

---

# AWS Client VPN

Guia do administrador



## AWS Client VPN: Guia do administrador

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

## Table of Contents

O que é o AWS Client VPN .....	1
Recursos do Client VPN .....	1
Componentes do Client VPN .....	1
Como acessar o Client VPN .....	2
Limitações do Client VPN .....	3
Definição de preços do Client VPN .....	3
Como Client VPN funciona .....	4
Autorização e autenticação de clientes .....	5
Autenticação .....	5
Autorização .....	7
Client VPN de túnel dividido .....	8
Benefícios do túnel dividido em endpoints do AWS Client VPN .....	8
Considerações sobre roteamento de endpoint de túnel dividido do AWS Client VPN .....	8
Uso de funções vinculadas a serviço .....	8
Permissões da função vinculada ao serviço para o Client VPN .....	8
Criar uma função vinculada ao serviço para o Client VPN .....	9
Editar uma função vinculada ao serviço para o Client VPN .....	9
Excluir uma função vinculada ao serviço para o Client VPN .....	9
Cenários e exemplos .....	11
Acesso a uma VPC .....	11
Acesso a uma VPC emparelhada .....	13
Acesso a uma rede no local .....	15
Acesso à Internet .....	17
Restringir o acesso a recursos específicos na sua VPC .....	19
Conceder acesso somente para a clientes do Client VPN .....	19
Negar acesso a clientes do Client VPN .....	20
Conceitos básicos .....	21
Pré-requisitos .....	21
Etapa 1: gerar chaves e certificados de servidor e cliente .....	21
Etapa 2: criar um endpoint do Client VPN .....	21
Etapa 3: habilitar a conectividade de VPN para clientes .....	23
Etapa 4: autorizar os clientes a acessar uma rede .....	23
Etapa 5: (opcional) habilitar o acesso a redes adicionais .....	24
Etapa 6: fazer download do arquivo de configuração do endpoint do Client VPN .....	24
Passo 7: conectar-se ao endpoint do Client VPN .....	26
Trabalho com o Client VPN .....	27
Endpoints do Client VPN .....	27
Criar um endpoint do Client VPN .....	27
Modificar um endpoint do Client VPN .....	29
Exportar a configuração do cliente .....	30
Visualizar endpoints do Client VPN .....	31
Excluir um endpoint do Client VPN .....	31
Redes de destino .....	31
Associar uma rede de destino a um endpoint do Client VPN .....	31
Aplicar um grupo de segurança a uma rede de destino .....	32
Desassociar uma rede de destino de um endpoint do Client VPN .....	33
Visualizar redes de destino .....	33
Regras de autorização .....	33
Adicionar uma regra de autorização a um endpoint do Client VPN .....	34
Remover uma regra de autorização de um endpoint do Client VPN .....	34
Visualizar regras de autorização .....	35
Rotas .....	35
Considerações sobre túnel dividido no endpoint do AWS Client VPN .....	35
Criar uma rota de endpoint .....	36

---

Visualizar rotas de endpoint .....	36
Excluir uma rota de endpoint .....	36
Listas de revogação de certificados de cliente .....	37
Gerar uma lista de revogação de certificados de cliente .....	37
Importar uma lista de revogação de certificados de cliente .....	38
Exportar uma lista de revogação de certificados de cliente .....	38
Conexões de cliente .....	38
Visualizar conexões de clientes .....	39
Encerrar uma conexão de cliente .....	39
Identity and Access Management for Client VPN .....	40
Monitorar o Client VPN .....	42
Monitorar com o CloudWatch .....	42
Monitorar com o CloudTrail .....	43
Informações sobre o Client VPN no CloudTrail .....	43
Noções básicas sobre as entradas dos arquivos de log do Client VPN .....	44
Cotas de Client VPN .....	45
Solução de problemas do AWS Client VPN .....	46
Não é possível resolver o nome DNS do endpoint do Client VPN .....	46
O tráfego não está sendo dividido entre as sub-redes .....	46
Regras de autorização para grupos do Active Directory não funcionando conforme esperado .....	47
Os clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet .....	48
O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente .....	50
O software cliente retorna erro TLS .....	51
O software cliente retorna erros de nome de usuário e senha (autenticação do Active Directory) .....	52
Clientes não conseguem se conectar (autenticação mútua) .....	52
Histórico do documento .....	53

# O que é o AWS Client VPN?

O AWS Client VPN é um serviço de VPN gerenciado no cliente que protege o acesso aos recursos da AWS na sua rede local. Com o Client VPN, você pode acessar seus recursos de qualquer local usando um cliente de VPN com base no OpenVPN.

## Tópicos

- [Recursos do Client VPN \(p. 1\)](#)
- [Componentes do Client VPN \(p. 1\)](#)
- [Como acessar o Client VPN \(p. 2\)](#)
- [Limitações do Client VPN \(p. 3\)](#)
- [Definição de preços do Client VPN \(p. 3\)](#)

## Recursos do Client VPN

O Client VPN oferece os seguintes recursos e funcionalidades:

- **Conexões seguras** — ele fornece uma conexão TLS segura de qualquer local usando o cliente OpenVPN.
- **Serviço gerenciado** — É um serviço gerenciado da AWS e, como tal, remove o peso operacional da implantação e do gerenciamento de uma solução de VPN com acesso remoto de terceiros.
- **Altamente disponível e elástico** — é escalado automaticamente para o número de usuários que se conectam aos seus recursos da AWS e aos recursos no local.
- **Autenticação** — Oferece suporte para autenticação de cliente usando o Active Directory e para autenticação baseada em certificado.
- **Controle granular** — permite implementar controles de segurança personalizados definindo regras de acesso baseadas na rede. Essas regras podem ser configuradas na granularidade dos grupos do Active Directory. Você também pode implementar o controle de acesso usando grupos de segurança.
- **Facilidade de uso** — Permite que você acesse seus recursos da AWS e recursos locais usando um único túnel VPN.
- **Capacidade de gerenciamento** — Permite que você visualize logs de conexão, que fornecem detalhes sobre tentativas de conexão de clientes. Você também pode gerenciar conexões de clientes ativas, com a capacidade de encerrá-las.
- **Integração profunda** — Integra-se aos serviços da AWS existentes, incluindo o AWS Directory Service e o Amazon VPC.

## Componentes do Client VPN

Veja a seguir os conceitos-chave do Client VPN:

### Endpoint do Client VPN

O endpoint do Client VPN é o recurso que você cria e configura para habilitar e gerenciar sessões de VPN de clientes. Ele é o recurso no qual todas as sessões de VPN de cliente são encerradas.

### Rede de destino

Uma rede de destino é a rede que você associa a um endpoint do Client VPN. Uma sub-rede de uma VPC é uma rede de destino. Associar uma sub-rede a um endpoint do Client VPN permite

estabelecer sessões de VPN. Você pode associar várias sub-redes a um endpoint Client VPN para alta disponibilidade. Todas as sub-redes devem ser provenientes da mesma VPC. Cada sub-rede deve pertencer a uma Zona de disponibilidade diferente.

#### Rota

Cada endpoint do Client VPN tem uma tabela de rotas que descreve as rotas de redes de destino disponíveis. Cada rota na tabela de rotas especifica o caminho do tráfego para recursos ou redes específicos.

#### Regras de autorização

Uma regra de autorização restringe os usuários que podem acessar uma rede. Para uma rede especificada, você configura o grupo do Active Directory que tem permissão de acesso. Somente os usuários pertencentes a esse grupo do Active Directory podem acessar a rede especificada. Por padrão, não há regras de autorização, e você deve configurá-las para permitir que os usuários acessem recursos e redes.

#### Cliente

O usuário final que se conecta ao endpoint do Client VPN para estabelecer uma sessão de VPN. Para estabelecerem uma sessão de VPN, os usuários finais precisam fazer download de um cliente OpenVPN e usar o arquivo de configuração do Client VPN que você criou.

#### Portas VPN do cliente

O AWS Client VPN é compatível com as portas 443 e 1194 para TCP e UDP. O padrão é a porta 443.

#### Interfaces de rede do Client VPN

Quando você associa uma sub-rede ao endpoint do Client VPN, criamos interfaces de rede do Client VPN nessa sub-rede. O tráfego enviado para a VPC do endpoint do Client VPN é enviado por meio de uma interface de rede do Client VPN. A conversão de endereço de rede de origem (SNAT) é aplicada e o endereço IP de origem é convertido para o endereço IP da interface de rede do Client VPN.

## Como acessar o Client VPN

Você pode trabalhar com o Client VPN de qualquer uma das seguintes formas:

#### Console do Amazon VPC

O console do Amazon VPC fornece uma interface de usuário baseada na web para o Client VPN. Se você estiver cadastrado para uma conta da AWS, poderá fazer login no console da [Amazon VPC](#) e selecionar Client VPN no painel de navegação.

#### AWS Command Line Interface (&CLI)

A AWS CLI fornece acesso direto às APIs públicas do Client VPN. É compatível com Windows, macOS e Linux. Para obter mais informações sobre os conceitos básicos da AWS CLI, consulte o [Guia do usuário do AWS Command Line Interface](#). Para mais informações sobre os comandos do Client VPN, consulte [AWS CLI Command Reference](#).

#### AWS Tools para Windows PowerShell

A AWS fornece comandos para um amplo conjunto de ofertas da AWS voltadas a usuários que desenvolvem scripts no ambiente do PowerShell. Para obter mais informações sobre os conceitos básicos do AWS Tools para Windows PowerShell, consulte o [Guia do usuário do AWS Tools para Windows PowerShell](#). Para obter mais informações sobre os cmdlets do Client VPN, consulte a [Referência de cmdlets do AWS Tools para Windows PowerShell](#).

#### API de consulta

A API de consulta HTTPS do Client VPN proporciona acesso programático ao Client VPN e à AWS. A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço.

Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para mais informações, consulte a [Referência da API do Client VPN](#).

## Limitações do Client VPN

O Client VPN tem as seguintes regras e limitações:

- Os intervalos CIDR de cliente não podem se sobrepor ao CIDR local da VPC na qual a sub-rede associada está localizada ou a quaisquer rotas adicionadas manualmente à tabela de rotas do endpoint do Client VPN.
- Os intervalos de CIDRs do cliente devem ter um tamanho de bloco de pelo menos /22 e não deve ser maior que /12.
- Uma parte dos endereços no intervalo e CIDRs do cliente é usada para oferecer suporte ao modelo de disponibilidade do endpoint do Client VPN e não pode ser atribuída aos clientes. Portanto, é recomendável atribuir um bloco CIDR que contenha o dobro do número de endereços IP necessários para habilitar o número máximo de conexões simultâneas às quais você planeja oferecer suporte no endpoint do Client VPN.
- O intervalo CIDR do cliente não pode ser alterado depois de criar o endpoint do Client VPN.
- O endpoint do Client VPN e a VPC na qual a sub-rede associada está localizada devem pertencer à mesma conta.
- As sub-redes associadas a um endpoint do Client VPN deve estar na mesma VPC.
- Você não pode associar várias sub-redes da mesma Zona de disponibilidade a um endpoint do Client VPN.
- O Client VPN oferece suporte somente para tráfego IPv4.
- O Client VPN não é compatível com a lei HIPAA (Health Insurance Portability and Accountability Act) ou o FIPS (Federal Information Processing Standards).
- Se a autenticação multifator (MFA) estiver desabilitada para o Active Directory, uma senha de usuário não poderá estar no seguinte formato.

```
SCRV1:<base64_encoded_string>:<base64_encoded_string>
```

## Definição de preços do Client VPN

Você é cobrado por cada associação ativa por endpoint do Client VPN de hora em hora. O faturamento é proporcional à hora.

Você será cobrado por cada conexão VPN de cliente por hora. O faturamento é proporcional à hora.

Para obter mais informações, consulte [Definição de preço do AWS Client VPN](#).

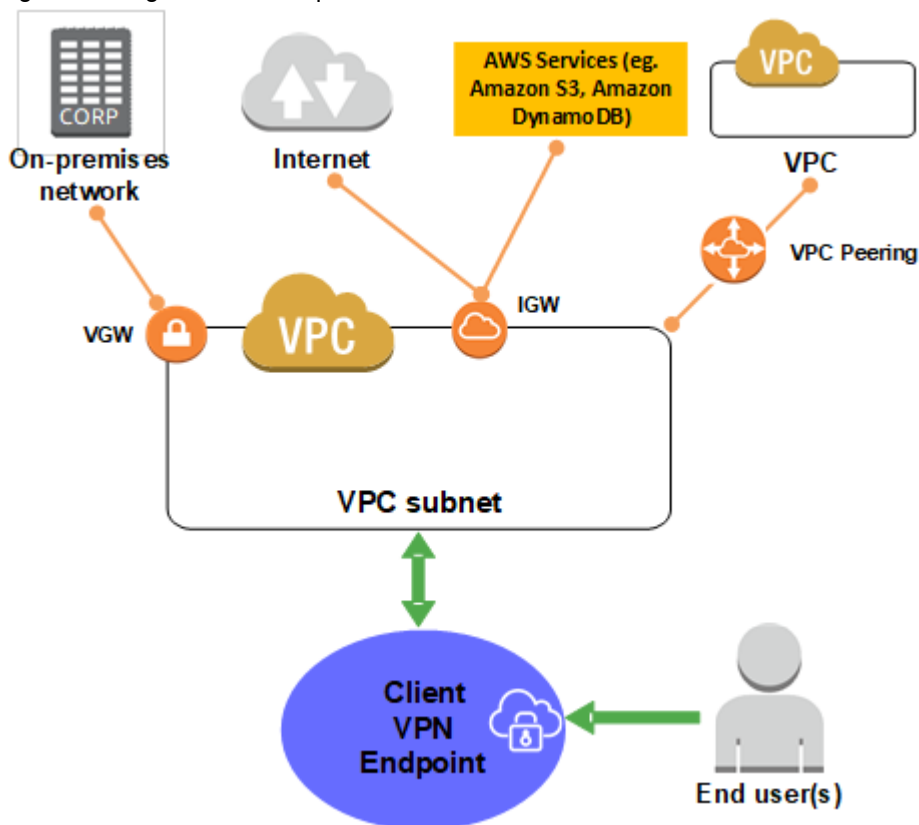
# Como AWS Client VPN funciona

Com o AWS Client VPN, há dois tipos de personas de usuário que interagem com o endpoint do Client VPN: administradores e clientes.

O administrador é responsável por criar e configurar o serviço. Isso envolve criar o endpoint do Client VPN, associar a rede de destino, configurar as regras de autorização e configurar rotas adicionais (se necessário). Depois que o endpoint do Client VPN é criado e configurado, o administrador faz download do arquivo de configuração do endpoint do Client VPN e o distribui aos clientes que precisam de acesso. O arquivo de configuração do endpoint do Client VPN inclui o nome DNS do endpoint do Client VPN e as informações de certificado necessárias para estabelecer uma sessão de VPN. Para obter mais informações sobre a configuração do serviço, consulte [Conceitos básicos do Client VPN \(p. 21\)](#).

O cliente é o usuário final. É a pessoa que se conecta ao endpoint do Client VPN para estabelecer uma sessão de VPN. O cliente estabelece a sessão de VPN em seu computador local ou dispositivo móvel usando um aplicativo cliente de VPN baseado no OpenVPN. Depois de estabelecer a sessão de VPN, ele pode acessar com segurança os recursos na VPC em que a sub-rede associada está localizada. Ele também poderá acessar outros recursos na AWS ou uma rede local, se a rota necessária e as devidas regras de autorização tiverem sido configuradas. Para obter mais informações sobre como se conectar a um endpoint do Client VPN para estabelecer uma sessão de VPN, consulte [Conceitos básicos](#) no Guia do usuário do AWS Client VPN.

O gráfico a seguir ilustra a arquitetura básica do Client VPN.





# Autorização e autenticação de clientes

O Client VPN fornece recursos de autenticação e autorização.

## Tópicos

- [Autenticação \(p. 5\)](#)
- [Autorização \(p. 7\)](#)

## Autenticação

A autenticação é implementada no primeiro ponto de entrada na Nuvem AWS. Ela é usada para determinar se os clientes têm permissão para se conectar ao endpoint do Client VPN. Se a autenticação for bem-sucedida, os clientes se conectarão ao endpoint do Client VPN e estabelecerão uma sessão de VPN. Se a autenticação falhar, a conexão será negada, e o cliente será impedido de estabelecer uma sessão de VPN.

O Client VPN oferece dois tipos de autenticação de cliente: autenticação via Active Directory e autenticação mútua. Você pode optar por usar um ou ambos os métodos de autenticação.

## Autenticação do Active Directory

O Client VPN fornece suporte ao Active Directory por meio da integração com o AWS Directory Service. Com a autenticação via Active Directory, os clientes são autenticados com grupos existentes do Active Directory. Usando o AWS Directory Service, o Client VPN pode se conectar a Active Directories provisionados na AWS ou na sua rede local. Isso permite que você use sua infraestrutura de autenticação de cliente existente. Se você estiver usando um Active Directory no local e não tiver um AWS Managed Microsoft AD existente, será necessário configurar um Active Directory Connector (AD Connector). Você pode usar um servidor do Active Directory para autenticar os usuários. Para mais informações, consulte o [AWS Directory Service Administration Guide](#).

Para criar um endpoint do Client VPN, você deve provisionar um certificado de servidor no AWS Certificate Manager. Para obter mais informações sobre como criar e provisionar um certificado de servidor, consulte as etapas em [Autenticação mútua \(p. 5\)](#).

O Client VPN é compatível com a autenticação multifator (MFA) quando ela está habilitada para o AWS Managed Microsoft AD ou o AD Connector. Se a MFA estiver habilitada, os clientes devem inserir um nome de usuário, senha e código MFA ao se conectarem a um endpoint do Client VPN. Para obter mais informações sobre como habilitar a MFA, consulte [Habilitar a autenticação multifator para o AWS Managed Microsoft AD](#) e [Habilitar a autenticação multifator para o AD Connector](#) no AWS Directory Service Administration Guide.

## Autenticação mútua

Com a autenticação mútua, o Client VPN usa certificados para realizar a autenticação entre o cliente e o servidor. Os certificados são uma forma digital de identificação emitida por uma autoridade certificadora (CA). O servidor usa certificados de cliente para autenticar clientes quando eles tentam se conectar ao endpoint do Client VPN. Os certificados de servidor e cliente devem ser obtidos por upload no AWS Certificate Manager (ACM). Para obter mais informações sobre o provisionamento e o upload de certificados no ACM, consulte o [Guia do usuário do AWS Certificate Manager](#).

Você só precisa fazer upload do certificado de cliente no ACM quando a Autoridade de certificação (emissor) do certificado de cliente é diferente da Autoridade de certificação (emissor) do certificado de servidor.

Você pode criar um certificado de cliente separado e uma chave para cada cliente que se conectará ao endpoint do Client VPN. Isso permite revogar um certificado de cliente específico se um usuário sair de sua organização.

Um endpoint do Client VPN é compatível apenas com tamanhos de chave RSA de 1024 bits e 2048 bits.

O procedimento a seguir usa o OpenVPN easy-rsa para gerar os certificados e as chaves de servidor e cliente e, em seguida, faz upload do certificado e da chave de servidor no ACM. Para obter mais informações, consulte o [LEIAME de início rápido do Easy-RSA 3](#). Os procedimentos a seguir exigem o OpenSSL.

Para gerar os certificados e as chaves de servidor e cliente e transferi-los por upload ao ACM

1. (Linux) Clone o repositório easy-rsa do OpenVPN para o computador local e navegue até a pasta easy-rsa/easyrsa3.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

(Windows) Faça download da versão mais recente para o Windows em <https://github.com/OpenVPN/easy-rsa/releases>. Descompacte a pasta e execute o arquivo EasyRSA-Start.bat.

2. Inicialize um novo ambiente PKI.

```
$ ./easyrsa init-pki
```

3. Crie uma nova autoridade de certificação (CA).

```
$ ./easyrsa build-ca nopass
```

Siga as instruções para criar a CA.

4. Gere o certificado e a chave de servidor.

```
$ ./easyrsa build-server-full server nopass
```

5. Gere o certificado e a chave de cliente.

Certifique-se de salvar o certificado de cliente e a chave privada de cliente, pois você precisará deles ao configurar o cliente.

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

Opcionalmente, você pode repetir essa etapa para cada cliente (usuário final) que exija um certificado e uma chave de cliente.

6. Copie os certificados e as chaves de servidor e de cliente para uma pasta personalizada e depois navegue até ela.

Antes de copiar os certificados e as chaves, crie a pasta personalizada usando o comando `mkdir`. O exemplo a seguir cria uma pasta personalizada em seu diretório base.

```
$ mkdir ~/custom_folder/  
$ cp pki/ca.crt ~/custom_folder/  
$ cp pki/issued/server.crt ~/custom_folder/  
$ cp pki/private/server.key ~/custom_folder/  
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
```

```
$ cp pki/private/client1.domain.tld.key ~/custom_folder/  
$ cd ~/custom_folder/
```

7. Faça upload do certificado e da chave do servidor e do certificado e da chave do cliente no ACM. Os seguintes comandos usam a AWS CLI.

```
$ aws acm import-certificate --certificate file://server.crt --private-key file://  
server.key --certificate-chain file://ca.crt --region region
```

```
$ aws acm import-certificate --certificate file://client1.domain.tld.crt --private-key  
file://client1.domain.tld.key --certificate-chain file://ca.crt --region region
```

Para fazer upload dos certificados usando o console do ACM, consulte [Importar um certificado](#) no Guia do usuário do AWS Certificate Manager.

#### Note

Certifique-se de fazer upload dos certificados e das chaves na mesma região em que você pretende criar o endpoint do Client VPN.

Se estiver usando a AWS CLI versão 2, use o prefixo `fileb://` em vez do prefixo `file://`.

Para obter mais informações, consulte [Informações sobre a migração da AWS CLI versão 2](#) no Guia do usuário do AWS Command Line Interface.

## Autorização

O Client VPN oferece suporte a dois tipos de autorização: grupos de segurança e autorização com base na rede (usando regras de autorização).

### Grupos de segurança

O Client VPN se integra automaticamente aos grupos de segurança da VPC. Os grupos de segurança estão associados às interfaces de rede do Client VPN. Ao criar um endpoint do Client VPN, você pode especificar os grupos de segurança de uma VPC específica a serem aplicados ao endpoint do Client VPN. Quando você associa uma sub-rede a um endpoint do Client VPN, aplicamos automaticamente o grupo de segurança padrão da VPC. Você pode alterar os grupos de segurança depois de criar o endpoint do Client VPN.

Você pode permitir que os usuários do Client VPN acessem seus aplicativos em uma VPC adicionando uma regra aos grupos de segurança para permitir o tráfego do grupo de segurança que foi aplicado à associação. De maneira oposta, você pode restringir o acesso para usuários do Client VPN ao não especificar o grupo de segurança que foi aplicado à associação. Para obter mais informações, consulte [Aplicar um grupo de segurança a uma rede de destino \(p. 32\)](#). As regras de grupo de segurança de que você precisa também podem depender do tipo de acesso VPN que você deseja configurar. Para obter mais informações, consulte [Cenários e exemplos \(p. 11\)](#).

Para obter mais informações sobre grupos de segurança, consulte [Grupos de segurança para sua VPC](#) no Guia do usuário da Amazon VPC.

### Autorização com base em rede

A autorização com base em rede é implementada com o uso de regras de autorização. Para cada rede à qual você deseja habilitar o acesso, é necessário configurar regras de autorização que limitam os usuários que têm esse acesso. Para uma rede especificada, você configura o grupo do Active Directory que tem permissão de acesso. Somente os usuários que pertencerem ao grupo do Active Directory especificado poderão acessar a rede especificada. Se você não estiver usando o Active Directory ou se quiser abrir o

acesso a todos os usuários, poderá especificar uma regra que conceda acesso a todos os clientes. Para obter mais informações, consulte [Regras de autorização \(p. 33\)](#).

## Túnel dividido em endpoints do AWS Client VPN

Por padrão, quando você tem um endpoint do AWS Client VPN, todo o tráfego do cliente é roteado pelo túnel do AWS Client VPN. Quando você habilita o túnel dividido no endpoint do AWS Client VPN, as rotas são enviadas por push na tabela de rotas do endpoint do AWS Client VPN para o dispositivo que está conectado ao AWS Client VPN. Isso garante que somente o tráfego com um destino para a rede correspondente a uma rota da tabela de rotas do endpoint do AWS Client VPN seja roteado por meio do túnel do Client VPN.

Você poderá usar um endpoint de túnel dividido do AWS Client VPN quando não quiser que todo o tráfego de usuário seja roteado pelo endpoint do AWS Client VPN.

### Benefícios do túnel dividido em endpoints do AWS Client VPN

O túnel dividido em endpoints do AWS Client VPN oferece os seguintes benefícios:

- Com o túnel dividido, os clientes podem otimizar o roteamento do tráfego do cliente, fazendo com que apenas o tráfego destinado pela AWS atravesse o túnel da VPN.
- Ao otimizar o tráfego, os clientes também reduzem o volume do tráfego de saída da AWS, reduzindo, portanto, o custo da transferência de dados.

### Considerações sobre roteamento de endpoint de túnel dividido do AWS Client VPN

Quando você habilita o túnel dividido em um endpoint do AWS Client VPN, todas as rotas que estão nas tabelas de rotas do AWS Client VPN são adicionadas à tabela de rotas do cliente quando a VPN é estabelecida. Essa operação é diferente da operação do endpoint do AWS Client VPN padrão, que substitui a tabela de rotas do cliente pela entrada 0.0.0.0/0 para rotear todo o tráfego pela VPN.

## Usar funções vinculadas ao serviço para o Client VPN

O AWS Client VPN usa uma função vinculada a serviço para as permissões das quais ele precisa para chamar outros serviços da AWS em seu nome. Para obter mais informações, consulte [Uso de funções vinculadas ao serviço](#) no Guia do usuário do IAM.

### Permissões da função vinculada ao serviço para o Client VPN

O AWS Client VPN usa a função vinculada a serviço `AWSServiceRoleForClientVPN` para chamar as seguintes ações em seu nome quando você trabalha com endpoints do Client VPN:

- `ec2:CreateNetworkInterface`

- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeInternetGateways`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ds:AuthorizeApplication`
- `ds:DescribeDirectories`
- `ds:GetDirectoryLimits`
- `ds:ListAuthorizedApplications`
- `ds:UnauthorizeApplication`
- `logs:DescribeLogStreams`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogGroups`
- `acm:GetCertificate`
- `acm:DescribeCertificate`

Essa função vinculada a serviço `AWSServiceRoleForClientVPN` confia no principal `clientvpn.amazonaws.com` para assumir a função.

## Criar uma função vinculada ao serviço para o Client VPN

Não é necessário criar manualmente a função `AWSServiceRoleForClientVPN`. O Client VPN a criará no momento em que você criar o primeiro endpoint do Client VPN na sua conta.

Para o Client VPN criar uma função vinculada a serviço em seu nome, você deve ter as permissões necessárias. Para obter mais informações, consulte [Permissões da função vinculada a serviço](#) no Guia do usuário do IAM.

## Editar uma função vinculada ao serviço para o Client VPN

O Client VPN não permite que você edite a função vinculada ao serviço `AWSServiceRoleForClientVPN`.

## Excluir uma função vinculada ao serviço para o Client VPN

Se você não precisa mais usar o Client VPN, recomendamos que exclua a função vinculada a serviço `AWSServiceRoleForClientVPN`.

Apenas será possível excluir a função vinculada a serviço `AWSServiceRoleForClientVPN` depois de excluir os recursos relacionados do Client VPN. Isso garante que você não remova por engano a permissão para acessar os recursos.

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao serviço `AWSServiceRoleForClientVPN`. Para obter mais informações, consulte [Exclusão de uma função vinculada a serviço](#) no Guia do usuário do IAM.

# Cenários e exemplos

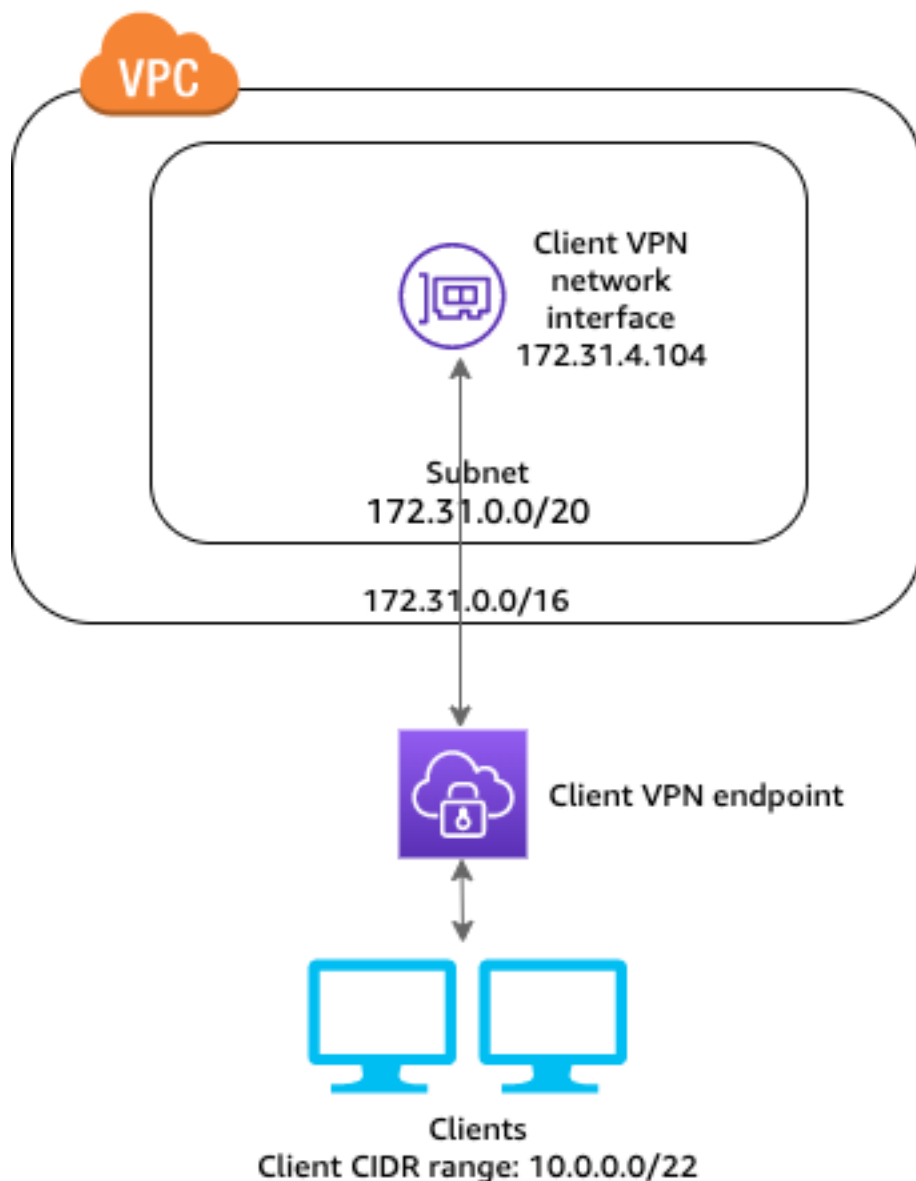
Esta seção fornece exemplos de como criar e configurar o acesso ao Client VPN para os seus clientes.

## Tópicos

- [Acesso a uma VPC \(p. 11\)](#)
- [Acesso a uma VPC emparelhada \(p. 13\)](#)
- [Acesso a uma rede no local \(p. 15\)](#)
- [Acesso à Internet \(p. 17\)](#)
- [Restringir o acesso a recursos específicos na sua VPC \(p. 19\)](#)

## Acesso a uma VPC

A configuração deste cenário inclui uma única VPC de destino. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte [VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN no [Limitações do Client VPN \(p. 3\)](#).
- Certifique-se de que o grupo de segurança que você usará para o endpoint do Client VPN permite tráfego de entrada e saída para os clientes e vice-versa. Para obter mais informações, consulte [Grupos de segurança \(p. 7\)](#).

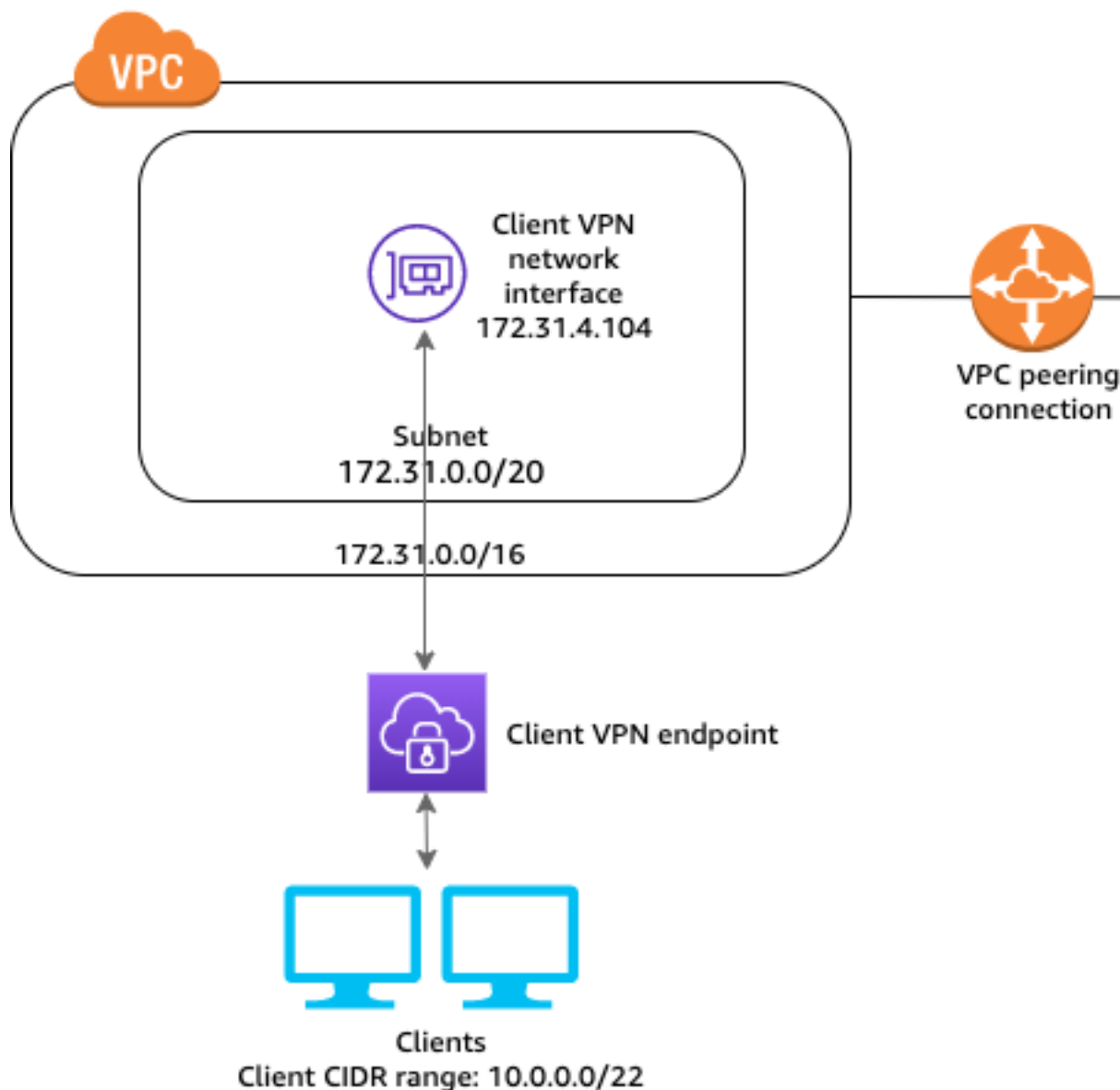


Para implementar essa configuração

1. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, realize as etapas descritas em [Criar um endpoint do Client VPN \(p. 27\)](#).
2. Associe a sub-rede ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em [Associar uma rede de destino a um endpoint do Client VPN \(p. 31\)](#) e selecione a sub-rede e a VPC que você identificou anteriormente.
3. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN \(p. 34\)](#) e, em Destination network (Rede de destino), insira o intervalo CIDR IPv4 da VPC.

## Acesso a uma VPC emparelhada

A configuração para esse cenário inclui uma única VPC e uma VPC adicional que é emparelhada com a VPC de destino. Ela é recomendada quando você precisar dar acesso para os clientes aos recursos dentro de uma VPC de destino e a outras VPCs que estejam emparelhadas com ela.



Antes de começar, faça o seguinte:

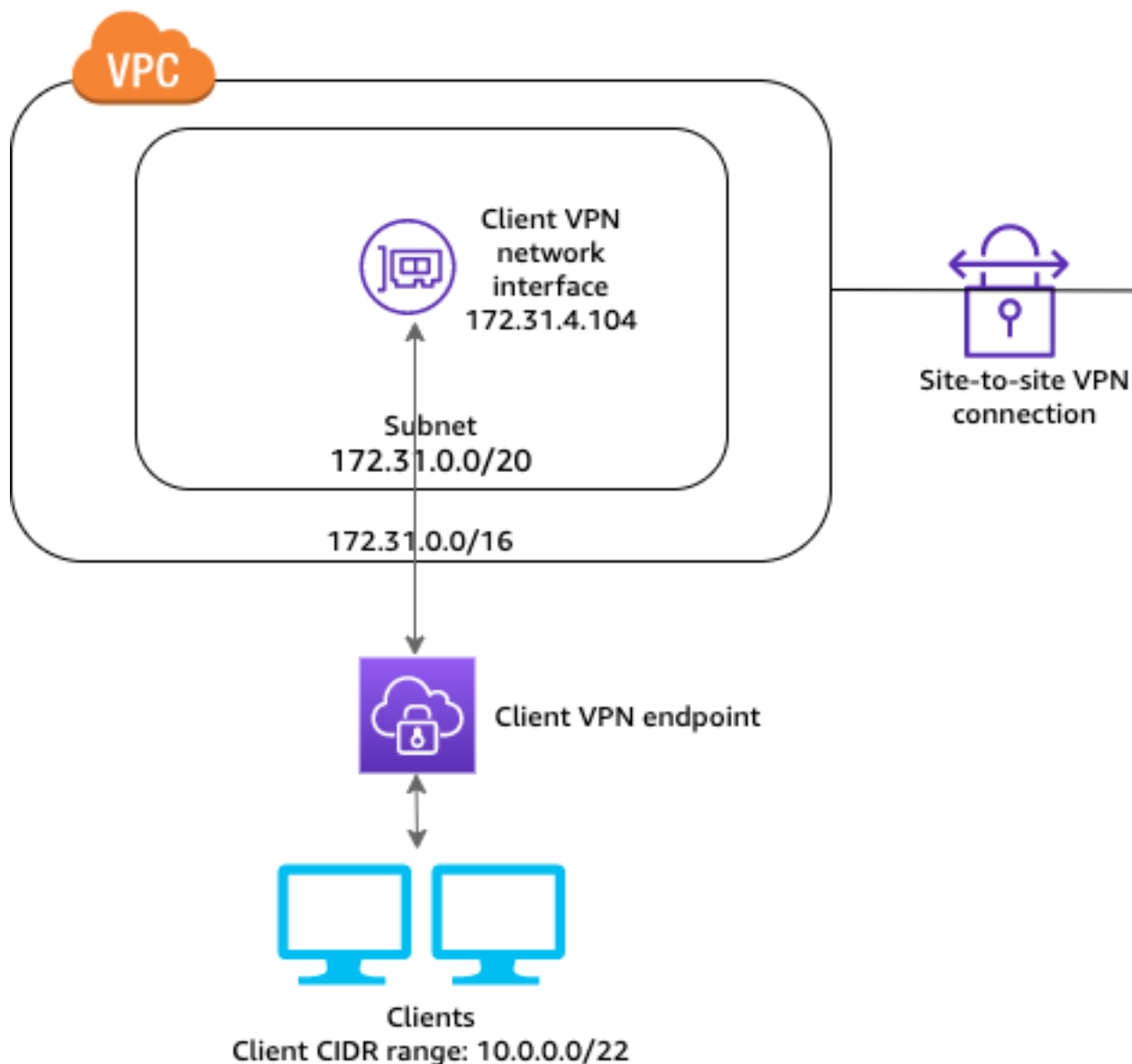
- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte [VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN no [Limitações do Client VPN \(p. 3\)](#).
- Certifique-se de que o grupo de segurança que você usará para o endpoint do Client VPN permite tráfego de entrada e saída para os clientes e vice-versa. Para obter mais informações, consulte [Grupos de segurança \(p. 7\)](#).

Para implementar essa configuração

1. Estabeleça a conexão de emparelhamento de VPCs entre as VPCs. Siga as etapas em [Criar e aceitar uma conexão de emparelhamento de VPC](#) no Amazon VPC Peering Guide.
2. Teste a conexão de emparelhamento de VPCs. Confirme se as instâncias em qualquer uma das VPCs podem se comunicar umas com as outras como se estivessem na mesma rede. Se a conexão de emparelhamento funcionar conforme esperado, siga para a próxima etapa.
3. Crie um endpoint do Client VPN na mesma região que a VPC identificada na Etapa 1. Realize as etapas descritas em [Criar um endpoint do Client VPN \(p. 27\)](#).
4. Associe a sub-rede anteriormente identificada ao endpoint do Client VPN que você criou. Para fazer isso, execute as etapas descritas em [Associar uma rede de destino a um endpoint do Client VPN \(p. 31\)](#) e selecione a sub-rede e a VPC.
5. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN \(p. 34\)](#) e, em Destination network to enable (Rede de destino para habilitar), insira o intervalo CIDR IPv4 da VPC.
6. Adicione uma rota para direcionar o tráfego à VPC emparelhada. Para fazer isso, realize as etapas descritas em [Criar uma rota de endpoint \(p. 36\)](#). Em Route destination (Destino da rota), insira o intervalo CIDR IPv4 da VPC emparelhada e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede que você associou ao endpoint do Client VPN.
7. Adicione uma regra de autorização para fornecer os acesso à VPC emparelhada para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN \(p. 34\)](#). Em Destination network (Rede de destino), insira o intervalo CIDR IPv4 da VPC emparelhada.

## Acesso a uma rede no local

A configuração deste cenário inclui acesso a uma rede local apenas. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma rede no local apenas.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte [VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN no [Limitações do Client VPN \(p. 3\)](#).
- Certifique-se de que o grupo de segurança que você usará para o endpoint do Client VPN permite tráfego de entrada e saída para os clientes e vice-versa. Para obter mais informações, consulte [Grupos de segurança \(p. 7\)](#).

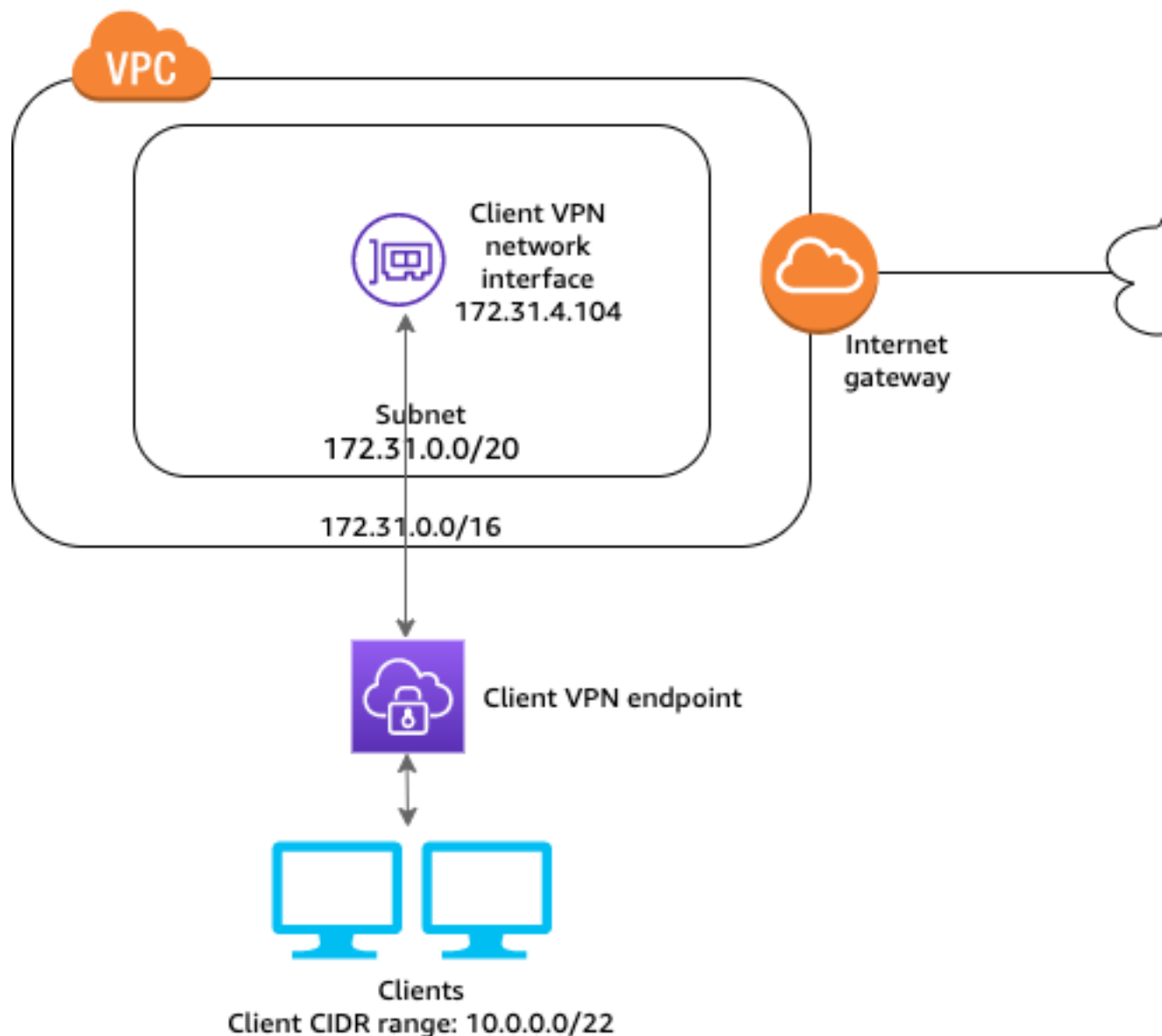
Para implementar essa configuração

1. Habilite a comunicação entre a VPC e sua própria rede no local por meio de uma conexão AWS Site-to-Site VPN. Para fazer isso, execute as etapas descritas em [Conceitos básicos](#) no Guia do usuário do AWS Site-to-Site VPN.
2. Teste a conexão AWS Site-to-Site VPN criada na etapa anterior. Para fazer isso, execute as etapas descritas em [Testar a conexão VPN de local para local](#) no Guia do usuário do AWS Site-to-Site VPN. Se a conexão VPN estiver funcionando conforme o esperado, continue para a próxima etapa.
3. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, realize as etapas descritas em [Criar um endpoint do Client VPN \(p. 27\)](#).
4. Associe a sub-rede que você identificou anteriormente ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em [Associar uma rede de destino a um endpoint do Client VPN \(p. 31\)](#) e selecione a VPC e a sub-rede.
5. Adicione uma rota que permita acesso à conexão AWS Site-to-Site VPN. Para fazer isso, execute as etapas descritas em [Criar uma rota de endpoint \(p. 36\)](#). Em Route destination (Destino da rota), insira o intervalo CIDR IPv4 da conexão AWS Site-to-Site VPN e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede que você associou ao endpoint do Client VPN.
6. Adicione uma regra de autorização para fornecer acesso à conexão AWS Site-to-Site VPN para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN \(p. 34\)](#). Em Destination network (Rede de destino), insira o intervalo CIDR IPv4 de conexão AWS Site-to-Site VPN.

## Acesso à Internet

A configuração deste cenário inclui uma única VPC de destino e acesso à Internet. Ela é recomendada quando você precisa permitir que os clientes tenham acesso aos recursos dentro de uma única VPC de destino e permitir o acesso à Internet.

Se você já concluiu o tutorial [Conceitos básicos do Client VPN \(p. 21\)](#), então já implementou esse cenário.



Antes de começar, faça o seguinte:

- Crie ou identifique uma VPC com pelo menos uma sub-rede. Identifique a sub-rede na VPC que você deseja associar ao endpoint do Client VPN e anote seus intervalos CIDR IPv4. Para obter mais informações, consulte [VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.
- Identifique um intervalo CIDR adequado para os endereços IP do cliente que não se sobrepõem ao CIDR da VPC.
- Revise as regras e as limitações dos endpoints do Client VPN no [Limitações do Client VPN \(p. 3\)](#).
- Certifique-se de que o grupo de segurança que você usará para o endpoint do Client VPN permite tráfego de entrada e saída para os clientes e vice-versa. Para obter mais informações, consulte [Grupos de segurança \(p. 7\)](#).

Para implementar essa configuração

1. Certifique-se de que o grupo de segurança que você usará para o endpoint do Client VPN permite tráfego de entrada e saída para a Internet e vice-versa. Para fazer isso, adicione regras de entrada e saída que permitam tráfego para 0.0.0.0/0 e vice-versa para tráfego HTTP e HTTPS.
2. Crie um gateway de internet e anexe-o à sua VPC. Para obter mais informações, consulte [Criação e anexação de um gateway de internet](#) no Guia do usuário da Amazon VPC.
3. Torne a sub-rede pública, adicionando uma rota para o gateway de internet à sua tabela de rotas. No console da VPC, escolha Subnets (Sub-redes), selecione a sub-rede que você pretende associar ao endpoint do Client VPN, escolha Route Table (Tabela de rotas) e, em seguida, escolha o ID da tabela de rotas. Escolha Actions (Ações), Edit routes (Editar rotas) e depois Add route (Adicionar rota). Em Destination (Destino), insira 0.0.0.0/0 e, em Target (Destino), escolha o gateway de internet da etapa anterior.
4. Crie um endpoint do Client VPN na mesma região que a VPC. Para fazer isso, realize as etapas descritas em [Criar um endpoint do Client VPN](#) (p. 27).
5. Associe a sub-rede que você identificou anteriormente ao endpoint do Client VPN. Para fazer isso, execute as etapas descritas em [Associar uma rede de destino a um endpoint do Client VPN](#) (p. 31) e selecione a VPC e a sub-rede.
6. Adicione uma regra de autorização para fornecer acesso à VPC para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN](#) (p. 34) e, em Destination network to enable (Rede de destino para habilitar), insira o intervalo CIDR IPv4 da VPC.
7. Adicione uma rota que permita tráfego para a Internet. Para fazer isso, realize as etapas descritas em [Criar uma rota de endpoint](#) (p. 36). Em Route destination (Destino da rota), insira 0.0.0.0/0 e, em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede que você associou ao endpoint do Client VPN.
8. Adicione uma regra de autorização para fornecer acesso à Internet para os clientes. Para fazer isso, execute as etapas descritas em [Adicionar uma regra de autorização a um endpoint do Client VPN](#) (p. 34). Em Destination network (Rede de destino), insira 0.0.0.0/0.

## Restringir o acesso a recursos específicos na sua VPC

Você pode conceder ou negar acesso a recursos específicos em sua VPC adicionando ou removendo regras de grupo de segurança que fazem referência ao grupo de segurança que foi aplicado à associação da rede de destino (o grupo de segurança do Client VPN).

Essa configuração é comentada no cenário descrito em [Acesso a uma VPC](#) (p. 11). Ela é aplicada além da regra de autorização configurada naquele cenário.

Antes de começar, verifique se o grupo de segurança do Client VPN está associado a outros recursos em sua VPC. Se você adicionar ou remover regras que fazem referência ao grupo de segurança do Client VPN, poderá conceder ou negar acesso aos outros recursos associados também. Para evitar isso, crie um grupo de segurança especificamente para uso com o endpoint do Client VPN.

## Conceder acesso somente para a clientes do Client VPN

Essa configuração concede acesso a um recurso específico de uma VPC somente para clientes do Client VPN.

No grupo de segurança associado à instância em que o recurso está sendo executado, crie uma regra de grupo de segurança que permita apenas o tráfego proveniente do grupo de segurança do Client VPN.

Como criar uma regra de grupo de segurança

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Security Groups (Grupos de segurança).
3. Escolha o grupo de segurança associado à instância em que o recurso está sendo executado.
4. Escolha Actions (Ações), Edit inbound rules (Editar regras de entrada).
5. Selecione Add Rule (Adicionar regra) e faça o seguinte:
  - Em Type (Tipo), escolha All traffic (Todo o tráfego), ou um tipo específico de tráfego que você deseja permitir.
  - Para Source (Origem), escolha Custom (Personalizar) e insira ou escolha o ID do grupo de segurança do Client VPN.
6. Selecione Save rules (Salvar regras).

## Negar acesso a clientes do Client VPN

Essa configuração impede que os clientes do Client VPN acessem um recurso específico em uma VPC.

Na instância em que o recurso está sendo executado, o grupo de segurança não deve permitir tráfego do grupo de segurança do Client VPN.

Como verificar as regras do grupo de segurança

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Security Groups (Grupos de segurança).
3. Escolha Inbound Rules (Regras de entrada).
4. Revise a lista de regras. Se houver uma regra em que Source (Origem) é o grupo de segurança do Client VPN, escolha Edit rules (Editar Regras) e selecione Delete (Excluir) (o ícone x) para a regra. Escolha Save rules (Salvar regras).



# Conceitos básicos do Client VPN

As tarefas a seguir ajudarão você a se familiarizar com o Client VPN. Neste tutorial, você criará um endpoint do Client VPN que faz o seguinte:

- Fornece acesso a uma única VPC.
- Fornece acesso à Internet.
- Use a autenticação mútua. Para obter mais informações, consulte [Autenticação mútua \(p. 5\)](#).

## Etapas

- [Pré-requisitos \(p. 21\)](#)
- [Etapa 1: gerar chaves e certificados de servidor e cliente \(p. 21\)](#)
- [Etapa 2: criar um endpoint do Client VPN \(p. 21\)](#)
- [Etapa 3: habilitar a conectividade de VPN para clientes \(p. 23\)](#)
- [Etapa 4: autorizar os clientes a acessar uma rede \(p. 23\)](#)
- [Etapa 5: \(opcional\) habilitar o acesso a redes adicionais \(p. 24\)](#)
- [Etapa 6: fazer download do arquivo de configuração do endpoint do Client VPN \(p. 24\)](#)
- [Passo 7: conectar-se ao endpoint do Client VPN \(p. 26\)](#)

## Pré-requisitos

Para concluir este tutorial de conceitos básicos, você precisa do seguinte:

- As permissões necessárias para trabalhar com endpoints do Client VPN.
- Uma VPC com pelo menos uma sub-rede, um gateway da Internet e uma rota para o gateway da Internet.

## Etapa 1: gerar chaves e certificados de servidor e cliente

Este tutorial usa a autenticação mútua. Com a autenticação mútua, o Client VPN usa certificados para realizar a autenticação entre o cliente e o servidor.

Para obter as etapas detalhadas de geração dos certificados e das chaves de servidor e cliente, consulte [Autenticação mútua \(p. 5\)](#).

## Etapa 2: criar um endpoint do Client VPN

Ao criar um endpoint do Client VPN, você cria a construção de VPN à qual os clientes podem se conectar para estabelecer uma conexão VPN.

Depois de criar o endpoint do Client VPN, observe o seguinte:

- O estado inicial do endpoint do Client VPN é `pending-associate`. Os clientes só poderão estabelecer uma conexão VPN depois que você associar pelo menos uma rede de destino.

- Você recebe um nome DNS para o endpoint do Client VPN. Esse é o nome DNS que os clientes usam para estabelecer uma conexão VPN.
- É possível fazer download do arquivo de configuração do endpoint do Client VPN. É possível fornecer esse arquivo aos clientes que desejam se conectar à VPN.

#### Para criar um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Client VPN Endpoints (Endpoints do Client VPN) e Create Client VPN Endpoint (Criar endpoint do Client VPN).
3. (Opcional) Em Description (Descrição), digite uma breve descrição do endpoint do Client VPN.
4. Em Client IPv4 CIDR (CIDR IPv4 do cliente), especifique um intervalo de endereços IP, em notação CIDR, do qual atribuir endereços IP do cliente.

#### Note

O intervalo de endereços IP não pode se sobrepor à rede de destino ou a qualquer uma das rotas que serão associadas ao endpoint do Client VPN. O intervalo CIDR do cliente deve ter um tamanho de bloco entre /12 e /22 e não pode se sobrepor ao CIDR da VPC ou a qualquer outra rota na tabela de rotas. Não é possível alterar o intervalo de endereços IP depois de criar o endpoint do Client VPN.

5. Para Server certificate ARN (ARN do certificado de servidor), especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint do Client VPN ao qual estão se conectando.

#### Note

O certificado de servidor deve ser provisionado no AWS Certificate Manager (ACM).

6. Especifique o método de autenticação a ser usado para autenticar os clientes quando eles estabelecer uma conexão VPN. Para usar a autenticação de certificado mútua, selecione Use mutual authentication (Usar autenticação mútua) e, para Client certificate ARN (ARN do certificado de cliente), especifique o ARN do certificado de cliente gerado na Etapa 1.
7. Especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Para Do you want to log the details on client connections? (Deseja registrar os detalhes sobre conexões de clientes?), siga um destes procedimentos:
  - Para habilitar o registro em log de conexões de clientes, selecione Yes (Sim). Em CloudWatch Logs log group name (Nome do grupo de logs do CloudWatch Logs), insira o nome do grupo de logs a ser usado e, em CloudWatch Logs log stream name (Nome do fluxo de logs do CloudWatch Logs), insira o nome do fluxo de logs a ser usado.
  - Para desabilitar o registro de conexões de clientes, escolha No (Não).
8. (Opcional) Especifique quais servidores DNS devem ser usados para a resolução de DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar um servidor DNS de VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

#### Note

Verifique se os servidores DNS possam ser acessados pelos clientes.

9. (Opcional) Para habilitar o túnel dividido em um endpoint da VPN, selecione Enable split-tunnel (Habilitar túnel dividido).

Por padrão, o túnel dividido em um endpoint da VPN está desabilitado.

10. (Opcional) Por padrão, o servidor do Client VPN usa o protocolo de transporte UDP. Para usar o protocolo de transporte TCP, em Transport Protocol (Protocolo de transporte), selecione TCP.

Note

Em geral, o UDP oferece melhor desempenho que o TCP.

11. (Opcional) Em VPC ID (ID da VPC), selecione a VPC a ser associada ao endpoint do Client VPN. Em Security Group ID (IDs de grupo de segurança), selecione um ou mais grupos de segurança da VPC a serem aplicados ao endpoint do Client VPN.
12. (Opcional) Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.
13. Escolha Create Client VPN Endpoint (Criar endpoint do Client VPN).

## Etapa 3: habilitar a conectividade de VPN para clientes

Para permitir que os clientes estabeleçam uma sessão de VPN, você deve associar uma rede de destino ao endpoint do Client VPN. Uma rede de destino é uma sub-rede em uma VPC.

Quando você associa a primeira sub-rede ao endpoint do Client VPN, acontece o seguinte:

- O estado do endpoint do Client VPN muda para `available`. Agora, os clientes podem estabelecer uma conexão VPN, mas não poderão acessar recursos na VPC até que você adicione as regras de autorização.
- A rota local da VPC é adicionada automaticamente à tabela de rotas do endpoint do Client VPN.
- O grupo de segurança padrão da VPC é aplicado automaticamente para a associação da sub-rede. É possível modificar o grupo de segurança após essa associação.

Para associar uma sub-rede ao endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual associar a sub-rede e escolha Associations (Associações), Associate (Associar).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada. Se você especificou uma VPC quando criou o endpoint do Client VPN, ela deve ser a mesma VPC.
5. Em Subnet to associate (Sub-rede para associar), escolha a sub-rede a ser associada ao endpoint do Client VPN.
6. Escolha Associate (Associar).

Note

Se as regras de autorização permitirem, uma associação de sub-rede é suficiente para que os clientes acessem toda a rede de uma VPC. É possível associar sub-redes adicionais para fornecer alta disponibilidade caso uma das zonas de disponibilidade seja desativada.

## Etapa 4: autorizar os clientes a acessar uma rede

Para autorizar os clientes a acessar a VPC na qual a sub-rede associada está localizada, você deve criar uma regra de autorização. Essa regra de autorização especifica quais clientes têm acesso à VPC. Neste tutorial, vamos conceder acesso a todos os usuários.

Para adicionar uma regra de autorização à rede de destino

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN que você deseja adicionar à regra de autorização, selecione Authorization (Autorização) e Authorize ingress (Autorizar entrada).
4. Em Destination network to enable (Rede de destino para habilitar), insira o endereço IP, em notação CIDR, da rede à qual você deseja permitir acesso.
5. Especifique quais clientes têm permissão para acessar a rede especificada. Para conceder acesso a todos os usuários, em Grant access to (Conceder acesso a), selecione Allow access to all users (Permitir acesso a todos os usuários).
6. Em Description (Descrição), insira uma breve descrição da regra de autorização.
7. Escolha Add authorization rule (Adicionar regra de autorização).

## Etapa 5: (opcional) habilitar o acesso a redes adicionais

Você pode habilitar o acesso a redes adicionais conectadas à VPC, como serviços da AWS, VPCs emparelhadas e redes locais. Para cada rede adicional, é necessário adicionar uma rota para a rede e configurar uma regra de autorização para dar acesso aos clientes.

Neste tutorial, adicionaremos uma rota para a Internet (0.0.0.0/0) e adicionaremos uma regra de autorização que conceda acesso a todos os usuários.

Para habilitar o acesso a redes adicionais (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN que você deseja adicionar a rota, escolha Route Table (Tabela de rotas) e depois Create Route (Criar rota).
4. Em Route destination (Destino da rota), insira 0.0.0.0/0.
5. Em Target VPC Subnet ID (ID da sub-rede da VPC de destino), especifique o ID da sub-rede pela qual rotear o tráfego.
6. Em Description (Descrição), insira uma breve descrição da rota.
7. Escolha Create Route (Criar rota).
8. Adicione uma regra de autorização para a rede, para especificar quais clientes têm acesso. Realize as etapas em [Etapa 4: autorizar os clientes a acessar uma rede \(p. 23\)](#). Na Etapa 4, insira 0.0.0.0/0 e, na Etapa 5, selecione Allow access to all users (Permitir acesso a todos os usuários).
9. Verifique se o grupo de segurança associado à sub-rede pela qual você está roteando tráfego permite tráfego de entrada e de saída de e para a Internet. Para fazer isso, adicione regras de entrada e de saída que permitam o tráfego da Internet de e para 0.0.0.0/0.

## Etapa 6: fazer download do arquivo de configuração do endpoint do Client VPN

A etapa final é fazer download do arquivo de configuração do endpoint do Client VPN e prepará-lo. O arquivo de configuração inclui as informações do endpoint do Client VPN e de certificado necessárias para estabelecer uma conexão VPN. Você deve fornecer esse arquivo aos clientes que precisam se conectar

ao endpoint do Client VPN para estabelecer uma conexão VPN. O cliente faz upload desse arquivo em seu aplicativo cliente de VPN. Para obter mais informações sobre como usar um aplicativo cliente para se conectar ao endpoint do Client VPN, consulte o [Guia do usuário do AWS Client VPN](#).

Depois de criar o endpoint do Client VPN na Etapa 2, o console exibe o nome DNS, por exemplo, `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`. Para especificar o nome DNS, é necessário especificar uma string aleatória na frente do nome exibido para que o formato seja *random\_string.displayed\_DNS\_name*, por exemplo, `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`.

Para fazer download do arquivo de configuração do endpoint do Client VPN e prepará-lo (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN cujo arquivo de configuração deve ser transferido por download e escolha Download Client Configuration (Fazer download da configuração do cliente).
4. Copie a chave e o certificado de cliente, que foram gerados na Etapa 1 para a mesma pasta que o arquivo de configuração do endpoint do Client VPN obtido por download. A chave e o certificado de cliente estão disponíveis nos seguintes locais no repositório clonado OpenVPN easy-rsa:
  - Certificado de cliente — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
  - Chave de cliente — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Abra o arquivo de configuração do endpoint do Client VPN usando o editor de texto de sua preferência e adicione o seguinte ao final desse arquivo. Substitua */path/* pelo local do certificado e da chave do cliente (o local é relativo ao cliente que está se conectando ao endpoint).

```
cert /path/client1.domain.tld.crt  
key /path/client1.domain.tld.key
```

6. Anexe uma string aleatória para o nome DNS do endpoint do Client VPN. Localize a linha que especifica o nome DNS do endpoint do Client VPN e preceda-a com uma string aleatória para que o formato seja *string\_aleatória.nome\_DNS\_exibido*. Por exemplo:
  - Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
  - Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
7. Salve e feche o arquivo de configuração do endpoint do Client VPN.
8. Distribua o arquivo de configuração do endpoint do Client VPN e o certificado do cliente e a chave aos clientes.

Para fazer download do arquivo de configuração do endpoint do Client VPN e prepará-lo (AWS CLI)

1. Faça download do arquivo de configuração do endpoint do Client VPN.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id  
--output text>client-config.ovpn
```

2. Copie a chave e o certificado de cliente, que foram gerados na Etapa 1 para a mesma pasta que o arquivo de configuração do endpoint do Client VPN obtido por download. A chave e o certificado de cliente estão disponíveis nos seguintes locais no repositório clonado OpenVPN easy-rsa:
  - Certificado de cliente — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
  - Chave de cliente — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`

3. Abra o arquivo de configuração do endpoint do Client VPN usando seu editor de texto preferido (como vim ou nano) ou use o comando `cat >> client-config.ovpn` e adicione o seguinte ao final do arquivo. Substitua `/path/` pelo local do certificado e da chave do cliente (o local é relativo ao cliente que está se conectando ao endpoint).

```
cert /path/client1.domain.tld.crt  
key /path/client1.domain.tld.key
```

4. Anexe uma string aleatória para o nome DNS do endpoint do Client VPN. Localize a linha que especifica o nome DNS do endpoint do Client VPN e preceda-a com uma string aleatória para que o formato seja `string_aleatória.nome_DNS_exibido`. Por exemplo:
  - Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
  - Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
5. Distribua o arquivo de configuração do endpoint do Client VPN e o certificado do cliente e a chave aos clientes.

## Passo 7: conectar-se ao endpoint do Client VPN

É possível se conectar ao endpoint do Client VPN usando o Cliente fornecido pela AWS ou outro aplicativo cliente baseado em OpenVPN. Para obter mais informações, consulte o [Guia do usuário do AWS Client VPN](#).

# Trabalho com o Client VPN

Você pode trabalhar com o Client VPN usando o console da Amazon VPC ou a CLI da AWS.

## Tópicos

- [Endpoints do Client VPN \(p. 27\)](#)
- [Redes de destino \(p. 31\)](#)
- [Regras de autorização \(p. 33\)](#)
- [Rotas \(p. 35\)](#)
- [Listas de revogação de certificados de cliente \(p. 37\)](#)
- [Conexões de cliente \(p. 38\)](#)

## Endpoints do Client VPN

Todas as sessões de VPN de cliente são encerradas no endpoint do Client VPN. Você configura o endpoint do Client VPN para gerenciar e controlar todas as sessões de VPN de cliente.

## Tópicos

- [Criar um endpoint do Client VPN \(p. 27\)](#)
- [Modificar um endpoint do Client VPN \(p. 29\)](#)
- [Exportar a configuração do cliente \(p. 30\)](#)
- [Visualizar endpoints do Client VPN \(p. 31\)](#)
- [Excluir um endpoint do Client VPN \(p. 31\)](#)

## Criar um endpoint do Client VPN

Crie um endpoint do Client VPN para permitir que seus clientes estabeleçam uma sessão de VPN.

O Client VPN deve ser criado na mesma conta da AWS na qual a rede de destino pretendida está provisionada.

## Pré-requisitos

Antes de começar, faça o seguinte:

- Revise as regras e as limitações em [Limitações do Client VPN \(p. 3\)](#).
- Gere o certificado do servidor e, se necessário, o certificado do cliente. Para obter mais informações, consulte [Autenticação \(p. 5\)](#).

Para criar um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Client VPN Endpoints (Endpoints do Client VPN) e Create Client VPN Endpoint (Criar endpoint do Client VPN).

3. (Opcional) Em Description (Descrição), digite uma breve descrição do endpoint do Client VPN.
4. Em Client IPv4 CIDR (CIDR IPv4 do cliente), especifique um intervalo de endereços IP, em notação CIDR, do qual atribuir endereços IP do cliente.
5. Para Server certificate ARN (ARN do certificado de servidor), especifique o ARN do certificado TLS a ser usado pelo servidor. Os clientes usam o certificado de servidor para autenticar o endpoint do Client VPN ao qual estão se conectando.

**Note**

O certificado de servidor deve ser provisionado no AWS Certificate Manager (ACM).

6. Especifique o método de autenticação a ser usado para autenticar os clientes quando eles estabelecer uma conexão VPN. Você deve selecionar pelo menos um método de autenticação.
  - Para usar a autenticação via Active Directory, selecione Use Active Directory authentication (Usar autenticação via Active Directory) e, em Directory ID (ID do diretório), especifique o ID do Active Directory a ser usado.
  - Para usar a autenticação de certificado mútua, selecione Use mutual authentication (Usar autenticação mútua) e, em Client certificate ARN (ARN do certificado de cliente), especifique o ARN do certificado de cliente provisionado no AWS Certificate Manager (ACM).

**Note**

Se o certificado de cliente tiver sido emitido pela mesma Autoridade de certificação (emissor) que o certificado de servidor, você poderá continuar a usar o ARN do certificado de servidor para o ARN do certificado de cliente. Se você gerou um certificado de cliente separado e uma chave para cada usuário que usa a mesma CA que o certificado do servidor, é possível usar o ARN do certificado do servidor.

7. Especifique se deseja registrar dados sobre conexões de clientes usando o Amazon CloudWatch Logs. Para Do you want to log the details on client connections? (Deseja registrar os detalhes sobre conexões de clientes?), siga um destes procedimentos:
  - Para habilitar o registro em log de conexões de clientes, selecione Yes (Sim). Em CloudWatch Logs log group name (Nome do grupo de logs do CloudWatch Logs), insira o nome do grupo de logs a ser usado e, em CloudWatch Logs log stream name (Nome do fluxo de logs do CloudWatch Logs), insira o nome do fluxo de logs a ser usado.
  - Para desabilitar o registro de conexões de clientes, escolha No (Não).
8. Especifique quais servidores DNS devem ser usados para a resolução de DNS. Para usar servidores DNS personalizados, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) e DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP dos servidores DNS a serem usados. Para usar o servidor DNS da VPC, em DNS Server 1 IP address (Endereço IP do servidor DNS 1) ou DNS Server 2 IP address (Endereço IP do servidor DNS 2), especifique os endereços IP e adicione o endereço IP do servidor DNS da VPC.

**Note**

Verifique se os servidores DNS possam ser acessados pelos clientes.

9. (Opcional) Para que o endpoint seja um endpoint de VPN de túnel dividido, selecione Enable split-tunnel (Habilitar túnel dividido).

Por padrão, o túnel dividido em um endpoint da VPN está desabilitado.

10. (Opcional) Por padrão, o servidor do Client VPN usa o protocolo de transporte UDP. Para usar o protocolo de transporte TCP, em Transport Protocol (Protocolo de transporte), selecione TCP.

**Note**

Em geral, o UDP oferece melhor desempenho que o TCP. Não é possível alterar o protocolo de transporte depois de criar o endpoint do Client VPN.



11. (Opcional) Em VPC ID (ID da VPC), selecione a VPC a ser associada ao endpoint do Client VPN. Em Security Group ID (IDs de grupo de segurança), selecione um ou mais grupos de segurança da VPC a serem aplicados ao endpoint do Client VPN.
12. (Opcional) Em VPN port (Porta VPN), selecione o número da porta VPN. O padrão é 443.
13. Escolha Create Client VPN Endpoint (Criar endpoint do Client VPN).

Depois de criar o endpoint do Client VPN, faça o seguinte para concluir a configuração e permitir que os clientes se conectem:

- O estado inicial do endpoint do Client VPN é `pending-associate`. Os clientes só poderão se conectar ao endpoint do Client VPN depois que você associar a primeira [rede de destino \(p. 31\)](#).
- Crie uma [regra de autorização \(p. 33\)](#) para especificar quais clientes têm acesso à rede.
- Baixe e prepare o [arquivo de configuração \(p. 30\)](#) do endpoint do Client VPN para distribuir aos seus clientes.
- Instrua seus clientes a usar o Cliente fornecido pela AWS ou outro aplicativo cliente baseado em OpenVPN para se conectarem ao endpoint do Client VPN. Para obter mais informações, consulte o [Guia do usuário do AWS Client VPN](#).

Para criar um endpoint do Client VPN (AWS CLI)

Use o comando [create-client-vpn-endpoint](#).

## Modificar um endpoint do Client VPN

Após a criação de um Client VPN, é possível modificar qualquer uma das seguintes configurações:

- A descrição
- O certificado de servidor
- As opções de registro em log da conexão do cliente
- Os servidores DNS
- A opção de túnel dividido
- A VPC e as associações do grupo de segurança
- O número da porta VPN

Não é possível modificar o intervalo CIDR IPv4 do cliente, as opções de autenticação nem o protocolo de transporte após a criação do endpoint do Client VPN.

É possível modificar um endpoint do Client VPN usando o console ou a AWS CLI.

Para modificar um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN a ser modificado, escolha Actions (Ações) e depois escolha Modify Client VPN Endpoint (Modificar endpoint do Client VPN).
4. Faça as alterações necessárias e escolha Modify Client VPN Endpoint (Modificar endpoint do Client VPN).

Para modificar um endpoint do Client VPN (AWS CLI)

Use o comando [modify-client-vpn-endpoint](#).

## Exportar a configuração do cliente

O arquivo de configuração do endpoint do Client VPN é o arquivo que os clientes (usuários) usam para estabelecer uma conexão VPN com o endpoint do Client VPN. Você deve fazer download desse arquivo e distribuí-lo a todos os clientes que precisam de acesso à VPN.

Se o endpoint do Client VPN usar a autenticação mútua, será necessário adicionar o certificado de cliente e a chave privada do cliente ao arquivo de configuração .ovpn do qual foi feito download. Depois de adicionar as informações, os clientes poderão importar o arquivo .ovpn para o software cliente OpenVPN.

### Important

É necessário adicionar o certificado de cliente e as informações de chave privada do cliente ao arquivo de configuração .ovpn. Caso contrário, os clientes não poderão se conectar ao endpoint do Client VPN.

Por padrão, a opção "--remote-random-hostname" na configuração do cliente OpenVPN habilita o DNS curinga. Como o DNS curinga está habilitado, o cliente não armazena em cache o endereço IP do endpoint, e você não poderá executar ping no nome DNS do endpoint.

Se o endpoint do Client VPN usar a autenticação do Active Directory e se você habilitar a autenticação multifator (MFA) no diretório após distribuir o arquivo de configuração do cliente, será necessário fazer download de um novo arquivo e redistribuí-lo aos clientes. Os clientes não podem usar o arquivo de configuração anterior para se conectar ao endpoint do Client VPN.

É possível exportar a configuração do cliente usando o console ou a AWS CLI.

### Para exportar configuração do cliente (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN cuja configuração do cliente deve ser transferida por download e escolha Download Client Configuration (Fazer download da configuração do cliente).

### Para exportar configuração do cliente (AWS CLI)

Use o comando `export-client-vpn-client-configuration` e especifique o nome do arquivo de saída.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id --  
output text>config_filename.ovpn
```

### Como adicionar o certificado de cliente e as informações de chave (autenticação mútua)

É possível distribuir o certificado do cliente e a chave aos clientes com o arquivo de configuração do endpoint do Client VPN. Nesse caso, especifique o caminho para o certificado e a chave no arquivo de configuração. Abra o arquivo de configuração usando o editor de texto de sua preferência e adicione o seguinte ao final desse arquivo. Substitua `/path/` pelo local do certificado e da chave do cliente (o local é relativo ao cliente que está se conectando ao endpoint).

```
cert /path/client1.domain.tld.crt  
key /path/client1.domain.tld.key
```

Como alternativa, adicione o conteúdo do certificado do cliente entre as tags `<cert></cert>` e o conteúdo da chave privada entre as tags `<key></key>` ao arquivo de configuração. Se você escolher essa opção, somente o arquivo de configuração será distribuído aos clientes.

Se você gerou certificados de clientes separados e chaves para cada usuário que se conectará ao endpoint do Client VPN, repita essa etapa para cada usuário.

## Visualizar endpoints do Client VPN

É possível visualizar informações sobre endpoints do Client VPN usando o console ou a AWS CLI.

Para visualizar endpoints do Client VPN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint Client VPN a ser visualizado.
4. Use as guias para visualizar as redes de destino, as regras de autorização, as rotas e as conexões de cliente associadas.

Para visualizar endpoints do Client VPN usando a AWS CLI

Use o comando [describe-client-vpn-endpoints](#).

## Excluir um endpoint do Client VPN

Ao excluir um endpoint do Client VPN, seu estado é alterado para `deleting`, e os clientes não podem mais se conectar a ele. Você deve desassociar todas as redes de destino associadas antes de excluir um endpoint do Client VPN.

É possível excluir um endpoint do Client VPN usando o console ou a AWS CLI.

Para excluir um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN a ser excluído, escolha Actions (Ações), escolha Delete Client VPN Endpoint (Excluir endpoint do Client VPN) e depois Yes, Delete (Sim, excluir).

Para excluir um endpoint do Client VPN (AWS CLI)

Use o comando [delete-client-vpn-endpoint](#).

## Redes de destino

Uma rede de destino é uma sub-rede em uma VPC. Um endpoint do Client VPN deve ter pelo menos uma rede de destino para permitir que os clientes se conectar a ele e estabeleçam uma conexão VPN.

Tópicos

- [Associar uma rede de destino a um endpoint do Client VPN \(p. 31\)](#)
- [Aplicar um grupo de segurança a uma rede de destino \(p. 32\)](#)
- [Desassociar uma rede de destino de um endpoint do Client VPN \(p. 33\)](#)
- [Visualizar redes de destino \(p. 33\)](#)

## Associar uma rede de destino a um endpoint do Client VPN

Você pode associar uma ou mais redes de destino (sub-redes) a um endpoint do Client VPN.

As seguintes regras se aplicam:

- A sub-rede deve ter um bloco CIDR com pelo menos uma máscara de bits /27, por exemplo 10.0.0.0/27. A sub-rede deve ter pelo menos 8 endereços IP disponíveis.
- Se você associar mais de uma sub-rede a um endpoint do Client VPN, cada sub-rede deverá estar em uma zona de disponibilidade diferente. Recomendamos que você associe pelo menos duas sub-redes para fornecer redundância de zona de disponibilidade.
- Se você especificou uma VPC ao criar o endpoint do Client VPN, a sub-rede deverá estar na mesma VPC. Se você ainda não associou uma VPC ao endpoint do Client VPN, poderá escolher qualquer sub-rede em qualquer VPC existente na mesma conta que o endpoint do Client VPN.

Todas as associações de sub-rede adicionais devem ser na mesma VPC. Para associar uma sub-rede de uma VPC diferente, primeiro você deve modificar o endpoint do Client VPN e alterar a VPC associada a ele. Para obter mais informações, consulte [Modificar um endpoint do Client VPN \(p. 29\)](#).

Quando você associa uma sub-rede a um endpoint do Client VPN, nós adicionamos automaticamente a rota local da VPC na qual a sub-rede associada está provisionada à tabela de rotas do endpoint do Client VPN.

Depois de associar a primeira sub-rede ao endpoint do Client VPN, o status do endpoint do Client VPN muda de `pending-associate` para `available`, e os clientes podem estabelecer uma conexão VPN.

Para associar uma rede de destino a um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual associar a rede de destino, escolha Associations (Associações) e escolha Associate (Associar).
4. Para VPC, selecione a VPC na qual a sub-rede está localizada. Se você especificou uma VPC ao criar o endpoint do Client VPN ou se tiver associações de sub-rede anteriores, ela deverá ser a mesma VPC.
5. Em Subnet to associate (Sub-rede para associar), escolha a sub-rede a ser associada ao endpoint do Client VPN.
6. Escolha Associate (Associar).

Para associar uma rede de destino a um endpoint do Client VPN (AWS CLI)

Use o comando [associate-client-vpn-target-network](#).

## Aplicar um grupo de segurança a uma rede de destino

Ao criar um endpoint do Client VPN, você pode especificar os grupos de segurança a serem aplicados à rede de destino. Quando você associa a primeira rede de destino a um endpoint Client VPN, aplicamos automaticamente o grupo de segurança padrão da VPC na qual a sub-rede associada está localizada. Para obter mais informações, consulte [Grupos de segurança \(p. 7\)](#).

Você pode alterar os grupos de segurança para o endpoint do Client VPN. As regras de grupo de segurança de que você precisa dependem do tipo de acesso VPN que você deseja configurar. Para obter mais informações, consulte [Cenários e exemplos \(p. 11\)](#).

Para aplicar um grupo de segurança a uma rede de destino (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual aplicar os grupos de segurança.

4. Escolha Security Groups (Grupos de segurança), selecione o grupo de segurança atual e escolha Apply Security Groups (Aplicar grupos de segurança).
5. Selecione os novos grupos de segurança na lista e escolha Apply Security Groups (Aplicar grupos de segurança).

Para aplicar um grupo de segurança a uma rede de destino (AWS CLI)

Use o comando [apply-security-groups-to-client-vpn-target-network](#).

## Desassociar uma rede de destino de um endpoint do Client VPN

Se você desassociar todas as redes de destino de um endpoint do Client VPN, os clientes não poderão mais estabelecer uma conexão VPN. Quando você desassocia uma sub-rede, removemos a rota que foi criada automaticamente quando a associação foi feita.

Para desassociar uma rede de destino de um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual a rede de destino está associada e escolha Associations (Associações).
4. Selecione a rede de destino a ser desassociada, escolha Disassociate (Desassociar) e escolha Yes, Disassociate (Sim, desassociar).

Para desassociar uma rede de destino de um endpoint do Client VPN (AWS CLI)

Use o comando [disassociate-client-vpn-target-network](#).

## Visualizar redes de destino

Você pode visualizar os destinos associados a um endpoint do Client VPN usando o console ou a AWS CLI.

Para visualizar redes de destino (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN e escolha Associations (Associações).

Para visualizar redes de destino usando a AWS CLI

Use o comando [describe-client-vpn-target-networks](#).

## Regras de autorização

Regras de autorização atuam como regras de firewall que concedem acesso a redes. Você deve ter uma autorização para cada regra de rede para a qual deseja conceder acesso.

Tópicos

- [Adicionar uma regra de autorização a um endpoint do Client VPN \(p. 34\)](#)

- [Remover uma regra de autorização de um endpoint do Client VPN \(p. 34\)](#)
- [Visualizar regras de autorização \(p. 35\)](#)

## Adicionar uma regra de autorização a um endpoint do Client VPN

Ao adicionar regras de autorização, você concede acesso à rede especificada para clientes específicos.

É possível adicionar regras de autorização a um endpoint do Client VPN usando o console e a AWS CLI.

Para adicionar uma regra de autorização a um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN que você deseja adicionar à regra de autorização, escolha Authorization (Autorização) e Authorize ingress (Autorizar entrada).
4. Em Destination network (Rede de destino), insira o endereço IP, em notação CIDR, da rede que você deseja que os usuários acessem (por exemplo, o bloco CIDR da VPC).
5. Especifique quais clientes têm permissão para acessar a rede especificada. Em For grant access to (Para conceder acesso a), siga um destes procedimentos:
  - Para conceder acesso a todos os clientes, escolha Allow access to all users (Permitir acesso a todos os usuários).
  - Para restringir o acesso a clientes específicos, escolha Allow access to users in a specific Active Directory group (Permitir acesso a usuários em um determinado grupo do Active Directory). Em seguida, em Active Directory group name (Nome do grupo do Active Directory), insira o identificador de segurança (SID) do grupo do Active Directory para conceder acesso.

É possível usar o cmdlet Get-ADGroup do Microsoft PowerShell para obter o SID. Para obter mais informações sobre Get-ADGroup, consulte a [página do comando Get-ADGroup](#) na Referência de módulos do PowerShell do Microsoft Windows 10 e do Windows Server 2016.

Exemplo

```
Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
```

6. Em Description (Descrição), insira uma breve descrição da regra de autorização.
7. Escolha Add authorization rule (Adicionar regra de autorização).

Para adicionar uma regra de autorização a um endpoint do Client VPN (AWS CLI)

Use o comando [authorize-client-vpn-ingress](#).

## Remover uma regra de autorização de um endpoint do Client VPN

Ao excluir uma regra de autorização, você remove o acesso à rede especificada.

É possível remover regras de autorização de um endpoint do Client VPN usando o console e a AWS CLI.

Para remover uma regra de autorização de um endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.

2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual a regra de autorização foi adicionado e escolha Authorization (Autorização).
4. Selecione a regra de autorização a ser excluída, escolha Revoke ingress (Revogar entrada) e depois Revoke ingress (Revogar entrada).

Para remover uma regra de autorização de um endpoint do Client VPN (AWS CLI)

Use o comando [revoke-client-vpn-ingress](#).

## Visualizar regras de autorização

É possível visualizar regras de autorização para um endpoint específico do Client VPN usando o console e a AWS CLI.

Para visualizar regras de autorização (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o Client VPN endpoint para o qual visualizar regras de autorização e escolha Authorization (Autorização).

Para visualizar regras de autorização (AWS CLI)

Use o comando [describe-client-vpn-authorization-rules](#).

## Rotas

Cada endpoint do Client VPN tem uma tabela de rotas que descreve as rotas de redes de destino disponíveis. Cada rota na tabela de rotas determina para onde o tráfego de rede é direcionado. Você deve configurar regras de autorização para cada rota do endpoint do Client VPN para especificar quais clientes têm acesso à rede de destino.

Quando você associa uma sub-rede de uma VPC a um endpoint do Client VPN, uma rota para essa VPC é automaticamente adicionada à tabela de rotas do endpoint do Client VPN. Para permitir o acesso de redes adicionais, como VPCs emparelhadas, redes no local e a Internet, adicione manualmente uma rota à tabela de rotas do endpoint do Client VPN.

Tópicos

- [Considerações sobre túnel dividido no endpoint do AWS Client VPN \(p. 35\)](#)
- [Criar uma rota de endpoint \(p. 36\)](#)
- [Visualizar rotas de endpoint \(p. 36\)](#)
- [Excluir uma rota de endpoint \(p. 36\)](#)

## Considerações sobre túnel dividido no endpoint do AWS Client VPN

Quando você usa túnel dividido em um endpoint do AWS Client VPN, todas as rotas que estão nas tabelas de rotas do AWS Client VPN são adicionadas à tabela de rotas do cliente quando a VPN é estabelecida. Se você adicionar uma rota após a VPN ser estabelecida, deverá redefinir a conexão para que a nova rota seja enviada ao cliente.

É recomendável contabilizar o número de rotas que o dispositivo cliente pode manipular antes de modificar a tabela de rotas do endpoint do Client VPN.

## Criar uma rota de endpoint

Ao criar uma rota, você especifica como o tráfego para a rede de destino deve ser direcionado.

Para permitir que os clientes acessem a Internet, adicione uma rota de destino 0.0.0.0/0.

É possível adicionar rotas a um endpoint do Client VPN usando o console e a AWS CLI.

Para criar uma rota de endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN que você deseja adicionar a rota, escolha Route Table (Tabela de rotas) e Create Route (Criar rota).
4. Em Route destination (Destino da rota), especifique o intervalo CIDR IPv4 da rede de destino. Por exemplo:
  - Para adicionar uma rota para acesso à Internet, insira 0.0.0.0/0.
  - Para adicionar uma rota a uma VPC emparelhada, insira o intervalo CIDR IPv4 da VPC emparelhada.
  - Para adicionar uma rota à uma rede no local, insira o intervalo CIDR IPv4 da conexão AWS Site-to-Site VPN.
5. Em Target VPC Subnet ID (ID da sub-rede da VPC de destino), selecione a sub-rede associada ao endpoint do Client VPN.
6. Em Description (Descrição), insira uma breve descrição da rota.
7. Escolha Create Route (Criar rota).

Para criar uma rota de endpoint do Client VPN (AWS CLI)

Use o comando [create-client-vpn-route](#).

## Visualizar rotas de endpoint

Você pode visualizar as rotas de um endpoint específico do Client VPN usando o console ou a AWS CLI.

Para visualizar rotas do endpoint do Client VPN (console)

1. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
2. Selecione o endpoint do Client VPN cujas rotas você deseja visualizar e escolha Route Table (Tabela de rotas).

Para visualizar rotas do endpoint do Client VPN (AWS CLI)

Use o comando [describe-client-vpn-routes](#).

## Excluir uma rota de endpoint

Você só pode excluir rotas que foram adicionadas manualmente. Não é possível excluir rotas que foram adicionadas automaticamente quando você associou uma sub-rede ao endpoint do Client VPN. Para excluir rotas que foram adicionadas automaticamente, você deve desassociar do Client VPN endpoint a sub-rede que iniciou sua criação.



É possível excluir uma rota de um endpoint do Client VPN usando o console ou a AWS CLI.

Para excluir uma rota de endpoint do Client VPN (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN do qual excluir a rota e escolha Route Table (Tabelas de rotas).
4. Selecione a rota a ser excluída, escolha Delete Route (Excluir rota) e escolha Delete Route (Excluir rota).

Para excluir uma rota de endpoint do Client VPN (AWS CLI)

Use o comando [delete-client-vpn-route](#).

## Listas de revogação de certificados de cliente

Você pode usar listas de revogação de certificados de cliente para marcar certificados de cliente específicos em uma lista negra. Colocar clientes em uma lista negra revoga o acesso deles ao endpoint do Client VPN.

### Note

Para obter mais informações sobre como gerar os certificados e as chaves de servidor e cliente, consulte [Autenticação mútua \(p. 5\)](#)

### Tópicos

- [Gerar uma lista de revogação de certificados de cliente \(p. 37\)](#)
- [Importar uma lista de revogação de certificados de cliente \(p. 38\)](#)
- [Exportar uma lista de revogação de certificados de cliente \(p. 38\)](#)

## Gerar uma lista de revogação de certificados de cliente

Você deve gerar uma lista de revogação de certificados de cliente usando o utilitário de linha de comando OpenVPN easy-rsa.

Para gerar uma lista de revogação de certificados de cliente usando o OpenVPN easy-rsa

1. Clone o repositório OpenVPN easy-rsa no seu computador local.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

2. Navegue até a pasta easy-rsa/easyrsa3 no seu repositório local.

```
$ cd easy-rsa/easyrsa3
```

3. Revogar o certificado de cliente e gerar a lista de revogação de cliente.

```
$ ./easyrsa revoke client_certificate_name  
$ ./easyrsa gen-crl
```

Digite yes quando solicitado.

## Importar uma lista de revogação de certificados de cliente

Você deve ter um arquivo de lista de revogação de certificados de cliente para importar. Para obter mais informações sobre como gerar uma lista de revogação de certificados de cliente, consulte [Gerar uma lista de revogação de certificados de cliente](#) (p. 37).

Você pode importar uma lista de revogação de certificados de cliente usando o console e a AWS CLI.

Para importar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN para o qual você deseja importar a lista de revogação de certificados de cliente.
4. Escolha Actions (Ações) e Import Client Certificate CRL (Importar CRL de certificados de cliente).
5. For Certificate Revocation List (Lista de revogação de certificado), insira o conteúdo do arquivo de lista de revogação de certificados de cliente e escolha Import CRL (Importar CRL).

Para importar uma lista de revogação de certificados de cliente (AWS CLI)

Use o comando `import-client-vpn-client-certificate-revocation-list`.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-revocation-list file:path_to_CRL_file --client-vpn-endpoint-id endpoint_id --region region
```

## Exportar uma lista de revogação de certificados de cliente

Você pode exportar listas de revogação de certificados de cliente usando o console e a AWS CLI.

Para exportar uma lista de revogação de certificados de cliente (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN do qual você deseja importar a lista de revogação de certificados de cliente.
4. Escolha Actions (Ações), Export Client Certificate CRL (Exportar CRL de certificados de cliente) e depois Yes, Export (Sim, exportar).

Para exportar uma revogação de certificado de cliente (AWS CLI)

Use o comando `export-client-vpn-client-certificate-revocation-list`.

## Conexões de cliente

Conexões são sessões de VPN que foram estabelecidas pelos clientes. Uma conexão é estabelecida quando um cliente se conecta com êxito a um endpoint do Client VPN.

Tópicos

- [Visualizar conexões de clientes \(p. 39\)](#)
- [Encerrar uma conexão de cliente \(p. 39\)](#)

## Visualizar conexões de clientes

Você pode visualizar conexões de clientes usando o console e a AWS CLI.

Para visualizar conexões de clientes (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN para o qual você deseja visualizar conexões de clientes.
4. Escolha a guia Connections (Conexões). A guia Connections (Conexões) lista todas as conexões de clientes ativas e encerradas.

Para visualizar conexões de clientes (AWS CLI)

Use o comando [describe-client-vpn-connections](#).

## Encerrar uma conexão de cliente

Quando você encerra uma conexão de cliente, a sessão de VPN também é encerrada.

É possível encerrar conexões de cliente usando o console e a AWS CLI.

Para encerrar uma conexão de cliente (console)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Client VPN Endpoints (Endpoints do Client VPN).
3. Selecione o endpoint do Client VPN ao qual o cliente está conectado e escolha Connections (Conexões).
4. Selecione a conexão a ser encerrada, escolha Terminate Connection (Encerrar conexão) e depois Terminate Connection (Encerrar conexão) novamente.

Para encerrar uma conexão de cliente (AWS CLI)

Use o comando [terminate-client-vpn-connections](#).

# Identity and Access Management for Client VPN

A AWS usa credenciais de segurança para identificar você e conceder acesso aos seus recursos da AWS. Você pode usar recursos do (AWS Identity and Access Management) IAM para permitir que outros usuários, serviços e aplicativos usem seus recursos da AWS totalmente ou de maneira limitada, sem compartilhar suas credenciais de segurança.

Por padrão, os usuários do IAM não têm permissão para criar, visualizar ou modificar recursos da AWS. Para permitir que um usuário do IAM acesse recursos, como um endpoint do Client VPN, e realizar tarefas, você deve criar uma política do IAM. Essa política deve conceder permissão ao usuário do IAM para usar os recursos específicos e as ações de API de que ele precisa. Em seguida, anexe a política ao usuário do IAM ou ao grupo ao qual ele pertence. Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos recursos especificados.

Por exemplo, a política a seguir permite acesso somente leitura. Os usuários podem visualizar endpoints do Client VPN e seus componentes, mas não podem criá-los, modificá-los ou excluí-los.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeClientVpnEndpoints"
      ],
      "Resource": "*"
    }
  ]
}
```

Você também pode usar permissões em nível de recurso para restringir quais recursos os usuários podem usar quando invocam ações do Client VPN. Por exemplo, a política a seguir permite que os usuários trabalhem com endpoints do Client VPN, mas somente se o endpoint do Client VPN tiver a tag `purpose=test`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteClientVpnEndpoint",
        "ec2:ModifyClientVpnEndpoint",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:DisassociateClientVpnTargetNetwork",
        "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:CreateClientVpnRoute",
        "ec2>DeleteClientVpnRoute",

```

```
        "ec2:RevokeClientVpnIngress"
      ],
      "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/purpose": "test"
        }
      }
    }
  ]
}
```

Para obter mais informações sobre o IAM, consulte o [Guia do usuário do IAM](#). Para obter uma lista de ações do Amazon EC2, incluindo ações do Client VPN, consulte [Ações, recursos e chaves de condição do Amazon EC2](#) no Guia do usuário do IAM.

Para obter mais informações sobre autenticação e autorização para conexão a um endpoint do Client VPN, consulte [Autorização e autenticação de clientes \(p. 5\)](#).

# Monitorar o Client VPN

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e do desempenho do AWS Client VPN e de outras soluções da AWS. Você pode usar os recursos a seguir para monitorar seus endpoints do Client VPN, analisar padrões de tráfego e solucionar problemas com seus endpoints do Client VPN.

## Amazon CloudWatch

Monitora seus recursos da AWS e os aplicativos que você executa na AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode fazer o CloudWatch acompanhar o uso da CPU ou outras métricas das instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

## AWS CloudTrail

Captura chamadas de API e eventos relacionados criados pela sua conta da AWS ou em nome dela e fornece arquivos de log ao bucket do Amazon S3 que você especifica. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [AWS CloudTrail User Guide](#).

## Amazon CloudWatch Logs

Permite monitorar as tentativas de conexão feitas a seu endpoint AWS Client VPN. Você pode exibir as tentativas de conexão e as redefinições de conexão para as conexões do Client VPN. Você pode ver as tentativas de conexão bem-sucedidas e com falha. Você pode especificar o fluxo de log do CloudWatch Logs para registrar os detalhes da conexão em log. Para obter mais informações, consulte o [Amazon CloudWatch Logs User Guide](#).

## Amazon CloudWatch

O AWS Client VPN publica as seguintes métricas no Amazon CloudWatch para seus endpoints do Client VPN. As métricas são publicadas no Amazon CloudWatch a cada cinco minutos.

Métrica	Descrição
ActiveConnectionsCount	O número de conexões ativas ao endpoint do Client VPN.  Unidade: contagem
AuthenticationFailures	O número de falhas de autenticação para o endpoint do Client VPN.  Unidade: contagem
EgressBytes	Número de bytes enviados do endpoint do Client VPN.  Unidade: bytes

Métrica	Descrição
EgressPackets	O número de pacotes enviados do endpoint do Client VPN.  Unidade: contagem
IngressBytes	O número de bytes recebidos pelo endpoint do Client VPN.  Unidade: bytes
IngressPackets	O número de pacotes recebidos pelo endpoint do Client VPN.  Unidade: contagem

Você pode filtrar as métricas de seu endpoint do Client VPN por endpoint.

O CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Considere uma métrica como variável a ser monitorada, e os pontos de dados como valores dessa variável ao longo do tempo. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um alarme do CloudWatch para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair do que você considera um intervalo aceitável.

Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

## AWS CloudTrail

O AWS Client VPN é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações executadas por um usuário, uma função ou um serviço da AWS no Client VPN. O CloudTrail captura todas as chamadas de API para o Client VPN como eventos. As chamadas capturadas incluem as chamadas de código do console do Client VPN e as chamadas para as operações da API do Client VPN. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Client VPN. Se não configurar uma trilha, você ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Use as informações coletadas pelo CloudTrail para determinar a solicitação feita para o Client VPN, o endereço IP dessa solicitação, o solicitante, quando ela foi feita e outros detalhes adicionais.

Para obter mais informações sobre o CloudTrail, consulte o [AWS CloudTrail User Guide](#).

## Informações sobre o Client VPN no CloudTrail

O CloudTrail está habilitado na sua conta da AWS ao criá-la. Quando ocorre uma atividade no Client VPN, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e fazer download de eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro contínuo de eventos na sua conta da AWS, incluindo eventos para o Client VPN, crie uma trilha. Uma trilha permite CloudTrail para fornecer arquivos de log a um bucket do Amazon S3.

Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log para o bucket do Amazon S3 que você especificar. Além disso, é possível configurar outros serviços da AWS para analisar mais profundamente e agir sobre os dados de evento coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços compatíveis e integrações do CloudTrail](#)
- [Configuração de notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [Receber arquivos de log do CloudTrail de várias contas](#)

Todas as ações do Client VPN são registradas em log pelo CloudTrail e documentadas no [Amazon EC2 API Reference](#). Por exemplo, as chamadas para as ações `CreateClientVpnEndpoint`, `AssociateClientVpnTargetNetwork` e `AuthorizeClientVpnIngress` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte [Elemento `userIdentity` do CloudTrail](#).

## Noções básicas sobre as entradas dos arquivos de log do Client VPN

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log em um bucket do Amazon S3 que você especificar. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e hora da ação, parâmetros de solicitação, e assim por diante. arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas da API pública. Assim, elas não são exibidas em nenhuma ordem específica.



# Cotas de AWS Client VPN

Sua conta da AWS tem as seguintes cotas relacionadas a endpoints do Client VPN. É possível solicitar o aumento de algumas dessas cotas.

- Número de endpoints do Client VPN por região: 5
- Número de regras de autorização por endpoint do Client VPN: 50
- Número de rotas por endpoint do Client VPN: 10
- Número de conexões de cliente simultâneas por endpoint do Client VPN: 2.000
- Número de operações simultâneas por endpoint do Client VPN: 10

As operações incluem:

- Associar ou desassociar sub-redes
- Criar ou excluir rotas
- Criar ou excluir regras de entrada e de saída
- Criar ou excluir grupos de segurança

Leve o seguinte em consideração ao usar endpoints do Client VPN.

- O endpoint do Client VPN deve pertencer à mesma conta que a VPC que contém a sub-rede que você deseja associar ao endpoint do Client VPN.
- Se você usar o Active Directory para autenticar o usuário, o endpoint do Client VPN deverá pertencer à mesma conta que o recurso do AWS Directory Service usado para autenticação do Active Directory.

# Solução de problemas do Client VPN

O tópico a seguir pode ajudar a solucionar problemas que possam surgir com um endpoint do Client VPN.

Para obter mais informações sobre como solucionar problemas de software baseado em OpenVPN que os clientes usam para se conectar a um Client VPN, consulte [Solução de problemas de conexão do Client VPN](#) no Guia do usuário do AWS Client VPN.

## Problemas comuns

- [Não é possível resolver o nome DNS do endpoint do Client VPN \(p. 46\)](#)
- [O tráfego não está sendo dividido entre as sub-redes \(p. 46\)](#)
- [Regras de autorização para grupos do Active Directory não funcionando conforme esperado \(p. 47\)](#)
- [Os clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet \(p. 48\)](#)
- [O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente \(p. 50\)](#)
- [O software cliente retorna erro TLS \(p. 51\)](#)
- [O software cliente retorna erros de nome de usuário e senha \(autenticação do Active Directory\) \(p. 52\)](#)
- [Clientes não conseguem se conectar \(autenticação mútua\) \(p. 52\)](#)

## Não é possível resolver o nome DNS do endpoint do Client VPN

### Problema

Não consigo resolver o nome DNS do endpoint do Client VPN.

### Causa

O arquivo de configuração do endpoint do Client VPN inclui um parâmetro chamado `remote-random-hostname`. Esse parâmetro força o cliente a preceder o nome DNS com uma string aleatória para impedir o armazenamento em cache de DNS. Alguns clientes não reconhecem esse parâmetro e, portanto, não precedem o nome DNS com a string aleatória necessária.

### Solução

Abra o arquivo de configuração do endpoint do Client VPN usando seu editor de texto preferido. Localize a linha que especifica o nome DNS do endpoint do Client VPN e preceda-a com uma string aleatória para que o formato seja `string_aleatória.nome_DNS_exibido`. Por exemplo:

- Nome DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nome DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

## O tráfego não está sendo dividido entre as sub-redes

### Problema

Estou tentando dividir o tráfego de rede entre duas sub-redes. O tráfego privado deve ser roteado por uma sub-rede privada, enquanto o tráfego da Internet deve ser roteado por uma sub-rede pública. No entanto, somente uma rota está sendo usada, embora eu tenha adicionado ambas as rotas à tabela de rotas do endpoint do Client VPN.

#### Causa

É possível associar várias sub-redes a um endpoint do Client VPN, mas somente uma sub-rede por zona de disponibilidade. O objetivo da associação de várias sub-redes é fornecer alta disponibilidade e redundância de zona de disponibilidade para os clientes. No entanto, o Client VPN não permite dividir o tráfego seletivamente entre as sub-redes associadas ao endpoint do Client VPN.

Os clientes se conectam a um endpoint do Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

Por exemplo, digamos que você configure as seguintes associações de sub-rede e rotas:

- Associações de sub-rede
  - Associação 1: sub-rede A (us-east-1a)
  - Associação 2: sub-rede B (us-east-1b)
- Rotas
  - Rota 1: 10.0.0.0/16 roteada para a sub-rede A
  - Rota 2: 172.31.0.0/16 roteada para a sub-rede B

Neste exemplo, os clientes que entrarem na sub-rede A quando se conectarem não poderão acessar a Rota 2, enquanto os clientes que aterrissarem na sub-rede B quando se conectarem não poderão acessar a Rota 1.

#### Solução

Verifique se o endpoint do Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede pela qual seu tráfego seja roteado.

## Regras de autorização para grupos do Active Directory não funcionando conforme esperado

#### Problema

Configurei regras de autorização para meus grupos do Active Directory, mas elas não estão funcionando como eu esperava. Adicionei uma regra de autorização para 0.0.0.0/0 para autorizar o tráfego para todas as redes, mas ainda há falha no tráfego para CIDRs de destino específicos.

#### Causa

As regras de autorização são indexadas em CIDRs de rede. As regras de autorização devem conceder aos grupos do Active Directory acesso a CIDRs de rede específicos. As regras de autorização para 0.0.0.0/0 são tratadas como um caso especial e, portanto, são avaliadas por último, independentemente da ordem na qual as regras de autorização são criadas.

Por exemplo, digamos que você crie três regras de autorização na seguinte ordem:

- Regra 1: acesso do grupo 1 a 10.1.0.0/16
- Regra 2: acesso do grupo 1, do grupo 2 e do grupo 3 a 0.0.0.0/0
- Regra 3: acesso do grupo 2 a 172.131.0.0/16

Neste exemplo, a regra 2 é avaliada por último. O grupo 1 tem acesso somente a 10.1.0.0/16, e o grupo 2 tem acesso somente a 172.131.0.0/16. O grupo 3 não tem acesso a 10.1.0.0/16 ou a 172.131.0.0/16, mas tem acesso a todas as outras redes. Se você remover as regras 1 e 3, todos os três grupos terão acesso a todas as redes.

Além disso, o Client VPN usa a correspondência de prefixo mais longa ao avaliar as regras de autorização.

#### Solução

Verifique se as regras de autorização criadas concedem explicitamente aos grupos do Active Directory acesso a CIDRs de rede específicos. Se você adicionar uma regra de autorização para 0.0.0.0/0, tenha em mente que ela será avaliada por último e que as regras de autorização anteriores podem limitar as redes às quais ela concede acesso.

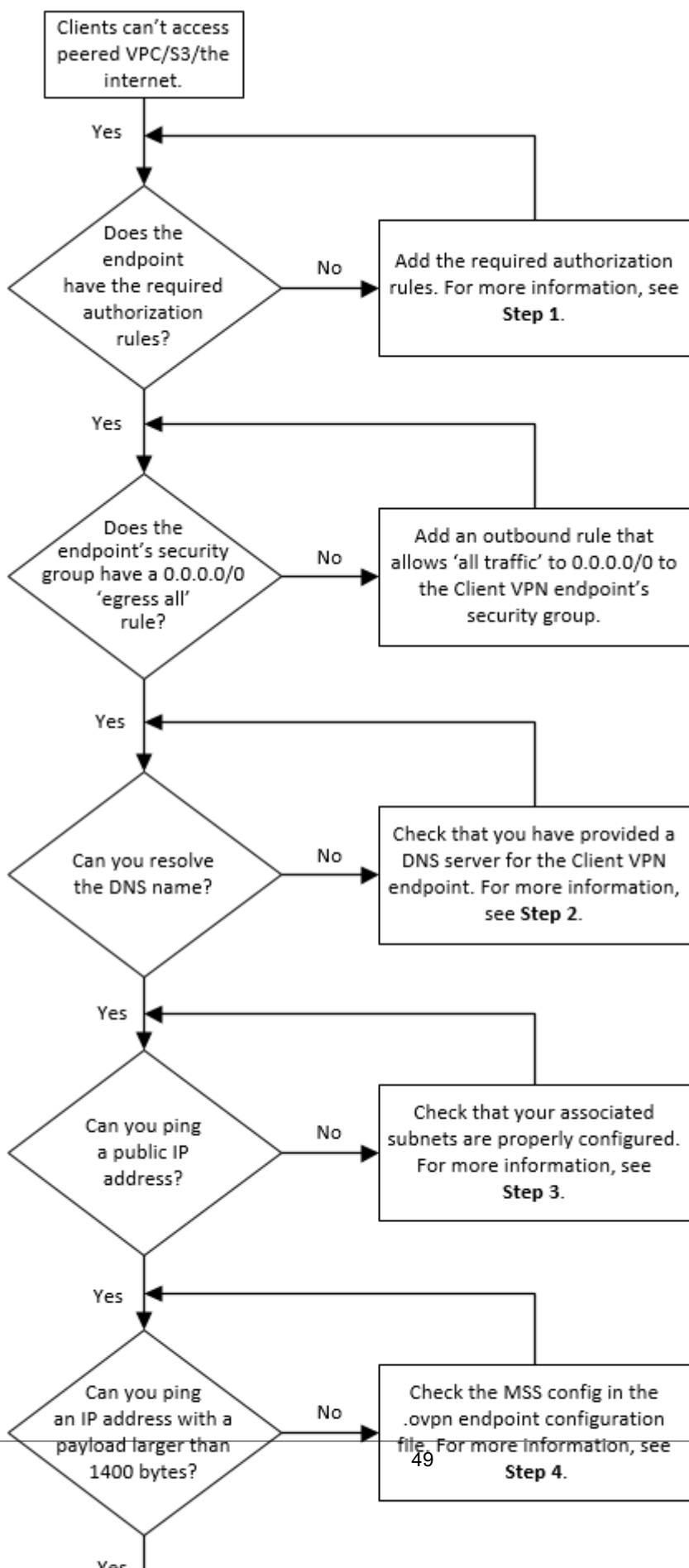
## Os clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet

#### Problema

Configurei corretamente minhas rotas do endpoint do Client VPN, mas meus clientes não podem acessar uma VPC emparelhada, o Amazon S3 ou a Internet.

#### Solução

O fluxograma a seguir contém as etapas para diagnosticar problemas de conectividade da Internet, da VPC emparelhada e do Amazon S3.



1. Para acesso à Internet, adicione uma regra de autorização para 0.0.0.0/0.

Para acesso a uma VPC emparelhada, adicione uma regra de autorização para o intervalo CIDR IPv4 da VPC.

Para acesso ao S3, especifique o endereço IP do endpoint do Amazon S3.

2. Verifique se é possível resolver o nome DNS.

Se não for possível resolver o nome DNS, verifique se você especificou os servidores DNS para o endpoint do Client VPN. Se você gerenciar seu próprio servidor DNS, especifique seu endereço IP. Verifique se o servidor DNS é acessível pela VPC.

Se você não tiver certeza sobre qual endereço IP usar, use o IP .2 do resolvedor de DNS da VPC.

3. Verifique se é possível executar ping em um endereço IP. Se não receber uma resposta, certifique-se de que a tabela de rotas para as sub-redes associadas tenha uma rota padrão que tenha como destino um gateway da Internet ou um gateway NAT. Se a rota padrão estiver em vigor, certifique-se de que a sub-rede associada não tenha regras de lista de controle de acesso à rede que bloqueiem o tráfego de entrada e saída.

Se você não conseguir acessar uma VPC emparelhada, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para a VPC emparelhada.

Se não conseguir acessar o Amazon S3, certifique-se de que a tabela de rotas da sub-rede associada tenha uma entrada de rota para o VPC endpoint do gateway.

4. Verifique se é possível executar ping em um endereço IP público com uma carga maior que 1400 bytes. Use um dos seguintes comandos:

- Windows

```
C:\> ping 8.8.8.8 -l 1480 -f
```

- Linux

```
$ ping -s 1480 8.8.8.8 -M do
```

Se não for possível executar ping em um endereço IP com uma carga útil maior que 1400 bytes, abra o arquivo de configuração .ovpn do endpoint do Client VPN usando seu editor de texto preferido e adicione o seguinte.

```
mssfix 1328
```

## O acesso a uma VPC emparelhada, ao Amazon S3 ou à Internet está intermitente

### Problema

Tenho problemas de conectividade intermitentes ao me conectar a uma VPC emparelhada, ao Amazon S3 ou à Internet, mas o acesso a sub-redes associadas não foi afetado. Preciso me desconectar e reconectar para resolver os problemas de conectividade.

### Causa

Os clientes se conectam a um endpoint do Client VPN com base no algoritmo round-robin do DNS. Isso significa que o tráfego pode ser roteado por qualquer uma das sub-redes associadas quando eles estabelecem uma conexão. Portanto, eles poderão enfrentar problemas de conectividade se estiverem em uma sub-rede associada que não tenha as entradas de rota necessárias.

#### Solução

Verifique se o endpoint do Client VPN tem as mesmas entradas de rota com destinos para cada rede associada. Isso garante que os clientes tenham acesso a todas as rotas, independentemente da sub-rede associada pela qual o tráfego é roteado.

Por exemplo, digamos que o endpoint do Client VPN tenha três sub-redes associadas (sub-rede A, B e C) e que você queira habilitar o acesso à Internet para seus clientes. Para fazer isso, adicione três rotas 0.0.0.0/0 – uma que tenha como destino cada sub-rede associada:

- Rota 1: 0.0.0.0/0 para a sub-rede A
- Rota 2: 0.0.0.0/0 para a sub-rede B
- Rota 3: 0.0.0.0/0 para a sub-rede C

## O software cliente retorna erro TLS

#### Problema

Antes eu podia conectar meus clientes ao Client VPN com êxito, mas agora o cliente baseado em OpenVPN-retorna o seguinte erro quando ele tenta se conectar:

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

#### Possíveis causas

Se você usa autenticação mútua e importou uma lista de revogação de certificados de cliente, a lista de revogação de certificados de cliente pode ter expirado. Durante a fase de autenticação, o endpoint do Client VPN verifica o certificado de cliente em relação à lista de revogação de certificados de cliente importada. Se a lista de revogação de certificados de cliente tiver expirado, não será possível conectar-se ao endpoint do Client VPN.

Como alternativa, pode haver um problema com o software baseado em OpenVPN que o cliente está usando para se conectar ao Client VPN.

#### Solução

Verifique a data de expiração da lista de revogação de certificados do cliente usando a ferramenta OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

A saída exibe a data e a hora de expiração. Se a lista de revogação de certificados do cliente tiver expirado, você deverá criar uma nova e importá-la para o endpoint do Client VPN. Para obter mais informações, consulte [Listas de revogação de certificados de cliente \(p. 37\)](#).

Para obter mais informações sobre como solucionar problemas de software baseado em OpenVPN, consulte [Solução de problemas de conexão do Client VPN](#) no Guia do usuário do AWS Client VPN.

## O software cliente retorna erros de nome de usuário e senha (autenticação do Active Directory)

### Problema

Uso a autenticação do Active Directory para meu endpoint do Client VPN e antes podia conectar meus clientes ao Client VPN com êxito. Mas agora, os clientes estão recebendo erros de nome de usuário e senha inválidos.

### Possíveis causas

Se usar a autenticação do Active Directory e se tiver habilitado a autenticação multifator (MFA) depois de distribuir o arquivo de configuração do cliente, o arquivo não conterá as informações necessárias para pedir aos usuários que insiram o código da MFA. Os usuários são solicitados a inserir o nome de usuário e a senha, mas há falha na autenticação.

### Solução

Baixe um novo arquivo de configuração do cliente e distribua-o para seus clientes. Verifique se o novo arquivo contém a seguinte linha:

```
static-challenge "Enter MFA code " 1
```

Para obter mais informações, consulte [Exportar a configuração do cliente \(p. 30\)](#). Teste a configuração de MFA para o Active Directory sem usar o endpoint do Client VPN para verificar se a MFA está funcionando conforme o esperado.

## Clientes não conseguem se conectar (autenticação mútua)

### Problema

Uso autenticação mútua para o meu endpoint do Client VPN. Os clientes estão recebendo erros de falha na negociação de chave TLS e erros de tempo limite.

### Possíveis causas

O arquivo de configuração que foi fornecido aos clientes não contém o certificado do cliente e a chave privada do cliente ou o certificado e a chave estão incorretos.

### Solução

Certifique-se de que o arquivo de configuração contenha o certificado e a chave do cliente corretos. Se necessário, corrija o arquivo de configuração e redistribua-o para seus clientes. Para obter mais informações, consulte [Exportar a configuração do cliente \(p. 30\)](#).



# Histórico do documento

A tabela a seguir descreve as atualizações do Guia do administrador do AWS Client VPN.

update-history-change	update-history-description	update-history-date
<a href="#">Especificar grupos de segurança durante a criação</a>	Você pode especificar uma VPC e grupos de segurança ao criar o endpoint do AWS Client VPN.	March 5, 2020
<a href="#">Portas VPN configuráveis</a>	Você pode especificar um número de porta VPN compatível para seu endpoint do AWS Client VPN.	January 16, 2020
<a href="#">Suporte à autenticação multifator (MFA)</a>	Seu endpoint do AWS Client VPN será compatível com a MFA se estiver habilitado para o Active Directory.	September 30, 2019
<a href="#">Suporte a túnel dividido</a>	Você pode habilitar o túnel dividido no endpoint do AWS Client VPN.	July 24, 2019
<a href="#">Versão inicial (p. 53)</a>	Essa versão apresenta o AWS Client VPN.	December 18, 2018