Guia do usuário

AWS Client VPN

AWS Client VPN: Guia do usuário

Table of Contents

O que é AWS Client VPN?

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

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

Componentes da Client VPN

A seguir estão os principais componentes para usar o AWS Client VPN.

- Endpoint da Client VPN: o administrador da Client VPN cria e configura um endpoint da Client VPN no formato AWS. O administrador controla quais redes e recursos você pode acessar ao estabelecer uma conexão VPN.
- Aplicação cliente da VPN: o software que você usa para se conectar ao endpoint da Client VPN e estabelecer uma conexão VPN segura.
- Arquivo de configuração de endpoint da Client VPN: arquivo de configuração fornecido pelo administrador da Client VPN. O arquivo inclui as informações sobre o endpoint da Client VPN e os certificados necessários para estabelecer uma conexão VPN. Você carrega esse arquivo na aplicação cliente da VPN escolhida. O cliente AWS fornecido permite que você se conecte a cinco sessões simultâneas, cada sessão com seu próprio arquivo de configuração fornecido pelo administrador do Client VPN. Para obter mais informações sobre sessões simultâneas, consulteSupport para conexões simultâneas.

Recursos adicionais para configurar a Client VPN

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

Comece com AWS Client VPN

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

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

Tópicos

Pré-requisitos para usar a Client VPN

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

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

Etapa 1: Obter uma aplicação cliente de VPN

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

É possível baixar a aplicação Client VPN por meio de um dos dois métodos, dependendo se o administrador criou o arquivo de configuração do endpoint para a aplicação:

- Se o administrador não configurou os arquivos de configuração do endpoint, baixe e instale o cliente em AWS Client VPN download. Depois de baixar e instalar a aplicação, continue com the section called “Etapa 2: Obter o arquivo de configuração do endpoint da Client VPN.” para obter o arquivo de configuração do endpoint do administrador. Se você estiver se conectando a vários perfis, precisará de um arquivo de configuração para cada perfil.
- Se o administrador já tiver pré-configurado o arquivo de configuração do endpoint, será possível poderá baixar a aplicação Client VPN, 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 “Download da Client VPN”. Depois de baixar e instalar a aplicação e o arquivo, acesse the section called “Etapa 3: Conectar-se à VPN”.

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

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

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

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

Etapa 3: Conectar-se à VPN

Importe o arquivo de configuração do endpoint do Client VPN para o cliente AWS fornecido ou para seu aplicativo cliente OpenVPN e conecte-se à VPN. Para ver as etapas para se conectar a uma VPN, incluindo a importação de um ou mais arquivos de configuração de endpoint para um determinado AWS cliente, 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 OpenVPN

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

Para endpoints do Client VPN que usam autenticação federada baseada em SAML (single sign-on), o cliente AWS fornecido abre uma janela do navegador em seu computador. Você será solicitado a inserir suas credenciais corporativas antes de poder se conectar ao endpoint da cliente VPN.

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 as versões mais recentes dos arquivos de configuração do endpoint do Client VPN. Se o administrador do endpoint Client VPN tiver pré-configurado um ou mais arquivos de configuração para o cliente Client VPN, você poderá baixar e instalar esse aplicativo Client VPN junto com esses arquivos de configuração a partir deste portal.

> **Note**
>
> Se você for um administrador e quiser configurar o portal de autoatendimento, consulte Client VPN endpoints no Guia do Administrador AWS Client VPN .

Antes de começar, você deve ter o ID de cada endpoint do Client VPN que deseja baixar. O administrador do endpoint do Client VPN pode fornecer o ID ou fornecer um URL do portal de autoatendimento que inclua o ID. Para várias conexões de endpoint, você precisará do ID do endpoint para cada perfil ao qual deseja se conectar.

Para acessar o portal de autoatendimento

1. Acesse o portal de autoatendimento em https://self-service.clientvpn.amazonaws.com/ou use a URL fornecida pelo administrador.
2. Se necessário, insira o ID do endpoint da Client VPN, por exemplo, `cvpn-endpoint-0123456abcd123456`. Escolha Próximo.
3. Digite seu nome de usuário e senha e escolha Sign In (Fazer login). Este é o mesmo nome de usuário e senha que você usa para se conectar ao endpoint da Client VPN.
4. No portal de autoatendimento, você pode fazer o seguinte:
   - Faça download da versão mais recente do arquivo de configuração do cliente para o endpoint da Client VPN. Se você quiser se conectar a vários endpoints, precisará baixar o arquivo de configuração de cada endpoint.
   - Baixe a versão mais recente do cliente AWS fornecido para sua plataforma.
5. Repita essas etapas para cada arquivo de configuração de endpoint para o qual você deseja criar um perfil de conexão.

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

Você pode se conectar a um endpoint Client VPN usando o cliente AWS fornecido, que é compatível com Windows, macOS e Ubuntu. O cliente AWS fornecido também suporta até cinco conexões simultâneas, bem como diretivas OpenVPN.

Tópicos

Support para conexões simultâneas usando um cliente AWS fornecido

O cliente AWS fornecido permite conectar-se a várias sessões simultâneas. Isso é útil se você precisar de acesso a recursos em vários AWS ambientes e tiver endpoints diferentes para esses recursos. Por exemplo, você pode precisar acessar um banco de dados em um ambiente em um endpoint diferente do endpoint ao qual você está conectado atualmente, mas não deseja desconectar a conexão atual. Para permitir que o cliente AWS fornecido se conecte às sessões atuais, baixe o arquivo de configuração que seu administrador criou para cada endpoint e, em seguida, crie um perfil de conexão para cada arquivo. Usando o cliente AWS fornecido, você pode se conectar a várias sessões sem se desconectar de nenhuma sessão aberta no momento. Isso é suportado somente para clientes AWS fornecidos. Para ver as etapas para se conectar a sessões simultâneas, consulte o seguinte:

- Conecte-se usando o cliente AWS fornecido para Windows
- Conecte-se usando o cliente AWS fornecido para macOS
- Conecte-se usando o cliente AWS fornecido para Linux

Ao se conectar a vários endpoints, o Client VPN implementa verificações para garantir que não haja conflitos com outras conexões de endpoint abertas — por exemplo, se duas sessões tiverem blocos CIDR ou políticas de roteamento conflitantes; ou se você já estiver conectado com uma conexão de túnel completa. Se a verificação encontrar conflitos, uma conexão não será estabelecida até

que você escolha uma conexão diferente que não esteja em conflito com a conexão aberta ou se desconecte da sessão aberta que está causando o conflito.

Conexões DNS simultâneas são permitidas. O servidor DNS de uma das conexões habilitadas para DNS será aplicado. Dependendo do servidor DNS, você pode ser solicitado a fazer a autenticação durante a reconexão.

> **Note**
>
> O número máximo de sessões simultâneas permitidas é cinco.

Diretivas do OpenVPN

O cliente AWS fornecido suporta as seguintes diretivas do OpenVPN. Para mais informações sobre essas diretivas, consulte a documentação no site do OpenVPN.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb

  dhcp-option
- ifconfig-ipv6

- inactive
- keepalive
- key
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- saída de 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
- toque-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN para Windows

Essas seções descrevem como estabelecer uma conexão VPN usando o cliente AWS fornecido para Windows. É possível baixar e instalar o cliente em Baixar AWS Client VPN. 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)
- .NET Framework 4.7.2 ou superior

Para endpoints Client VPN que usam autenticação federada baseada em SAML (single sign-on), o cliente reserva as portas TCP 8096-8115 em seu computador.

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

Tópicos

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. Para o Arquivo de configuração de VPN, navegue e selecione o arquivo de configuração que você recebeu de seu administrador do VPN do Cliente e escolha Adicionar perfil.

6. Se você quiser criar várias conexões, repita as etapas Adicionar Perfil para cada arquivo de configuração que você deseja adicionar. Você pode adicionar quantos perfis quiser, mas só pode ter até cinco conexões abertas.
7. Na janela AWS VPN Cliente, escolha o perfil ao qual você deseja se conectar e escolha Conectar. Se o endpoint da Client VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha. Repita essa etapa para cada conexão de perfil que você deseja iniciar, conectando até cinco endpoints simultâneos.

   > **Note**
   >
   > Se algum perfil ao qual você se conectar estiver em conflito com uma sessão aberta no momento, você não poderá fazer a conexão. Escolha uma nova conexão ou desconecte-se da sessão que está causando o conflito.

8. Para ver as estatísticas de uma conexão, escolha Conexão na janela do cliente AWS VPN, escolha Mostrar detalhes e escolha a conexão sobre a qual você deseja ver detalhes.
9. Para desconectar uma conexão, escolha uma conexão na janela do cliente AWS VPN e escolha Desconectar. Se você tiver várias conexões abertas, feche cada conexão individualmente. 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. Recomendamos fortemente que você use a versão mais recente para cada plataforma. As versões anteriores podem ser afetadas por problemas de and/or segurança de usabilidade. Consulte as notas de lançamento completas para obter detalhes.

Versão	Alterações	Data	Link para download e SHA256
5.2.2	Procedimento de segurança aprimorado.	2 de junho de 2025	Baixe a versão 5.2.2 sha256: f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	• Foi adicionada compatibilidade com o sinalizador `ping-exit` OpenVPN. • Atualizou a biblioteca OpenSSL. • Pequenas correções de bugs e melhorias.	21 de abril de 2025	Não é mais compatível.
5.2.0	• Aprimoramentos secundários. • Foi adicionado suporte para o Client Route Enforcement.	8 de abril de 2025	Não é mais compatível.
5.1.0	• Corrigido um problema que fazia com que a AWS Client VPN versão 5.0.x se reconectasse automaticamente à VPN após uma desconexão do tempo limite de inatividade. • Pequenas correções de bugs e melhorias.	17 de março de 2025	Não é mais compatível.
5.0.2	• Corrigido um problema de DNS para conexões simultâneas. • Problemas esporádicos corrigidos ao instalar novos adaptadores TAP.	24 de fevereiro de 2025	Não é mais compatível.

Versão	Alterações	Data	Link para download e SHA256
5.0.1	Corrigido um problema que causava erros esporádicos de conexão VPN no cliente Windows versão 5.0.0.	30 de janeiro de 2025	Não é mais compatível.
5.0.0	• Foi adicionado suporte para conexões simultâneas. • Atualizou a versão do driver TAP. • Atualizou a interface gráfica do usuário. • Pequenas correções de bugs e melhorias	21 de janeiro de 2025	Não é mais compatível.
4.1.0	Pequenas correções de bugs e melhorias .	12 de novembro de 2024	Não é mais compatível.
4.0.0	Aprimoramentos secundários.	25 de setembro de 2024	Baixar a versão 4.0.0 sha256: 6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc

Versão	Alterações	Data	Link para download e SHA256
3.14.2	Foi adicionada compatibilidade com o sinalizador `mssfix` OpenVPN.	4 de setembro de 2024	Baixar a versão 3.14.2 sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Pequenas correções de bugs e melhorias .	22 de agosto de 2024	Baixar a versão 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	• Foi adicionada compatibilidade com o sinalizador `tap-sleep` OpenVPN. • As bibliotecas OpenVPN e OpenSSL foram atualizadas.	12 de agosto de 2024	Baixar a versão 3.14.0 sha256: 812fb2f6d 263288c66 4d598f6bd 70e3f601d 11dcb89e6 3b281b0a9 6b96354516

Versão	Alterações	Data	Link para download e SHA256
3.13.0	As bibliotecas OpenVPN e OpenSSL foram atualizadas.	29 de julho de 2024	Baixar a versão 3.13.0 sha256: c9cc896e81a74411840951e349eed9384507c53337fb703c5ec64d522c29388b
3.12.1	Corrigido um problema que impede que a versão 3.12.0 do cliente Windows estabeleça uma conexão VPN para alguns usuários.	18 de julho de 2024	Baixar a versão 3.12.1 sha256: 5ed34aee6c03aa281e625acdbed272896c67046364a9e5846ca697e05dbfec08
3.12.0	• Reconecte-se automaticamente quando os intervalos da rede local mudarem. • O foco automático da aplicação foi removido quando conectado aos endpoints SAML.	21 de maio de 2024	Não é mais compatível

Versão	Alterações	Data	Link para download e SHA256
3.11.2	Resolveu um problema de autenticação SAML com navegadores baseados em Chromium desde a versão 123.	11 de abril de 2024	Baixar a versão 3.11.2 sha256: 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc
3.11.1	• Corrigida uma ação de estouro de buffer que poderia permitir que um ator local executasse comandos arbitrários com permissões elevadas. • Procedimento de segurança aprimorado.	16 de fevereiro de 2024	Baixar a versão 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Corrigido um problema de conectividade causado pelo Windows VMs. • Problemas de conectividade corrigidos em algumas configurações de LAN. • Acessibilidade melhorada.	6 de dezembro de 2023	Baixar a versão 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Versão	Alterações	Data	Link para download e SHA256
3.10.0	• 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: d46721aad40ccb816f163e406c366ff03b1120abbb43a20607e06d3b1fa8667f
3.9.0	Procedimento de segurança aprimorado.	3 de agosto de 2023	Baixar a versão 3.9.0 sha256: de9a3800ea2349155540bd32bbae472404c636d8d8267a0e1fb2173a8aae21ed
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

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	• Foi adicionada compatibilidade com a sinalização “verify-x509-name” da OpenVPN. • 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	Procedimento de segurança aprimorado.	23 de maio de 2022	Não é mais compatível
3.0.0	• Foi adicionada compatibilidade com o Windows 11. • Corrigida a nomeação do driver TAP Windows fazendo com que outros nomes de driver 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

Versão	Alterações	Data	Link para download e SHA256
2.0.0	• Foi adicionada compatibilidade com 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	• 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	• Foi adicionado suporte para os sinalizadores do OpenVPN: 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	• Foi adicionada compatibilidade com o sinalizador OpenVPN: dhcp-option. • Pequenas correções de bugs e melhorias.	4 de agosto de 2021	Não é mais compatível

Versão	Alterações	Data	Link para download e SHA256
1.3.3	• Foi adicionada compatibilidade com sinalizadores do OpenVPN: inativo, pull-filter, 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	• Adicione a prevenção de IPv6 vazamentos, quando estiver configura da. • 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	• Foi adicionada compatibilidade com 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 adicionada compatibilidade com a diretiva “route-ipv6” do OpenVPN. • Pequenas correções de bugs e melhorias.	5 de abril de 2021	Não é mais compatível

Versão	Alterações	Data	Link para download e SHA256
1.3.0	Recursos de compatibilidade 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	• Foi adicionada compatibilidade com a diretiva cryptoapicert do OpenVPN. • 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	• Foi adicionada compatibilidade com comentários na configuração do OpenVPN. • Adicionada uma mensagem de erro para erros de handshake do TLS.	8 de outubro de 2020	Não é mais compatível
1.2.4	Pequenas correções de bugs e melhorias.	1.º de setembro de 2020	Não é mais compatível
1.2.3	Reverter alterações na versão 1.2.2.	20 de agosto de 2020	Não é mais compatível
1.2.1	Pequenas correções de bugs e melhorias.	1.º de julho de 2020	Não é mais compatível
1.2.0	• Foi adicionada compatibilidade com autenticação federada baseada em SAML 2.0. • Compatibilidade obsoleta para a plataforma Windows 7.	19 de maio de 2020	Não é mais compatível

Versão	Alterações	Data	Link para download e SHA256
1.1.1	Pequenas correções de bugs e melhorias .	21 de abril de 2020	Não é mais compatível
1.1.0	• Foi adicionada compatibilidade com a funcionalidade de eco de desafio estático do OpenVPN 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 conexão VPN usando o cliente AWS fornecido para macOS. É possível baixar e instalar o cliente em Baixar AWS Client VPN. O cliente AWS fornecido não oferece suporte a atualizações automáticas.

Requisitos

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

- macOS Ventura (13.0), Sonoma (14.0) ou Sequoia (15.0).
- Compatível com o processador x86_64.
- Para endpoints Client VPN que usam autenticação federada baseada em SAML (single sign-on), o cliente reserva as portas TCP 8096-8115 em seu computador.

> **Note**
>
> Se estiver usando um Mac com processador Apple Silicon, você precisará instalar o Rosetta 2 para executar o software cliente. Para obter mais detalhes, consulte sobre o Rosetta Translation Environment no site da Apple.

Tópicos

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

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

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. Para o Arquivo de configuração de VPN, navegue e selecione o arquivo de configuração que você recebeu de seu administrador do VPN do Cliente e escolha Adicionar perfil.
6. Se você quiser criar várias conexões, repita as etapas Adicionar Perfil para cada arquivo de configuração que você deseja adicionar. Você pode adicionar quantos perfis quiser, mas só pode ter até cinco conexões abertas.
7. Na janela AWS VPN Cliente, escolha o perfil ao qual você deseja se conectar e escolha Conectar. Se o endpoint da Client VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha. Repita essa etapa para cada conexão de perfil que você deseja iniciar, conectando até cinco endpoints simultâneos.

> **Note**
>
> Se algum perfil ao qual você se conectar estiver em conflito com uma sessão aberta no momento, você não poderá fazer a conexão. Escolha uma nova conexão ou desconecte-se da sessão que está causando o conflito.

8. Para ver as estatísticas de uma conexão, escolha Conexão na janela do cliente AWS VPN, escolha Mostrar detalhes e escolha a conexão sobre a qual você deseja ver detalhes.
9. Para desconectar uma conexão, escolha uma conexão na janela do cliente AWS VPN e escolha Desconectar. Se você tiver várias conexões abertas, feche cada conexão individualmente.

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. Recomendamos fortemente que você use a versão mais recente para cada plataforma. As versões anteriores podem ser afetadas por problemas de and/or segurança de usabilidade. Consulte as notas de lançamento completas para obter detalhes.

Versão	Alterações	Data	Link para fazer download
5.2.1	• Foi adicionado suporte para o sinalizador OpenVPN de saída de ping. • Atualizou a biblioteca OpenSSL. • Procedimento de segurança aprimorado. • Pequenas correções de bugs e melhorias.	18 de junho de 2025	Baixe a versão 5.2.1 sha256:906f77fbca3334fbdcd1145dd6f2725beab82a30b9b51ea

Versão	Alterações	Data	Link para fazer download
			fd1a25c3f e7d669eb
5.2.0	• Aprimoramentos secundários. • Foi adicionado suporte para o Client Route Enforcement.	8 de abril de 2025	Baixe a versão 5.2.0 sha256: f062e971a 84e98d8a6 1caced3d7 f6be322c2 8dab02ec8 1194c0f9a 3e62bd8249
5.1.0	• Corrigido um problema que fazia com que a AWS Client VPN versão 5.0.x se reconectasse automaticamente à VPN após uma desconexão do tempo limite de inatividade. • Correção de um problema que AWS Client VPN impedia o estabelecimento de uma conexão VPN para arquivos de configuração com terminações de linha no estilo Windows. • Pequenas correções de bugs e melhorias.	17 de março de 2025	Baixe a versão 5.1.0 sha256: ef7ff34ae 85a29f902 12514568c 93849ef6e 67f30b2c8 3ae1494d3 07f7650e10

Versão	Alterações	Data	Link para fazer download
5.0.3	Pequenas correções de bugs e melhorias .	6 de março de 2025	Baixe a versão 5.0.3 sha256:8c e0f91ce81 c322cead3 ed27948dd eda4d5a61 f5ed5a611 5ab8e18f5 d8963f6b
5.0.2	Corrigido um problema que gerava erros esporádicos ao escolher Connect.	17 de fevereiro de 2025	Baixe a versão 5.0.2 sha256: e81287746 08147e65b 14f992a4b 5a6d75364 6424fe3b6 8fab23181 0addac1f7c
5.0.1	Correção de um problema que impedia que a versão 5.0.0 do cliente estabelec esse uma conexão VPN para nomes de perfil que continham espaços.	22 de janeiro de 2025	Baixe a versão 5.0.1 sha256:7d 9de8c8915 4c9a99bfd 56b196600 a9a09eb6a 952cb10a7 b16d01bdb adb0e57a

Versão	Alterações	Data	Link para fazer download
5.0.0	• Foi adicionado suporte para conexões simultâneas. • Atualizou a interface gráfica do usuário. • Pequenas correções de bugs e melhorias.	21 de janeiro de 2025	Baixe a versão 5.0.0 sha256: e9c95ecdd6d582e72e1af0b05d03fe678f96b8b1028b5f569f962902943ecf02
4.1.0	Pequenas correções de bugs e melhorias .	12 de novembro de 2024	Baixe a versão 4.1.0 sha256: afe1ec8a6d7e2e1d618a6507f44a8c41db744fb55f94573e318d75bc5e96cd269
4.0.0	Aprimoramentos secundários.	25 de setembro de 2024	Baixar a versão 4.0.0 sha256: ad574475a80b614499c97ae75612ef1ff905bb4aa1b5f7109420e80bf95aefcbd

Versão	Alterações	Data	Link para fazer download
3.12.1	Foi adicionada compatibilidade com o sinalizador `mssfix` OpenVPN.	4 de setembro de 2024	Baixar a versão 3.12.1 sha256: a5c31d3e0 e8bf89376 82805c9ff f76ca9205 875e009e9 49ad1b053 2f449cee47
3.12.0	• Foi adicionada compatibilidade com o sinalizador `tap-sleep` OpenVPN. • As bibliotecas OpenVPN e OpenSSL foram atualizadas.	12 de agosto de 2024	Baixar a versão 3.12.0 sha256: 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• As bibliotecas OpenVPN e OpenSSL foram atualizadas.	29 de julho de 2024	Baixar a versão 3.11.0 sha256: 44b5e6f84 788bf45dd b77871d74 3e09007e1 597555850 6221b8cae a81732848f

Versão	Alterações	Data	Link para fazer download
3.10.0	• Reconecte-se automaticamente quando os intervalos da rede local mudarem. • Corrigido um problema de restauração de DNS durante a troca de rede. • O foco automático da aplicação foi removido quando conectado aos endpoints SAML.	21 de maio de 2024	Baixar a versão 3.10.0 sha256: 28bf26fa134b01ff12703cf59ffa4adba7c44ceb793dce4addd4404e84287dd
3.9.2	• Resolveu um problema de autenticação SAML com navegadores baseados em Chromium desde a versão 123. • Foi adicionada compatibilidade com macOS Sonoma. Compatibilidade obsoleta com macOS Big Sur. • Procedimento de segurança aprimorado.	11 de abril de 2024	Baixar a versão 3.9.2 sha256: 374467d991e8953b5032e5b985cda80a0ea27fb5d5f23cf16c556a1568b0d480
3.9.1	• Corrigida uma ação de estouro de buffer que poderia permitir que um ator local executasse comandos arbitrários com permissões elevadas. • Barra de progresso do download da atualização da aplicação fixa. • Procedimento de segurança aprimorado.	16 de fevereiro de 2024	Baixar a versão 3.9.1 sha256: 9bba4b27a635e75038703e2cf4cd814aa75306179fac8e500e2c7af4e899e971

Versão	Alterações	Data	Link para fazer download
3.9.0	• Problemas de conectividade corrigidos em algumas configurações de LAN. • Acessibilidade melhorada.	6 de dezembro de 2023	Baixar a versão 3.9.0 sha256: f0f6a5579fe9431577452e8aac07241c36cb34c2b3f028dfdd07f41d00ff80d8
3.8.0	• 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: d5a229b12efa2e88627127a6dc27f5c6a1bc9c426a8c466131ecbdbd6bbb4461
3.7.0	• Procedimento de segurança aprimorado.	3 de agosto de 2023	Baixar a versão 3.7.0 sha256: 4a34b25b48233b02d6107638a3868f7e419a84d20bb4989f7b394aae9a9de00a

Versão	Alterações	Data	Link para fazer download
3.6.0	• Procedimento de segurança aprimorado.	15 de julho de 2023	Não é mais compatível
3.5.0	• Reversão das alterações da versão 3.4.0.	15 de julho de 2023	Não é mais compatível
3.4.0	• Procedimento de segurança aprimorado.	14 de julho de 2023	Não é mais compatível
3.3.0	• Foi adicionada compatibilidade com macOS Ventura (13.0). • Pequenas correções de bugs e melhorias.	27 de abril de 2023	Não é mais compatível
3.2.0	• Foi adicionada compatibilidade com a sinalização “verify-x509-name” da OpenVPN. • 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	• Foi adicionada compatibilidade com macOS Monterey. • Corrigido um problema na detecção do tipo de unidade. • Procedimento de segurança aprimorado.	23 de maio de 2022	Não é mais compatível

Versão	Alterações	Data	Link para fazer download
3.0.0	• 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.
2.0.0	• Foi adicionada compatibilidade com 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	• Adicionado o monitoramento do servidor DNS durante a conexão. As configurações serão reconfiguradas se não corresponderem às configurações de VPN. • 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	• Foi adicionado suporte para os sinalizadores do OpenVPN: 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.

Versão	Alterações	Data	Link para fazer download
1.3.4	• Foi adicionada compatibilidade com o sinalizador OpenVPN: dhcp-option. • Pequenas correções de bugs e melhorias.	4 de agosto de 2021	Não é mais compatível.
1.3.3	• Foi adicionada compatibilidade com sinalizadores do OpenVPN: inativo, pull-filter, 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	• Adicione a prevenção de IPv6 vazamentos, quando estiver configura da. • 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.

Versão	Alterações	Data	Link para fazer download
1.3.1	• Foi adicionada compatibilidade com macOS Big Sur (10.16). • Corrigido o problema que removia as configurações de DNS definidas por outras aplicações. • Corrigido um problema ao usar um certificado inválido para autenticação mútua que causava problemas de conectividade. • Foi adicionada compatibilidade com a diretiva “route-ipv6” do OpenVPN. • Pequenas correções de bugs e melhorias.	5 de abril de 2021	Não é mais compatível.
1.3.0	Recursos de compatibilidade 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	• Foi adicionada compatibilidade com comentários na configuração do OpenVPN. • Adicionada uma mensagem de erro para erros de handshake do TLS. • Corrigido um erro de desinstalação que estava afetando alguns usuários.	8 de outubro de 2020	Não é mais compatível.

Versão	Alterações	Data	Link para fazer download
1.2.2	Pequenas correções de bugs e melhorias .	12 de agosto de 2020	Não é mais compatível.
1.2.1	• Foi adicionada compatibilidade com desinstalar a aplicação. • Pequenas correções de bugs e melhorias.	1.º de julho de 2020	Não é mais compatível.
1.2.0	• Foi adicionada compatibilidade com autenticação federada baseada em SAML 2.0. • Foi adicionada compatibilidade com 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	• Corrigido um problema em que o DNS não estava resolvendo. • Corrigido um problema de falha da aplicação causada por conexões mais longas. • Corrigido um problema de MFA.	2 de abril de 2020	Não é mais compatível.
1.1.0	• Foi adicionada compatibilidade com a configuração de DNS do macOS. • Foi adicionada compatibilidade com a funcionalidade de eco de desafio estático do OpenVPN 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.

Versão	Alterações	Data	Link para fazer download
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 conexão VPN 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 o the section called “Notas da versão”.

Requisitos para conexão com a Client VPN com um cliente da AWS fornecido para Linux

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

- Ubuntu 22.04 LTS (AMD64) ou Ubuntu 24.04 LTS (somente) AMD64

Para endpoints Client VPN que usam autenticação federada baseada em SAML (single sign-on), o cliente reserva as portas TCP 8096-8115 em seu computador.

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

Tópicos

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 do AWS VPN Client ao seu sistema operacional Ubuntu.

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. Use o comando a seguir para adicionar o repositório ao seu sistema operacional Ubuntu (versão 22.04 e superior):

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

3. 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 Client VPN download (Baixar VPN do cliente da AWS) ou usando o comando a seguir.

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

2. 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 (Baixar VPN do Cliente).
2. Depois de baixar 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. Para Arquivo de configuração da VPN, navegue até o arquivo de configuração que você recebeu do administrador do VPN do Cliente. Escolha Abrir.
6. Escolha Adicionar perfil.
7. Se você quiser criar várias conexões, repita as etapas Adicionar Perfil para cada arquivo de configuração que você deseja adicionar. Você pode adicionar quantos perfis quiser, mas só pode ter até cinco conexões abertas.
8. Na janela AWS VPN Cliente, escolha o perfil ao qual você deseja se conectar e, em seguida, escolha Conectar. Se o endpoint da Client VPN foi configurado para usar autenticação baseada em credencial, você será solicitado a inserir um nome de usuário e uma senha. Repita essa etapa para cada conexão de perfil que você deseja iniciar, conectando até cinco endpoints simultâneos.

> **Note**
>
> Se algum perfil ao qual você se conectar estiver em conflito com uma sessão aberta no momento, você não poderá fazer a conexão. Escolha uma nova conexão ou desconecte-se da sessão que está causando o conflito.

9. Para ver as estatísticas de uma conexão, escolha Conexão na janela do cliente AWS VPN, escolha Mostrar detalhes e escolha a conexão sobre a qual você deseja ver detalhes.
10. Para desconectar uma conexão, escolha uma conexão na janela do cliente AWS VPN e escolha Desconectar. Se você tiver várias conexões abertas, feche cada conexão individualmente.

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. Recomendamos fortemente que você use a versão mais recente para cada plataforma. As versões anteriores podem ser afetadas por problemas de usabilidade e/ou segurança. Consulte as notas de lançamento completas para obter detalhes.

Versão	Alterações	Data	Link para fazer download
5.2.0	• Aprimoramentos secundários. • Foi adicionado suporte para o Client Route Enforcement.	8 de abril de 2025	Baixe a versão 5.2.0 sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• Corrigido um problema que fazia com que a AWS Client VPN versão 5.0.x se reconectasse automaticamente à VPN após uma desconexão do tempo limite de inatividade.	17 de março de 2025	Baixe a versão 5.1.0 sha256:14f26c05b11

Versão	Alterações	Data	Link para fazer download
	• Pequenas correções de bugs e melhorias.		b0cc484b0 8a8f8d207 39de3d815 c268db3bb a9ac70c0e 766b70ba
5.0.0	• Foi adicionado suporte para várias conexões simultâneas. • Atualizou a interface gráfica do usuário. • Pequenas correções de bugs e melhorias.	21 de janeiro de 2025	Baixe a versão 5.0.0 sha256:64 5126b5698 cb550e9dc 822e58ed8 99a5730d2 e204f28f4 023ec6719 15fdda0c
4.1.0	• Foi adicionado suporte para o Ubuntu 22.04 e 24.04. • Correções de erros.	12 de novembro de 2024	Baixe a versão 4.1.0 sha256:33 4d0022245 8fbfe9dad e16c99fe9 7e9ebcbd5 1fff017d0 d6b1d1b76 4e7af472

Versão	Alterações	Data	Link para fazer download
4.0.0	Aprimoramentos secundários.	25 de setembro de 2024	Baixar a versão 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Foi adicionada compatibilidade com o sinalizador `mssfix` OpenVPN.	4 de setembro de 2024	Baixar a versão 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2
3.15.0	• Foi adicionada compatibilidade com o sinalizador `tap-sleep` OpenVPN. • As bibliotecas OpenVPN e OpenSSL foram atualizadas.	12 de agosto de 2024	Baixar a versão 3.15.0 sha256: 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012

Versão	Alterações	Data	Link para fazer download
3.14.0	• As bibliotecas OpenVPN e OpenSSL foram atualizadas.	29 de julho de 2024	Baixar a versão 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3.13.0	• Reconecte-se automaticamente quando os intervalos da rede local mudarem.	21 de maio de 2024	Baixar a versão 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1
3.12.2	• Resolveu um problema de autenticação SAML com navegadores baseados em Chromium desde a versão 123.	11 de abril de 2024	Baixar a versão 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d

Versão	Alterações	Data	Link para fazer download
3.12.1	• Corrigida uma ação de estouro de buffer que poderia permitir que um ator local executasse comandos arbitrários com permissões elevadas. • Procedimento de segurança aprimorado.	16 de fevereiro de 2024	Baixar a versão 3.12.1 sha256: 547c4ffd3e35c54db8e0b792aed9de1510f6f31a6009e55b8af4f0c2f5cf31d0
3.12.0	• Problemas de conectividade corrigidos em algumas configurações de LAN.	19 de dezembro de 2023	Baixar a versão 3.12.0 sha256: 9b73987309f1dca1960a322c5dd86eec1568ed270bfd25f78cc430e3b5f85cc1
3.11.0	• Reversão para “Problemas de conectividade corrigidos em algumas configurações de LAN”. • Acessibilidade melhorada.	6 de dezembro de 2023	Baixar a versão 3.11.0 sha256: 86c0fa1bf1c97194082835a739ec7f1c87e540194955f414a35c679b94538970

Versão	Alterações	Data	Link para fazer download
3.10.0	• Problemas de conectividade corrigidos em algumas configurações de LAN. • Acessibilidade melhorada.	6 de dezembro de 2023	Baixar a versão 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	• 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 3.9.0 sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454
3.8.0	• Procedimento de segurança aprimorado.	3 de agosto de 2023	Baixar a versão 3.8.0 sha256: 5fe479236 cc0a1940b a37fe168e 551096f8d ae4c68d45 560a164e4 1edea3e5bd

Versão	Alterações	Data	Link para fazer download
3.7.0	• Procedimento de segurança aprimorado.	15 de julho de 2023	Não é mais compatível
3.6.0	• Reversão das alterações da versão 3.5.0.	15 de julho de 2023	Não é mais compatível
3.5.0	• Procedimento de segurança aprimorado.	14 de julho de 2023	Não é mais compatível
3.4.0	• Foi adicionada compatibilidade com a sinalização “verify-x509-name” da OpenVPN.	14 de fevereiro de 2023	Não é mais compatível
3.1.0	• Corrigido um problema na detecção do tipo de unidade. • Procedimento de segurança aprimorado.	23 de maio de 2022	Não é mais compatível
3.0.0	• 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.
2.0.0	• Foi adicionada compatibilidade com 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.

Versão	Alterações	Data	Link para fazer download
1.0.3	• 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	• Foi adicionado suporte para os sinalizadores do OpenVPN: 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	• Opção habilitada para sair da barra de aplicações do Ubuntu. • Foi adicionada compatibilidade com sinalizadores do OpenVPN: inativo, pull-filter, 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 OpenVPN

É possível estabelecer uma conexão com um endpoint da Client VPN usando aplicações clientes Open VPN comuns. a Client VPN é compatível com os seguintes sistemas operacionais:

- Windows

  Use um certificado e uma chave privada do Windows Certificate Store. Depois de gerar o certificado e a chave, você pode estabelecer uma conexão de AWS cliente usando o aplicativo cliente OpenVPN GUI ou o OpenVPN GUI Connect Client. Para obter as etapas para criar o certificado e a chave, consulte Estabeleça uma conexão VPN usando um certificado no Windows.

- Android e iOS

  Estabeleça uma conexão VPN usando a aplicação cliente OpenVPN em um dispositivo Android ou iOS. Para obter mais informações, consulte Conexões Client VPN no Android e iOS.

- macOS

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

- Linux

  Estabeleça uma conexão VPN no Linux usando a interface OpenVPN - Network Manager ou a aplicação OpenVPN. Para usar a interface OpenVPN - Network Manager, primeiro você precisa instalar o módulo gerenciador de rede, se ainda não estiver instalado. Para obter mais informações, consulte Estabeleça uma conexão VPN no Linux.

Important

Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN. Isso inclui qualquer arquitetura baseada em ARM. Se você estiver usando um dispositivo com um processador ARM (como Apple Silicon Macs ou dispositivos

Windows baseados em ARM), você deve usar endpoints VPN baseados em SAML com o AWS cliente fornecido em vez de clientes OpenVPN.

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 cliente OpenVPN

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

Estas seções descrevem como estabelecer uma conexão VPN usando clientes VPN baseados em Windows.

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

Para obter informações sobre a solução de problemas, consulte Solução de problemas de conexões AWS Client VPN com clientes baseados em Windows.

Important

Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN. Isso inclui qualquer arquitetura baseada em ARM. Se você estiver usando um dispositivo com um processador ARM (como Apple Silicon Macs ou dispositivos Windows baseados em ARM), você deve usar endpoints VPN baseados em SAML com o AWS cliente fornecido em vez de clientes OpenVPN.

Tarefas

- Use um certificado e estabeleça uma conexão AWS Client VPN no Windows

Use um certificado e estabeleça uma conexão AWS Client VPN no Windows

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

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

Para usar 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 snap-in MMC no site da Microsoft.
3. Verifique se sua conta tem permissões para ler o certificado do computador local. É possível usar o Console de Gerenciamento da Microsoft para modificar as permissões. Para obter mais informações, consulte Direitos para ver o armazenamento local de certificados de computador no site da Microsoft.
4. Atualize o arquivo de configuração do OpenVPN e especifique o certificado usando o assunto ou a impressão digital do certificado.

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

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

   Veja a seguir um exemplo de especificação do certificado usando uma impressão digital. É possível 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.

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

5. Depois de concluir a configuração, use o OpenVPN para estabelecer uma conexão VPN seguindo um destes procedimentos:

   - Use a aplicação cliente OpenVPN GUI

     1. Inicie a aplicação cliente OpenVPN.
     2. Na barra de tarefas do Windows, escolha Mostrar/Ocultar ícones. Clique com o botão direito do mouse na GUI do OpenVPN e escolha Importar arquivo.
     3. Na caixa de diálogo Open (Abrir), selecione o arquivo de configuração recebido do administrador da cliente VPN e escolha Open (Abrir).
     4. Na barra de tarefas do Windows, escolha Mostrar/Ocultar ícones. Clique com o botão direito do mouse na GUI do OpenVPN e escolha Conectar.

   - Use o OpenVPN GUI Connect Client

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

AWS Client VPN conexões em aplicativos Android e iOS

> **Important**
>
> Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN. Isso inclui qualquer arquitetura baseada em ARM. Se você estiver usando um dispositivo com um processador ARM (como Apple Silicon Macs ou dispositivos Windows baseados em ARM), você deve usar endpoints VPN baseados em SAML com o AWS cliente fornecido em vez de clientes OpenVPN.

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

> **Note**
>
> Para obter mais informações sobre como baixar e usar a aplicação cliente OpenVPN para iOS ou Android, consulte o Guia do usuário do OpenVPN Connect no site do OpenVPN.

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

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

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

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

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

Para obter informações sobre a solução de problemas, consulte Solução de problemas de conexões AWS Client VPN com clientes macOS.

> **Important**
>
> Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN. Isso inclui qualquer arquitetura baseada em ARM. Se você estiver usando um dispositivo com um processador ARM (como Apple Silicon Macs ou dispositivos Windows baseados em ARM), você deve usar endpoints VPN baseados em SAML com o AWS cliente fornecido em vez de clientes OpenVPN.

Tópicos

- Estabeleça uma AWS Client VPN conexão no macOS

Estabeleça uma AWS Client VPN conexão no macOS

Você pode estabelecer uma conexão VPN 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 conexão VPN 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 recebido do administrador da VPN no painel Configurations (Configurações).
3. Selecione o arquivo de configuração no painel Configurations (Configurações) e escolha Connect (Conectar).

Para estabelecer uma conexão VPN usando o AWS Client VPN.

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

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

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

Antes de começar, certifique-se de que o administrador da Client VPN criou um endpoint da Client VPN e forneceu o arquivo de configuração do endpoint da Client VPN. Se você quiser se conectar a vários perfis simultaneamente, precisará de um arquivo de configuração para cada perfil.

Para obter informações sobre a solução de problemas, consulte Solução de problemas de conexões AWS Client VPN com clientes baseados em Linux.

> **Important**
>
> Se o endpoint da cliente VPN foi configurado para usar a autenticação federada baseada em SAML, não será possível usar a cliente VPN baseada no OpenVPN para se conectar a um endpoint da cliente VPN. Isso inclui qualquer arquitetura baseada em ARM. Se você estiver usando um dispositivo com um processador ARM (como Apple Silicon Macs ou dispositivos Windows baseados em ARM), você deve usar endpoints VPN baseados em SAML com o AWS cliente fornecido em vez de clientes OpenVPN.

Tópicos

Estabeleça uma AWS Client VPN conexão no Linux

Estabeleça uma conexão VPN usando a GUI do Network Manager em um computador Ubuntu ou a aplicação OpenVPN.

Para estabelecer uma conexão VPN usando o OpenVPN - 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 VPN e escolha Import from file... (Importar do arquivo...).
4. Navegue até o arquivo de configuração que você recebeu do administrador da VPN e escolha Open (Abrir).
5. Na janela Add VPN (Adicionar VPN), escolha Add (Adicionar).
6. Inicie a conexão habilitando o seletor ao lado do perfil de VPN que você adicionou.

Para estabelecer uma conexão VPN usando o OpenVPN

1. Instale o OpenVPN usando o comando a seguir.

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

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

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

Solução de problemas de conexões AWS Client VPN

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

Tópicos

Solução de problemas do endpoint da VPN do Cliente para administradores

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

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

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 logs 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 janelaEnviar logs de diagnóstico, execute uma das seguintes operações:

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

   Ao entrar em contato 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 a área de transferência.

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

Solução de problemas de conexões AWS Client VPN 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 de 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 aplicações: contêm informações sobre a aplicação. Esses logs são prefixados com "aws_vpn_client_".
- Logs do OpenVPN: contêm informações sobre os processos do OpenVPN. Esses logs são prefixados com "ovpn_aws_vpn_client_".

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

- GUI do OpenVPN
- Cliente OpenVPN Connect
- Não é possível resolver o DNS
- Pseudônimo do PKI ausente

O cliente não consegue se conectar

Problema

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

Causa

A causa desse problema pode ser uma das seguintes:

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

Solução

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

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

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

Problema

O cliente AWS fornecido não consegue se conectar ao endpoint do Client VPN e a seguinte mensagem de erro aparece nos registros do aplicativo: “Não há adaptadores TAP-Windows neste sistema. Você conseguirá 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 adaptador TAP-Windows.

O cliente está travado em um estado de reconexão

Problema

O cliente AWS fornecido está tentando se conectar ao endpoint do Client VPN, 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 nome de host DNS não resolve para um endereço IP.
- Um processo OpenVPN está tentando se conectar ao endpoint indefinidamente.

Solução

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

O processo de conexão VPN é encerrado inesperadamente

Problema

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

Causa

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

Solução

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

Falha ao iniciar a aplicação

Problema

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

Causa

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

Solução

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

Solução

Certifique-se de que o administrador de Client VPN 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 .

VPN se desconecta com uma mensagem pop-up

Problema

A VPN é desconectada com uma mensagem pop-up que diz: “A conexão VPN está sendo encerrada porque o espaço de endereço da rede local à qual seu dispositivo está conectado foi alterado. Estabeleça uma nova conexão VPN.”

Causa

O adaptador TAP-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 configuração de

VPN. 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.DBRBackupOverlayIcon.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
- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.dll

Solução

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

Além disso, siga um destes procedimentos:

- Se estiver utilizando a aplicação 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 da aplicação.
- Se você não estiver usando a aplicação Dell Backup and Recovery, algumas ações ainda precisarão ser tomadas se você estiver enfrentando esse problema. Se você não quiser atualizar a

aplicação, como alternativa, você pode excluir ou renomear os arquivos DLL. No entanto, observe que isso impedirá que a aplicação Dell Backup and Recovery funcione completamente.

Excluir ou renomear os arquivos DLL

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

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

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

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

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

GUI do OpenVPN

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

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

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

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

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

Cliente OpenVPN Connect

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

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

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

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

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

Não é possível resolver o DNS

Problema

A conexão falha com o erro a seguir.

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

Causa

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

Solução

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

Pseudônimo do PKI ausente

Problema

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

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

Causa

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

Solução

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

Solução de problemas de conexões AWS Client VPN 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 aplicações: contêm informações sobre a aplicação. Esses logs são prefixados com "aws_vpn_client_".
- Logs do OpenVPN: contêm informações sobre os processos do OpenVPN. Esses logs são prefixados com "ovpn_aws_vpn_client_".

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

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

```
/var/log/AWSVPNClient/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

Problema

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

Causa

A causa desse problema pode ser uma das seguintes:

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

Solução

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

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

O cliente está travado em um estado de reconexão

Problema

O cliente AWS fornecido está tentando se conectar ao endpoint do Client VPN, 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 nome de host DNS não resolve para um endereço IP.
- Um processo OpenVPN está tentando se conectar ao endpoint indefinidamente.

Solução

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

O cliente não consegue criar um perfil

Problema

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

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

Causa

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

Solução

Certifique-se de que o administrador de Client VPN 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 a VPN.

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

Solução

Veja o seguinte artigo no AWS re:POST. AWS VPN Client — A ferramenta auxiliar é um erro obrigatório

Tunnelblick

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

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

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

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

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

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

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

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

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

Problema

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

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

Causa

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

Solução

Escolha uma versão compatível do OpenVPN fazendo o seguinte:

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

A conexão para de responder e é redefinida

Problema

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

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
```

```
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

Causa

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

Solução

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

Uso estendido de chave (EKU)

Problema

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

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

Causa

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

Solução

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

Certificado expirado

Problema

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

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

Causa

A validade do certificado do cliente expirou.

Solução

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

OpenVPN

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

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

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

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

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

Não é possível resolver o DNS

Problema

A conexão falha com o erro a seguir.

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

Causa

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

Solução

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

Solução de problemas de conexões AWS Client VPN 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
- As consultas ao DNS vão para um servidor de nomes padrão
- OpenVPN (linha de comando)
- OpenVPN pelo gerenciador de rede (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 up/down scripts de DNS que causam a falha da conexão:

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

As consultas ao DNS vão para um servidor de nomes padrão

Problema

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

Causa

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

Solução

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

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

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

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

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

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

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

OpenVPN (linha de comando)

Problema

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

Causa

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

Solução

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

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

   ```
   Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
   WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
    'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
   ```

```
gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
 10.0.0.98 255.255.255.224,peer-id 0
```

Se não houver nenhum servidor DNS especificado, peça ao administrador de VPN do Cliente para modificar o endpoint da VPN do Cliente e verifique se um servidor DNS (por exemplo, o servidor DNS da VPC) foi especificado para o endpoint da VPN do Cliente. Para obter mais informações, consulte Endpoints da cliente VPN no Guia do administrador da AWS Client VPN .

2. Certifique-se de que o pacote `resolvconf` esteja instalado executando o comando a seguir.

```
sudo apt list resolvconf
```

A saída deve retornar o seguinte:

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

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

```
sudo apt install resolvconf
```

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

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

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

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

OpenVPN pelo gerenciador de rede (GUI)

Problema

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

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

Causa

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

Solução

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

Solução de problemas comuns AWS do Client VPN

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

Falha na negociação de chave TLS

Problema

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

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

Causa

A causa desse problema pode ser uma das seguintes:

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

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

Solução

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

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

Histórico do documento

A tabela a seguir descreve as atualizações do AWS Client VPN User Guide.

Alteração	Descrição	Data
AWS cliente fornecido (5.2.1) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	18 de junho de 2025
AWS cliente fornecido (5.2.2) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	2 de junho de 2025
AWS cliente fornecido (5.2.1) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	21 de abril de 2025
AWS cliente fornecido (5.2.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	8 de abril de 2025
AWS cliente fornecido (5.2.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	8 de abril de 2025
AWS cliente fornecido (5.2.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	8 de abril de 2025
AWS cliente fornecido (5.1.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	17 de março de 2025
AWS cliente fornecido (5.1.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	17 de março de 2025

AWS cliente fornecido (5.1.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	17 de março de 2025
Suporte removido para macOS Monterey e suporte adicionado para macOS Sonoma (14.0)	Consulte os requisitos do Client VPN para macOS para obter detalhes.	12 de março de 2025
Suporte removido para Ubuntu 18.0.4 (LTS) e Ubuntu 20.04 LTS (somente) AMD64	Consulte Requisitos do Client VPN para Linux para obter detalhes.	12 de março de 2025
AWS cliente fornecido (5.0.3) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	6 de março de 2025
AWS cliente fornecido (5.0.2) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	24 de fevereiro de 2025
AWS cliente fornecido (5.0.2) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	17 de fevereiro de 2025
AWS cliente fornecido (5.0.1) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	30 de janeiro de 2025
AWS cliente fornecido (5.0.1) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	22 de janeiro de 2025
O cliente AWS fornecido agora suporta até cinco conexões simultâneas	Consulte Support para conexões simultâneas usando um cliente AWS fornecido para obter detalhes.	21 de janeiro de 2025

AWS cliente fornecido (5.0.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	21 de janeiro de 2025
AWS cliente fornecido (5.0.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	21 de janeiro de 2025
AWS cliente fornecido (5.0.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de novembro de 2024
AWS cliente fornecido (4.1.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de novembro de 2024
AWS cliente fornecido (4.1.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de novembro de 2024
AWS cliente fornecido (4.1.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de novembro de 2024
AWS cliente fornecido (4.0.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (4.0.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (4.0.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	25 de setembro de 2024
AWS cliente fornecido (3.15.1) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	4 de setembro de 2024

AWS cliente fornecido (3.14.2) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	4 de setembro de 2024
AWS cliente fornecido (3.12.1) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	4 de setembro de 2024
AWS cliente fornecido (3.14.1) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	22 de agosto de 2024
AWS cliente fornecido (3.15.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.14.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.12.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	12 de agosto de 2024
AWS cliente fornecido (3.14.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	29 de julho de 2024
AWS cliente fornecido (3.13.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	29 de julho de 2024
AWS cliente fornecido (3.11.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	29 de julho de 2024
AWS cliente fornecido (3.12.1) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	18 de julho de 2024

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

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

AWS cliente fornecido (3.8.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.7.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.7.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.6.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.6.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.5.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	15 de julho de 2023
AWS cliente fornecido (3.6.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.5.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.4.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	14 de julho de 2023
AWS cliente fornecido (3.3.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	27 de abril de 2023

AWS cliente fornecido (3.5.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	3 de abril de 2023
AWS cliente fornecido (3.4.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	28 de março de 2023
AWS cliente fornecido (3.3.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	17 de março de 2023
AWS cliente fornecido (3.4.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	14 de fevereiro de 2023
AWS cliente fornecido (3.2.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	23 de janeiro de 2023
AWS cliente fornecido (3.2.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	23 de janeiro de 2023
AWS cliente fornecido (3.1.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.1.0) para Windows lançado	Consulte as notas de lançamento completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.1.0) para Ubuntu lançado	Consulte as notas de lançamento completas para obter detalhes.	23 de maio de 2022
AWS cliente fornecido (3.0.0) para macOS lançado	Consulte as notas de lançamento completas para obter detalhes.	3 de março de 2022

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

AWS cliente fornecido para Ubuntu 18.04 LTS e Ubuntu 20.04 LTS lançado	Você pode usar o cliente AWS fornecido no Ubuntu 18.04 LTS e no Ubuntu 20.04 LTS.	11 de junho de 2021
Compatibilidade com o OpenVPN usando um certificado da Windows Certificate System Store	É possível usar o OpenVPN usando um certificado da Windows Certificate System Store.	25 de fevereiro de 2021
Portal de autoatendimento	Você pode acessar um portal de autoatendimento para obter o cliente 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 endpoint Client VPN.	4 de fevereiro de 2020
Lançamento inicial	Esta versão apresenta o AWS Client VPN.	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.