



Manual do usuário

AWS Cliente VPN



AWS Cliente VPN: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é AWS clienteVPN?	1
VPNComponentes do cliente	1
Recursos adicionais para configurar o Client VPN	1
Comece com o Client VPN	2
Pré-requisitos para usar o Client VPN	2
Etapa 1: obter um aplicativo VPN cliente	2
Etapa 2: Obter o arquivo de configuração do VPN endpoint do cliente	3
Etapa 3: Conecte-se ao VPN	3
Cliente de download VPN	4
Conecte-se usando um cliente AWS fornecido	6
Windows	7
Requisitos	8
Connect usando o cliente	8
Notas de release	9
macOS	18
Requisitos	18
Connect usando o cliente	19
Notas de release	19
Linux	29
Requisitos para conexão VPN com o Cliente com um cliente AWS fornecido para Linux	29
Instale o cliente	29
Connect usando o cliente	31
Notas de release	31
Connect usando um VPN cliente Open	38
Windows	39
Estabeleça uma VPN conexão usando um certificado no Windows	39
VPNConexões de clientes no Android e iOS	41
macOS	42
Estabeleça uma VPN conexão no macOS	42
Linux	43
Estabeleça uma VPN conexão no Linux	43
Solução de problemas	45
Solução de problemas VPN em terminais de clientes para administradores	45
Envie registros de diagnóstico para AWS Support o cliente AWS fornecido	45

Enviar registros de diagnóstico	19
Solução de problemas do Windows	47
AWS registros de eventos do cliente fornecidos	47
O cliente não consegue se conectar	48
O cliente não pode se conectar com a mensagem de TAP log “sem adaptadores do Windows”	48
O cliente está travado em um estado de reconexão	49
VPN o processo de conexão é encerrado inesperadamente	49
Falha ao iniciar o aplicativo	50
O cliente não consegue criar um perfil	50
VPN desconecta com uma mensagem pop-up	51
A falha do cliente ocorre na Dell PCs usando o Windows 10 ou 11	51
Aberto VPN GUI	53
Cliente Open VPN Connect	54
Não foi possível resolver DNS	54
PKI apelido ausente	54
Solução de problemas macOS	55
AWS registros de eventos do cliente fornecidos	55
O cliente não consegue se conectar	56
O cliente está travado em um estado de reconexão	57
O cliente não consegue criar um perfil	57
A ferramenta auxiliar é um erro obrigatório	58
Tunnelblick	58
Algoritmo de cifra 'AES-256-GCM' não encontrado	59
A conexão para de responder e é redefinida	59
Uso estendido da chave (EKU)	60
Certificado expirado	61
Aberto VPN	61
Não é possível resolver DNS	61
Solução de problemas Linux	62
AWS registros de eventos do cliente fornecidos	47
DNS as consultas vão para um servidor de nomes padrão	63
Abrir VPN (linha de comando)	64
Abrir VPN por meio do Network Manager (GUI)	65
Problemas comuns	66
TLS falhou a negociação chave	66

Histórico do documento	68
.....	Ixxiv

O que é AWS clienteVPN?

AWS VPNO cliente é um VPN serviço gerenciado baseado em cliente que permite acessar com segurança AWS recursos e recursos em sua rede local.

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

VPNComponentes do cliente

A seguir estão os principais componentes para usar o AWS ClientVPN.

- VPNEndpoint do cliente — Seu VPN administrador do cliente cria e configura um VPN endpoint do cliente em. AWS Seu administrador controla quais redes e recursos você pode acessar ao estabelecer uma VPN conexão.
- VPNaplicativo cliente — O aplicativo de software que você usa para se conectar ao VPN endpoint do cliente e estabelecer uma VPN conexão segura.
- Arquivo de configuração do VPN endpoint do cliente — Um arquivo de configuração fornecido a você pelo VPN administrador do cliente. O arquivo inclui informações sobre o VPN endpoint do cliente e os certificados necessários para estabelecer uma VPN conexão. Você carrega esse arquivo no aplicativo VPN cliente escolhido.

Recursos adicionais para configurar o Client VPN

Se você for VPN administrador do cliente, consulte o [Guia do AWS Client VPN administrador](#) para obter mais informações sobre como criar e configurar um VPN endpoint do cliente.

Comece com AWS Client VPN

Antes de estabelecer uma VPN sessão, o VPN administrador do cliente deve criar e configurar um VPN endpoint do cliente. Seu administrador controla quais redes e recursos você pode acessar ao estabelecer uma VPN sessão. Em seguida, você usa um aplicativo VPN cliente para se conectar a um VPN endpoint do cliente e estabelecer uma VPN conexão segura.

Se você é um administrador que precisa criar um VPN endpoint de cliente, consulte o [Guia do AWS Client VPN administrador](#).

Tópicos

- [Pré-requisitos para usar o Client VPN](#)
- [Etapa 1: obter um aplicativo VPN cliente](#)
- [Etapa 2: Obter o arquivo de configuração do VPN endpoint do cliente](#)
- [Etapa 3: Conecte-se ao VPN](#)
- [Faça o download AWS Client VPN do portal de autoatendimento](#)

Pré-requisitos para usar o Client VPN

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

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

Etapa 1: obter um aplicativo VPN cliente

Você pode se conectar a um VPN endpoint do cliente e estabelecer uma VPN conexão usando o cliente AWS fornecido ou outro aplicativo cliente VPN baseado em Open.

O cliente AWS fornecido é compatível com Windows, macOS, Ubuntu 18.04 e Ubuntu 20.04LTS.
LTS

Você pode baixar o VPN aplicativo cliente por meio de um dos dois métodos, dependendo se o administrador criou o arquivo de configuração do endpoint para o aplicativo:

- Se o administrador não configurou o arquivo de configuração do endpoint, baixe e instale o cliente em [VPNDownload do AWS cliente](#). Depois de baixar e instalar o aplicativo, prossiga [the section called “Etapa 2: Obter o arquivo de configuração do VPN endpoint do cliente”](#) para obter o arquivo de configuração do endpoint com seu administrador.
- Se o administrador já tiver pré-configurado o arquivo de configuração do endpoint, você poderá baixar o VPN aplicativo Cliente, junto com o arquivo de configuração, do portal de autoatendimento. Para obter as etapas para baixar o cliente e o arquivo de configuração do portal de autoatendimento, consulte [the section called “Cliente de download VPN”](#). Depois de baixar e instalar o aplicativo e o arquivo, acesse [the section called “Etapa 3: Conecte-se ao VPN”](#).

Como alternativa, baixe e instale um aplicativo VPN cliente Open no dispositivo a partir do qual você pretende estabelecer a VPN conexão.

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

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

Como alternativa, se o VPN administrador do cliente tiver configurado um portal de autoatendimento para o VPN endpoint do cliente, você mesmo poderá baixar a versão mais recente do cliente AWS fornecido e a versão mais recente do arquivo de configuração do VPN endpoint do cliente. Para obter mais informações, consulte [Faça o download AWS Client VPN do portal de autoatendimento](#).

Etapa 3: Conecte-se ao VPN

Importe o arquivo de configuração do VPN endpoint do cliente para o cliente AWS fornecido ou para o aplicativo Open VPN Client e conecte-se aoVPN. Para ver as etapas de conexão com umVPN, incluindo a importação do arquivo de configuração do endpoint, consulte os tópicos a seguir:

- [Conecte-se a um AWS Client VPN endpoint usando um cliente AWS fornecido](#)
- [Conecte-se a um AWS Client VPN endpoint usando um cliente Open VPN](#)

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

Para VPN endpoints do cliente que usam autenticação federada SAML baseada (login único), o cliente AWS fornecido abre uma janela do navegador em seu computador. Você será solicitado a inserir suas credenciais corporativas antes de se conectar ao endpoint do ClienteVPN.

Faça o download AWS Client VPN do portal de autoatendimento

O portal de autoatendimento é uma página da Web que permite baixar a versão mais recente do cliente AWS fornecido e a versão mais recente do arquivo de configuração do VPN endpoint do cliente. Se o administrador do VPN endpoint do cliente tiver pré-configurado o arquivo de configuração para o cliente VPN cliente, você poderá baixar e instalar esse VPN aplicativo cliente junto com o arquivo de configuração, a partir deste portal.

Note

Se você for administrador e quiser configurar o portal de autoatendimento, consulte [VPNEndpoints do cliente no Guia](#) do AWS Client VPN Administrador.

Antes de começar, você deve ter o ID do VPN endpoint do cliente. O administrador do VPN endpoint do cliente pode fornecer a ID ou fornecer um portal de autoatendimento URL que inclua a 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 VPN endpoint do cliente, por exemplo, cvpn-endpoint-0123456abcd123456. Escolha Próximo.
3. Digite seu nome de usuário e senha e escolha Sign In (Fazer login). Esse é o mesmo nome de usuário e senha que você usa para se conectar ao VPN endpoint do cliente.
4. No portal de autoatendimento, você pode fazer o seguinte:

- Baixe a versão mais recente do arquivo de configuração do cliente para o VPN endpoint do cliente.
- Baixe a versão mais recente do cliente AWS fornecido para sua plataforma.

Conecte-se a um AWS Client VPN endpoint usando um cliente AWS fornecido

Você pode se conectar a um VPN endpoint do cliente usando o cliente AWS fornecido. O cliente AWS fornecido é compatível com Windows, macOS, Ubuntu 18.04 e Ubuntu 20.04LTS. LTS

Clientes

- [AWS Client VPN para Windows](#)
- [AWS Client VPN para macOS](#)
- [AWS Client VPN para Linux](#)

VPN Diretivas abertas

O cliente AWS fornecido oferece suporte às seguintes VPN diretivas abertas. Para obter mais informações sobre essas diretivas, consulte a documentação no [VPNsite da Open](#).

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

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

AWS Client VPN para Windows

Essas seções descrevem como estabelecer uma VPN conexão usando o cliente AWS fornecido para Windows. Você pode baixar e instalar o cliente em [VPNDownload AWS do cliente](#). O cliente AWS fornecido não oferece suporte a atualizações automáticas.

Requisitos

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

- Windows 10 ou Windows 11 (sistema operacional de 64 bits, processador x64)
- .NETFramework 4.7.2 ou superior

O cliente reserva a TCP porta 8096 no seu computador. Para VPN endpoints do cliente que usam autenticação federada SAML baseada (login único), o cliente reserva a porta 35001. TCP

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Tópicos

- [AWS Client VPN Conecte-se a um cliente AWS fornecido para Windows](#)
- [AWS Client VPN para notas de versão do Windows](#)

AWS Client VPN Conecte-se a um cliente AWS fornecido para Windows

Antes de começar, certifique-se de que leu os [Requisitos](#). O cliente AWS fornecido também é chamado de AWS VPN Cliente nas etapas a seguir.

Para se conectar usando o cliente AWS fornecido 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. Em Arquivo de VPN configuração, navegue até o arquivo de configuração que você recebeu do VPN administrador do cliente e selecione Adicionar perfil.
6. Na janela AWS VPN Client (Cliente VPN), verifique se seu perfil está selecionado e escolha Connect (Conectar). Se o VPN endpoint do cliente tiver sido configurado para usar autenticação baseada em credenciais, 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 Disconnect (Desconectar). Como alternativa, escolha o ícone do cliente na barra de tarefas do Windows e escolha (Desconectar-se).

AWS Client VPN para notas de versão do Windows

A tabela a seguir contém as notas de versão e os links de download das versões atual e anterior do AWS Client VPN para Windows.

Note

Continuamos fornecendo correções de usabilidade e segurança a cada lançamento. É altamente recomendável que você use a versão mais recente para todas as plataformas. As versões anteriores podem ser afetadas por problemas de usabilidade e/ou segurança. Consulte as notas de release completas para obter detalhes.

Version (Versão)	Alterações	Data	Link para download e SHA256
4.0.0	Pequenos aprimoramentos.	25 de setembro de 2024	Baixe a versão 4.0.0 sha256:65 32f911385 ec8fac149 4d0847c8f 90a999b3b d7380844e 2ea4318e9 db4a2ebc
3.14.2	Foi adicionado suporte para a VPN bandeira mssfix Open.	04 de setembro de 2024	Baixe a versão 3.14.2 sha256: c171639d7 e07e5fd48

Version (Versão)	Alterações	Data	Link para download e SHA256
			998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Pequenas correções de bugs e melhorias .	22 de agosto de 2024	Baixe a versão 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	<ul style="list-style-type: none"> Foi adicionado suporte para a VPN bandeira tap-sleep Open. As SSL bibliotecas Open VPN e Open foram atualizadas. 	12 de agosto de 2024	Baixe a versão 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96354516

Version (Versão)	Alterações	Data	Link para download e SHA256
3.13.0	As SSL bibliotecas Open VPN e Open foram atualizadas.	29 de julho de 2024	Baixe a versão 3.13.0 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12.1	Problema corrigido que impede que a versão 3.12.0 do cliente Windows estabeleça VPN conexão para alguns usuários.	18 de julho de 2024	Baixe a versão 3.12.1 sha256:5e d34aee6c0 3aa281e62 5acdbed27 2896c6704 6364a9e58 46ca697e0 5dbfec08
3.12.0	<ul style="list-style-type: none">• Reconecte-se automaticamente quando os intervalos da rede local mudarem.• Removeu o foco automático do aplicativo quando conectado aos SAML endpoints.	21 de maio de 2024	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
3.11.2	Resolveu um problema SAML de autenticação com navegadores baseados em Chromium desde a versão 123.	11 de abril de 2024	Baixe a versão 3.11.2 sha256:8b a258dd15b ea3e861ad ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc
3.11.1	<ul style="list-style-type: none"> Corrigida uma ação de estouro de buffer que poderia potencialmente permitir que um ator local executasse comandos arbitrários com permissões elevadas. Procedimento de segurança aprimorado. 	16 de fevereiro de 2024	Baixe a versão 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	<ul style="list-style-type: none"> Corrigido um problema de conectividade causado pelo WindowsVMs. Problemas de conectividade corrigidos em algumas LAN configurações. Acessibilidade melhorada. 	6 de dezembro de 2023	Baixar a versão 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Version (Versão)	Alterações	Data	Link para download e SHA256
3.10.0	<ul style="list-style-type: none"> Corrigido um problema de conectividade quando NAT64 está ativado na rede do cliente. Corrigido um problema de conectividade quando os adaptadores de rede Hyper-V são instalados na máquina cliente. Pequenas correções de bugs e melhorias. 	24 de agosto de 2023	Baixar a versão 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	Procedimento de segurança aprimorado.	3 de agosto de 2023	Baixar a versão 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	Procedimento de segurança aprimorado.	15 de julho de 2023	Não é mais compatível
3.7.0	Reversão das alterações da versão 3.6.0.	15 de julho de 2023	Não é mais compatível
3.6.0	Procedimento de segurança aprimorado.	14 de julho de 2023	Não é mais compatível
3.5.0	Pequenas correções de bugs e melhorias	3 de abril de 2023	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
3.4.0	Reversão das alterações da versão 3.3.0.	28 de março de 2023	Não é mais compatível
3.3.0	Pequenas correções de bugs e melhorias	17 de março de 2023	Não é mais compatível
3.2.0	<ul style="list-style-type: none">Foi adicionado suporte para o sinalizador aberto “verify-x509-name”. VPNDetectado automaticamente quando versões atualizadas do cliente são disponibilizadas.Foi adicionada a capacidade de instalar automaticamente novas versões do cliente quando disponíveis.	23 de janeiro de 2023	Não é mais compatível
3.1.0	Procedimento de segurança aprimorado.	23 de maio de 2022	Não é mais compatível
3.0.0	<ul style="list-style-type: none">Adicionado suporte ao Windows 11.A nomenclatura de drivers TAP do Windows foi corrigida, fazendo com que outros nomes de drivers fossem afetados.Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada.Corrigida a exibição do texto do banner para texto mais longo.Aprimorada a postura de segurança.	03 de março de 2022	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
2.0.0	<ul style="list-style-type: none"> Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida. Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco Pequenas correções de bugs e melhorias. 	20 de janeiro de 2022	Não é mais compatível
1.3.7	<ul style="list-style-type: none"> Tentativa de conexão de autenticação federada corrigida em alguns casos. Pequenas correções de bugs e melhorias. 	8 de novembro de 2021	Não é mais compatível
1.3.6	<ul style="list-style-type: none"> Foi adicionado suporte para Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, . server-poll-timeout 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	<ul style="list-style-type: none"> Foi adicionado suporte para Open VPN flag: dhcp-option. Pequenas correções de bugs e melhorias. 	4 de agosto de 2021	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
1.3.3	<ul style="list-style-type: none"> Foi adicionado suporte para VPN bandeiras abertas: inativo, filtro de tração, rota. Corrigido um problema que causava uma falha na aplicação na desconexão ou saída. Corrigido um problema com nomes de usuário do Active Directory com barra invertida. Corrigido o travamento da aplicação ao manipular a lista de perfis fora da aplicação. Pequenas correções de bugs e melhorias. 	1.º de julho de 2021	Não é mais compatível
1.3.2	<ul style="list-style-type: none"> Adicione a prevenção de IPv6 vazamentos, quando estiver configurada. 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	<ul style="list-style-type: none"> Adicionado suporte para vários certificados de cliente com o mesmo assunto. Os certificados expirados serão ignorados. Retenção de log local corrigida para reduzir o uso do disco. Foi adicionado suporte para a diretiva aberta 'route-ipv6'. VPN Pequenas correções de bugs e melhorias. 	5 de abril de 2021	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
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	<ul style="list-style-type: none"> Foi adicionado suporte para a diretiva Cryptoapicert Open. VPN Rotas obsoletas fixas entre conexões. 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	<ul style="list-style-type: none"> Foi adicionado suporte para comentários na VPN configuração aberta. Foi adicionada uma mensagem de erro para erros de TLS handshake. 	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	<ul style="list-style-type: none"> Foi adicionado suporte para autenticação SAMLfederada baseada em 2.0. Suporte obsoleto para a plataforma Windows 7. 	19 de maio de 2020	Não é mais compatível
1.1.1	Pequenas correções de bugs e melhorias .	21 de abril de 2020	Não é mais compatível

Version (Versão)	Alterações	Data	Link para download e SHA256
1.1.0	<ul style="list-style-type: none">Foi adicionado suporte à funcionalidade Open VPN static challenge echo para ocultar ou mostrar o texto exibido na interface do usuário.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

Essas seções descrevem como estabelecer uma VPN conexão usando o cliente AWS fornecido para macOS. Você pode baixar e instalar o cliente em [VPNDownload AWS do cliente](#). O cliente AWS fornecido não oferece suporte a atualizações automáticas.

Requisitos

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

- macOS Monterey (12.0), Ventura (13.0) ou Sonoma (14.0).
- Compatível com o processador x86_64.
- O cliente reserva a TCP porta 8096 no seu computador.
- Para VPN endpoints do cliente que usam autenticação federada SAML baseada (login único), o cliente reserva a porta 35001. TCP

Note

Se você estiver usando Mac com um processador de silício Apple, precisará instalar o [Rosetta 2](#) para executar o software cliente. Para obter mais detalhes, consulte [Sobre o ambiente de tradução Rosetta](#) no site da Apple.

Tópicos

- [Conecte-se AWS Client VPN com um cliente AWS fornecido para macOS](#)
- [AWS Client VPN para notas de versão do macOS](#)

Conecte-se AWS Client VPN com um cliente AWS fornecido para macOS

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Além disso, leia os [requisitos](#). O cliente AWS fornecido também é chamado de AWS VPN Cliente nas etapas a seguir.

Para se conectar usando o cliente AWS fornecido 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. Em Arquivo de VPN configuração, navegue até o arquivo de configuração que você recebeu do VPN administrador 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 VPN endpoint do cliente tiver sido configurado para usar autenticação baseada em credenciais, 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 Disconnect (Desconectar). Como alternativa, escolha o ícone do cliente na barra de menu e escolha Desconectar < your-profile-name >.

AWS Client VPN para notas de versão do macOS

A tabela a seguir contém as notas de lançamento e os links de download das versões atual e anterior do AWS Client VPN para macOS.

Note

Continuamos fornecendo correções de usabilidade e segurança a cada lançamento. É altamente recomendável que você use a versão mais recente para todas as plataformas. As versões anteriores podem ser afetadas por problemas de usabilidade e/ou segurança. Consulte as notas de release completas para obter detalhes.

Version (Versão)	Alterações	Data	Link para fazer download
4.0.0	Pequenos aprimoramentos.	25 de setembro de 2024	Baixe a versão 4.0.0 sha256: ad574475a 80b614499 c97ae7561 2ef1ff905 bb4aa1b5f 7109420e8 0bf95aefcbd
3.12.1	Foi adicionado suporte para a VPN bandeira <code>mssfix</code> Open.	04 de setembro de 2024	Baixe a versão 3.12.1 sha256: a5c31d3e0 e8bf89376 82805c9ff f76ca9205 875e009e9 49ad1b053 2f449cee47
3.12.0	<ul style="list-style-type: none"> Foi adicionado suporte para a VPN bandeira <code>tap-sleep</code> Open. 	12 de agosto de 2024	Baixar a versão 3.12.0

Version (Versão)	Alterações	Data	Link para fazer download
	<ul style="list-style-type: none"> As SSL bibliotecas Open VPN e Open foram atualizadas. 		sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13
3.11.0	<ul style="list-style-type: none"> As SSL bibliotecas Open VPN e Open foram atualizadas. 	29 de julho de 2024	Baixar a versão 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062 21b8caea8 1732848f
3.10.0	<ul style="list-style-type: none"> Reconecte-se automaticamente quando os intervalos da rede local mudarem. Corrigido um problema de DNS restauração durante a troca de rede. Removeu o foco automático do aplicativo quando conectado aos SAML endpoints. 	21 de maio de 2024	Baixar a versão 3.10.0 sha256:28 bf26fa134 b01ff12703cf59ffa 4adba7c44 ceb793dce 4addd4404 e84287dd

Version (Versão)	Alterações	Data	Link para fazer download
3.9.2	<ul style="list-style-type: none"> • Resolveu um problema SAML de autenticação com navegadores baseados em Chromium desde a versão 123. • Foi adicionado suporte para macOS Sonoma. Suporte obsoleto para macOS Big Sur. • Procedimento de segurança aprimorado. 	11 de abril de 2024	Baixe a versão 3.9.2 sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480
3.9.1	<ul style="list-style-type: none"> • Corrigida uma ação de estouro de buffer que poderia potencialmente permitir que um ator local executasse comandos arbitrários com permissões elevadas. • Barra de progresso do download da atualização do aplicativo fixa. • Procedimento de segurança aprimorado. 	16 de fevereiro de 2024	Baixe a versão 3.9.1 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e899e971
3.9.0	<ul style="list-style-type: none"> • Problemas de conectividade corrigidos em algumas LAN configurações. • Acessibilidade melhorada. 	6 de dezembro de 2023	Baixar a versão 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8

Version (Versão)	Alterações	Data	Link para fazer download
3.8.0	<ul style="list-style-type: none"> Corrigido um problema de conectividade quando NAT64 está ativado na rede do cliente. Pequenas correções de bugs e melhorias. 	24 de agosto de 2023	Baixar a versão 3.8.0 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	<ul style="list-style-type: none"> Procedimento de segurança aprimorado. 	3 de agosto de 2023	Baixar a versão 3.7.0 sha256: 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a
3.6.0	<ul style="list-style-type: none"> Procedimento de segurança aprimorado. 	15 de julho de 2023	Não é mais compatível
3.5.0	<ul style="list-style-type: none"> Reversão das alterações da versão 3.4.0. 	15 de julho de 2023	Não é mais compatível
3.4.0	<ul style="list-style-type: none"> Procedimento de segurança aprimorado. 	14 de julho de 2023	Não é mais compatível

Version (Versão)	Alterações	Data	Link para fazer download
3.3.0	<ul style="list-style-type: none"> • Adição de suporte para macOS Ventura (13.0). • Pequenas correções de bugs e melhorias. 	27 de abril de 2023	Não é mais compatível
3.2.0	<ul style="list-style-type: none"> • Foi adicionado suporte para o sinalizador aberto “verify-x509-name”. VPN • Detectado automaticamente quando versões atualizadas do cliente são disponibilizadas. • Foi adicionada a capacidade de instalar automaticamente novas versões do cliente quando disponíveis. 	23 de janeiro de 2023	Não é mais compatível
3.1.0	<ul style="list-style-type: none"> • Suporte adicionado para macOS Monterey. • Problema corrigido para detecção de tipo de unidade. • Procedimento de segurança aprimorado. 	23 de maio de 2022	Não é mais compatível
3.0.0	<ul style="list-style-type: none"> • Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada. • Corrigida a exibição do texto do banner para texto mais longo. • Aprimorada a postura de segurança. 	03 de março de 2022	Não é mais compatível.

Version (Versão)	Alterações	Data	Link para fazer download
2.0.0	<ul style="list-style-type: none"> Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida. Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco Pequenas correções de bugs e melhorias. 	20 de janeiro de 2022	Não é mais compatível.
1.4.0	<ul style="list-style-type: none"> Foi adicionado monitoramento DNS do servidor durante a conexão. As configurações serão redefinidas se não corresponderem às VPN configurações. Tentativa de conexão de autenticação federada corrigida em alguns casos. Pequenas correções de bugs e melhorias. 	9 de novembro de 2021	Não é mais compatível.
1.3.5	<ul style="list-style-type: none"> Foi adicionado suporte para Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout Pequenas correções de bugs e melhorias. 	20 de setembro de 2021	Não é mais compatível.
1.3.4	<ul style="list-style-type: none"> Foi adicionado suporte para Open VPN flag: dhcp-option. Pequenas correções de bugs e melhorias. 	4 de agosto de 2021	Não é mais compatível.

Version (Versão)	Alterações	Data	Link para fazer download
1.3.3	<ul style="list-style-type: none">• Foi adicionado suporte para VPN bandeiras abertas: inativo, filtro de tração, rota.• Corrigido um problema com nomes de arquivos de configuração com espaços ou Unicode.• Corrigido um problema que causava uma falha na aplicação na desconexão ou saída.• Corrigido um problema com nomes de usuário do Active Directory com barra invertida.• Corrigido o travamento da aplicação ao manipular a lista de perfis fora da aplicação.• Pequenas correções de bugs e melhorias.	1.º de julho de 2021	Não é mais compatível.
1.3.2	<ul style="list-style-type: none">• Adicione a prevenção de IPv6 vazamentos, quando estiver configurada.• Falha em potencial corrigida quando a opção Show Details (Mostrar detalhes) em Connection (Conexão) foi usada.• Adicione rotação de log daemon.	12 de maio de 2021	Não é mais compatível.

Version (Versão)	Alterações	Data	Link para fazer download
1.3.1	<ul style="list-style-type: none"> • Adicionado suporte para macOS Big Sur (10.16). • Problema corrigido que DNS removia as configurações definidas por outros aplicativos. • Corrigido um problema ao usar um certificado inválido para autenticação mútua que causava problemas de conectividade. • Foi adicionado suporte para a diretiva aberta 'route-ipv6'. VPN • 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	<ul style="list-style-type: none"> • Foi adicionado suporte para comentários na VPN configuração aberta. • Foi adicionada uma mensagem de erro para erros de TLS handshake. • 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.

Version (Versão)	Alterações	Data	Link para fazer download
1.2.1	<ul style="list-style-type: none"> • Adicionado suporte para desinstalar a aplicação. • Pequenas correções de bugs e melhorias. 	1.º de julho de 2020	Não é mais compatível.
1.2.0	<ul style="list-style-type: none"> • Foi adicionado suporte para autenticação SAMLfederada baseada em 2.0. • 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.
1.1.1	<ul style="list-style-type: none"> • Problema corrigido em DNS que não estava sendo resolvido. • Corrigido um problema de falha da aplicação causada por conexões mais longas. • Corrigido um MFA problema. 	2 de abril de 2020	Não é mais compatível.
1.1.0	<ul style="list-style-type: none"> • Foi adicionado suporte para a configuração do macOS DNS. • Foi adicionado suporte à funcionalidade Open VPN static challenge echo para ocultar ou mostrar o texto exibido na interface do usuário. • 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

Essas seções descrevem a instalação do cliente AWS fornecido para Linux e, em seguida, o estabelecimento de uma VPN conexão usando o cliente AWS fornecido. O cliente AWS fornecido para Linux não oferece suporte a atualizações automáticas. Para obter as atualizações e downloads mais recentes, consulte [the section called “Notas de release”](#) o.

Requisitos para conexão VPN com o Cliente com um cliente AWS fornecido para Linux

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

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

O cliente reserva a TCP porta 8096 no seu computador. Para VPN endpoints do cliente que usam autenticação federada SAML baseada (login único), o cliente reserva a porta 35001. TCP

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Tópicos

- [Instale o fornecido AWS Client VPN para Linux](#)
- [Conecte-se ao fornecido AWS Client VPN para Linux](#)
- [AWS Client VPN para notas de lançamento do Linux](#)

Instale o fornecido AWS Client VPN para Linux

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

Opção 1: instalar via repositório de pacotes

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

```
wget -q0- https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/awsvpnclient_public_key.asc
```

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://d20adtpz83p9s.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://d20adtpz83p9s.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 AWS fornecido para Linux.

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

Opção 2: instalar usando o arquivo de pacote.deb

1. Baixe o arquivo.deb em [AWS Client VPN download](#) ou usando o comando a seguir.

```
curl https://d20adtpz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o awsvpnclient_amd64.deb
```

2. Instale o cliente AWS fornecido para Linux usando o dpkg utilitário.

```
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.
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](#).

Conecte-se ao fornecido AWS Client VPN para Linux

O cliente AWS fornecido também é chamado de AWS VPN Cliente nas etapas a seguir.

Para se conectar usando o cliente AWS fornecido 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. Em Arquivo de VPN configuração, navegue até o arquivo de configuração que você recebeu do VPN administrador 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 VPN endpoint do cliente tiver sido configurado para usar autenticação baseada em credenciais, 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 Disconnect (Desconectar).

AWS Client VPN para notas de lançamento do Linux

A tabela a seguir contém as notas de lançamento e os links de download das versões atuais e anteriores do AWS Client VPN para Linux.

Note

Continuamos fornecendo correções de usabilidade e segurança a cada lançamento. É altamente recomendável que você use a versão mais recente para todas as plataformas.

As versões anteriores podem ser afetadas por problemas de usabilidade e/ou segurança. Consulte as notas de release completas para obter detalhes.

Version (Versão)	Alterações	Data	Link para fazer download
4.0.0	Pequenos aprimoramentos.	25 de setembro de 2024	Baixe a versão 4.0.0 sha256: c26327187 4217d7978 3fcc1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Foi adicionado suporte para a VPN bandeira <code>mssfix</code> Open.	04 de setembro de 2024	Baixe a versão 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2
3.15.0	<ul style="list-style-type: none"> Foi adicionado suporte para a VPN bandeira <code>tap-sleep</code> Open. As SSL bibliotecas Open VPN e Open foram atualizadas. 	12 de agosto de 2024	Baixe a versão 3.15.0 sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d

Version (Versão)	Alterações	Data	Link para fazer download
			5490a3edb 772dfd89a 6d89d012
3.14.0	<ul style="list-style-type: none">As SSL bibliotecas Open VPN e Open foram atualizadas.	29 de julho de 2024	Baixe a versão 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3.13.0	<ul style="list-style-type: none">Reconecte-se automaticamente quando os intervalos da rede local mudarem.	21 de maio de 2024	Baixe a versão 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1

Version (Versão)	Alterações	Data	Link para fazer download
3.12.2	<ul style="list-style-type: none"> Resolveu um problema SAML de autenticação com navegadores baseados em Chromium desde a versão 123. 	11 de abril de 2024	Baixe a versão 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	<ul style="list-style-type: none"> Corrigida uma ação de estouro de buffer que poderia potencialmente permitir que um ator local executasse comandos arbitrários com permissões elevadas. Procedimento de segurança aprimorado. 	16 de fevereiro de 2024	Baixe a versão 3.12.1 sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0
3.12.0	<ul style="list-style-type: none"> Problemas de conectividade corrigidos em algumas LAN configurações. 	19 de dezembro de 2023	Baixar a versão 3.12.0 sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1

Version (Versão)	Alterações	Data	Link para fazer download
3.11.0	<ul style="list-style-type: none"> • Reversão para “Problemas de conectividade corrigidos em algumas LAN configurações”. • Acessibilidade melhorada. 	6 de dezembro de 2023	Baixar a versão 3.11.0 sha256: 86c0fa1bf1c97194082835a739ec7f1c87e540194955f414a35c679b94538970
3.10.0	<ul style="list-style-type: none"> • Problemas de conectividade corrigidos em algumas LAN configurações. • Acessibilidade melhorada. 	6 de dezembro de 2023	Baixar a versão 3.10.0 sha256: e7450b2490f3b96ab7d589a8000d838d9fd2adcdd72ae80666c4c0d900687e51
3.9.0	<ul style="list-style-type: none"> • Corrigido um problema de conectividade quando NAT64 está habilitado na rede do cliente. • Pequenas correções de bugs e melhorias. 	24 de agosto de 2023	Baixar a versão 3.9.0 sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454

Version (Versão)	Alterações	Data	Link para fazer download
3.8.0	<ul style="list-style-type: none"> • Procedimento de segurança aprimorado. 	3 de agosto de 2023	Baixar a versão 3.8.0 sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd
3.7.0	<ul style="list-style-type: none"> • Procedimento de segurança aprimorado. 	15 de julho de 2023	Não é mais compatível
3.6.0	<ul style="list-style-type: none"> • Reversão das alterações da versão 3.5.0. 	15 de julho de 2023	Não é mais compatível
3.5.0	<ul style="list-style-type: none"> • Procedimento de segurança aprimorado. 	14 de julho de 2023	Não é mais compatível
3.4.0	<ul style="list-style-type: none"> • Foi adicionado suporte para o sinalizador aberto "verify-x509-name". VPN 	14 de fevereiro de 2023	Não é mais compatível
3.1.0	<ul style="list-style-type: none"> • Problema corrigido para detecção de tipo de unidade. • Procedimento de segurança aprimorado. 	23 de maio de 2022	Não é mais compatível
3.0.0	<ul style="list-style-type: none"> • Corrigida a mensagem de banner não sendo exibida ao usar autenticação federada. • Corrigida a exibição do texto do banner para texto mais longo e sequências de caracteres específicas. • Aprimorada a postura de segurança. 	03 de março de 2022	Não é mais compatível.

Version (Versão)	Alterações	Data	Link para fazer download
2.0.0	<ul style="list-style-type: none"> Foi adicionado suporte para texto de banner após uma nova conexão ser estabelecida. Foi removida a capacidade de usar pull-filter em relação ao eco., ou seja, pull-filter * eco Pequenas correções de bugs e melhorias. 	20 de janeiro de 2022	Não é mais compatível.
1.0.3	<ul style="list-style-type: none"> Tentativa de conexão de autenticação federada corrigida em alguns casos. Pequenas correções de bugs e melhorias. 	8 de novembro de 2021	Não é mais compatível.
1.0.2	<ul style="list-style-type: none"> Foi adicionado suporte para Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, . server-poll-timeout Pequenas correções de bugs e melhorias. 	28 de setembro de 2021	Não é mais compatível.
1.0.1	<ul style="list-style-type: none"> Opção habilitada para sair da barra de aplicações do Ubuntu. Foi adicionado suporte para VPN bandeiras abertas: inativo, filtro de tração, rota. 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.

Conecte-se a um AWS Client VPN endpoint usando um cliente Open VPN

Você pode estabelecer uma conexão com um VPN endpoint do Cliente usando aplicativos Open VPN Client comuns. VPN Client é compatível com os seguintes sistemas operacionais:

- Windows

Use um certificado e uma chave privada da Loja de Certificados do Windows. Depois de gerar o certificado e a chave, você pode estabelecer uma conexão de AWS cliente usando o aplicativo VPN GUI cliente Open ou o Open VPN GUI Connect Client. Para obter as etapas para criar o certificado e a chave, consulte [Estabeleça uma VPN conexão usando um certificado no Windows](#).

- Android e iOS

Estabeleça uma VPN conexão usando o aplicativo VPN cliente Open em um dispositivo Android ou iOS. Para ter mais informações, consulte [VPNConexões de clientes no Android e iOS](#).

- macOS

Estabeleça uma VPN conexão usando um arquivo de configuração para Tunnelblick baseado em macOS ou para Client. AWS VPN Para obter mais informações, consulte [Estabeleça uma VPN conexão no macOS](#).

- Linux

Estabeleça uma VPN conexão no Linux usando a interface Open VPN - Network Manager ou o VPN aplicativo Open. Para usar a interface Open VPN - Network Manager, primeiro você precisará instalar o módulo gerenciador de rede, caso ele ainda não esteja instalado. Para obter mais informações, consulte [Estabeleça uma VPN conexão no Linux](#).

Important

Se o VPN endpoint do cliente tiver sido configurado para usar a [autenticação federada SAML baseada](#), você não poderá usar o VPN cliente VPN baseado em Open para se conectar a um endpoint do clienteVPN.

Aplicativos cliente

- [Conecte-se a um AWS Client VPN endpoint usando um aplicativo cliente do Windows](#)
- [AWS Client VPN conexões em aplicativos Android e iOS](#)
- [Conecte-se a um AWS Client VPN endpoint usando um aplicativo cliente macOS](#)
- [Conecte-se a um AWS Client VPN endpoint usando um aplicativo VPN cliente Open](#)

Conecte-se a um AWS Client VPN endpoint usando um aplicativo cliente do Windows

Essas seções descrevem como estabelecer uma VPN conexão usando clientes baseados no WindowsVPN.

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Para obter informações sobre a solução de problemas, consulte [Solução de problemas de VPN conexões de AWS clientes com clientes baseados em Windows](#).

Important

Se o VPN endpoint do cliente tiver sido configurado para usar a [autenticação federada SAML baseada](#), você não poderá usar o VPN cliente VPN baseado em Open para se conectar a um endpoint do clienteVPN.

Tarefas

- [Use um certificado e estabeleça uma VPN conexão de AWS cliente no Windows](#)

Use um certificado e estabeleça uma VPN conexão de AWS cliente no Windows

Você pode configurar o VPN cliente Open para usar um certificado e uma chave privada do Windows Certificate System Store. Essa opção é útil quando você usa um cartão inteligente como parte da VPN conexão do Cliente. Para obter informações sobre a opção Open VPN client cryptoapicert, consulte o [Manual de referência para Open VPN no site Open](#). VPN

Note

O certificado deve ser armazenado no computador local.

Para usar um certificado e estabelecer uma conexão

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 MMC snap-in 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 VPN configuração Open e especifique o certificado usando o assunto do certificado 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"
```

5. Depois de concluir a configuração, use Abrir VPN para estabelecer uma VPN conexão fazendo o seguinte:
 - Use o aplicativo VPN GUI cliente Open
 1. Inicie o aplicativo VPN cliente Open.
 2. Na barra de tarefas do Windows, escolha Mostrar/Ocultar ícones. Clique com o botão direito do mouse em Abrir VPN GUI e escolha Importar arquivo.

3. Na caixa de diálogo Abrir, selecione o arquivo de configuração que você recebeu do VPN administrador do Cliente e escolha Abrir.
 4. Na barra de tarefas do Windows, escolha Mostrar/Ocultar ícones. Clique com o botão direito do mouse em Abrir VPN GUI e escolha Conectar.
- Use o cliente Open VPN GUI Connect
 1. Inicie o VPN aplicativo Abrir e escolha Importar, Do arquivo local... .
 2. Navegue até o arquivo de configuração que você recebeu do VPN administrador e escolha Abrir.

AWS Client VPN conexões em aplicativos Android e iOS

Important

Se o VPN endpoint do cliente tiver sido configurado para usar a [autenticação federada SAML baseada](#), você não poderá usar o VPN cliente VPN baseado em Open para se conectar a um endpoint do clienteVPN.

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

Note

Para obter mais informações sobre como baixar e usar o aplicativo VPN cliente Open para iOS ou Android, consulte o [Guia do usuário do Open VPN Connect](#) no VPN site da Open.

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Para estabelecer a conexão, inicie o aplicativo VPN cliente Open e, em seguida, importe o arquivo que você recebeu do VPN administrador do cliente.

Conecte-se a um AWS Client VPN endpoint usando um aplicativo cliente macOS

Essas seções descrevem como estabelecer uma VPN conexão usando o VPN cliente baseado em macOS, o Tunnelblick ou o Client. AWS VPN

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Para obter informações sobre a solução de problemas, consulte [Solução de problemas de VPN conexões de AWS clientes com clientes macOS](#).

Important

Se o VPN endpoint do cliente tiver sido configurado para usar a [autenticação federada SAML baseada](#), você não poderá usar o VPN cliente VPN baseado em Open para se conectar a um endpoint do clienteVPN.

Tópicos

- [Estabeleça uma AWS Client VPN conexão no macOS](#)

Estabeleça uma AWS Client VPN conexão no macOS

Você pode estabelecer uma VPN conexão usando o aplicativo 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 VPN conexão usando o Tunnelblick

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

2. Arraste e solte o arquivo de configuração que você recebeu VPN do administrador no painel Configurações.
3. Selecione o arquivo de configuração no painel Configurations (Configurações) e escolha Connect (Conectar).

Para estabelecer uma VPN conexão usando o AWS ClienteVPN.

1. Inicie o VPN aplicativo Abrir e escolha Importar, Do arquivo local... .
2. Navegue até o arquivo de configuração que você recebeu do VPN administrador e escolha Abrir.

Conecte-se a um AWS Client VPN endpoint usando um aplicativo VPN cliente Open

Essas seções descrevem como estabelecer uma VPN conexão usando Open VPN - Network Manager ou OpenVPN.

Antes de começar, verifique se o VPN administrador do cliente [criou um VPN endpoint do cliente](#) e forneceu o arquivo de [configuração do VPN endpoint do cliente](#).

Para obter informações sobre a solução de problemas, consulte [Solução de problemas de VPN conexões de AWS clientes com clientes baseados em Linux](#).

Important

Se o VPN endpoint do cliente tiver sido configurado para usar a [autenticação federada SAML baseada](#), você não poderá usar o VPN cliente VPN baseado em Open para se conectar a um endpoint do clienteVPN.

Tópicos

- [Estabeleça uma AWS Client VPN conexão no Linux](#)

Estabeleça uma AWS Client VPN conexão no Linux

Estabeleça uma VPN conexão usando o Network Manager GUI em um computador Ubuntu ou o VPN aplicativo Open.

Para estabelecer uma VPN conexão usando o Open VPN - Network Manager

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 e VPN, em seguida, escolha Importar do arquivo... .
4. Navegue até o arquivo de configuração que você recebeu do VPN administrador e escolha Abrir.
5. Na VPN janela Adicionar, escolha Adicionar.
6. Inicie a conexão ativando o botão ao lado do VPN perfil que você adicionou.

Para estabelecer uma VPN conexão usando Abrir VPN

1. Instale o Open VPN usando o comando a seguir.

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

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

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

Solução de problemas de VPN conexões de AWS clientes

Use os tópicos a seguir para solucionar problemas que você possa ter ao usar um aplicativo cliente para se conectar a um VPN endpoint do cliente.

Tópicos

- [Solução de problemas VPN em terminais de clientes para administradores](#)
- [Envie registros de diagnóstico para AWS Support o cliente AWS fornecido](#)
- [Solução de problemas de VPN conexões de AWS clientes com clientes baseados em Windows](#)
- [Solução de problemas de VPN conexões de AWS clientes com clientes macOS](#)
- [Solução de problemas de VPN conexões de AWS clientes com clientes baseados em Linux](#)
- [Solução de problemas comuns AWS do cliente VPN](#)

Solução de problemas VPN em terminais de clientes para administradores

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

Para obter informações adicionais sobre a solução de problemas de VPN endpoint do cliente, consulte [Solução de problemas do cliente VPN](#) no Guia do AWS Client VPN administrador.

Envie registros de diagnóstico para AWS Support o cliente AWS fornecido

Se você tiver problemas com o cliente AWS fornecido e precisar entrar em contato AWS Support para ajudar a solucionar o problema, o cliente AWS fornecido tem a opção de enviar os registros de diagnóstico para AWS Support. A opção está disponível nas aplicações de cliente do Windows, macOS e Linux.

Antes de enviar os arquivos, você deve concordar em permitir o acesso AWS Support aos seus registros de diagnóstico. Depois de concordar, fornecemos um número de referência que você pode fornecer para AWS Support que eles possam acessar imediatamente os arquivos.

Enviar registros de diagnóstico

O cliente AWS fornecido também é chamado de AWS VPN Cliente nas etapas a seguir.

Para enviar registros de diagnóstico usando o cliente AWS fornecido 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 janela Enviar 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 AWS Support, você precisará fornecer o número de referência.

Para enviar registros de diagnóstico usando o cliente AWS fornecido 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 AWS Support, você precisará fornecer o número de referência.

Para enviar registros de diagnóstico usando o cliente AWS fornecido para o 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 sua prancheta.

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

Solução de problemas de VPN conexões de AWS clientes com clientes baseados em 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 do Cliente. VPN

AWS registros de eventos do cliente fornecidos

O cliente AWS fornecido cria registros de eventos e os armazena no seguinte local em 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_".
- VPNRegistros abertos: contêm informações sobre VPN processos abertos. Esses logs são prefixados com "ovpn_aws_vpn_client_".

O cliente AWS fornecido usa o serviço Windows para realizar 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 de solução de problemas

- [O cliente não consegue se conectar](#)
- [O cliente não pode se conectar com a mensagem de TAP log “sem adaptadores do Windows”](#)
- [O cliente está travado em um estado de reconexão](#)
- [VPN o processo de conexão é encerrado inesperadamente](#)
- [Falha ao iniciar o aplicativo](#)
- [O cliente não consegue criar um perfil](#)
- [VPN desconecta com uma mensagem pop-up](#)
- [A falha do cliente ocorre na Dell PCs usando o Windows 10 ou 11](#)

- [Aberto VPN GUI](#)
- [Cliente Open VPN Connect](#)
- [Não foi possível resolver DNS](#)
- [PKIApelido ausente](#)

O cliente não consegue se conectar

Problema

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

Causa

A causa desse problema pode ser uma das seguintes:

- Outro VPN processo aberto já está sendo executado no seu computador, o que impede que o cliente se conecte.
- Seu arquivo de configuração (.ovpn) é inválido.

Solução

Verifique se há outros VPN aplicativos abertos em execução no seu computador. Se houver, interrompa ou encerre esses processos e tente se conectar novamente ao VPN endpoint do cliente. Verifique se há erros VPN nos registros abertos e peça ao VPN administrador do cliente que verifique 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 .
- Que o ainda CRL é válido. Para obter mais informações, consulte [Clientes que não conseguem se conectar a um VPN endpoint de cliente](#) no Guia do AWS Client VPN administrador.

O cliente não pode se conectar com a mensagem de TAP log “sem adaptadores do Windows”

Problema

O cliente AWS fornecido não consegue se conectar ao VPN endpoint do cliente e a seguinte mensagem de erro aparece nos registros do aplicativo: “Não há adaptadores TAP -Windows neste sistema. Você deve conseguir criar um adaptador TAP -Windows acessando Iniciar -> Todos os programas -> TAP -Windows -> Utilitários -> Adicionar um novo adaptador Ethernet virtual TAP -Windows”.

Solução

É possível corrigir esse problema executando uma ou mais das seguintes ações:

- Reinicie o adaptador TAP -Windows.
- Reinstale o driver TAP -Windows.
- Crie um novo adaptador TAP -Windows.

O cliente está travado em um estado de reconexão

Problema

O cliente AWS fornecido está tentando se conectar ao VPN endpoint do cliente, mas está preso em um estado de reconexão.

Causa

A causa desse problema pode ser uma das seguintes:

- O computador não está conectado à Internet.
- O DNS nome do host não é resolvido como um endereço IP.
- Um VPN processo aberto está tentando se conectar indefinidamente ao endpoint.

Solução

Verifique se o computador está conectado à Internet. Peça ao VPN administrador do cliente que verifique se a `remote` diretiva no arquivo de configuração é resolvida para um endereço IP válido. Você também pode desconectar a VPN sessão escolhendo Desconectar na janela AWS VPN Cliente e tentar se conectar novamente.

VPN processo de conexão é encerrado inesperadamente

Problema

Ao se conectar a um VPN endpoint do cliente, o cliente sai inesperadamente.

Causa

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

Solução

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

Falha ao iniciar o aplicativo

Problema

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

Causa

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

Solução

Execute novamente o instalador do cliente AWS fornecido 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 VPN endpoint do cliente usar autenticação mútua, o arquivo de configuração (.ovpn) não conterá o certificado e a chave do cliente.

Solução

Certifique-se de que o VPN administrador 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 .

VPNdesconecta com uma mensagem pop-up

Problema

VPNEle se desconecta com uma mensagem pop-up que diz: “A VPN conexão está sendo encerrada porque o espaço de endereço da rede local à qual seu dispositivo está conectado foi alterado. Por favor, estabeleça uma nova VPN conexão.”

Causa

TAP- O adaptador Windows não contém a descrição necessária.

Solução

Se o Description campo não corresponder abaixo, primeiro remova o adaptador TAP -Windows e, em seguida, execute novamente o instalador do cliente AWS fornecido para instalar todas as dependências necessárias.

```
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
```

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

Problema

Em alguns Dell PCs (desktop e laptop) que executam o Windows 10 ou 11, pode ocorrer uma falha quando você estiver navegando no sistema de arquivos para importar um arquivo de VPN

configuração. Se esse problema ocorrer, você verá mensagens como as seguintes nos registros 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.DBROverlayIcon.initComponent()
```

Causa

O sistema de Backup e Recuperação da Dell no Windows 10 e 11 pode causar conflitos com o cliente AWS fornecido, especialmente com os três seguintes DLLs:

- DBRShellExtension.dll
- DBROverlayIconBackupid.dll
- DBROverlayIconNotBackupid.dll

Solução

Para evitar esse problema, primeiro certifique-se de que seu cliente esteja atualizado com a versão mais recente do cliente AWS fornecido. Vá para [VPNDownload AWS do cliente](#) e, se uma versão mais recente estiver 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 DLL arquivos. No entanto, observe que isso impedirá que o aplicativo Dell Backup and Recovery funcione completamente.

Exclua ou renomeie os DLL arquivos

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

- DBRShellExtension.dll
- DBROverlayIconBackupped.dll
- DBROverlayIconNotBackupped.dll

Você pode renomear os arquivos adicionando “.bak” ao final do nome do arquivo, por exemplo, .dll.bak. DBROverlayIconBackupped

Aberto VPN GUI

As informações de solução de problemas a seguir foram testadas nas versões 11.10.0.0 e 11.11.0.0 do VPN GUI software Open 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\OpenVPN\config
```

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

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

Cliente Open VPN Connect

As informações de solução de problemas a seguir foram testadas nas versões 2.6.0.100 e 2.7.1.101 do software Open VPN Connect Client 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 foi possível resolver 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 DNS nome não pode ser resolvido. O cliente deve acrescentar uma string aleatória ao DNS nome para evitar o armazenamento em DNS cache; no entanto, alguns clientes não fazem isso.

Solução

Consulte a solução para [Não foi possível resolver o DNS nome do VPN endpoint do cliente](#) no Guia do AWS Client VPN administrador.

PKIApelido ausente

Problema

Uma conexão com um VPN endpoint do cliente que não usa autenticação mútua falha com o seguinte erro.

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

Causa

O software Open VPN Connect Client tem um problema conhecido em que ele tenta se 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 de cliente e um certificado aleatórios no arquivo de VPN configuração do cliente e importe a nova configuração para o software Open VPN Connect Client. Como alternativa, use um cliente diferente, como o cliente Open (v11.12.0.0) ou o VPN GUI cliente Viscosity (v.1.7.14).

Solução de problemas de VPN conexões de AWS clientes com clientes 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.

AWS registros de eventos do cliente fornecidos

O cliente AWS fornecido cria registros de eventos e os armazena no seguinte local em 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_".
- VPNRegistros abertos: contêm informações sobre VPN processos abertos. Esses logs são prefixados com "ovpn_aws_vpn_client_".

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

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

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

O cliente AWS fornecido armazena os arquivos de configuração no seguinte local em seu computador.

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

Tópicos de solução de problemas

- [O cliente não consegue se conectar](#)
- [O cliente está travado em um estado de reconexão](#)
- [O cliente não consegue criar um perfil](#)
- [A ferramenta auxiliar é um erro obrigatório](#)
- [Tunnelblick](#)
- [Algoritmo de cifra 'AES-256-GCM' não encontrado](#)
- [A conexão para de responder e é redefinida](#)
- [Uso estendido da chave \(EKU\)](#)
- [Certificado expirado](#)
- [Aberto VPN](#)
- [Não é possível resolver DNS](#)

O cliente não consegue se conectar

Problema

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

Causa

A causa desse problema pode ser uma das seguintes:

- Outro VPN processo aberto já está sendo executado no seu computador, o que impede que o cliente se conecte.
- Seu arquivo de configuração (.ovpn) é inválido.

Solução

Verifique se há outros VPN aplicativos abertos em execução no seu computador. Se houver, interrompa ou encerre esses processos e tente se conectar novamente ao VPN endpoint do cliente. Verifique se há erros VPN nos registros abertos e peça ao VPN administrador do cliente que verifique 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 .
- Que o ainda CRL é válido. Para obter mais informações, consulte [Clientes que não conseguem se conectar a um VPN endpoint de cliente](#) no Guia do AWS Client VPN administrador.

O cliente está travado em um estado de reconexão

Problema

O cliente AWS fornecido está tentando se conectar ao VPN endpoint do cliente, mas está preso em um estado de reconexão.

Causa

A causa desse problema pode ser uma das seguintes:

- O computador não está conectado à Internet.
- O DNS nome do host não é resolvido como um endereço IP.
- Um VPN processo aberto está tentando se conectar indefinidamente ao endpoint.

Solução

Verifique se o computador está conectado à Internet. Peça ao VPN administrador do cliente que verifique se a `remote` diretiva no arquivo de configuração é resolvida para um endereço IP válido. Você também pode desconectar a VPN sessão escolhendo Desconectar na janela AWS VPN Cliente 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 VPN endpoint do cliente usar autenticação mútua, o arquivo de configuração (.ovpn) não conterá o certificado e a chave do cliente.

Solução

Certifique-se de que o VPN administrador 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 ferramenta auxiliar é um erro obrigatório

Problema

Você recebe o seguinte erro ao tentar conectar VPN o.

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

Solução

Veja o seguinte artigo no AWS re:POST. [AWSVPNErro entre cliente e ferramenta auxiliar é necessária](#)

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 a verbosidade do registro, abra o aplicativo Tunnelblick, escolha Configurações e ajuste o valor para o nível do registro. VPN

Algoritmo de cifra '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 VPN versão aberta que não suporta o algoritmo de criptografia AES -256-. GCM

Solução

Escolha uma VPN versão Open compatível fazendo o seguinte:

1. Abra o aplicativo Tunnelblick.
2. Escolha Configurações.
3. Para a VPN versão aberta, escolha 2.4.6 - A SSL versão aberta 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 do VPN administrador do cliente.

Uso estendido da 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, a autenticação do cliente falha porque o certificado do cliente tem o campo de uso estendido da 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 VPN administrador do cliente. Esse erro pode ocorrer se você estiver usando o certificado do servidor e não o certificado do cliente para se conectar ao VPN endpoint 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 de cliente ao VPN administrador do cliente.

Aberto VPN

As informações de solução de problemas a seguir foram testadas na versão 2.7.1.100 do software Open VPN Connect Client 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 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 Open VPN Connect não consegue resolver o VPN DNS nome do cliente.

Solução

Consulte a solução para [Não foi possível resolver o DNS nome do VPN endpoint do cliente](#) no Guia do AWS Client VPN administrador.

Solução de problemas de VPN conexões de AWS clientes com clientes baseados em 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

- [AWS registros de eventos do cliente fornecidos](#)
- [DNSas consultas vão para um servidor de nomes padrão](#)
- [Abrir VPN \(linha de comando\)](#)
- [Abra VPN por meio do Network Manager \(GUI\)](#)

AWS registros de eventos do cliente fornecidos

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

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

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

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

Por exemplo, você pode verificar os seguintes arquivos de log para encontrar erros nos scripts DNS ativos/inativos que causam a falha na conexão:

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

DNSas consultas vão para um servidor de nomes padrão

Problema

Em algumas circunstâncias, após o estabelecimento de uma VPN conexão, DNS as consultas ainda serão direcionadas para o servidor de nomes padrão do sistema, em vez dos servidores de nomes configurados para o endpoint do cliente. VPN

Causa

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

Solução

1. Adicione a seguinte diretiva na primeira linha do arquivo de VPN configuração Open, para garantir que todas as DNS consultas sejam enviadas para o VPN túnel.

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

2. Use o resolvidor 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 você não quiser que o systemd resolva DNS consultas de proxy e, em vez disso, gostaria que as consultas fossem enviadas diretamente aos servidores de DNS nomes reais, crie um link simbólico para. `/etc/resolv.conf /run/systemd/resolve/resolv.conf`

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

Talvez você queira fazer esse procedimento para ignorar a configuração resolvida pelo systemd, por exemplo, para armazenamento em cache de DNS respostas, configuração por interface, imposição e assim por DNS diante. DNSSEC Essa opção é especialmente útil quando você precisa substituir um DNS registro público por um registro privado quando conectado a. VPN Por exemplo, você pode ter um DNS resolvedor privado em sua conta privada VPC com um registro para `www.exemplo.com`, que resolve para um IP privado. Esta opção pode ser usada para substituir o registro público de `www.example.com`, que resolve para um IP público.

Abrir VPN (linha de comando)

Problema

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

Causa

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

Solução

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

1. Certifique-se de que uma entrada DNS do servidor esteja presente nos registros. No exemplo a seguir, o DNS servidor `192.168.0.2` (configurado no VPN endpoint 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 DNS servidor especificado, peça ao VPN administrador do cliente que modifique o VPN endpoint do cliente e garanta que um DNS servidor (por exemplo, o VPC DNS servidor) tenha sido especificado para o VPN endpoint do cliente. Para obter mais informações, consulte [Client VPN Endpoints](#) no Guia do AWS Client VPN administrador.

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 VPN configuração 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
```

Abra VPN por meio do Network Manager (GUI)

Problema

Ao usar o VPN cliente Network Manager Open, a conexão falha com o seguinte erro.

```
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, LZ0 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 foi possível resolver o DNS nome do VPN endpoint do cliente](#) no Guia do AWS Client VPN administrador.

Solução de problemas comuns AWS do cliente VPN

A seguir estão os problemas comuns que você pode ter ao usar um cliente para se conectar a um VPN endpoint do cliente.

TLSfalhou a negociação chave

Problema

A TLS negociação falha com o seguinte erro.

```
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 UDP TCP o tráfego.
- Você está usando a chave e o certificado do cliente incorretos no arquivo de configuração (.ovpn).

- A lista de revogação de certificados do cliente (CRL) expirou.

Solução

Verifique se as regras de firewall do seu computador estão bloqueando a entrada ou saída ou o UDP tráfego nas portas 443 TCP ou 1194. Peça ao VPN administrador do cliente que verifique as seguintes informações:

- Que as regras de firewall para o VPN endpoint do Cliente não TCP bloqueiem nem UDP trafeguem 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 .
- Que o ainda CRL é válido. Para obter mais informações, consulte [Clientes que não conseguem se conectar a um VPN endpoint de cliente](#) no Guia do AWS Client VPN administrador.

Histórico do documento

A tabela a seguir descreve as atualizações VPN do Guia do Usuário do AWS Cliente.

Alteração	Descrição	Data
AWS cliente fornecido (4.0.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (4.0.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (4.0.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (3.15.1) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	04 de setembro de 2024
AWS cliente fornecido (3.14.2) para Windows lançado	Consulte as notas de release completas para obter detalhes.	04 de setembro de 2024
AWS cliente fornecido (3.12.1) para macOS lançado	Consulte as notas de release completas para obter detalhes.	04 de setembro de 2024
AWS cliente fornecido (3.14.1) para Windows lançado	Consulte as notas de release completas para obter detalhes.	22 de agosto de 2024
AWS cliente fornecido (3.15.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.14.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.12.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.14.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	29 de julho de 2024

AWS cliente fornecido (3.13.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	29 de julho de 2024
AWS cliente fornecido (3.11.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	29 de julho de 2024
AWS cliente fornecido (3.12.1) para Windows lançado	Consulte as notas de release completas para obter detalhes.	18 de julho de 2024
AWS cliente fornecido (3.13.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	21 de maio de 2024
AWS cliente fornecido (3.12.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	21 de maio de 2024
AWS cliente fornecido (3.10.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	21 de maio de 2024
AWS cliente fornecido (3.9.2) para macOS lançado	Consulte as notas de release completas para obter detalhes.	11 de abril de 2024
AWS cliente fornecido (3.12.2) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	11 de abril de 2024
AWS cliente fornecido (3.11.2) para Windows lançado	Consulte as notas de release completas para obter detalhes.	11 de abril de 2024
AWS cliente fornecido (3.9.1) para macOS lançado	Consulte as notas de release completas para obter detalhes.	16 de fevereiro de 2024
AWS cliente fornecido (3.12.1) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	16 de fevereiro de 2024
AWS cliente fornecido (3.11.1) para Windows lançado	Consulte as notas de release completas para obter detalhes.	16 de fevereiro de 2024
AWS cliente fornecido (3.12.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	19 de dezembro de 2023

AWS cliente fornecido (3.9.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	6 de dezembro de 2023
AWS cliente fornecido (3.11.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	6 de dezembro de 2023
AWS cliente fornecido (3.11.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	6 de dezembro de 2023
AWS cliente fornecido (3.10.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	6 de dezembro de 2023
AWS cliente fornecido (3.9.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	24 de agosto de 2023
AWS cliente fornecido (3.8.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	24 de agosto de 2023
AWS cliente fornecido (3.10.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	24 de agosto de 2023
AWS cliente fornecido (3.9.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	3 de agosto de 2023
AWS cliente fornecido (3.8.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	3 de agosto de 2023
AWS cliente fornecido (3.7.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	3 de agosto de 2023
AWS cliente fornecido (3.8.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.7.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.7.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023

AWS cliente fornecido (3.6.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.6.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.5.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.6.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.5.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.4.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.3.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	27 de abril de 2023
AWS cliente fornecido (3.5.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	3 de abril de 2023
AWS cliente fornecido (3.4.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	28 de março de 2023
AWS cliente fornecido (3.3.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	17 de março de 2023
AWS cliente fornecido (3.4.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	14 de fevereiro de 2023
AWS cliente fornecido (3.2.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	23 de janeiro de 2023
AWS cliente fornecido (3.2.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	23 de janeiro de 2023

AWS cliente fornecido (3.1.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.1.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.1.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.0.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	3 de março de 2022
AWS cliente fornecido (3.0.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	3 de março de 2022
AWS cliente fornecido (3.0.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	3 de março de 2022
AWS cliente fornecido (2.0.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	20 de janeiro de 2022
AWS cliente fornecido (2.0.0) para Windows lançado	Consulte as notas de release completas para obter detalhes.	20 de janeiro de 2022
AWS cliente fornecido (2.0.0) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	20 de janeiro de 2022
AWS cliente fornecido (1.4.0) para macOS lançado	Consulte as notas de release completas para obter detalhes.	9 de novembro de 2021
AWS cliente fornecido para Windows (1.3.7) lançado	Consulte as notas de release completas para obter detalhes.	8 de novembro de 2021
AWS cliente fornecido (1.0.3) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	8 de novembro de 2021
AWS cliente fornecido (1.0.2) para Ubuntu lançado	Consulte as notas de release completas para obter detalhes.	28 de setembro de 2021

AWS cliente fornecido para Windows (1.3.6) e macOS (1.3.5) lançado	Consulte as notas de release completas para obter detalhes.	20 de setembro de 2021
AWS cliente fornecido para Ubuntu 18.04 LTS e Ubuntu LTS 20.04 lançado	Você pode usar o cliente AWS fornecido no Ubuntu 18.04 LTS e no Ubuntu 20.04. LTS	11 de junho de 2021
Support for Open VPN usando um certificado da Windows Certificate System Store	Você pode usar Abrir VPN com um certificado do Windows Certificate System Store.	25 de fevereiro de 2021
Portal de autoatendimento	Você pode acessar um portal de autoatendimento para obter o cliente e o arquivo de configuração mais recentes AWS fornecidos.	29 de outubro de 2020
AWS cliente fornecido	Você pode usar o cliente AWS fornecido para se conectar a um VPN endpoint do cliente.	4 de fevereiro de 2020
Lançamento inicial	Esta versão apresenta o AWS ClientVPN.	18 de dezembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.