	下载链接和 SHA256
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
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

版本	更改	Date	下载链接和 SHA256
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。	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。 • 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功能。	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

版本	更改	Date	下载链接和 SHA256
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
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

以下过程说明如何使用 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。

内容

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 Big Sur（11.0）、Monterey（12.0）或 Ventura（13.0）。
- 与 x86_64 处理器兼容。
- 客户端保留您计算机上的 TCP 端口 8096。
- 对于使用基于 SAML 的联合身份验证（单点登录）的客户端 VPN 终端节点，客户端保留 TCP 端口 35001。

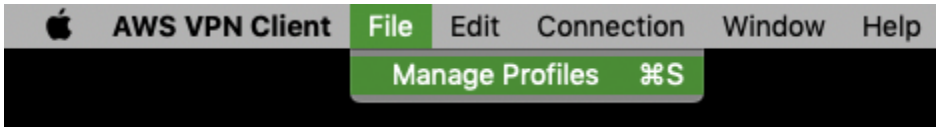
连接

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。

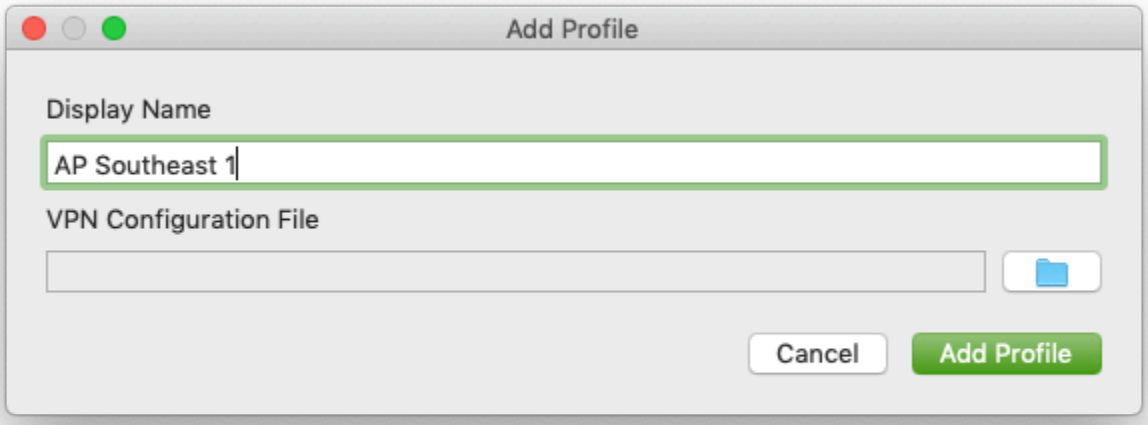
此外，请您务必阅读要求。在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

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)。

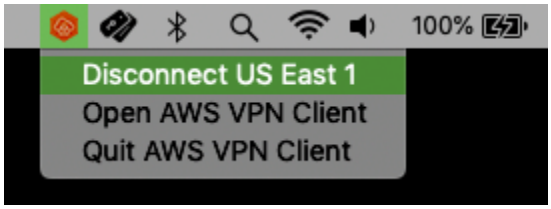


3. 选择 Add Profile (添加配置文件)。
4. 对于 Display name (显示名称)，输入配置文件的名称。



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. 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证的身份验证，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 >。



发布说明

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。

版本	更改	日期	下载链接
3.9.1	• 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 sha256：9bba4b27a635e7503870 3e2cd4cd8 14aa75306 179fac8e5 00e2c7af4 e8e8e8e8e 899e971
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: f0f6a5579fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8
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	下载版本 3.8.0 sha256：d5a229b12ef a2e886271 27a6dc27f 5c6a1bc9c 426a8c466 131ecbdbd 6bbb4461
3.7.0	• 改进了安保状况。	2023 年 8 月 3 日	下载版本 3.7.0

版本	更改	日期	下载链接
			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
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 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。
1.3.4	• 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。

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

以下过程说明如何安装 AWS 所提供的 Linux 客户端，以及如何使用 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。

内容

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 LTS（仅限 AMD64）

客户端保留您计算机上的 TCP 端口 8096。对于使用基于 SAML 的联合身份验证（单点登录）的客户端 VPN 终端节点，客户端保留 TCP 端口 35001。

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。

安装

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 Amazon VPN Client 公有密钥添加到您的 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 程序包文件安装

1. 通过 AWS 客户端 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

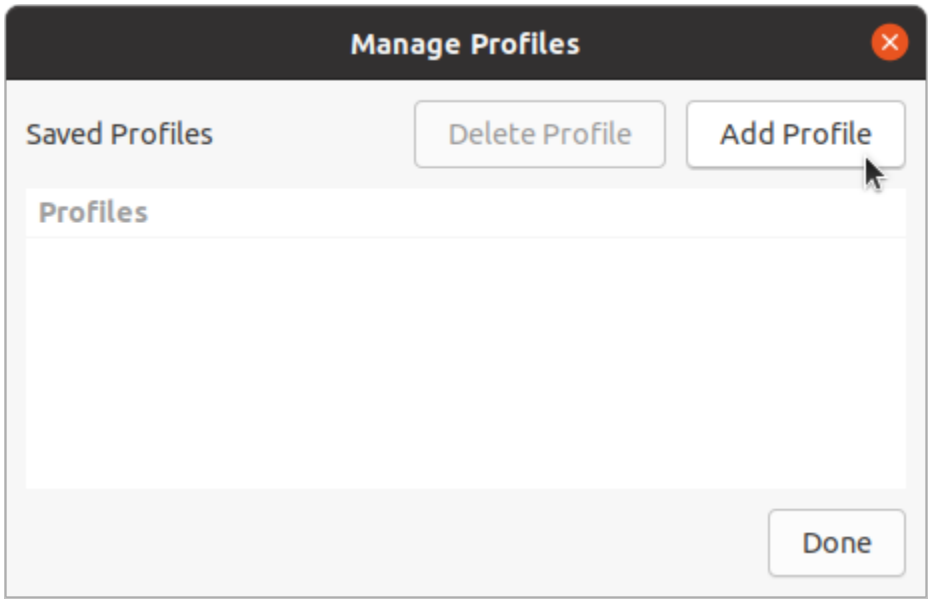
1. 通过 AWS 客户端 VPN 下载下载 .deb 程序包文件。
2. 下载 .deb 程序包文件后，通过 Ubuntu 软件中心安装程序包。按照 Ubuntu Wiki 上所述的步骤，通过 Ubuntu 软件中心安装独立的 .deb 程序包。

连接

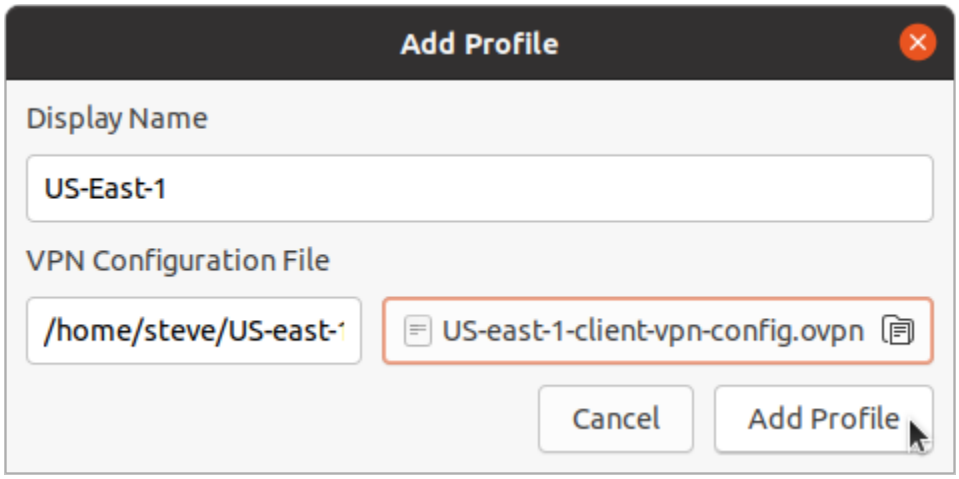
在以下步骤中，所 AWS 提供的AWS VPN 客户也被称为客户。

使用 AWS 提供的适用于 Linux 的客户端进行连接

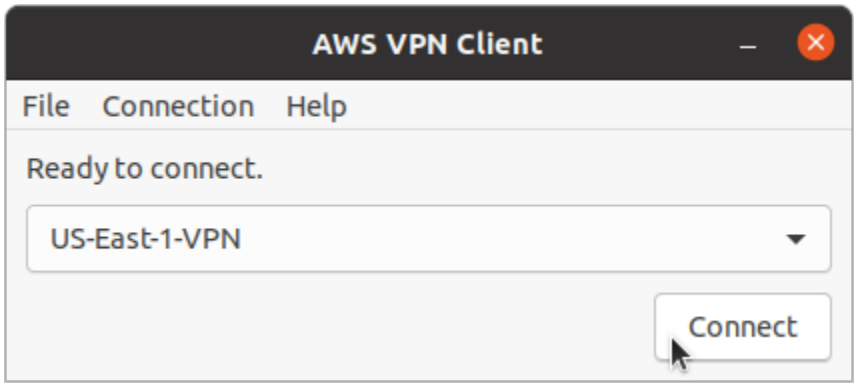
1. 打开 AWS VPN 客户端应用程序。
2. 选择 File (文件)、Manage Profiles (管理配置文件)。
3. 选择 Add Profile (添加配置文件)。



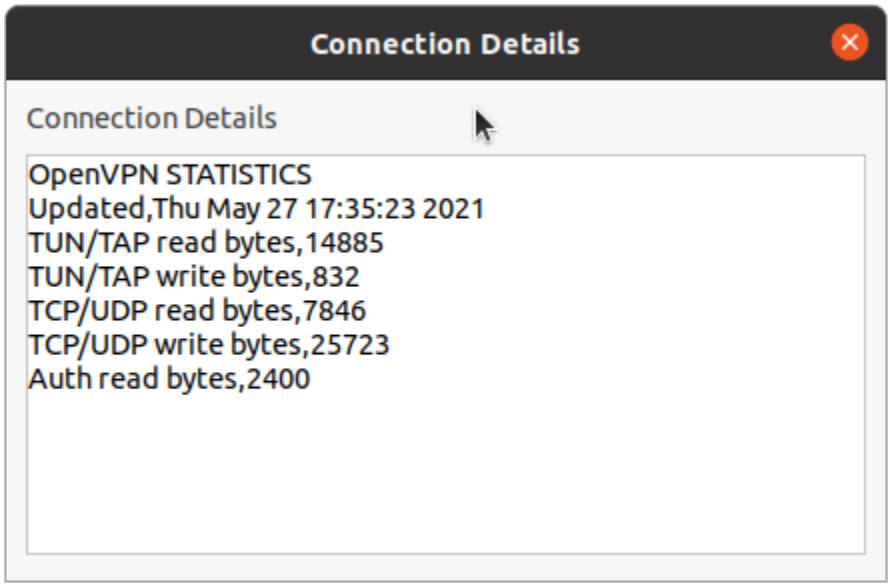
4. 对于 Display name (显示名称)，输入配置文件的名称。
5. 对于 VPN 配置文件，浏览到您从客户端 VPN 管理员那里收到的配置文件。选择 Open。
6. 选择 Add Profile (添加配置文件)。



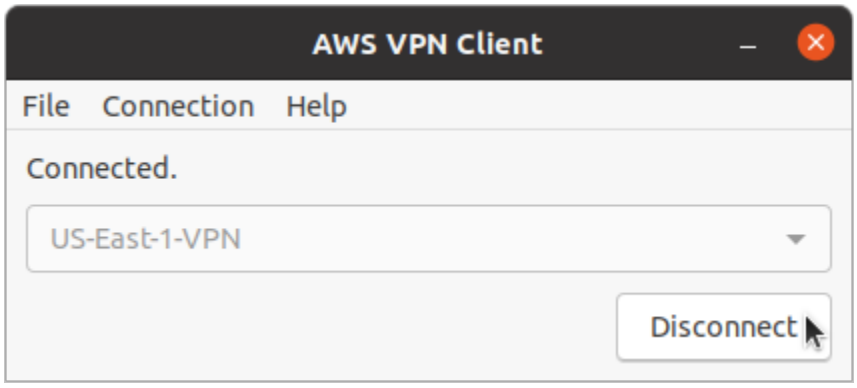
7. 在 AWS VPN Client 窗口中，确保选择了您的配置文件，然后选择 Connect（连接）。如果已将客户端 VPN 终端节点配置为使用基于凭证的身份验证，系统将提示您输入用户名和密码。



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）。



发布说明

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。

版本	更改	日期	下载链接
3.12.1	• 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	• 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: 86c0fa1bf1c9719408 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

版本	更改	日期	下载链接
			d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
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 sha256：6cde9cfff82 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
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

版本	更改	日期	下载链接
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 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 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。

使用 OpenVPN 客户端进行连接

您可以使用常见的 OpenVPN 客户端应用程序连接到客户端 VPN 终端节点。

> **Note**
>
> 对于基于 SAML 的联合身份验证，您必须使用 AWS 提供的客户端连接到 Client VPN 终端节点。有关更多信息，请请阅使用 AWS 提供的客户端进行连接或联系您的 VPN 管理员。

客户端应用程序

- 使用 Windows 客户端应用程序进行连接
- 使用 Android 或 iOS VPN 客户端应用程序进行连接
- 使用 macOS 客户端应用程序进行连接
- 使用 OpenVPN 客户端应用程序进行连接

使用 Windows 客户端应用程序进行连接

以下过程说明如何使用基于 Windows 的 VPN 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。

有关故障排除信息，请参阅Windows 故障排查。

使用 Windows 证书系统存储区中证书的 OpenVPN

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客户端 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。

将 cryptoapicert 选项与 OpenVPN 一起使用

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 Technet 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 Technet 网站上的如何检索证书的指纹。

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

完成配置后，您可以使用 OpenVPN 来建立连接。

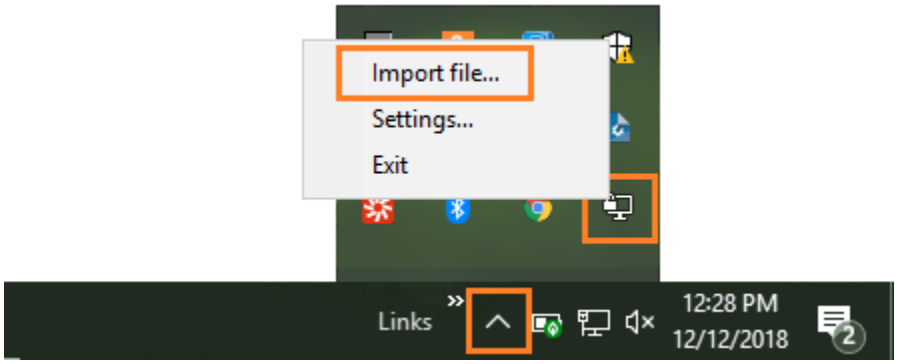
OpenVPN GUI

以下过程说明如何在 Windows 计算机上使用 OpenVPN GUI 客户端应用程序建立 VPN 连接。

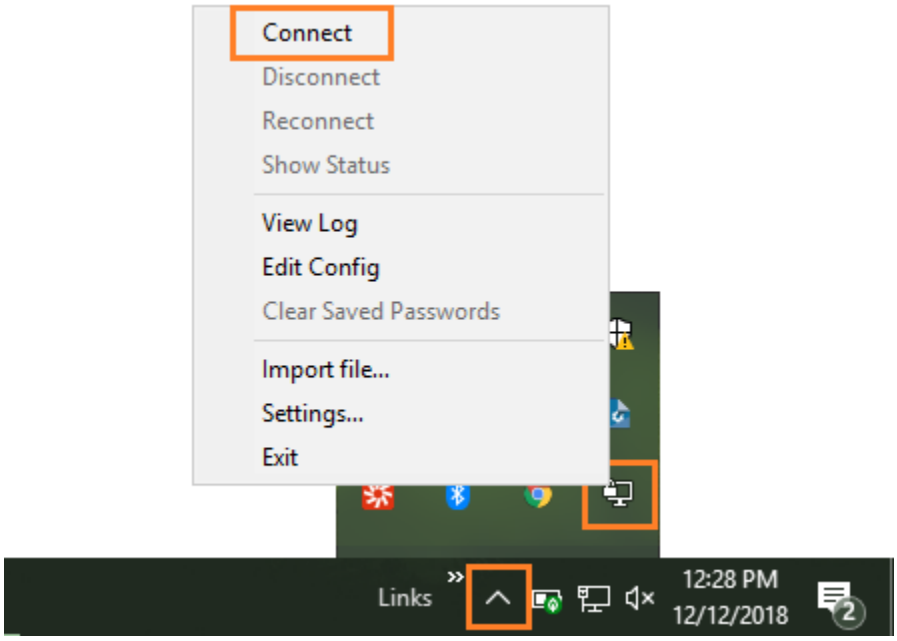
> **Note**
>
> 有关 OpenVPN 客户端应用程序的信息，请参阅 OpenVPN 网站上的社区下载。

建立 VPN 连接

1. 启动 OpenVPN 客户端应用程序。
2. 在 Windows 任务栏上，选择 Show/Hide icons (显示/隐藏图标)，右键单击 OpenVPN GUI，然后选择 Import file (导入文件)。



3. 在“打开”对话框中，选择从您的客户端 VPN 管理员处收到的配置文件，然后选择打开。
4. 在 Windows 任务栏中，单击 Show/Hide icons (显示/隐藏图标)，右键单击 OpenVPN GUI，然后选择 Connect (连接)。



OpenVPN Connect 客户端

以下过程说明如何在 Windows 计算机上使用 OpenVPN Connect 客户端应用程序建立 VPN 连接。

> **Note**
>
> 有关更多信息，请参阅 OpenVPN 网站上的使用 Windows 连接到访问服务器。

建立 VPN 连接

1. 启动 OpenVPN Connect 客户端应用程序。
2. 在 Windows 任务栏上，选择 Show/Hide icons (显示/隐藏图标)，右键单击 OpenVPN，然后选择 Import file (导入文件)。
3. 选择从文件导入，然后选择从客户端 VPN 管理员处收到的配置文件。
4. 要开始连接，请选择连接配置文件。

使用 Android 或 iOS VPN 客户端应用程序进行连接

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**
>
> 有关用于 Android 的 OpenVPN 客户端应用程序的更多信息，请参阅 OpenVPN 网站上的有关 OpenVPN Connect Android 的常见问题。

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。

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

使用 macOS 客户端应用程序进行连接

以下过程说明如何使用基于 macOS 的 VPN 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。

有关故障排除信息，请参阅macOS 故障排查。

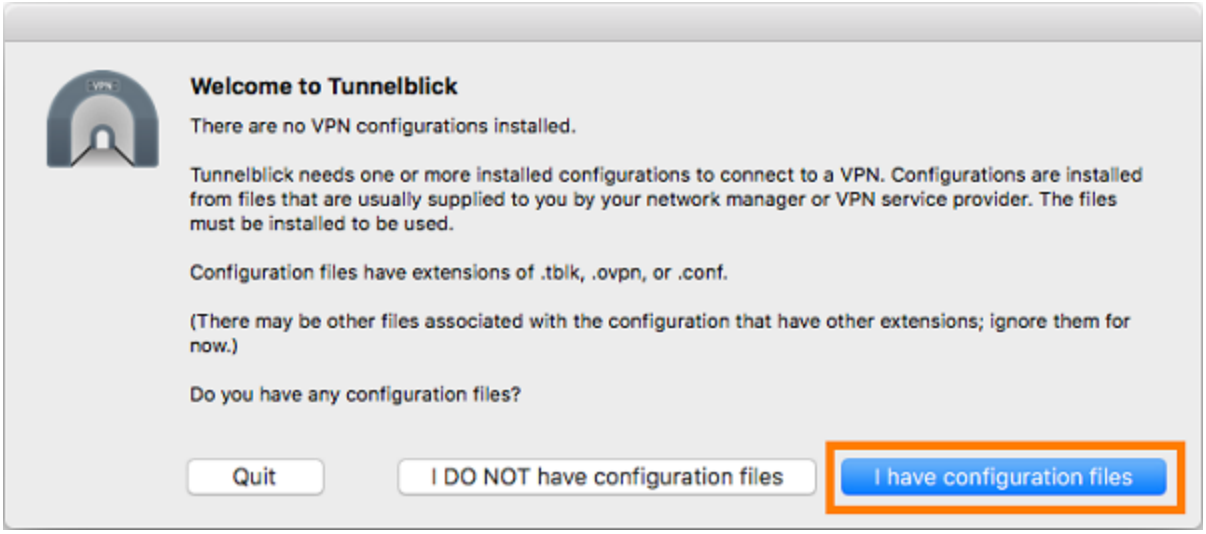
Tunnelblick

以下过程说明如何在 macOS 计算机上使用 Tunnelblick 客户端应用程序建立 VPN 连接。

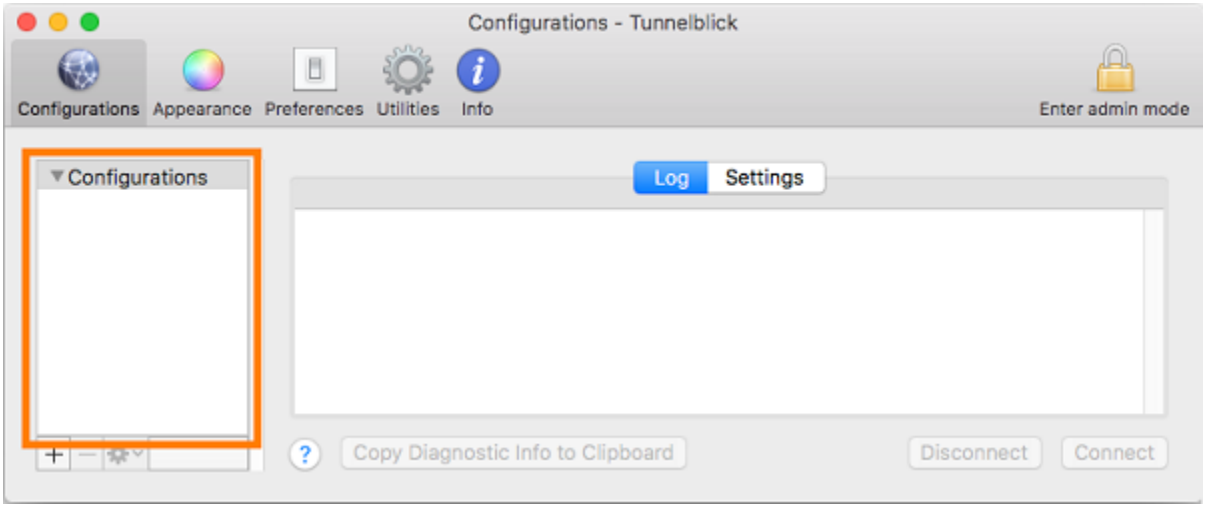
> **Note**
>
> 有关用于 macOS 的 Tunnelblick 客户端应用程序的更多信息，请参阅 Tunnelblick 网站上的 Tunnelblick 文档。

建立 VPN 连接

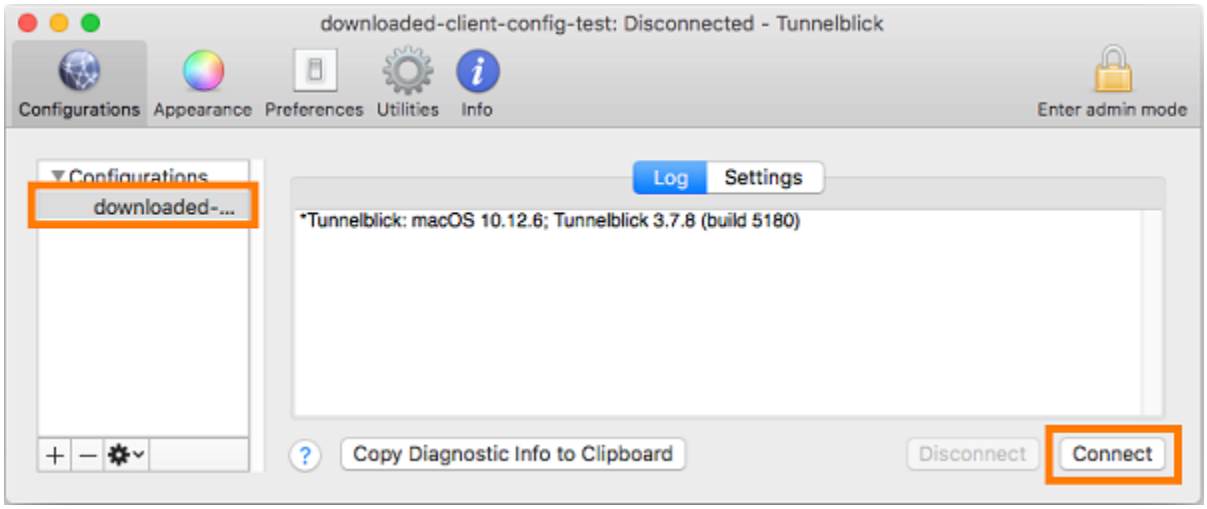
1. 启动 Tunnelblick 客户端应用程序，然后选择 I have configuration files (我拥有配置文件)。



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)。



OpenVPN Connect 客户端

以下过程说明如何在 macOS 计算机上使用 OpenVPN Connect 客户端应用程序建立 VPN 连接。

> **Note**
>
> 有关更多信息，请参阅 OpenVPN 网站上的使用 macOS 连接到访问服务器。

建立 VPN 连接

1. 启动 OpenVPN 应用程序，然后依次选择 Import (导入) 和 From local file... (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)。

使用 OpenVPN 客户端应用程序进行连接

以下过程说明如何使用基于 OpenVPN 的 VPN 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。

有关故障排除信息，请参阅Linux 故障排查。

> **Important**
>
> 如果客户端 VPN 终端节点已配置为使用基于 SAML 的联合身份验证，则无法使用基于 OpenVPN 的 VPN 客户端连接到客户端 VPN 终端节点。

OpenVPN - 网络管理器

以下过程说明如何在 Ubuntu 计算机上通过网络管理器 GUI 使用 OpenVPN 应用程序来建立 VPN 连接。

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 Import from file... (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。

OpenVPN

以下过程说明如何在 Ubuntu 计算机上使用 OpenVPN 客户端应用程序建立 VPN 连接。

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
```

客户端 VPN 连接故障排查

使用以下主题对您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进行故障排查。

主题

管理员的客户端 VPN 终端节点故障排查

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。

有关对客户端 VPN 终端节点问题进行故障排查的其他信息，请参阅 AWS Client VPN 管理员指南中的客户端 VPN 故障排查。

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，则该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。

   当您联系时 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。

   当您联系时 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。如果您愿意，您可以选择将信息复制到剪贴板。

   当您联系时 AWS Support，您需要向他们提供参考号。

Windows 故障排查

以下部分包含您在使用基于 Windows 的客户端连接到客户端 VPN 终端节点时可能遇到的问题相关信息。

主题

- OpenVPN 连接客户端

AWS 提供的客户

AWS 提供的客户

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
```

主题

- 客户端无法连接
- 客户端无法连接，显示“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
- 使用 Windows 10 或 11 的 Dell PC 上出现客户端崩溃问题
- VPN 断开连接并显示弹出消息

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，显示“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 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。您应该能够通过转至“开始”->“所有程序”->“TAP-Windows”->“实用程序”->“添加新的 TAP-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 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

连接到客户端 VPN 终端节点时，客户端意外退出。

原因

计算机上未安装 TAP-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

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

如果客户端 VPN 终端节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。

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：

- DBR.dll ShellExtension
- DBR.dll OverlayIconBackuped
- DBR.dll OverlayIconNotBackuped

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。

   - DBR.dll ShellExtension
   - DBR.dll OverlayIconBackuped
   - DBR.dll OverlayIconNotBackuped

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

VPN 断开连接并显示弹出消息

问题

VPN 断开连接并弹出一条消息，上面写着：“由于您的设备所连接的本地网络的地址空间已更改，VPN 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
```

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客户端 VPN 终端节点的连接失败，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

在客户端 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)。

macOS 故障排查

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。

主题

AWS 提供的客户

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。

```
/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
```

主题

- 客户端卡在重新连接状态
- 客户端无法创建配置文件

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

如果客户端 VPN 终端节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。

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。

找不到密码算法“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

该应用程序使用不支持密码算法 AES-256-GCM 的 OpenVPN 版本。

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

请求客户端 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，请与您的客户端 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客户端 VPN 终端节点，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

请求客户端 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 无法解析客户端 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。

Linux 故障排查

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
- OpenVPN（命令行）
- 通过 Network Manager 建立 OpenVPN (GUI)

AWS 提供的客户

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/username/
```

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 终端节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。它用于配置从客户端 VPN 终端节点推送的 DNS 服务器。出现问题的原因是 systemd-resolved 未为客户端 VPN 终端节点提供的 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

客户端 VPN 终端节点上未配置 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（在客户端 VPN 终端节点中配置）。

```
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）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。请客户端 VPN 管理员验证以下信息：

- 客户端 VPN 终端节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 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
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 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。