# VPN do cliente da AWS

## Guia do usuário

# VPN do cliente da AWS: Guia do usuário

# Table of Contents

# O que é AWS Client VPN?

O AWS Client VPN é um serviço de VPN gerenciado baseado no cliente que protege o acesso aos recursos da AWS e aos recursos na sua rede on-premises.

Este guia fornece as etapas para estabelecer uma conexão VPN com um endpoint do Client VPN usando uma aplicação cliente em seu dispositivo.

## Componentes

Veja a seguir os principais componentes para usar o AWS Client VPN.

- Endpoint do Client VPN: o administrador do Client VPN cria e configura um endpoint do Client VPN na AWS. O administrador controla quais redes e recursos você pode acessar ao estabelecer uma conexão VPN.
- Aplicação cliente da VPN: o software que você usa para se conectar ao endpoint do Client VPN e estabelecer uma conexão VPN segura.
- Arquivo de configuração de endpoint do Client VPN: arquivo de configuração fornecido pelo administrador do Client VPN. O arquivo inclui informações sobre o endpoint do Client VPN e os certificados necessários para estabelecer uma conexão VPN. Você carrega esse arquivo na aplicação cliente da VPN escolhida.

## Recursos adicionais

Se você for um administrador do Client VPN, consulte o AWS Client VPN: Guia do administrador para obter mais informações sobre como criar e configurar um endpoint do Client VPN.

# Conceitos básicos da cliente VPN

Para poder estabelecer uma sessão de VPN, o administrador da cliente VPN deve criar e configurar um endpoint da cliente VPN. Seu administrador controla quais redes e recursos você pode acessar ao estabelecer uma sessão de VPN. Você pode usar uma aplicação cliente de VPN para se conectar a um endpoint da cliente VPN. e estabelecer uma conexão VPN segura.

Se você for um administrador que precisa criar um endpoint da cliente VPN, consulte o Guia do administrador da AWS Client VPN.

Tópicos



# Prerequisites

Para estabelecer uma conexão VPN, você deve ter o seguinte:

- Acesso à Internet
- Um dispositivo compatível
- Para endpoints da cliente VPN que usam autenticação federada baseada em SAML (autenticação única), um dos seguintes navegadores:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

# Etapa 1: Obter uma aplicação cliente de VPN

Você pode se conectar a um endpoint da cliente VPN e estabelecer uma conexão VPN usando o cliente fornecido pela AWS ou outra aplicação do cliente baseada no OpenVPN.

O cliente fornecido pela AWS é compatível no Windows, macOS, Ubuntu 18.04 LTS e Ubuntu 20.04 LTS. Você pode fazer download do cliente em AWS Client VPN download (Fazer download da VPN do cliente da AWS).

Faça download de uma aplicação cliente OpenVPN e instale-a no dispositivo no qual você pretende estabelecer a conexão VPN.

# Etapa 2: Obter o arquivo de configuração do endpoint da cliente VPN.

É necessário obter o arquivo de configuração do endpoint da cliente VPN. do seu administrador. O arquivo de configuração inclui as informações sobre o endpoint da cliente VPN e os certificados necessários para estabelecer uma conexão VPN.

Como alternativa, se o administrador da cliente VPN configurou um portal de autoatendimento para o endpoint da cliente VPN, você pode fazer download da versão mais recente do cliente fornecido pela AWS e da versão mais recente do arquivo de configuração do endpoint da cliente VPN. Para obter mais informações, consulte Usar o portal de autoatendimento (p. 3).

# Etapa 3: Conectar-se à VPN

Importe o arquivo de configuração do endpoint da cliente VPN para o cliente fornecido pela AWS ou a sua aplicação de cliente do OpenVPN e conecte-se à VPN. Para obter as etapas para se conectar a uma VPN, consulte os seguintes tópicos:

- Conecte-se usando um cliente fornecido pela AWS (p. 4)
- Conectar-se usando um cliente OpenVPN (p. 18)

Para endpoints da cliente VPN. que usam a autenticação do Active Directory, será solicitado que você insira seu nome de usuário e senha. Se a autenticação multifator (MFA) tiver sido habilitada para o diretório, também será solicitado que você insira o código da MFA.

Para endpoints da cliente VPN que usam autenticação federada baseada em SAML (autenticação única), o cliente fornecido pela AWS abre uma janela do navegador no computador. Você será solicitado a inserir suas credenciais corporativas antes de poder se conectar ao endpoint da cliente VPN.

# Usar o portal de autoatendimento

O administrador do endpoint da cliente VPN. pode configurar um portal de autoatendimento para o endpoint da cliente VPN. O portal de autoatendimento é uma página da Web que habilita que você faça download da versão mais recente do cliente fornecido pela AWS e da versão mais recente do arquivo de configuração do endpoint da cliente VPN. Para obter mais informações sobre como configurar o portal de autoatendimento, consulte Endpoints da cliente VPN no Guia do administrador da AWS Client VPN.

Antes de começar, você deve ter o ID do endpoint da cliente VPN. O administrador do endpoint da cliente VPN pode fornecer a você o ID ou um URL do portal de autoatendimento que inclui o ID.

### Para acessar o portal de autoatendimento

1. Acesse o portal de autoatendimento em https://self-service.clientvpn.amazonaws.com/ ou use o URL que foi fornecido pelo seu administrador.
2. Se necessário, insira o ID do endpoint da cliente VPN, por exemplo, `cvpn-endpoint-0123456abcd123456`. Escolha Next (Próximo).
3. Digite seu nome de usuário e senha e escolha Sign In (Fazer login). Este é o mesmo nome de usuário e senha que você usa para se conectar ao endpoint da cliente VPN.
4. No portal de autoatendimento, você pode fazer o seguinte:
   - Faça download da versão mais recente do arquivo de configuração do cliente para o endpoint da cliente VPN.
   - Faça download da versão mais recente do cliente fornecido pela AWS para a sua plataforma.

# Conecte-se usando um cliente fornecido pela AWS

É possível se conectar a um endpoint da cliente VPN usando o cliente fornecido pela AWS. O cliente fornecido pela AWS é compatível no Windows, macOS, Ubuntu 18.04 LTS e Ubuntu 20.04 LTS.

Clientes

- AWS Client VPN para Windows: (p. 4)
- AWS Client VPN para macOS (p. 9)
- AWS Client VPN para Linux (p. 13)

Diretivas do OpenVPN

O cliente fornecido pela AWS é compatível com as seguintes diretivas do OpenVPN:

- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- cryptoapicert (Somente Windows)
- dev
- key
- nobind
- persist-key
- persist-tun
- proto
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb

## AWS Client VPN para Windows:

O procedimento a seguir mostra como estabelecer uma conexão de VPN usando o cliente fornecido pela AWS para Windows. Você pode baixar e instalar o cliente em AWS Client VPN download (Baixar VPN do cliente da AWS). O cliente fornecido pela AWS não é compatível com atualizações automáticas.

Índice



# Requisitos

Para usar o cliente fornecido pela AWS para Windows, é necessário o seguinte:

- Sistema operacional Windows 10 de 64 bits, processador x64
- .NET Framework 4.7.2 ou superior

O cliente reserva a porta TCP 8096 no computador. Para endpoints da cliente VPN que usam autenticação federada baseada em SAML (autenticação única), o cliente reserva a porta TCP 35001.

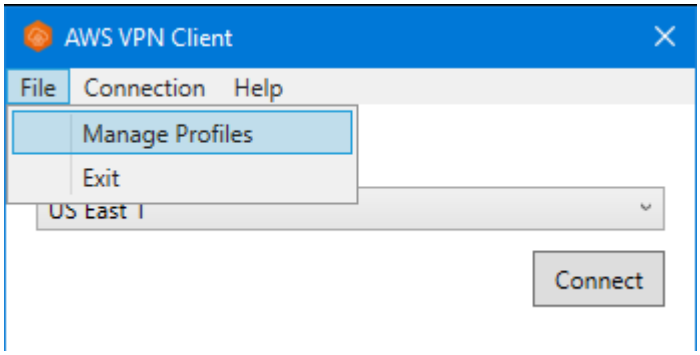
Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

# Conexão

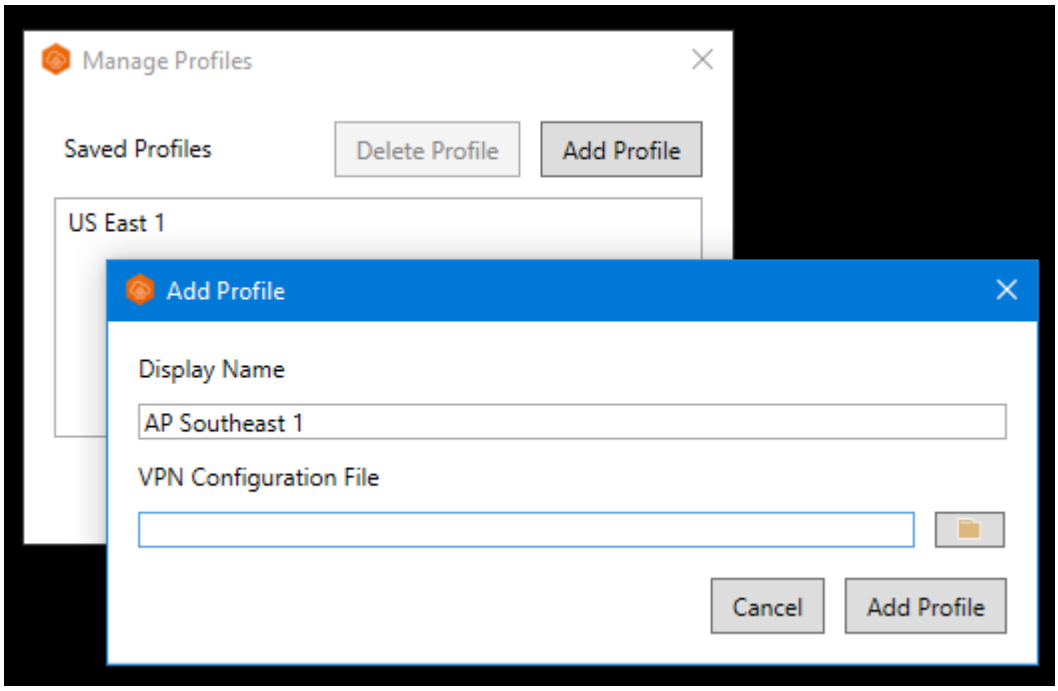
Antes de começar, certifique-se de que leu os Requisitos (p. 5). O cliente fornecido da AWS também será referido como cliente AWS VPN nas etapas a seguir.

### Para se conectar usando o cliente fornecido pela AWS para Windows

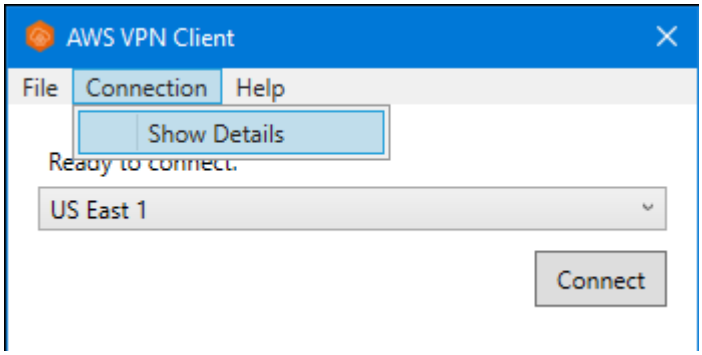
1. Abra a aplicação cliente AWS VPN.
2. Escolha Arquivo, Gerenciar Perfis.



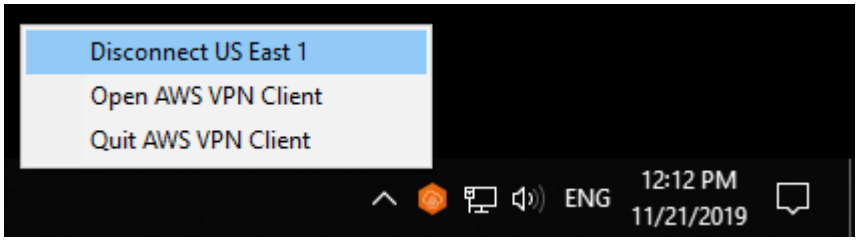

3. Escolha Adicionar perfil.




4. Em Nome para exibição, insira um nome para o perfil.
5. Para o Arquivo de configuração de VPN, navegue e selecione o arquivo de configuração que você recebeu de seu administrador do VPN do Cliente e escolha Adicionar perfil.
6. Na janela AWS VPN Client (Cliente VPN), verifique se seu perfil está selecionado e escolha Connect (Conectar). Se o endpoint da cliente VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha.
7. Para visualizar as estatísticas de sua conexão, escolha Conexão, Mostrar detalhes.




8. Para se desconectar, na janela AWS VPN Cliente (cliente VPN), selecione Desconnect (Desconectar). Como alternativa, escolha o ícone do cliente na barra de tarefas do Windows e escolha (Desconectar-se.



# Notas de lançamento

A tabela a seguir contém as notas de release e os links para baixar as versões atual e anteriores da AWS Client VPN para Windows.

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 3.1.0 | • Procedimento de segurança aprimorado. | 23 de maio de 2022 | Baixar a versão 3.1.0<br>sha256: 74ad66c5062d484173581deaa9bd6 |
| 3.0.0 | • Adicionado suporte ao Windows 11.<br>• Corrigida a nomeação do driver TAP Windows fazendo com que outros nomes de driver fossem afetados.<br>• Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada.<br>• Corrigida a exibição do texto do banner para texto mais longo.<br>• Aprimorada a postura de segurança. | 03 de março de 2022 | Não é mais compatível. |
| 2.0.0 | • Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida.<br>• Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco<br>• Pequenas correções de bugs e melhorias. | 20 de janeiro de 2022 | Não é mais compatível. |
| 1.3.7 | • Tentativa de conexão de autenticação federada corrigida em alguns casos.<br>• Pequenas correções de bugs e melhorias. | 8 de novembro de 2021 | Não é mais compatível. |
| 1.3.6 | • Adição de suporte a sinalizadores OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Pequenas correções de bugs e melhorias. | 20 de setembro de 2021 | Não é mais compatível. |
| 1.3.5 | • Patch para excluir grandes arquivos de log do Windows. | 16 de agosto de 2021 | Não é mais compatível. |
| 1.3.4 | • Adicionado suporte para o sinalizador OpenVPN: dhcp-option.<br>• Pequenas correções de bugs e melhorias. | 4 de agosto de 2021 | Não é mais compatível. |
| 1.3.3 | • Adicionado suporte para sinalizadores do OpenVPN: inativo, pull-filter, rota.<br>• Corrigido um problema que causava uma falha na aplicação na desconexão ou saída. | 1.º de julho de 2021 | Não é mais compatível. |

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| | • Corrigido um problema com nomes de usuário do Active Directory com barra invertida.<br>• Corrigido o travamento da aplicação ao manipular a lista de perfis fora da aplicação.<br>• Pequenas correções de bugs e melhorias. | | |
| 1.3.2 | • Adicione prevenção de vazamento IPv6, quando é configurado.<br>• Falha em potencial corrigida quando a opção Show Details (Mostrar detalhes) em Connection (Conexão) foi usada. | 12 de maio de 2021 | Não é mais compatível. |
| 1.3.1 | • Adicionado suporte para vários certificados de cliente com o mesmo assunto. Os certificados expirados serão ignorados.<br>• Retenção de log local corrigida para reduzir o uso do disco.<br>• Adicionado suporte para a diretiva “route-ipv6” do OpenVPN.<br>• Pequenas correções de bugs e melhorias. | 5 de abril de 2021 | Não é mais compatível. |
| 1.3.0 | Recursos de suporte adicionados, como relatórios de erros, envio de logs de diagnóstico e análise de dados. | 8 de março de 2021 | Não é mais compatível. |
| 1.2.7 | • Adicionado suporte para a diretiva cryptoapicert do OpenVPN.<br>• Rotas obsoletas fixas entre conexões.<br>• Pequenas correções de bugs e melhorias. | 25 de fevereiro de 2021 | Não é mais compatível. |
| 1.2.6 | Pequenas correções de bugs e melhorias. | 26 de outubro de 2020 | Não é mais compatível. |
| 1.2.5 | • Adicionado suporte para comentários na configuração do OpenVPN.<br>• Adicionada uma mensagem de erro para erros de handshake do TLS. | 8 de outubro de 2020 | Não é mais compatível. |
| 1.2.4 | Pequenas correções de bugs e melhorias. | 1.º de setembro de 2020 | Não é mais compatível. |
| 1.2.3 | Reverter alterações na versão 1.2.2. | 20 de agosto de 2020 | Não é mais compatível. |
| 1.2.1 | Pequenas correções de bugs e melhorias. | 1.º de julho de 2020 | Não é mais compatível. |
| 1.2.0 | • Adicionado suporte para autenticação federada baseada em SAML 2.0.<br>• Suporte obsoleto para a plataforma Windows 7. | 19 de maio de 2020 | Não é mais compatível. |

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 1.1.1 | Pequenas correções de bugs e melhorias. | 21 de abril de 2020 | Não é mais compatível. |
| 1.1.0 | • Adicionado suporte para a funcionalidade de eco de desafio estático do OpenVPN para ocultar ou mostrar o texto exibido na interface do usuário.<br>• Pequenas correções de bugs e melhorias. | 9 de março de 2020 | Não é mais compatível. |
| 1.0.0 | A versão inicial. | 4 de fevereiro de 2020 | Não é mais compatível. |

# AWS Client VPN para macOS

O procedimento a seguir mostra como estabelecer uma conexão VPN usando o cliente fornecido pela AWS pelo cliente para macOS. Você pode baixar e instalar o cliente em AWS Client VPN download (Baixar VPN do cliente da AWS). O cliente fornecido pela AWS não é compatível com atualizações automáticas.

Índice



## Requisitos

Para usar o cliente fornecido pela AWS para macOS, é necessário o seguinte:

- macOS Mojave (10.14), Catalina (10.15) ou Big Sur (11.0) de 64 bits

O cliente reserva a porta TCP 8096 no computador. Para endpoints da cliente VPN que usam autenticação federada baseada em SAML (autenticação única), o cliente reserva a porta TCP 35001.

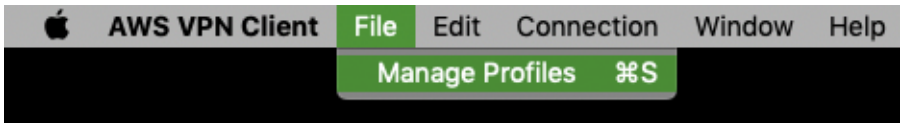
Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

## Conexão

Antes de começar, certifique-se de que leu os Requisitos (p. 9). O cliente fornecido pela AWS também será referido como cliente AWS VPN nas etapas a seguir.

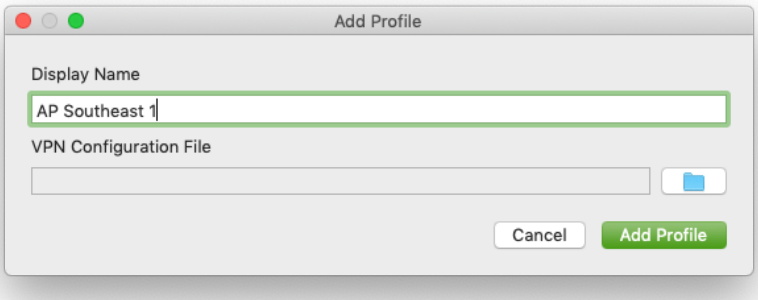
### Para se conectar usando o cliente fornecido pela AWS para macOS

1. Abra a aplicação cliente AWS VPN.
2. Escolha Arquivo, Gerenciar Perfis.



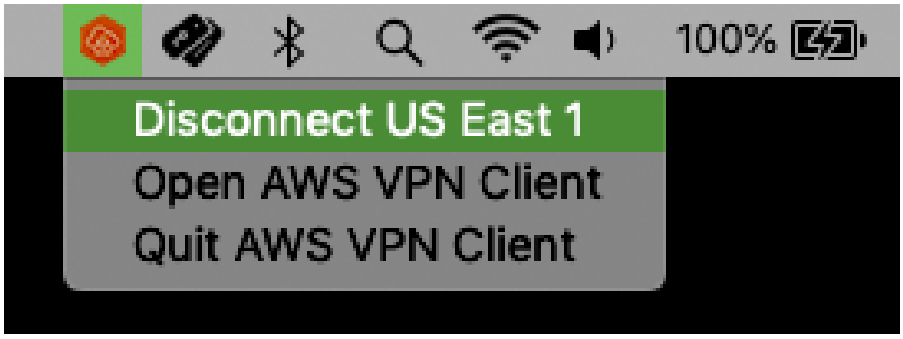

3. Escolha Adicionar perfil.

4. Em Nome para exibição, insira um nome para o perfil.




5. Para Arquivo de configuração da VPN, navegue até o arquivo de configuração que você recebeu do administrador do VPN do Cliente. Escolha Abrir.
6. Escolha Adicionar perfil.
7. Na janela AWS VPN Client (cliente VPN), verifique se seu perfil está selecionado e escolha Connect (Conectar). Se o endpoint da cliente VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha.
8. Para visualizar as estatísticas de sua conexão, escolha Conexão, Mostrar detalhes.


9. Para se desconectar, na janela AWS VPN Cliente (cliente VPN), selecione Desconnect (Desconectar). Como alternativa, escolha o ícone do cliente na barra de menus e escolha Desconectar <nome-do-seu-perfil>.




# Notas de lançamento

As tabelas a seguir contêm as notas de release e os links para baixar as versões atual e anteriores da AWS Client VPN para macOS.

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 3.1.0 | • Suporte adicionado para macOS Monterey.<br>• Problema corrigido para detecção de tipo de unidade. | 23 de maio de 2022 | Baixar a versão 3.1.0<br><br>sha256: d88a4b5c9c0f9e64cef52ab508c65a |

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| | • Procedimento de segurança aprimorado. | | |
| 3.0.0 | • Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada.<br>• Corrigida a exibição do texto do banner para texto mais longo.<br>• Aprimorada a postura de segurança. | 03 de março de 2022 | Não é mais compatível. |
| 2.0.0 | • Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida.<br>• Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco<br>• Pequenas correções de bugs e melhorias. | 20 de janeiro de 2022 | Não é mais compatível. |
| 1.4.0 | • Adicionado o monitoramento do servidor DNS durante a conexão. As configurações serão reconfiguradas se não corresponderem às configurações de VPN.<br>• Tentativa de conexão de autenticação federada corrigida em alguns casos.<br>• Pequenas correções de bugs e melhorias. | 9 de novembro de 2021 | Não é mais compatível. |
| 1.3.5 | • Adição de suporte a sinalizadores OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Pequenas correções de bugs e melhorias. | 20 de setembro de 2021 | Não é mais compatível. |
| 1.3.4 | • Adicionado suporte para o sinalizador OpenVPN: dhcp-option.<br>• Pequenas correções de bugs e melhorias. | 4 de agosto de 2021 | Não é mais compatível. |
| 1.3.3 | • Adicionado suporte para sinalizadores do OpenVPN: inativo, pull-filter, rota.<br>• Corrigido um problema com nomes de arquivos de configuração com espaços ou Unicode.<br>• Corrigido um problema que causava uma falha na aplicação na desconexão ou saída.<br>• Corrigido um problema com nomes de usuário do Active Directory com barra invertida.<br>• Corrigido o travamento da aplicação ao manipular a lista de perfis fora da aplicação.<br>• Pequenas correções de bugs e melhorias. | 1.º de julho de 2021 | Não é mais compatível. |

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 1.3.2 | • Adicione prevenção de vazamento IPv6, quando é configurado.<br>• Falha em potencial corrigida quando a opção Show Details (Mostrar detalhes) em Connection (Conexão) foi usada.<br>• Adicione rotação de log daemon. | 12 de maio de 2021 | Não é mais compatível. |
| 1.3.1 | • Adicionado suporte para macOS Big Sur (10.16).<br>• Corrigido o problema que removia as configurações de DNS definidas por outras aplicações.<br>• Corrigido um problema ao usar um certificado inválido para autenticação mútua que causava problemas de conectividade.<br>• Adicionado suporte para a diretiva “route-ipv6” do OpenVPN.<br>• Pequenas correções de bugs e melhorias. | 5 de abril de 2021 | Não é mais compatível. |
| 1.3.0 | Recursos de suporte adicionados, como relatórios de erros, envio de logs de diagnóstico e análise de dados. | 8 de março de 2021 | Não é mais compatível. |
| 1.2.5 | Pequenas correções de bugs e melhorias. | 25 de fevereiro de 2021 | Não é mais compatível. |
| 1.2.4 | Pequenas correções de bugs e melhorias. | 26 de outubro de 2020 | Não é mais compatível. |
| 1.2.3 | • Adicionado suporte para comentários na configuração do OpenVPN.<br>• Adicionada uma mensagem de erro para erros de handshake do TLS.<br>• Corrigido um erro de desinstalação que estava afetando alguns usuários. | 8 de outubro de 2020 | Não é mais compatível. |
| 1.2.2 | Pequenas correções de bugs e melhorias. | 12 de agosto de 2020 | Não é mais compatível. |
| 1.2.1 | • Adicionado suporte para desinstalar a aplicação.<br>• Pequenas correções de bugs e melhorias. | 1.º de julho de 2020 | Não é mais compatível. |
| 1.2.0 | • Adicionado suporte para autenticação federada baseada em SAML 2.0.<br>• Adicionado suporte para macOS Catalina (10.15). | 19 de maio de 2020 | Não é mais compatível. |
| 1.1.2 | Pequenas correções de bugs e melhorias. | 21 de abril de 2020 | Não é mais compatível. |

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 1.1.1 | • Corrigido um problema em que o DNS não estava resolvendo.<br>• Corrigido um problema de falha da aplicação causada por conexões mais longas.<br>• Corrigido um problema de MFA. | 2 de abril de 2020 | Não é mais compatível. |
| 1.1.0 | • Adicionado suporte para a configuração de DNS do macOS.<br>• Adicionado suporte para a funcionalidade de eco de desafio estático do OpenVPN para ocultar ou mostrar o texto exibido na interface do usuário.<br>• Pequenas correções de bugs e melhorias. | 9 de março de 2020 | Não é mais compatível. |
| 1.0.0 | A versão inicial. | 4 de fevereiro de 2020 | Não é mais compatível. |

# AWS Client VPN para Linux

Os procedimentos a seguir mostram como instalar o cliente fornecido pela AWS para Linux e estabelecer uma conexão VPN usando o cliente fornecido pela AWS. O cliente fornecido pela AWS não é compatível com atualizações automáticas.

Índice



## Requisitos

Para usar o cliente fornecido pela AWS para Linux, é necessário o seguinte:

- Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS (somente AMD64)

O cliente reserva a porta TCP 8096 no computador. Para endpoints da cliente VPN que usam autenticação federada baseada em SAML (autenticação única), o cliente reserva a porta TCP 35001.

Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

## Instalação

Existem vários métodos que podem ser usados para instalar o cliente fornecido pela AWS para Linux. Use um dos métodos fornecidos nas opções a seguir. Antes de começar, certifique-se de que leu os Requisitos (p. 13).

### Opção 1: Instalar via repositório de pacotes

1. Adicione a chave pública da VPN do cliente da AWS ao seu sistema operacional Ubuntu.

```
wget -q -O - https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo/
awsvpnclient_public_key.asc | sudo apt-key add -
```

2. Use o comando aplicável para adicionar o repositório ao seu sistema operacional Ubuntu, dependendo da sua versão do Ubuntu:

   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. Use o comando a seguir para atualizar os repositórios no seu sistema.

```
sudo apt-get update
```

4. Use o comando a seguir para instalar o cliente fornecido pela AWS para Linux.

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

### Opção 2: Instalar usando o arquivo de pacote. deb

1. Baixe o arquivo .deb em Client VPN downloadAWS (Baixar VPN do cliente da AWS) ou usando o comando a seguir.

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

2. Instalar o cliente fornecido pela AWS para Linux usando a utilidade `dpkg`.

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

### Opção 3: Instale o pacote .deb usando o Ubuntu Software Center

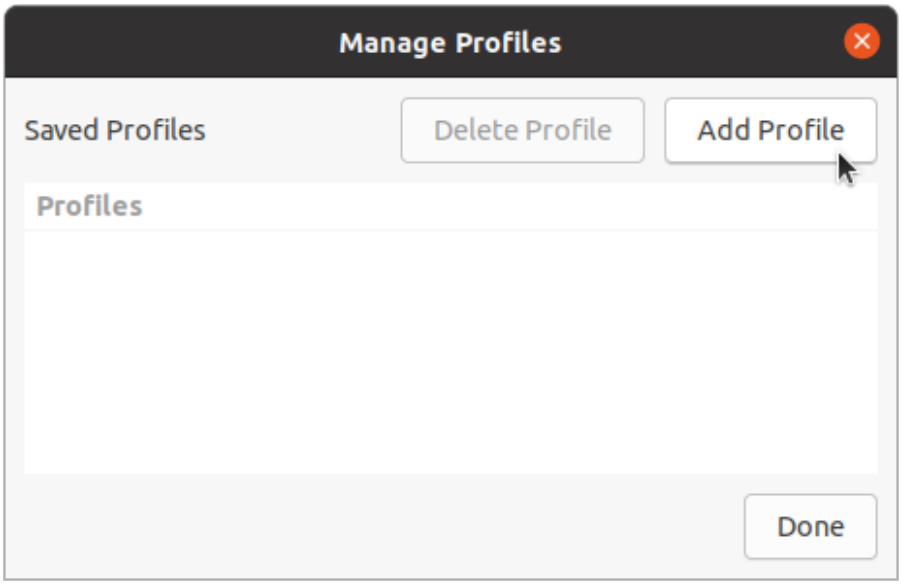
1. Baixe o arquivo do pacote. deb em AWS Client VPN download (Baixar VPN do Cliente).
2. Depois de fazer download do arquivo do pacote.deb, use o Ubuntu Software Center para instalar o pacote. Siga as etapas para instalar de um pacote. deb autônomo usando o Ubuntu Software Center, conforme descrito no Wiki do Ubuntu.

# Conexão

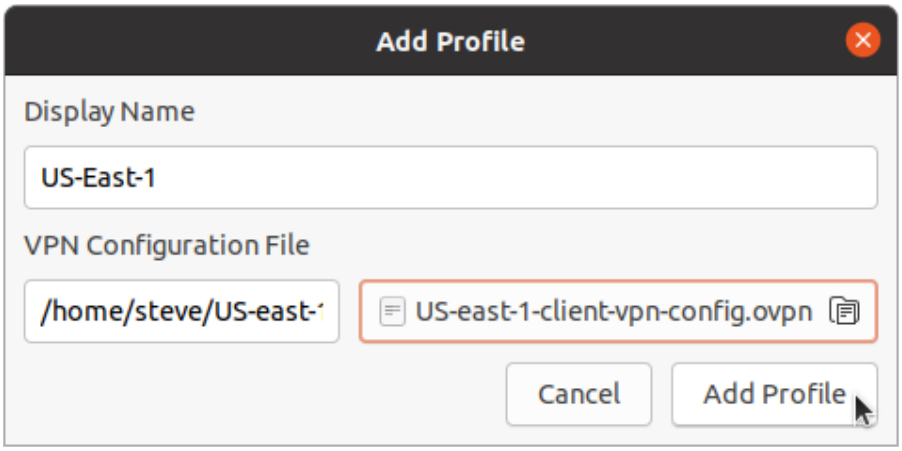
O cliente fornecido pela AWS também será referido como cliente AWS VPN nas etapas a seguir.

Para se conectar usando o cliente fornecido pela AWS para Linux

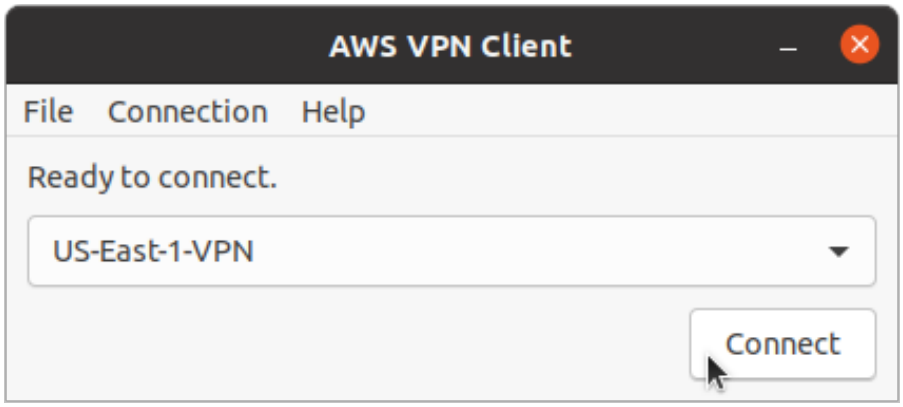
1. Abra a aplicação cliente AWS VPN.
2. Escolha  Arquivo, Gerenciar Perfis.
3. Escolha Adicionar perfil.



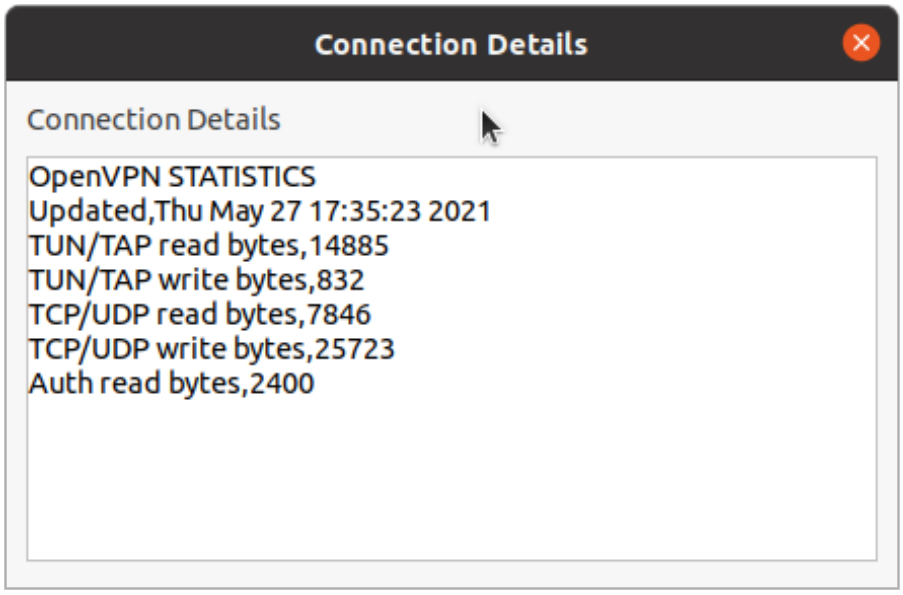

4. Em Nome para exibição, insira um nome para o perfil.
5. Para Arquivo de configuração da VPN, navegue até o arquivo de configuração que você recebeu do administrador do VPN do Cliente. Escolha Abrir.
6. Escolha Adicionar perfil.



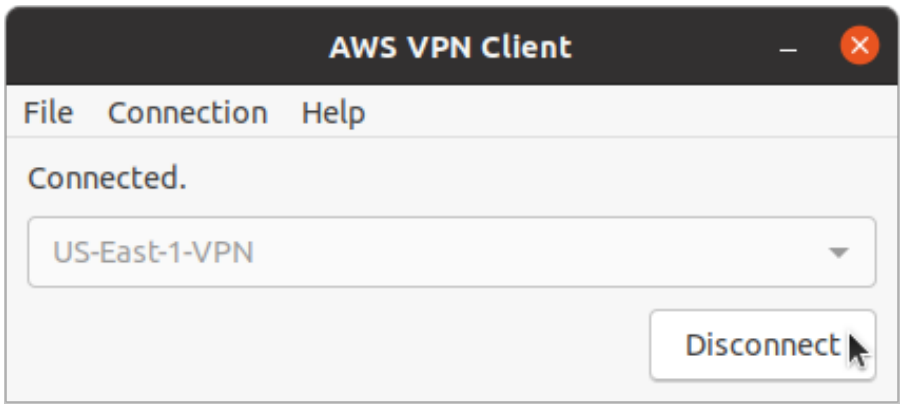

7. Na janela AWS VPN Client (Cliente VPN), verifique se seu perfil está selecionado e escolha Connect (Conectar). Se o endpoint da cliente VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha.




8. Para visualizar as estatísticas de sua conexão, escolha Conexão, Mostrar detalhes.




9. Para se desconectar, na janela AWS VPN Cliente (cliente VPN), selecione Desconnect (Desconectar).




# Notas de lançamento

As tabelas a seguir contêm as notas de release e os links para baixar as versões atual e anteriores do AWS Client VPN para Linux.

| Versão | Alterações | Data | Link para fazer download |
|---|---|---|---|
| 3.1.0 | • Problema corrigido para detecção de tipo de unidade.<br>• Procedimento de segurança aprimorado. | 23 de maio de 2022 | Baixar a versão 3.1.0<br>sha256: c43581e87262b5424f5a96c8a7553 |
| 3.0.0 | • Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada.<br>• Corrigida a exibição do texto do banner para texto mais longo e sequências de caracteres específicas.<br>• Aprimorada a postura de segurança. | 03 de março de 2022 | Não é mais compatível. |
| 2.0.0 | • Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida.<br>• Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco<br>• Pequenas correções de bugs e melhorias. | 20 de janeiro de 2022 | Não é mais compatível. |
| 1.0.3 | • Tentativa de conexão de autenticação federada corrigida em alguns casos.<br>• Pequenas correções de bugs e melhorias. | 8 de novembro de 2021 | Não é mais compatível. |
| 1.0.2 | • Adição de suporte a sinalizadores OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Pequenas correções de bugs e melhorias. | 28 de setembro de 2021 | Não é mais compatível. |
| 1.0.1 | • Opção habilitada para sair da barra de aplicações do Ubuntu.<br>• Adicionado suporte para sinalizadores do OpenVPN: inativo, pull-filter, rota.<br>• Pequenas correções de bugs e melhorias. | 4 de agosto de 2021 | Não é mais compatível. |
| 1.0.0 | A versão inicial. | 11 de junho de 2021 | Não é mais compatível. |

# Conectar-se usando um cliente OpenVPN

Você pode se conectar a um endpoint do Client VPN usando aplicações comuns do cliente OpenVPN.

> Note
>
> No caso da autenticação federada baseada em SAML, é necessário usar o cliente fornecido pela AWS para se conectar a um endpoint da VPN do cliente. Para obter mais informações, consulte Conecte-se usando um cliente fornecido pela AWS (p. 4) ou entre em contato com o administrador da VPN.

Aplicativos cliente

- Conectar usando uma aplicação cliente do Windows (p. 18)
- Conecte-se usando uma aplicação do VPN do Cliente para Android ou iOS (p. 20)
- Conectar usando uma aplicação cliente do macOS (p. 21)
- Conectar usando uma aplicação cliente do OpenVPN (p. 23)

# Conectar usando uma aplicação cliente do Windows

Os procedimentos a seguir mostram como estabelecer uma conexão VPN usando clientes VPN baseadas no Windows.

Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

Para obter informações sobre a solução de problemas, consulte Solução de problemas do Windows (p. 25).

## OpenVPN usando um certificado da Windows Certificate System Store

Você pode configurar o cliente OpenVPN para usar um certificado e uma chave privada na Windows Certificate System Store. Esta opção é útil quando você usa um cartão inteligente como parte da conexão da cliente VPN. Para obter informações sobre a opção cryptoapicert do cliente OpenVPN, consulte o Manual de referência para o OpenVPN no site do OpenVPN.

> Note
>
> O certificado deve ser armazenado no computador local.

Para usar a opção cryptoapicert com o OpenVPN

1. Crie um arquivo .pfx que contenha o certificado do cliente e a chave privada.

2. Importe o arquivo .pfx para o seu armazenamento de certificados pessoais, no computador local. Para obter mais informações, consulte Como: exibir certificados com o snap-in MMC no site da Microsoft.
3. Verifique se sua conta tem permissões para ler o certificado do computador local. Você pode usar o Console de Gerenciamento da Microsoft para modificar as permissões. Para obter mais informações, consulte Direitos para ver o armazenamento de certificados no computador local no site da Microsoft Technet.
4. Atualize o arquivo de configuração do OpenVPN e especifique o certificado usando o assunto ou a impressão digital do certificado.

   Veja a seguir um exemplo de especificação do certificado usando um assunto.

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

   Veja a seguir um exemplo de especificação do certificado usando uma impressão digital. Você pode encontrar a impressão digital usando o Console de Gerenciamento da Microsoft. Para obter mais informações, consulte Como recuperar a impressão digital de um certificado no site da Microsoft Technet.

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

Depois de concluir a configuração, use o OpenVPN para estabelecer uma conexão.

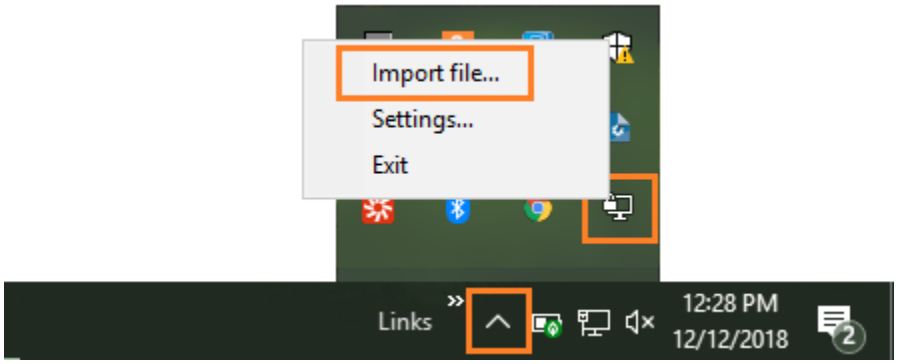
# GUI do OpenVPN

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação cliente GUI do OpenVPN em um computador Windows.

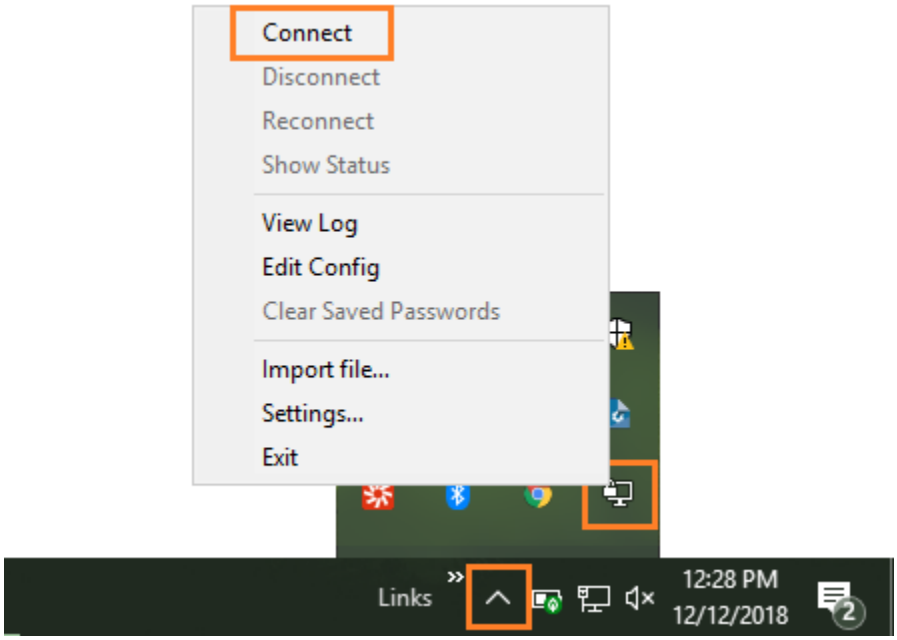
> Note
>
> Para obter informações sobre a aplicação cliente OpenVPN, consulte Downloads da comunidade no site do OpenVPN.

### Para estabelecer uma conexão VPN

1. Inicie a aplicação cliente OpenVPN.
2. Na barra de tarefas do Windows, escolha Show/Hide icons (Mostrar/ocultar ícones), clique com o botão direito do mouse em OpenVPN GUI (GUI do OpenVPN) e escolha Import file (Importar arquivo).




3. Na caixa de diálogo Open (Abrir), selecione o arquivo de configuração recebido do administrador da cliente VPN e escolha Open (Abrir).
4. Na barra de tarefas do Windows, escolha Show/Hide icons (Mostrar/ocultar ícones), clique com o botão direito do mouse em OpenVPN GUI (GUI do OpenVPN) e escolha Connect (Conectar).




## Cliente OpenVPN Connect

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação cliente OpenVPN Connect em um computador Windows.

> **Note**
>
> Para obter mais informações, consulte Como se conectar ao servidor de acesso com o Windows no site do OpenVPN.

Para estabelecer uma conexão VPN

1. Inicie a aplicação cliente OpenVPN Connect.
2. Na barra de tarefas do Windows, escolha Show/Hide icons (Mostrar/ocultar ícones), clique com o botão direito do mouse em OpenVPN e escolha Import profile (Importar perfil).
3. Escolha Import from File (Importar de arquivo) e selecione o arquivo de configuração que você recebeu do administrador da cliente VPN.
4. Escolha o perfil de conexão para iniciar a conexão.

# Conecte-se usando uma aplicação do VPN do Cliente para Android ou iOS

As informações a seguir mostram como estabelecer uma conexão VPN usando a aplicação cliente do OpenVPN em um dispositivo móvel Android ou iOS. As etapas para o Android e o iOS são as mesmas.

> **Note**
>
> Para obter mais informações sobre a aplicação cliente OpenVPN para Android, consulte Perguntas frequentes sobre OpenVPN Connect Android no site do OpenVPN.

Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

Para estabelecer a conexão, inicie a aplicação cliente do OpenVPN e importe o arquivo que recebeu do administrador da cliente VPN.

# Conectar usando uma aplicação cliente do macOS

Os procedimentos a seguir mostram como estabelecer uma conexão VPN usando clientes VPN baseados no macOS.

Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

Para obter informações sobre a solução de problemas, consulte Solução de problemas macOS (p. 30).

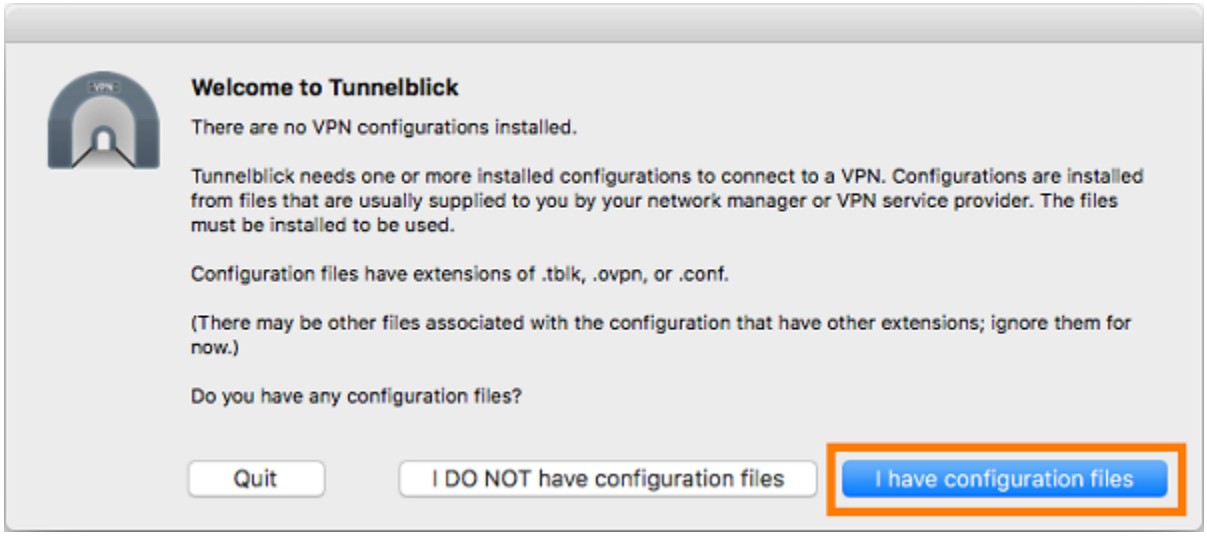
## Tunnelblick

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação cliente Tunnelblick em um computador macOS.

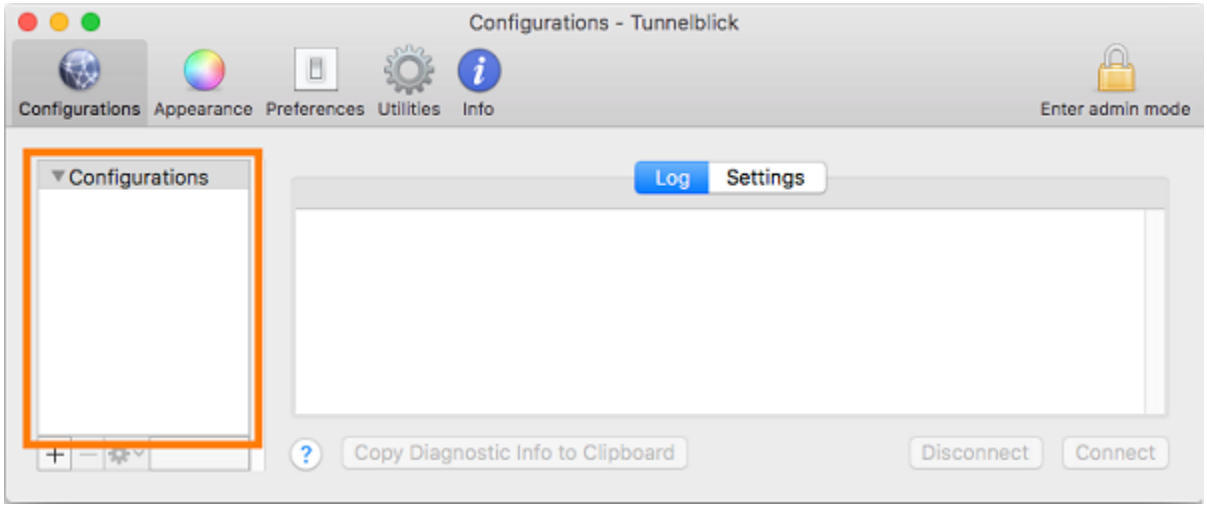
> **Note**
>
> Para obter mais informações sobre a aplicação cliente Tunnelblick para macOS, consulte a documentação do Tunnelblick no site do Tunnelblick.

### Para estabelecer uma conexão VPN

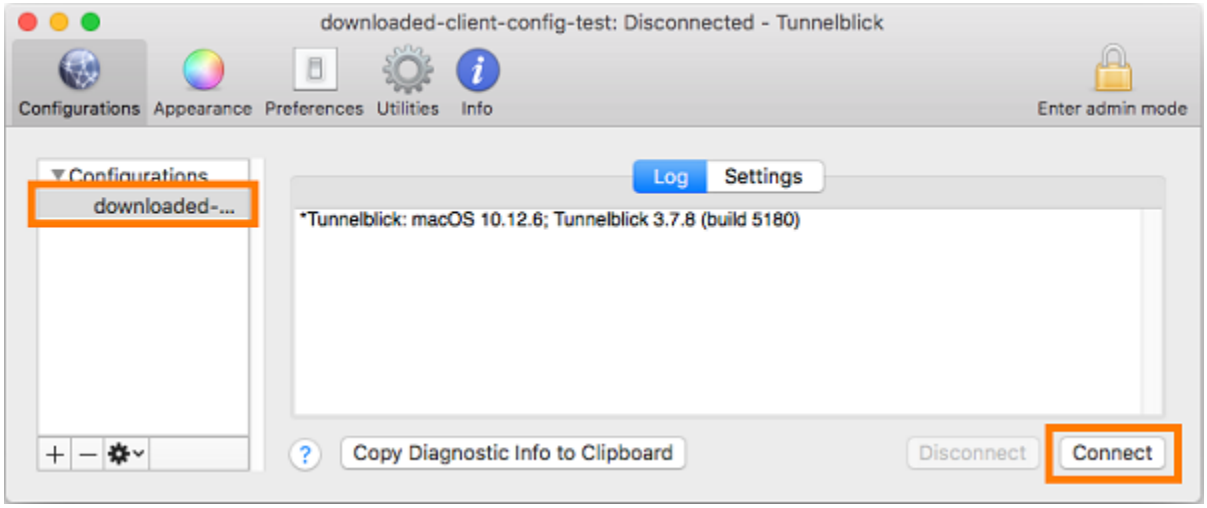
1. Inicie a aplicação cliente Tunnelblick e escolha I have configuration files (Tenho arquivos de configuração).




2. Arraste e solte o arquivo de configuração recebido do administrador da VPN no painel Configurations (Configurações).




3. Selecione o arquivo de configuração no painel Configurations (Configurações) e escolha Connect (Conectar).




# Cliente OpenVPN Connect

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação cliente OpenVPN Connect em um computador macOS.

> Note
>
> Para obter mais informações, consulte Como se conectar ao servidor de acesso com o macOS no site do OpenVPN.

### Para estabelecer uma conexão VPN

1. Inicie a aplicação OpenVPN e selecione Import (Importar), From local file... (Do arquivo local...).
2. Navegue até o arquivo de configuração que você recebeu do administrador da VPN e selecione Open (Abrir).

# Conectar usando uma aplicação cliente do OpenVPN

Os procedimentos a seguir mostram como estabelecer uma conexão VPN usando clientes VPN baseados no OpenVPN.

Antes de começar, certifique-se de que o administrador da cliente VPN criou um endpoint da cliente VPN e forneceu o arquivo de configuração do endpoint da cliente VPN.

Para obter informações sobre a solução de problemas, consulte Solução de problemas Linux (p. 35).

> **Important**
>
> Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN.

## OpenVPN - Gerenciador de rede

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação OpenVPN por meio da GUI do Gerenciador de rede em um computador Ubuntu.

### Para estabelecer uma conexão VPN

1. Instale o módulo do gerenciador de rede usando o comando a seguir.

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

2. Vá para Settings (Configurações), Network (Rede).
3. Escolha o símbolo de adição (+) ao lado de VPN e escolha Import from file... (Importar do arquivo...).
4. Navegue até o arquivo de configuração que você recebeu do administrador da VPN e escolha Open (Abrir).
5. Na janela Add VPN (Adicionar VPN), escolha Add (Adicionar).
6. Inicie a conexão habilitando o seletor ao lado do perfil de VPN que você adicionou.

## OpenVPN

O procedimento a seguir mostra como estabelecer uma conexão VPN usando a aplicação OpenVPN em um computador Ubuntu.

### Para estabelecer uma conexão VPN

1. Instale o OpenVPN usando o comando a seguir.

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

2. Inicie a conexão carregando o arquivo de configuração que você recebeu do administrador da VPN.

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

# Solução de problemas de conexão VPN do Cliente

Use os tópicos a seguir para solucionar problemas que podem ocorrer ao usar uma aplicação cliente para se conectar a um endpoint da VPN do Cliente.

Tópicos



## Solução de problemas do endpoint da VPN do Cliente para administradores

Algumas das etapas deste guia podem ser executadas por você. Outras etapas devem ser executadas pelo administrador de VPN do Cliente no próprio endpoint da VPN do Cliente. As seções a seguir permitem que você saiba quando deverá entrar em contato com o administrador.

Para obter mais informações sobre como solucionar problemas do endpoint da cliente VPN, consulte Solucionar problemas de cliente VPN no Guia do administrador da AWS Client VPN.

## Enviar logs de diagnóstico para o AWS Support no cliente fornecido pela AWS

Se você tiver problemas com o cliente fornecido pela AWS e precisar entrar em contato com o AWS Support para ajudar a solucioná-los, o cliente terá a opção de enviar os logs de diagnóstico para o AWS Support. A opção está disponível nas aplicações de cliente do Windows, macOS e Linux.

Antes de enviar os arquivos, você deverá concordar em permitir que o AWS Support acesse seus logs de diagnóstico. Depois que você concordar, forneceremos um número de referência, que você pode informar ao AWS Support para que eles possam acessar os arquivos imediatamente.

### Enviando logs de diagnóstico

O cliente fornecido pela AWS também será referido como cliente AWS VPN nas etapas a seguir.

Para enviar logs de diagnóstico usando o cliente fornecido pela AWS para Windows

1. Abra a aplicação cliente AWS VPN.
2. Escolha Ajuda, Enviar logs de diagnóstico.
3. Na janela Enviar logs de diagnóstico, escolha  Sim.

4. Na janelaEnviar logs de diagnóstico, execute uma das seguintes operações:

   - Para copiar o número de referência para a área de transferência, escolha Yes (Sim) e, em seguida, OK.
   - Para monitorar manualmente o número de referência, escolha Não.

   Ao entrar em contato com o AWS Support, você precisará fornecer o número de referência.

Para enviar logs de diagnóstico usando o cliente fornecido pela AWS para macOS

1. Abra a aplicação cliente AWS VPN.
2. Escolha Ajuda, Enviar logs de diagnóstico.
3. Na janela Enviar logs de diagnóstico, escolha Sim.
4. Anote o número de referência na janela de confirmação e, em seguida, escolha OK .

   Ao entrar em contato com o AWS Support, você precisará fornecer o número de referência.

Para enviar logs de diagnóstico usando o cliente fornecido pela AWS para Ubuntu

1. Abra a aplicação cliente AWS VPN.
2. Escolha Ajuda, Enviar logs de diagnóstico.
3. Na janela Send Diagnostic Logs (Enviar registros de diagnóstico), selecione Send (Enviar).
4. Anote o número de referência na janela de confirmação. Você tem a opção de copiar as informações para a sua área de transferência, se desejar.

   Ao entrar em contato com o AWS Support, você precisará fornecer o número de referência.

# Solução de problemas do Windows

As seções a seguir contêm informações sobre problemas que você pode ter ao usar clientes baseados no Windows para se conectar a um endpoint de cliente VPN.

Tópicos



## cliente fornecido pela AWS

### cliente fornecido pela AWS

O cliente fornecido pela AWS cria logs de eventos e os armazena no local a seguir no seu computador.

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

Os seguintes tipos de logs estão disponíveis:

- Logs de aplicativos: contêm informações sobre o aplicativo. Esses logs são prefixados com "aws_vpn_client_".

- Logs do OpenVPN: contêm informações sobre os processos do OpenVPN. Esses logs são prefixados com "ovpn_aws_vpn_client_".

O cliente fornecido pela AWS usa o serviço Windows para executar operações raiz. Os logs de serviço do Windows são armazenados no seguinte local no computador:

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

Tópicos



## O cliente não consegue se conectar

Problema

O cliente fornecido pela AWS não pode se conectar ao endpoint da cliente VPN.

Causa

A causa desse problema pode ser uma das seguintes:

- Outro processo OpenVPN já está em execução no computador, o que impede que o cliente se conecte.
- Seu arquivo de configuração (.ovpn) é inválido.

Solução

Verifique se não há outras aplicações do OpenVPN em execução no computador. Se houver, pare ou feche esses processos e tente se conectar ao endpoint da cliente VPN novamente. Verifique se há erros nos logs do OpenVPN e peça ao administrador de VPN do Cliente para verificar as seguintes informações:

- Se o arquivo de configuração contém a chave e o certificado do cliente corretos. Para obter mais informações, consulte Exportar configuração do cliente no Guia do administrador da AWS Client VPN.
- Se a CRL ainda é válida. Para obter mais informações, consulte Clientes não conseguem se conectar a um endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

## O cliente está travado em um estado de reconexão

Problema

O cliente fornecido pela AWS está tentando se conectar ao endpoint da cliente VPN, mas está travado em um estado de reconexão.

Causa

A causa desse problema pode ser uma das seguintes:

- O computador não está conectado à Internet.
- O nome de host DNS não resolve para um endereço IP.

- Um processo OpenVPN está tentando se conectar ao endpoint indefinidamente.

Solução

Verifique se o computador está conectado à Internet. Peça ao administrador de VPN do Cliente para verificar se a diretiva `remote` no arquivo de configuração é resolvida para um endereço IP válido. Também é possível desconectar a sessão de VPN escolhendo Disconnect (Desconectar) na janela da VPN do cliente da AWS e tentar se conectar novamente.

## O processo de conexão VPN é encerrado inesperadamente

Problema

Ao se conectar a um endpoint da VPN do Cliente, o cliente fecha inesperadamente.

Causa

O TAP-Windows não está instalado no computador. Esse software é necessário para executar o cliente.

Solução

Execute novamente o instalador do cliente fornecido pela AWS para instalar todas as dependências necessárias.

## Falha ao iniciar o aplicativo

Problema

No Windows 7, o cliente fornecido pela AWS não é iniciado quando você tenta abri-lo.

Causa

O .NET Framework 4.7.2 ou superior não está instalado no computador. Isso é necessário para executar o cliente.

Solução

Execute novamente o instalador do cliente fornecido pela AWS para instalar todas as dependências necessárias.

## O cliente não consegue criar um perfil

Problema

Você obtém o erro a seguir ao tentar criar um perfil usando o cliente fornecido pela AWS.

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

Causa

Se o endpoint da cliente VPN usar autenticação mútua, o arquivo de configuração (.ovpn) não conterá o certificado e a chave do cliente.

Solução

Certifique-se de que o administrador de VPN do Cliente adicione o certificado e a chave do cliente ao arquivo de configuração. Para obter mais informações, consulte Exportar configuração do cliente no Guia do administrador da AWS Client VPN.

## A falha do cliente ocorre em PCs Dell usando o Windows 10 ou 11

Problema

Em determinados PCs Dell (desktop e laptop) que estão executando o Windows 10 ou 11, uma falha pode ocorrer quando você estiver navegando em seu sistema de arquivos para importar um arquivo de configuração VPN. Se esse problema ocorrer, você verá mensagens como as seguintes nos logs do cliente AWS fornecido:

```
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()
```

Causa

O sistema Dell Backup and Recovery no Windows 10 e 11 pode causar conflitos com o cliente AWS fornecido, particularmente com as três DLLs a seguir:

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

Solução

Para evitar esse problema, primeiro certifique-se de que seu cliente esteja atualizado com a versão mais recente do cliente AWS fornecido. Acesse Download da VPN do Cliente AWS e, se houver uma versão mais nova disponível, atualize para a versão mais recente.

Além disso, siga um destes procedimentos:

- Se estiver utilizando o aplicativo Dell Backup and Recovery, verifique se ele está atualizado. Uma Publicação no fórum da Dell afirma que esse problema foi resolvido em versões mais recentes do aplicativo.
- Se você não estiver usando o aplicativo Dell Backup and Recovery, algumas ações ainda precisarão ser tomadas se você estiver enfrentando esse problema. Se você não quiser atualizar o aplicativo, como alternativa, você pode excluir ou renomear os arquivos DLL. No entanto, observe que isso impedirá que o aplicativo Dell Backup and Recovery funcione completamente.

### Excluir ou renomear os arquivos DLL

1. Vá para o Windows Explorer e navegue até o local onde o Dell Backup and Recovery está instalado. Normalmente, ele é instalado no local a seguir, mas talvez seja necessário pesquisar para encontrá-lo.

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

2. Exclua manualmente os seguintes arquivos DLL do diretório de instalação ou renomeie-os. Qualquer ação impedirá que elas sejam carregadas.

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

Você pode renomear os arquivos adicionando ".bak" ao final do nome do arquivo, por exemplo, DBROverlayIconBackuped.dll.bak.

# GUI do OpenVPN

As informações de solução de problemas a seguir foram testadas nas versões 11.10.0.0 e 11.11.0.0 do software OpenVPN GUI no Windows 10 Home (64 bits) e Windows Server 2016 (64 bits).

O arquivo de configuração é armazenado no seguinte local no computador:

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

Os logs de conexão são armazenados no seguinte local no computador:

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

# Cliente OpenVPN Connect

As informações de solução de problemas a seguir foram testadas nas versões 2.6.0.100 e 2.7.1.101 do software cliente OpenVPN Connect no Windows 10 Home (64 bits) e no Windows Server 2016 (64 bits).

O arquivo de configuração é armazenado no seguinte local no computador:

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

Os logs de conexão são armazenados no seguinte local no computador:

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

## Não é possível resolver o DNS

Problema

A conexão falha com o erro a seguir.

```
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.
```

Causa

O nome DNS não pode ser resolvido. O cliente deve ter precedido o nome DNS com uma string aleatória para impedir o armazenamento em cache DNS. No entanto, alguns clientes não fazem isso.

Solução

Consulte a solução para Não é possível resolver o nome DNS do endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

### Pseudônimo do PKI ausente

Problema

Há falha em uma conexão a um endpoint da VPN do Cliente que não usa autenticação mútua com o erro a seguir.

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

Causa

O software cliente OpenVPN Connect tem um problema conhecido em que tenta autenticar usando autenticação mútua. Se o arquivo de configuração não contiver uma chave e um certificado do cliente, haverá falha na autenticação.

Solução

Especifique uma chave e um certificado do cliente aleatórios no arquivo de configuração de VPN do Cliente e importe a nova configuração para o software cliente OpenVPN Connect. Como alternativa, use um cliente diferente, como o cliente OpenVPN GUI (v11.12.0.0) ou o cliente Viscosity (v.1.7.14).

# Solução de problemas macOS

As seções a seguir contêm informações sobre registro em log e problemas que você pode ter ao usar clientes macOS. Certifique-se de que esteja executando a versão mais recente desses clientes.

Tópicos



## AWScliente fornecido pela

O cliente fornecido pela AWS cria logs de eventos e os armazena no local a seguir no seu computador.

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

Os seguintes tipos de logs estão disponíveis:

- Logs de aplicativos: contêm informações sobre o aplicativo. Esses logs são prefixados com "aws_vpn_client_".
- Logs do OpenVPN: contêm informações sobre os processos do OpenVPN. Esses logs são prefixados com "ovpn_aws_vpn_client_".

O cliente fornecido pela AWS usa o daemon do cliente para executar operações raiz. Os logs do daemon são armazenados nos seguintes locais no seu computador:

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

O cliente fornecido pela AWS armazena os arquivos de configuração no local a seguir do seu computador.

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

Tópicos



# O cliente não consegue se conectar

Problema

O cliente fornecido pela AWS não pode se conectar ao endpoint da cliente VPN.

Causa

A causa desse problema pode ser uma das seguintes:

- Outro processo OpenVPN já está em execução no computador, o que impede que o cliente se conecte.
- Seu arquivo de configuração (.ovpn) é inválido.

Solução

Verifique se não há outras aplicações do OpenVPN em execução no computador. Se houver, pare ou feche esses processos e tente se conectar ao endpoint da cliente VPN novamente. Verifique se há erros nos logs do OpenVPN e peça ao administrador de VPN do Cliente para verificar as seguintes informações:

- Se o arquivo de configuração contém a chave e o certificado do cliente corretos. Para obter mais informações, consulte Exportar configuração do cliente no Guia do administrador da AWS Client VPN.
- Se a CRL ainda é válida. Para obter mais informações, consulte Clientes não conseguem se conectar a um endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

# O cliente está travado em um estado de reconexão

Problema

O cliente fornecido pela AWS está tentando se conectar ao endpoint da cliente VPN, mas está travado em um estado de reconexão.

Causa

A causa desse problema pode ser uma das seguintes:

- O computador não está conectado à Internet.
- O nome de host DNS não resolve para um endereço IP.
- Um processo OpenVPN está tentando se conectar ao endpoint indefinidamente.

Solução

Verifique se o computador está conectado à Internet. Peça ao administrador de VPN do Cliente para verificar se a diretiva `remote` no arquivo de configuração é resolvida para um endereço IP válido. Também é possível desconectar a sessão de VPN escolhendo Disconnect (Desconectar) na janela da VPN do cliente da AWS e tentar se conectar novamente.

## O cliente não consegue criar um perfil

Problema

Você obtém o erro a seguir ao tentar criar um perfil usando o cliente fornecido pela AWS.

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

Causa

Se o endpoint da cliente VPN usar autenticação mútua, o arquivo de configuração (.ovpn) não conterá o certificado e a chave do cliente.

Solução

Certifique-se de que o administrador de VPN do Cliente adicione o certificado e a chave do cliente ao arquivo de configuração. Para obter mais informações, consulte Exportar configuração do cliente no Guia do administrador da AWS Client VPN.

# Tunnelblick

As informações de solução de problemas a seguir foram testadas na versão 3.7.8 (compilação 5180) do software Tunnelblick no macOS High Sierra 10.13.6.

O arquivo de configuração para configurações privadas é armazenado no seguinte local no computador:

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

O arquivo de configuração para configurações compartilhadas é armazenado no seguinte local no computador:

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

Os logs de conexão são armazenados no seguinte local no computador:

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

Para aumentar o detalhamento do log, abra o aplicativo Tunnelblick, escolha Configurações e ajuste o valor para o Nível de log da VPN.

## Algoritmo de codificação "AES-256-GCM" não encontrado

Problema

Há falha na conexão e erro a seguir é retornado nos logs.

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

Causa

O aplicativo está usando uma versão do OpenVPN que não oferece suporte ao algoritmo de codificação AES-256-GCM.

Solução

Escolha uma versão compatível do OpenVPN fazendo o seguinte:

1. Abra o aplicativo Tunnelblick.
2. Escolha Configurações.
3. Em Versão do OpenVPN, escolha 2.4.6 – a versão do OpenSSL é v1.0.2q.

## A conexão para de responder e é redefinida

Problema

Há falha na conexão e erro a seguir é retornado nos logs.

```
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
```

Causa

O certificado do cliente foi revogado. A conexão para de responder depois de tentar autenticar e, por fim, é redefinida no lado do servidor.

Solução

Solicite um novo arquivo de configuração ao administrador de VPN do Cliente.

## Uso estendido de chave (EKU)

Problema

Há falha na conexão e erro a seguir é retornado nos logs.

```
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,,,,,
```

Causa

A autenticação do servidor teve êxito. No entanto, há falha na autenticação de cliente porque o certificado do cliente tem o campo de uso estendido de chave (EKU) habilitado para autenticação do servidor.

Solução

Certifique-se de que esteja usando o certificado e a chave do cliente corretos. Se necessário, verifique com o administrador de VPN do Cliente. Esse erro poderá ocorrer se você estiver usando o certificado do servidor e não o certificado do cliente para se conectar ao endpoint da VPN do Cliente.

## Certificado expirado

Problema

A autenticação do servidor tem êxito, mas há falha na autenticação do cliente com o erro a seguir.

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

Causa

A validade do certificado do cliente expirou.

Solução

Solicite um novo certificado do cliente ao administrador de VPN do Cliente.

# OpenVPN

As informações de solução de problemas a seguir foram testadas na versão 2.7.1.100 do software cliente OpenVPN Connect no macOS High Sierra 10.13.6.

O arquivo de configuração é armazenado no seguinte local no computador:

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

Os logs de conexão são armazenados no seguinte local no computador:

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

## Não é possível resolver o DNS

Problema

A conexão falha com o erro a seguir.

```
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
```

Causa

O OpenVPN Connect não consegue resolver o nome DNS de VPN do Cliente.

Solução

Consulte a solução para Não é possível resolver o nome DNS do endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

# Solução de problemas Linux

As seções a seguir contêm informações sobre registro em log e sobre problemas que você pode ter ao usar clientes baseados em Linux. Certifique-se de que esteja executando a versão mais recente desses clientes.

Tópicos



## AWScliente fornecido pela

O cliente fornecido pela AWS armazena arquivos de log e arquivos de configuração no seguinte local em seu sistema:

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

O processo do daemon do cliente fornecido pela AWS armazena arquivos de log no seguinte local em seu sistema:

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

Problema

Em algumas circunstâncias, depois que uma conexão VPN é estabelecida, as consultas DNS ainda irão para o servidor de nomes do sistema padrão, em vez dos servidores de nomes que estão configurados para o endpoint da cliente VPN.

Causa

A VPN do cliente da AWS interage com o systemd-resolve, um serviço disponível em sistemas Linux, que serve como uma peça central do gerenciamento DNS. Ele é usado para configurar servidores DNS que são enviados do endpoint da cliente VPN. O problema ocorre porque systemd-resolve não define a prioridade mais alta para servidores DNS que são fornecidos pelo endpoint da cliente VPN. Em vez disso, anexa os servidores à lista existente de servidores DNS configurados no sistema local. Como resultado, os servidores DNS originais ainda podem ter a prioridade mais alta e, portanto, podem ser usados para resolver consultas de DNS.

Solução

1. Adicione a seguinte diretiva na configuração do OpenVPN para garantir que todas as consultas de DNS sejam enviadas para o túnel da VPN.

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

2. Use o resolvedor de stub fornecido por systemd-resolve. Para fazer isso, symlink `/etc/resolv.conf` para `/run/systemd/resolve/stub-resolv.conf` executando o seguinte comando no sistema.

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

3. (Opcional) Se não quiser systemd-resolve para consultas de DNS de proxy e, em vez disso, gostaria que as consultas fossem enviadas para os servidores de nomes DNS reais diretamente, crie um symlink `/etc/resolv.conf` para `/run/systemd/resolve/resolv.conf`.

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

   Você pode querer fazer esse procedimento para ignorar o rsystemd-resolved, por exemplo, para cache de resposta DNS, configuração de DNS por interface, imposição de DNSsec e assim por diante. Esta opção é especialmente útil quando você precisa substituir um registro DNS público por um registro privado quando conectado à VPN. Por exemplo, você pode ter um resolvedor DNS privado em sua VPC privada com um registro para www.example.com, que é resolvido para um IP privado. Esta opção pode ser usada para substituir o registro público de www.example.com, que resolve para um IP público.

# OpenVPN (linha de comando)

Problema

A conexão não funciona corretamente porque a resolução DNS não está funcionando.

Causa

O servidor DNS não está configurado no endpoint da VPN do Cliente ou não está sendo honrado pelo software cliente.

Solução

Use as etapas a seguir para verificar se o servidor DNS está configurado e funcionando corretamente.

1. Certifique-se de que uma entrada de servidor DNS esteja presente nos logs. No exemplo a seguir, o servidor DNS `192.168.0.2` (configurado no endpoint da VPN do Cliente) é retornado na última linha.

   ```
   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
   ```

   Se não houver nenhum servidor DNS especificado, peça ao administrador de VPN do Cliente para modificar o endpoint da VPN do Cliente e verifique se um servidor DNS (por exemplo, o servidor DNS da VPC) foi especificado para o endpoint da VPN do Cliente. Para obter mais informações, consulte Endpoints da cliente VPN no Guia do administrador da AWS Client VPN.
2. Certifique-se de que o pacote `resolvconf` esteja instalado executando o comando a seguir.

   ```
   sudo apt list resolvconf
   ```

   A saída deve retornar o seguinte:

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

   Se não estiver instalado, instale-o usando o comando a seguir.

```
sudo apt install resolvconf
```

3. Abra o arquivo de configuração de VPN do Cliente (o arquivo .ovpn) em um editor de texto e adicione as linhas a seguir.

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

Confira os logs para verificar se o script `resolvconf` foi chamado. Os logs devem conter uma linha semelhante à seguinte:

```
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
```

## OpenVPN pelo gerenciador de rede (GUI)

Problema

Ao usar o cliente OpenVPN do Gerenciador de rede, há falha na conexão com o erro a seguir.

```
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
```

Causa

O sinalizador `remote-random-hostname` não é honrado e o cliente não consegue se conectar usando o pacote `network-manager-gnome`.

Solução

Consulte a solução para Não é possível resolver o nome DNS do endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

# Problemas comuns

Veja a seguir os problemas comuns que podem ocorrer ao usar um cliente para se conectar a um endpoint da cliente VPN.

## Falha na negociação de chave TLS

Problema

Há falha na negociação de TLS com o erro a seguir.

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

```
TLS Error: TLS handshake failed
```

Causa

A causa desse problema pode ser uma das seguintes:

- As regras de firewall estão bloqueando o tráfego UDP ou TCP.
- Você está usando a chave e o certificado do cliente incorretos no arquivo de configuração (.ovpn).
- A lista de revogação de certificados de cliente (CRL) expirou.

Solução

Verifique se as regras de firewall no computador não estão bloqueando o tráfego TCP ou UDP de entrada ou saída nas portas 443 ou 1194. Peça ao administrador de VPN do Cliente para verificar as seguintes informações:

- Se as regras de firewall para o endpoint da cliente VPN não bloqueiam o tráfego TCP ou UDP nas portas 443 ou 1194.
- Se o arquivo de configuração contém a chave e o certificado do cliente corretos. Para obter mais informações, consulte Exportar configuração do cliente no Guia do administrador da AWS Client VPN.
- Se a CRL ainda é válida. Para obter mais informações, consulte Clientes não conseguem se conectar a um endpoint da cliente VPN no Guia do administrador da AWS Client VPN.

# Histórico do documento

A tabela a seguir descreve as atualizações do Guia do usuário da VPN do cliente da AWS.

| atualização das alterações do histórico | update-history-description | update-history-date |
| --- | --- | --- |
| Lançamento do cliente fornecido pela AWS para macOS (3.1.0) | Consulte as notas de release completas para obter detalhes. | 23 de maio de 2022 |
| Lançamento do cliente fornecido pela AWS para Windows (3.1.0) | Consulte as notas de release completas para obter detalhes. | 23 de maio de 2022 |
| Lançamento do cliente fornecido pela AWS para Ubuntu (3.1.0) | Consulte as notas de release completas para obter detalhes. | 23 de maio de 2022 |
| Lançamento do cliente fornecido pela AWS para macOS (3.0.0) | Consulte as notas de release completas para obter detalhes. | 3 de março de 2022 |
| Lançamento do cliente fornecido pela AWS para Windows (3.0.0) | Consulte as notas de release completas para obter detalhes. | 03 de março de 2022 |
| Lançamento do cliente fornecido pela AWS para Ubuntu (3.0.0) | Consulte as notas de release completas para obter detalhes. | 3 de março de 2022 |
| Lançamento do cliente fornecido pela AWS para macOS (2.0.0) | Consulte as notas de release completas para obter detalhes. | 20 de janeiro de 2022 |
| Lançamento do cliente fornecido pela AWS para Windows (2.0.0) | Consulte as notas de release completas para obter detalhes. | 20 de janeiro de 2022 |
| Lançamento do cliente fornecido pela AWS para Ubuntu (2.0.0) | Consulte as notas de release completas para obter detalhes. | 20 de janeiro de 2022 |
| Lançamento do cliente fornecido pela AWS para macOS (1.4.0) | Consulte as notas de release completas para obter detalhes. | 9 de novembro de 2021 |
| Lançamento do cliente fornecido pela AWS para Windows (1.3.7) | Consulte as notas de release completas para obter detalhes. | 8 de novembro de 2021 |
| Lançamento do cliente fornecido pela AWS para Ubuntu (1.0.3) | Consulte as notas de release completas para obter detalhes. | 8 de novembro de 2021 |
| Lançamento do cliente fornecido pela AWS para Ubuntu (1.0.2) | Consulte as notas de release completas para obter detalhes. | 28 de setembro de 2021 |
| Lançamento do cliente fornecido pela AWS para Windows (1.3.6) e macOS (1.3.5) | Consulte as notas de release completas para obter detalhes. | 20 de setembro de 2021 |
| Lançamento do cliente fornecido pela AWS para Ubuntu 18.04 LTS e Ubuntu 20.04 LTS | Você pode usar o cliente fornecido pela AWS no Ubuntu 18.04 LTS e Ubuntu 20.04 LTS. | 11 de junho de 2021 |
| Suporte para o OpenVPN usando um certificado da Windows Certificate System Store | Você pode usar o OpenVPN usando um certificado da Windows Certificate System Store. | 25 de fevereiro de 2021 |

| | | |
|---|---|---|
| Portal de autoatendimento | Você pode acessar um portal de autoatendimento para obter o cliente fornecido pela AWS mais recente e o arquivo de configuração. | 29 de outubro de 2020 |
| Cliente fornecido pela AWS | É possível usar o cliente fornecido pela AWS para se conectar a um endpoint da cliente VPN. | 4 de fevereiro de 2020 |
| Versão inicial (p. 39) | Esta versão apresenta a VPM do cliente da AWS. | 18 de dezembro de 2018 |