Manual do usuário

AWS Direct Connect

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Direct Connect: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

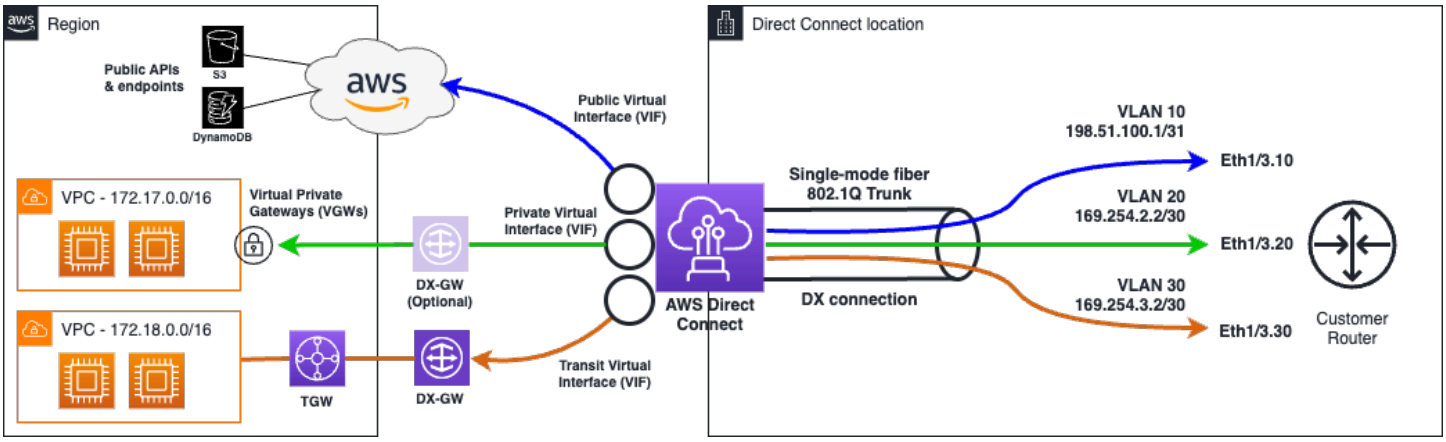
Table of Contents

O que é o Direct Connect?

O Direct Connect vincula sua rede interna a um local do Direct Connect usando um cabo de fibra óptica Ethernet padrão. Uma extremidade do cabo é conectada ao roteador, e a outra é conectada a um roteador do Direct Connect. Com essa conexão, é possível criar interfaces virtuais diretamente para serviços públicos da AWS (p. ex., para o Amazon S3) ou para a Amazon VPC, ignorando provedores de serviço de Internet no caminho da rede. Um local do Direct Connect dá acesso à AWS na região à qual está associado. É possível usar uma só conexão em uma região pública ou na região AWS GovCloud (US) para acessar serviços públicos da AWS em todas as outras regiões públicas.

- Para obter uma lista das localizações do Direct Connect às quais você pode se conectar, consulte AWS Direct Connect Locations.
- Para obter respostas a perguntas sobre o Direct Connect, consulte as Perguntas frequentes do Direct Connect.

O diagrama a seguir apresenta uma visão de alto nível de como o Direct Connect faz interface com sua rede.



Conteúdo

- Direct Connect políticas de roteamento e comunidades BGP

Componentes do Direct Connect

A seguir, apresentamos os principais componentes que você usa no Direct Connect:

Conexões

Crie uma conexão em um local do Direct Connect para estabelecer uma conexão de rede do seu local até uma região da AWS. Para obter mais informações, consulte Direct Connect conexões dedicadas e hospedadas.

Interfaces virtuais

Crie uma interface virtual para viabilizar o acesso a serviços da AWS. Uma interface virtual pública permite acessar serviços públicos, como o Amazon S3. Uma interface virtual privada permite o acesso à VPC. Os tipos de interfaces compatíveis estão descritos abaixo em the section called “Tipos de interfaces virtuais compatíveis com o Direct Connect”. Para obter mais detalhes sobre as interfaces compatíveis, consulte Direct Connect interfaces virtuais e interfaces virtuais hospedadas e Pré-requisitos para interfaces virtuais.

Requisitos de rede

Para usar o Direct Connect em um local do Direct Connect, a rede deve atender a uma das seguintes condições:

- A rede é co-locada com um local do Direct Connect existente. Para obter mais informações sobre locais disponíveis do Direct Connect, consulte Detalhes do produto AWS Direct Connect.
- Você está trabalhando com um parceiro do Direct Connect que integra a Rede de Parceiros da AWS (APN). Para obter informações, consulte Parceiros da APN que oferecem o AWS Direct Connect.
- Você está trabalhando com um provedor de serviços independente para se conectar ao Direct Connect.

Além disso, a rede deve atender às seguintes condições:

- Sua rede deve usar fibra monomodo com um transceptor 1000BASE-LX (1.310 nm) para Ethernet de 1 gigabit, um transceptor 10GBASE-LR (1.310 nm) para 10 gigabits, um 100GBASE-LR4 para Ethernet de 100 gigabits, ou um 400GBASE-LR4 para Ethernet de 400 gigabits.
- Dependendo do endpoint do AWS Direct Connect que forneça sua conexão, pode ser necessário habilitar ou desabilitar a negociação automática de dispositivo on-premises para qualquer conexão dedicada. Se uma interface virtual permanecer inativa quando uma conexão do Direct Connect estiver ativa, consulte Solucionar problemas da camada 2 (link de dados).
- É necessário ter compatibilidade com o encapsulamento 802.1Q de VLAN em toda a conexão, incluindo em dispositivos intermediários.
- O dispositivo deve ser compatível com Protocolo de Gateway da Borda (BGP) e autenticação MD5 do BGP.
- (Opcional) Você também pode configurar a Bidirectional Forwarding Detection (BFD – Detecção de encaminhamento bidirecional) em sua rede. A BFD assíncrona é habilitada automaticamente para cada interface virtual do Direct Connect. Ela é habilitada automaticamente para interfaces virtuais do Direct Connect, mas não entrará em vigor até você configurá-la em seu roteador. Para obter mais informações, consulte Habilitar a BFD para uma conexão do Direct Connect.

O Direct Connect é compatível com os protocolos de comunicação IPv4 e IPv6. Os endereços IPv6 fornecidos por serviços públicos da AWS são acessíveis por meio de interfaces virtuais públicas do Direct Connect.

O Direct Connect oferece suporte a um quadro Ethernet de 1.522 ou 9.023 bytes (cabeçalho Ethernet de 14 bytes + tag VLAN de 4 bytes + bytes para o datagrama IP + FCS de 4 bytes) na camada de link. Você pode definir a MTU de suas interfaces virtuais privadas. Para obter mais informações, consulte MTUs para interfaces virtuais privadas ou interfaces virtuais de trânsito.

Tipos de interfaces virtuais compatíveis com o Direct Connect

O AWS Direct Connect é compatível com os seguintes três tipos de interface virtual (VIF):

- Interface virtual privada

  Esse tipo de interface é usado para acessar uma Amazon Virtual Private Cloud (VPC) com endereços IP privados. Com uma interface virtual privada, é possível:

  - Conectar-se diretamente a uma única VPC por interface virtual privada para acessar os recursos dela usando IPs privados dentro da mesma região.

  - Conectar uma interface virtual privada a um gateway do Direct Connect para acessar diversos gateways privados virtuais em qualquer conta e região da AWS (com exceção das regiões da AWS na China).
- Interface virtual pública

  Esse tipo de interface virtual é usado para acessar todos os serviços públicos da AWS usando endereços IP públicos. Com uma interface virtual pública, é possível estabelecer conexão com todos os endereços IP públicos e serviços da AWS globalmente.
- Interface virtual de trânsito

  Esse tipo de interface é usado para acessar um ou mais gateways de trânsito da Amazon VPC associados a gateways do Direct Connect. Com uma interface virtual de trânsito, é possível estabelecer conexão com diversos gateways de trânsito da Amazon VPC entre várias contas e Regiões da AWS (exceto nas regiões da AWS na China).

> **Note**
>
> Existem limites para o número de diferentes tipos de associações entre um gateway do Direct Connect e uma interface virtual. Para obter mais informações sobre os limites específicos, consulte a página Cotas do Direct Connect.

Para obter mais informações sobre as interfaces virtuais, consulte Interfaces virtuais e interfaces virtuais hospedadas.

Preços para o Direct Connect

O AWS Direct Connect tem dois elementos de faturamento: horas de porta e transferência de dados de saída. A definição de preço de porta-hora é determinada pela capacidade e pelo tipo de conexão (conexão dedicada ou hospedada).

As cobranças de transferência de dados de saída de interfaces privadas e interfaces virtuais de trânsito são alocadas para a conta da AWS responsável pela transferência de dados. Não há cobranças adicionais para usar um gateway do AWS Direct Connect de várias contas.

Para recursos endereçáveis publicamente da AWS (p. ex., buckets do Amazon S3, instâncias do EC2 Classic ou tráfego do EC2 que passe por um gateway da Internet), se o tráfego de saída for destinado a prefixos públicos de propriedade da mesma conta pagante da AWS e anunciado

ativamente para a AWS por meio de uma interface virtual pública do Direct Connect, o uso de transferência de dados de saída (DTO) será medido para o proprietário do recurso segundo a taxa de transferência de dados do Direct Connect.

Para obter mais informações, consulte Preços do AWS Direct Connect.

Acesso a regiões remotas do Direct Connect

Os locais do Direct Connect em regiões públicas ou na região AWS GovCloud (US) podem acessar serviços públicos em qualquer outra região pública (exceto China [Pequim e Ningxia]). Além disso, as conexões do Direct Connect em regiões públicas ou na região AWS GovCloud (US) podem ser configuradas para acessar uma VPC em sua conta de qualquer outra região pública (exceto China [Pequim e Ningxia]). Dessa forma, você pode usar uma única conexão do Direct Connect para criar serviços em várias Regiões. Todo o tráfego de rede permanece no backbone da rede global da AWS, independentemente de você acessar serviços públicos da AWS ou uma VPC em outra Região.

Toda transferência de dados fora de uma Região remota é cobrada segundo a taxa de transferência de dados da Região remota. Para obter mais informações sobre os preços de transferência de dados, consulte a seção Preços na página de detalhes do AWS Direct Connect.

Para obter mais informações sobre as políticas de roteamento e comunidades BGP compatíveis para uma conexão do Direct Connect, consulte Políticas de roteamento e comunidades BGP.

Acesso a serviços públicos em uma região remota

Para acessar recursos públicos em uma Região remota, é necessário configurar uma interface virtual pública e estabelecer uma sessão do Border Gateway Protocol (BGP). Para obter mais informações, consulte Interfaces virtuais e interfaces virtuais hospedadas.

Após a criação de uma interface virtual pública e o estabelecimento de uma sessão do BGP nela, o roteador aprenderá as rotas das outras Regiões públicas da AWS. Para obter mais informações sobre os prefixos anunciados pela AWS no momento, consulte Intervalos de endereços IP da AWS no Referência geral da Amazon Web Services.

Acesso a VPCs em uma região remota

Crie um Direct Connect gateway (Gateway Direct Connect) em qualquer região pública. Use-o para conectar sua conexão do Direct Connect por meio de uma interface virtual privada às VPCs em sua conta localizadas em regiões diferentes ou a um gateway de trânsito. Para obter mais informações, consulte Gateways do Direct Connect.

Como alternativa, crie uma interface virtual pública para sua conexão do Direct Connect e, em seguida, estabeleça uma conexão VPN com sua VPC na Região remota. Para obter mais informações sobre como configurar a conectividade da VPN para uma VPC, consulte Cenários de uso da Amazon Virtual Private Cloud no Guia do usuário da Amazon VPC.

Opções de conectividade de rede para Amazon VPC

É possível usar a configuração a seguir para conectar redes remotas ao seu ambiente Amazon VPC. Essas opções são úteis para integrar recursos da AWS aos seus serviços existentes no local:

- Opções de conectividade da Amazon Virtual Private Cloud

Direct Connect políticas de roteamento e comunidades BGP

Direct Connect aplica políticas de roteamento de entrada (do seu data center local) e de saída (da sua AWS região) para uma conexão pública. Direct Connect Você também pode usar tags da comunidade do Protocolo de Gateway da Borda (BGP) em rotas anunciadas pela Amazon e aplicar tags da comunidade do BGP às rotas que você anuncia para a Amazon.

Políticas de roteamento de interface virtual pública

Se você estiver usando Direct Connect para acessar AWS serviços públicos, você deve especificar os prefixos públicos ou IPv4 IPv6 prefixos para anunciar no BGP.

As seguintes políticas de roteamento de entrada se aplicam:

- Você deve ter os prefixos públicos e eles devem estar registrados como tal no registro regional da Internet apropriado.
- O tráfego deve ser destinado a prefixos públicos da Amazon. Não há suporte para o roteamento transitivo entre as conexões.
- Direct Connect executa a filtragem de pacotes de entrada para validar se a origem do tráfego se originou do prefixo anunciado.

As seguintes políticas de roteamento de saída se aplicam:

- AS_PATH e Longest Prefix Match são usados para determinar o caminho de roteamento. AWS recomenda anunciar rotas mais específicas usando Direct Connect se o mesmo prefixo estiver sendo anunciado na Internet e em uma interface virtual pública.

- Direct Connect anuncia todos os prefixos de AWS região locais e remotos quando disponíveis e inclui prefixos na rede de outros pontos de presença (PoP) AWS fora da região, quando disponíveis; por exemplo, e o Route 53. CloudFront

  > **Note**
  >
  > - Os prefixos listados no arquivo JSON de intervalos de endereços AWS IP, ip-ranges.json, para as regiões da China são anunciados somente nas regiões da AWS China. AWS
  > - Os prefixos listados no arquivo JSON de intervalos de endereços AWS IP, ip-ranges.json, para as regiões comerciais são anunciados somente nas regiões AWS comerciais. AWS
  >
  > Para obter mais informações sobre o arquivo ip-ranges.json, consulte Intervalos de endereços IP da AWS no Referência geral da AWS.

- Direct Connect anuncia prefixos com um comprimento mínimo de caminho de 3.
- Direct Connect anuncia todos os prefixos públicos na conhecida comunidade `NO_EXPORT` BGP.
- Se você anunciar os mesmos prefixos de duas regiões diferentes usando duas interfaces virtuais públicas diferentes e ambas tiverem os mesmos atributos de BGP e o maior comprimento de prefixo, AWS priorizará a região de origem para tráfego de saída.
- Se você tiver várias Direct Connect conexões, poderá ajustar o compartilhamento de carga do tráfego de entrada anunciando prefixos com os mesmos atributos de caminho.
- Os prefixos anunciados por não Direct Connect devem ser anunciados além dos limites da rede da sua conexão. Por exemplo, esses prefixos não devem ser incluídos em nenhuma tabela de roteamento de Internet pública.
- Direct Connect mantém os prefixos anunciados pelos clientes na rede Amazon. Não reanunciamos os prefixos de clientes aprendidos em uma VIF pública para nenhuma das seguintes opções:
  - Outros Direct Connect clientes
  - Redes que se relacionam com a Rede AWS Global
  - Provedores de trânsito da Amazon
- Ao usar uma interface pública, você pode usar um ASN público ou privado. No entanto, há considerações importantes:
  - Público ASNs: você deve possuir o ASN e ter o direito de anunciá-lo. AWS verificará sua propriedade do ASN. Tanto ASNs (1-2147483647) quanto longos ASNs (1-4294967295) são suportados.

- Privado ASNs: você pode usar o privado a ASNs partir dos seguintes intervalos:
  - privado ASNs: 64512-65534
  - longo privado ASNs: 4200000000-4294967294

  No entanto, Direct Connect substituirá o ASN privado pelo AWS ASN (7224) ao anunciar seus prefixos para outros AWS clientes ou para a Internet.
- Prefixos do ASN:
  - Com um ASN público (tanto ASN quanto ASN longo), o prefixo funcionará conforme esperado e o prefixo do ASN ficará visível para outras redes.
  - Com um ASN privado (tanto ASN quanto ASN longo), qualquer prependência que você fizer será eliminada ao AWS substituir seu ASN privado por 7224. Isso significa que a prependência de ASN não é eficaz para influenciar decisões de roteamento fora do uso de AWS um ASN privado em uma interface virtual pública.
- Ao estabelecer uma sessão de emparelhamento do BGP com AWS uma interface virtual pública, use 7224 para os números do sistema autônomo (ASN) para estabelecer a sessão do BGP na lateral. AWS O ASN em seu roteador ou dispositivo de gateway do cliente deve ser diferente desse ASN. O ASN do seu cliente pode ser um ASN (1-2147483647, excluindo os intervalos reservados) ou um ASN longo (1-4294967295, excluindo os intervalos reservados).

Comunidades BGP de interface virtual pública

Direct Connect suporta tags de comunidade BGP de escopo para ajudar a controlar o escopo (regional ou global) e a preferência de rota do tráfego em interfaces virtuais públicas. AWS trata todas as rotas recebidas de uma VIF pública como se estivessem marcadas com a tag da comunidade NO_EXPORT BGP, o que significa que somente a AWS rede usará essas informações de roteamento.

Definir o escopo de comunidades BGP

Você pode aplicar tags da comunidade BGP nos prefixos públicos anunciados na Amazon para indicar a distância de propagação de seus prefixos na rede da Amazon, somente para a região local da AWS , em todas as regiões de um continente ou em todas as regiões públicas.

Região da AWS comunidades

Para políticas de roteamento de entrada, você pode usar as seguintes comunidades do BGP para seus prefixos:

- `7224:9100`— Local Regiões da AWS
- `7224:9200`—Tudo Regiões da AWS por um continente:
  - Por toda a extensão da América do Norte
  - Ásia-Pacífico
  - Europa, Oriente Médio e África
- `7224:9300`—Global (todas as AWS regiões públicas)

> **Note**
>
> Se você não aplicar nenhuma tag de comunidade, os prefixos serão anunciados em todas as AWS regiões públicas (globais) por padrão.
> Os prefixos marcados com as mesmas comunidades e que contêm atributos AS_PATH idênticos são candidatos à utilização de vários caminhos.

As comunidades `7224:1` – `7224:65535` são reservadas pelo Direct Connect.

Para políticas de roteamento de saída, Direct Connect aplica as seguintes comunidades BGP às rotas anunciadas:

- `7224:8100`—Rotas que se originam da mesma AWS região em que o Direct Connect ponto de presença está associado.
- `7224:8200`—Rotas originárias do mesmo continente ao qual o Direct Connect ponto de presença está associado.
- Sem tag: rotas com origem em outros continentes.

> **Note**
>
> Para receber todos os prefixos AWS públicos, não aplique nenhum filtro.

As comunidades que não têm suporte para uma conexão Direct Connect pública são removidas.

Comunidade BGP **NO_EXPORT**

Para políticas de roteamento de saída, a tag NO_EXPORT de comunidade do BGP é compatível com interfaces virtuais públicas.

Direct Connect também fornece tags comunitárias do BGP nas rotas anunciadas da Amazon. Se você usa Direct Connect para acessar AWS serviços públicos, pode criar filtros com base nessas tags da comunidade.

Para interfaces virtuais públicas, todas as rotas Direct Connect anunciadas aos clientes são marcadas com a tag da comunidade NO_EXPORT.

Políticas de roteamento da interface virtual privada e da interface virtual de trânsito

Se você estiver usando AWS Direct Connect para acessar seus AWS recursos privados, você deve especificar os IPv6 prefixos IPv4 ou para anunciar no BGP. Esses prefixos podem ser públicos ou privados.

As seguintes regras de rotas de saída se aplicam com base nos prefixos anunciados:

- AWS avalia primeiro o comprimento do prefixo mais longo. AWS recomenda anunciar rotas mais específicas usando várias interfaces virtuais do Direct Connect se os caminhos de roteamento desejados forem destinados a active/passive conexões. Para obter mais informações, consulte Influencing Traffic over Hybrid Networks using Longest Prefix Match.
- A preferência local é o atributo BGP recomendado para uso quando os caminhos de roteamento desejados são destinados a active/passive conexões e os comprimentos de prefixo anunciados são os mesmos. Esse valor é definido por região para preferir AWS Direct Connect locais que tenham o mesmo associado Região da AWS usando o valor 7224:7200 —Médio da comunidade de preferência local. Quando a região local não está associada à localização do Direct Connect, ocorre a atribuição de um valor inferior. Isso se aplica somente se não houver etiquetas de comunidade de preferência local atribuídas.
- O comprimento do AS_PATH pode ser usado para determinar o caminho de rota quando o comprimento do prefixo e a preferência local são semelhantes.
- O Multi-Exit Discriminator (MED) pode ser usado para determinar o caminho de roteamento quando o comprimento do prefixo, a preferência local e AS_PATH são iguais. AWS não recomenda o uso de valores de MED devido à sua menor prioridade na avaliação.

- AWS usa roteamento de vários caminhos (ECMP) de custo igual em várias interfaces virtuais privadas ou de trânsito quando os prefixos têm o mesmo comprimento AS_PATH e atributos BGP. Os prefixos ASNs no AS_PATH não precisam corresponder.

Comunidades BGP de interface virtual privada e interface virtual de trânsito

Quando um Região da AWS roteia o tráfego para locais locais por meio de interfaces virtuais privadas ou de trânsito do Direct Connect, o associado ao local Região da AWS do Direct Connect influencia a capacidade de usar o ECMP. Regiões da AWS prefira locais do Direct Connect no mesmo local associado Região da AWS por padrão. Consulte AWS Direct Connect Locations para identificar a Região da AWS associada a uma determinada localização do Direct Connect.

Quando não existem etiquetas de comunidade de preferência local aplicadas, o Direct Connect fornece suporte para ECMP em interfaces virtuais privadas ou de trânsito para prefixos com o mesmo comprimento do AS_PATH e valor do MED em dois ou mais caminhos nos seguintes cenários:

- O tráfego de Região da AWS envio tem dois ou mais caminhos de interface virtual de locais no mesmo local associado Região da AWS, seja na mesma instalação ou em instalações de colocation diferentes.
- O tráfego de Região da AWS envio tem dois ou mais caminhos de interface virtual de locais que não estão na mesma região.

Para obter mais informações, consulte Como faço para configurar uma conexão Active/Active ou Active/Passive Direct Connect a AWS partir de uma interface virtual privada ou de trânsito?

> **Note**
>
> Isso não tem efeito no ECMP Região da AWS de e para locais locais.

Para controlar as preferências de direcionamento, o Direct Connect fornece suporte para etiquetas de comunidade de preferência local de BGP para interfaces virtuais privadas e para interfaces virtuais de trânsito.

Comunidades BGP de preferência local

Você pode usar as tags de comunidade BGP de preferência local para obter o balanceamento de carga e a preferência de rota para o tráfego de entrada para sua rede. Para cada prefixo anunciado em uma sessão BGP, você pode aplicar uma tag de comunidade para indicar a prioridade do caminho associado no qual retornar o tráfego.

As seguintes tags de comunidade BGP de preferência local têm suporte:

- `7224:7100`- baixa preferência
- `7224:7200`- média preferência
- `7224:7300`- alta preferência

As tags de comunidade BGP de preferência local são mutuamente exclusivas. Para balancear a carga do tráfego em várias Direct Connect conexões (ativas/ativas) hospedadas na mesma região ou em AWS regiões diferentes, aplique a mesma tag de comunidade; por exemplo, `7224:7200` (preferência média) nos prefixos das conexões. Caso uma das conexões apresente falhas, o tráfego terá sua carga distribuída ao usar ECMP entre as conexões ativas remanescentes, sem considerar as associações de suas regiões de origem. Para oferecer suporte a failover em várias conexões do Direct Connect (ativas/passivas), aplique uma tag de comunidade com uma preferência mais alta aos prefixos da interface virtual principal ou ativa e uma preferência mais baixa aos prefixos da interface virtual passiva ou de backup. Por exemplo, defina as tags de comunidade do BGP para suas interfaces virtuais primárias ou ativas como `7224:7300` (alta preferência) e `7224:7100` (baixa preferência) para suas interfaces virtuais passivas.

As tags de comunidade BGP de preferência local são avaliadas antes de qualquer atributo AS_PATH e da menor para a maior preferência (quando a maior preferência tiver prioridade).

Suporte longo de ASN em Direct Connect

Support for long ASNs (4 bytes) permite que você configure números longos de sistema autônomo (ASNs) como parte dos parâmetros da sessão BGP estabelecida entre o dispositivo de rede e seu dispositivo de AWS rede. Esse recurso é habilitado ou desabilitado de acordo com a conta.

Você pode definir um intervalo de ASN ou ASN longo no console ou por meio do. APIs

- Ao usar o console, o campo ASN suporta ambos ASNs e por muito tempo ASNs. Você pode adicionar qualquer intervalo de 1 a 4294967294.

- Ao usar o APIs para criar uma interface virtual, você pode especificar um ASN (`asn`) ou o ASN longo (`asnLong`), mas não ambos. Para obter mais informações sobre como usar ASN ou ASN longo, consulte o seguinte APIs na Referência da Direct Connect API:
  - `BGPPeer`
  - `DeleteBGPPeerRequest`
  - `NewBGPPeer`
  - `NewPrivateVirtualInterface`
  - `NewPrivateVirtualInterfaceAllocation`
  - `NewPublicVirtualInterface`
  - `NewPublicVirtualInterfaceAllocation`
  - `NewTransitVirtualInterface`
  - `NewTransitVirtualInterfaceAllocation`
  - `VirtualInterface`

Considerações

Ao usar um ASN ou um ASN longo, observe o seguinte:

- Compatibilidade com versões anteriores: o Direct Connect gerencia automaticamente as sessões do BGP com roteadores compatíveis com ASN e ASN longo. Se o roteador não suportar muito tempo ASNs, a sessão do BGP operará no modo ASN.
- Formato ASN: você pode especificar 4 bytes ASNs em um formato simples — por exemplo, `4200000000` ou em formato asdot — por exemplo,. `64086.59904` O Direct Connect aceita os dois formatos, mas é exibido ASNs em um formato simples
- Intervalos de ASN privados: ao usar private long ASNs (`4200000000-4294967294`), o mesmo comportamento de substituição se aplica ao private ASNs. O Direct Connect substituirá seu ASN privado por `7224` quando anunciar para outras redes.
- Tags da comunidade BGP: todas as tags existentes da comunidade BGP (`7224:xxxx`) funcionam por muito tempo. ASNs O formato da tag da comunidade permanece inalterado.
- Monitoramento e solução de problemas: CloudWatch métricas, registros de sessão do BGP e ferramentas de solução de problemas são exibidos por muito tempo ASNs em um formato simples para fins de consistência.

Disponibilidade e preços

Observe o seguinte para suporte longo de ASN com Direct Connect:

- Disponibilidade: o ASN longo está disponível em todas as AWS regiões em que Direct Connect há suporte.
- Preços: Não há cobranças adicionais pelo suporte longo de ASN além do Direct Connect preço padrão.

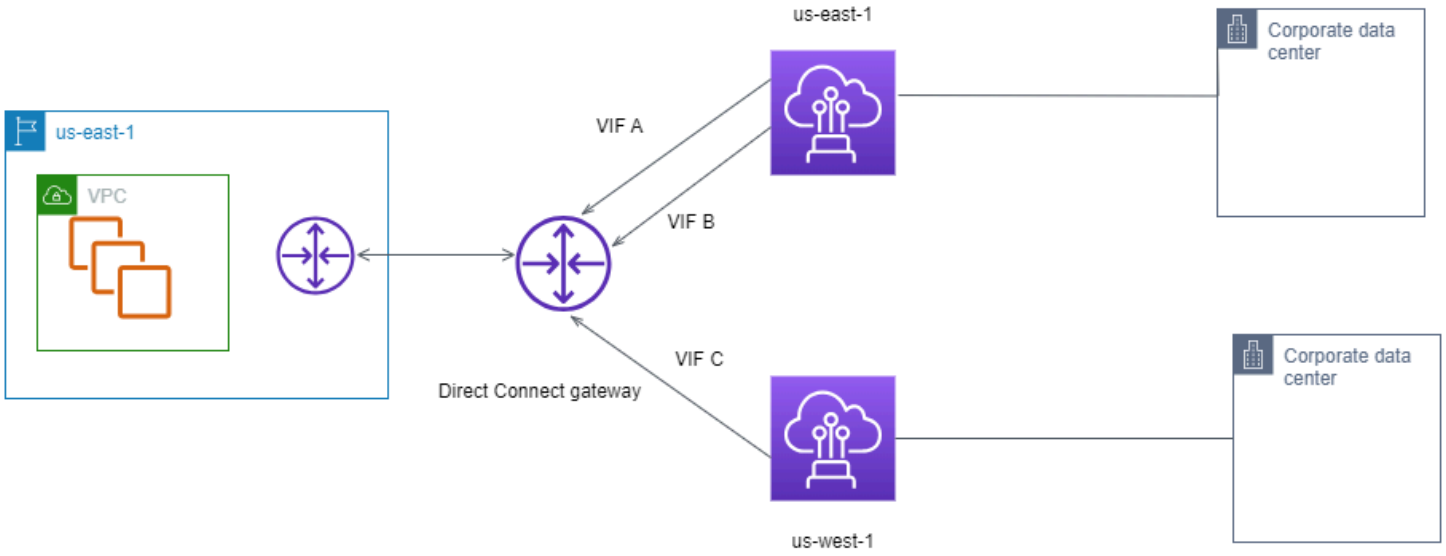
> **Note**
>
> A ativação de ASN longo se aplica a toda a sua conta. AWS Você não pode habilitar o suporte a ASN longo para interfaces virtuais individuais ou pares do BGP.

Direct Connect exemplo de roteamento de interface virtual privada

Considere a configuração em que a região de origem do Direct Connect local 1 é igual à região de origem da VPC. Há um Direct Connect local redundante em uma região diferente. Há dois locais privados VIFs (VIF A e VIF B) do local Direct Connect 1 (us-east-1) até o gateway Direct Connect. Há uma VIF privada (VIF C) do Direct Connect local (us-west-1) até o gateway Direct Connect. Para AWS rotear o tráfego pela VIF B antes da VIF A, defina o atributo AS_PATH da VIF B como menor do que o atributo AS_PATH da VIF A.

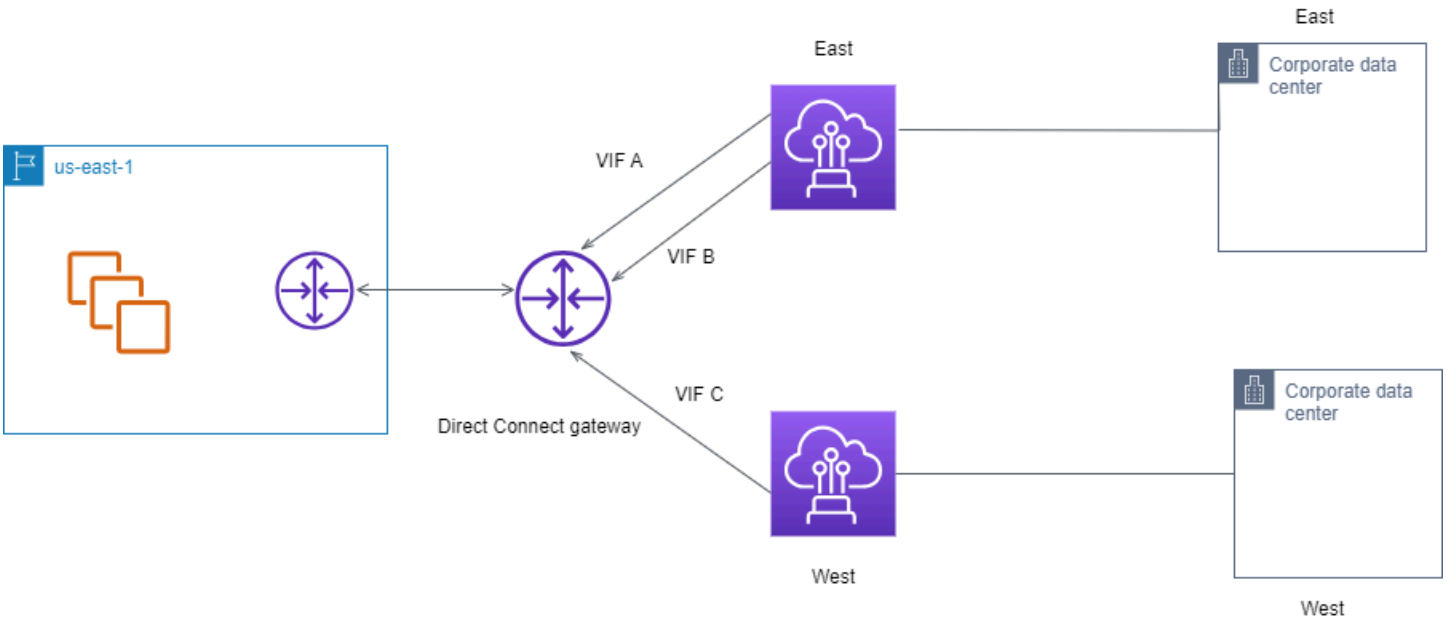
Eles VIFs têm as seguintes configurações:

- A VIF A (em us-east-1) anuncia 172.16.0.0/16 e tem um atributo AS_PATH de 65001, 65001, 65001
- A VIF B (em us-east-1) anuncia 172.16.0.0/16 e tem um atributo AS_PATH de 65001, 65001
- A VIF C (em us-west-1) anuncia 172.16.0.0/16 e tem um atributo AS_PATH de 65001



Se você alterar a configuração do intervalo de CIDR da VIF C, os direcionamentos que se enquadram no intervalo de CIDR da VIF C usarão a VIF C devido ao seu comprimento do prefixo mais longo.

- A VIF C (em us-west-1) anuncia 172.16.0.0/24 e tem um atributo AS_PATH de 65001



Direct Connect opções de conexão

AWS oferece aos clientes a capacidade de obter conexões de rede altamente resilientes entre a Amazon Virtual Private Cloud (Amazon VPC) e sua infraestrutura local. O AWS Direct Connect Resiliency Toolkit fornece um assistente de conexão com vários modelos de resiliência. Esses modelos ajudam você a determinar e solicitar o número de conexões dedicadas para atingir o objetivo de SLA. Você seleciona um modelo de resiliência e, em seguida, o AWS Direct Connect Resiliency Toolkit o orienta pelo processo de pedido de conexão dedicado. Os modelos de resiliência são projetados para garantir que você tenha o número apropriado de conexões dedicadas em vários locais.

As seguintes opções de conexão estão disponíveis para Direct Connect.

- Resiliência máxima: esse modelo está disponível no AWS Direct Connect Resiliency Toolkit e fornece uma maneira de solicitar conexões dedicadas para atingir um SLA de 99,99%. Ele exige que você atenda a todos os requisitos para obter o SLA especificado no Acordo de nível de serviço do Direct Connect. Para obter mais informações, consulte o AWS Direct Connect Kit de ferramentas de resiliência.
- Alta resiliência: esse modelo está disponível no AWS Direct Connect Resiliency Toolkit e fornece uma maneira de solicitar conexões dedicadas para atingir um SLA de 99,9%. Ele exige que você atenda a todos os requisitos para obter o SLA especificado no Acordo de nível de serviço do Direct Connect. Para obter mais informações, consulte o AWS Direct Connect Kit de ferramentas de resiliência.
- Desenvolvimento e teste: esse modelo está disponível no AWS Direct Connect Resiliency Toolkit e fornece um modo de obter resiliência de desenvolvimento e teste para workloads não críticas usando conexões separadas que são encerradas em dispositivos separados em um único local. Para obter mais informações, consulte o AWS Direct Connect Kit de ferramentas de resiliência.
- Clássico: Uma conexão clássica cria uma conexão sem a necessidade do AWS Direct Connect Resiliency Toolkit. É ideal para os usuários que já possuem conexões e desejam incluir conexões adicionais sem usar o kit de ferramentas. Esse modelo tem um SLA de 95%, mas não fornece resiliência ou redundância. Para obter mais informações, consulte Conexão clássica.

Tópicos

- Direct Connect Conexão clássica

Pré-requisitos de conexão

Direct Connect suporta as seguintes velocidades de porta em fibra monomodo: transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, transceptor 10GBASE-LR (1310 nm) para 10 gigabit, 100GBASE para Ethernet de 100 gigabit ou 400GBASE para Ethernet de 400 Gbps. LR4 LR4

Você pode configurar uma Direct Connect conexão usando o AWS Direct Connect Resiliency Toolkit ou uma conexão clássica de uma das seguintes formas:

Modelo	Largura de banda	Método
Conexão dedicada	1 Gbps, 10 Gbps, 100 Gbps e 400 Gbps	Trabalhe com um Direct Connect parceiro ou um provedor de rede para conectar um roteador do seu data center, escritório ou ambiente de colocation a um Direct Connect local. O provedor de rede não precisa ser um AWS Direct Connect parceiro para conectar você a uma conexão dedicada. Direct Connect conexões dedicadas suportam essas velocidades de porta em fibra monomodo: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm), 100 Gbps: 100GBASE- ou 400GBASE- para Ethernet de 400 Gbps. LR4 LR4
Conexão hospedada	50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps,	Trabalhe com um AWS Direct Connect parceiro no Programa

Modelo	Largura de banda	Método
	400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps e 25 Gbps.	de Parceria para conectar um roteador do seu data center, escritório ou ambiente de colocation a um Direct Connect local. Somente determinados parceiros oferecem conexões de maior capacidade.

Para conexões Direct Connect com larguras de banda de 1 Gbps ou mais, certifique-se de que sua rede atenda aos seguintes requisitos:

- Sua rede deve usar fibra monomodo com um transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, um transceptor 10GBASE-LR (1310 nm) para 10 gigabit, 100GBASE para Ethernet de 100 gigabit ou 400GBASE para Ethernet de 400 Gbps. LR4 LR4
- Dependendo do endpoint do AWS Direct Connect que atende à sua conexão, talvez seja necessário habilitar ou desabilitar a negociação automática de dispositivos locais para qualquer conexão dedicada. Se uma interface virtual permanecer inativa quando uma conexão do Direct Connect estiver ativa, consulte Solucionar problemas da camada 2 (link de dados).
- É necessário ter compatibilidade com o encapsulamento 802.1Q de VLAN em toda a conexão, incluindo em dispositivos intermediários.
- Seu dispositivo deve suportar o Border Gateway Protocol (BGP) e a autenticação MD5 BGP.
- (Opcional) Você também pode configurar a Bidirectional Forwarding Detection (BFD – Detecção de encaminhamento bidirecional) em sua rede. O BFD assíncrono é ativado automaticamente para cada interface virtual. Direct Connect Ela é habilitada automaticamente para interfaces virtuais do Direct Connect, mas não entrará em vigor até você configurá-la em seu roteador. Para obter mais informações, consulte Habilitar a BFD para uma conexão do Direct Connect.

Verifique se você tem as seguintes informações antes de iniciar a configuração:

- O modelo de resiliência que você deseja usar se não estiver criando uma conexão clássica. Para opções de conexão do AWS Direct Connect Resiliency Toolkit, consulte o. AWS Direct Connect Kit de ferramentas de resiliência

- A velocidade, o local e o parceiro de todas as conexões.

  Você só precisa da velocidade para uma conexão.

AWS Direct Connect Kit de ferramentas de resiliência

AWS oferece aos clientes a capacidade de obter conexões de rede altamente resilientes entre a Amazon Virtual Private Cloud (Amazon VPC) e sua infraestrutura local. O AWS Direct Connect Resiliency Toolkit fornece um assistente de conexão com vários modelos de resiliência. Esses modelos ajudam você a determinar e solicitar o número de conexões dedicadas para atingir o objetivo de SLA. Você seleciona um modelo de resiliência e, em seguida, o AWS Direct Connect Resiliency Toolkit o orienta pelo processo de pedido de conexão dedicado. Os modelos de resiliência são projetados para garantir que você tenha o número apropriado de conexões dedicadas em vários locais.

O kit de ferramentas AWS Direct Connect de resiliência tem os seguintes benefícios:

- Fornece orientações sobre como você determina e solicita as conexões dedicadas redundantes apropriadas do Direct Connect .
- Garante que as conexões dedicadas redundantes tenham a mesma velocidade.
- Configura automaticamente os nomes das conexões dedicadas.
- Aprova automaticamente suas conexões dedicadas quando você tem uma AWS conta existente e seleciona um AWS Direct Connect parceiro conhecido. A Letter of Authority (LOA – Carta de autoridade) está disponível para download imediato.
- Cria automaticamente um ticket de suporte para a aprovação da conexão dedicada quando você é um novo AWS cliente ou seleciona um parceiro desconhecido (Outro).
- Fornece um resumo de pedidos para as conexões dedicadas, com o SLA que você pode atingir e o custo por hora de porta para conexões dedicadas solicitadas.
- Cria grupos de agregação de links (LAGs) e adiciona o número apropriado de conexões dedicadas ao LAGs quando você escolhe uma velocidade diferente de 1 Gbps, 10 Gbps, 100 Gbps ou 400 Gbps.
- Fornece um resumo do LAG com o SLA da conexão dedicada que você pode obter e o custo total por hora de porta para conexões dedicadas solicitadas como parte do LAG.
- Impede que você encerre as conexões dedicadas no mesmo dispositivo do Direct Connect .

- Fornece uma maneira de testar a configuração quanto à resiliência. Você trabalha com a AWS para interromper a sessão de emparelhamento de BGP a fim de verificar se o tráfego é roteado para uma das interfaces virtuais redundantes. Para obter mais informações, consulte the section called “Teste de failover do Direct Connect”.
- Fornece CloudWatch métricas da Amazon para conexões e interfaces virtuais. Para obter mais informações, consulte Monitoramento de recursos do Direct Connect.

Depois de selecionar o modelo de resiliência, o AWS Direct Connect Resiliency Toolkit orienta você pelos seguintes procedimentos:

- Selecionar o número de conexões dedicadas
- Selecionar a capacidade de conexão e o local da conexão dedicada
- Solicitar as conexões dedicadas
- Verificar se as conexões dedicadas estão prontas para uso
- Fazer download da Letter of Authority (LOA-CFA – Carta de autoridade) para cada conexão dedicada
- Verificar se a configuração atende aos requisitos de resiliência

Modelos de resiliência disponíveis

Os seguintes modelos de resiliência estão disponíveis no AWS Direct Connect Resiliency Toolkit:

- Resiliência máxima: esse modelo fornece uma maneira de solicitar conexões dedicadas para atingir um SLA de 99,99%. Ele exige que você atenda a todos os requisitos para obter o SLA especificado no Acordo de nível de serviço do Direct Connect.
- Alta resiliência: esse modelo fornece uma maneira de solicitar conexões dedicadas para atingir um SLA de 99,9%. Ele exige que você atenda a todos os requisitos para obter o SLA especificado no Acordo de nível de serviço do Direct Connect.
- Desenvolvimento e teste: este modelo permite que você obtenha resiliência de desenvolvimento e teste para workloads não críticas usando conexões separadas que são encerradas em dispositivos separados em um único local.

A melhor prática é usar o assistente de conexão no AWS Direct Connect Resiliency Toolkit para atingir seu objetivo de SLA.

> **Note**
>
> Se você não quiser criar um modelo de resiliência usando o AWS Direct Connect Resiliency Toolkit, você pode criar uma conexão clássica. Para mais informações sobre conexões clássicas, consulte Conexão clássica.

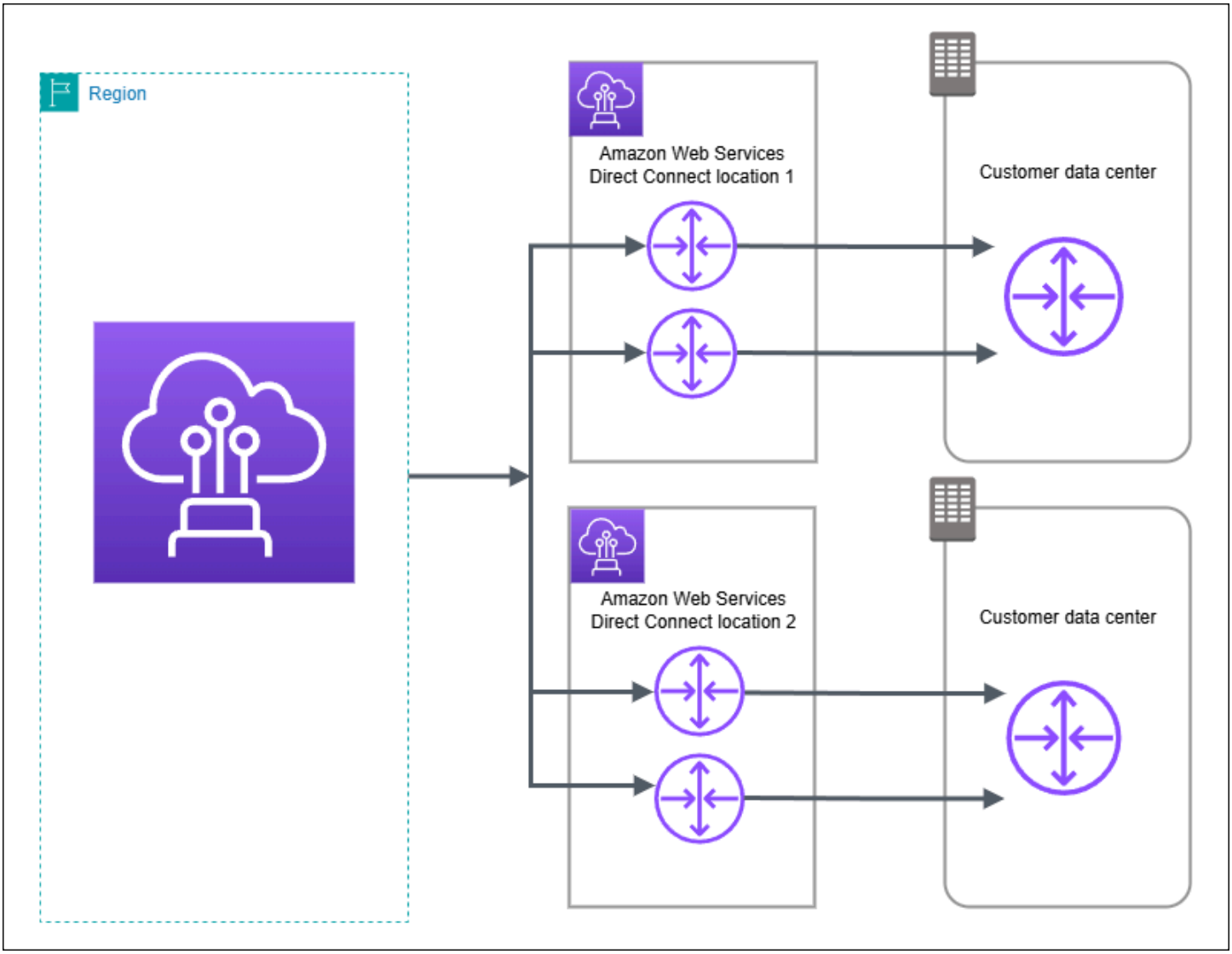
AWS Direct Connect Pré-requisitos do kit de ferramentas de resiliência

Observe as seguintes informações antes de iniciar sua configuração:

- Familiarize-se com Pré-requisitos de conexão.
- O modelo de resiliência disponível que você deseja usar.

Resiliência máxima

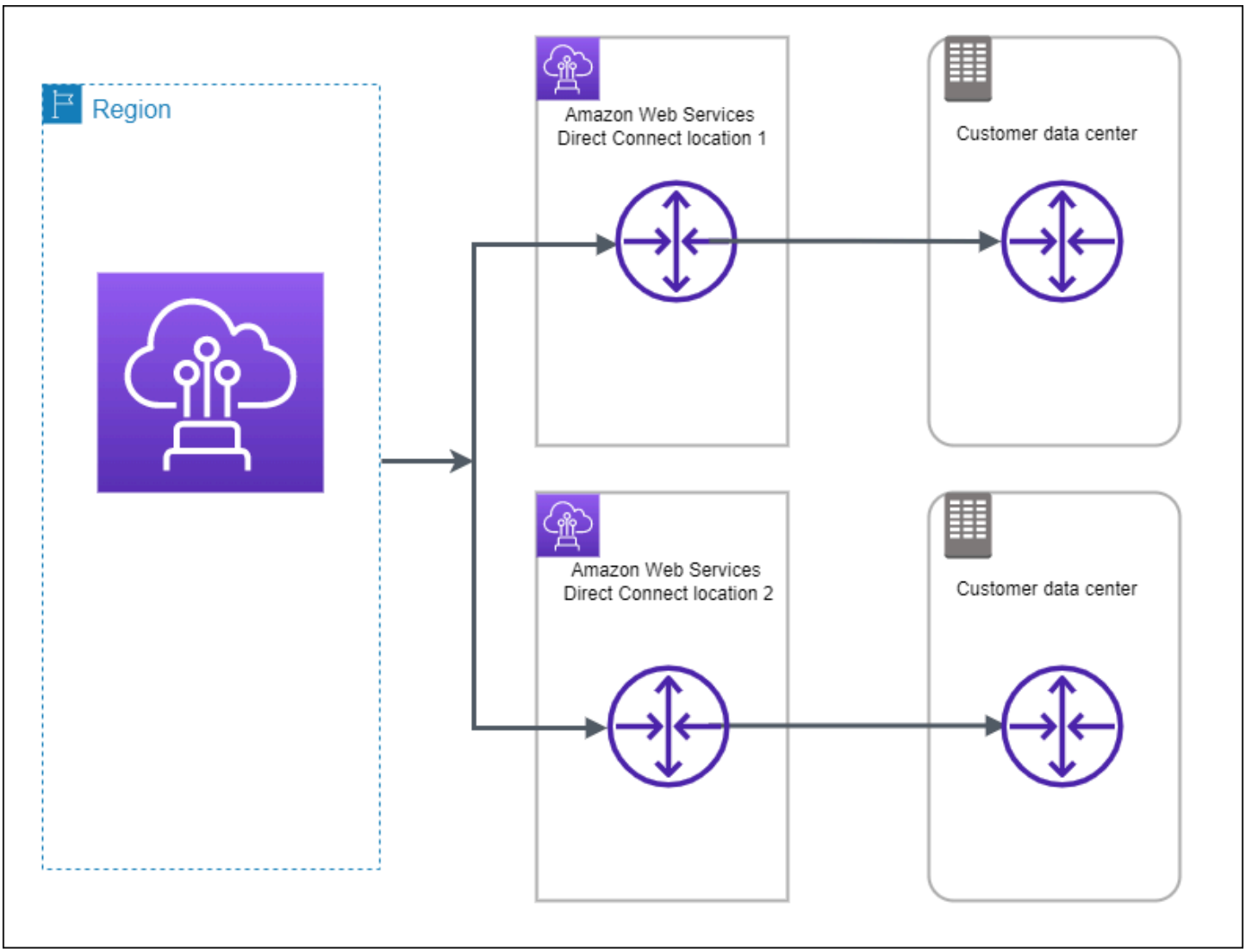
Você pode alcançar a máxima resiliência para cargas de trabalho críticas usando conexões separadas que são encerradas em dispositivos separados em mais de um local (conforme mostrado na figura). Esse modelo fornece resiliência contra falhas de dispositivo, conectividade e localização completa. A figura a seguir mostra as duas conexões de cada data center do cliente indo para os mesmos Direct Connect locais. Opcionalmente, você pode fazer com que cada conexão de um data center do cliente siga para locais diferentes.



Para obter o procedimento de uso do AWS Direct Connect Resiliency Toolkit para configurar um modelo de resiliência máxima, consulte. Configuração da resiliência máxima

Alta resiliência

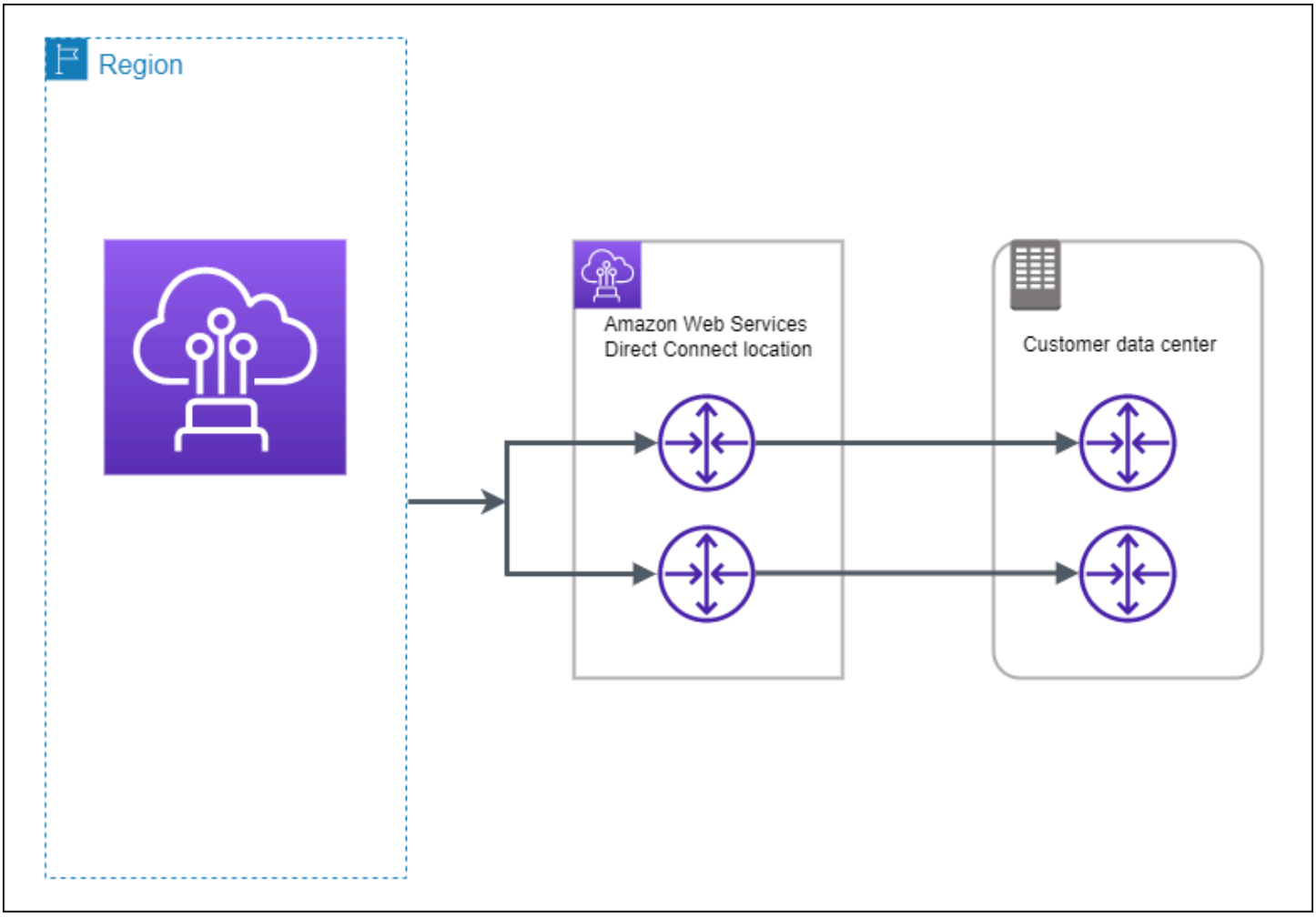
Você pode obter alta resiliência para cargas de trabalho críticas usando duas conexões únicas para vários locais (conforme mostrado na figura). Esse modelo fornece resiliência contra falhas de conectividade causadas por um corte de fibra ou uma falha de dispositivo. Ele também ajuda a evitar uma falha completa no local.



Para o procedimento de uso do AWS Direct Connect Resiliency Toolkit para configurar um modelo de alta resiliência, consulte. Configuração da alta resiliência

Desenvolvimento e testes

Você pode obter resiliência de desenvolvimento e teste para cargas de trabalho não críticas usando conexões separadas que são encerradas em dispositivos separados em um único local (conforme mostrado na figura). Esse modelo fornece resiliência contra falhas de dispositivo, mas não fornece resiliência contra falhas de localização.



Para obter o procedimento de uso do AWS Direct Connect Resiliency Toolkit para configurar um modelo de resiliência máxima, consulte. Configuração da resiliência em desenvolvimentos e testes

AWS Direct Connect FailoverTest

Use o AWS Direct Connect Resiliency Toolkit para verificar as rotas de tráfego e se essas rotas atendem aos seus requisitos de resiliência.

Para obter os procedimentos de uso do AWS Direct Connect Resiliency Toolkit para realizar testes de failover, consulte. Teste de failover do Direct Connect

Configure o Direct Connect para obter máxima resiliência com o AWS Direct Connect Resiliency Toolkit

Neste exemplo, o Direct Connect Resiliency Toolkit é usado para configurar um modelo de resiliência máxima

Tarefas

- Etapa 1: inscrever-se em AWS
- Etapa 2: Configurar o modelo de resiliência
- Etapa 3: Criar interfaces virtuais
- Etapa 4: Verificar a configuração de resiliência da interface virtual
- Etapa 5: Verificar a conectividade das interfaces virtuais

Etapa 1: inscrever-se em AWS

Para usar Direct Connect, você precisa de uma AWS conta, caso ainda não tenha uma.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Etapa 2: Configurar o modelo de resiliência

Configurar um modelo de resiliência máxima

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Conexões e Criar uma conexão.
3. Em Connection ordering type (Tipo de solicitação de conexão), escolha Connection wizard (Assistente de conexão).
4. Em Resiliency level (Nível de resiliência), escolha Maximum Resiliency (Resiliência máxima) e selecione Next (Avançar).
5. No painel Configure connections (Definir conexões), em Connection settings (Configurações de conexão), faça o seguinte:

   a. Em Bandwidth (Largura de banda), selecione a largura de banda da conexão dedicada.

      Essa largura de banda se aplica a todas as conexões criadas.

   b. Em First location service provider, selecione o Direct Connect local apropriado para a conexão dedicada.

   c. Se aplicável, para First Sub Location (Primeiro sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

   d. Se você tiver selecionado Other (Outro) para First location service provider (Provedor de serviço do primeiro local), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

   e. Em Segundo provedor de serviços de localização, selecione o Direct Connect local apropriado.

f. Se aplicável, para Second Sub Location (Segundo sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

g. Se você tiver selecionado Other (Outro) para Second location service provider (Provedor de serviço do segundo local), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

h. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

6. Escolha Próximo.

7. Revise suas conexões e escolha Continue (Continuar).

   Se LOAs estiver pronto, você pode escolher Baixar LOA e clicar em Continuar.

   Pode levar até 72 horas úteis AWS para analisar sua solicitação e provisionar uma porta para sua conexão. Durante esse período, você pode receber um e-mail com uma solicitação para obter mais informações sobre o caso de uso ou o local especificado. O e-mail é enviado para o endereço de e-mail que você usou quando se inscreveu AWS. Você deve responder em até 7 dias, ou a conexão será excluída.

Etapa 3: Criar interfaces virtuais

Crie uma interface virtual privada para se conectar à VPC. Ou você pode criar uma interface virtual pública para se conectar a AWS serviços públicos que não estão em uma VPC. Ao criar uma interface virtual privada para uma VPC, você precisa de uma interface virtual privada para cada VPC à qual se conecta. Por exemplo, você precisa de três interfaces virtuais privadas para se conectar a três VPCs.

Antes de começar, verifique se você tem as seguintes informações:

Recurso	Informações necessárias
Conexão	A Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se você estiver criando a interface virtual para outra conta, precisará do AWS ID da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma AWS região, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário , a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect.
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect . Se você tiver uma conexão hospedada, seu AWS Direct Connect parceiro fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.
Endereços IP de par	Uma interface virtual pode suportar uma sessão de emparelhamento BGP para IPv4, IPv6, ou uma de cada (pilha dupla). Não use Elastic IPs (EIPs) nem Traga seus próprios endereços IP (BYOIP) do Amazon Pool para criar uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalo s de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP.

Recurso	Informações necessárias

	• IPv4:
	  • (Somente interface virtual pública) Você deve especificar IPv4 endereços públicos exclusivos de sua propriedade. O valor pode ser um dos seguintes:
	  • Um CIDR de propriedade do cliente IPv4
	
	Elas podem ser públicas IPs (de propriedade do cliente ou fornecida s por ele AWS), mas a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/31` intervalo, como`203.0.113.0/31` , você poderia usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível AWS . Ou, se você alocar um `/24` intervalo, como`198.51.100.0/24` , você poderia usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível AWS .
	  • Um intervalo de IP de propriedade do seu AWS Direct Connect parceiro ou ISP, junto com uma autorização LOA-CFA
	  • Um AWS CIDR /31 fornecido. Entre em contato com o AWS Support para solicitar um IPv4 CIDR público (e fornecer um caso de uso em sua solicitação)
	
	Note
	Não podemos garantir que seremos capazes de atender a todas as solicitações AWS de IPv4 endereços públicos fornecidos.
	  • (Somente interface virtual privada) A Amazon pode gerar IPv4 endereços privados para você. Se você especificar o seu, certifique-se de especific ar privado CIDRs para a interface do roteador e somente para a interface do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Semelhante a uma interface virtual pública, a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/30` intervalo, como`192.168.0.0/30` ,

Recurso	Informações necessárias
	você poderia usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível AWS . • IPv6: A Amazon aloca automaticamente um CIDR IPv6 /125. Você não pode especificar seus próprios IPv6 endereços de pares.
Família de endereços	Se a sessão de emparelhamento do BGP terminará ou. IPv4 IPv6
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar na faixa de 1 a 4294967294. A adição de prefixo do Sistema autônomo (AS) não funcionar á se você usar um ASN privado para uma interface virtual pública. • AWS ativa MD5 por padrão. Não é possível modificar essa opção. • Uma chave MD5 de autenticação BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	IPv4 Rotas públicas ou IPv6 rotas para anunciar no BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: O IPv4 CIDR pode se sobrepor a outro IPv4 CIDR público anunciado usando Direct Connect quando uma das seguintes afirmações for verdadeir a:
	  • Eles CIDRs são de diferentes AWS regiões. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usa AS_PATH quando tem um ASN público em uma configuração. active/passive
	  Para obter mais informações consulte Políticas de roteamento e comunidad es do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para. IPv6
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	A unidade máxima de transmissão (MTU) dos pacotes acima. Direct Connect O padrão é 1500. Definir o MTU de uma interface virtual para 9001 (frames jumbo) pode resultar em uma atualização para a conexão física subjacente se ele não foi atualizado para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Os quadros jumbo se aplicam somente às rotas propagadas de. Direct Connect Se você adicionar rotas estáticas a uma tabela de rotas que aponte para seu gateway privado virtual, o tráfego roteado pelas rotas estáticas será enviado usando 1.500 MTU. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Se seus prefixos públicos ASNs pertencerem a um ISP ou operadora de rede, solicitamos informações adicionais de você. Pode ser um documento usando um papel timbrado oficial da empresa ou um e-mail do nome de domínio da empresa verificando se a rede prefix/ASN pode ser usada por você.

Quando você cria uma interface virtual pública, pode levar até 72 horas úteis AWS para analisar e aprovar sua solicitação.

Para provisionar uma interface virtual pública para serviços que não sejam VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public virtual interface settings (Configurações de interface virtual pública), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   d. Em BGP ASN (ASN do BGP), informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) de seu gateway.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para fornecer sua própria chave BGP, insira sua chave MD5 BGP.

   Se você não inserir um valor, geraremos uma chave BGP.

c. Para anunciar prefixos na Amazon, para prefixos que você deseja anunciar, insira os endereços de destino IPv4 CIDR (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.

d. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Para provisionar uma interface virtual privada para uma VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, para Tipo, escolha Pública.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Para o Tipo de gateway, escolha Gateway privado virtual ou Gateway do Direct Connect.

   d. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, insira a AWS conta.

   e. Em Gateway privado virtual, selecione o gateway privado virtual que deseja usar nessa interface.

f. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

g. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

      > **Important**
      >
      > Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
      >
      > - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade máxima de transmissão (MTU) de 1500 (padrão) para 9001 (frames jumbo), selecione MTU jumbo (tamanho de MTU 9001).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Etapa 4: Verificar a configuração de resiliência da interface virtual

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, execute um teste de failover de interface virtual para verificar se sua configuração atende aos requisitos de resiliência. Para obter mais informações, consulte the section called “Teste de failover do Direct Connect”.

Etapa 5: Verificar a conectividade das interfaces virtuais

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, você pode verificar sua AWS Direct Connect conexão usando os procedimentos a seguir.

Para verificar sua conexão de interface virtual com a AWS nuvem

- Execute `traceroute` e verifique se o Direct Connect identificador está no rastreamento da rede.

Para verificar a conexão da interface virtual com a Amazon VPC

1. Usando uma AMI compatível com ping, como uma AMI do Amazon Linux, inicie uma instância do EC2 na VPC anexada ao seu gateway privado virtual. O Amazon Linux AMIs está disponível

na guia Quick Start quando você usa o assistente de execução de instâncias no console do Amazon EC2. Para obter mais informações, consulte Executar uma instância no Guia do usuário do Amazon EC2. Certifique-se de que o grupo de segurança associado à instância inclua uma regra que permita tráfego ICMP de entrada (para a solicitação de ping).

2. Depois que a instância estiver em execução, obtenha o endereço IPv4 privado (por exemplo, 10.0.0.4). O console do Amazon EC2 exibe o endereço como parte dos detalhes da instância.
3. Faça ping no IPv4 endereço privado e obtenha uma resposta.

Configure o Direct Connect para alta resiliência com o Resiliency AWS Direct Connect Toolkit

Neste exemplo, o Direct Connect Resiliency Toolkit é usado para configurar um modelo de alta resiliência

Tarefas

- Etapa 1: inscrever-se em AWS
- Etapa 2: Configurar o modelo de resiliência
- Etapa 3: Criar interfaces virtuais
- Etapa 4: Verificar a configuração de resiliência da interface virtual
- Etapa 5: Verificar a conectividade das interfaces virtuais

Etapa 1: inscrever-se em AWS

Para usar Direct Connect, você precisa de uma AWS conta, caso ainda não tenha uma.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Etapa 2: Configurar o modelo de resiliência

Configurar um modelo de alta resiliência

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Conexões e Criar uma conexão.
3. Em Connection ordering type (Tipo de solicitação de conexão), escolha Connection wizard (Assistente de conexão).
4. Em Resiliency level (Nível de resiliência), escolha High Resiliency (Alta resiliência) e selecione Next (Avançar).
5. No painel Configure connections (Definir conexões), em Connection settings (Configurações de conexão), faça o seguinte:

   a. Para bandwidth (largura de banda), escolha a largura de banda da conexão.

      Essa largura de banda se aplica a todas as conexões criadas.

   b. Em First location service provider, selecione o Direct Connect local apropriado.

c. Se aplicável, para First Sub Location (Primeiro sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

d. Se você tiver selecionado Other (Outro) para First location service provider (Provedor de serviço do primeiro local), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

e. Em Segundo provedor de serviços de localização, selecione o Direct Connect local apropriado.

f. Se aplicável, para Second Sub Location (Segundo sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

g. Se você tiver selecionado Other (Outro) para Second location service provider (Provedor de serviço do segundo local), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

h. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

6. Escolha Próximo.
7. Revise suas conexões e escolha Continue (Continuar).

   Se LOAs estiver pronto, você pode escolher Baixar LOA e clicar em Continuar.

   Pode levar até 72 horas úteis AWS para analisar sua solicitação e provisionar uma porta para sua conexão. Durante esse período, você pode receber um e-mail com uma solicitação para obter mais informações sobre o caso de uso ou o local especificado. O e-mail é enviado para o endereço de e-mail que você usou quando se inscreveu AWS. Você deve responder em até 7 dias, ou a conexão será excluída.

Etapa 3: Criar interfaces virtuais

Crie uma interface virtual privada para se conectar à VPC. Ou você pode criar uma interface virtual pública para se conectar a AWS serviços públicos que não estão em uma VPC. Ao criar uma

interface virtual privada para uma VPC, você precisa de uma interface virtual privada para cada VPC à qual se conecta. Por exemplo, você precisa de três interfaces virtuais privadas para se conectar a três VPCs.

Antes de começar, verifique se você tem as seguintes informações:

Recurso	Informações necessárias
Conexão	A Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se você estiver criando a interface virtual para outra conta, precisará do AWS ID da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma AWS região, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário , a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect.
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect . Se você tiver uma conexão hospedada, seu AWS Direct Connect parceiro fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.
Endereços IP de par	Uma interface virtual pode suportar uma sessão de emparelhamento BGP para IPv4, IPv6, ou uma de cada (pilha dupla). Não use Elastic IPs (EIPs) nem Traga seus próprios endereços IP (BYOIP) do Amazon Pool para criar

Recurso	Informações necessárias
	uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalos de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP. • IPv4: • (Somente interface virtual pública) Você deve especificar IPv4 endereços públicos exclusivos de sua propriedade. O valor pode ser um dos seguintes: • Um CIDR de propriedade do cliente IPv4 Elas podem ser públicas IPs (de propriedade do cliente ou fornecidas por ele AWS), mas a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/31` intervalo, como`203.0.113.0/31` , você poderia usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível AWS . Ou, se você alocar um `/24` intervalo, como`198.51.100.0/24` , você poderia usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível AWS . • Um intervalo de IP de propriedade do seu AWS Direct Connect parceiro ou ISP, junto com uma autorização LOA-CFA • Um AWS CIDR /31 fornecido. Entre em contato com o AWS Support para solicitar um IPv4 CIDR público (e fornecer um caso de uso em sua solicitação) **Note** Não podemos garantir que seremos capazes de atender a todas as solicitações AWS de IPv4 endereços públicos fornecidos. • (Somente interface virtual privada) A Amazon pode gerar IPv4 endereços privados para você. Se você especificar o seu, certifique-se de especificar privado CIDRs para a interface do roteador e somente para a interface

Recurso	Informações necessárias
	do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Semelhante a uma interface virtual pública, a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/30` intervalo, como`192.168.0.0/30` , você poderia usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível AWS . • IPv6: A Amazon aloca automaticamente um CIDR IPv6 /125. Você não pode especificar seus próprios IPv6 endereços de pares.
Família de endereços	Se a sessão de emparelhamento do BGP terminará ou. IPv4 IPv6
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar na faixa de 1 a 4294967294. A adição de prefixo do Sistema autônomo (AS) não funcionar á se você usar um ASN privado para uma interface virtual pública. • AWS ativa MD5 por padrão. Não é possível modificar essa opção. • Uma chave MD5 de autenticação BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	IPv4 Rotas públicas ou IPv6 rotas para anunciar no BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: O IPv4 CIDR pode se sobrepor a outro IPv4 CIDR público anunciado usando Direct Connect quando uma das seguintes afirmações for verdadeir a:
	  • Eles CIDRs são de diferentes AWS regiões. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usa AS_PATH quando tem um ASN público em uma configuração. active/passive
	  Para obter mais informações consulte Políticas de roteamento e comunidad es do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para. IPv6
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	A unidade máxima de transmissão (MTU) dos pacotes acima. Direct Connect O padrão é 1500. Definir o MTU de uma interface virtual para 9001 (frames jumbo) pode resultar em uma atualização para a conexão física subjacente se ele não foi atualizado para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Os quadros jumbo se aplicam somente às rotas propagadas de. Direct Connect Se você adicionar rotas estáticas a uma tabela de rotas que aponte para seu gateway privado virtual, o tráfego roteado pelas rotas estáticas será enviado usando 1.500 MTU. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Se seus prefixos públicos ASNs pertencerem a um ISP ou operadora de rede, AWS solicita informações adicionais de você. Pode ser um documento usando um papel timbrado oficial da empresa ou um e-mail do nome de domínio da empresa verificando se a rede prefix/ASN pode ser usada por você.

Quando você cria uma interface virtual pública, pode levar até 72 horas úteis AWS para analisar e aprovar sua solicitação.

Para provisionar uma interface virtual pública para serviços que não sejam VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public virtual interface settings (Configurações de interface virtual pública), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   d. Em BGP ASN (ASN do BGP), informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) de seu gateway.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para fornecer sua própria chave BGP, insira sua chave MD5 BGP.

   Se você não inserir um valor, geraremos uma chave BGP.

c. Para anunciar prefixos na Amazon, para prefixos que você deseja anunciar, insira os endereços de destino IPv4 CIDR (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.

d. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Para provisionar uma interface virtual privada para uma VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, para Tipo, escolha Pública.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Para o Tipo de gateway, escolha Gateway privado virtual ou Gateway do Direct Connect.

   d. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, insira a AWS conta.

   e. Em Gateway privado virtual, selecione o gateway privado virtual que deseja usar nessa interface.

f. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

g. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

      > **Important**
      >
      > Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
      >
      > - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade máxima de transmissão (MTU) de 1500 (padrão) para 9001 (frames jumbo), selecione MTU jumbo (tamanho de MTU 9001).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Etapa 4: Verificar a configuração de resiliência da interface virtual

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, execute um teste de failover de interface virtual para verificar se sua configuração atende aos requisitos de resiliência. Para obter mais informações, consulte the section called “Teste de failover do Direct Connect”.

Etapa 5: Verificar a conectividade das interfaces virtuais

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, você pode verificar sua AWS Direct Connect conexão usando os procedimentos a seguir.

Para verificar sua conexão de interface virtual com a AWS nuvem

- Execute `traceroute` e verifique se o Direct Connect identificador está no rastreamento da rede.

Para verificar a conexão da interface virtual com a Amazon VPC

1. Usando uma AMI compatível com ping, como uma AMI do Amazon Linux, inicie uma instância do EC2 na VPC anexada ao seu gateway privado virtual. O Amazon Linux AMIs está disponível

na guia Quick Start quando você usa o assistente de execução de instâncias no console do Amazon EC2. Para obter mais informações, consulte Executar uma instância no Guia do usuário do Amazon EC2. Certifique-se de que o grupo de segurança associado à instância inclua uma regra que permita tráfego ICMP de entrada (para a solicitação de ping).

2. Depois que a instância estiver em execução, obtenha o endereço IPv4 privado (por exemplo, 10.0.0.4). O console do Amazon EC2 exibe o endereço como parte dos detalhes da instância.
3. Faça ping no IPv4 endereço privado e obtenha uma resposta.

Configure AWS Direct Connect para desenvolver e testar a resiliência com o Resiliency AWS Direct Connect Toolkit

Neste exemplo, o Direct Connect Resiliency Toolkit é usado para configurar um modelo de resiliência de desenvolvimento e teste.

Tarefas

- Etapa 1: inscrever-se em AWS
- Etapa 2: Configurar o modelo de resiliência
- Etapa 3: Criar uma interface virtual
- Etapa 4: Verificar a configuração de resiliência da interface virtual
- Etapa 5: Verificar a interface virtual

Etapa 1: inscrever-se em AWS

Para usar Direct Connect, você precisa de uma AWS conta, caso ainda não tenha uma.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Etapa 2: Configurar o modelo de resiliência

Configurar o modelo de resiliência

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Conexões e Criar uma conexão.
3. Em Connection ordering type (Tipo de solicitação de conexão), escolha Connection wizard (Assistente de conexão).
4. Em Resiliency level (Nível de resiliência), escolha Development and test (Desenvolvimento e teste) e selecione Next (Avançar).
5. No painel Configure connections (Definir conexões), em Connection settings (Configurações de conexão), faça o seguinte:

   a. Para bandwidth (largura de banda), escolha a largura de banda da conexão.

      Essa largura de banda se aplica a todas as conexões criadas.

   b. Em First location service provider, selecione o Direct Connect local apropriado.

c. Se aplicável, para First Sub Location (Primeiro sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

d. Se você tiver selecionado Other (Outro) para First location service provider (Provedor de serviço do primeiro local), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

e. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

6. Escolha Próximo.
7. Revise suas conexões e escolha Continue (Continuar).

Se LOAs estiver pronto, você pode escolher Baixar LOA e clicar em Continuar.

Pode levar até 72 horas úteis AWS para analisar sua solicitação e provisionar uma porta para sua conexão. Durante esse período, você pode receber um e-mail com uma solicitação para obter mais informações sobre o caso de uso ou o local especificado. O e-mail é enviado para o endereço de e-mail que você usou quando se inscreveu AWS. Você deve responder em até 7 dias, ou a conexão será excluída.

Etapa 3: Criar uma interface virtual

Para começar a usar sua Direct Connect conexão, você deve criar uma interface virtual. Crie uma interface virtual privada para se conectar à VPC. Ou você pode criar uma interface virtual pública para se conectar a AWS serviços públicos que não estão em uma VPC. Ao criar uma interface virtual privada para uma VPC, você precisa de uma interface virtual privada para cada VPC à qual se conecta. Por exemplo, você precisa de três interfaces virtuais privadas para se conectar a três VPCs.

Antes de começar, verifique se você tem as seguintes informações:

Recurso	Informações necessárias
Conexão	A Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se você estiver criando a interface virtual para outra conta, precisará do AWS ID da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma AWS região, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário , a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect.
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect . Se você tiver uma conexão hospedada, seu AWS Direct Connect parceiro fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.
Endereços IP de par	Uma interface virtual pode suportar uma sessão de emparelhamento BGP para IPv4, IPv6, ou uma de cada (pilha dupla). Não use Elastic IPs (EIPs) nem Traga seus próprios endereços IP (BYOIP) do Amazon Pool para criar uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalo s de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP.

Recurso	Informações necessárias
	• IPv4: • (Somente interface virtual pública) Você deve especificar IPv4 endereços públicos exclusivos de sua propriedade. O valor pode ser um dos seguintes: • Um CIDR de propriedade do cliente IPv4 Elas podem ser públicas IPs (de propriedade do cliente ou fornecida s por ele AWS), mas a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/31` intervalo, como`203.0.113.0/31` , você poderia usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível AWS . Ou, se você alocar um `/24` intervalo, como`198.51.100.0/24` , você poderia usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível AWS . • Um intervalo de IP de propriedade do seu AWS Direct Connect parceiro ou ISP, junto com uma autorização LOA-CFA • Um AWS CIDR /31 fornecido. Entre em contato com o AWS Support para solicitar um IPv4 CIDR público (e fornecer um caso de uso em sua solicitação) **Note** Não podemos garantir que seremos capazes de atender a todas as solicitações AWS de IPv4 endereços públicos fornecidos. • (Somente interface virtual privada) A Amazon pode gerar IPv4 endereços privados para você. Se você especificar o seu, certifique-se de especific ar privado CIDRs para a interface do roteador e somente para a interface do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Semelhante a uma interface virtual pública, a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/30` intervalo, como`192.168.0.0/30` ,

Recurso	Informações necessárias
	você poderia usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível AWS . • IPv6: A Amazon aloca automaticamente um CIDR IPv6 /125. Você não pode especificar seus próprios IPv6 endereços de pares.
Família de endereços	Se a sessão de emparelhamento do BGP terminará ou. IPv4 IPv6
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar na faixa de 1 a 4294967294. A adição de prefixo do Sistema autônomo (AS) não funcionar á se você usar um ASN privado para uma interface virtual pública. • AWS ativa MD5 por padrão. Não é possível modificar essa opção. • Uma chave MD5 de autenticação BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	IPv4 Rotas públicas ou IPv6 rotas para anunciar no BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: O IPv4 CIDR pode se sobrepor a outro IPv4 CIDR público anunciado usando Direct Connect quando uma das seguintes afirmações for verdadeir a:
	  • Eles CIDRs são de diferentes AWS regiões. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usa AS_PATH quando tem um ASN público em uma configuração. active/passive
	  Para obter mais informações consulte Políticas de roteamento e comunidad es do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para. IPv6
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	A unidade máxima de transmissão (MTU) dos pacotes acima. Direct Connect O padrão é 1500. Definir o MTU de uma interface virtual para 9001 (frames jumbo) pode resultar em uma atualização para a conexão física subjacente se ele não foi atualizado para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Os quadros jumbo se aplicam somente às rotas propagadas de. Direct Connect Se você adicionar rotas estáticas a uma tabela de rotas que aponte para seu gateway privado virtual, o tráfego roteado pelas rotas estáticas será enviado usando 1.500 MTU. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Se seus prefixos públicos ASNs pertencerem a um ISP ou operadora de rede, solicitamos informações adicionais de você. Pode ser um documento usando um papel timbrado oficial da empresa ou um e-mail do nome de domínio da empresa verificando se a rede prefix/ASN pode ser usada por você.

Quando você cria uma interface virtual pública, pode demorar até 72 horas úteis para que a AWS revise e aprove sua solicitação.

Para provisionar uma interface virtual pública para serviços que não sejam VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public virtual interface settings (Configurações de interface virtual pública), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   d. Em BGP ASN (ASN do BGP), informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) de seu gateway.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para fornecer sua própria chave BGP, insira sua chave MD5 BGP.

   Se você não inserir um valor, geraremos uma chave BGP.

c. Para anunciar prefixos na Amazon, para prefixos que você deseja anunciar, insira os endereços de destino IPv4 CIDR (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.

d. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Para provisionar uma interface virtual privada para uma VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, para Tipo, escolha Pública.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Para o Tipo de gateway, escolha Gateway privado virtual ou Gateway do Direct Connect.

   d. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, insira a AWS conta.

   e. Em Gateway privado virtual, selecione o gateway privado virtual que deseja usar nessa interface.

f. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

g. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

      > **Important**
      >
      > Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
      >
      > - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade máxima de transmissão (MTU) de 1500 (padrão) para 9001 (frames jumbo), selecione MTU jumbo (tamanho de MTU 9001).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Etapa 4: Verificar a configuração de resiliência da interface virtual

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, execute um teste de failover de interface virtual para verificar se sua configuração atende aos requisitos de resiliência. Para obter mais informações, consulte the section called “Teste de failover do Direct Connect”.

Etapa 5: Verificar a interface virtual

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, você pode verificar sua AWS Direct Connect conexão usando os procedimentos a seguir.

Para verificar sua conexão de interface virtual com a AWS nuvem

- Execute `traceroute` e verifique se o Direct Connect identificador está no rastreamento da rede.

Para verificar a conexão da interface virtual com a Amazon VPC

1. Usando uma AMI compatível com ping, como uma AMI do Amazon Linux, inicie uma instância do EC2 na VPC anexada ao seu gateway privado virtual. O Amazon Linux AMIs está disponível

na guia Quick Start quando você usa o assistente de execução de instâncias no console do Amazon EC2. Para obter mais informações, consulte Executar uma instância no Guia do usuário do Amazon EC2. Certifique-se de que o grupo de segurança associado à instância inclua uma regra que permita tráfego ICMP de entrada (para a solicitação de ping).

2. Depois que a instância estiver em execução, obtenha o endereço IPv4 privado (por exemplo, 10.0.0.4). O console do Amazon EC2 exibe o endereço como parte dos detalhes da instância.
3. Faça ping no IPv4 endereço privado e obtenha uma resposta.

Teste de failover do Direct Connect

Os modelos de resiliência do kit de ferramentas de resiliência do AWS Direct Connect são projetados para garantir que você tenha o número adequado de conexões de interface virtual em vários locais. Após concluir o assistente, use o teste de failover do kit de ferramentas de resiliência do AWS Direct Connect para interromper a sessão de emparelhamento do BGP a fim de verificar se o tráfego é roteado para uma das interfaces virtuais redundantes e atende aos seus requisitos de resiliência.

Use o teste para verificar se o tráfego roteia por interfaces virtuais redundantes quando uma interface virtual não está funcionando. Você inicia o teste selecionando uma interface virtual, uma sessão de emparelhamento de BGP e o tempo de execução do teste. A AWS coloca a sessão de emparelhamento de BGP da interface virtual selecionada no estado inativo. Quando a interface está nesse estado, o tráfego deve passar por uma interface virtual redundante. Se a configuração não contiver as conexões redundantes apropriadas, a sessão de emparelhamento de BGP falhará e o tráfego não será roteado. Quando o teste for concluído ou você interrompê-lo manualmente, a AWS restaurará a sessão de BGP. Após a conclusão do teste, você poderá usar o kit de ferramentas de resiliência do AWS Direct Connect para ajustar a configuração.

> **Note**
>
> Não faça uso deste recurso durante um período de manutenção do Direct Connect, pois a sessão do BGP pode ser restaurada antes do tempo, durante ou após a manutenção.

Histórico do teste

A AWS exclui o histórico de testes após 365 dias. O histórico de testes inclui o status dos testes que foram executados em todos os peers de BGP. O histórico inclui quais sessões de emparelhamento

do BPG foram testadas, os horários de início e término, além do status do teste, que pode ser qualquer um dos seguintes valores:

- Em andamento: o teste está sendo executado no momento.
- Concluído: o teste foi executado pelo tempo especificado.
- Cancelado: o teste foi cancelado antes do horário especificado.
- Falhou: o teste não foi executado durante o tempo especificado. Isso pode acontecer quando há um problema com o roteador.

Para obter mais informações, consulte the section called “Visualização de um histórico de testes de failover da interface virtual”.

Permissões de validação

A única conta que tem permissão para executar o teste de failover é a conta que é proprietária da interface virtual. O proprietário da conta recebe uma indicação por meio do AWS CloudTrail de que um teste foi executado em uma interface virtual.

Tópicos

Inicie um teste de AWS Direct Connect failover da interface virtual do Resiliency Toolkit

Você pode iniciar o teste de failover da interface virtual usando o Direct Connect console ou o. AWS CLI

Para iniciar o teste de failover da interface virtual a partir do console Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Escolha Interfaces virtuais.
3. Selecione as interfaces virtuais e escolha Ações, Reduzir o BGP.

   É possível executar o teste em uma interface virtual pública, privada ou de trânsito.

4. Na caixa de diálogo Iniciar teste de falha, faça o seguinte:

   a. Para que os Peerings possam ser baixados para testar, escolha quais sessões de peering testar, por exemplo. IPv4
   b. Em Tempo máximo de teste, insira o número de minutos da duração do teste.

      O valor máximo é de 4.320 minutos (72 horas úteis).

      O valor padrão é 180 minutos (3 horas).
   c. Em Para confirmar o teste, digite Confirmar.
   d. Escolha Confirmar.

   A sessão de emparelhamento de BGP é colocada no estado DOWN. É possível enviar tráfego para verificar se não há interrupções. Se necessário, é possível interromper o teste imediatamente.

Para iniciar o teste de failover da interface virtual usando o AWS CLI

Use StartBgpFailoverTest.

Veja o histórico de testes de failover da interface virtual do AWS Direct Connect Resiliency Toolkit

Você pode visualizar o histórico de testes de failover da interface virtual usando o Direct Connect console ou o. AWS CLI

Para visualizar o histórico de testes de failover da interface virtual a partir do console Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Escolha Interfaces virtuais.
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).
4. Escolha Histórico de testes.

   O console exibe os testes executados para a interface virtual.
5. Para visualizar os detalhes de um teste específico, selecione o ID de teste.

Para visualizar o histórico de testes de failover da interface virtual usando o AWS CLI

Use ListVirtualInterfaceTestHistory.

Interrompa um teste de failover da interface virtual do AWS Direct Connect Resiliency Toolkit

Você pode interromper o teste de failover da interface virtual usando o Direct Connect console ou o. AWS CLI

Para interromper o teste de failover da interface virtual a partir do console Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Escolha Interfaces virtuais.
3. Selecione a interface virtual e escolha Ações, Cancelar teste.
4. Escolha Confirmar.

AWS restaura a sessão de emparelhamento do BGP. O histórico de testes exibe “cancelado” para o teste.

Para interromper o teste de failover da interface virtual usando o AWS CLI

Use StopBgpFailoverTest.

Direct Connect Conexão clássica

Uma conexão clássica oferece uma abordagem direta para estabelecer conectividade de rede dedicada entre sua infraestrutura on-premises e a AWS. Esse tipo de conexão é ideal para organizações que preferem gerenciar suas próprias configurações de rede e ter a infraestrutura atual do Direct Connect instalada. A conexão clássica não depende do AWS Direct Connect Resiliency Toolkit.

Selecione Clássica quando você tiver conexões e quiser adicionar outras. Uma conexão clássica tem um SLA de 95%. No entanto, ele não fornece resiliência ou redundância, que são encontradas somente no AWS Direct Connect Resiliency Toolkit ao criar uma conexão.

> **Note**
>
> Antes de configurar uma conexão Clássica, familiarize-se com o Pré-requisitos de conexão.

Tarefas

- Configurar uma conexão Direct Connect clássica

Configurar uma conexão Direct Connect clássica

Configure uma conexão Classic quando você tiver conexões existentes do Direct Connect.

Etapa 1: inscrever-se em AWS

Para usar Direct Connect, você precisa de uma conta, caso ainda não tenha uma.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Etapa 2: solicitar uma conexão Direct Connect dedicada

Para conexões dedicadas, você pode enviar uma solicitação de conexão usando o Direct Connect console. Para conexões hospedadas, trabalhe com um AWS Direct Connect parceiro para solicitar uma conexão hospedada. Verifique se você tem as seguintes informações:

- A velocidade da porta que você precisa. Você não poderá alterar a velocidade da porta após a criação da solicitação de conexão.
- O Direct Connect local em que a conexão deve ser encerrada.

> **Note**
>
> Você não pode usar o Direct Connect console para solicitar uma conexão hospedada. Em vez disso, entre em contato com um AWS Direct Connect parceiro, que pode criar uma conexão hospedada para você, que você aceita. Ignore o procedimento a seguir e vá até Aceitar a conexão hospedada.

Para criar uma nova Direct Connect conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Conexões e Criar uma conexão.
3. Escolha Classic (Clássica).
4. No painel Create Connection (Criar conexão), em Connection settings (Configurações de conexão), faça o seguinte:

   a. Em Name (Nome), insira um nome para a conexão.

   b. Em Location (Local), selecione o local do Direct Connect apropriado.

c. Se aplicável, para Sub Location (Sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.

d. Em Port Speed (Velocidade da porta), selecione a largura de banda da conexão.

e. Em Local, selecione Conectar por meio de um Direct Connect parceiro ao usar essa conexão para se conectar ao seu data center.

f. Em Provedor de serviços, selecione o AWS Direct Connect Parceiro. Caso use um parceiro que não esteja na lista, selecione Other (Outro).

g. Se você tiver selecionado Other (Outro) em Service provider (Provedor de serviços), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.

h. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

5. Escolha Criar conexão.

Pode levar até 72 horas úteis AWS para analisar sua solicitação e provisionar uma porta para sua conexão. Durante esse período, você pode receber um e-mail com uma solicitação para obter mais informações sobre o caso de uso ou o local especificado. O e-mail é enviado para o endereço de e-mail que você usou quando se inscreveu AWS. Você deve responder em até 7 dias, ou a conexão será excluída.

Para obter mais informações, consulte Direct Connect conexões dedicadas e hospedadas.

Aceitar a conexão hospedada

Você deve aceitar a conexão hospedada no Direct Connect console antes de criar uma interface virtual. Essa etapa se aplica somente a conexões hospedadas.

Para aceitar uma interface virtual hospedada

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione a conexão hospedada e escolha Aceitar.

Escolha Accept (Aceitar).

(Conexão dedicada) Etapa 3: Fazer download da LOA-CFA

Depois que você solicitar uma conexão, disponibilizaremos uma Letter of Authorization and Connecting Facility Assignment (LOA-CFA – Carta de autorização e atribuição da instalação de conexão) para download ou enviaremos por e-mail uma solicitação para obter mais informações. O LOA-CFA é a autorização para AWS se conectar e é exigido pelo provedor de colocation ou pelo seu provedor de rede para estabelecer a conexão entre redes (conexão cruzada).

Para baixar a LOA-CFA

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione a conexão e escolha View Details (Visualizar detalhes).
4. Escolha Download LOA-CFA (Fazer download da LOA-CFA).

   A LOA-CFA é baixada no computador como um arquivo PDF.

   > **Note**
   >
   > Caso o link não esteja habilitado, a LOA-CFA ainda não está disponível para download. Consulte o e-mail para uma solicitação de mais informações. Caso ela ainda esteja indisponível, ou você não tenha recebido um e-mail após 72 horas úteis, entre em contato com o AWS Support.

5. Após fazer download da LOA-CFA, siga um destes procedimentos:

   - Se você estiver trabalhando com um AWS Direct Connect parceiro ou provedor de rede, envie a eles o LOA-CFA para que eles possam solicitar uma conexão cruzada para você no local. Direct Connect Caso ele não consiga solicitar a conexão cruzada, você pode entrar em contato com o provedor de colocação diretamente.
   - Se você tiver equipamento no Direct Connect local, entre em contato com o provedor de colocation para solicitar uma conexão entre redes. É necessário ser um cliente do provedor de colocação. Você também deve apresentar a eles a LOA-CFA que autoriza a conexão com o AWS roteador e as informações necessárias para se conectar à sua rede.

Direct Connect locais listados como vários locais (por exemplo, Equinix DC1 - DC6 & DC1 0-DC11) são configurados como um campus. Se o equipamento do provedor de rede ou o seu estiver em um desses locais, solicite uma conexão cruzada com a porta atribuída, mesmo que resida em um prédio diferente no campus.

> **Important**
>
> Um campus é tratado como um único Direct Connect local. Para obter alta disponibilidade, configure conexões a locais diferentes do Direct Connect .

Se você ou seu provedor de rede tiver problemas para estabelecer uma conexão física, consulte Solucionar problemas da camada 1 (física).

Etapa 4: Criar uma interface virtual

Para começar a usar sua Direct Connect conexão, você deve criar uma interface virtual. Crie uma interface virtual privada para se conectar à VPC. Ou você pode criar uma interface virtual pública para se conectar a AWS serviços públicos que não estão em uma VPC. Ao criar uma interface virtual privada para uma VPC, você precisa de uma interface virtual privada para cada VPC à qual se conecta. Por exemplo, você precisa de três interfaces virtuais privadas para se conectar a três VPCs.

Antes de começar, verifique se você tem as seguintes informações:

Recurso	Informações necessárias
Conexão	A Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se você estiver criando a interface virtual para outra conta, precisará do AWS ID da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma AWS região, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário

Recurso	Informações necessárias
	, a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect.
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect . Se você tiver uma conexão hospedada, seu AWS Direct Connect parceiro fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.

Recurso	Informações necessárias

Endereços IP de par	Uma interface virtual pode suportar uma sessão de emparelhamento BGP para IPv4, IPv6, ou uma de cada (pilha dupla). Não use Elastic IPs (EIPs) nem Traga seus próprios endereços IP (BYOIP) do Amazon Pool para criar uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalos de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP.
	
	• IPv4:
	  • (Somente interface virtual pública) Você deve especificar IPv4 endereços públicos exclusivos de sua propriedade. O valor pode ser um dos seguintes:
	  • Um CIDR de propriedade do cliente IPv4
	
	Elas podem ser públicas IPs (de propriedade do cliente ou fornecidas por ele AWS), mas a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/31` intervalo, como`203.0.113.0/31` , você poderia usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível AWS . Ou, se você alocar um `/24` intervalo, como`198.51.100.0/24` , você poderia usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível AWS .
	  • Um intervalo de IP de propriedade do seu AWS Direct Connect parceiro ou ISP, junto com uma autorização LOA-CFA
	  • Um AWS CIDR /31 fornecido. Entre em contato com o AWS Support para solicitar um IPv4 CIDR público (e fornecer um caso de uso em sua solicitação)
	
	Note
	Não podemos garantir que seremos capazes de atender a todas as solicitações AWS de IPv4 endereços públicos fornecidos.

Recurso	Informações necessárias
	• (Somente interface virtual privada) A Amazon pode gerar IPv4 endereços privados para você. Se você especificar o seu, certifique-se de especific ar privado CIDRs para a interface do roteador e somente para a interface do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Semelhante a uma interface virtual pública, a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/30` intervalo, como`192.168.0.0/30` , você poderia usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível AWS . • IPv6: A Amazon aloca automaticamente um CIDR IPv6 /125. Você não pode especificar seus próprios IPv6 endereços de pares.
Família de endereços	Se a sessão de emparelhamento do BGP terminará ou. IPv4 IPv6
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar na faixa de 1 a 4294967294. A adição de prefixo do Sistema autônomo (AS) não funcionar á se você usar um ASN privado para uma interface virtual pública. • AWS ativa MD5 por padrão. Não é possível modificar essa opção. • Uma chave MD5 de autenticação BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	IPv4 Rotas públicas ou IPv6 rotas para anunciar no BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: O IPv4 CIDR pode se sobrepor a outro IPv4 CIDR público anunciado usando Direct Connect quando uma das seguintes afirmações for verdadeir a:
	  • Eles CIDRs são de diferentes AWS regiões. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usa AS_PATH quando tem um ASN público em uma configuração. active/passive
	  Para obter mais informações consulte Políticas de roteamento e comunidad es do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para. IPv6
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	A unidade máxima de transmissão (MTU) dos pacotes acima. Direct Connect O padrão é 1500. Definir o MTU de uma interface virtual para 9001 (frames jumbo) pode resultar em uma atualização para a conexão física subjacente se ele não foi atualizado para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Os quadros jumbo se aplicam somente às rotas propagadas de. Direct Connect Se você adicionar rotas estáticas a uma tabela de rotas que aponte para seu gateway privado virtual, o tráfego roteado pelas rotas estáticas será enviado usando 1.500 MTU. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Solicitamos informações adicionais de você se seus prefixos públicos ASNs pertencerem a um ISP ou operadora de rede. Pode ser um documento usando um papel timbrado oficial da empresa ou um e-mail do nome de domínio da empresa, verificando se a rede prefix/ASN pode ser usada por você.

Para interface virtual privada e interfaces virtuais públicas, a unidade máxima de transmissão (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permitido que pode ser transmitido pela conexão. A MTU de uma interface virtual privada pode ser 1500 ou 9001 (frames jumbo). A MTU de uma interface virtual privada pode ser 1500 ou 8500 (frames jumbo). Você pode especificar a MTU ao criar a interface ou atualizá-la depois que criá-la. Definir a MTU de uma interface virtual para 8500 (frames jumbo) ou 9001 (frames jumbo) pode resultar em uma atualização da conexão física subjacente se ela não foi atualizada para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre Jumbo Frame Capable na guia Resumo.

Quando você cria uma interface virtual pública, pode levar até 72 horas úteis AWS para analisar e aprovar sua solicitação.

Para provisionar uma interface virtual pública para serviços que não sejam VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public virtual interface settings (Configurações de interface virtual pública), faça o seguinte:
   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.
   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.
   c. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).
   d. Em BGP ASN insira o Número de sistema autônomo do Border Gateway Protocol do roteador on-premises de mesmo nível para a nova interface virtual. Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

   [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

   - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
   - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

   [IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para fornecer sua própria chave BGP, insira sua chave MD5 BGP.

   Se você não inserir um valor, geraremos uma chave BGP.

c. Para anunciar prefixos na Amazon, para prefixos que você deseja anunciar, insira os endereços de destino IPv4 CIDR (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.

d. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Para provisionar uma interface virtual privada para uma VPC

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, para Tipo, escolha Pública.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

c. Para o Tipo de gateway, escolha Gateway privado virtual ou Gateway do Direct Connect.

d. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, insira a AWS conta.

e. Em Gateway privado virtual, selecione o gateway privado virtual que deseja usar nessa interface.

f. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

g. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulte Suporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

      > **Important**
      >
      > Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point

- Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
- Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade máxima de transmissão (MTU) de 1500 (padrão) para 9001 (frames jumbo), selecione MTU jumbo (tamanho de MTU 9001).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).
8. Você precisa usar seu dispositivo BGP para anunciar a rede usada para a conexão VIF pública.

Etapa 5: Fazer download da configuração do roteador

Depois de criar uma interface virtual para sua Direct Connect conexão, você pode baixar o arquivo de configuração do roteador. O arquivo contém os comandos necessários para configurar o roteador para uso com a interface virtual pública ou privada.

Para baixar uma configuração do roteador

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a conexão e escolha View Details (Visualizar detalhes).
4. Selecione Download router configuration (Fazer download da configuração do roteador).

5. Em Download router configuration (Fazer download da configuração do roteador), faça o seguinte:

   a. Em Fornecedor, selecione o fabricante do roteador.

   b. Em Plataforma, selecione o modelo do roteador.

   c. Em Software, selecione a versão do software do roteador.

6. Escolha Download e use a configuração apropriada para o roteador a fim de garantir que você consiga se conectar ao Direct Connect.

Para obter mais informações sobre como configurar manualmente seu roteador, consulte Baixar arquivo de configuração do roteador.

Depois que você configura o roteador, o status da interface virtual vai para UP. Se a interface virtual permanecer inativa e você não conseguir fazer ping no endereço IP do mesmo nível do Direct Connect dispositivo, consulteSolucionar problemas da camada 2 (link de dados). Se você conseguir executar ping no endereço IP par, consulte Solucionar problemas das camadas 3/4 (rede/transporte). Caso a sessão de mesmo nível BGP seja estabelecida, mas você não consiga rotear o tráfego, consulte Solução de problemas de roteamento.

Etapa 6: Verificar a interface virtual

Depois de estabelecer interfaces virtuais para a AWS nuvem ou para a Amazon VPC, você pode verificar sua AWS Direct Connect conexão usando os procedimentos a seguir.

Para verificar sua conexão de interface virtual com a AWS nuvem

- Execute `traceroute` e verifique se o Direct Connect identificador está no rastreamento da rede.

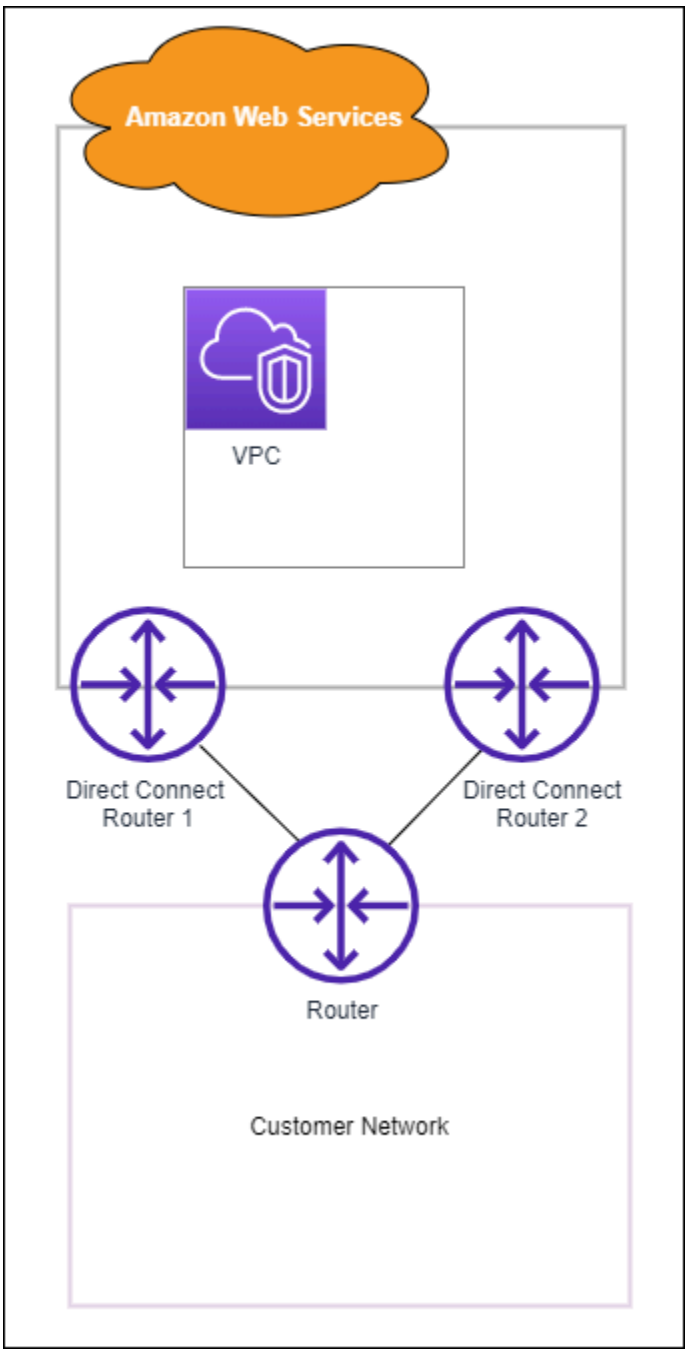
Para verificar a conexão da interface virtual com a Amazon VPC

1. Usando uma AMI pingável, como uma Amazon Linux AMI, execute uma EC2 instância na VPC que está conectada ao seu gateway privado virtual. O Amazon Linux AMIs está disponível na guia Quick Start quando você usa o assistente de execução de instâncias no EC2 console da Amazon. Para obter mais informações, consulte Iniciar uma instância no Guia EC2 do usuário da Amazon. Certifique-se de que o grupo de segurança associado à instância inclua uma regra que permita tráfego ICMP de entrada (para a solicitação de ping).

2. Depois que a instância estiver em execução, obtenha seu IPv4 endereço privado (por exemplo, 10.0.0.4). O EC2 console da Amazon exibe o endereço como parte dos detalhes da instância.
3. Faça ping no IPv4 endereço privado e obtenha uma resposta.

(Recomendado) Etapa 7: Configurar conexões redundantes

Para fornecer o failover, recomendamos que você solicite e configure duas conexões dedicadas para AWS, conforme mostrado na figura a seguir. Essas conexões podem ser encerradas em um ou dois roteadores na rede.



Existem diferentes opções de configuração disponíveis quando você provisiona duas conexões dedicadas:

- Ativa/ativa (multicaminho BGP). Essa é a configuração padrão, na qual as duas conexões estão ativas. Direct Connect suporta vários caminhos para várias interfaces virtuais no mesmo local, e a carga do tráfego é compartilhada entre interfaces com base no fluxo. Caso uma conexão fique indisponível, todo o tráfego é direcionado para outra conexão.

- Ativa/passiva (failover). Uma conexão lida com o tráfego, e a outra permanece em espera. Caso a conexão ativa fique indisponível, todo o tráfego é roteado por meio da conexão passiva. Você precisa acrescentar o caminho AS às rotas em um dos links para que este seja o link passivo.

A maneira como você configura as conexões não afeta a redundância, mas afeta as políticas que determinam como os dados são roteados em ambas as conexões. Recomendamos configurar ambas as conexões como ativas.

Se você usar uma conexão VPN para redundância, implemente uma verificação de integridade e um mecanismo de failover. Se você usar qualquer uma das seguintes configurações, será necessário verificar o roteamento da tabela de rotas para a nova interface de rede.

- Você usa suas próprias instâncias para roteamento, por exemplo, a instância é o firewall.
- Você usa sua própria instância que encerra uma conexão VPN.

Para obter alta disponibilidade, é altamente recomendável que você configure conexões com Direct Connect locais diferentes.

Para obter mais informações sobre Direct Connect resiliência, consulte Recomendações de Direct Connect resiliência.

Direct Connect manutenção

Direct Connect está comprometida em garantir a segurança, a disponibilidade e a escalabilidade do serviço. Para manter esses padrões, é necessário realizar manutenção periódica nos dispositivos de rede de hardware. A manutenção do Direct Connect está dividida em dois tipos: planejada e emergencial.

Esses eventos de manutenção incluem abordar vulnerabilidades de segurança, problemas de hardware, realizar migrações de dispositivos para cumprir os padrões, corrigir defeitos e fornecer novos recursos. Seguindo as práticas descritas em Preparação para os eventos de manutenção, você pode preparar melhor o ambiente do Direct Connect para evitar interrupções durante os eventos de manutenção. Se você tiver uma configuração de rede não resiliente ou uma única conexão, você enfrentará uma interrupção na conectividade entre sua rede local e os recursos. AWS

O Direct Connect envia notificações por e-mail sobre eventos de manutenção planejados e emergenciais para o endereço de e-mail associado à AWS conta proprietária da conexão ou do recurso de interface virtual do Direct Connect. Se você estiver usando uma conexão hospedada pelo Direct Connect com um dos parceiros de entrega do Direct Connect, as notificações por e-mail sobre o evento de manutenção serão enviadas para você e para a conta do parceiro. Você também pode adicionar outros endereços de e-mail ou listas de distribuição para receber notificações. Consulte Atualizar os contatos alternativos da sua AWS conta para obter mais informações.

Evento de manutenção

- Manutenção planejada do Direct Connect
- Manutenção emergencial do Direct Connect
- Manutenção de terceiros
- Preparação para os eventos de manutenção
- Solicitações de adiamento ou cancelamento de eventos de manutenção

Manutenção planejada do Direct Connect

Os eventos de manutenção planejada envolvem atualizações de rede, como patches do sistema operacional e atualizações de configuração nos endpoints de dispositivos de hardware. Essas atualizações são necessárias para melhorar a disponibilidade e fornecer novos recursos.

Esses eventos de manutenção são programados com 14 dias de antecedência e geralmente ocorrem durante um período de quatro horas em horários de baixo tráfego no local do Direct Connect onde o endpoint do dispositivo reside. As atividades de manutenção geralmente são concluídas antes que o período completo de quatro horas expire. Você receberá uma notificação quando o trabalho for concluído. Em casos raros em que circunstâncias imprevistas exijam a extensão do período de manutenção, enviaremos uma notificação separada com a estimativa de conclusão revisada.

Usando a programação a seguir, a notificação inicial e as notificações de lembrete são enviadas para a AWS conta proprietária do recurso:

- 14 dias corridos antes do evento de manutenção planejado;
- 7 dias corridos antes do evento de manutenção planejado; e
- 1 dia antes do evento de manutenção planejado.

> **Note**
>
> Os dias corridos incluem dias não úteis e feriados locais.

Além disso,

- Receba notificações em seu sistema de monitoramento ou emissão de tíquetes por meio da integração com o AWS Health. Para integrar AWS Health, consulte Monitoramento de eventos AWS Health com a Amazon EventBridge no Guia AWS Health do usuário.
- Veja os cronogramas de manutenção planejada em seu Health Dashboard.

Em raras circunstâncias, um evento de manutenção planejado talvez não ocorra conforme programado. Se isso acontecer, enviaremos uma notificação de cancelamento e remarcaremos o evento para uma data futura, seguindo o mesmo processo descrito acima.

Manutenção emergencial do Direct Connect

Os eventos de manutenção emergencial são iniciados de acordo com a situação crítica para evitar eventos iminentes de impacto no serviço ou para resolver deficiências que já tenham resultado em interrupção na conectividade. Nesses casos, é necessário tomar medidas imediatas para restaurar o endpoint afetado a um estado íntegro.

Embora nos esforcemos para fornecer um aviso prévio sempre que possível, algumas situações podem exigir que a manutenção seja iniciada imediatamente. Você receberá notificações quando a manutenção emergencial estiver programada ou em andamento e novamente quando for concluída.

Esses eventos de manutenção ocorrem normalmente durante um período de duas horas no local do Direct Connect onde o endpoint do dispositivo reside. As atividades de manutenção geralmente são concluídas nesse período. Em casos raros em que circunstâncias imprevistas exijam a extensão do período de manutenção, como troca de hardware, enviaremos uma notificação separada com a estimativa de conclusão revisada.

Manutenção de terceiros

Além dos eventos de manutenção AWS iniciados, seu parceiro de entrega do Direct Connect ou provedor de serviços de rede que está fornecendo conectividade de rede do seu local para o local do Direct Connect pode realizar atividades de manutenção. Os parceiros do Direct Connect Delivery recebem notificações de eventos de manutenção AWS para que possam planejar seus próprios cronogramas de manutenção para evitar sobreposições. AWS não tem visibilidade das atividades de manutenção de um parceiro, então você precisará verificar com ele o processo de agendamento, os métodos de notificação e as melhores práticas.

Preparação para os eventos de manutenção

Para garantir que as cargas de trabalho de produção continuem funcionando durante um evento de manutenção, o Direct Connect recomenda que você use o AWS Direct Connect Resiliency Toolkit para configurar suas conexões de rede para obter a máxima resiliência. Para obter um exemplo de modelo de resiliência máxima, consulte Resiliência máxima.

Usando a máxima resiliência, as conexões são distribuídas em pelo menos dois locais do Direct Connect, com terminação em dois endpoints de dispositivos exclusivos em cada local do Direct Connect. Isso fornece várias camadas de redundância, o que reduz o risco de uma única falha no endpoint e ajuda a manter a conectividade durante os eventos de manutenção. O Direct Connect nunca agendará um evento de manutenção planejado que desative simultaneamente suas conexões redundantes. Para obter as etapas de uso do AWS Direct Connect Resiliency Toolkit para configurar a resiliência máxima, consulte. Configuração da resiliência máxima

Durante um evento de manutenção planejado, o Direct Connect drena o tráfego de e para o endpoint de conexão em manutenção e força o tráfego a usar suas conexões redundantes. Isso permite um redirecionamento mais contínuo do tráfego de rede sem a necessidade de intervenção manual se

a resiliência máxima não estiver configurada. Como alternativa, você pode optar por controlar o redirecionamento de tráfego entre as conexões redundantes durante as janelas de manutenção usando comunidades de Protocolo de Gateway da Borda (BGP) de preferência do local. Para obter mais informações sobre as comunidades do BGP, consulte Políticas de roteamento e comunidades BGP.

Configurar seu ambiente do Direct Connect com o modelo de resiliência máxima ajuda a garantir que sua empresa não seja afetada durante eventos de manutenção e falhas na infraestrutura. Quando implementados e testados adequadamente, você normalmente não precisa realizar nenhuma ação relacionada a esses eventos de manutenção.

Validação de resiliência

Se você configurou seu ambiente do Direct Connect para ser resiliente, valide regularmente se seu tráfego é roteado por outras conexões redundantes quando houver uma conexão. out-of-service Testes proativos regulares podem ajudar a identificar e resolver possíveis problemas antes que eles afetem as workloads de produção durante um evento real de manutenção ou um cenário de falha. Isso garante maior confiabilidade da sua rede durante um evento de manutenção. Use o teste de failover do Direct Connect para validar a resiliência de suas conexões redundantes. Para obter as etapas para usar o teste de failover do Direct Connect , consulte Teste de failover do Direct Connect.

Você também pode utilizar o Amazon CloudWatch Network Monitor para fornecer monitoramento ativo de suas conexões do Direct Connect. Para obter mais informações, consulte Monitore a conectividade híbrida com o Amazon CloudWatch Network Synthetic Monitor.

Solicitações de adiamento ou cancelamento de eventos de manutenção

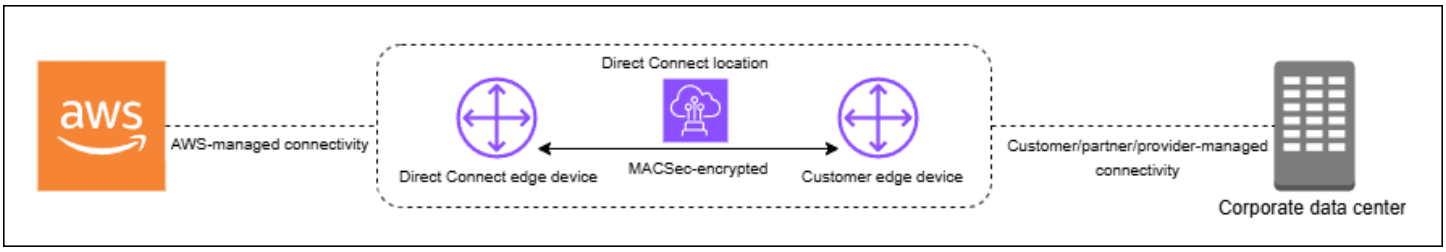
Os dispositivos do Direct Connect são compartilhados entre vários clientes. Portanto, não atendemos solicitações específicas de reagendamentos ou cancelamentos de manutenção. As solicitações de reagendamento ou cancelamento de um cliente podem impactar negativamente outros clientes que estiverem usando esse endpoint. Isso também pode representar um risco para mitigar problemas de disponibilidade ou segurança em tempo hábil.

Segurança MAC em Direct Connect

O MAC Security (MACsec) é um padrão IEEE que fornece confidencialidade, integridade e autenticidade da origem dos dados. MACsec fornece point-to-point criptografia de camada 2 por meio da conexão cruzada AWS, operando entre dois roteadores de camada 3. Enquanto MACsec protege a conexão entre seu roteador e o local do Direct Connect na camada 2, AWS fornece segurança adicional ao criptografar todos os dados na camada física à medida que eles fluem pela rede entre Direct Connect locais e AWS regiões. Isso cria uma abordagem de segurança em camadas em que seu tráfego é protegido durante a entrada inicial AWS e durante o trânsito pela AWS rede.

No diagrama a seguir, a Direct Connect conexão cruzada deve estar conectada a uma interface MACsec compatível no dispositivo de ponta do cliente. MACsec over Direct Connect fornece criptografia de camada 2 para o point-to-point tráfego entre o dispositivo de borda do Direct Connect e o dispositivo de borda do cliente. Essa criptografia ocorre depois que as chaves de segurança são permutadas e verificadas entre as interfaces nas duas extremidades da conexão cruzada.

> **Note**
>
> MACsec fornece point-to-point segurança em links Ethernet; portanto, não fornece end-to-end criptografia em vários segmentos sequenciais de Ethernet ou outros segmentos de rede.



MACsec conceitos

A seguir estão os conceitos-chave para MACsec:

- MAC Security (MACsec) — Um padrão IEEE 802.1 de camada 2 que fornece confidencialidade, integridade e autenticidade da origem dos dados. Para obter mais informações sobre o protocolo, consulte 802.1AE: Segurança MAC () MACsec.

- Chave de associação segura (SAK) — Uma chave de sessão que estabelece a MACsec conectividade entre o roteador local do cliente e a porta de conexão no local do Direct Connect. O SAK não é pré-compartilhado, mas derivado automaticamente do CKN/CAK par por meio de um processo de geração de chave criptográfica. Essa derivação acontece nas duas extremidades da conexão depois que você fornece e provisiona o CKN/CAK par. O SAK é regenerado periodicamente para fins de segurança e sempre que uma MACsec sessão é estabelecida.
- Nome da chave de associação de conectividade (CKN) e chave de associação de conectividade (CAK) — Os valores desse par são usados para gerar a MACsec chave. Você gera os valores do par, os associa a uma Direct Connect conexão e, em seguida, os provisiona em seu dispositivo de borda no final da Direct Connect conexão. O Direct Connect aceita somente o modo CAK estático, mas não o modo CAK dinâmico. Como somente o modo CAK estático é aceito, é recomendável que você siga suas próprias políticas de gerenciamento de chaves para geração, distribuição e rotação de chaves.
- Formato da chave: o formato da chave deve usar caracteres hexadecimais e conter, exatamente, 64 caracteres. O Direct Connect aceita somente chaves de 256 bits do Advanced Encryption Standard (AES) para conexões dedicadas, o que corresponde a uma sequência hexadecimal de 64 caracteres.
- Modos de criptografia — o Direct Connect suporta dois modos de MACsec criptografia:
  - must_encrypt — Nesse modo, a conexão exige MACsec criptografia para todo o tráfego. Se MACsec a negociação falhar ou a criptografia não puder ser estabelecida, a conexão não transmitirá nenhum tráfego. Esse modo oferece a maior garantia de segurança, mas pode afetar a disponibilidade se houver algum problema MACsec relacionado.
  - should_encrypt — Nesse modo, a conexão tenta estabelecer a MACsec criptografia, mas retornará à comunicação não criptografada se a negociação falhar. MACsec Esse modo oferece mais flexibilidade e maior disponibilidade, mas também pode permitir tráfego não criptografado em alguns cenários de falha.

  O modo de criptografia pode ser definido durante a configuração da conexão e também pode ser modificado posteriormente. Por padrão, novas conexões MACsec habilitadas são definidas no modo “should_encrypt” para evitar possíveis problemas de conectividade durante a configuração inicial.

MACsec rotação de chaves

- Rotação CNN/CAK (manual)

O Direct Connect MACsec suporta MACsec chaveiros com capacidade para armazenar até três CKN/CAK pares. Isso permite que você faça manualmente a rotação dessas chaves de longo prazo sem interromper a conexão. Ao associar um novo CKN/CAK par usando o `associate-mac-sec-key` comando, você deve configurar o mesmo par no seu dispositivo. O dispositivo Direct Connect tenta usar a chave adicionada mais recentemente. Se essa chave não corresponder à chave do seu dispositivo, ela retorna para a chave operacional anterior, garantindo a estabilidade da conexão durante a rotação.

Para obter informações sobre o uso`associate-mac-sec-key`, consulte associate-mac-sec-key.

- Rotação (automática) da Chave de associação segura (SAK)

  O SAK, que é derivado do CKN/CAK par ativo, passa por rotação automática com base no seguinte:

  - intervalos de tempo;
  - volume de tráfego criptografado;
  - MACsec estabelecimento da sessão

  Essa rotação é feita automaticamente pelo protocolo, ocorre de forma transparente sem interromper a conexão e não requer intervenção manual. A SAK nunca é armazenada de forma persistente, sendo regenerada por meio de um processo seguro de derivação de chave que segue o padrão IEEE 802.1X.

Conexões compatíveis

MACsec está disponível em conexões Direct Connect dedicadas e grupos de agregação de links:

MACsec Conexões suportadas

- Conexões dedicadas do
- LAGs
- Interconexões de parceiros

> **Note**
>
> Os parceiros que usam dispositivos compatíveis podem usar MACsec para criptografar a conexão de camada 2 entre seu dispositivo de rede de borda e o dispositivo Direct Connect.

Os parceiros que ativam o recurso podem criptografar todo o tráfego que atravessa o link protegido. MACsec a criptografia opera entre os dois dispositivos específicos na camada 2 e não é suportada em conexões hospedadas.

Para obter informações sobre como solicitar conexões compatíveis MACsec, consulte AWS Direct Connect.

Conexões dedicadas do

O seguinte ajuda você a se familiarizar com MACsec as conexões Direct Connect dedicadas. Não há cobranças adicionais pelo uso MACsec. As etapas para configurar MACsec em uma conexão dedicada podem ser encontradas emComece com MACsec uma conexão dedicada.

As operações de interconexão de parceiros seguem os mesmos procedimentos das conexões dedicadas. Quando você executa comandos CLI ou SDK para interconexões de parceiros, as respostas incluirão informações MACsec relacionadas, quando aplicável.

MACsec pré-requisitos para conexões dedicadas

Observe os seguintes requisitos para MACsec conexões dedicadas:

- MACsec é suportado em conexões Direct Connect dedicadas de 10 Gbps, 100 Gbps e 400 Gbps em pontos de presença selecionados. Para essas conexões, os seguintes conjuntos de MACsec cifras são suportados:
  - Para conexões de 10 Gbps: GCM-AES-256 e GCM-AES-XPN-256.
  - Para conexões de 100 Gbps e 400 Gbps, GCM-AES-XPN -256.
- Somente MACsec chaves de 256 bits são suportadas.
- A numeração de pacotes estendida (XPN, na sigla em inglês) é necessária para conexões de 100 Gbps e de 400 Gbps. Para conexões de 10 Gbps, o Direct Connect suporta GCM-AES-256 e -256. GCM-AES-XPN Conexões de alta velocidade, como conexões dedicadas de 100 Gbps e 400 Gbps, podem esgotar MACsec rapidamente o espaço original de numeração de pacotes de 32 bits, o que exigiria que você girasse suas chaves de criptografia a cada poucos minutos para estabelecer uma nova Associação de Conectividade. Para evitar essa situação, a emenda IEEE Std 802.1 AEbw -2013 introduziu a numeração estendida de pacotes, aumentando o espaço de numeração para 64 bits, facilitando o requisito de pontualidade para rotação de chaves.

- O Identificador de Canal Seguro (SCI, na sigla em inglês) é obrigatório e deve estar ativado. Esta configuração não pode ser ajustada.
- O IEEE 802.1Q (Dot1: q/VLAN) tag offset/dot 1) não q-in-clear é suportado para mover uma tag de VLAN para fora de uma carga criptografada.

Além disso, você deve concluir as tarefas a seguir antes de configurar MACsec em uma conexão dedicada.

- Crie um CKN/CAK par para a MACsec chave.

  Você pode criar o par usando uma ferramenta aberta padrão. O par deve atender aos requisitos especificados em the section called “Configurar um roteador on-premises”.
- Verifique se você tem um dispositivo na sua extremidade da conexão que ofereça suporteMACsec.
- O Identificador de Canal Seguro (SCI) deve estar ativado.
- Somente MACsec chaves de 256 bits são suportadas, fornecendo a proteção de dados avançada mais recente.

LAGs

Os requisitos a seguir ajudam você a se familiarizar com os grupos MACsec de agregação de links do Direct Connect (LAGs):

- LAGs deve ser composto por conexões MACsec dedicadas capazes de suportar criptografia MACsec
- Todas as conexões dentro de um LAG devem ter a mesma largura de banda e suporte MACsec
- MACsec a configuração se aplica uniformemente em todas as conexões no LAG
- Habilitando a criação de LAG e MACsec pode ser feito simultaneamente
- Somente uma única MACsec chave pode ser utilizada em todos os links do LAG a qualquer momento. A capacidade de oferecer suporte a várias MACsec chaves é apenas para fins de rotação de chaves.

Interconexões de parceiros

A conta do parceiro que possui a interconexão pode ser usada MACsec nessa conexão física ou LAG. As operações são as mesmas das conexões dedicadas, mas são realizadas usando as chamadas específicas do parceiro API/SDK .

Perfis vinculados a serviço

Direct Connect usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. Direct Connect As funções vinculadas ao serviço são predefinidas Direct Connect e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome. Uma função vinculada ao serviço facilita a configuração Direct Connect porque você não precisa adicionar manualmente as permissões necessárias. Direct Connect define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só Direct Connect pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM. Para obter mais informações, consulte the section called “Perfis vinculados a serviço”.

MACsec CKN/CAK principais considerações pré-compartilhadas

AWS Direct Connect usos AWS gerenciados CMKs para as chaves pré-compartilhadas que você associa às conexões ou LAGs. O Secrets Manager armazena seus pares CKN e CAK pré-compartilhados como um segredo que a chave raiz do Secrets Manager criptografa. Para obter mais informações, consulte AWS gerenciado CMKs no Guia do AWS Key Management Service desenvolvedor.

Por padrão, a chave armazenada é somente para leitura, mas você pode agendar uma exclusão de sete a trinta dias usando o console ou a API do Secrets Manager AWS . Quando você agenda uma exclusão, o CKN não pode ser lido e isso poderá afetar sua conectividade de rede. Quando isso acontece, aplicamos as seguintes regras:

- Se a conexão estiver em um estado pendente, desassociaremos o CKN da conexão.
- Se a conexão estiver em um estado disponível, notificaremos o proprietário da conexão por e-mail. Se você não adotar nenhuma medida em até 30 dias, desassociaremos o CKN da sua conexão.

Quando desassociarmos o último CKN da sua conexão e o modo de criptografia da conexão estiver definido como “deve criptografar”, definiremos o modo como “should_encrypt” para evitar a perda repentina de pacotes.

Comece a usar MACsec em uma Direct Connect conexão dedicada

A tarefa a seguir ajuda você a começar a configurar MACsec para usar em uma conexão dedicada do Direct Connect.

Etapa 1: Criar uma conexão

Para começar a usar MACsec, você deve ativar o recurso ao criar uma conexão dedicada.

(Opcional) Etapa 2: criar um grupo de agregação de link (LAG)

Se você usar várias conexões para redundância, poderá criar um LAG compatível. MACsec Para obter mais informações, consulte Considerações sobre MACsec e Criação de um LAG.

Etapa 3: associar o à CKN/CAK conexão ou ao LAG

Depois de criar a conexão ou o LAG compatível MACsec, você precisa associar a à conexão. CKN/CAK Para obter mais informações, consulte um dos seguintes:

- Associar um MACsec CKN/CAK a uma conexão
- Associar um CKN/CAK de MACsec a um LAG

Etapa 4: configurar um roteador on-premises

Atualize seu roteador local com a chave MACsec secreta. A chave MACsec secreta no roteador local e no Direct Connect local deve corresponder. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Etapa 5: (opcional) remover a associação entre a CKN/CAK e a conexão ou o LAG

Opcionalmente, você pode remover a associação entre o CKN/CAK e a conexão ou LAG. Se precisar remover a associação, consulte uma das seguintes opções:

- Remover a associação entre uma chave MACsec secreta e uma conexão
- Remover a associação entre uma chave MACsec secreta e um LAG

Direct Connect conexões dedicadas e hospedadas

Direct Connect permite que você estabeleça uma conexão de rede dedicada entre sua rede e um dos Direct Connect locais.

Há dois tipos de conexões:

- Conexão dedicada: uma conexão Ethernet física associada a um único cliente. Os clientes podem solicitar uma conexão dedicada por meio do Direct Connect console, da CLI ou da API. Para obter mais informações, consulte Conexões dedicadas do .
- Conexão hospedada: uma conexão Ethernet física que um AWS Direct Connect parceiro provisiona em nome de um cliente. Os clientes solicitam uma conexão hospedada entrando em contato com um parceiro no Programa de parceiros do AWS Direct Connect , que provisiona a conexão. Para obter mais informações, consulte Conexões hospedadas do .

Tópicos

Direct Connect Conexões dedicadas

Para criar uma conexão dedicada do Direct Connect , são necessárias as seguintes informações:

Direct Connect location

Trabalhe com um AWS Direct Connect parceiro no Programa de Parceria para ajudá-lo a estabelecer circuitos de rede entre um Direct Connect local e seu data center, escritório ou ambiente de colocation. Eles também podem ajudar a oferecer espaço de colocação dentro da mesma instalação do local. Para obter mais informações, consulte Parceiros da APN que oferecem suporte ao Direct Connect.

Port speed (Velocidade da porta)

Os valores possíveis são 1 Gbps, 10 Gbps, 100 Gbps e 400 Gbps.

Não será possível alterar a velocidade da porta após a criação da solicitação de conexão. Para alterar a velocidade da porta, é necessário criar e configurar uma nova conexão.

Você poderá criar uma conexão usando o assistente de conexão ou criar uma conexão clássica. Usando o assistente de conexão, é possível configurar conexões usando recomendações de resiliência. Recomenda-se o uso do assistente se você estiver configurando conexões pela primeira vez. Se preferir, você pode usar o Classic para criar conexões one-at-a-time. Recomenda-se usar a conexão clássica se você já tiver uma configuração existente à qual deseja adicionar conexões. Você pode criar uma conexão independente ou criar uma conexão a ser associada a um LAG na conta. Se você associar uma conexão a um LAG, ela será criada com a mesma velocidade de porta e o mesmo local especificados no LAG.

Após solicitar a conexão, disponibilizamos para você uma carta de autorização e atribuição de instalação de conexão (LoA-CFA) para download ou enviamos um e-mail solicitando mais informações. Caso receba uma solicitação para obter mais informações, você deve responder em até 7 dias, ou a conexão é excluída. O LOA-CFA é a autorização para se conectar AWS e é exigido pelo seu provedor de rede para solicitar uma conexão cruzada para você. Se você não tiver equipamento no Direct Connect local, não poderá solicitar uma conexão cruzada para você lá.

As operações a seguir estão disponíveis para conexões dedicadas:

- Criar uma conexão usando o Assistente de conexão
- Criar uma conexão clássica
- the section called “Visualização de detalhes da conexão do ”
- the section called “Atualizar uma conexão”
- Associar um MACsec CKN/CAK a uma conexão
- the section called “Remover a associação entre uma chave MACsec secreta e uma conexão”
- the section called “Excluir uma conexão”

Você pode adicionar uma conexão dedicada a um grupo de agregação de links (LAG) permitindo tratar várias conexões como uma só. Para mais informações, consulte Associar uma conexão a um LAG.

Após criar uma conexão, crie uma interface virtual para se conectar a recursos públicos e privados da AWS . Para obter mais informações, consulte Interfaces virtuais e interfaces virtuais hospedadas.

Se você não tiver equipamento em um Direct Connect local, primeiro entre em contato com um AWS Direct Connect AWS Direct Connect parceiro no Programa de parceiros. Para obter mais informações, consulte Parceiros da APN que oferecem suporte ao Direct Connect.

Se você quiser criar uma conexão que use o MAC Security (MACsec), revise os pré-requisitos antes de criar a conexão. Para obter mais informações, consulte the section called “MACsec pré-requisitos para conexões dedicadas”.

Carta de autorização e atribuição de instalação de conexão (LoA-CFA)

Assim que tivermos processado sua solicitação de conexão, você poderá fazer download da LOA-CFA. Caso o link não esteja habilitado, a LOA-CFA ainda não está disponível para download. Verifique o seu e-mail para uma solicitação de informações.

A LoA baixada é assinada digitalmente e contém uma marca d’água para validar a autenticidade da LoA emitida pela AWS. A assinatura digital e a marca d'água na LoA. O documento PDF impede que uma LoA modificada ou potencialmente fraudulenta seja utilizada pelo provedor de instalações nos locais do Direct Connect. A assinatura digital pode ser autenticada ao abrir o PDF e ao analisar o painel de assinatura. Um documento válido mostrará as mensagens “A assinatura é válida” e “O documento não foi modificado desde que a assinatura foi aplicada”. A marca d’água reproduz o painel de conexões e os fios designados ao longo do documento da LoA, servindo como um indicador visual, mas não seguro, de autenticidade.

O faturamento começará automaticamente quando a porta estiver ativa ou 90 dias após a emissão da LOA, o que ocorrer primeiro. Você pode evitar cobranças de faturamento excluindo a porta antes da ativação ou até 90 dias após a emissão da LOA.

Se sua conexão não estiver ativa após 90 dias e a LOA-CFA não tiver sido emitida, enviaremos um e-mail alertando que a porta será excluída em 10 dias. Se você não conseguir ativar a porta durante o período adicional de 10 dias, a porta será automaticamente excluída e você precisará reiniciar o processo de criação da porta.

Para obter as etapas para download da LoA-CFA, consulte Download da LoA-CFA do .

> **Note**
>
> Para saber mais sobre precificação, consulte Precificação do Direct Connect. Caso não queira mais a conexão após reemitir a LOA-CFA, exclua a conexão por conta própria. Para obter mais informações, consulte Excluir uma Direct Connect conexão.

Tópicos

Crie uma conexão Direct Connect dedicada usando o assistente de conexão

Esta seção descreve a criação de uma conexão usando o Assistente de conexão. Se você preferir criar uma conexão clássica, veja as etapas em the section called “Etapa 2: solicitar uma conexão Direct Connect dedicada”.

Para criar uma conexão usando o Assistente de conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Conexões e Criar conexão.
3. Na página Criar conexão, em Tipo de pedido de conexão, escolha Assistente de conexão.
4. Escolha um nível de resiliência para suas conexões de rede. O nível de resiliência pode ser um dos seguintes:

   - Resiliência máxima
   - Alta resiliência
   - Desenvolvimento e teste

   Para obter descrições e informações mais detalhadas sobre esses níveis de resiliência, consulte the section called “AWS Direct Connect Kit de ferramentas de resiliência”.
5. Escolha Próximo.
6. Na página Configurar conexões, forneça os detalhes a seguir.

   a. Na lista suspensa Largura de banda, escolha a largura de banda necessária para a conexão. Isso pode variar de 1 Gbps a 400 Gbps.

b. Em Local, escolha o Direct Connect local apropriado e, em seguida, escolha o primeiro provedor de serviços de localização, selecione o provedor de serviços que fornece conectividade para a conexão nesse local.

c. Em Segundo local, escolha o apropriado Direct Connect no segundo local e, em seguida, escolha o provedor de serviços de segundo local, selecione o provedor de serviços que fornece conectividade para a conexão nesse segundo local.

d. (Opcional) Configure a segurança MAC (MACsec) para a conexão. Em Configurações adicionais, selecione Solicitar uma porta MACsec compatível.

   MACsec só está disponível em conexões dedicadas.

e. (Opcional) Escolha Adicionar tag para adicionar key/value pares e ajudar ainda mais a identificar essa conexão.

   - Em Chave, insira o nome da chave.
   - Em Valor insira o valor da chave.

   Para remover uma tag existente, escolha a tag e, em seguida, escolha Remover tag. Você não pode ter tags vazias.

7. Escolha Próximo.
8. Na página Revisar e criar, verifique a conexão. Essa página também exibe as estimativas do custo de uso da porta e taxas adicionais de transferência de dados.
9. Escolha Criar.
10. Baixe sua Carta de autorização e atribuição da instalação de conexão (LOA-CFA). Para obter mais informações, consulte the section called “Carta de autorização e atribuição de instalação de conexão (LoA-CFA)”.

Use um dos seguintes comandos.

- create-connection (AWS CLI)
- CreateConnection(Direct Connect API)

Crie uma conexão Direct Connect clássica

Para conexões dedicadas, você pode enviar uma solicitação de conexão usando o Direct Connect console. Para conexões hospedadas, trabalhe com um AWS Direct Connect parceiro para solicitar uma conexão hospedada. Verifique se você tem as seguintes informações:

- A velocidade da porta que você precisa. Para conexões dedicadas, não será possível alterar a velocidade da porta após a criação da solicitação de conexão. Para conexões hospedadas, seu parceiro do AWS Direct Connect poderá alterar a velocidade.
- O Direct Connect local em que a conexão deve ser encerrada.

> **Note**
>
> Você não pode usar o Direct Connect console para solicitar uma conexão hospedada. Em vez disso, entre em contato com um AWS Direct Connect parceiro, que pode criar uma conexão hospedada para você, que você aceita. Ignore o procedimento a seguir e vá até Aceitar a conexão hospedada.

Para criar uma nova Direct Connect conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Na tela do Direct Connect, em Get started (Conceitos básicos), selecione Create a connection (Criar uma conexão).
3. Escolha Classic (Clássica).
4. Em Name (Nome), insira um nome para a conexão.
5. Em Location (Local), selecione o local do Direct Connect apropriado.
6. Se aplicável, para Sub Location (Sublocal), escolha o andar mais próximo de você ou do provedor de rede. Essa opção só está disponível se o local tiver salas de reunião (MMRs) em vários andares do edifício.
7. Em Port Speed (Velocidade da porta), selecione a largura de banda da conexão.
8. Em On-premises, selecione Conectar por meio de um parceiro do Direct Connect ao usar essa conexão para se conectar ao seu data center.
9. Em Provedor de serviços, selecione o AWS Direct Connect Parceiro. Caso use um parceiro que não esteja na lista, selecione Other (Outro).
10. Se você tiver selecionado Other (Outro) em Service provider (Provedor de serviços), em Name of other provider (Nome de outro provedor), insira o nome do parceiro que você usa.
11. (Opcional) Escolha Adicionar tag para adicionar key/value pares e ajudar ainda mais a identificar essa conexão.

    - Em Chave, insira o nome da chave.

- Em Valor insira o valor da chave.

Para remover uma tag existente, escolha a tag e, em seguida, escolha Remover tag. Você não pode ter tags vazias.

12. Escolha Criar conexão.

Pode levar até 72 horas úteis AWS para analisar sua solicitação e provisionar uma porta para sua conexão. Durante esse período, você pode receber um e-mail com uma solicitação para obter mais informações sobre o caso de uso ou o local especificado. O e-mail é enviado para o endereço de e-mail que você usou quando se inscreveu AWS. Você deve responder em até 7 dias, ou a conexão será excluída.

Para obter mais informações, consulte Conexões dedicadas e hospedadas.

Baixe o programa Direct Connect LOA-CFA

Você pode baixar o LOA-CFA usando o Direct Connect console ou pela linha de comando. Após fazer o download da LoA-CFA e fornecê-la ao seu provedor de rede ou de colocalização, esse provedor poderá solicitar a conexão cruzada para você.

Para baixar a LOA-CFA

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione a conexão e escolha Visualizar detalhes.
4. Escolha Download LOA-CFA (Fazer download da LOA-CFA).

> **Note**
>
> Caso o link não esteja habilitado, a LOA-CFA ainda não está disponível para download. Um caso do Support será criado solicitando informações adicionais. Após responder à solicitação e processá-la, a LOA-CFA estará disponível para download. Se ainda não estiver disponível, entre em contato com o AWS Support.

5. Envie a LOA-CFA ao provedor de rede ou de colocação, de maneira que ele possa solicitar uma conexão cruzada para você. O processo de contato pode variar para cada provedor de

colocação. Para obter mais informações, consulte Solicitar conexões cruzadas em locais do Direct Connect.

Para baixar a LOA-CFA usando a linha de comando ou a API

- describe-loa (AWS CLI)
- DescribeLoa(Direct Connect API)

Associar um MACsec CKN/CAK a uma conexão Direct Connect

Depois de criar a conexão que oferece suporte MACsec, você pode associar a CKN/CAK à conexão. Você pode criar a associação usando o Direct Connect console ou por meio da linha de comando ou da API.

> **Note**
>
> Você não pode modificar uma chave MACsec secreta depois de associá-la a uma conexão. Se você precisar modificar a chave, desassocie a chave da conexão e associe uma nova chave à conexão. Para obter mais informações sobre como remover uma associação, consulte Remover a associação entre uma chave MACsec secreta e uma conexão.

Para associar uma MACsec chave a uma conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de à esquerda, selecione Connections (Conexões).
3. Selecione uma conexão e escolha Visualizar detalhes.
4. Escolha Associar chave.
5. Insira a MACsec chave.

   [Use o CAK/CKN par] Escolha o par de chaves e faça o seguinte:

   - Em Chave de associação de conectividade (CAK), insira a CAK.
   - Em Nome da chave de associação de conectividade (CKN), insira a CKN.

[Use o segredo] Escolha o segredo existente do Secret Manager e, em seguida, em Secret, selecione a chave MACsec secreta.

6. Escolha Associar chave.

Para associar uma MACsec chave a uma conexão usando a linha de comando ou a API

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(Direct Connect API)

Remover a associação entre uma chave MACsec secreta e uma Direct Connect conexão

Você pode remover a associação entre a conexão e a MACsec chave usando o Direct Connect console ou por meio da linha de comando ou da API.

Para remover uma associação entre uma conexão e uma MACsec chave

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2.
3. No painel de à esquerda, selecione Connections (Conexões).
4. Selecione uma conexão e escolha Visualizar detalhes.
5. Selecione o MACsec segredo a ser removido e, em seguida, escolha Desassociar chave.
6. Na caixa de diálogo de confirmação, digite desassociar e escolha Desassociar.

Para remover uma associação entre uma conexão e uma MACsec chave usando a linha de comando ou a API

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(Direct Connect API)

Direct Connect Conexões hospedadas

Para criar uma conexão Direct Connect hospedada, você precisa das seguintes informações:

Direct Connect location

Trabalhe com um AWS Direct Connect AWS Direct Connect parceiro no Programa de parceiros para ajudá-lo a estabelecer circuitos de rede entre um Direct Connect local e seu data center, escritório ou ambiente de colocation. Eles também podem ajudar a oferecer espaço de colocação dentro da mesma instalação do local. Para obter mais informações, consulte Parceiros de entrega do Direct Connect.

> **Note**
>
> Você não pode solicitar uma conexão hospedada por meio do Direct Connect console. No entanto, um AWS Direct Connect parceiro pode criar e configurar uma conexão hospedada para você. Após a configuração, a conexão aparecerá no painel Conexões do console.
>
> Você deve aceitar a conexão hospedada antes de poder usá-la. Para obter mais informações, consulte Aceitar uma conexão hospedada.

Port speed (Velocidade da porta)

Para conexões hospedadas, os valores possíveis são 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps e 25 Gbps. Observe que somente os Direct Connect parceiros que atenderam aos requisitos específicos podem criar uma conexão hospedada de 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps ou 25 Gbps. As conexões de 25 Gbps estão disponíveis somente em localizações do Direct Connect que disponibilizam velocidades de porta de 100 Gbps.

Observe o seguinte:

- As velocidades das portas de conexão só podem ser alteradas pelo seu parceiro AWS Direct Connect. Verifique com seu parceiro do AWS Direct Connect se ele oferece suporte ao upgrade ou downgrade de uma conexão existente. Se seu parceiro aceita upgrade/downgrade da sua conexão, não é mais necessário excluir e, em seguida, criar novamente uma conexão para fazer upgrade ou downgrade da largura de banda de uma conexão hospedada atual.
- AWS usa o policiamento de tráfego em conexões hospedadas, o que significa que, quando a taxa de tráfego atinge a taxa máxima configurada, o excesso de tráfego é eliminado. Isso pode resultar em tráfego intermitente com throughput mais baixo do que tráfego não intermitente.

- Só é possível habilitar os frames jumbo em conexões se eles tiverem sido originalmente habilitados na conexão principal hospedada do Direct Connect . Se os frames jumbo não estiverem habilitados nessa conexão principal, não será possível habilitá-los em nenhuma conexão.

As seguintes operações do console estarão disponíveis depois que você tiver solicitado e aceitado uma conexão hospedada:

- Excluir uma conexão
- Atualizar uma conexão
- Visualização de detalhes da conexão do

Após aceitar uma conexão, crie uma interface virtual para se conectar a recursos públicos e privados da AWS . Para obter mais informações, consulte Interfaces virtuais e interfaces virtuais hospedadas.

Aceitar uma conexão Direct Connect hospedada

Se você estiver interessado em comprar uma conexão hospedada, entre em contato com um AWS Direct Connect AWS Direct Connect parceiro no Programa de parceiros. O parceiro provisiona a conexão para você. Depois que for configurada, a conexão será visualizada no painel Connections (Conexões) do console do Direct Connect .

Para usar uma conexão hospedada, você deve aceitar a conexão. Você pode aceitar uma conexão hospedada usando o Direct Connect console ou usando a linha de comando ou a API.

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione a conexão hospedada e escolha Visualizar detalhes.
4. Marque a caixa de seleção de confirmação e escolha Aceitar.

Para aceitar uma conexão hospedada usando a linha de comando ou a API

- confirm-connection (AWS CLI)
- ConfirmConnection(Direct Connect API)

Excluir uma Direct Connect conexão

Você pode excluir uma conexão, desde que não haja interfaces virtuais conectadas. A exclusão da conexão interrompe todas as cobranças por hora de porta dessa conexão, mas você ainda pode incorrer em cobranças de conexão cruzada ou de circuito de rede (veja abaixo). Direct Connect as taxas de transferência de dados estão associadas às interfaces virtuais. Para obter mais informações sobre como excluir uma interface virtual, consulte Exclusão de uma interface virtual.

Antes de excluir uma conexão, faça o download da LoA para a conexão que contém as informações entre contas, para que você tenha as informações relevantes sobre os circuitos que estão sendo desconectados. Para ver as etapas de download da LOA de conexão, consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA).

Ao excluir uma conexão, AWS instruirá o provedor de colocation a desconectar seu dispositivo de rede do roteador Direct Connect removendo o cabo de conexão cruzada de fibra óptica do patch panel aplicável. AWS No entanto, o provedor de colocalização ou de circuito ainda pode aplicar cobranças por conexão cruzada ou por circuito de rede, uma vez que o cabo de conexão cruzada pode continuar conectado ao seu dispositivo de rede. Essas cobranças pela conexão cruzada são independentes do Direct Connect e devem ser canceladas com o provedor de colocalização ou de circuito usando as informações contidas na LoA.

Caso a conexão faça parte de um grupo de agregação de links (LAG), não será possível excluir a conexão caso isso faça o LAG ficar abaixo da configuração do número mínimo de conexões operacionais.

Você pode excluir uma conexão usando o Direct Connect console ou a linha de comando ou a API.

Para excluir uma conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione as conexões e escolha Delete (Excluir).
4. Na caixa de diálogo de confirmação Delete (Excluir), escolha Delete (Excluir).

Para excluir uma conexão usando a linha de comando ou a API

- delete-connection (AWS CLI)
- DeleteConnection(Direct Connect API)

Atualizar uma Direct Connect conexão

Você pode atualizar o seguinte atributo de conexão usando o Direct Connect console ou usando a linha de comando ou a API.

- O nome da conexão.
- O modo de MACsec criptografia da conexão.

> **Note**
>
> Embora você não possa modificar diretamente MACSec as propriedades em conexões hospedadas, os parceiros podem habilitar MACSec suas próprias interconexões para fornecer conexões hospedadas seguras a seus clientes.

Os valores válidos são:

- `should_encrypt`
- `must_encrypt`

  Quando você define o modo de criptografia para esse valor, a conexão fica inativa quando a criptografia estiver inativa.
- `no_encrypt`

Para atualizar uma conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione a conexão e escolha Editar.
4. Modifique a conexão:

   [Alterar o nome] Em Name (Nome), insira um novo nome para a conexão.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

5. Escolha Edit connection (Editar conexão).

Para atualizar uma conexão usando a linha de comando ou a API

- update-connection (AWS CLI)
- UpdateConnection(Direct Connect API)

Exibir detalhes da Direct Connect conexão

Você pode ver o status atual da sua conexão usando o Direct Connect console ou usando a linha de comando ou a API. Você também pode visualizar o ID de conexão (por exemplo, `dxcon-12nikabc`) e verificar se ele é compatível com o ID de conexão na LOA-CFA que recebeu ou obteve por download.

Para obter informações sobre como monitorar conexões, consulte Monitoramento de recursos do Direct Connect.

Para visualizar detalhes sobre uma conexão

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de à esquerda, selecione Connections (Conexões).
3. Selecione uma conexão e escolha Visualizar detalhes.

Para descrever uma conexão usando a linha de comando ou a API

- describe-connections (AWS CLI)
- DescribeConnections(Direct Connect API)

Solicitar conexões cruzadas em locais do Direct Connect

Após fazer download da Letter of Authorization and Connecting Facility Assignment (LOA-CFA – Carta de autorização e atribuição da instalação de conexão), é necessário completar a conexão de rede cruzada, também conhecida como conexão cruzada. Se você já tiver equipamentos localizados em um local do Direct Connect, entre em contato com o provedor apropriado para completar a conexão cruzada. Para obter instruções específicas para cada provedor, consulte as tabelas apresentadas abaixo. Os parceiros e as informações de contato estão organizados por região. Para obter preços específicos de conexão cruzada, será necessário entrar em contato diretamente com o parceiro do Direct Connect. Depois que a conexão cruzada for estabelecida, você poderá criar as interfaces virtuais usando o console do Direct Connect.

Alguns locais estão configurados como um campus. Para obter mais informações, incluindo as velocidades disponíveis em cada local, consulte Locais do Direct Connect.

Se ainda não tiver equipamentos localizados em um local do Direct Connect, você poderá trabalhar com um dos parceiros na Rede de Parceiros da AWS (APN). Eles te ajudam a se conectar a um local do Direct Connect. Para obter mais informações, consulte Parceiros da APN que oferecem suporte ao Direct Connect. É necessário compartilhar a LOA-CFA com o provedor selecionado para facilitar a solicitação de conexão cruzada.

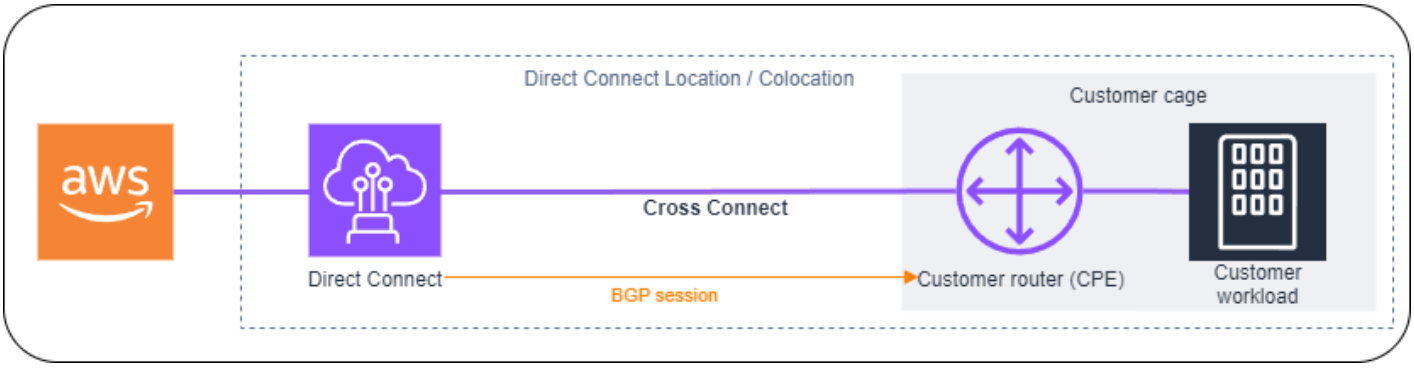
Uma conexão do Direct Connect pode fornecer acesso a recursos em outras Regiões. Para obter mais informações, consulte Acesso a regiões remotas do Direct Connect.

> **Note**
>
> Caso a conexão cruzada não seja completada dentro de 90 dias, a autoridade concedida pela LOA-CFA expire. Para renovar uma LOA-CFA que tenha expirado, você pode baixá-la novamente do console do Direct Connect. Para obter mais informações, consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA).

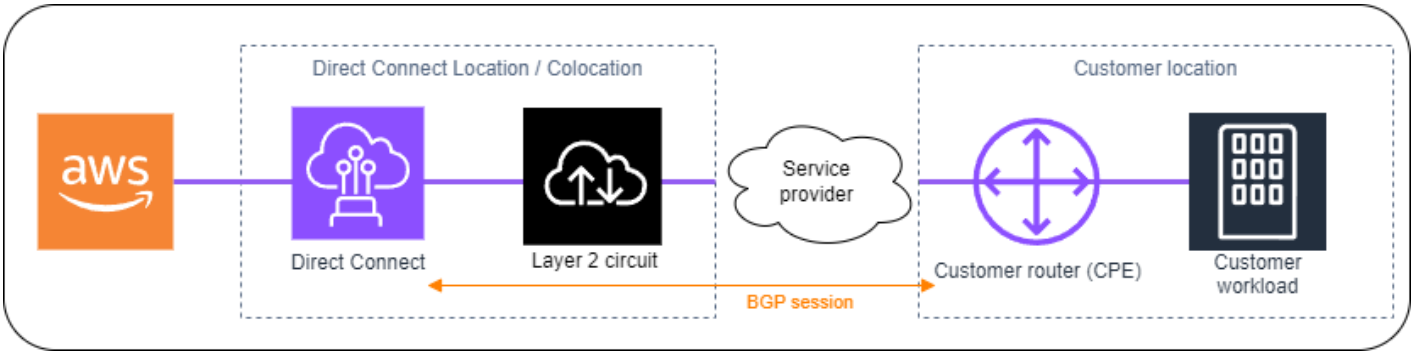
Opções de conectividade

As opções disponíveis para conexão com uma localização do Direct Connect podem variar de acordo com o parceiro e com a região da AWS. É possível colaborar com um dos parceiros da Rede de Parceiros da AWS (APN), que pode fornecer uma ou mais das seguintes opções de conectividade:

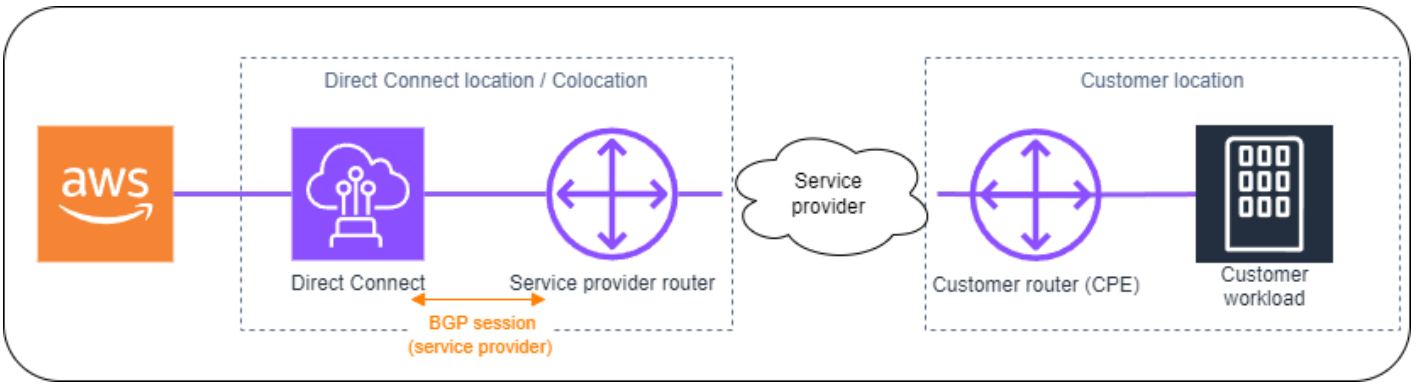
- Caso você tenha recursos implantados no mesmo data center ou na mesma instalação de colocalização que a localização do Direct Connect, a instalação pode fornecer uma conexão cruzada entre o equipamento do Direct Connect e seus recursos. É necessário fornecer a LoA-CFA à instalação antes de prosseguir com isso. Consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA) para obter mais informações. A seguir, é apresentado um exemplo dessa opção de conectividade do Direct Connect:



- Amplie a conexão do Direct Connect na Camada 2 (camada de enlace de dados) por meio de um “circuito” da localização do Direct Connect até a localização do cliente ao colaborar com os parceiros do Direct Connect. O roteador instalado na localização do cliente estabelecerá uma sessão do BGP direta com o equipamento da AWS. Exemplos de tecnologias que podem ser usadas incluem Metro Ethernet, fibra óptica escura ou Wavelength. A seguir, é apresentado um exemplo dessa opção de conectividade do Direct Connect.



- Amplie a conexão do Direct Connect na Camada 3 (camada de rede) desde a localização do Direct Connect até a sua localização ao colaborar com os parceiros do Direct Connect. Nesta opção de conectividade, o parceiro do Direct Connect fornece um roteador na localização do Direct Connect que estabelece uma sessão do Protocolo de Gateway da Borda (BGP) com o equipamento da AWS. Em seguida, o parceiro do Direct Connect estabelece outra sessão do BGP com você. Isso pode ser realizado, por exemplo, por meio do Multiprotocol Label Switching (MPLS). A seguir, é apresentado um exemplo dessa opção de conectividade do Direct Connect.



Leste dos EUA (Ohio)

Local	Como solicitar uma conexão
Cologix COL2, Columbus	Entre em contato com a Cologix pelo e-mail sales@cologix.com.
Cologix MIN3, Minneapolis	Entre em contato com a Cologix pelo e-mail sales@cologix.com.
CyrusOne West III, Houston	Envie uma solicitação usando o formulário de contato do cliente.
Equinix CH2, Chicago	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
QTS, Chicago	Entre em contato com a QTS pelo e-mail AConnect@qtsdatacenters.com.
Netrality Data Centers, 1102 Grand, Kansas City	Entre em contato com a Netrality Data Centers pelo e-mail support@netrality.com.

Leste dos EUA (Norte da Virgínia)

Local	Como solicitar uma conexão
165 Halsey Street, Newark	Entre em contato com operations@165halsey.com.

Local	Como solicitar uma conexão
CoreSite 32k, Nova York	Faça um pedido usando o CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
CoreSite VA1-VA2, Reston	Faça um pedido no CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
Digital Realty ATL1 e ATL2, Atlanta	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
Digital Realty IAD38, Ashburn	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
Equinix DC1-DC6 e DC10-D12, Ashburn	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix DAA1-DC3 e DC6, Dallas	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix MI1, Miami	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix NY5, Secaucus	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
KIO Networks QRO 1, Querétaro, México	Entre em contato com a KIO Networks.
Markley, One Summer Street, Boston	Para clientes atuais, crie uma solicitação usando o portal do cliente. Para novas consultas, entre em contato pelo e-mail sales@markleygroup.com.
Netrality Data Centers, 2nd floor MMR, Philadelphia	Entre em contato com a Netrality Data Centers pelo e-mail support@netrality.com.

Local	Como solicitar uma conexão
QTS ATL1, Atlanta	Entre em contato com a QTS pelo e-mail AConnect@qtsdatacenters.com.

Oeste dos EUA (Norte da Califórnia)

Local	Como solicitar uma conexão
CoreSite, LA1, Los Angeles	Faça um pedido usando o CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
CoreSite SV2, Milpitas	Faça um pedido usando o CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
CoreSite SV4, Santa Clara	Faça um pedido usando o CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site MyCoreSite.
EdgeConneX, Phoenix	Faça um pedido usando o EdgeOS Customer Portal. Depois que você tiver enviado o formulário, o EdgeConneX fornecerá um formulário de pedido de serviço para aprovação. Você pode enviar perguntas para o e-mail cloudaccess@edgeconnex.com.
Equinix LA3, El Segundo	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix SV1 e SV5, San José	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Entre em contato com a phoenixNAP pelo e-mail provisioning@phoenixnap.com.

Oeste dos EUA (Oregon)

Local	Como solicitar uma conexão
CoreSite DE1, Denver	Faça um pedido usando o CoreSite Customer Portal. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
Digital Realty SEA10, Westin Building, Seattle	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Faça um pedido usando o EdgeOS Customer Portal. Depois que você tiver enviado o formulário, o EdgeConneX fornecerá um formulário de pedido de serviço para aprovação. Você pode enviar perguntas para o e-mail cloudaccess@edgeconnex.com.
Equinix SE2, Seattle	Entre em contato com a Equinix pelo e-mail support@equinix.com.
Pittock Block, Portland	Envie solicitações por e-mail para crossconnect@pittock.com ou faça as solicitações pelo telefone +1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Entre em contato com a Switch SUPERNAP pelo e-mail orders@supernap.com.
TierPoint Seattle	Entre em contato com a TierPoint pelo e-mail sales@tierpoint.com.

África (Cidade do Cabo)

Local	Como solicitar uma conexão
Ponto de troca de Internet da Cidade do Cabo/Data centers da Teraco	Entre em contato com a Teraco pelo e-mail support@teraco.co.za para clientes Teraco já existentes e connect@teraco.co.za para novos clientes.

Local	Como solicitar uma conexão
Teraco JB1, Joanesburgo, África do Sul	Entre em contato com a Teraco pelo e-mail support@teraco.co.za para clientes Teraco já existentes e connect@teraco.co.za para novos clientes.

Ásia-Pacífico (Jacarta)

Local	Como solicitar uma conexão
DCI JK3, Jacarta	Entre em contato com a DCI Indonesia pelo e-mail awsdx@dci-indonesia.com.
NTT 2 Data Center, Jacarta	Entre em contato com a NTT pelo e-mail tps.cms.presales@global.ntt.

Ásia-Pacífico (Mumbai)

Local	Como solicitar uma conexão
Equinix, Mumbai	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Entre em contato com o departamento de vendas e marketing da NetMagic gratuitamente em 18001033130 ou pelo e-mail marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Entre em contato com a Sify pelo e-mail aws.directconnect@sifycorp.com.
STT Delhi DC2, Delhi	Entre em contato com a STT no e-mail enquiry.AWSDX@sttelemediagdc.in.
STT GDC Pvt. Ltd. VSB, Chennai	Entre em contato com a STT no e-mail enquiry.AWSDX@sttelemediagdc.in.

Local	Como solicitar uma conexão
STT Hyderabad DC1, Hyderabad	Entre em contato com a STT no e-mail enquiry.AWSDX@sttelemediagdc.in.

Ásia-Pacífico (Seul)

Local	Como solicitar uma conexão
Digital Realty ICN1, Seul	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
KINX Gasan Data Center, Seul	Entre em contato com a KINX pelo e-mail sales@kinx.net.
LG U+ Pyeong-Chon Mega Center, Seul	Envie o documento da LOA para kidcadmin@lguplus.co.kr e center8@kidc.net.

Ásia-Pacífico (Singapura)

Local	Como solicitar uma conexão
Equinix HK1, Tsuen Wan N.T., RAE de Hong Kong	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix SG2, Cingapura	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Global Switch, Cingapura	Entre em contato com a Global Switch pelo e-mail salessingapore@globalswitch.com.
GPX, Mumbai	Entre em contato com a GPX (Equinix) pelo e-mail awsdealreg@equinix.com.

Local	Como solicitar uma conexão
iAdvantage Mega-i, Hong Kong	Entre em contato com a iAdvantage pelo e-mail cs@iadvantage.net ou faça um pedido por meio do formulário eletrônico iAdvantage Cabling Order.
Menara AIMS, Kuala Lumpur	Os clientes existentes da AIMS podem solicitar um pedido de X-Connect usando o portal de Atendimento ao cliente, preenchendo o formulário de solicitação de ordem de trabalho de engenharia. Entrar em contato com service.delivery@aims.com.my se houver problemas ao enviar a solicitação.
TCC Data Center, Bangkok	Entre em contato com a TCC Technology Co., Ltd pelo e-mail gateway.ne@tcc-technology.com.

Ásia-Pacífico (Sydney)

Local	Como solicitar uma conexão
CDC Hume 2, Camberra	Faça login no portal do cliente em CDC Customer Portal.
Datacom DH6, Auckland	Entre em contato com a Datacom em Datacom Orbit – Auckland.
Equinix ME2, Melbourne	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix SY3, Sydney	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Global Switch, Sydney	Entre em contato com a Global Switch pelo e-mail salessydney@globalswitch.com.
NEXTDC C1, Canberra	Entre em contato com a NEXTDC pelo e-mail nxtops@nextdc.com.
NEXTDC M1, Melbourne	Entre em contato com a NEXTDC pelo e-mail nxtops@nextdc.com.

Local	Como solicitar uma conexão
NEXTDC P1, Perth	Entre em contato com a NEXTDC pelo e-mail nxtops@nextdc.com.
NEXTDC S2, Sydney	Entre em contato com a NEXTDC pelo e-mail nxtops@nextdc.com.

Ásia-Pacífico (Tóquio)

Local	Como solicitar uma conexão
AT Tokyo Chuo Data Center, Tóquio	Entre em contato com a AT TOKYO no e-mail at-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Entre em contato com a Chief Telecom pelo e-mail vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Entre em contato com a CHT Taipei IDC NOC pelo e-mail taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix TY2, Tóquio	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
NEC Inzai, Inzai	Entre em contato com a NEC Inzai pelo e-mail connection_support@ices.jp.nec.com.

Canadá (Central)

Local	Como solicitar uma conexão
Telehouse, 250 Front St W, Toronto	Entre em contato com product@ca.telehouse.com.

Local	Como solicitar uma conexão
Cologix MTL3, Montreal	Entre em contato com a Cologix pelo e-mail sales@cologix.com.
Cologix VAN2, Vancouver	Entre em contato com a Cologix pelo e-mail sales@cologix.com.
eStruxture, Montreal	Entre em contato com a eStruxture pelo e-mail directconnect@estruxture.com.

China (Pequim)

Local	Como solicitar uma conexão
CIDS Jiachuang IDC, Beijing	Entre em contato pelo e-mail dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao IDC, Beijing	Entre em contato pelo e-mail dx-order@sinnet.com.cn.
GDS No. 3 Data Center, Shanghai	Entre em contato pelo e-mail dx@nwcdcloud.cn.
GDS No. 3 Data Center, Shenzhen	Entre em contato pelo e-mail dx@nwcdcloud.cn.

China (Ningxia)

Local	Como solicitar uma conexão
Industrial Park IDC, Ningxia	Entre em contato pelo e-mail dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Entre em contato pelo e-mail dx@nwcdcloud.cn.

Europa (Frankfurt)

Local	Como solicitar uma conexão
CE Colo, Praga, República Tcheca	Entre em contato com a CE Colo pelo e-mail info@cecolo.com.
DigiPlex Ulven, Oslo, Noruega	Entre em contato com a DigiPlex pelo e-mail helpme@digiplex.com.
Equinix AM3, Amsterdã, Holanda	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix FR5, Frankfurt	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix HE6, Helsinki	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix MU1, Munique	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix WA1, Varsóvia	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Interxion AMS7, Amsterdã	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
Interxion CPH2, Copenhague	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
Interxion FRA6, Frankfurt	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
Interxion MAD2, Madri	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
Interxion VIE2, Viena	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.

Local	Como solicitar uma conexão
Interxion ZUR1, Zurique	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
IPB, Berlim	Entre em contato com a IPB pelo e-mail kontakt@ipb.de.
Equinix ITConic MD2, Madri	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.

Europa (Irlanda)

Local	Como solicitar uma conexão
Digital Realty (Reino Unido), Docklands	Entre em contato com a Digital Realty (Reino Unido) pelo e-mail amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Entre em contato com a Eircom em datacentre@eirevo.ie.
Equinix DX1, Dublin	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix LD5, Londres (Slough)	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Interxion DUB2, Dublin	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.
Interxion MRS1, Marselha	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.

Europa (Milão)

Local	Como solicitar uma conexão
CDLAN srl Via Caldera 21, Milão	Entre em contato com a CDLAN em sales@cdlan.it.
Equinix, ML2, Milão, Itália	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.

Europa (Londres)

Local	Como solicitar uma conexão
Digital Realty (Reino Unido), Docklands	Entre em contato com a Digital Realty (Reino Unido) pelo e-mail amazon.orders@digitalrealty.com.
Equinix LD5, Londres (Slough)	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix MA3, Manchester	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Telehouse West, Londres	Entre em contato com a Telehouse do Reino Unido pelo e-mail sales.support@uk.telehouse.net.

Europa (Paris)

Local	Como solicitar uma conexão
Equinix PA3, Paris	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Interxion PAR7, Paris	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.

Local	Como solicitar uma conexão
Telehouse Voltaire, Paris	Entre em contato com a Telehouse Paris Voltaire usando a página Contact Us.

Europa (Estocolmo)

Local	Como solicitar uma conexão
Interxion STO1, Estocolmo	Entre em contato com a Interxion pelo e-mail customer.services@interxion.com.

Europa (Zurique)

Local	Como solicitar uma conexão
Equinix ZRH51, Oberengstringen, Suíça	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.

Israel (Tel Aviv)

Local	Como solicitar uma conexão
MedOne, Haifa	Entre em contato com a MedOne em support@Medone.co.il
EdgeConneX, Herzliya	Entre em contato com a EdgeConneX em info@edgeconnecx.com.

Oriente Médio (Bahrein)

Local	Como solicitar uma conexão
AWS Bahrain DC53, Manama	Para concluir a conexão, é possível trabalhar com um de nossos provedores de rede parceiros no local para estabelecer conectividade. Em seguida, você fornecerá uma Letter of Authorization (LOA – Carta de autorização) do provedor de rede para a AWS por meio do Support Center da AWS e a AWS concluirá a conexão cruzada nesse local.
AWS Bahrain DC52, Manama	Para concluir a conexão, é possível trabalhar com um de nossos provedores de rede parceiros no local para estabelecer conectividade. Em seguida, você fornecerá uma Letter of Authorization (LOA – Carta de autorização) do provedor de rede para a AWS por meio do Support Center da AWS e a AWS concluirá a conexão cruzada nesse local.

Oriente Médio (Emirados Árabes Unidos)

Local	Como solicitar uma conexão
Equinix DX1, Dubai, Emirados Árabes Unidos	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Etisalat SmartHub Data Centre, Fujairah, Emirados Árabes Unidos	Entre em contato com o Etisalat SmartHub Data Centre pelo e-mail IntlSales-C&WS@etisalat.ae.

América do Sul (São Paulo)

Local	Como solicitar uma conexão
Cirion BNARAGMS, Buenos Aires	Entre em contato com a Cirion em cloud.connect@ciriontechnologies.com.
Equinix RJ2, Rio de Janeiro	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix SP4, São Paulo	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Tivit	Entre em contato com a Tivit pelo e-mail aws@tivit.com.br.

AWS GovCloud (Leste dos EUA)

Você não pode solicitar conexões nessa região.

AWS GovCloud (Oeste dos EUA)

Local	Como solicitar uma conexão
Equinix SV5, San Jose	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.

Direct Connect interfaces virtuais e interfaces virtuais hospedadas

Você deve criar uma das seguintes interfaces virtuais (VIFs) para começar a usar sua Direct Connect conexão.

- Interface virtual privada: uma interface virtual privada deve ser usada para acessar uma Amazon VPC usando endereços IP privados.
- Interface virtual pública: uma interface virtual pública pode acessar todos os serviços AWS públicos usando endereços IP públicos.
- Interface virtual de trânsito: é necessário usar uma interface virtual de trânsito para acessar um ou mais gateways de trânsito da Amazon VPC associados a gateways do Direct Connect. Você pode usar interfaces virtuais de trânsito com qualquer conexão Direct Connect dedicada ou hospedada de qualquer velocidade. Para obter informações sobre configurações de gateway Direct Connect, consulte Gateways Direct Connect.

Para se conectar a outros AWS serviços usando IPv6 endereços, consulte a documentação do serviço para verificar se o IPv6 endereçamento é suportado.

Regras de anúncio de prefixo da interface virtual pública

Nós anunciamos os prefixos apropriados da Amazon para que você possa acessar os endereços IP públicos das cargas de trabalho em seu VPCs e em outros serviços. AWS Você pode acessar todos os AWS prefixos por meio dessa conexão; por exemplo, endereços IP públicos usados por instâncias do Amazon EC2, Amazon S3, endpoints AWS de API para serviços e Amazon.com. Você não tem acesso a prefixos que não sejam da Amazon. Para obter uma lista atual dos prefixos usados por AWS, consulte Intervalos de endereços AWS IP no Guia do usuário da Amazon VPC. Nesta página, você pode baixar um `.json` arquivo dos intervalos de AWS IP publicados atualmente. Observe que, para intervalos de endereços IP publicados:

- Os prefixos anunciados via BGP em uma interface virtual pública podem ser agregados ou desagregados em comparação com o que está listado na lista de intervalos de endereços IP. AWS
- Qualquer intervalo de endereços IP que você acesse AWS por meio de seus próprios endereços IP (BYOIP) não é incluído no `.json` arquivo, mas AWS ainda anuncia esses endereços BYOIP em uma interface virtual pública.

- AWS não anuncia novamente os prefixos de clientes que foram recebidos pelas interfaces virtuais públicas do Direct Connect para redes externas. AWS Os prefixos anunciados em uma interface virtual pública estarão visíveis para todos os clientes na AWS.

> **Note**
>
> Recomendamos que você use um filtro de firewall (com base no source/destination endereço dos pacotes) para controlar o tráfego de e para alguns prefixos.

Para obter mais informações sobre interfaces virtuais públicas e políticas de roteamento, consulte the section called “Políticas de roteamento de interface virtual pública”.

SiteLink

Se você estiver criando uma interface virtual privada ou de trânsito, você pode usar SiteLink.

SiteLink é um recurso opcional do Direct Connect para interfaces virtuais privadas que permite a conectividade entre quaisquer dois pontos de presença do Direct Connect (PoPs) na mesma AWS partição usando o caminho mais curto disponível na AWS rede. Isso permite que você conecte sua rede on-premises por meio da rede global da AWS sem precisar rotear seu tráfego por uma região. Para obter mais informações, SiteLink consulte Apresentando Direct Connect SiteLink.

> **Note**
>
> - SiteLink não está disponível nas regiões da China AWS GovCloud (US) e nas regiões da China.
> - SiteLink não funciona se um roteador local anunciar a mesma rota AWS em várias interfaces virtuais.

Há uma taxa de preço separada para uso SiteLink. Para obter mais informações, consulte Preços do AWS Direct Connect.

SiteLink não oferece suporte a todos os tipos de interface virtual. A tabela a seguir mostra o tipo de interface e se ela é compatível.

Tipo de interface virtual	Compatível/não compatível
Interface virtual de trânsito	Compatível
Interface virtual privada anexada a um gateway do Direct Connect com um gateway virtual	Compatível
Interface virtual privada anexada a um gateway do Direct Connect não associado a um gateway virtual ou gateway de trânsito	Compatível
Interface virtual privada anexada a um gateway virtual	Não compatível
Interface virtual pública	Não compatível

O comportamento de roteamento de tráfego de Regiões da AWS (gateways virtuais ou de trânsito) para locais locais por meio de uma interface virtual SiteLink habilitada varia um pouco do comportamento padrão da interface virtual do Direct Connect com um AWS prefixo de caminho. Quando SiteLink ativada, as interfaces virtuais de um Região da AWS preferem um caminho BGP com um comprimento de caminho AS menor a partir de um local do Direct Connect, independentemente da região associada. Por exemplo, uma região associada é anunciada para cada local do Direct Connect. Se SiteLink estiver desativado, por padrão, o tráfego proveniente de um gateway virtual ou de trânsito prefere um local do Direct Connect associado a ele Região da AWS, mesmo que o roteador de locais do Direct Connect associados a diferentes regiões anuncie um caminho com um comprimento de caminho AS menor. O gateway virtual ou de trânsito ainda preferirá o caminho dos locais do Direct Connect que sejam locais em relação à Região da AWS associada.

SiteLink suporta um tamanho máximo de MTU de quadro jumbo de 8500 ou 9001, dependendo do tipo de interface virtual. Para obter mais informações, consulte MTUs para interfaces virtuais privadas ou interfaces virtuais de trânsito.

Pré-requisitos para interfaces virtuais

Antes de criar uma interface virtual, faça o seguinte:

- Crie uma conexão. Para obter mais informações, consulte Criar uma conexão usando o Assistente de conexão.
- Crie um grupo de agregação de links (LAG) quando você tiver várias conexões que deseja tratar como uma única. Para mais informações, consulte Associar uma conexão a um LAG.

Para criar uma interface virtual, você precisa das seguintes informações:

Recurso	Informações necessárias
Conexão	A Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se você estiver criando a interface virtual para outra conta, precisará do AWS ID da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma AWS região, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário , a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect. **Note** • Você não pode usar o mesmo ASN para o gateway do cliente e o gateway gateway/Direct Connect virtual na interface virtual.

Recurso	Informações necessárias
	• Você pode usar o mesmo ASN do gateway do cliente em diversas interfaces virtuais. • Diversas interfaces virtuais podem ter o mesmo gateway virtual ou o mesmo ASN do gateway do Direct Connect e ASN do gateway do cliente, desde que façam parte de conexões do Direct Connect separadas. Por exemplo: Gateway virtual (ASN 64.496) <---Interface virtual 1 (conexão do Direct Connect 1) ---> Gateway do cliente (ASN 64.511) Gateway virtual (ASN 64.496) <---Interface virtual 2 (conexão do Direct Connect 2) ---> Gateway do cliente (ASN 64.511)
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect . Se você tiver uma conexão hospedada, seu AWS Direct Connect parceiro fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.

Recurso	Informações necessárias
Endereços IP de par	Uma interface virtual pode suportar uma sessão de emparelhamento BGP para IPv4, IPv6, ou uma de cada (pilha dupla). Não use Elastic IPs (EIPs) nem Traga seus próprios endereços IP (BYOIP) do Amazon Pool para criar uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalos de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP. • IPv4: • (Somente interface virtual pública) Você deve especificar IPv4 endereços públicos exclusivos de sua propriedade. **Note** • O peering IPs para interfaces virtuais privadas e de trânsito pode ser de qualquer intervalo de IP válido. Isso também pode incluir endereços IP públicos de propriedade do cliente, desde que sejam usados apenas para criar a sessão de emparelhamento do BGP e não sejam anunciados na interface virtual ou usados para NAT. • Não podemos garantir que seremos capazes de atender a todas as solicitações de IPv4 endereços públicos AWS fornecidos. O valor pode ser um dos seguintes: • Um CIDR de propriedade do cliente IPv4 Elas podem ser públicas IPs (de propriedade do cliente ou fornecidas por ele AWS), mas a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível

Recurso	Informações necessárias
	do AWS roteador. Por exemplo, se você alocar um `/31` intervalo, como`203.0.113.0/31` , você poderia usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível AWS . Ou, se você alocar um `/24` intervalo, como`198.51.100.0/24` , você poderia usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível AWS . • Um intervalo de IP de propriedade do seu AWS Direct Connect parceiro ou ISP, junto com uma autorização LOA-CFA. • E AWS forneceu um CIDR 3/1. Entre em contato com o AWS Support para solicitar um IPv4 CIDR público (e fornecer um caso de uso em sua solicitação) • (Somente interface virtual privada) A Amazon pode gerar IPv4 endereços privados para você. Se você especificar o seu, certifique-se de especificar privado CIDRs para a interface do roteador e somente para a interface do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Semelhante a uma interface virtual pública, a mesma máscara de sub-rede deve ser usada tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do AWS roteador. Por exemplo, se você alocar um `/30` intervalo, como`192.168.0.0/30` , você poderia usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível AWS . • IPv6: A Amazon aloca automaticamente um CIDR IPv6 /125. Você não pode especificar seus próprios IPv6 endereços de pares.
Família de endereços	Se a sessão de emparelhamento do BGP terminará ou. IPv4 IPv6

Recurso	Informações necessárias
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar no intervalo de 1 a 2147483647. A adição de prefixo do Sistema autônomo (AS) não funcionará se você usar um ASN privado para uma interface virtual pública. • AWS ativa MD5 por padrão. Não é possível modificar essa opção. • Uma chave MD5 de autenticação BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	IPv4 Rotas públicas ou IPv6 rotas para anunciar no BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: O IPv4 CIDR pode se sobrepor a outro IPv4 CIDR público anunciado usando Direct Connect quando uma das seguintes afirmações for verdadeira:
	  • Eles CIDRs são de diferentes AWS regiões. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usa AS_PATH quando tem um ASN público em uma configuração. active/passive
	  Para obter mais informações consulte Políticas de roteamento e comunidades do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para. IPv6
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

Recurso	Informações necessárias
(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	A unidade máxima de transmissão (MTU) dos pacotes acima. Direct Connect O padrão é 1500. Definir o MTU de uma interface virtual para 8500 (frames jumbo) pode resultar em uma atualização na conexão física subjacente se ela não tiver sido atualizada para compatibilidade com frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Para o Direct Connect, há compatibilidade com frames jumbo até 8500 MTU. As rotas estáticas e as rotas propagadas configuradas na tabela de rotas do Transit Gateway serão compatíveis com frames jumbo, inclusive de instâncias do EC2 com entradas da tabela de rotas estáticas de VPC no anexo do gateway de trânsito. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Ao criar uma interface virtual, é possível especificar a conta que possui a interface virtual. Quando você escolhe uma AWS conta que não é sua conta, as seguintes regras se aplicam:

- Para uso privado VIFs e de trânsito VIFs, a conta se aplica à interface virtual e ao destino do gateway gateway/Direct Connect privado virtual.
- Para o público VIFs, a conta é usada para cobrança da interface virtual. O uso da transferência de dados para fora (DTO) é medido em relação ao proprietário do recurso na taxa de transferência Direct Connect de dados.

> **Note**
>
> Os prefixos de 31 bits são compatíveis com todos os tipos de interface virtual do Direct Connect. Consulte RFC 3021: Usando prefixos de 31 bits em IPv4 Point-to-Point links para obter mais informações.

MTUs para interfaces virtuais privadas ou interfaces virtuais de trânsito

Direct Connect suporta um tamanho de quadro Ethernet de 1522 ou 9023 bytes (cabeçalho Ethernet de 14 bytes + tag VLAN de 4 bytes + bytes para o datagrama IP + 4 bytes FCS) na camada de link.

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. A MTU de uma interface virtual privada pode ser 1500 ou 9001 (frames jumbo). A MTU de uma interface virtual privada pode ser 1500 ou 8500 (frames jumbo). Você pode especificar a MTU ao criar a interface ou atualizá-la depois que criá-la. Definir a MTU de uma interface virtual para 8500 (frames jumbo) ou 9001 (frames jumbo) pode resultar em uma atualização da conexão física subjacente se ela não foi atualizada para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no Direct Connect console e encontre Jumbo Frame Capable na guia Resumo.

Após ter habilitado os frames jumbo para sua interface virtual privada ou interface virtual de trânsito, você só poderá associá-la a uma conexão ou LAG que seja compatível com frames jumbo. Os frames jumbo são compatíveis com uma interface virtual privada anexada a um gateway virtual privado ou um gateway do Direct Connect, ou com uma interface virtual de trânsito anexada a um gateway do Direct Connect. Se você tiver duas interfaces virtuais privadas que anunciam a mesma rota, mas usam valores de MTU diferentes, ou se você tem uma Site-to-Site VPN que anuncia a mesma rota, 1500 MTU são usadas.

Important

Os quadros jumbo se aplicarão somente a rotas propagadas via Direct Connect e rotas estáticas por meio de gateways de trânsito. Os frames jumbo em gateways de trânsito são compatíveis apenas com 8.500 bytes.

Se uma instância do EC2 não for compatível com frames jumbo, ela descartará os frames jumbo do Direct Connect. Todos os tipos de instância do EC2 oferecem suporte a quadros jumbo, exceto C1 CC1, T1 e M1. Para obter mais informações, consulte Unidade de transmissão máxima (MTU) de rede para a instância do EC2 no Guia do usuário do Amazon EC2.

Para conexões hospedadas, só é possível habilitar os frames jumbo se eles tiverem sido originalmente habilitados na conexão principal hospedada do Direct Connect. Se os frames

jumbo não estiverem habilitados nessa conexão principal, não será possível habilitá-los em nenhuma conexão.

Para obter as etapas necessárias para definir a MTU para uma interface virtual privada, consulte Definição da MTU de uma interface virtual privada.

Interfaces virtuais do Direct Connect

Você pode criar uma interface virtual de trânsito para se conectar a um gateway de trânsito, uma interface virtual pública para se conectar a recursos públicos (serviços não VPC) ou uma interface virtual privada para se conectar a uma VPC.

Para criar uma interface virtual para contas em seu AWS Organizations ou em um AWS Organizations diferente do seu, crie uma interface virtual hospedada.

Confira a seguir como criar uma interface virtual:

- Criar uma interface virtual pública
- Criar uma interface virtual privada
- Criar uma interface virtual de trânsito para o gateway do Direct Connect

Pré-requisitos

Antes de começar, verifique se você leu as informações em Pré-requisitos para interfaces virtuais.

Pré-requisitos para interfaces virtuais de trânsito para um gateway do Direct Connect

Para conectar sua conexão do Direct Connect com o gateway de trânsito, você deve criar uma interface de trânsito para a conexão. Especifique o gateway Direct Connect ao qual se conectar.

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. A MTU de uma interface virtual privada pode ser 1500 ou 9001 (frames jumbo). A MTU de uma interface virtual privada pode ser 1500 ou 8500 (frames jumbo). Você pode especificar a MTU ao criar a interface ou atualizá-la depois que criá-la. Definir a MTU de uma interface virtual para 8500 (frames jumbo) ou 9001 (frames jumbo)

pode resultar em uma atualização da conexão física subjacente se ela não foi atualizada para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Para verificar se uma conexão ou interface virtual oferece suporte a frames jumbo, selecione-a no console do Direct Connect e localize Jumbo Frame Capable (Com capacidade de frames jumbo) na guia Summary (Resumo).

> **Important**
>
> Se você associar seu gateway de trânsito a um ou mais gateways do Direct Connect, o número de sistema autônomo (ASN) usado pelo gateway de trânsito e pelo gateway do Direct Connect devem ser diferentes. Por exemplo, a solicitação de associação falhará se você usar o ASN 64512 padrão para o gateway de trânsito e o gateway do Direct Connect.

Criação de uma interface virtual pública do Direct Connect

Quando você cria uma interface virtual pública, pode demorar até 72 horas úteis para que possamos revisar e aprovar sua solicitação.

Para provisionar uma interface virtual pública

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public virtual interface settings (Configurações de interface virtual pública), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.
   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.
   c. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).
   d. Em ASN do BGP insira o número de sistema autônomo (ASN) do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Inclui suporte para ASNs (1-2147483647) e ASNs longos (1-4294967294). Para obter mais informações sobre ASNs e ASNs longos, consulte Suporte longo de ASN em Direct Connect.

> **Note**
>
> Quando for estabelecer uma sessão de emparelhamento do BGP com a AWS por uma interface virtual pública, use 7224 como ASN para estabelecer a sessão do BGP pela AWS. O ASN em seu roteador ou dispositivo de gateway do cliente deve ser diferente desse ASN.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um par BGP IPv4 ou IPv6, faça o seguinte:

      [IPv4] Para configurar um par BGP IPv4, escolha IPv4 e siga um destes procedimentos:

      - Para especificar esses endereços IP por conta própria, em Your router peer ip (Seu IP de par do roteador), insira o endereço de destino CIDR IPv4 para o qual a Amazon deve enviar tráfego.
      - Em Amazon router peer IP (IP de par do roteador da Amazon), insira o endereço CIDR IPv4 a ser usado para enviar tráfego à AWS.

      [IPv6] Para configurar um par BGP IPv6, selecione IPv6. Os endereços IPv6 de mesmo nível são atribuídos automaticamente com base no pool de endereços IPv6 da Amazon. Não é possível especificar endereços IPv6 personalizados.

   b. Para fornecer sua própria chave BGP, insira sua chave MD5 BGP.

      Se você não inserir um valor, geraremos uma chave BGP. Se você tiver fornecido sua própria chave ou se tivermos gerado a chave para você, esse valor será exibido na coluna Chave de autenticação do BGP na página de detalhes de interface virtual de Interfaces virtuais.

   c. Para anunciar prefixos na Amazon, em Prefixes you want to advertise (Prefixos que deseja anunciar), insira os endereços de destino CIDR IPv4 (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.

      > **Important**
      >
      > Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).
8. Faça download da configuração do roteador para o dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual pública usando a linha de comando ou a API

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface (API do Direct Connect)

Criação de uma interface privada virtual do Direct Connect

Você pode provisionar uma interface virtual privada para um gateway privado virtual na mesma região que sua conexão do Direct Connect. Para obter mais informações sobre o provisionamento de uma interface virtual privada para um gateway Direct Connect, consulte Gateways do Direct Connect.

Caso use o assistente de VPC para criar uma VPC, a propagação de rotas é habilitada automaticamente para você. Com a propagação da rota, as rotas são preenchidas automaticamente para as tabelas de rotas na VPC. Você pode desabilitar a propagação de rota, caso opte por isso. Para obter mais informações, consulte Habilitar a propagação de rota em sua tabela de rotas no Guia do usuário da Amazon VPC.

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. A MTU de uma interface virtual privada pode ser 1500 ou 9001 (frames jumbo). A MTU de uma interface virtual privada pode ser 1500 ou 8500 (frames jumbo). Você pode especificar a MTU ao criar a interface ou atualizá-la depois que criá-la. Definir a MTU de uma interface virtual para 8500 (frames jumbo) ou 9001 (frames jumbo) pode resultar em uma atualização da conexão física subjacente se ela não foi atualizada para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Para verificar se uma conexão ou

interface virtual oferece suporte a frames jumbo, selecione-a no console do Direct Connect e localize Jumbo Frame Capable (Com capacidade de frames jumbo) na guia Summary (Resumo).

Para provisionar uma interface virtual privada para uma VPC

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, escolha Privado.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em Proprietário da interface virtual, escolha Minha conta da AWS caso a interface virtual seja para sua conta da AWS.

   d. Em Direct Connect gateway (Gateway Direct Connect), selecione o gateway Direct Connect.

   e. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   f. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Inclui suporte para ASNs (1-2147483647) e ASNs longos (1-4294967294). Para obter mais informações sobre ASNs e ASNs longos, consulte Suporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um par BGP IPv4 ou IPv6, faça o seguinte:

      [IPv4] Para configurar um par BGP IPv4, escolha IPv4 e siga um destes procedimentos:

      - Para especificar esses endereços IP por conta própria, em Your router peer ip (Seu IP de par do roteador), insira o endereço de destino CIDR IPv4 para o qual a Amazon deve enviar tráfego.
      - Em IP de par do roteador da Amazon, insira o endereço CIDR IPv4 a ser usado no envio de tráfego para a AWS.

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando a RFC 1918, usar outros esquemas de endereçamento ou optar pelos endereços CIDR IPv4 /29 atribuídos pela AWS, alocados do intervalo IPv4 Link-Local da RFC 3927 169.254.0.0/16 para conectividade ponto a ponto. Essas conexões ponto a ponto devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como a AWS Site-to-Site Private IP VPN ou Transit Gateway Connect, a AWS recomenda usar uma interface de loopback ou LAN no roteador gateway do cliente como endereço de origem ou destino, em vez de conexões ponto a ponto.
>
> - Para obter mais informações sobre o RFC 1918, consulte Alocação de endereços para Internet privada.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços de local de link IPv4.

[IPv6] Para configurar um par BGP IPv6, selecione IPv6. Os endereços IPv6 de mesmo nível são atribuídos automaticamente com base no pool de endereços IPv6 da Amazon. Não é possível especificar endereços IPv6 personalizados.

b. Para alterar a unidade de transmissão máxima (MTU) de 1500 (padrão) para 8500 (frames jumbo), selecione Jumbo MTU (MTU size 8500) (MTU jumbo (tamanho da MTU 8500)).

c. (Opcional) Em Habilitar o SiteLink, escolha Habilitado para habilitar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).
8. Faça download da configuração do roteador para o dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual privada usando a linha de comando ou a API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (API do Direct Connect)

Crie uma interface virtual de trânsito para o Direct Connect gateway

Antes de estabelecer a conexão entre uma interface virtual de trânsito e o gateway do Direct Connect, familiarize-se com o conteúdo do texto.

Como provisionar uma interface virtual de trânsito para um gateway Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), em Type (Tipo), selecione Transit (Trânsito).
5. Em Private virtual interface settings (Configurações de interface virtual privada), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Para Proprietário da interface virtual, escolha Minha AWS conta se a interface virtual for para sua AWS conta.

   d. Em Direct Connect gateway (Gateway Direct Connect), selecione o gateway Direct Connect.

   e. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   f. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

- Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
- Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
>
> - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade de transmissão máxima (MTU) de 1500 (padrão) para 8500 (frames jumbo), selecione Jumbo MTU (MTU size 8500) (MTU jumbo (tamanho da MTU 8500)).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Depois que tiver criado a interface virtual, você poderá fazer download da configuração do roteador no dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual de trânsito usando a linha de comando ou a API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(Direct Connect API)

Como visualizar as interfaces virtuais que estão anexadas a um gateway Direct Connect usando a linha de comando ou a API

- describe-direct-connect-gateway-anexos ()AWS CLI
- DescribeDirectConnectGatewayAttachments(Direct Connect API)

Download do arquivo de configuração do roteador do Direct Connect

Depois que tiver criado a interface virtual e o estado da interface estiver ativo, você poderá fazer download do arquivo de configuração do roteador para o roteador.

Se você usar qualquer um dos roteadores a seguir para interfaces virtuais com o MACsec ativado, criaremos automaticamente o arquivo de configuração para seu roteador:

- Switches Cisco Nexus 9K+ Series executando software NX-OS 9.3 ou posterior
- Roteadores Juniper Networks M/MX Series executando o software JunOS 9.5 ou posterior

Para fazer o download do arquivo de configuração do roteador

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).
4. Selecione Download router configuration (Fazer download da configuração do roteador).

5. Em Download router configuration (Fazer download da configuração do roteador), faça o seguinte:

   a. Em Fornecedor, selecione o fabricante do roteador.

   b. Em Plataforma, selecione o modelo do roteador.

   c. Em Software, selecione a versão do software do roteador.

6. Escolha Download e use a configuração apropriada para o roteador a fim de garantir que você consiga se conectar ao Direct Connect.

7. Use a tabela a seguir como diretriz caso precise configurar manualmente seu roteador para MACsec.

Parameter	Descrição
Comprimento do CKN	Uma string de 64 caracteres hexadecimais (0-9, A-E). Use o comprimento total para maximizar a compatibilidade entre plataformas.
Comprimento do CAK	Uma string de 64 caracteres hexadecimais (0-9, A-E). Use o comprimento total para maximizar a compatibilidade entre plataformas.
Algoritmo criptográfico	AES_256_CMAC
Pacote de criptografia SAK	• Para conexões de 100 Gbps: GCM_AES_XPN_256 • Para conexões de 10 Gbps: GCM_AES_XPN_256 ou GCM_AES_256
Pacote de criptografia de chave	16
Deslocamento de confidencialidade	0
Indicador ICV	Não

Parameter	Descrição
Tempo de rechaveamento do SAK	PN Rollover>

Interfaces virtuais hospedadas do Direct Connect

Para usar a conexão do Direct Connect com outra conta, você pode criar uma interface virtual hospedada para essa conta. O proprietário da outra conta deve aceitar a interface virtual hospedada para começar a usá-la. Uma interface virtual hospedada funciona como uma interface virtual padrão e pode se conectar a recursos públicos ou a uma VPC.

É possível usar interfaces virtuais de trânsito com conexões dedicadas ou hospedadas do Direct Connect de qualquer velocidade. Conexões hospedadas só são compatíveis com uma interface virtual.

Para criar uma interface virtual, você precisa das seguintes informações:

Recurso	Informações necessárias
Conexão	A conexão ou o grupo de agregação de link (LAG) do Direct Connect para o qual você está criando a interface virtual.
Nome da interface virtual	Um nome para a interface virtual.
Proprietário da interface virtual	Se estiver criando a interface virtual para outra conta, você precisará do ID de conta da AWS da outra conta.
(Somente interface virtual privada) Conexão	Para se conectar a uma VPC na mesma região da AWS, você precisa do gateway privado virtual para sua VPC. O ASN para o lado da Amazon da sessão BGP é herdado do gateway privado virtual. Ao criar um gateway privado virtual, você pode especificar seu próprio ASN privado. Caso contrário , a Amazon fornece um ASN padrão. Para obter mais informações, consulte Criar um gateway privado virtual no Guia do usuário da Amazon VPC. Para se conectar a uma VPC por meio de um gateway do Direct Connect, você

Recurso	Informações necessárias
	precisa do gateway do Direct Connect. Para obter mais informações, consulte Gateways Direct Connect.
VLAN	Uma tag exclusiva de rede de área local virtual (VLAN) que ainda não esteja em uso em sua conexão. O valor precisa estar entre 1 e 4.094 e estar em conformidade com o padrão Ethernet 802.1Q. Esta tag é obrigatória para qualquer tráfego que cruza a conexão do Direct Connect. Se você tiver uma conexão hospedada, seu parceiro do AWS Direct Connect fornecerá esse valor. Não é possível modificar o valor após a criação da interface virtual.

Recurso	Informações necessárias

Endereços IP de par	Uma interface virtual pode dar suporte a uma sessão de emparelhamento do BGP para IPv4, IPv6 ou um de cada (pilha dupla). Não use endereços IPs elásticos (EIPs) ou endereços no formato traga seu próprio IP (BYOIP) do grupo da Amazon para criar uma interface virtual pública. Você não pode criar várias sessões BGP para a mesma família de endereços IP na mesma interface virtual. Os intervalos de endereços IP são atribuídos a cada extremidade da interface virtual da sessão de emparelhamento do BGP.
	
	• IPv4:
	  • (Somente interface virtual pública) você precisa especificar endereços IPv4 públicos exclusivos e de sua propriedade. O valor pode ser um dos seguintes:
	  • Um CIDR IPv4 de propriedade do cliente
	
	Isso pode ser qualquer IP público (de propriedade do cliente ou fornecido pela AWS), mas sendo necessário usar a mesma máscara de sub-rede tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do roteador da AWS. Por exemplo, se você alocar um intervalo `/31`, como `203.0.113.0/31` , você poderá usar `203.0.113.0` para seu IP de mesmo nível e `203.0.113.1` para o IP de mesmo nível da AWS. Como alternativa, se você alocar um intervalo `/24`, como `198.51.100.0/24` , você poderá usar `198.51.100.10` para seu IP de mesmo nível e `198.51.100.20` para o IP de mesmo nível da AWS.
	  • Um intervalo de IP de propriedade do seu parceiro do AWS Direct Connect ou provedor de Internet, junto com uma autorização LOA-CFA
	  • Um CIDR /31 fornecido pela AWS. Entre em contato com o AWS Support para solicitar um CIDR IPv4 público (e informe um caso de uso na solicitação)

Recurso	Informações necessárias
	> **Note** > Não podemos garantir que seremos capazes de atender a todas as solicitações de endereços IPv4 públicos fornecidos pela AWS. • (Somente interface virtual privada) A Amazon pode gerar endereços IPv4 privados para você. Se você especificar seus próprios endereços, não se esqueça de especificar CIDRs privados para a interface do roteador e somente para a interface do AWS Direct Connect. Por exemplo, não especifique outros endereços IP da sua rede local. Assim como em uma interface virtual pública, é necessário usar a mesma máscara de sub-rede tanto para seu IP de mesmo nível quanto para o IP de mesmo nível do roteador da AWS. Por exemplo, se você alocar um intervalo `/30`, como `192.168.0.0/30` , você poderá usar `192.168.0.1` para seu IP de mesmo nível e `192.168.0.2` para o IP de mesmo nível da AWS. • IPv6: a Amazon aloca automaticamente um CIDR IPv6 /125 para você. Você não pode especificar os próprios endereços IPv6 de mesmo nível.
Família de endereços	Indica se a sessão de emparelhamento do BGP acontecerá por IPv4 ou IPv6.
Informações sobre o BGP	• Um número de sistema autônomo (ASN) público ou privado de Protocolo de Gateway da Borda (BGP) para a sua extremidade da sessão do BGP. Caso esteja usando um ASN público, você precisa ser o proprietário dele. Se você estiver usando um ASN privado, poderá definir um valor de ASN personalizado. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar no intervalo de 1 a 4294967294. A adição de prefixo do Sistema autônomo (AS) não funcionará se você usar um ASN privado para uma interface virtual pública. • A AWS habilita o MD5 por padrão. Não é possível modificar essa opção. • Uma chave de autenticação MD5 do BGP. Você pode fornecer sua própria chave ou permitir que a Amazon gere uma para você.

Recurso	Informações necessárias

(Somente interface virtual pública) Prefixos que você deseja anunciar	Rotas IPv4 ou rotas IPv6 públicas para anunciar pelo BGP. Você deve anunciar pelo menos um prefixo usando BGP, até um máximo de 1.000 prefixos.
	• IPv4: poderá haver sobreposição do CIDR IPv4 a outro CIDR IPv4 público anunciado usando o Direct Connect quando uma das seguintes situações for verdadeira:
	  • Os CIDRs forem de diferentes regiões da AWS. Não se esqueça de aplicar as tags de comunidade do BGP nos prefixos públicos.
	  • Você usar AS_PATH quando tiver um ASN público em uma configuração ativa/passiva.
	  Para obter mais informações consulte Políticas de roteamento e comunidades do BGP.
	• Em uma interface virtual pública do Direct Connect, você pode especificar qualquer tamanho de prefixo de /1 a /32 para IPv4 e de /1 a /64 para IPv6.
	• Entrando em contato com o AWS Support, você poderá acrescentar prefixos adicionais a um VIF público existente e anunciá-los. Em seu caso de suporte, forneça uma lista de prefixos CIDR adicionais que você deseja adicionar ao VIF público e anunciar.

(Somente interfaces privadas e interfaces virtuais de trânsito) Frames jumbo	Unidade de transmissão máxima (MTU) de pacotes pelo Direct Connect. O padrão é 1500. Definir o MTU de uma interface virtual para 9001 (frames jumbo) pode resultar em uma atualização para a conexão física subjacente se ele não foi atualizado para oferecer suporte a frames jumbo. Atualizar a conexão interrompe a conectividade de rede para todas as interfaces virtuais associadas à conexão por até 30 segundos. Os frames jumbo se aplicam somente a rotas propagadas do Direct Connect. Se você adicionar rotas estáticas a uma tabela de rotas que aponte para seu gateway privado virtual, o tráfego roteado pelas rotas estáticas será enviado usando 1.500 MTU. Para verificar se uma conexão ou interface virtual é compatível com frames jumbo, selecione-a no console do Direct Connect e localize Com capacidade de frames jumbo na guia Resumo.

Crie uma interface virtual privada hospedada no Direct Connect

Antes de começar, verifique se você leu as informações em Pré-requisitos para interfaces virtuais.

Para criar uma interface virtual privada hospedada

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, para Tipo, escolha Pública.
5. Em Configurações de interface virtual pública, faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em Proprietário da interface virtual, escolha Outra conta da AWS e, em seguida, em Proprietário da interface virtual, insira o ID da conta que será proprietária dessa interface virtual.

   d. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   e. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador de gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
>
> - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade de transmissão máxima (MTU) de 1500 (padrão) para 8500 (frames jumbo), selecione Jumbo MTU (MTU size 8500) (MTU jumbo (tamanho da MTU 8500)).

c. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Após a interface virtual hospedada ser aceita pelo proprietário da outra conta da AWS , você poderá fazer o download do arquivo de configuração. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual privada hospedada usando a linha de comando ou a API

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(Direct Connect API)

Crie uma interface virtual pública hospedada no Direct Connect

Antes de começar, verifique se você leu as informações em Pré-requisitos para interfaces virtuais.

Para criar uma interface virtual pública hospedada

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), para Type (Tipo), escolha Public (Pública).
5. Em Public Virtual Interface Settings (Configurações de interface virtual pública), faça o seguinte:

   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.

   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

   c. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, em Proprietário da interface virtual, insira o ID da conta que possui essa interface virtual.

   d. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

   e. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.

6. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

   [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

   - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.

- Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

  [IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

7. Para anunciar prefixos na Amazon, para prefixos que você deseja anunciar, insira os endereços de destino IPv4 CIDR (separados por vírgulas) para os quais o tráfego deve ser roteado pela interface virtual.
8. Para fornecer sua própria chave para autenticar a sessão do BGP, em Additional Settings (Configurações adicionais), para BGP authentication key (Chave de autenticação do BGP), digite a chave.

   Se você não inserir um valor, geraremos uma chave BGP.
9. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).
10. Selecione Create virtual interface (Criar interface virtual).
11. Após a interface virtual hospedada ser aceita pelo proprietário da outra conta da AWS , você poderá fazer o download do arquivo de configuração. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual pública hospedada usando a linha de comando ou a API

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(Direct Connect API)

Crie uma interface virtual de trânsito Direct Connect hospedado

Para criar uma interface virtual de trânsito hospedada

> **Important**
>
> Se você associar seu gateway de trânsito a um ou mais gateways do Direct Connect, o número de sistema autônomo (ASN) usado pelo gateway de trânsito e pelo gateway do Direct Connect devem ser diferentes. Por exemplo, a solicitação de associação falhará se você usar o ASN 64512 padrão para o gateway de trânsito e o gateway do Direct Connect.

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), em Type (Tipo), selecione Transit (Trânsito).
5. Em Private virtual interface settings (Configurações de interface virtual privada), faça o seguinte:
   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.
   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.
   c. Em Proprietário da interface virtual, escolha Outra AWS conta e, em seguida, em Proprietário da interface virtual, insira o ID da conta que possui essa interface virtual.
   d. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).
   e. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

      Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.
6. Em Additional settings (Configurações adicionais), faça o seguinte:
   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

- Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
- Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
>
> - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade de transmissão máxima (MTU) de 1500 (padrão) para 8500 (frames jumbo), selecione Jumbo MTU (MTU size 8500) (MTU jumbo (tamanho da MTU 8500)).

c. [Opcional] Adicione uma tag. Faça o seguinte:

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

8. Após a interface virtual hospedada ser aceita pelo proprietário da outra conta da AWS , você poderá fazer o download do arquivo de configuração do roteador para o seu dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual de trânsito hospedada usando a linha de comando ou a API

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(Direct Connect API)

Visualização de detalhes da interface virtual do Direct Connect

É possível visualizar o status atual da interface virtual usando o console do Direct Connect ou a linha de comando ou a API. Os detalhes incluem:

- Estado da conexão
- Name
- Local
- VLAN
- Detalhes de BGP
- Endereços IP de par

Para visualizar detalhes sobre uma interface virtual

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel à esquerda, selecione Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).

Para descrever interfaces virtuais usando a linha de comando ou a API

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces (API do Direct Connect)

Adição de um par do BGP a uma interface virtual do Direct Connect

Adicione ou exclua uma sessão de emparelhamento do BGP para IPv4 ou IPv6 à interface virtual usando o console do Direct Connect ou a linha de comando ou a API.

Uma interface virtual pode dar suporte a uma única sessão de mesmo nível BGP IPv4 e uma única sessão de mesmo nível BGP IPv6. Você não pode especificar os próprios endereços IPv6 de mesmo nível para uma sessão de mesmo nível BGP IPv6. A Amazon aloca automaticamente para você um CIDR IPv6 /125.

Não há compatibilidade com BGP multiprotocolo. IPv4 e IPv6 funcionam em modo de pilha dupla para interface virtual.

A AWS habilita o MD5 por padrão. Não é possível modificar essa opção.

Use o procedimento a seguir para adicionar um par BGP.

Para adicionar um BGP de mesmo nível

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).
4. Escolha Add peering (Adicionar emparelhamento).
5. (Interface virtual privada) Para adicionar BGPs IPv4 de mesmo nível, faça o seguinte:
   - Escolha IPv4.
   - Para especificar esses endereços IP por conta própria, em Your router peer ip (Seu IP de par do roteador), insira o endereço de destino CIDR IPv4 para o qual a Amazon deve enviar tráfego. Em IP de par do roteador da Amazon, insira o endereço CIDR IPv4 a ser usado no envio de tráfego para a AWS.
6. (Interface virtual pública) Para adicionar BGPs IPv4 de mesmo nível, faça o seguinte:
   - Em Your router peer ip (Seu IP de par do roteador), insira o endereço de destino CIDR IPv4 para o qual o tráfego deve ser enviado.
   - Em Amazon router peer IP (IP de par do roteador da Amazon), insira o endereço CIDR IPv4 a ser usado para enviar tráfego à AWS.

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando a RFC 1918, usar outros esquemas de endereçamento ou optar pelos endereços CIDR IPv4 /29 atribuídos pela AWS, alocados do intervalo IPv4 Link-Local da RFC 3927 169.254.0.0/16 para conectividade ponto a ponto. Essas conexões ponto a ponto devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como a AWS Site-to-Site Private IP VPN ou Transit Gateway Connect, a AWS recomenda usar uma interface de loopback ou LAN no roteador gateway do cliente como endereço de origem ou destino, em vez de conexões ponto a ponto.
>
> - Para obter mais informações sobre o RFC 1918, consulte Alocação de endereços para Internet privada.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços de local de link IPv4.

7. (Interface virtual privada ou pública) Para adicionar pares BGP IPv6, escolha IPv6. Os endereços IPv6 de mesmo nível são atribuídos automaticamente pelo grupo de endereços IPv6 da Amazon. Você não pode especificar endereços IPv6 personalizados.
8. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Para obter uma interface virtual pública, o ASN deve ser privado ou já estar na lista de permissões da interface virtual.

   Os valores válidos são de 1 a 4294967294. Inclui suporte para ASNs (1-2147483646) e ASNs longos (1-4294967294). Para obter mais informações sobre ASNs e ASNs longos, consulte Suporte longo de ASN em Direct Connect.

   Observe que atribuiremos um valor automaticamente se você não inserir um valor.
9. Para fornecer sua própria chave BGP, em BGP Authentication Key (Chave de autenticação BGP), insira sua chave MD5 BGP.
10. Escolha Add peering (Adicionar emparelhamento).

Para criar um BGP de mesmo nível usando a linha de comando ou a API

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (API do Direct Connect)

Exclusão de um par do BGP da interface virtual do Direct Connect

Caso a interface virtual tenha uma sessão de mesmo nível BGP IPv4 e IPv6, você pode excluir uma das sessões de mesmo nível BGP (mas não ambas). É possível excluir um par do BGP de uma interface virtual usando o console do Direct Connect ou a linha de comando ou a API.

Para excluir um BGP de mesmo nível

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).
4. Em Peerings (Emparelhamentos), selecione o emparelhamento que deseja excluir e escolha Delete (Excluir).
5. Na caixa de diálogo Remove peering from virtual interface (Remover emparelhamento da interface virtual), escolha Delete (Excluir).

Para excluir um BGP de mesmo nível usando a linha de comando ou a API

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (API do Direct Connect)

Definir a MTU de uma interface virtual Direct Connect privada

Se sua interface virtual tiver uma sessão de emparelhamento IPv6 BGP IPv4 e uma sessão de emparelhamento de BGP, você poderá excluir uma das sessões de emparelhamento de BGP (mas não ambas). Para obter mais informações sobre MTUs interfaces virtuais privadas, consulte MTUs para interfaces virtuais privadas ou interfaces virtuais de trânsito.

Você pode definir a MTU de uma interface virtual privada usando o Direct Connect console ou usando a linha de comando ou a API.

Para definir a MTU de uma interface virtual privada

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha Edit (Editar).
4. Em MTU jumbo (tamanho da MTU 8500), selecione Ativado.
5. Em Acknowledge (Confirmar), selecione I understand the selected connection(s) will go down for a brief period (Entendo que as conexões selecionadas serão desativadas por um breve período de tempo). O estado da interface virtual é `pending` até que a atualização seja concluída.

Para definir a MTU de uma interface virtual privada usando a linha de comando ou a API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(Direct Connect API)

Adição ou remoção de etiquetas da interface virtual do Direct Connect

As tags fornecem uma maneira de identificar a interface virtual. É possível adicionar ou remover uma etiqueta usando o console do Direct Connect ou a linha de comando ou da API, caso você seja o proprietário da conta da interface virtual.

Para adicionar ou remover uma tag da interface virtual

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha Edit (Editar).
4. Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).
5. Escolha Edit virtual interface (Editar interface virtual).

Para adicionar ou remover tags usando a linha de comando

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Exclusão de uma interface virtual do Direct Connect

Exclua uma ou mais interfaces virtuais. Para excluir uma conexão, você deve excluir a interface virtual. A exclusão de uma interface virtual interrompe cobranças de transferência de dados do Direct Connect associados à interface virtual.

É possível excluir uma interface virtual usando o console do Direct Connect ou a linha de comando ou a API.

Para excluir uma interface virtual

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel à esquerda, selecione Virtual Interfaces (Interfaces virtuais).
3. Selecione as interfaces virtuais e escolha Delete (Excluir).
4. Na caixa de diálogo de confirmação Delete (Excluir), escolha Delete (Excluir).

Para excluir uma interface virtual usando a linha de comando ou a API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface (API do Direct Connect)

Aceite uma interface Direct Connect virtual hospedada

Para usar uma interface virtual hospedada, você deve aceitar a interface virtual. Para uma interface virtual privada, também é necessário ter um gateway privado virtual ou um gateway Direct Connect. Para obter uma interface virtual de trânsito, você deve ter um gateway de trânsito existente ou um gateway Direct Connect.

Você pode aceitar uma interface virtual hospedada usando o Direct Connect console, a linha de comando ou a API.

Para aceitar uma interface virtual hospedada

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha View details (Visualizar detalhes).
4. Escolha Accept (Aceitar).
5. Isso se aplica a interfaces virtuais privadas e a interfaces virtuais de trânsito.

   (Interface virtual de trânsito) Na caixa de diálogo Accept virtual interface (Aceitar interface virtual), escolha um gateway Direct Connect e selecione Accept virtual interface (Aceitar interface virtual).

   (Interface virtual privada) Na caixa de diálogo Accept virtual interface (Aceitar interface virtual), escolha um gateway privado virtual ou um gateway Direct Connect e selecione Accept virtual interface (Aceitar interface virtual).
6. Depois que aceitar a interface virtual hospedada, o proprietário da conexão do Direct Connect poderá fazer download do arquivo de configuração do roteador. A opção Download router configuration (Fazer download de configuração do roteador) não está disponível para a conta que aceita a interface virtual hospedada.

Para aceitar uma interface virtual privada hospedada usando a linha de comando ou a API

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(Direct Connect API)

Para aceitar uma interface virtual pública hospedada usando a linha de comando ou a API

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(Direct Connect API)

Para aceitar uma interface virtual de trânsito hospedada usando a linha de comando ou a API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(Direct Connect API)

Migração de uma interface virtual do Direct Connect

Utilize este procedimento quando quiser realizar qualquer uma das seguintes operações de migração de interface virtual:

- Migrar uma interface virtual existente associada a uma conexão para outro LAG.
- Migrar uma interface virtual existente associada a um LAG existente para um novo LAG.
- Migrar uma interface virtual existente associada a uma conexão para outra conexão.

> **Note**
>
> - É possível migrar uma interface virtual para uma nova conexão na mesma região, mas não é possível migrá-la de uma região para outra. Ao migrar ou associar uma interface virtual existente a uma nova conexão, os parâmetros de configuração associados a essas interfaces virtuais serão os mesmos. Para contornar isso, você pode preparar a configuração na conexão e, em seguida, atualizar a configuração do BGP.
> - Você não pode migrar uma VIF de uma conexão hospedada para outra. As IDs de VLAN são exclusivas. Portanto, migrar uma VIF dessa forma faria com que as VLANs não correspondam. Você precisa excluir a conexão ou a VIF e então recriá-la usando uma VLAN que seja a mesma para a conexão e a VIF.

> **Important**
>
> A interface virtual ficará inativa por um breve período. Recomendamos que você execute esse procedimento durante uma janela de manutenção.

Como migrar uma interface virtual

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione a interface virtual e escolha Editar.
4. Para Conexão, selecione o LAG ou a conexão.
5. Escolha Edit virtual interface (Editar interface virtual).

Como migrar uma interface virtual usando a linha de comando ou a API

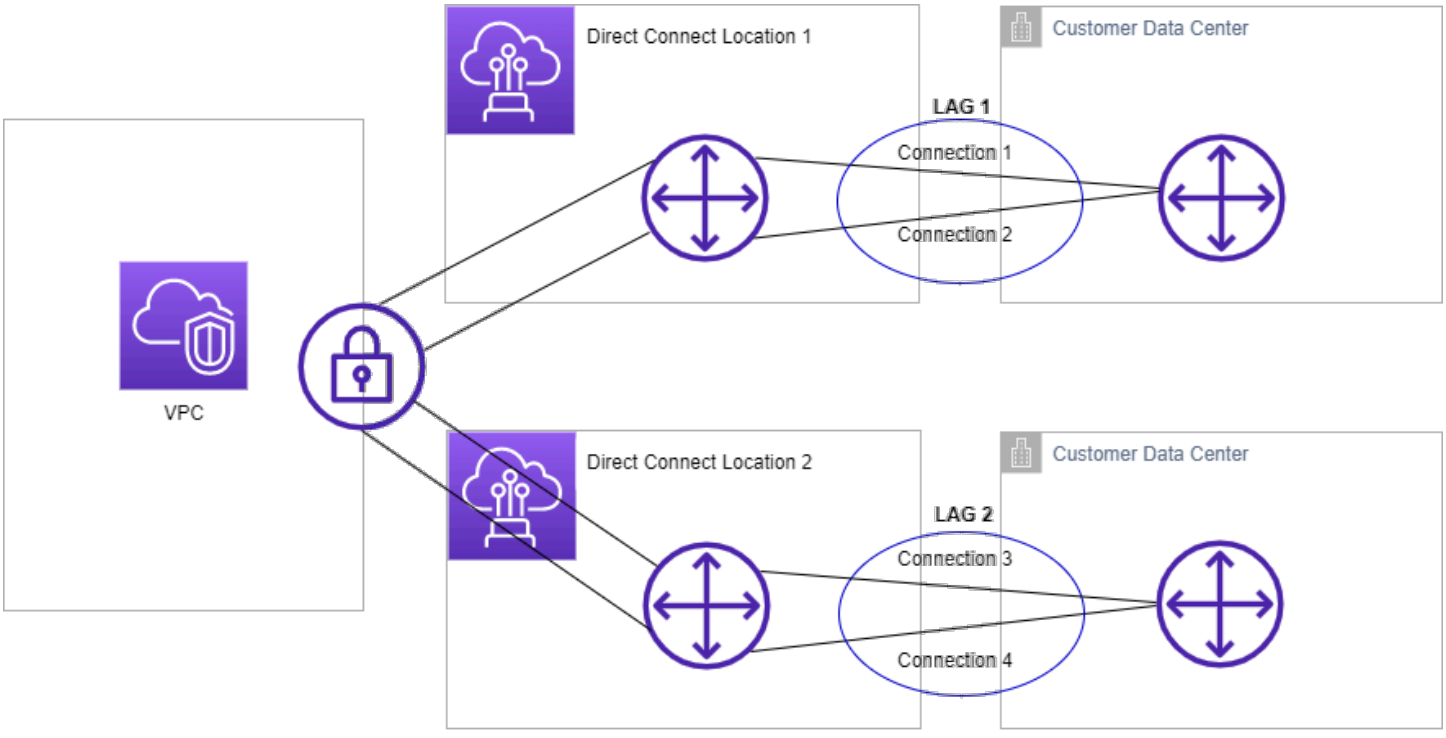
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (API do Direct Connect)

Grupos de agregação de links (LAGs) do Direct Connect

Você pode usar várias conexões para aumentar a largura de banda disponível. LAG é uma interface lógica que usa o protocolo Link Aggregation Control Protocol (LACP) para agregar várias conexões a um único endpoint do Direct Connect, o que permite tratá-las como uma única conexão gerenciada. Os LAGs simplificam a configuração porque a configuração do LAG se aplica a todas as conexões no grupo.

> **Note**
>
> O AWS não é compatível com LAG de vários chassis (MLAG).

No diagrama a seguir, você tem quatro conexões, com duas conexões para cada local. É possível criar um LAG para as conexões que são encerradas no mesmo dispositivo da AWS e na mesma localização e, em seguida, usar os dois LAGs em vez das quatro conexões para realizar a configuração e o gerenciamento.



Você pode criar um LAG com base em conexões existentes ou provisionar conexões novas. Depois que tiver criado o LAG, você poderá associar conexões existentes (independentes ou parte de outro LAG) ao LAG.

As seguintes regras se aplicam:

- Todas as conexões devem ser dedicadas e ter uma velocidade de porta de 1 Gbps, 10 Gbps, 100 Gbps ou 400 Gbps.
- Todas as conexões no LAG devem usar a mesma largura de banda.
- É possível ter, no máximo, duas conexões de 100 Gbps ou de 400 Gbps, ou quatro conexões com uma velocidade de porta menor que 100 Gbps em um LAG. Cada conexão no LAG é contabilizada no limite geral de conexões para a Região.
- Todas as conexões no LAG devem ser encerradas no mesmo endpoint do Direct Connect.
- Os LAGs são compatíveis com todos os tipos de interface virtual: pública, privada e de trânsito.

Ao criar um LAG, é possível fazer o download da carta de autorização e atribuição de instalação de conexão (LoA-CFA) para uma nova conexão física individualmente ao usar o console do Direct Connect. Para obter mais informações, consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA).

Todos os LAGs têm um atributo que determina o número mínimo de conexões no LAG que deve estar funcionando para o LAG propriamente dito estar operacional. Por padrão, novos LAGs têm esse atributo definido como 0. Você pode atualizar o LAG para especificar um valor diferente. Isso significa que todo o LAG ficará inoperante caso o número de conexões operacionais fique abaixo desse limite. Este atributo pode ser usado para evitar a utilização em excesso das conexões restantes.

Todas as conexões em um LAG funcionam em modo ativo/ativo.

> **Note**
>
> Quando você cria um LAG ou associa mais conexões ao LAG, não podemos garantir portas disponíveis o suficiente em um determinado endpoint do Direct Connect.

Tópicos

- Considerações sobre o protocolo MACsec para o Direct Connect
- Criação de um LAG em um endpoint do Direct Connect
- Veja os detalhes do LAG em um endpoint Direct Connect
- Atualização de um LAG em um endpoint do Direct Connect

- Associação de uma conexão com um LAG em um endpoint do Direct Connect
- Desassociação de uma conexão de um LAG no endpoint do Direct Connect
- Associação de chaves CKN/CAK do MACsec a um LAG de endpoint do Direct Connect
- Remova a associação entre uma chave MACsec secreta e um LAG de Direct Connect endpoint
- Exclusão de um LAG de endpoint do Direct Connect

Considerações sobre o protocolo MACsec para o Direct Connect

Leve o seguinte em consideração ao configurar o MACsec em LAGs:

- Quando você cria um LAG com base em conexões existentes, desassociamos todas as chaves MACsec das conexões. Em seguida, adicionamos as conexões ao LAG e associamos a chave MACsec do LAG às conexões.
- Quando você associa uma conexão existente a um LAG, as chaves MACsec associadas ao LAG na ocasião serão associadas à conexão. Portanto, desassociamos as chaves MACsec da conexão, adicionamos a conexão ao LAG e, em seguida, associamos a chave MACsec do LAG à conexão.
- Somente uma única chave MACsec pode ser usada em todos os links do LAG a qualquer momento. A capacidade de suportar várias chaves do MACsec serve apenas para a rotação de chaves.

Criação de um LAG em um endpoint do Direct Connect

Você pode criar um LAG provisionando novas conexões ou agregando conexões existentes.

Você não pode criar um LAG com novas conexões caso isso resulte no excesso do limite geral de conexões para a Região.

Para criar um LAG com base em conexões existentes, as conexões devem estar no mesmo dispositivo da AWS (terminar no mesmo endpoint do Direct Connect). Também devem usar a mesma largura de banda. Não é possível migrar uma conexão de um LAG existente caso a remoção da conexão original deixe o LAG original abaixo da configuração para o número mínimo de conexões operacionais.

> **Important**
>
> Para conexões existentes, a conectividade com a AWS é interrompida durante a criação do LAG.

Para criar um LAG com novas conexões

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione LAGs.
3. Escolha Criar LAG.
4. Em Lag creation type (Tipo de criação de LAG), escolha Request new connections (Solicitar novas conexões) e forneça as seguintes informações:
   - LAG name (Nome do LAG): um nome para o LAG.
   - Location (Local): o local do LAG.
   - Port speed (Velocidade da porta): a velocidade da porta para as conexões.
   - Number of new connections (Número de novas conexões): o número de novas conexões a serem criadas. Você pode ter, no máximo, quatro conexões quando a velocidade da porta é de 1 G ou de 10 G, ou duas quando a velocidade da porta é de 100 Gbps ou de 400 Gbps.
   - (Opcional) Configure o MAC Security (MACsec) para a conexão. Em Configurações adicionais, selecione Solicitar uma porta compatível com MACsec.

     O MACsec só está disponível para conexões dedicadas.
   - (Opcional) Adicione ou remova uma tag.

     [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:
     - Em Key (Chave), insira o nome da chave.
     - Em Valor insira o valor da chave.

     [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).
5. Escolha Criar LAG.

Para criar um LAG com base em conexões existentes

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.

2. No painel de navegação, selecione LAGs.
3. Escolha Criar LAG.
4. Em Lag creation type (Tipo de criação de LAG), escolha Use existing connections (Usar conexões existentes) e forneça as seguintes informações:
   - LAG name (Nome do LAG): um nome para o LAG.
   - Conexões existentes: a conexão do Direct Connect a ser usada para o LAG.
   - (Opcional) Número de novas conexões: o número de novas conexões a serem criadas. Você pode ter, no máximo, quatro conexões quando a velocidade da porta é de 1 G ou de 10 G, ou duas quando a velocidade da porta é de 100 Gbps ou de 400 Gbps.
5. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:
   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).
6. Escolha Criar LAG.

Para criar um LAG usando a linha de comando ou a API

- create-lag (AWS CLI)
- CreateLag (API do Direct Connect)

Para descrever os LAGs usando a linha de comando ou a API

- describe-lags (AWS CLI)
- DescribeLags (API do Direct Connect)

Para baixar a LOA-CFA usando a linha de comando ou a API

- describe-loa (AWS CLI)
- DescribeLoa (API do Direct Connect)

Após criar um LAG, você poderá associar ou desassociar conexões dele. Para obter mais informações, consulte Associação de uma conexão com um LAG e Desassociação de uma conexão de um LAG.

Veja os detalhes do LAG em um endpoint Direct Connect

Depois de criar um LAG, você pode ver seus detalhes usando o Direct Connect console ou usando a linha de comando ou a API.

Para visualizar informações sobre o LAG

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha LAGs.
3. Selecione o LAG e escolha View details (Visualizar detalhes).
4. Você pode visualizar informações sobre o LAG, incluindo seu ID e o Direct Connect endpoint no qual as conexões terminam.

Para visualizar informações sobre seu LAG usando a linha de comando ou a API

- describe-lags (AWS CLI)
- DescribeLags(Direct Connect API)

Atualização de um LAG em um endpoint do Direct Connect

É possível atualizar os seguintes atributos do grupo de agregação de links (LAG) usando o console do Direct Connect ou a linha de comando ou a API:

- O nome do LAG.
- O valor para o número mínimo de conexões que devem estar operacionais para que o LAG fique operacional.
- O modo de criptografia MACsec do LAG.

  O MACsec só está disponível para conexões dedicadas.

  A AWS atribui esse valor a cada conexão que faz parte do LAG.

  Os valores válidos são:

- `should_encrypt`
- `must_encrypt`

  Quando você define o modo de criptografia para esse valor, as conexões ficam inativas quando a criptografia estiver inativa.
- `no_encrypt`

- As tags.

> **Note**
>
> Caso você ajuste o valor limite para o número mínimo de conexões operacionais, certifique-se de que o novo valor não faça o LAG ficar abaixo do limite e ficar não operacional.

Para atualizar um LAG

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione LAGs.
3. Selecione o LAG e escolha Editar.
4. Modificar o LAG

   [Alterar o nome] Em LAG Name (Nome do LAG), insira um novo nome para o LAG.

   [Ajustar o número mínimo de conexões] Em Links mínimos, insira o número mínimo de conexões operacionais.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).
5. Escolha Edit LAG (Editar LAG).

Para atualizar um LAG usando a linha de comando ou a API

- update-lag (AWS CLI)

- UpdateLag (API do Direct Connect)

Associação de uma conexão com um LAG em um endpoint do Direct Connect

É possível associar uma conexão existente com um LAG usando o console do Direct Connect ou a linha de comando ou a API. A conexão pode ser independente ou fazer parte de outro LAG. A conexão deve estar no mesmo dispositivo da AWS e usar a mesma largura de banda do LAG. Caso a conexão já esteja associada a outro LAG, não será possível reassociá-la caso a remoção da conexão faça o LAG ficar abaixo do limite para o número mínimo de conexões operacionais.

A associação de uma conexão a um LAG reassocia automaticamente as interfaces virtuais ao LAG.

> **Important**
>
> A conectividade com a AWS pela conexão é interrompida durante a associação.

Para associar uma conexão a um LAG

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione LAGs.
3. Selecione o LAG e escolha Visualizar detalhes.
4. Em Connections (Conexões), escolha Associate connection (Associar conexão).
5. Em Connection (Conexão), escolha a conexão do Direct Connect a ser usada para o LAG.
6. Escolha Associate Connection (Associar conexão).

Para associar uma conexão usando a linha de comando ou a API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (API do Direct Connect)

Desassociação de uma conexão de um LAG no endpoint do Direct Connect

Converta uma conexão em autônoma ao desassociá-la de um LAG usando o console do Direct Connect ou a linha de comando ou a API. Você não poderá desassociar uma conexão se ela fizer o LAG ficar abaixo do limite para o número mínimo de conexões operacionais.

A desassociação de uma conexão de um LAG não desassocia automaticamente interfaces virtuais.

> **Important**
>
> Sua conexão com a AWS é interrompida durante a desassociação.

Para desassociar uma conexão de um LAG

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel à esquerda, selecione LAGs.
3. Selecione o LAG e escolha Visualizar detalhes.
4. Em Connections (Conexões), selecione a conexão na lista de conexões disponíveis e escolha Disassociate (Desassociar).
5. Na caixa de diálogo de confirmação, escolha Desassociar.

Para desassociar uma conexão usando a linha de comando ou a API

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (API do Direct Connect)

Associação de chaves CKN/CAK do MACsec a um LAG de endpoint do Direct Connect

Após a criação de um LAG compatível com o protocolo MACsec, é possível associar chaves CKN/CAK à conexão usando o console do Direct Connect ou a linha de comando ou a API.

> **Note**
>
> Você não poderá modificar uma chave secreta MACsec após associá-la a um LAG. Se você precisar modificar a chave, desassocie a chave da conexão e associe uma nova chave à conexão. Para obter mais informações sobre como remover uma associação, consulte the section called “Remover a associação entre uma chave MACsec secreta e um LAG”.

Para associar uma chave MACsec a um LAG

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione LAGs.
3. Selecione o LAG e escolha View details (Visualizar detalhes).
4. Escolha Associar chave.
5. Insira a chave MACsec.

   [Usar o par CAK/CKN] Escolha o Par de chaves e faça o seguinte:

   - Em Chave de associação de conectividade (CAK), insira a CAK.
   - Em Nome da chave de associação de conectividade (CKN), insira a CKN.

   [Usar o segredo] Escolha o Segredo existente do Secret Manager e, em seguida, selecione a chave secreta MACsec para Segredo.
6. Escolha Associar chave.

Para associar uma chave do MACsec a um LAG usando a linha de comando ou a API

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey (Direct Connect API)

Remova a associação entre uma chave MACsec secreta e um LAG de Direct Connect endpoint

Você pode remover a associação entre o LAG e a MACsec chave usando o Direct Connect console ou a linha de comando ou a API.

Para remover uma associação entre um LAG e uma chave MACsec

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha LAGs.
3. Selecione o LAG e escolha View details (Visualizar detalhes).
4. Selecione o MACsec segredo a ser removido e, em seguida, escolha Desassociar chave.
5. Na caixa de diálogo de confirmação, digite desassociar e escolha Desassociar.

Para remover uma associação entre um LAG e uma MACsec chave usando a linha de comando ou a API

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(Direct Connect API)

Exclusão de um LAG de endpoint do Direct Connect

Você poderá excluir LAGs quando não precisar mais deles. Não será possível excluir um LAG se ele tiver interfaces virtuais associadas a ele. Primeiro é necessário excluir as interfaces virtuais ou associá-las a outro LAG ou a outra conexão. A exclusão de um LAG não remove as conexões no LAG; você deve excluir as conexões do tipo "faça você mesmo". Para obter mais informações, consulte Excluir uma conexão.

É possível excluir um LAG usando o console do Direct Connect ou a linha de comando ou a API.

Para excluir um LAG

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione LAGs.
3. Selecione os LAGs e escolha Excluir.
4. Na caixa de diálogo de confirmação, escolha Excluir.

Para excluir um LAG usando a linha de comando ou a API

- delete-lag (AWS CLI)
- DeleteLag (API do Direct Connect)

Gateways do Direct Connect

Você pode trabalhar com gateways do Direct Connect usando o console da Amazon VPC ou a AWS CLI.

- Gateways Direct Connect

  É possível associar o gateway do Direct Connect a um gateway de trânsito que tenha diversas VPCs, a um gateway privado virtual ou, se você usa a AWS Cloud WAN, a uma rede principal da Cloud WAN.

- Associações de gateways privados virtuais

  Ao usar um gateway privado virtual, é possível associar o gateway do Direct Connect por meio de uma interface virtual privada a uma ou mais VPCs em qualquer conta localizada na mesma região ou em regiões diferentes.

- Associações de gateways de trânsito

  Use um gateway do Direct Connect para estabelecer a conexão do seu Direct Connect, por meio de uma interface virtual de trânsito, às VPCs ou VPNs que estão conectadas ao seu gateway de trânsito.

- Associações de rede principal da Cloud WAN

  Use um gateway do Direct Connect para associar um gateway do Direct Connect a uma rede principal do AWS Network Manager.

- Interações de prefixos permitidos

  Use os prefixos permitidos para interagir com gateways de trânsito e gateways privados virtuais.

Tópicos

Direct Connect gateways

Use o Direct Connect gateway para conectar seu VPCs. Você associa um Direct Connect gateway a qualquer um dos seguintes:

- Um gateway de trânsito quando você tem vários VPCs na mesma região
- Um gateway privado virtual
- Uma rede principal de WAN em AWS nuvem

Você também pode usar um gateway privado virtual para ampliar sua zona local. Essa configuração permite que a VPC associada à zona local se conecte a um gateway do Direct Connect. O gateway do Direct Connect se conecta a um local do Direct Connect em uma região. O data center on-premises tem uma conexão do Direct Connect com o local do Direct Connect. Para obter mais informações, consulte Como acessar zonas locais usando um gateway do Direct Connect no Guia do usuário da Amazon VPC.

Um gateway Direct Connect é um recurso disponível globalmente. É possível se conectar a qualquer região do mundo usando um gateway do Direct Connect. Isso inclui AWS GovCloud (US), mas não inclui as regiões da AWS China. Um gateway do Direct Connect é um componente virtual do Direct Connect projetado para atuar como um conjunto distribuído de refletores de rota do BGP. Como opera fora do caminho do tráfego de dados, ele evita criar um único ponto de falha ou introduzir dependências em Regiões da AWS específicas. A alta disponibilidade foi inerentemente incorporada ao projeto, eliminando a necessidade de vários gateways do Direct Connect.

Os clientes que usam o Direct Connect e VPCs que atualmente ignoram uma zona de disponibilidade principal não poderão migrar suas conexões ou interfaces virtuais do Direct Connect.

Veja a seguir os cenários nos quais você pode usar um gateway do Direct Connect.

Um gateway Direct Connect não permite que associações de gateway que estejam no mesmo gateway Direct Connect enviem tráfego uma para a outra (por exemplo, um gateway privado virtual para outro gateway privado virtual). Uma exceção a essa regra, implementada em novembro de 2021, é quando uma superrede é anunciada em duas ou mais VPCs, que têm seus gateways privados virtuais conectados (VGWs) associados ao mesmo gateway Direct Connect e na mesma interface virtual. Nesse caso, VPCs podem se comunicar entre si por meio do endpoint Direct Connect. Por exemplo, se você anunciar uma superrede (por exemplo, 10.0.0.0/8 ou 0.0.0.0/0) que se sobrepõe à conectada VPCs a um gateway Direct Connect (por exemplo, 10.0.0.0/24 e

10.0.1.0/24) e na mesma interface virtual, a partir da sua rede local, elas podem se comunicar umas com as outras. VPCs

Se você quiser bloquear a VPC-to-VPC comunicação em um gateway Direct Connect, faça o seguinte:

1. Configure grupos de segurança nas instâncias e em outros recursos na VPC para bloquear o tráfego entre elas VPCs, também usando isso como parte do grupo de segurança padrão na VPC.
2. Evite anunciar uma superrede de sua rede local que se sobreponha à sua. VPCs Em vez disso, você pode anunciar rotas mais específicas da sua rede local que não se sobreponham à sua. VPCs
3. Provisione um único Direct Connect Gateway para cada VPC que você deseja conectar à sua rede local em vez de usar o mesmo Direct Connect Gateway para várias. VPCs Por exemplo, em vez de usar um único Direct Connect Gateway para seu desenvolvimento e produção VPCs, use Direct Connect Gateways separados para cada um deles VPCs.

Um gateway do Direct Connect não impede o envio do tráfego de uma associação de gateway de volta para a própria associação de gateway (p. ex., quando você tiver uma rota de super-rede on-premises que contenha os prefixos da associação de gateway). Se você tiver uma configuração com vários gateways VPCs conectados a trânsito associados ao mesmo gateway Direct Connect, eles VPCs poderão se comunicar. Para evitar que eles VPCs se comuniquem, associe uma tabela de rotas aos anexos da VPC que têm a opção blackhole definida.

Tópicos

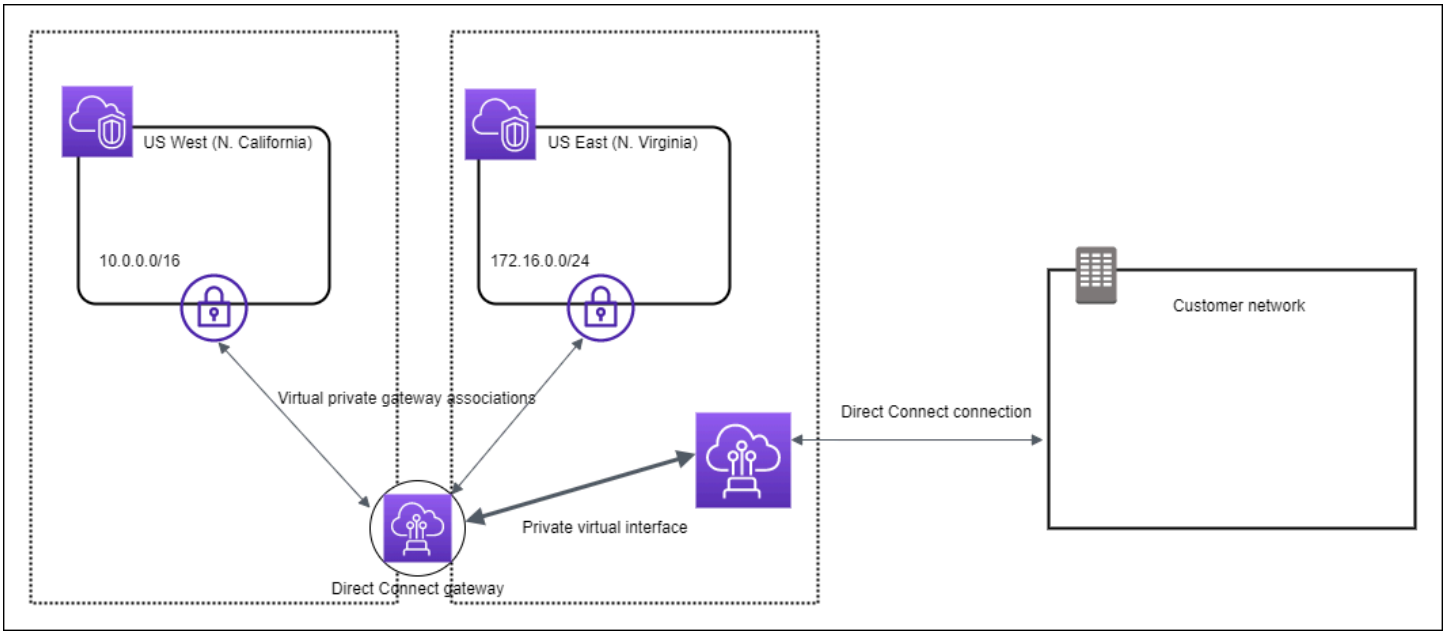
Cenários

A seguir, são descritos apenas alguns cenários para o uso de gateways do Direct Connect.

Cenário: associações de gateways privados virtuais

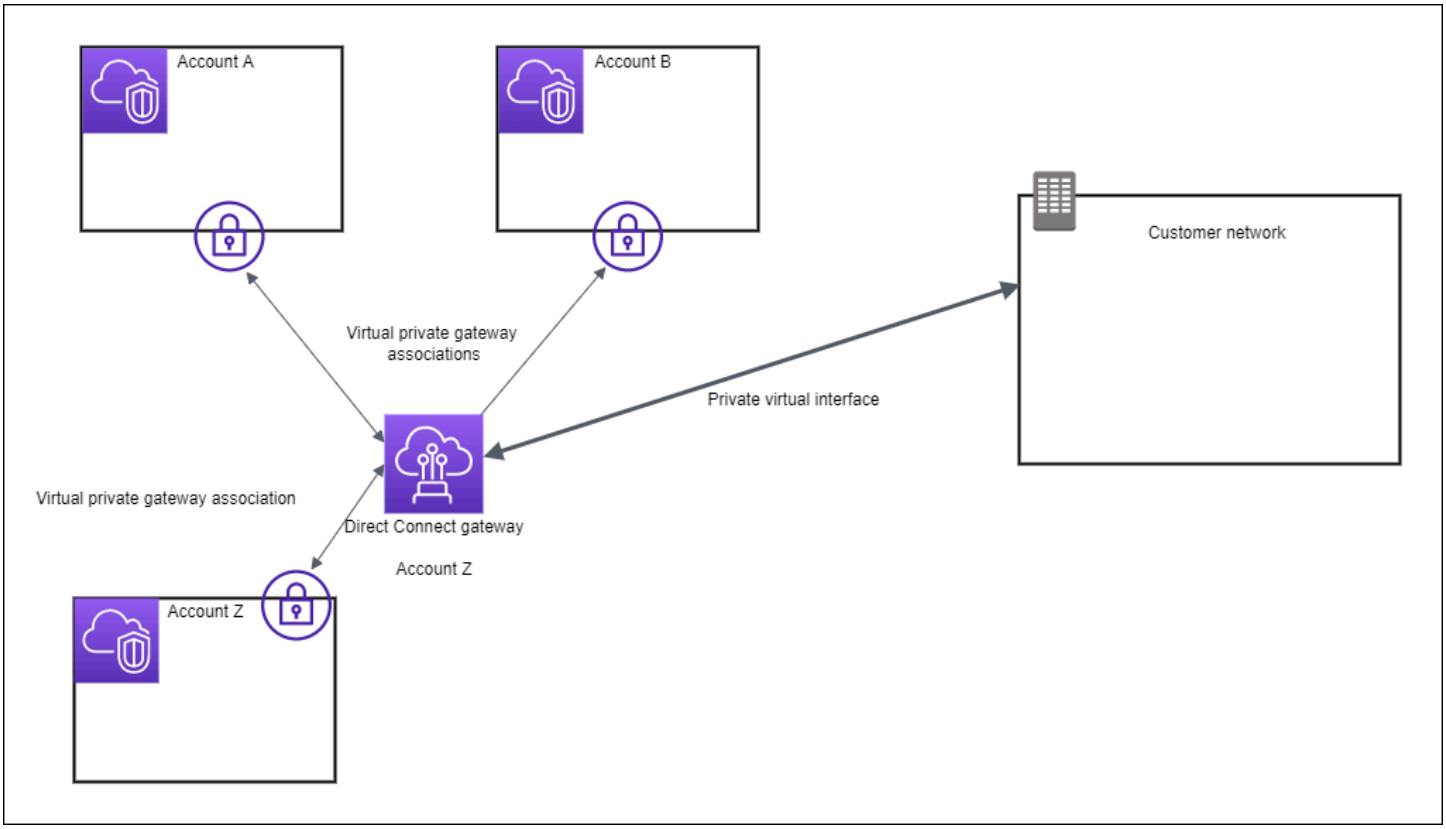
No diagrama a seguir, o gateway Direct Connect permite que você use sua Direct Connect conexão na região Leste dos EUA (Norte da Virgínia) para acessar VPCs sua conta nas regiões Leste dos EUA (Norte da Virgínia) e Oeste dos EUA (Norte da Califórnia).

Cada VPC tem um gateway privado virtual que se conecta ao gateway do Direct Connect usando uma associação de gateway privado virtual. O gateway Direct Connect usa uma interface virtual privada para a conexão com o Direct Connect local. Há uma conexão do Direct Connect proveniente do local para o data center do cliente.



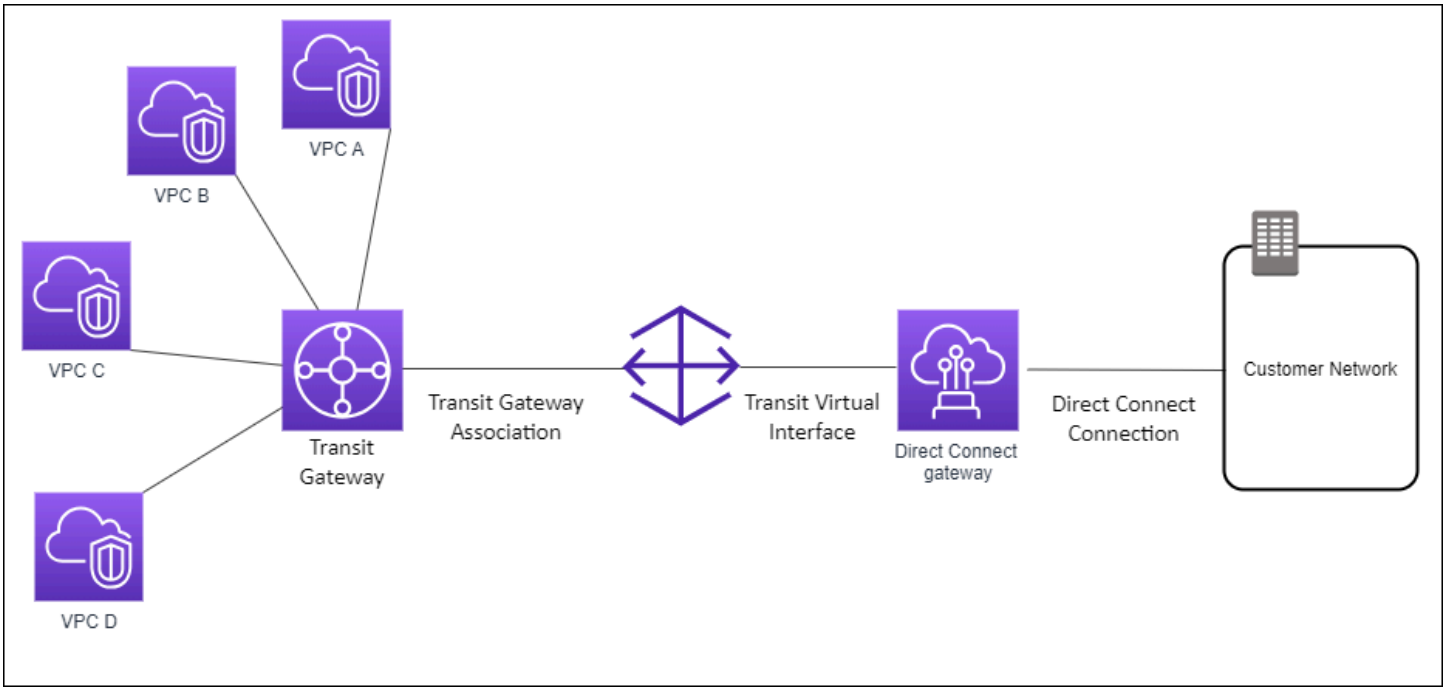
Cenário: associações de gateways privados virtuais entre contas

Considere este cenário de uma conta proprietária do gateway Direct Connect (Conta Z) que é proprietária do gateway Direct Connect. A Conta A e a Conta B desejam usar o gateway Direct Connect. A Conta A e a Conta B enviam uma proposta de associação à Conta Z. A Conta Z aceita as propostas de associação e pode, opcionalmente, atualizar os prefixos que são permitidos no gateway privado virtual da Conta A ou no gateway privado virtual da Conta B. Depois que a Conta Z aceitar as propostas, a Conta A e a Conta B poderão rotear o tráfego de seu gateway privado virtual para o gateway Direct Connect. A Conta Z também é proprietária do roteamento para os clientes porque a Conta Z é proprietária do gateway.



Cenário: associações de gateways de trânsito

O diagrama a seguir ilustra como o gateway Direct Connect permite que você crie uma única conexão com sua conexão Direct Connect que todos VPCs possam usar.



A solução envolve os componentes abaixo:

- Um gateway de trânsito com três anexos de VPC.
- Gateway do Direct Connect
- Uma associação entre o gateway do Direct Connect e o gateway de trânsito.
- Uma interface virtual de trânsito que é anexada ao gateway do Direct Connect.

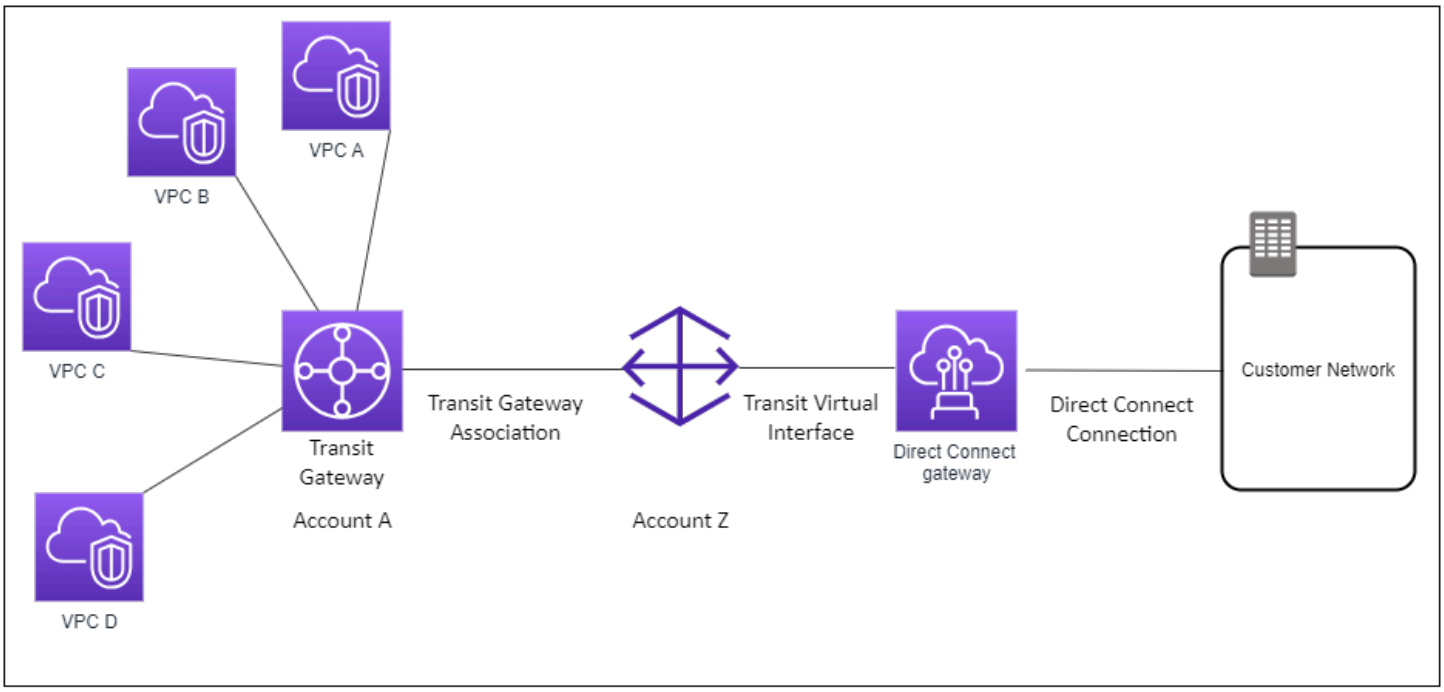
Essa configuração oferece os benefícios abaixo. Você pode:

- Gerencie uma única conexão para várias VPCs ou VPNs que estejam na mesma região.
- Anuncie prefixos do local para AWS e do AWS local para o local.

Para obter mais informações sobre como configurar os gateways de trânsito, consulte Como trabalhar com gateways de trânsito no Guia de gateways de trânsito da Amazon VPC.

Cenário: associações de gateways de trânsito entre contas

Considere este cenário de uma conta proprietária do gateway Direct Connect (Conta Z) que é proprietária do gateway Direct Connect. A Conta A é proprietária do gateway de trânsito e quer usar o gateway do Direct Connect. A Conta Z aceita as propostas de associação e pode, como opção, atualizar os prefixos que são permitidos no gateway de trânsito da Conta A. Depois que a Conta Z aceitar as propostas, o VPCs anexo ao gateway de trânsito poderá rotear o tráfego do gateway de trânsito para o gateway Direct Connect. A Conta Z também é proprietária do roteamento para os clientes porque a Conta Z é proprietária do gateway.



Criação de um gateway do Direct Connect

É possível criar um gateway do Direct Connect em qualquer região compatível usando o console do Direct Connect ou a linha de comando ou a API.

Para criar um gateway Direct Connect

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Gateways Direct Connect.
3. Escolha Create Direct Connect gateway (Criar gateway Direct Connect).
4. Especifique as informações a seguir e selecione Create Direct Connect gateway (Criar gateway Direct Connect).
   - Nome: digite um nome para ajudá-lo a identificar o gateway Direct Connect.
   - ASN do lado da Amazon: especifique o ASN para o lado da Amazon da sessão BGP. O ASN deve estar no intervalo 64.512 a 65.534 ou 4.200.000.000 a 4.294.967.294.

> **Note**
>
> Se você quiser criar um gateway do Direct Connect para usar com uma rede principal da AWS Cloud WAN. O ASN não deve estar no mesmo intervalo que o ASN da rede principal.

Para criar um gateway Direct Connect usando a linha de comando ou a API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway (API do Direct Connect)

Migrar de um gateway privado virtual para um Direct Connect gateway

É possível migrar de um gateway privado virtual conectado a uma interface virtual para um gateway do Direct Connect.

Se você estiver usando o Direct Connect com VPCs o qual atualmente ignora uma zona de disponibilidade principal, você não poderá migrar suas conexões ou interfaces virtuais do Direct Connect.

As etapas apresentadas a seguir descrevem as ações necessárias para migrar um gateway privado virtual para um gateway do Direct Connect.

Como migrar para um gateway Direct Connect

1. Crie um gateway Direct Connect.

   Caso o gateway do Direct Connect ainda não exista, será necessário criá-lo. Para obter as etapas para a criação de um gateway do Direct Connect, consulte Criação de um gateway do Direct Connect.
2. Crie uma interface virtual para o gateway Direct Connect.

   Uma interface virtual é necessária para a migração. Caso a interface ainda não exista, será necessário criá-la. Para obter as etapas para a criação da interface virtual, consulte Interfaces virtuais.
3. Associe o gateway privado virtual ao gateway Direct Connect.

O gateway do Direct Connect e um gateway privado virtual devem estar associados. Para obter as etapas para a criação de uma associação, consulte Associação ou desassociação de gateways privados virtuais.

4. Exclua a interface virtual que estava associada ao gateway privado virtual. Para obter mais informações, consulte Exclusão de uma interface virtual.

Excluir um Direct Connect gateway

Caso não precise mais de um gateway Direct Connect, exclua-o. Você deve primeiro desassociar todos os gateways privados virtuais e excluir a interface virtual privada conectada. Depois de desassociar todos os gateways virtuais privados associados e excluir todas as interfaces virtuais privadas conectadas, você pode excluir o gateway Direct Connect usando o Direct Connect console ou a linha de comando ou a API.

- Para obter as etapas para desassociação de um gateway privado virtual, consulte Associação ou desassociação de gateways privados virtuais.
- Para obter as etapas para a exclusão de uma interface virtual, consulte Exclusão de uma interface virtual.

Para excluir um gateway do Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Gateways Direct Connect.
3. Selecione os gateways e selecione Delete (Excluir).

Para excluir um gateway Direct Connect usando a linha de comando ou a API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(Direct Connect API)

Associações de gateway privado virtual do Direct Connect

Você pode associar um gateway privado virtual a um gateway do Direct Connect para habilitar a conectividade entre sua conexão Direct Connect e VPCs em diferentes contas e regiões. Cada

VPC exige que você associe um gateway privado virtual ao gateway do Direct Connect. Depois que essas associações forem estabelecidas, interfaces virtuais privadas são criadas na conexão do Direct Connect com o gateway Direct Connect, permitindo que várias VPCs compartilhem a mesma conexão do Direct Connect por meio de suas respectivas associações de gateway privado virtual.

As seguintes regras são aplicadas às associações de gateway privado virtual:

- Evite habilitar a propagação de rotas até que a associação de um gateway virtual com um gateway do Direct Connect tenha sido realizada. Caso você habilite a propagação de rotas antes de associar os gateways, as rotas podem ser propagadas de maneira incorreta.
- Há limites para criação e uso de gateways Direct Connect. Para obter mais informações, consulte Cotas do Direct Connect.
- Você não pode anexar um gateway do Direct Connect a um gateway privado virtual quando o gateway do Direct Connect já estiver associado a um gateway de trânsito.
- As VPCs às quais você se conecta por meio de um gateway Direct Connect não podem ter blocos CIDR sobrepostos. Se você adicionar um bloco CIDR IPv4 a uma VPC associada com um gateway Direct Connect, verifique se o bloco CIDR não se sobrepõe a um bloco CIDR existente de nenhuma outra VPC associada. Para obter mais informações, consulte Adicionar blocos CIDR IPv4 a uma VPC no Guia do usuário da Amazon VPC.
- Você não pode criar uma interface virtual pública para um gateway Direct Connect.
- Um gateway do Direct Connect é compatível com comunicação exclusivamente entre interfaces virtuais privadas anexadas e gateways privados virtuais associados, e pode habilitar um gateway privado virtual para outro gateway privado. Não há suporte para os seguintes fluxos de tráfego:
  - Comunicação direta entre as VPCs associadas a um único gateway Direct Connect. Isso inclui o tráfego de uma VPC para outra usando uma passagem por uma rede on-premises por meio de um só gateway do Direct Connect.
  - Comunicação direta entre as interfaces virtuais que estão associadas a um único gateway Direct Connect.
  - Comunicação direta entre as interfaces virtuais associadas a um único gateway Direct Connect e uma conexão VPN em um gateway privado virtual associado ao mesmo gateway Direct Connect.
- Você não pode associar um gateway privado virtual com mais de um gateway Direct Connect e não pode conectar uma interface virtual privada a mais de um gateway Direct Connect.
- Um gateway privado virtual que você associa a um gateway Direct Connect deve ser conectado a uma VPC.

- Uma proposta de associação do gateway privado virtual expira sete dias após ser criada.
- Uma proposta de gateway privado virtual aceita ou uma proposta de gateway privado virtual excluída permanece visível por três dias.
- Um gateway privado virtual pode ser associado a um gateway Direct Connect e também associado a uma interface virtual.
- A desanexação de um gateway privado virtual de uma VPC também desassocia o gateway privado virtual de um gateway do Direct Connect.
- Se você está planejando usar o gateway privado virtual para um gateway Direct Connect e uma conexão VPN dinâmica, defina o ASN no gateway privado virtual como o valor de que você precisa para a conexão VPN. Caso contrário, o ASN no gateway privado virtual pode ser definido como qualquer valor permitido. O gateway Direct Connect anuncia todas as VPCs conectadas pelo ASN atribuído a ele.

Para conectar sua conexão do Direct Connect a uma VPC somente na mesma Região, crie um gateway Direct Connect. Outra opção é criar uma interface virtual privada e anexá-la ao gateway privado virtual da VPC. Para obter mais informações, consulte Criar uma interface virtual privada e VPN CloudHub.

Para usar sua conexão do Direct Connect com uma VPC em outra conta, você pode criar uma interface virtual privada hospedada para essa conta. Ao aceitar a interface virtual hospedada, o proprietário da outra conta pode optar por anexá-la a um gateway privado virtual ou a um gateway Direct Connect na conta. Para obter mais informações, consulte Interfaces virtuais e interfaces virtuais hospedadas.

Tópicos

- Criação de um gateway privado virtual do Direct Connect
- Associar ou desassociar Direct Connect gateways privados virtuais
- Crie uma interface virtual privada para o Direct Connect gateway
- Associação de um gateway privado virtual do Direct Connect entre contas

Criação de um gateway privado virtual do Direct Connect

O gateway privado virtual deve estar conectado à VPC com a qual você deseja se conectar. É possível criar um gateway privado virtual e conectá-lo a uma VPC usando o console do Direct Connect ou a linha de comando ou a API.

> **Note**
>
> Se você está planejando usar o gateway privado virtual para um gateway Direct Connect e uma conexão VPN dinâmica, defina o ASN no gateway privado virtual como o valor de que você precisa para a conexão VPN. Caso contrário, o ASN no gateway privado virtual pode ser definido como qualquer valor permitido. O gateway Direct Connect anuncia todas as VPCs conectadas pelo ASN atribuído a ele.

Depois que você criar um gateway privado virtual, você deve anexá-lo à sua VPC.

Para criar um gateway privado virtual e anexá-lo à sua VPC

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Gateways privados virtuais e então Criar gateway privado virtual.
3. (Opcional) Insira um nome para o gateway privado virtual. Ao fazer isso, é criada uma marcação com a chave de `Name` e o valor que você especificar.
4. Em ASN, deixe a seleção padrão para usar o ASN padrão da Amazon. Caso contrário, selecione Custom ASN (Personalizar ASN) e insira um valor. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar no intervalo de 4200000000 a 4294967294.
5. Escolha Create Virtual Private Gateway (Criar gateway privado virtual).
6. Selecione o gateway privado virtual e, em seguida, escolha Actions (Ações), Attach to VPC (Anexar à VPC).
7. Selecione a VPC na lista e escolha Yes, Attach (Sim, anexar).

Para criar um gateway privado virtual usando a linha de comando ou a API

- CreateVpnGateway (API de consulta do Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para anexar um gateway privado virtual a uma VPC usando a linha de comando ou a API

- AttachVpnGateway (API de consulta do Amazon EC2)

- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Associar ou desassociar Direct Connect gateways privados virtuais

Você pode associar ou desassociar um gateway privado virtual e um gateway Direct Connect usando o Direct Connect console ou usando a linha de comando ou a API. O proprietário da conta do gateway privado virtual executa essas operações.

Para associar um gateway privado virtual

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Gateways do Direct Connect e selecione o gateway do Direct Connect.
3. Escolha Exibir detalhes.
4. Escolha Associações de gateway e Associar gateway.
5. Em Gateways, escolha os gateways privados virtuais a serem associados e selecione Associate gateway (Associar gateway).

Você pode visualizar todos os gateways privados virtuais que estão associados com o gateway Direct Connect selecionando Gateway associations (Associações de gateways).

Para desassociar um gateway privado virtual

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Direct Connect gateways (Gateways Direct Connect) e selecione o gateway Direct Connect.
3. Escolha Exibir detalhes.
4. Escolha Gateway associations (Associações de gateway e selecione o gateway privado virtual.
5. Escolha Desassociar.

Para associar um gateway privado virtual usando a linha de comando ou a API

- create-direct-connect-gateway-associação ()AWS CLI
- CreateDirectConnectGatewayAssociation(Direct Connect API)

Para visualizar os gateways privados virtuais associados a um gateway Direct Connect usando a linha de comando ou a API

- describe-direct-connect-gateway-associações ()AWS CLI
- DescribeDirectConnectGatewayAssociations(Direct Connect API)

Para desassociar um gateway privado virtual usando a linha de comando ou a API

- delete-direct-connect-gateway-associação ()AWS CLI
- DeleteDirectConnectGatewayAssociation(Direct Connect API)

Crie uma interface virtual privada para o Direct Connect gateway

Para conectar sua Direct Connect conexão à VPC remota, você deve criar uma interface virtual privada para sua conexão. Especifique o gateway Direct Connect ao qual se conectar. Você pode criar uma interface virtual privada usando o Direct Connect console ou usando a linha de comando ou a API.

> **Note**
>
> Caso esteja aceitando uma interface virtual privada hospedada, você pode associá-la a um gateway Direct Connect na conta. Para obter mais informações, consulte Aceitação de uma interface virtual hospedada do .

Para provisionar uma interface virtual privada para um gateway Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Tipo de interface virtual, escolha Privado.
5. Em Configurações de interface virtual pública, faça o seguinte:
   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.
   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.

c. Para Proprietário da interface virtual, escolha Minha AWS conta se a interface virtual for para sua AWS conta.

d. Em Direct Connect gateway (Gateway Direct Connect), selecione o gateway Direct Connect.

e. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

f. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

   Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulte Suporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

   a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

      [IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

      - Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
      - Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

      > **Important**
      >
      > Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
      >
      > - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.

- Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade máxima de transmissão (MTU) de 1500 (padrão) para 9001 (frames jumbo), selecione MTU jumbo (tamanho de MTU 9001).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Valor insira o valor da chave.

[Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Depois que você tiver criado a interface virtual, você poderá fazer download da configuração do roteador no dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual privada usando a linha de comando ou a API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (API do Direct Connect)

Como visualizar as interfaces virtuais que estão anexadas a um gateway Direct Connect usando a linha de comando ou a API

- describe-direct-connect-gateway-anexos ()AWS CLI
- DescribeDirectConnectGatewayAttachments(Direct Connect API)

Associação de um gateway privado virtual do Direct Connect entre contas

É possível associar um gateway do Direct Connect a um gateway privado virtual pertencente a qualquer conta da AWS. O gateway Direct Connect pode ser um gateway existente ou é possível criar um novo gateway. O proprietário do gateway privado virtual cria uma proposta de associação e o proprietário do gateway Direct Connect deve aceitá-la.

Uma proposta de associação pode conter prefixos que serão permitidos a partir do gateway privado virtual. O proprietário do gateway Direct Connect pode opcionalmente substituir qualquer prefixo solicitado na proposta de associação.

Prefixos permitidos

Quando associa um gateway privado virtual com um gateway Direct Connect, você especifica uma lista de prefixos da Amazon VPC a serem anunciados no gateway Direct Connect. A lista de prefixos atua como um filtro que permite que os mesmos CIDRs, ou CIDRs menores, sejam anunciados no gateway Direct Connect. Você deve definir os Allowed prefixes (Prefixos permitidos) como um intervalo que seja igual ou maior do que o CIDR da VPC porque provisionamos todo o CIDR da VPC no gateway privado virtual.

Considere o caso em que o CIDR da VPC seja 10.0.0.0/16. Você pode definir os Allowed prefixes (Prefixos permitidos) como 10.0.0.0/16 (o valor do CIDR da VPC) ou 10.0.0.0/15 (um valor maior do que o CIDR da VPC).

Qualquer interface virtual que faz parte dos prefixos de rede anunciados pelo Direct Connect é propagada apenas para gateways de trânsito em regiões diferentes, e não na mesma região. Para obter mais informações sobre como os prefixos permitidos interagem com gateways privados virtuais e gateways de trânsito, consulte Interações de prefixos permitidos.

Associações entre gateways do Direct Connect e gateways de trânsito

É possível usar o gateway do Direct Connect para estabelecer uma conexão entre a conexão do Direct Connect usando uma interface virtual de trânsito e as VPCs ou VPNs que estão conectadas ao gateway de trânsito. Você associa um gateway do Direct Connect com o gateway de trânsito. Em seguida, crie uma interface virtual privada para sua conexão do Direct Connect com o gateway Direct Connect.

As seguintes regras se aplicam às associações do gateway de trânsito:

- Você não pode anexar um gateway do Direct Connect a um gateway de trânsito quando o gateway do Direct Connect já estiver associado a um gateway privado virtual ou estiver anexado a uma interface virtual privada.
- Há limites para criação e uso de gateways Direct Connect. Para obter mais informações, consulte Cotas do Direct Connect.
- Um gateway do Direct Connect fornece suporte para a comunicação entre interfaces virtuais de trânsito conectadas e gateways de trânsito associados.
- Se você se conectar a vários gateways de trânsito que estejam em regiões diferentes, use ASNs exclusivos para cada gateway de trânsito.
- Qualquer endereço de conectividade ponto a ponto usando um intervalo `/30`, por exemplo, `192.168.0.0/30`, não se propaga para um gateway de trânsito.

Associar um gateway de trânsito entre contas

É possível associar um gateway existente do Direct Connect ou um novo gateway do Direct Connect a um gateway de trânsito pertencente a qualquer conta da AWS. O proprietário do gateway de trânsito cria uma proposta de associação e o proprietário do gateway do Direct Connect deve aceitá-la.

Uma proposta de associação pode conter prefixos que serão permitidos por parte do gateway de trânsito. O proprietário do gateway Direct Connect pode opcionalmente substituir qualquer prefixo solicitado na proposta de associação.

Prefixos permitidos

Para uma associação de gateway de trânsito, você provisiona a lista de prefixos permitidos no gateway do Direct Connect. A lista é usada para rotear o tráfego do ambiente on-premises para a AWS no gateway de trânsito mesmo que as VPCs anexadas ao gateway de trânsito não tenham CIDRs atribuídos. Os prefixos na lista de prefixos permitidos do gateway Direct Connect são originados no gateway Direct Connect e são anunciados para a rede on-premises. Para obter mais informações sobre como os prefixos permitidos interagem com o gateway de trânsito e com os gateways privados virtuais, consulte Interações de prefixos permitidos.

Tópicos

- Associar ou desassociar Direct Connect com um gateway de trânsito
- Crie uma interface virtual de trânsito para o Direct Connect gateway

- Crie um gateway de trânsito e uma proposta de Direct Connect associação
- Aceitação ou rejeição de uma proposta de associação entre um gateway de trânsito e o Direct Connect
- Atualize os prefixos permitidos para um gateway de trânsito e associação Direct Connect
- Excluir um gateway de trânsito e uma proposta de Direct Connect associação

Associar ou desassociar Direct Connect com um gateway de trânsito

Associe ou desassocie um gateway de trânsito usando o Direct Connect console ou usando a linha de comando ou a API.

Para associar um gateway de trânsito

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Direct Connect gateways (Gateways Direct Connect) e selecione o gateway Direct Connect.
3. Escolha Exibir detalhes.
4. Escolha Gateways associations (Associações de gateways) e Associate gateway (Associar gateway).
5. Em Gateways, escolha o gateway de trânsito que deseja associar.
6. Em Prefixos permitidos, insira os prefixos (separados por uma vírgula ou em uma nova linha) que o gateway do Direct Connect anuncia para o data center on-premises. Para obter mais informações sobre prefixos permitidos, consulte Interações de prefixos permitidos.
7. Escolher o gateway associado

Você pode visualizar todos os gateways que estão associados com o gateway Direct Connect selecionando Gateway associations (Associações de gateways).

Para desassociar um gateway de trânsito

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Direct Connect gateways (Gateways Direct Connect) e selecione o gateway Direct Connect.
3. Escolha Exibir detalhes.
4. Escolha Gateway associations (Associações de gateways) e selecione o gateway de trânsito.

5. Escolha Desassociar.

Para atualizar os prefixos permitidos para um gateway de trânsito

É possível adicionar ou remover prefixos permitidos do gateway de trânsito.

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Gateways do Direct Connect e, em seguida, escolha o gateway do Direct Connect para o qual deseja adicionar ou remover prefixos permitidos.
3. Escolha a guia Associações de gateway.
4. Escolha o gateway que deseja modificar os prefixos permitidos e, em seguida, escolha Editar.
5. Em Prefixos permitidos, insira os prefixos que o gateway do Direct Connect anuncia para o data center on-premises. Para vários prefixos, separe cada prefixo com uma vírgula ou coloque cada prefixo em uma nova linha. Os prefixos que você adiciona devem corresponder ao Amazon CIDRs VPC para todos os gateways privados virtuais. Para obter mais informações sobre prefixos permitidos, consulte Interações de prefixos permitidos.
6. Escolha Edit association.

   Na seção Associação de gateway, o Estado exibe o texto atualizando. Quando concluído, o Estado mudará para associado. A conclusão dessa operação pode levar vários minutos ou ainda mais tempo.

Para associar um gateway de trânsito usando a linha de comando ou a API

- create-direct-connect-gateway-associação ()AWS CLI
- CreateDirectConnectGatewayAssociation(Direct Connect API)

Para visualizar os gateways de trânsito associados a um gateway do Direct Connect usando a linha de comando ou a API

- describe-direct-connect-gateway-associações ()AWS CLI
- DescribeDirectConnectGatewayAssociations(Direct Connect API)

Para desassociar um gateway de trânsito usando a linha de comando ou a API

- delete-direct-connect-gateway-associação ()AWS CLI

- DeleteDirectConnectGatewayAssociation(Direct Connect API)

Para atualizar os prefixos permitidos de um gateway de trânsito usando a linha de comando ou a API

- update-direct-connect-gateway-associação ()AWS CLI
- UpdateDirectConnectGatewayAssociation(Direct Connect API)

Crie uma interface virtual de trânsito para o Direct Connect gateway

Para conectar sua Direct Connect conexão ao gateway de trânsito, você deve criar uma interface de trânsito para sua conexão. Especifique o gateway Direct Connect ao qual se conectar. Você pode usar o Direct Connect console ou usar a linha de comando ou a API.

> **Important**
>
> Se você associar seu gateway de trânsito a um ou mais gateways do Direct Connect, o número de sistema autônomo (ASN) usado pelo gateway de trânsito e pelo gateway do Direct Connect devem ser diferentes. Por exemplo, a solicitação de associação falhará se você usar o ASN 64512 padrão para o gateway de trânsito e o gateway do Direct Connect.

Como provisionar uma interface virtual de trânsito para um gateway Direct Connect

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Virtual Interfaces (Interfaces virtuais).
3. Selecione Create virtual interface (Criar interface virtual).
4. Em Virtual interface type (Tipo de interface virtual), em Type (Tipo), selecione Transit (Trânsito).
5. Em Private virtual interface settings (Configurações de interface virtual privada), faça o seguinte:
   a. Em Virtual interface name (Nome da interface virtual), insira um nome para a interface virtual.
   b. Em Connection (Conexão), escolha a conexão do Direct Connect que deseja usar para essa interface.
   c. Para Proprietário da interface virtual, escolha Minha AWS conta se a interface virtual for para sua AWS conta.
   d. Em Direct Connect gateway (Gateway Direct Connect), selecione o gateway Direct Connect.
   e. Em VLAN, informe o número do ID para sua rede local virtual (VLAN).

f. Em ASN do BGP insira o número de sistema autônomo do Protocolo de Gateway da Borda do roteador de mesmo nível on-premises para a nova interface virtual.

Os valores válidos são de 1 a 4294967294. Isso inclui suporte para ASNs (1-2147483647) e longo (1-4294967294). ASNs Para obter mais informações sobre ASNs e por muito tempo, ASNs consulteSuporte longo de ASN em Direct Connect.

6. Em Additional settings (Configurações adicionais), faça o seguinte:

a. Para configurar um IPv4 BGP ou um IPv6 peer, faça o seguinte:

[IPv4] Para configurar um peer IPv4 BGP, escolha IPv4e faça o seguinte:

- Para especificar você mesmo esses endereços IP, para o IP do seu roteador, insira o endereço IPv4 CIDR de destino para o qual a Amazon deve enviar tráfego.
- Para o IP de mesmo nível do roteador Amazon, insira o endereço IPv4 CIDR a ser usado para enviar tráfego. AWS

> **Important**
>
> Ao configurar as interfaces virtuais do AWS Direct Connect, você pode especificar seus próprios endereços IP usando o RFC 1918, usar outros esquemas de endereçamento ou optar por endereços CIDR IPv4 /29 AWS atribuídos alocados do intervalo Link-Local da RFC 3927 169.254.0.0/16 para conectividade. IPv4 point-to-point Essas point-to-point conexões devem ser usadas exclusivamente para emparelhamento eBGP entre o roteador do gateway do cliente e o endpoint do Direct Connect. Para fins de tráfego de VPC ou tunelamento, como VPN IP AWS Site-to-Site privada ou Transit Gateway Connect, AWS recomenda usar uma interface de loopback ou LAN no roteador do gateway do cliente como endereço de origem ou destino em vez das conexões. point-to-point
>
> - Para ter mais informações sobre a RFC 1918, consulte Address Allocation for Private Internets.
> - Para obter mais informações sobre o RFC 3927, consulte Configuração dinâmica de endereços locais de IPv4 link.

[IPv6] Para configurar um peer IPv6 BGP, escolha. IPv6 Os IPv6 endereços dos pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon. Você não pode especificar IPv6 endereços personalizados.

b. Para alterar a unidade de transmissão máxima (MTU) de 1500 (padrão) para 8500 (frames jumbo), selecione Jumbo MTU (MTU size 8500) (MTU jumbo (tamanho da MTU 8500)).

c. (Opcional) Em Ativar SiteLink, escolha Ativado para ativar a conectividade direta entre os pontos de presença do Direct Connect.

d. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Selecione Add tag (Adicionar tag) e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Valor insira o valor da chave.

   [Remover uma tag] Ao lado da tag, escolha Remove tag (Remover tag).

7. Selecione Create virtual interface (Criar interface virtual).

Depois que você tiver criado a interface virtual, você poderá fazer download da configuração do roteador no dispositivo. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual de trânsito usando a linha de comando ou a API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface (API do Direct Connect)

Como visualizar as interfaces virtuais que estão anexadas a um gateway Direct Connect usando a linha de comando ou a API

- describe-direct-connect-gateway-anexos ()AWS CLI
- DescribeDirectConnectGatewayAttachments(Direct Connect API)

Crie um gateway de trânsito e uma proposta de Direct Connect associação

Se você for proprietário do gateway de trânsito, deverá criar a proposta de associação. O gateway de trânsito deve estar conectado a uma VPC ou VPN em sua AWS conta. O proprietário do gateway do Direct Connect deve compartilhar o ID do gateway do Direct Connect e o ID de sua conta da AWS . Depois que a proposta for criada, o proprietário do gateway Direct Connect deverá aceitá-la para que você tenha acesso à rede on-premises pelo Direct Connect. Você pode criar uma proposta de associação usando o Direct Connect console ou usando a linha de comando ou a API.

Para criar uma proposta de associação

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione Gateways de trânsito e escolha o gateway de trânsito.
3. Escolha Exibir detalhes.
4. Selecione Direct Connect gateway associations (Associações de gateway Direct Connect) e selecione Associate Direct Connect gateway (Associar gateway Direct Connect).
5. Em Association account type (Tipo de conta de associação), em Account owner (Proprietário da conta), selecione Another account (Outra conta).
6. Em Proprietário do gateway do Direct Connect, insira o ID da conta da proprietária do gateway do Direct Connect.
7. Em Association settings (Configurações da associação), faça o seguinte:
   a. Em Direct Connect gateway ID (ID do gateway Direct Connect), insira o ID do gateway Direct Connect.
   b. Em Proprietário da interface virtual, insira o ID da conta proprietária da interface virtual da associação.
   c. (Opcional) Para especificar uma lista de prefixos a serem permitidos pelo gateway de trânsito, adicione os prefixos a Prefixos permitidos, separando-os com vírgulas ou inserindo-os em linhas separadas.
8. Escolha Associate Direct Connect gateway (Associar gateway Direct Connect).

Para criar uma proposta de associação usando a linha de comando ou a API

- create-direct-connect-gateway-proposta de associação ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(Direct Connect API)

Aceitação ou rejeição de uma proposta de associação entre um gateway de trânsito e o Direct Connect

Se for proprietário do gateway Direct Connect, você deverá aceitar a proposta de associação para criá-la. Você também tem a opção de rejeitar a proposta de associação. É possível aceitar ou rejeitar uma proposta de associação usando o console do Direct Connect ou a linha de comando ou a API.

Para aceitar uma proposta de associação

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Direct Connect gateways (Gateways Direct Connect).
3. Selecione o gateway Direct Connect com propostas pendentes e escolha View details (Visualizar detalhes).
4. Na guia Pending proposals (Propostas pendentes), escolha a proposta e depois Accept proposal (Aceitar proposta).
5. (Opcional) Para especificar uma lista de prefixos a serem permitidos pelo gateway de trânsito, adicione os prefixos a Prefixos permitidos, separando-os com vírgulas ou inserindo-os em linhas separadas.
6. Escolha Accept proposal (Aceitar proposta).

Para rejeitar uma proposta de associação

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Direct Connect gateways (Gateways Direct Connect).
3. Selecione o gateway Direct Connect com propostas pendentes e escolha View details (Visualizar detalhes).
4. Na guia Pending proposals (Propostas pendentes), selecione o gateway de trânsito e, e escolha Reject proposal (Rejeitar proposta).
5. Na caixa de diálogo Reject proposal (Rejeitar proposta), insira Delete (Excluir) e escolha Reject proposal (Rejeitar proposta).

Para visualizar propostas de associação usando a linha de comando ou a API

- describe-direct-connect-gateway-association-proposals (AWS CLI)
- DescribeDirectConnectGatewayAssociationProposals (API do Direct Connect)

Para aceitar uma proposta de associação usando a linha de comando ou a API

- accept-direct-connect-gateway-association-proposal (AWS CLI)
- AcceptDirectConnectGatewayAssociationProposal (API do Direct Connect)

Para rejeitar uma proposta de associação usando a linha de comando ou a API

- delete-direct-connect-gateway-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (API do Direct Connect)

Atualize os prefixos permitidos para um gateway de trânsito e associação Direct Connect

Você pode atualizar os prefixos permitidos do gateway de trânsito pelo gateway Direct Connect usando o Direct Connect console ou usando a linha de comando ou a API. Para atualizar os prefixos permitidos para um gateway de trânsito e uma associação do Direct Connect usando o Direct Connect console,

- caso você seja o proprietário do gateway de trânsito, será necessário criar uma nova proposta de associação para esse gateway do Direct Connect, especificando os prefixos a serem permitidos. Para obter as etapas para a criação de uma nova proposta de associação, consulte Criação de uma proposta de associação do gateway de trânsito.
- Caso você seja o proprietário do gateway do Direct Connect, é possível atualizar os prefixos permitidos ao aceitar a proposta de associação ou ao modificar os prefixos para uma associação existente. Para obter as etapas para a atualização dos prefixos permitidos ao aceitar a associação, consulte Aceitação ou rejeição de uma proposta de associação do gateway de trânsito.

Para atualizar os prefixos permitidos para uma associação existente usando a linha de comando ou a API

- update-direct-connect-gateway-associação ()AWS CLI
- UpdateDirectConnectGatewayAssociation(Direct Connect API)

Excluir um gateway de trânsito e uma proposta de Direct Connect associação

O proprietário do gateway de trânsito poderá excluir a proposta de associação do gateway do Direct Connect se ela ainda estiver aguardando aceitação. Depois que uma proposta de associação for aceita, ela não poderá ser excluída, mas você poderá desassociar o gateway de trânsito do gateway

Direct Connect. Para obter mais informações, consulte Criação de uma proposta de associação do gateway de trânsito.

Você pode excluir um gateway de trânsito e uma proposta de associação do Direct Connect usando o Direct Connect console ou a linha de comando ou a API.

Para excluir uma proposta de associação

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione Gateways de trânsito e escolha o gateway de trânsito.
3. Escolha Exibir detalhes.
4. Escolha Pending gateway associations (Associações de gateway pendentes), selecione a associação e escolha Delete association (Excluir associação).
5. Na caixa de diálogo Delete association proposal (Excluir proposta de associação), insira Delete (Excluir) e selecione Delete (Excluir).

Para excluir uma proposta de associação usando a linha de comando ou a API

- delete-direct-connect-gateway-proposta de associação ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(Direct Connect API)

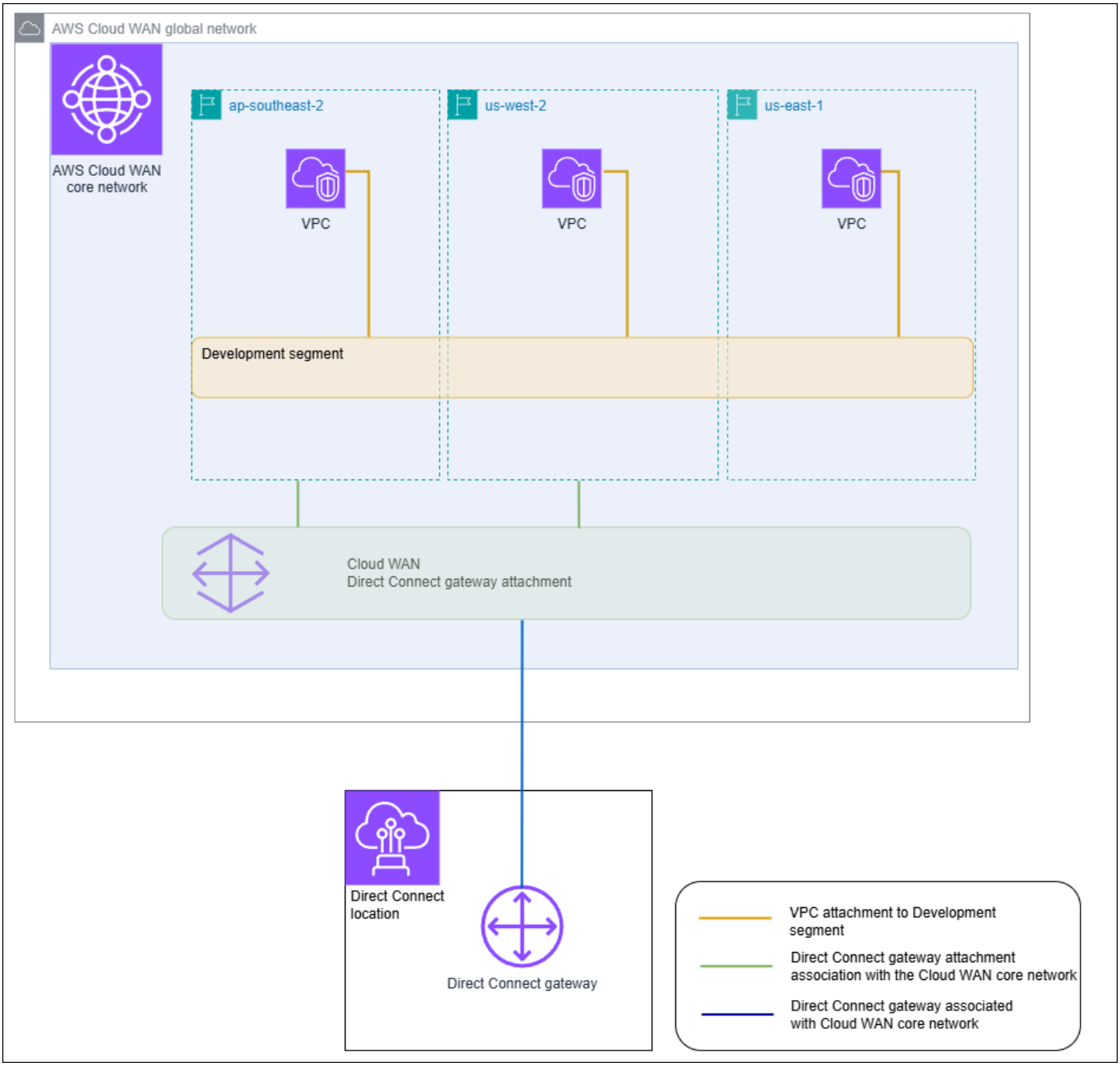
Direct Connect associações de gateway e rede principal de AWS Cloud WAN

Associe um Direct Connect gateway a uma rede principal do AWS Cloud WAN usando um tipo de anexo Direct Connect no Cloud WAN. Essa associação direta direciona o tráfego entre os locais da borda selecionados da sua rede principal e suas conexões do Direct Connect usando o caminho mais curto disponível.

O tipo de conexão do gateway do Direct Connect oferece suporte ao BGP (protocolo Border Gateway) para propagação automática de informações de roteamento entre sua rede principal e on-premises. A conexão Direct Connect também oferece suporte aos recursos padrão da Cloud WAN, como gerenciamento central baseado em políticas, automação de conexões baseada em tags e segmentação para configurações avançadas de segurança.

> **Note**
>
> A associação entre uma rede principal e um gateway do Direct Connect é criada, excluída e gerenciada a partir do console da Cloud WAN no Gerenciador de rede. Ao usar um gateway Direct Connect com o Cloud WAN, o console do Direct Connect APIs e a CLI refletirão a associação, mas não poderão ser usados para modificá-la. No entanto, você pode usar a API ou a linha de comando do Direct Connect para verificar se uma associação foi criada.

O exemplo a seguir mostra uma rede global da Cloud WAN com três regiões dentro da rede principal da Cloud WAN. Cada região tem sua própria VPC conectada a um segmento de desenvolvimento de rede principal compartilhado entre essas três regiões. Usando a Cloud WAN, uma conexão do gateway do Direct Connect é criada dentro da Cloud WAN usando um gateway criado com o uso do Direct Connect. A conexão está associada a duas das três regiões, ap-southeast-2 e us-west-2, e tem permissão de acesso ao segmento de desenvolvimento. Embora us-east-1 compartilhe o mesmo segmento de desenvolvimento, a conexão do gateway do Direct Connect não é compartilhada com essa região e, portanto, não está disponível.



Tópicos

- Pré-requisitos
- Considerações
- Associações de gateway do Direct Connect a uma rede principal da Cloud WAN
- Verificar uma associação de Direct Connect gateway a uma rede principal de WAN em AWS nuvem

Pré-requisitos

A associação do gateway do Direct Connect com uma rede principal da Cloud WAN exige o seguinte:

- Um gateway atual do Direct Connect. Para obter as etapas para a criação de um gateway do Direct Connect, consulte Criação de um gateway do Direct Connect.
- Uma rede principal de WAN em AWS nuvem. Para obter mais informações sobre Cloud WAN, consulte o Guia do usuário do AWS Cloud WAN.

Considerações

Os limites a seguir são aplicados às associações do gateway do Direct Connect com uma rede principal da Cloud WAN:

- Um gateway do Direct Connect pode ser associado a uma única rede principal da Cloud WAN e a um único segmento dessa rede principal. Depois que uma associação é criada, esse gateway não pode ser associado a outros recursos nas AWS regiões. Se você dissociar o gateway da rede principal, poderá usá-lo para outros tipos de associação.
- A conexão entre o gateway do Direct Connect e a Cloud WAN usa o tipo de interface virtual de trânsito para realizar a conectividade.
- A conexão da Cloud WAN não é compatível com as listas de prefixos permitidos. Todos os prefixos em um segmento da rede principal serão anunciados no gateway do Direct Connect associado a esse segmento.
- A cota para o máximo de prefixos que podem ser anunciados de on-premises para a AWS por meio de uma interface virtual de trânsito é diferente da cota para prefixos anunciados de uma rede central da Cloud WAN para on-premises. As cotas para outros recursos do Direct Connect usados com uma associação da Cloud WAN também são aplicáveis. Consulte Cotas do Direct Connect.
- O atributo AS-PATH BGP será mantido na rede principal, no gateway do Direct Connect e na interface virtual.
- O ASN de um gateway do Direct Connect deve estar fora do intervalo de ASN configurado para a rede principal da Cloud WAN. Por exemplo, se você tiver um intervalo de ASN de 64512 a 65534 para a rede principal, o ASN do gateway do Direct Connect deverá usar um ASN fora desse intervalo.
- A Cloud WAN pode não oferecer suporte a tipos específicos de conexão que usam o tipo de conexão do Direct Connect para transporte. Para obter mais informações sobre os anexos do

gateway Direct Connect a uma rede principal do Cloud WAN, consulte Anexos do gateway Direct Connect no Cloud WAN no Guia do usuário do AWSAWS Cloud WAN.

- CloudWatch O Network Monitor suporta métricas de latência e perda de pacotes quando usado com um tipo de anexo de gateway Cloud WAN Direct Connect. O recurso Indicador de integridade da rede não é aceito. Para obter mais informações, consulte Usando o Monitor de rede do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch .

Associações de gateway do Direct Connect a uma rede principal da Cloud WAN

A associação de um gateway Direct Connect a uma rede principal do AWS Cloud WAN é realizada usando o console AWS Cloud WAN, o Cloud WAN APIs ou a linha de comando.

Para associar um gateway do Direct Connect existente a uma rede principal da Cloud WAN, crie um nova conexão do Direct Connect no console da Cloud WAN. Depois que a conexão do Direct Connect for criada, a associação será estabelecida. Por padrão, ao criar a associação, você pode escolher o padrão para incluir todos os locais da borda da rede principal no segmento de rede principal escolhido. Como alternativa, você pode especificar locais da borda individuais.

Para obter mais informações sobre os anexos do gateway Direct Connect a uma rede principal do Cloud WAN, consulte Anexos do gateway Direct Connect no Cloud WAN no Guia do usuário do AWSAWS Cloud WAN.

Verificar uma associação de Direct Connect gateway a uma rede principal de WAN em AWS nuvem

Você pode verificar a associação de um gateway do Direct Connect a uma rede principal da Cloud WAN usando o console do Direct Connect ou a API ou a linha de comando do Direct Connect.

Para verificar a associação do gateway do Direct Connect a uma rede principal da Cloud WAN usando o console

1. Abra o Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, selecione Gateways do Direct Connect.
3. Escolha a conexão do gateway do Direct Connect para a qual você deseja visualizar a associação.
4. Escolha a guia Associações de gateway.

- A coluna ID exibe o ID da rede principal à qual o gateway do Direct Connect está associado.
- A coluna Estado exibe Associada.
- A coluna Tipo de associação exibe Rede principal da Cloud WAN.

Para verificar a associação do gateway do Direct Connect a uma rede principal da Cloud WAN usando a linha de comando ou a API

- DescribeDirectConnectGatewayAssociations(Direct Connect API)
- describe-direct-connect-gateway-associação ()AWS CLI

Interações de prefixos permitidos para gateways do Direct Connect

Saiba como os prefixos permitidos interagem com gateways de trânsito e gateways privados virtuais. Para obter mais informações, consulte Políticas de roteamento e comunidades BGP.

Associações de gateways privados virtuais

A lista de prefixos (IPv4 e IPv6) atua como um filtro que permite que os mesmos CIDRs, ou um intervalo menor de CIDRs, sejam anunciados no gateway do Direct Connect. É necessário definir os prefixos para um intervalo que seja o mesmo ou maior que o bloco CIDR da VPC.

> **Note**
>
> A lista de permissões só funciona como um filtro, e somente o CIDR de VPC associado será anunciado no gateway do cliente.

Considere o cenário em que você tem uma VPC com CIDR 10.0.0.0/16 anexada a um gateway privado virtual.

- Quando a lista de prefixos permitidos é definida como 22.0.0.0/24, você não recebe nenhuma rota porque 22.0.0.0/24 não é igual nem maior do que 10.0.0.0/16.
- Quando a lista de prefixos permitidos é definida como 10.0.0.0/24, você não recebe nenhuma rota porque 10.0.0.0/24 não é igual a 10.0.0.0/16.
- Quando a lista de prefixos permitidos é definida como 10.0.0.0/15, você recebe 10.0.0.0/16 porque o endereço IP é maior do que 10.0.0.0/16.

Quando você remover ou adicionar um prefixo permitido, o tráfego que não usar esse prefixo não será afetado. Durante as atualizações, o status muda de `associated` para `updating`. A modificação de um prefixo existente pode atrasar ou reduzir somente o tráfego que usa esse prefixo.

Associações de gateways de trânsito

Para uma associação de gateway de trânsito, você provisiona a lista de prefixos permitidos no gateway do Direct Connect. A lista roteia o tráfego do ambiente on-premises de ou para um gateway do Direct Connect para o gateway de trânsito mesmo que as VPCs anexadas ao gateway de trânsito não tenham CIDRs atribuídos. Os prefixos permitidos funcionam de forma diferente de acordo com o tipo de gateway:

- Para associações de gateway de trânsito, somente os prefixos permitidos inseridos serão anunciados no ambiente on-premises. Eles serão exibidos como originários do ASN do gateway do Direct Connect.
- Para gateways privados virtuais, os prefixos permitidos inseridos atuam como um filtro para permitir os mesmos CIDRs ou CIDRs menores.

Considere o cenário no qual você tem uma VPC com CIDR 10.0.0.0/16 anexada a um gateway de trânsito.

- Quando a lista de prefixos permitidos é definida como 22.0.0.0/24, você recebe 22.0.0.0/24 via BGP em sua interface virtual de trânsito. Você não receberá 10.0.0.0/16 porque provisionamos diretamente os prefixos que estão na lista de prefixos permitidos.
- Quando a lista de prefixos permitidos é definida como 10.0.0.0/24, você recebe 10.0.0.0/24 via BGP em sua interface virtual de trânsito. Você não receberá 10.0.0.0/16 porque provisionamos diretamente os prefixos que estão na lista de prefixos permitidos.
- Quando a lista de prefixos permitidos é definida como 10.0.0.0/8, você recebe 10.0.0.0/8 via BGP em sua interface virtual de trânsito.

Não é permitido ter sobreposições de prefixos permitidos quando houver vários gateways de trânsito associados a um gateway do Direct Connect. Por exemplo, se você tiver um gateway de trânsito com uma lista de prefixos permitidos que inclua 10.1.0.0/16 e um segundo gateway de trânsito com uma lista de prefixos permitidos que inclua 10.2.0.0/16 e 0.0.0.0/0, você não poderá definir as associações do segundo gateway de trânsito como 0.0.0.0/0. Como 0.0.0.0/0 inclui todas as redes IPv4, não é possível configurar 0.0.0.0/0 se houver vários gateways de trânsito associados a um

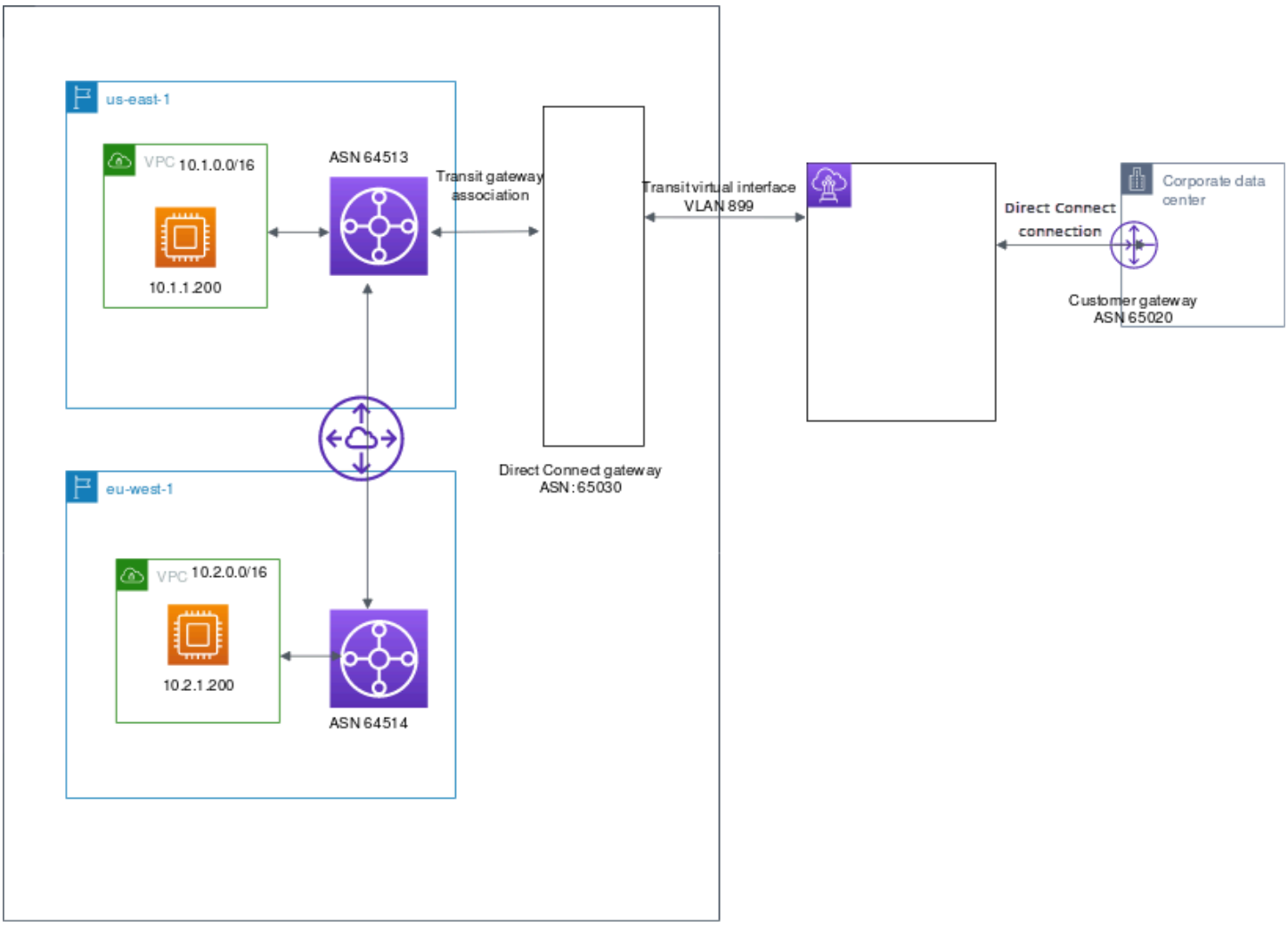
gateway do Direct Connect. Um erro será retornado indicando que as rotas permitidas se sobrepõem a uma ou mais rotas permitidas existentes no gateway do Direct Connect.

Quando você remover ou adicionar um prefixo permitido, o tráfego que não usar esse prefixo não será afetado. Durante as atualizações, o status muda de `associated` para `updating`. A modificação de um prefixo existente pode atrasar ou reduzir somente o tráfego que usa esse prefixo.

Exemplo: permitido em prefixos em uma configuração de gateway de trânsito

Considere a configuração na qual você tem instâncias em duas regiões diferentes da AWS que precisam acessar o data center corporativo. É possível usar os seguintes recursos para essa configuração:

- Um gateway de trânsito em cada região.
- Uma conexão de emparelhamento de gateway de trânsito.
- Um gateway do Direct Connect.
- Uma associação de gateway de trânsito entre um dos gateways de trânsito (o que está em us-east-1) para o gateway do Direct Connect.
- Uma interface virtual de trânsito do local on-premises e do local do Direct Connect.



Configure as opções a seguir para os recursos:

- Gateway do Direct Connect: defina o ASN como 65030. Para obter mais informações, consulte Criação de um gateway do Direct Connect.
- Interface virtual de trânsito: defina a VLAN como 899 e o ASN de par do roteador do cliente como 65020. Para obter mais informações, consulte Criar uma interface virtual de trânsito para o gateway do Direct Connect.
- Associação do gateway do Direct Connect com o gateway de trânsito: defina os prefixos permitidos como 10.0.0.0/8.

  Este bloco CIDR inclui tanto os blocos CIDR da VPC (10.0.0.0/16 e 10.2.0.0/16). Para obter mais informações, consulte Associe ou desassocie um gateway de trânsito com o Direct Connect..
- Rota da VPC: para rotear o tráfego da VPC 10.2.0.0/16, crie uma rota na tabela de rotas da VPC que tenha um destino de 0.0.0.0/0 e a ID do gateway de trânsito como destino. Isso permite que

o tráfego da VPC chegue ao gateway do Direct Connect. Para obter mais informações sobre o roteamento para um gateway de trânsito, consulte Como rotear para um gateway de trânsito no Guia do usuário da Amazon VPC.

Marcar recursos do AWS Direct Connect

Uma tag é um rótulo que um proprietário de recursos atribui aos recursos do Direct Connect. Cada tag consiste de uma chave e um valor opcional, que podem ser definidos. As tags permitem que o proprietário de recursos categorize os recursos do Direct Connect de diferentes maneiras, como por finalidade ou por ambiente. Isso é útil quando há muitos recursos do mesmo tipo; você pode identificar rapidamente um recurso específico com base nas tags atribuídas a ele.

Por exemplo, você tem duas conexões do Direct Connect em uma Região, cada uma em locais diferentes. Conexão `dxcon-11aa22bb` é uma conexão que oferece tráfego de produção e está associada à interface virtual `dxvif-33cc44dd`. Conexão `dxcon-abcabcab` é uma conexão redundante (backup) e está associada à interface virtual `dxvif-12312312`. Convém optar por identificar as conexões e as interfaces virtuais da seguinte maneira para ajudar a diferenciá-las:

ID do recurso	Chave de tag	Valor da tag
`dxcon-11aa22bb`	Finalidade	Produção
	Local	Amsterdã
`dxvif-33cc44dd`	Finalidade	Produção
`dxcon-abcabcab`	Finalidade	Backup
	Local	Frankfurt
`dxvif-12312312`	Finalidade	Backup

Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos. As tags não têm significado semântico atrelado a Direct Connect e são interpretadas estritamente como string de caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

É possível marcar os recursos do Direct Connect a seguir usando o console do Direct Connect, a API do Direct Connect, a AWS CLI, o AWS Tools for Windows PowerShell ou um SDK da AWS. Ao usar essas ferramentas para gerenciar tags, é necessário especificar o nome de recurso da Amazon (ARN) para o recurso. Para obter mais informações sobre ARNs, consulte Nomes de recurso da Amazon (ARNs) no Referência geral da Amazon Web Services.

Recurso	Compatível com tags	Oferece suporte a tags na criação	Oferece suporte a tags que controlam o acesso e a alocação de recursos	Oferece suporte à alocação de custos
Conexões	Sim	Sim	Sim	Sim
Interfaces virtuais	Sim	Sim	Sim	Não
Link aggregation groups (LAG — Grupos de agregação de links)	Sim	Sim	Sim	Sim
Interconexões	Sim	Sim	Sim	Sim
Gateways Direct Connect	Sim	Sim	Sim	Não

Restrições de tag

As seguintes regras e restrições se aplicam a tags:

- Número máximo de tags por recurso: 50
- Comprimento máximo da chave: 128 caracteres Unicode
- Comprimento máximo de valor: 265 caracteres Unicode
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.

- O prefixo `aws:` é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com o prefixo `aws:`. As tags com chave de tag com o prefixo `aws:` não são contabilizadas para o limite de tags por recurso.
- Os caracteres permitidos são letras, espaços e números representáveis em UTF-8, além dos seguintes caracteres especiais: + - = . _ : / @
- Somente o proprietário do recurso pode adicionar ou remover tags. Por exemplo, se houver uma conexão hospedada, o parceiro não poderá adicionar, remover ou visualizar as tags.
- As tags de alocação de custos são compatíveis somente com conexões, interconexões e LAGs. Para obter informações sobre como usar tags com o gerenciamento de custos, consulte Usar tags de alocação de custos no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS.

Trabalhar com tags usando CLI ou a API

Use o seguinte para adicionar, atualizar, listar e excluir as tags para seus recursos.

Tarefa	API	CLI
Adicione ou sobrescreva uma ou mais tags.	TagResource	tag-resource
Exclua uma ou mais tags.	UntagResource	untag-resource
Descreva uma ou mais tags.	DescribeTags	describe-tags

Exemplos

Use o comando tag-resource para marcar a conexão `dxcon-11aa22bb`.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Use o comando describe-tags para descrever as tags da conexão `dxcon-11aa22bb`.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Use o comando untag-resource para remover uma tag da conexão `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Segurança em AWS Direct Connect

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Direct Connect, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar Direct Connect. Os tópicos a seguir mostram como configurar para atender Direct Connect aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus Direct Connect recursos.

Tópicos

Proteção de dados no AWS Direct Connect

O AWS modelo de responsabilidade compartilhada se aplica à proteção de dados no Direct Connect. Conforme descrito nesse modelo, AWS é responsável por proteger a infraestrutura global

que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure os logs de API e atividade do usuário com AWS CloudTrail. Para obter informações sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte Working with CloudTrail trails no Guia do usuário do AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui trabalhar com a Direct Connect ou outros Serviços da AWS usando o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Consulte mais informações sobre proteção de dados na publicação do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Tópicos

- Privacidade do tráfego entre redes em AWS Direct Connect
- Criptografia em AWS Direct Connect

Privacidade do tráfego entre redes em AWS Direct Connect

Tráfego entre clientes de serviço e on-premises e as aplicações

Você tem duas opções de conectividade entre sua rede privada e AWS:

- Uma associação a um AWS Site-to-Site VPN. Para obter mais informações, consulte Segurança da infraestrutura.
- Uma associação para VPCs. Para obter mais informações, consulte Associações de gateways privados virtuais e Associações de gateways de trânsito.

Tráfego entre AWS recursos na mesma região

Você tem duas opções de conectividade:

- Uma associação a um AWS Site-to-Site VPN. Para obter mais informações, consulte Segurança da infraestrutura.
- Uma associação para VPCs. Para obter mais informações, consulte Associações de gateways privados virtuais e Associações de gateways de trânsito.

Criptografia em AWS Direct Connect

AWS Direct Connect não criptografa o tráfego que está em trânsito por padrão. Para criptografar os dados em trânsito que passam AWS Direct Connect, você deve usar as opções de criptografia de trânsito desse serviço. Para saber mais sobre a criptografia do tráfego de instâncias do EC2, consulte Criptografia em trânsito no Guia do usuário do Amazon EC2.

Com AWS Direct Connect e AWS Site-to-Site VPN, você pode combinar uma ou mais conexões de rede AWS Direct Connect dedicadas com o Amazon VPC VPN. Essa combinação fornece uma conexão privada IPsec criptografada que também reduz os custos da rede, aumenta a taxa

de transferência da largura de banda e fornece uma experiência de rede mais consistente do que as conexões VPN baseadas na Internet. Para obter mais informações, consulte Opções de conectividade da Amazon VPC-to-Amazon VPC.

O MAC Security (MACsec) é um padrão IEEE que fornece confidencialidade, integridade e autenticidade da origem dos dados. Você pode usar Direct Connect conexões que oferecem suporte MACsec para criptografar seus dados do data center corporativo até o Direct Connect local. Para obter mais informações, consulte Segurança MAC (MACsec).

Gerenciamento de identidade e acesso para o Direct Connect

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do Direct Connect. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso do Direct Connect).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Funcionamento do Direct Connect com o IAM)

- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para o Direct Connect)

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.

- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Funcionamento do Direct Connect com o IAM

Antes de usar o IAM para gerenciar o acesso ao Direct Connect, saiba quais recursos do IAM estão disponíveis para uso com o Direct Connect.

Recursos do IAM que você pode usar com o Direct Connect

Recurso do IAM	Compatibilidade com o Direct Connect
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim

Recurso do IAM	Compatibilidade com o Direct Connect
Perfis vinculados a serviço	Não

Para ter uma visão de alto nível de como o Direct Connect e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para o Direct Connect

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o Direct Connect

Para visualizar exemplos de políticas do Direct Connect baseadas em identidade, consulte Exemplos de políticas baseadas em identidade para o Direct Connect.

Políticas baseadas em recursos no Direct Connect

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de política para o Direct Connect

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para obter uma lista de ações do Direct Connect, consulte Actions Defined by Direct Connect na Referência de autorização de serviço.

As ações de política no Direct Connect usam o seguinte prefixo antes da ação:

```
Direct Connect
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Recursos de política para o Direct Connect

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Direct Connect e seus ARNs, consulte Recursos definidos pelo Direct Connect na Referência da AWS Direct Connect API. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Direct Connect.

Para visualizar exemplos de políticas do Direct Connect baseadas em identidade, consulte Exemplos de políticas baseadas em identidade para o Direct Connect.

Para visualizar exemplos de políticas do Direct Connect baseadas em recurso, consulte Exemplos de política baseada em identidade do Direct Connect usando condições baseadas em tag.

Chaves de condição de política para o Direct Connect

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do Direct Connect, consulte Chaves de condição para o Direct Connect na Referência de API do AWS Direct Connect . Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Actions, Resources, and Condition Keys for Direct Connect na Referência de autorização de serviço.

Para visualizar exemplos de políticas do Direct Connect baseadas em identidade, consulte Exemplos de políticas baseadas em identidade para o Direct Connect.

ACLs no Direct Connect

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com o Direct Connect

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Direct Connect

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões de entidade principal entre serviços para o Direct Connect

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Perfis de serviço para o Direct Connect

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Direct Connect. Edite perfis de serviço somente quando o Direct Connect fornecer orientação para tal.

Perfis vinculados a serviço para o Direct Connect

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o Direct Connect

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Direct Connect. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Direct Connect, incluindo o formato ARNs de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do Direct Connect na Referência de autorização de serviço.

Tópicos

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Direct Connect em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando

SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Ações, recursos e condições do Direct Connect

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. O Direct Connect oferece suporte a ações, recursos e chaves de condição específicos. Para conhecer todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Direct Connect usam o seguinte prefixo antes da ação: `directconnect:`. Por exemplo, para conceder permissão a alguém para executar uma instância do Amazon

EC2 com a operação da API `DescribeVpnGateways` do Amazon EC2, inclua a ação `ec2:DescribeVpnGateways` na política da pessoa. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Direct Connect define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

O exemplo de política a seguir concede acesso de Direct Connect leitura a.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

O exemplo de política a seguir concede acesso total Direct Connect a.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Para ver uma lista de ações do Direct Connect, consulte Ações definidas pelo Direct Connect no Guia do usuário do IAM.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

O Direct Connect usa o seguinte ARNs:

Recurso de conexão direta ARNs

Tipo de recurso	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Para obter mais informações sobre o formato de ARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

Por exemplo, para especificar a interface `dxcon-11aa22bb` em sua instrução, use o seguinte ARN:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Para especificar todas as instâncias de banco de dados que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Algumas ações do Direct Connect, como as ações para a criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, é necessário utilizar o caractere curinga (*).

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Direct Connect e seus ARNs, consulte Tipos de recursos definidos por Direct Connect no Guia do usuário do IAM. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Direct Connect.

Se um ARN de recurso ou um padrão de ARN de recurso diferente do `*` especificado no `Resource` campo da declaração de política do IAM para DescribeConnections,,, ou DescribeVirtualInterfaces DescribeDirectConnectGateways DescribeInterconnects, o especificado não `Effect` ocorrerá DescribeLags, a menos que o ID do recurso correspondente também seja passado na chamada da API. No entanto, se você fornecer `*` como recurso, em vez de um ID de recurso específico na instrução de política do IAM, o `Effect` especificado funcionará.

No exemplo a seguir, nenhum dos `Effect` especificados será bem-sucedido se a ação `DescribeConnections` for chamada sem um `connectionId` passado na solicitação.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
```

```
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

No entanto, no exemplo a seguir, `"Effect": "Allow"` será bem-sucedido para a ação `DescribeConnections`, pois `*` foi fornecido para o campo `Resource` da instrução de política do IAM, independentemente de `connectionId` ter sido especificado na solicitação.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

Chaves de condição

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

O Direct Connect define seu próprio conjunto de chaves de condição e também é compatível com o uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia do usuário do IAM.

Você pode usar chaves de condição com o recurso de tag. Para obter mais informações, consulte Exemplo: restrição de acesso a uma Região específica.

Para ver uma lista das chaves de condição do Direct Connect, consulte Chaves de condição para o Direct Connect no Guia do usuário do IAM. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte Ações definidas pelo Direct Connect.

Uso do console do Direct Connect

Para acessar o console do Direct Connect, você precisa ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Direct Connect em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como planejado para entidades (usuários ou perfis) com essa política.

Para garantir que essas entidades ainda possam usar o console do Direct Connect, anexe também a seguinte política AWS gerenciada às entidades. Para obter mais informações, consulte Adição de permissões a um usuário no Manual do usuário do IAM:

```
directconnect
```

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acesso somente para leitura a Direct Connect

O exemplo de política a seguir concede acesso de Direct Connect leitura a.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Acesso total ao Direct Connect

O exemplo de política a seguir concede acesso total Direct Connect a.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplos de política baseada em identidade do Direct Connect usando condições baseadas em tag

É possível controlar o acesso a recursos e solicitações usando condições de chave de tag. Também é possível usar uma condição em sua política do IAM para controlar se chaves de tag específicas podem ser usadas em um recurso ou em uma solicitação.

Para obter informações sobre como usar tags com políticas do IAM, consulte Como controlar o acesso com tags no Guia do usuário do IAM.

Associar interfaces virtuais do Direct Connect com base em tags

O exemplo a seguir mostra como você pode criar uma política que permite associar uma interface virtual somente se a tag contiver a chave de ambiente e os valores de produção ou pré-produção.

JSON

```
      {
     "Version":"2012-10-17",
```

```
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "directconnect:AssociateVirtualInterface"
        ],
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/environment": [
              "preprod",
              "production"
            ]
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": "directconnect:DescribeVirtualInterfaces",
        "Resource": "*"
      }
    ]
  }
```

Controlar o acesso a solicitações com base em tags

Você pode usar condições em suas políticas do IAM para controlar quais pares de chave-valor de tag podem ser passados em uma solicitação que marca um AWS recurso. O exemplo a seguir mostra como você pode criar uma política que permita usar a Direct Connect TagResource ação para anexar tags a uma interface virtual somente se a tag contiver a chave de ambiente e os valores de pré-produção ou produção. Como uma prática recomendada, use o modificador `ForAllValues` com a chave de condição `aws:TagKeys` para indicar que somente a chave de ambiente é permitida na solicitação.

JSON

```
  {
      "Version":"2012-10-17",
      "Statement": {
          "Effect": "Allow",
```

```
            "Action": "directconnect:TagResource",
            "Resource": "arn:aws:directconnect:*:*:dxvif/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": [
                        "preprod",
                        "production"
                    ]
                },
                "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
            }
        }
    }
```

Controlar as chaves de tag

É possível usar uma condição em suas políticas do IAM para controlar se chaves de tag específicas podem ser usadas em um recurso ou em uma solicitação.

O exemplo a seguir mostra como você pode criar uma política que permite marcar recursos, mas somente com a chave de tag de ambiente.

JSON

```
    {
     "Version":"2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "directconnect:TagResource",
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringEquals": {
           "aws:TagKeys": [
             "environment"
           ]
         }
       }
     }
    }
```

Funções vinculadas a serviços para Direct Connect

AWS Direct Connect usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. Direct Connect As funções vinculadas ao serviço são predefinidas Direct Connect e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração Direct Connect porque você não precisa adicionar manualmente as permissões necessárias. Direct Connect define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só Direct Connect pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus Direct Connect recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para Direct Connect

Direct Connect usa uma função vinculada ao serviço chamada. `AWSServiceRoleForDirectConnect` Isso Direct Connect permite recuperar o MACSec segredo armazenado AWS Secrets Manager em seu nome.

O perfil vinculado ao serviço `AWSServiceRoleForDirectConnect` confia nos seguintes serviços para aceitar o perfil:

- `directconnect.amazonaws.com`

O perfil vinculado a serviço `AWSServiceRoleForDirectConnect` usa a política gerenciada `AWSDirectConnectServiceRolePolicy`.

É necessário configurar as permissões para permitir que uma entidade do IAM (como um usuário, grupo ou perfil) crie, edite ou exclua uma função vinculada ao serviço. Para que o perfil vinculado a serviço `AWSServiceRoleForDirectConnect` seja criado com êxito, a identidade do IAM com a

qual você usa o Direct Connect deve ter as permissões necessárias. Para conceder as permissões necessárias, anexe a política a seguir à identidade do IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Para obter mais informações, consulte Permissões do perfil vinculado a serviço no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para Direct Connect

Você não precisa criar manualmente uma função vinculada ao serviço. AWS Direct Connect cria a função vinculada ao serviço para você. Quando você executa o `associate-mac-sec-key` comando, AWS cria uma função vinculada Direct Connect ao serviço que permite recuperar os MACsec segredos armazenados em AWS Secrets Manager seu nome na Console de gerenciamento da AWS, na ou na AWS CLI API. AWS

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar o mesmo processo para recriar a função na sua conta. Direct Connect cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar um perfil vinculado a serviço com o caso de uso do AWS Direct Connect. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `directconnect.amazonaws.com` serviço. Para saber mais, consulte Criar um perfil vinculado a serviço no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editando uma função vinculada ao serviço para Direct Connect

Direct Connect não permite que você edite a função `AWSServiceRoleForDirectConnect` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para Direct Connect

Você não precisa excluir manualmente a função `AWSServiceRoleForDirectConnect`. Ao excluir sua função vinculada ao serviço, você deve excluir todos os recursos associados que estão armazenados no serviço AWS Secrets Manager web. A Console de gerenciamento da AWS, a AWS CLI, ou a AWS API, Direct Connect limpa os recursos e exclui a função vinculada ao serviço para você.

Também é possível usar o console do IAM para excluir o perfil vinculado a serviço. Para fazer isso, primeiro você deve limpar manualmente os recursos de seu perfil vinculado a serviço e depois excluí-lo manualmente.

> **Note**
>
> Se o Direct Connect serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente executar a operação novamente.

Para excluir Direct Connect recursos usados pelo **`AWSServiceRoleForDirectConnect`**

1. Remova a associação entre todas MACsec as chaves e conexões. Para obter mais informações, consulte the section called “Remover a associação entre uma chave MACsec secreta e uma conexão”.
2. Remova a associação entre todas MACsec as chaves LAGs e. Para obter mais informações, consulte the section called “Remover a associação entre uma chave MACsec secreta e um LAG”.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForDirectConnect` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a Direct Connect serviços

Direct Connect suporta o uso de funções vinculadas a serviços em todos os Regiões da AWS lugares em que o recurso MAC Security está disponível. Para obter mais informações, consulte Locais do AWS Direct Connect.

AWS políticas gerenciadas para AWS Direct Connect

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: AWSDirect ConnectFullAccess

É possível anexar a política `AWSDirectConnectFullAccess` às identidades do IAM. Essa política concede permissões que permitem acesso total Direct Connect a.

Para visualizar as permissões para esta política, consulte AWSDirectConnectFullAccess no Console de gerenciamento da AWS.

AWS política gerenciada: AWSDirect ConnectReadOnlyAccess

É possível anexar a política `AWSDirectConnectReadOnlyAccess` às identidades do IAM. Essa política concede permissões que permitem acesso somente para leitura a. Direct Connect

Para visualizar as permissões para esta política, consulte AWSDirectConnectReadOnlyAccess no Console de gerenciamento da AWS.

AWS política gerenciada: AWSDirect ConnectServiceRolePolicy

Essa política é anexada à função vinculada ao serviço nomeada AWSServiceRoleForDirectConnectpara permitir Direct Connect a recuperação de segredos de segurança MAC em seu nome. Para obter mais informações, consulte the section called “Perfis vinculados ao serviço”.

Para visualizar as permissões para esta política, consulte AWSDirectConnectServiceRolePolicy no Console de gerenciamento da AWS.

Direct Connect atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas Direct Connect desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do Direct Connect documento.

Alteração	Descrição	Data
AWSDirectConnectServiceRolePolicy - Nova política	Para oferecer suporte à segurança MAC, a função AWSServiceRoleForDirectConnectvinculada ao serviço foi adicionada.	31 de março de 2021
Direct Connect começou a rastrear alterações	Direct Connect começou a rastrear as alterações em suas políticas AWS gerenciadas.	31 de março de 2021

Solução de problemas de identidade e acesso do Direct Connect

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Direct Connect e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Direct Connect
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Direct Connect

Não tenho autorização para executar uma ação no Direct Connect

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `directconnect:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `directconnect:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, será necessário atualizar suas políticas para permitir a transmissão de um perfil para o Direct Connect.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro do exemplo a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Direct Connect. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Direct Connect

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Direct Connect é compatível com esses recursos, consulte Funcionamento do Direct Connect com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Registrar em log e monitorar no AWS Direct Connect

Você pode usar as seguintes ferramentas de monitoramento automatizadas para observar o Direct Connect e gerar relatórios quando algo estiver errado:

- Alarmes do Amazon CloudWatch: observe uma só métrica durante um período especificado. Execute uma ou mais ações com base no valor da métrica, relativa a um limite especificado em um número de períodos. A ação é uma notificação enviada para um tópico do Amazon SNS. Os alarmes do CloudWatch não invocam ações simplesmente por estarem em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte Monitore com a Amazon CloudWatch.
- Monitoramento de log do AWS CloudTrail: compartilhe arquivos de log entre contas e monitore arquivos de log do CloudTrail em tempo real enviando-os para o CloudWatch Logs. Também é possível criar aplicativos de processamento de log em Java e confirmar se os arquivos de log não foram alterados após a entrega pelo CloudTrail. Para obter mais informações, consulte Registre chamadas de Direct Connect API usando AWS CloudTrail e Como trabalhar com arquivos de log do CloudTrail no Guia do usuário do AWS CloudTrail.

Para obter mais informações, consulte Monitoramento de recursos do Direct Connect.

Validação de conformidade do AWS Direct Connect

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de Conformidade da AWS.

É possível baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. Para ter mais informações sobre sua responsabilidade pela conformidade ao usar Serviços da AWS, consulte a documentação da AWS sobre segurança.

Resiliência no AWS Direct Connect

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, as quais são conectadas com baixa latência, alto throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Além da infraestrutura global da AWS, o Direct Connect oferece vários atributos para ajudar a oferecer suporte às suas necessidades de resiliência de dados e backup.

Para obter informações sobre como usar a VPN com o AWS Direct Connect, consulte VPN com o AWS Direct Connect.

Failover

O kit de ferramentas de resiliência do AWS Direct Connect fornece um assistente de conexão com vários modelos de resiliência que ajuda você a solicitar conexões dedicadas para atingir seu objetivo de SLA. Você seleciona um modelo de resiliência e o kit de ferramentas de resiliência do AWS Direct

Connect o orientará durante o processo de pedido de conexão dedicada. Os modelos de resiliência são projetados para garantir que você tenha o número apropriado de conexões dedicadas em vários locais.

- Resiliência máxima: você pode alcançar a resiliência máxima para workloads críticas usando conexões separadas que terminem em dispositivos distintos em mais de um local. Esse modelo fornece resiliência contra falhas de dispositivo, conectividade e localização completa.
- Alta resiliência: você pode obter alta resiliência para workloads críticas usando duas conexões individuais para vários locais. Esse modelo fornece resiliência contra falhas de conectividade causadas por um corte de fibra ou uma falha de dispositivo. Ele também ajuda a evitar uma falha completa no local.
- Desenvolvimento e teste: você pode obter resiliência de desenvolvimento e teste para workloads não críticas usando conexões distintas que terminem em dispositivos distintos em um único local. Esse modelo fornece resiliência contra falhas de dispositivo, mas não fornece resiliência contra falhas de localização.

Para obter mais informações, consulte the section called “AWS Direct Connect Kit de ferramentas de resiliência”.

Segurança da infraestrutura no Direct Connect

Por ser um serviço gerenciado, o AWS Direct Connect é protegido pelos procedimentos de segurança da rede global da AWS. Você usa chamadas de API publicadas do AWS para acessar a Direct Connect por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.2 ou posterior. Recomendamos o TLS 1.3. Os clientes também devem ter compatibilidade com conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece compatibilidade com esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você pode chamar essas operações de API de qualquer local da rede, mas o Direct Connect oferece suporte a políticas de acesso com base em recursos, que podem incluir restrições com base no endereço IP de origem. Você também pode usar políticas do Direct Connect para controlar

o acesso de Amazon Virtual Private Cloud (Amazon VPC) endpoints ou de VPCs específicas. Efetivamente, isso isola o acesso à rede para um determinado recurso do Direct Connect apenas da VPC específica dentro da rede da AWS. Por exemplo, consulte the section called “Exemplos de políticas baseadas em identidade para o Direct Connect”.

Segurança do Protocolo de Gateway da Borda (BGP)

A Internet depende em grande parte do BGP para rotear informações entre sistemas de rede. Às vezes, o roteamento do BGP pode ser suscetível a ataques maliciosos ou a sequestro do BGP. Para entender como a AWS atua para proteger com mais segurança sua rede contra o sequestro do BGP, consulte Como a AWS está ajudando a proteger o roteamento da Internet.

Uso da Direct Connect CLI

Você pode usar a AWS CLI para criar e trabalhar com recursos do Direct Connect.

O exemplo a seguir usa os comandos da AWS CLI para criar uma conexão do Direct Connect. Você também pode fazer download da Letter of Authorization and Connecting Facility Assignment (LOA-CFA – Carta de autorização e atribuição da instalação de conexão) ou provisionar uma interface virtual privada ou pública.

Antes de começar, certifique-se de que você tenha instalado e configurado a AWS CLI. Para obter mais informações, consulte o Guia do usuário do AWS Command Line Interface.

Conteúdo

Etapa 1: Criar uma conexão

A primeira etapa é enviar uma solicitação de conexão. Certifique-se de que você saiba a velocidade da porta de que precisa e o local do Direct Connect. Para obter mais informações, consulte Conexões dedicadas e hospedadas.

Para criar uma solicitação de conexão

1. Descreva os locais do Direct Connect da sua Região atual. Na saída retornada, anote o código do local no qual você deseja estabelecer a conexão.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
```

```
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
    ]
}
```

2. Crie a conexão e especifique um nome, a velocidade da porta e o código do local. Na saída retornada, anote a ID da conexão. Você precisa da ID para obter a LOA-CFA na próxima etapa.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Etapa 2: Baixar a LOA-CFA

Depois que tiver solicitado uma conexão, você poderá obter a LOA-CFA usando o comando `describe-loa`. A saída é codificada em base64. Você deve extrair o conteúdo LOA relevante, decodificá-lo e criar um arquivo PDF.

Para obter a LOA-CFA usando Linux ou macOS

Neste exemplo, a parte final do comando decodifica o conteúdo usando o utilitário base64 e envia a saída para um arquivo PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Para obter a LOA-CFA usando o Windows

Neste exemplo, a saída é extraída para um arquivo chamado myLoaCfa.base64. O segundo comando usa o utilitário `certutil` para decodificar o arquivo e enviar a saída a um arquivo PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Depois que você tiver baixado a LOA-CFA, envie-a para o provedor de rede ou colocação.

Etapa 3: Criar uma interface virtual e obter a configuração do roteador

Depois de ter feito o pedido de uma conexão do Direct Connect, você deverá criar uma interface virtual para começar a usá-la. Crie uma interface virtual privada para se conectar à VPC. Outra opção é criar uma interface virtual pública para se conectar aos serviços da AWS que não estejam em uma VPC. Você pode criar uma interface virtual compatível com tráfego IPv4 ou IPv6.

Antes de começar, certifique-se de que você tenha lido os pré-requisitos em the section called “Pré-requisitos para interfaces virtuais”.

Ao criar uma interface virtual usando a AWS CLI, a saída inclui informações de configuração do roteador genéricas. Para criar uma configuração de roteador específica para o dispositivo, use o console do Direct Connect. Para obter mais informações, consulte Baixar arquivo de configuração do roteador.

Para criar uma interface virtual privada

1. Obtenha a ID do gateway privado virtual (vgw-xxxxxxxx) conectado à VPC. Você precisará da ID para criar a interface virtual na próxima etapa.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
                       "Key": "Name"
   ```

```
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Crie uma interface virtual privada. Você deve especificar um nome, uma ID de VLAN e um Autonomous System Number (ASN - Número de sistema autônomo) BGP.

   Para tráfego IPv4, você precisa de endereços IPv4 privados para cada fim de sessão de mesmo nível BGP. Você pode especificar os próprios endereços IPv4 ou permitir que a Amazon gere endereços para você. No exemplo a seguir, os endereços IPv4 são gerados para você.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
```

```
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

Para criar uma interface virtual privada compatível com tráfego IPv6, use o mesmo comando acima e especifique `ipv6` para o parâmetro `addressFamily`. Você não pode especificar os próprios endereços IPv6 para a sessão de mesmo nível BGP; a Amazon aloca endereços IPv6 para você.

3. Para visualizar as informações de configuração do roteador em formato XML, descreva a interface virtual criada por você. Use o parâmetro `--query` para extrair as informações `customerRouterConfig` e o parâmetro `--output` para organizar o texto em linhas delimitadas por tabulações.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
```

```
</logical_connection>
```

Para criar uma interface virtual pública

1. Para criar uma interface virtual pública, você deve especificar um nome, uma ID VLAN e um ASN BGP.

   Para tráfego IPv4, você também deve especificar endereços IPv4 públicos para cada fim de sessão de mesmo nível BGP e rotas IPv4 que anunciará via BGP. O exemplo a seguir cria uma interface virtual pública para tráfego IPv4.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
```

```
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Para criar uma interface virtual pública compatível com tráfego IPv6, você pode especificar rotas IPv6 que anunciará via BGP. Você não pode especificar endereços IPv6 para a sessão de mesmo nível; a Amazon aloca endereços IPv6 para você. O exemplo a seguir cria uma interface virtual pública para tráfego IPv6.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. Para visualizar as informações de configuração do roteador em formato XML, descreva a interface virtual criada por você. Use o parâmetro `--query` para extrair as informações `customerRouterConfig` e o parâmetro `--output` para organizar o texto em linhas delimitadas por tabulações.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
```

```
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Registre chamadas de Direct Connect API usando AWS CloudTrail

Direct Connect é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em Direct Connect. CloudTrail captura todas as chamadas de API Direct Connect como eventos. As chamadas capturadas incluem chamadas do Direct Connect console e chamadas de código para as operações Direct Connect da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. Direct Connect Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita Direct Connect, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Direct Connect informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre em Direct Connect, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para Direct Connect, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas Direct Connect as ações são registradas CloudTrail e documentadas na Referência da Direct Connect API. Por exemplo, chamadas para as `CreatePrivateVirtualInterface` ações `CreateConnection` e geram entradas nos arquivos de CloudTrail log.

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

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

Para obter mais informações, consulte Elemento do CloudTrail `userIdentity`.

Entenda as entradas do arquivo de Direct Connect log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

A seguir estão exemplos de registros de CloudTrail log para Direct Connect.

Example Exemplo: CreateConnection.

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
```

```
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Exemplo: CreatePrivateVirtualInterface.

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
```

```
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
```

```
    },
    ...
  ]
}
```

Example Exemplo: DescribeConnections.

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example Exemplo: DescribeVirtualInterfaces.

```
{
    "Records": [
    {
```

```
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

Monitore Direct Connect os recursos

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e da performance dos seus recursos do Direct Connect. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. Entretanto, antes de iniciar o monitoramento do Direct Connect, é recomendável criar um plano de monitoramento que contenha respostas para as seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos devem ser monitorados?
- Com que frequência esses recursos devem ser monitorados?
- Quais ferramentas de monitoramento você pode usar?
- Quem realiza as tarefas de monitoramento?
- Quem deve ser notificado quando algo der errado?

A próxima etapa consiste em estabelecer uma linha de base para a performance normal do Direct Connect em seu ambiente, medindo a performance em diferentes momentos e sob diferentes condições de carga. À medida que você monitora o Direct Connect, armazene dados históricos de monitoramento. Assim, poderá compará-los com os dados de desempenho atuais, identificar padrões de desempenho normais e anomalias de desempenho, e elaborar métodos para resolver problemas.

Para estabelecer uma linha de base, você deve monitorar o uso, o estado e a integridade das suas conexões físicas do Direct Connect.

Tópicos

Ferramentas de monitoramento

AWS fornece várias ferramentas que você pode usar para monitorar uma Direct Connect conexão. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

É possível usar as seguintes ferramentas de monitoramento automatizado para acompanhar o Direct Connect e efetuar notificações quando algo estiver errado:

- Amazon CloudWatch Alarms — Observe uma única métrica durante um período de tempo especificado por você. Execute uma ou mais ações com base no valor da métrica, relativa a um limite especificado em um número de períodos. A ação é uma notificação enviada para um tópico do Amazon SNS. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para obter informações sobre as métricas e dimensões disponíveis, consulte Monitore com a Amazon CloudWatch.
- AWS CloudTrail Monitoramento de registros — compartilhe arquivos de log entre contas e monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs. Também é possível criar aplicativos de processamento de log em Java e confirme se os arquivos de log não foram alterados após a entrega pelo CloudTrail. Para obter mais informações, consulte Registrar chamadas de API da Trabalhar com arquivos de CloudTrail log no Guia AWS CloudTrail do usuário.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento de uma Direct Connect conexão envolve o monitoramento manual dos itens que os CloudWatch alarmes não cobrem. O Direct Connect e os painéis do CloudWatch console fornecem uma at-a-glance visão do estado do seu AWS ambiente.

- O Direct Connect console mostra:
  - Status da conexão (consulte a coluna Estado)
  - Status da interface virtual (consulte a coluna Estado)
- A página CloudWatch inicial mostra:
  - Alertas e status atual
  - Gráficos de alertas e recursos
  - Estado de integridade do serviço

  Além disso, você pode usar CloudWatch para fazer o seguinte:
  - Criar painéis personalizados para monitorar os serviços com os quais você se preocupa.
  - Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências.

- Pesquise e navegue por todas as suas métricas AWS de recursos.
- Criar e editar alertas para ser notificado sobre problemas.

Monitore com a Amazon CloudWatch

Você pode monitorar Direct Connect conexões físicas e interfaces virtuais usando CloudWatch. CloudWatch coleta dados brutos do Direct Connect e os processa em métricas legíveis. Por padrão, CloudWatch fornece dados métricos do Direct Connect em intervalos de 5 minutos. Os dados de métricas em cada intervalo são uma agregação de, pelo menos, duas amostras coletadas durante esse intervalo.

Para obter informações detalhadas sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon. Você também pode monitorar seus serviços CloudWatch para ver quais estão usando recursos. Para obter mais informações, consulte AWS serviços que publicam CloudWatch métricas.

Conteúdo

Direct Connect métricas e dimensões

As métricas estão disponíveis para conexões Direct Connect físicas e interfaces virtuais.

Direct Connect Métricas de conexão

As métricas apresentadas a seguir estão disponíveis ao usar conexões dedicadas do Direct Connect.

Métrica	Description
`ConnectionState`	O estado da conexão. 1 indica ativa e 0 indica inativa. Esta métrica está disponível para conexões dedicadas e hospedadas.

Métrica	Description
	Note Essa métrica também está disponível nas contas do proprietário da interface virtual hospedada, além das contas do proprietário da conexão. Unidades: não há unidades retornadas para essa métrica.
`ConnectionBpsEgress`	A taxa de bits para dados de saída do AWS lado da conexão. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão, mínimo de 1 minuto). Você pode alterar o agregado padrão. Esta métrica pode não estar disponível para uma nova conexão ou quando um dispositivo é reinicial izado. A métrica começa quando a conexão é usada para enviar ou receber tráfego. Unidades: bits por segundo
`ConnectionBpsIngress`	A taxa de bits dos dados de entrada ao AWS lado da conexão. Esta métrica pode não estar disponível para uma nova conexão ou quando um dispositivo é reinicial izado. A métrica começa quando a conexão é usada para enviar ou receber tráfego. Unidades: bits por segundo

Métrica	Description
`ConnectionPpsEgress`	` A taxa de pacotes para dados de saída do AWS lado da conexão. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão, mínimo de 1 minuto). Você pode alterar o agregado padrão. Esta métrica pode não estar disponível para uma nova conexão ou quando um dispositivo é reinicial izado. A métrica começa quando a conexão é usada para enviar ou receber tráfego. Unidades: pacotes por segundo
`ConnectionPpsIngress`	A taxa de pacotes para dados de entrada no AWS lado da conexão. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão, mínimo de 1 minuto). Você pode alterar o agregado padrão. Esta métrica pode não estar disponível para uma nova conexão ou quando um dispositivo é reinicial izado. A métrica começa quando a conexão é usada para enviar ou receber tráfego. Unidades: pacotes por segundo
`ConnectionCRCErrorCount`	Esta contagem não está mais em uso. Use `ConnectionErrorCount` em vez disso.

Métrica	Description
`ConnectionErrorCount`	A contagem total de erros para todos os tipos de erros de nível MAC registrados pelo AWS dispositivo. O total inclui erros de verificação de redundância cíclica (CRC). A causa raiz desses erros pode estar no lado do cliente ou no AWS lado do cliente. Essa métrica é a contagem de erros que ocorreram desde o último ponto de dados relatado. Quando houver erros na interface, a métrica relatará valores diferentes de zero. Para obter a contagem total de todos os erros do intervalo selecionado em CloudWatch, por exemplo, 5 minutos, aplique a estatística “soma”. O valor da métrica será definido como 0 quando os erros na interface cessarem. **Note** Essa métrica substitui `ConnectionCRCErrorCount`, que não está mais em uso. Unidades: contagem
`ConnectionLightLevelTx`	Indica a integridade da conexão de fibra para tráfego de saída (saída) do AWS lado da conexão. Há duas dimensões para essa métrica. Para obter mais informações, consulte Dimensões disponíveis do Direct Connect. Unidades: dBm

Métrica	Description
`ConnectionLightLevelRx`	Indica a integridade da conexão de fibra para tráfego de entrada (entrada) na AWS lateral da conexão. Há duas dimensões para essa métrica. Para obter mais informações, consulte Dimensões disponíveis do Direct Connect. Unidades: dBm
`ConnectionEncryptionState`	Indica o status de criptografia da conexão. O valor 1 indica que a criptografia da conexão está up, enquanto 0 indica que a criptografia da conexão está down. Quando essa métrica é aplicada a um LAG, o valor 1 indica que todas as conexões no LAG têm criptografia up, enquanto 0 indica que a criptografia de pelo menos uma conexão do LAG está down.
`ConnectionDiscardsPpsEgress`	A taxa de descarte de pacotes para dados de saída do AWS lado da conexão. Essa métrica rastreia pacotes que são descartados devido a estouros de buffer, congestionamento de interface ou outras condições de rede. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão, mínimo de 1 minuto). Você pode alterar o agregado padrão. Unidades: pacotes por segundo

Direct Connect métricas de interface virtual

As métricas a seguir estão disponíveis nas interfaces Direct Connect virtuais.

Métrica	Description
`VirtualInterfaceBpsEgress`	A taxa de bits para dados de saída do AWS lado da interface virtual. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão). Unidades: bits por segundo
`VirtualInterfaceBpsIngress`	A taxa de bits dos dados de entrada ao AWS lado da interface virtual. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão). Unidades: bits por segundo
`VirtualInterfacePpsEgress`	A taxa de pacotes para dados de saída do AWS lado da interface virtual. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão). Unidades: pacotes por segundo
`VirtualInterfacePpsIngress`	A taxa de pacotes para dados de entrada ao AWS lado da interface virtual. O número informado é o agregado (média) ao longo do período especificado (5 minutos por padrão). Unidades: pacotes por segundo

Direct Connect dimensões disponíveis

Você pode filtrar os Direct Connect dados usando as seguintes dimensões.

Dimensão	Description
`ConnectionId`	Esta dimensão está disponível nas métricas para a conexão do Direct Connect e a interface virtual. Essa dimensão filtra os dados pela conexão.
`OpticalLaneNumber`	Esta dimensão filtra os dados de `ConnectionLightLevelTx` e os dados de`ConnectionLightLevelRx` , e filtra os dados pelo número da faixa óptica da conexão do Direct Connect..
`VirtualInterfaceId`	Esta dimensão está disponível nas métricas da interface virtual do Direct Connect e filtra os dados pela interface virtual.

Tópicos

- Visualização de métricas do CloudWatch para o Direct Connect
- Criação de alarmes do Amazon CloudWatch para monitorar conexões do Direct Connect

Visualização de métricas do CloudWatch para o Direct Connect

O Direct Connect envia as métricas apresentadas a seguir referentes às suas conexões do Direct Connect. Em seguida, o Amazon CloudWatch agrega esses pontos de dados em intervalos de um minuto ou de cinco minutos. Por padrão, os dados de métricas do Direct Connect são gravados no CloudWatch em intervalos de cinco minutos.

> **Note**
>
> Ao monitorar o Direct Connect por meio do CloudWatch, você pode solicitar métricas em intervalos de um minuto. No entanto, a frequência real de atualização é controlada pelo CloudWatch. Como o CloudWatch controla o intervalo, o Direct Connect nem sempre pode garantir intervalos menores que cinco minutos.

É possível usar os procedimentos apresentados a seguir para visualizar as métricas das conexões do Direct Connect.

Para exibir métricas usando o console do CloudWatch

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace. Para obter mais informações sobre como usar o Amazon CloudWatch para visualizar as métricas do Direct Connect, incluindo a adição de funções matemáticas ou consultas predefinidas, consulte Como usar métricas do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.

1. Abra o console do CloudWatch, em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Metrics (Métricas) e, em seguida, All metrics (Todas as métricas).
3. Na seção Métricas, escolha DX.
4. Escolha um ConnectionID ou Nome de métrica e, em seguida, escolha qualquer uma das opções a seguir para definir adicionalmente a métrica:

   - Adicionar à pesquisa: adiciona essa métrica aos resultados da pesquisa.
   - Pesquisar somente essa métrica: pesquisa somente essa métrica.
   - Remover do gráfico: remove essa métrica do gráfico.
   - Representar apenas esta métrica no gráfico: representa graficamente somente essa métrica.
   - Representar em gráfico todos os resultados da pesquisa: representa graficamente todas as métricas.
   - Gráfico com consulta SQL: abre o Metrics Insights - construtor de consultas, permitindo que você crie uma consulta SQL para escolher o que deseja representar graficamente. Para obter mais informações sobre o uso do Metric Insights, consulte Consulte suas métricas com o CloudWatch Metrics Insights no Guia do usuário do Amazon CloudWatch.

Para visualizar as métricas usando o console do Direct Connect

1. Abra o console do Direct Connect em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha Connections.
3. Selecione sua conexão.
4. Escolha a guia Monitoramento para exibir as métricas da sua conexão.

Para visualizar métricas usando a AWS CLI

Em um prompt de comando, use o seguinte comando.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Criação de alarmes do Amazon CloudWatch para monitorar conexões do Direct Connect

Você pode criar um alarme do CloudWatch que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Ele envia uma notificação a um tópico do Amazon SNS com base no valor da métrica em relação a um limite especificado em um número de períodos.

Por exemplo, você pode criar um alarme que monitora o estado de uma conexão do Direct Connect. Ele envia uma notificação quando o estado da conexão ficar inativo durante cinco períodos consecutivos de 1 minuto. Para obter detalhes sobre o que você precisa saber para criar um alarme e obter mais informações sobre como criar um alarme, consulte Como usar alarmes do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.

Criar um alarme do CloudWatch.

1. Abra o console do CloudWatch, em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarms (Alarmes) e depois escolha All alarms (Todos os alarmes).
3. Escolha Create Alarm.
4. Em seguida, Selecionar métrica e escolha DX.
5. Escolha a métrica Métricas de conexão.
6. Selecione a conexão do Direct Connect e, em seguida, escolha a métrica Selecionar métrica.
7. Na página Especificar métricas e condições, configure os parâmetros para o alarme. Para obter mais informações sobre a especificação de métricas e condições, consulte Como usar alarmes do Amazon CloudWatch no Guia do usuário do Amazon CloudWatch.
8. Escolha Próximo.
9. Configure as ações de alarme na página Configurar ações. Para obter mais informações sobre como configurar ações de alarme, consulte Ações de alarme no Guia do usuário do Amazon CloudWatch.
10. Escolha Próximo.
11. Na página Adicionar nome e descrição, insira o Nome e uma Descrição do alarme (opcional) para descrever esse alarme. Em seguida, escolha Próximo.

12. Verifique o alarme proposto na página Visualizar e criar.
13. Se necessário, escolha Editar para alterar qualquer informação e, em seguida, escolha Criar alarme.

    A página Alarmes exibe uma nova linha com informações sobre o novo alarme. O status Ações exibe Ações habilitadas, indicando que o alarme está ativo.

Cotas do Direct Connect

A tabela a seguir lista as cotas relacionadas ao Direct Connect.

Componente	Quota	Comentários
Interfaces virtuais privadas ou públicas por conexão dedicada do Direct Connect	50	Este limite não pode ser aumentado.
Interfaces virtuais de trânsito por conexão dedicada do Direct Connect. As interfaces virtuais de trânsito podem ser usadas para conectar a um Transit Gateway ou a uma rede central AWS Cloud WAN. Para obter mais informaçõ es, consulte Gateways.	4	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Interfaces virtuais privadas ou públicas por conexão dedicada do Direct Connect e interfaces virtuais de trânsito por conexão dedicada do Direct Connect	51	Quando a compatibilidade do AWS Direct Connect com gateways de trânsito da Amazon VPC foi lançada, uma cota de uma (1) interface virtual de trânsito era adicionada à cota de 50 interfaces virtuais públicas ou privadas por conexão dedicada. Agora, o número permitido de interfaces virtuais de trânsito é de quatro (4), sendo contabilizado em relação ao máximo de 51 interfaces virtuais por conexão dedicada. Este limite não pode ser aumentado.
Interfaces virtuais privadas, públicas ou de trânsito por conexão hospedada do Direct Connect	1	Este limite não pode ser aumentado.

Componente	Quota	Comentários
Conexões ativas do Direct Connect por local do Direct Connect por região por conta	10	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Número de interfaces virtuais por Grupo de agregação de links (LAG)	51	Quando a compatibilidade do AWS Direct Connect com gateways de trânsito da Amazon VPC foi lançada, uma cota de uma (1) interface virtual de trânsito era adicionada à cota de 50 interfaces virtuais públicas ou privadas por LAG. Agora, o número permitido de interfaces virtuais de trânsito é de quatro (4), sendo contabilizado em relação ao máximo de 51 interfaces virtuais por LAG. Este limite não pode ser aumentado.
Rotas por sessão Protocolo de Gateway da Borda (BGP) em uma interface virtual privada ou interface virtual de trânsito do ambiente on-premises para a AWS. Se você anunciar mais de 100 rotas cada para IPv4 e IPv6 por sessão do BGP, a sessão do BGP entrará em um estado ocioso com a sessão do BGP INATIVA.	100 cada para IPv4 e IPv6	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Sessão de rotas por Border Gateway Protocol (BGP) em uma interface virtual pública	1.000	Este limite não pode ser aumentado.

Componente	Quota	Comentários
Número de conexões por grupo de agregação de links (LAG)	4 quando a velocidade da porta for inferior a 100G 2 quando a velocidade da porta for 100G	
Grupos de agregação de links (LAGs) por região	10	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Gateways do Direct Connect por conta	200	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Virtual private gateways por gateway Direct Connect	20	Este limite não pode ser aumentado.
Gateways de trânsito por gateway Direct Connect	6	Este limite não pode ser aumentado.

Componente	Quota	Comentários
Número máximo de prefixos de rota anunciados de uma conexão on-premises do gateway do Direct Connect da rede principal da AWS Cloud WAN. **Note** Todas as interfaces virtuais de trânsito conectadas a esse gateway do Direct Connect receberão todos os prefixos de rota anunciados pela rede principal.	5.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Interfaces virtuais (privadas ou de trânsito) por gateway do Direct Connect	30	Este limite não pode ser aumentado.
Número de prefixos por AWS Transit Gateway da AWS para o ambiente on-premises em uma interface virtual de trânsito	Total combinado de 200 para IPv4 e IPv6	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Número de interfaces virtuais por gateway privado virtual	Não há limite.	
Número de gateways do Direct Connect associados a um gateway de trânsito	20	Este limite não pode ser aumentado.
Limite de prefixo do SiteLink	100	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.

O Direct Connect oferece suporte a essas velocidades de porta por fibra monomodo: 1 Gbps: 1000BASE-LX (1.310 nm), 10 Gbps: 10GBASE-LR (1.310 nm) e 100 Gbps: 100GBASE-LR4 e 400 Gbps: 400GBASE-LR4.

Cotas do BGP

Veja a seguir as cotas do BGP. Os temporizadores do BGP negociam até o valor mais baixo entre os roteadores. Os intervalos do BFD são definidos pelo dispositivo mais lento.

- Temporizador de espera padrão: 90 segundos
- Temporizador mínimo de espera: 3 segundos

  Não há compatibilidade com um valor de retenção de 0.
- Temporizador padrão de manutenção de atividade: 30 segundos
- Temporizador mínimo de manutenção de atividade: 1 segundo
- Temporizador de reinicialização suave: 120 segundos

  Recomendamos que você não configure a reinicialização tranquila e o BFD ao mesmo tempo.
- Intervalo mínimo de detecção de atividade do BFD: 300 ms
- Multiplicador mínimo do BFD: 3

Limites do ASN

Os limites a seguir se aplicam aos números de sistema autônomo (ASNs) usados com Direct Connect:

- Intervalo do ASN do cliente: de 1 a 4.294.967.294
  - ASNs: 1 a 2147483647
  - ASNs longos: 1 a 4294967294
- ASN da Amazon: valores fixos atribuídos pela AWS (normalmente 7224 para interfaces virtuais públicas)
- Intervalos de ASN privados:
  - ASNs privados: 64.512 a 65.534
  - ASNs longos privados: 4.200.000.000 a 4.294.967.294

> **Note**
>
> Para interfaces virtuais públicas, seu ASN deve ser um ASN privado ou já estar registrado e ter permissão para uso com a interface virtual.

Considerações sobre balanceamento de carga

Se você quiser usar o balanceamento de carga com várias VIFs públicas, todas as VIFs deverão estar na mesma região.

Solução de problemas do Direct Connect

As seguintes informações sobre resolução de problemas podem ajudar você a diagnosticar e corrigir problemas com sua conexão do Direct Connect.

Sumário

Solucionar problemas da camada 1 (física)

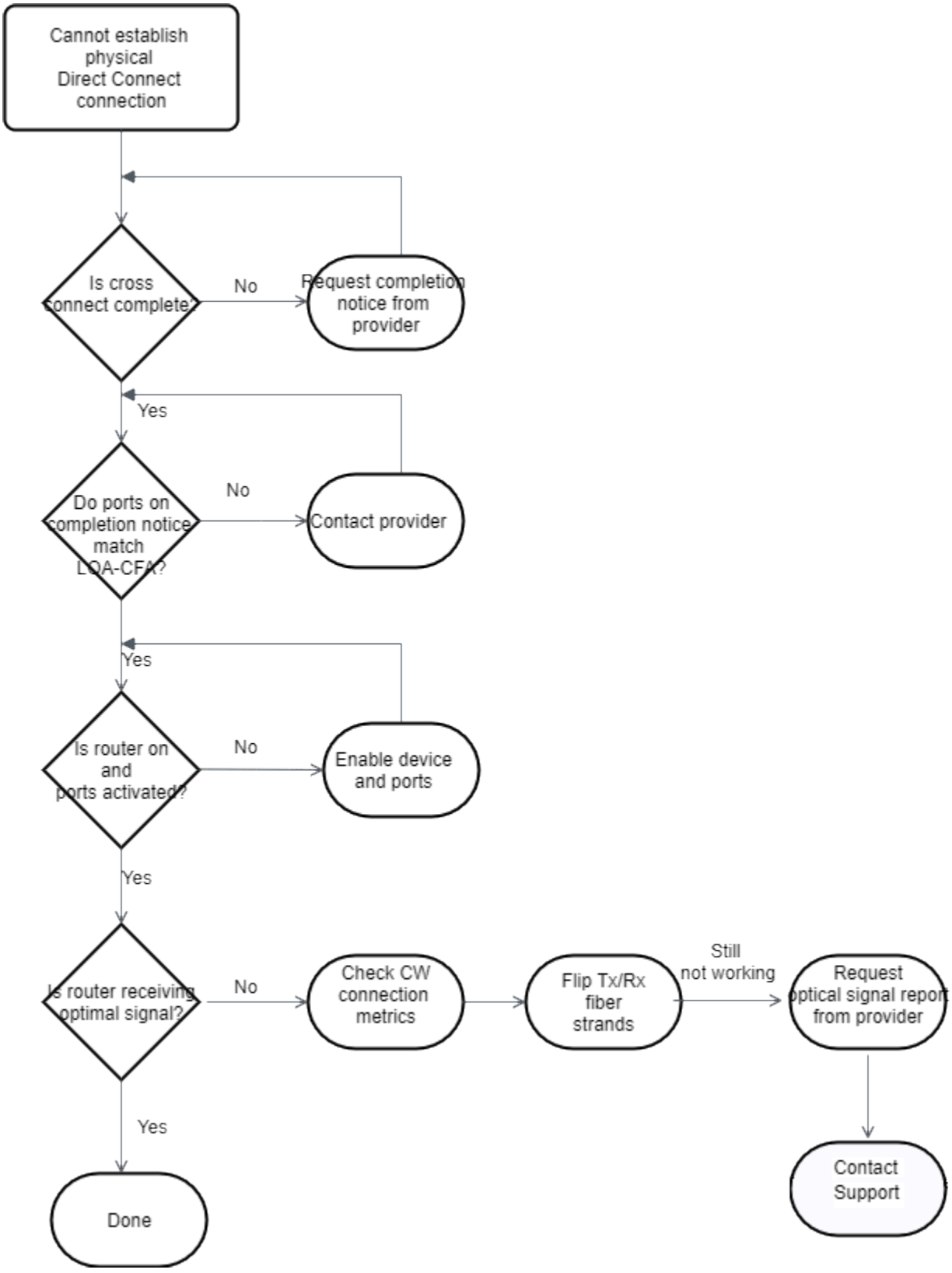
Caso você ou o provedor de rede esteja tendo dificuldade para estabelecer conectividade física com um dispositivo do Direct Connect, use as etapas a seguir para resolver o problema.

1. Verifique com o provedor de colocação se a conexão cruzada está concluída. Peça para ele ou o provedor de rede dar um aviso de conclusão de conexão cruzada e comparar as portas com as listadas no LOA-CFA.
2. Verifique se o roteador ou o roteador do provedor está ligado e se as portas estão ativadas.
3. Verifique se os roteadores estão usando o transceptor óptico correto. É necessário desabilitar a negociação automática da porta se você tiver uma conexão com uma velocidade de porta superior a 1 Gbps. No entanto, dependendo do endpoint do AWS Direct Connect que forneça sua conexão, pode ser necessário habilitar ou desabilitar a negociação automática para conexões de 1 Gbps. Se for necessário desabilitar a negociação automática para suas conexões, a velocidade da porta e o modo full-duplex deverão ser configurados manualmente. Se sua interface virtual permanecer inativa, consulte Solucionar problemas da camada 2 (link de dados). Dependendo do endpoint do Direct Connect que forneça sua conexão, pode ser necessário habilitar ou desabilitar a negociação automática adequadamente.
4. Verifique se o roteador está recebendo um sinal óptico aceitável pela conexão cruzada.
5. Tente virar (também conhecido como rolar) as fibras Tx/Rx.
6. Verifique o Direct Connect nas métricas do Amazon CloudWatch. É possível verificar as leituras ópticas de Tx/Rx do dispositivo do Direct Connect (tanto de 1 Gbps quanto de 10 Gbps), a

contagem de erros físicos e o status operacional. Para obter mais informações, consulte Monitoramento com o Amazon CloudWatch.

7. Entre em contato com o provedor de colocação e solicite um relatório por escrito para o sinal óptico Tx/Rx em toda a conexão cruzada.
8. Caso as etapas acima não resolvam problemas de conectividade física, entre em contato com o AWS Support e forneça um aviso de conexão cruzada concluída e um relatório de sinal óptico do provedor de colocalização.

O fluxograma a seguir contém as etapas para diagnosticar problemas com a conexão física.

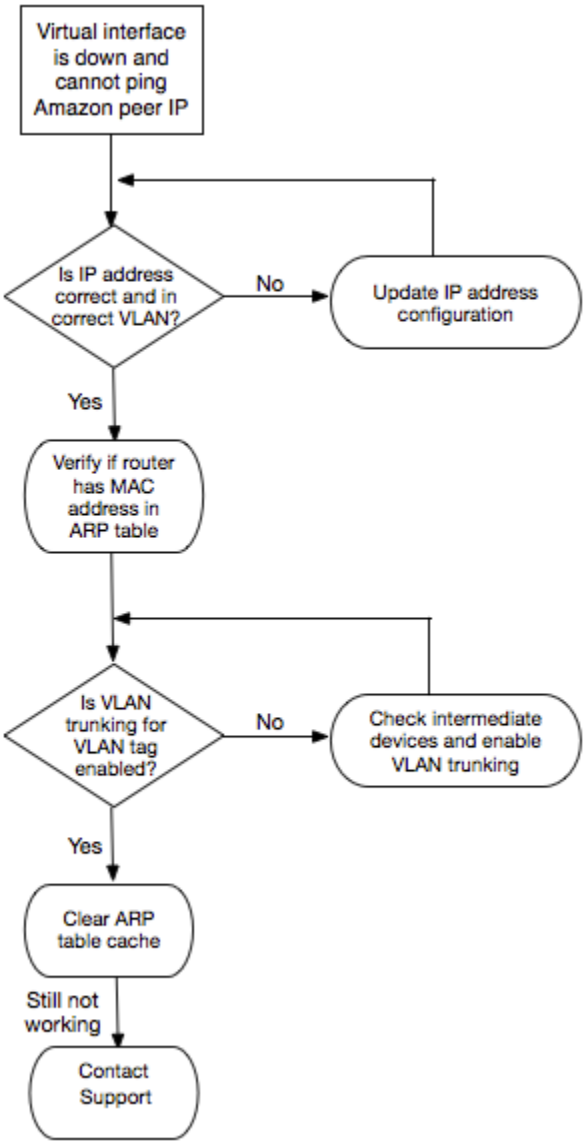

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Solucionar problemas da camada 2 (link de dados)

Caso a conexão física do Direct Connect esteja ativa, mas a interface virtual esteja inativa, use as etapas a seguir para resolver o problema.

1. Caso você não consiga executar ping no endereço IP par da Amazon, verifique se o endereço IP par está configurado corretamente e na VLAN correta. Verifique se o endereço IP está configurado na subinterface VLAN, e não na interface física (por exemplo, GigabitEthernet0/0.123, em vez de GigabitEthernet0/0).
2. Verifique se o roteador tem uma entrada de endereço MAC do endpoint da AWS em sua tabela do Protocolo de resolução do endereço (ARP).
3. Verifique se algum dispositivo intermediário entre endpoints tem entroncamento VLAN habilitado para a tag VLAN 802.1Q. Não será possível estabelecer o ARP no lado da AWS até que a AWS receba o tráfego marcado.
4. Apague o cache da tabela ARP do provedor.
5. Caso as etapas acima não estabeleçam ARP ou você continue sem conseguir executar ping no IP de par da Amazon, entre em contato com o AWS Support.

O fluxograma a seguir contém as etapas para diagnosticar problemas com o link de dados.



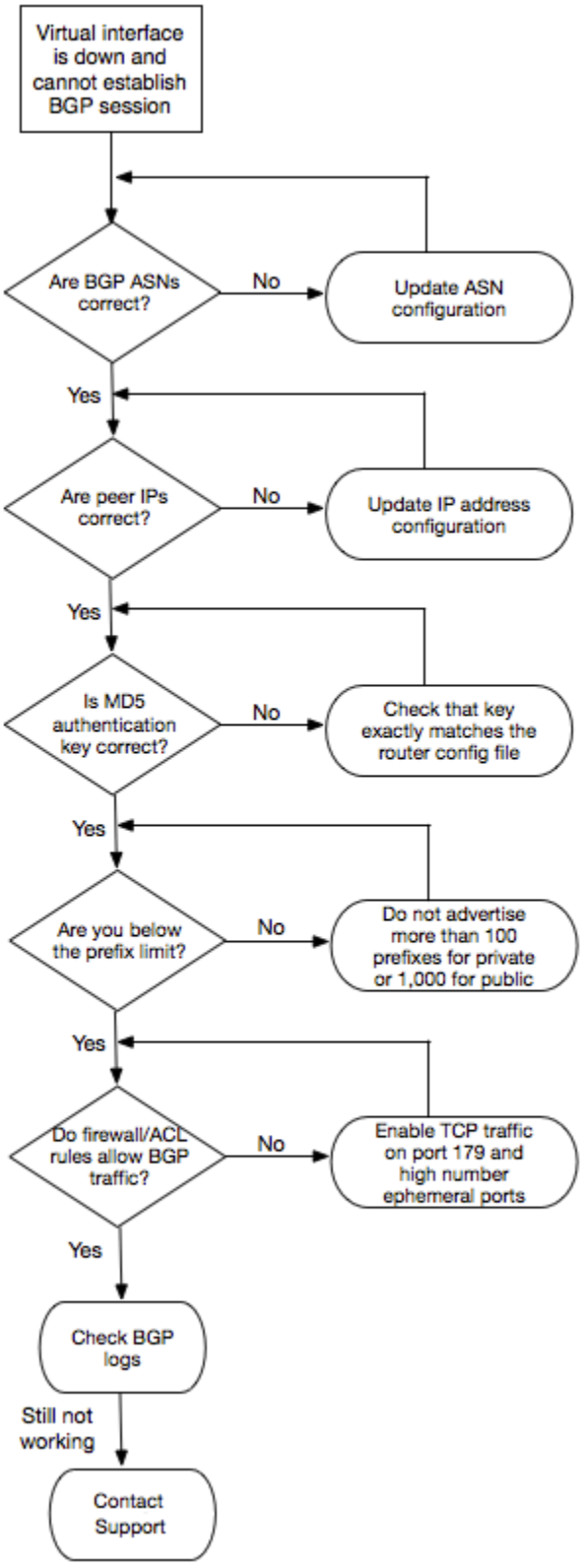
Caso a sessão BGP ainda não seja estabelecida após a verificação dessas etapas, consulte Solucionar problemas das camadas 3/4 (rede/transporte). Caso a sessão BGP seja estabelecida, mas você esteja enfrentando problemas de roteamento, consulte Solução de problemas de roteamento.

Solucionar problemas das camadas 3/4 (rede/transporte)

Considere uma situação em que a conexão física do Direct Connect está ativa e você pode executar ping no endereço IP par da Amazon. Caso sua interface virtual esteja em funcionamento, mas a sessão de emparelhamento do BGP não possa ser estabelecida, siga as seguintes etapas para solucionar o problema:

1. Verifique se o Autonomous System Number (ASN – Número de sistema autônomo) local BGP e o ASN da Amazon estão configurados corretamente.
2. Verifique se os IPs par de ambos os lados da sessão de mesmo nível BGP estão configurados corretamente.
3. Verifique se a chave de autenticação MD5 está configurada e corresponde exatamente à chave no arquivo de configuração do roteador obtido por download. Verifique se não há espaços ou caracteres extras.
4. Verifique se você ou o provedor não estão anunciando mais de 100 prefixos para interfaces virtuais privadas ou 1.000 prefixos públicos para interfaces virtuais públicas. Esses são limites fixos e não podem ser excedidos.
5. Verifique se não há regras ACL ou de firewall bloqueando a porta TCP 179 ou qualquer outra porta TCP alta efêmera de numeração alta. Essas portas são necessárias para BGP estabelecer uma conexão TCP entre os pares.
6. Verifique os logs BGP em busca de eventuais erros ou mensagens de aviso.
7. Caso as etapas acima não estabeleçam a sessão de emparelhamento do BGP, entre em contato com o AWS Support.

O fluxograma a seguir contém as etapas para diagnosticar problemas com a sessão de mesmo nível BGP.



Caso a sessão de mesmo nível BGP seja estabelecida, mas você esteja enfrentando problemas de roteamento, consulte Solução de problemas de roteamento.

Solucionar problemas de ASN longo

Se você tiver problemas com as configurações de ASN longo, use as etapas a seguir para solucioná-los:

A sessão do BGP falha com um ASN longo

Sintomas: a sessão do BGP não pode ser estabelecida após a configuração de um ASN longo

Causa: o roteador on-premises pode não suportar o recurso de ASN longo

Resolução:

- Verifique se seu roteador é compatível com RFC 6793
- Verifique a configuração do BGP para obter um formato ASN consistente
- Analise os logs do BGP em busca de erros de negociação de capacidade

As respostas da API mostram o ASN como 0

Sintomas: as respostas da API exibem o campo `asn` como 0

Causa: esse é o comportamento esperado quando o ASN real excede 2.147.483.647

Resolução: use o campo `asnLong` nas respostas da API para obter o valor correto do ASN

Problemas de migração do ASN para ASN longo

Sintomas: perda de conectividade durante a migração do ASN

Causa: é necessário restabelecer a sessão do BGP para alterações no ASN

Resolução:

- Planeje a migração durante as janelas de manutenção
- Atualize uma interface virtual por vez
- Monitore o status da sessão do BGP durante as alterações
- Verifique a convergência da tabela de rotas após a migração

Se você continuar tendo problemas com configurações de ASN longo depois de seguir as etapas de solução de problemas descritas, entre em contato com o AWS Support com as seguintes informações:

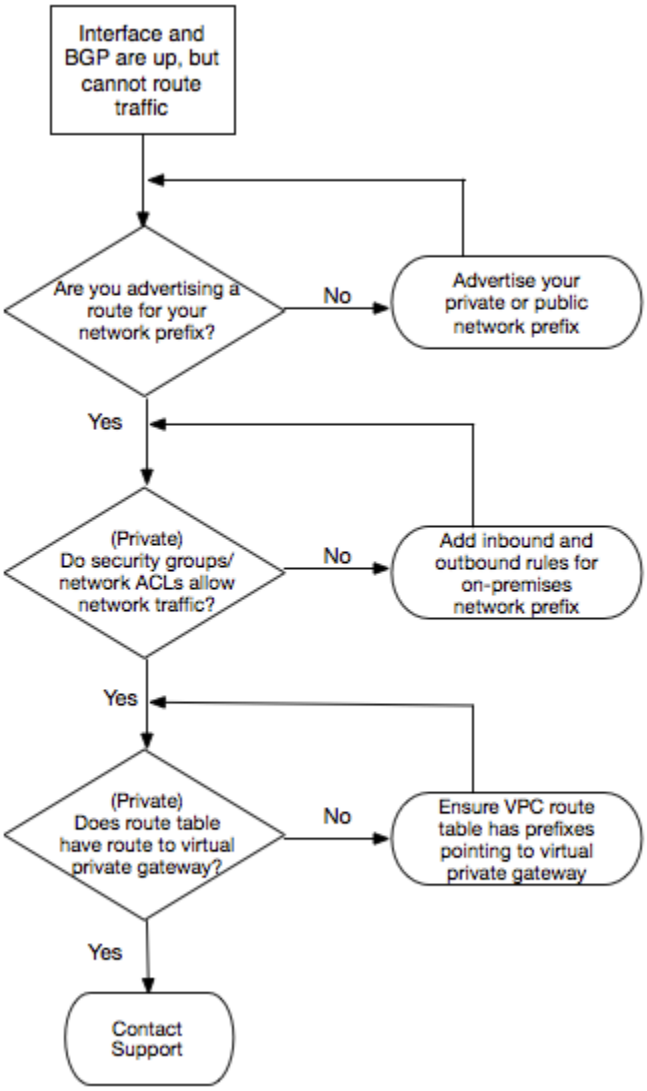
- ID da interface virtual ou ID do par BGP
- Valores de ASN configurados (tanto ASN quanto ASN longo)
- Modelo do roteador e versão do software
- Configuração e logs do BGP
- Mensagens ou sintomas de erro observados

Solução de problemas de roteamento

Considere uma situação em que a interface virtual está ativa e você tiver estabeleceu uma sessão de mesmo nível BGP. Se não for possível rotear o tráfego pela interface virtual, use as etapas a seguir para solucionar o problema:

1. Verifique se você está anunciando uma rota para o prefixo de rede on-premises pela sessão BGP. Para obter uma interface virtual privada, pode ser um prefixo de rede pública ou privada. Para obter uma interface virtual pública, ele deve ser um prefixo de rede roteável publicamente.
2. Para obter uma interface virtual privada, verifique se os security groups da VPC e as ACLs de rede permitem o tráfego de entrada e de saída do prefixo de rede on-premises. Para obter mais informações, consulte Grupos de segurança e ACLs de rede no Guia do usuário da Amazon VPC.
3. Para obter uma interface virtual privada, verifique se as tabelas de rotas VPC têm prefixos apontando para o gateway privado virtual ao qual a interface virtual privada está conectada. Por exemplo, se preferir ter todo o tráfego roteado para a rede on-premises por padrão, poderá adicionar a rota padrão (0.0.0.0/0 e/ou ::/0) com o gateway privado virtual como destino nas tabelas de rotas da VPC.
   - Como alternativa, habilite a propagação de rota para atualizar automaticamente rotas nas tabelas de rotas com base no anúncio de rota BGP dinâmico. Você pode ter até 100 rotas propagadas por tabela de rotas. Este limite não pode ser aumentado. Para obter mais informações, consulte Habilitar e desabilitar a propagação de rota no Guia do usuário da Amazon VPC.
4. Caso as etapas acima não resolvam o problema de roteamento, entre em contato com o AWS Support.

O fluxograma a seguir contém as etapas para diagnosticar problemas de roteamento.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Histórico do documento

A seguinte tabela descreve todas as versões de AWS Direct Connect. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Suporte para ASN longo	Agora você pode usar valores para ASN longo para as sessões do BGP com interfaces virtuais do Direct Connect.	24 de julho de 2025
Criar uma associação entre o gateway do Direct Connect e uma rede principal do AWS Network Manager	Agora você pode criar uma associação de gateway do Direct Connect diretamente entre o Direct Connect e uma rede principal da AWS Cloud WAN.	25 de novembro de 2024
Compatibilidade com 400G	Tópicos atualizados para incluir suporte a conexões 400G.	18 de julho de 2024
Adicionado o limite de prefixo para o SiteLink	Um limite de prefixo para o SiteLink foi adicionado ao tópico de cotas e limites.	15 de junho de 2023
Compatibilidade com SiteLink	Você pode criar uma interface virtual privada que habilite a conectividade entre dois pontos de presença (PoPs) do Direct Connect na mesma região da AWS.	1º de dezembro de 2021
Compatibilidade com MAC Security	Você pode usar conexões do Direct Connect compatíveis com MACsec para criptografar seus dados do data center	31 de março de 2021

	corporativo para o local do Direct Connect.	
Compatibilidade com 100G	Atualização de tópicos para incluir a compatibilidade com conexões dedicadas 100G.	12 de fevereiro de 2021
Nova localização na Itália	Atualização do tópico para incluir a adição do novo local na Itália.	22 de janeiro de 2021
Novo local em Israel	Atualização do tópico para incluir a adição do novo local em Israel.	7 de julho de 2020
Suporte a testes de failover do toolkit de resiliência	Use o atributo Testes de failover do Resiliency Toolkit para testar a resiliência das conexões.	3 de junho de 2020
Compatibilidade com a métrica de VIF do CloudWatch	Você pode monitorar conexões físicas do Direct Connect e interfaces virtuais usando o CloudWatch.	11 de maio de 2020
AWS Direct Connect Kit de ferramentas de resiliência do	O kit de ferramentas de resiliência do AWS Direct Connect fornece um assistente de conexão com vários modelos de resiliência que ajuda você a solicitar conexões dedicadas para atingir seu objetivo de SLA.	7 de outubro de 2019
Suporte de região adicional para o AWS Transit Gateway em várias contas	Suporte de região adicional para o AWS Transit Gateway em várias contas.	30 de setembro de 2019

AWS Direct Connect Compatibilidade com AWS Transit Gateway	É possível usar um gateway do Direct Connect para criar uma conexão do Direct Connect por meio de uma interface virtual de trânsito às VPCs ou VPNs anexadas ao seu gateway de trânsito. Você associa um gateway do Direct Connect com o gateway de trânsito. Em seguida, crie uma interface virtual privada para sua conexão do Direct Connect com o gateway Direct Connect.	27 de março de 2019
Suporte a frames jumbo	Você pode enviar frames jumbo (9001 MTU) pelo Direct Connect.	11 de outubro de 2018
Comunidades BGP de preferência local	Você pode usar as tags de comunidade BGP de preferência local para obter o balanceamento de carga e a preferência de rota para o tráfego de entrada para sua rede.	6 de fevereiro de 2018
Direct Connect Gateway do	Use um gateway Direct Connect para conectar sua conexão do Direct Connect a VPCs em Regiões remotas.	1 de novembro de 2017
Métricas do Amazon CloudWatch	Você pode visualizar métricas do CloudWatch para suas conexões do Direct Connect.	29 de junho de 2017

Grupos de agregação de link	Você pode criar um LAG para agregar várias conexões do Direct Connect.	13 de fevereiro de 2017
Suporte a IPv	A interface virtual já pode dar suporte a uma sessão de mesmo nível BGP IPv6.	1° de dezembro de 2016
Suporte a marcação	Você já pode identificar os recursos do Direct Connect.	4 de novembro de 2016
LOA-CFA de autoatendimento	Você já pode baixar a Letter of Authorization and Connecting Facility Assignment (LOA-CFA - Carta de autorização e atribuição da instalação de conexão) usando o console ou a API do Direct Connect.	22 de junho de 2016
Novo local no Vale do Silício	Atualização do tópico para incluir a adição do novo local no Vale do Silício na região Oeste dos EUA (N. da Califórnia).	3 de junho de 2016
Novo local em Amsterdã	Atualização do tópico para incluir a adição do novo local em Amsterdã na região Europa (Frankfurt).	19 de maio de 2016
Novos locais em Portland, Oregon e Cingapura	Atualização do tópico para incluir a adição dos novos locais em Portland, Oregon e Singapura nas regiões Oeste dos EUA (Oregon) e Ásia-Pacífico (Singapura).	27 de abril de 2016

Novo local em São Paulo, Brasil	Atualização do tópico para incluir a adição do novo local em São Paulo na região América do Sul (São Paulo).	9 de dezembro de 2015
Novos locais em Dallas, Londres, Vale do Silício e Mumbai	Atualização dos tópicos para incluir a adição de novos locais em Dallas (região Leste dos EUA [Norte da Virgínia]), Londres (região Europa [Irlanda]), Vale do Silício (região AWS GovCloud [Oeste dos EUA]) e Mumbai (região Ásia-Pacífico [Singapura]).	27 de novembro de 2015
Nova localização na região China (Pequim	Atualização do tópico para incluir a adição do novo local em Pequim na região China (Pequim).	14 de abril de 2015
Novo local em Las Vegas na Região Oeste dos EUA (Oregon	Tópicos atualizados para incluir a adição do novo local em Las Vegas do Direct Connect na Região Oeste dos EUA (Oregon).	10 de novembro de 2014
Nova Região UE (Frankfurt	Tópicos atualizados para incluir a adição dos novos locais do Direct Connect que atendem à Região UE (Frankfurt).	23 de outubro de 2014
Novos locais na Região Ásia-Pacífico (Sydney	Tópicos atualizados para incluir a adição dos novos locais do Direct Connect que atendem à Região Ásia-Pací fico (Sydney).	14 de julho de 2014

Suporte para AWS CloudTrail	Adição de um novo tópico para explicar como você pode usar o CloudTrail para registrar atividade em log no Direct Connect.	4 de abril de 2014
Suporte para acessar regiões remotas da AWS	Adição de um novo tópico para explicar como você pode acessar recursos públicos em uma Região remota.	19 de dezembro de 2013
Suporte para conexões hospedadas	Tópicos atualizados para incluir suporte a conexões hospedadas.	22 de outubro de 2013
Novo local na Região UE (Irlanda	Tópicos atualizados para incluir a adição do novo local do Direct Connect que atende à Região UE (Irlanda).	24 de junho de 2013
Novo local em Seattle na Região Oeste dos EUA (Oregon	Tópicos atualizados para incluir a adição do novo local em Seattle do Direct Connect na Região Oeste dos EUA (Oregon).	8 de maio de 2013
Compatibilidade com o uso do IAM com o Direct Connect	Tópico adicionado sobre como usar o AWS Identity and Access Management com o Direct Connect.	21 de dezembro de 2012
Nova Região Ásia-Pacífico (Sydney	Tópicos atualizados para incluir a adição do novo local do Direct Connect que atende à Região Ásia-Pacífico (Sydney).	14 de dezembro de 2012

Novo console do AWS Direct Connect e as regiões Leste dos EUA (Norte da Virgínia) e América do Sul (São Paulo	Substituído o Guia de conceitos básicos do Direct Connect pelo Guia do usuário do Direct Connect. Adição de novos tópicos para abordar o novo console do Direct Connect, adição de um tópico de faturamento, adição de informações de configuração do roteador e atualização dos tópicos para incluir a adição de dois novos locais do Direct Connect que atendem às Regiões Leste dos EUA (Norte da Virgínia) e América do Sul (São Paulo).	13 de agosto de 2012
Suporte para as Regiões UE (Irlanda), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio	Adição de uma nova seção de solução de problemas e atualização dos tópicos para incluir a adição de quatro novos locais do Direct Connect que atendem às Regiões Oeste dos EUA (Norte da Califórnia), UE (Irlanda), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio).	10 de janeiro de 2012
Suporte para a Região Oeste dos EUA (Norte da Califórnia	Tópicos atualizados para incluir a adição da Região Oeste dos EUA (Norte da Califórnia).	8 de setembro de 2011
Versão pública	A primeira versão do Direct Connect.	3 de agosto de 2011

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