Guia do usuário

AWS Direct Connect

AWS Direct Connect: Guia do usuário

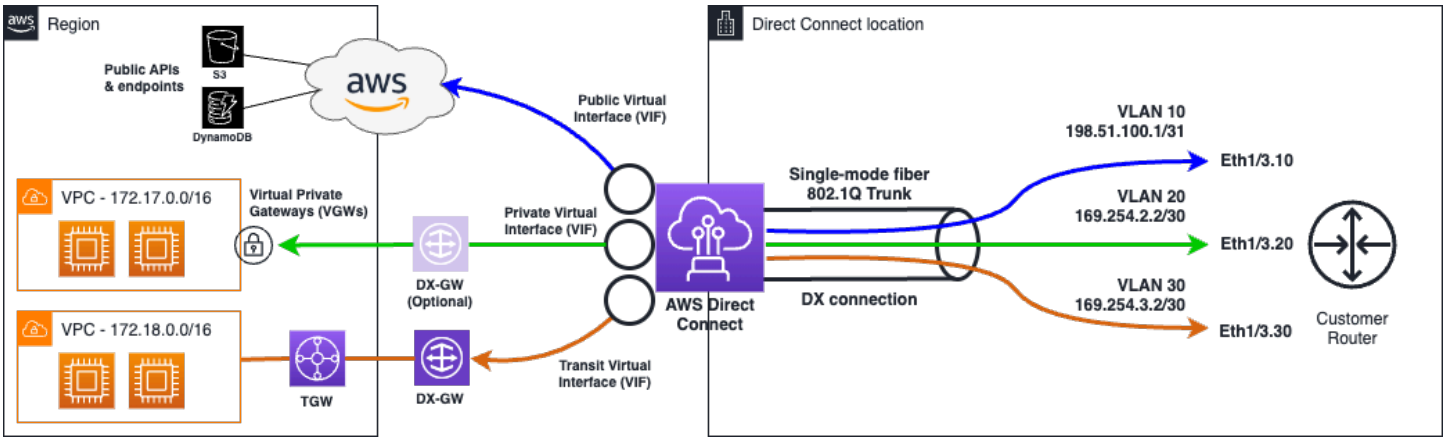
Table of Contents

O que AWS Direct Connecté

AWS Direct Connect conecta sua rede interna a um AWS Direct Connect local por meio de um cabo de fibra óptica Ethernet padrão. Uma extremidade do cabo é conectada ao roteador, e a outra é conectada a um roteador do AWS Direct Connect . Com essa conexão, você pode criar interfaces virtuais diretamente para AWS serviços públicos (por exemplo, para o Amazon S3) ou para o Amazon VPC, ignorando os provedores de serviços de Internet em seu caminho de rede. Um AWS Direct Connect local fornece acesso à AWS região à qual está associado. Você pode usar uma única conexão em uma região pública ou AWS GovCloud (US) acessar AWS serviços públicos 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 mostra uma visão geral de alto nível de como AWS Direct Connect interage com sua rede.



Conteúdo

- AWS Direct Connect políticas de roteamento e comunidades BGP

AWS Direct Connect componentes

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

Conexões

Crie uma conexão em um AWS Direct Connect local para estabelecer uma conexão de rede entre suas instalações e uma AWS região. Para obter mais informações, consulte AWS Direct Connect conexões dedicadas e hospedadas.

Interfaces virtuais

Crie uma interface virtual para permitir o acesso aos AWS serviços. 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 AWS Direct Connect interfaces virtuais e interfaces virtuais hospedadas e Pré-requisitos para interfaces virtuais.

Requisitos de rede

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

- Sua rede está localizada em um AWS Direct Connect local existente. Para obter mais informações sobre os AWS Direct Connect locais disponíveis, consulte os detalhes do produto AWS Direct Connect.
- Você está trabalhando com um AWS Direct Connect parceiro que é membro da AWS Partner Network (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 AWS Direct Connect.

Além disso, a rede deve atender às seguintes condições:

- 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 Direct Connect estiver ativa, consulteSolucionar 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. AWS 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.

AWS Direct Connect suporta os protocolos de IPv6 comunicação IPv4 e de comunicação. IPv6 endereços fornecidos por AWS serviços públicos são acessíveis por meio de interfaces virtuais AWS Direct Connect públicas.

O AWS 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

AWS Direct Connect suporta os três tipos de interface virtual (VIF) a seguir:

- Interface virtual privada

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

  - Conecte-se diretamente a uma única VPC por interface virtual privada para acessar esses recursos usando private IPs na mesma região.

  - Conecte uma interface virtual privada a um gateway Direct Connect para acessar vários gateways privados virtuais em qualquer conta e AWS região (exceto nas regiões da AWS China).
- Interface virtual pública

  Esse tipo de interface virtual é usado para acessar todos os serviços AWS públicos usando endereços IP públicos. Com uma interface virtual pública, você pode se conectar a todos os endereços IP e serviços AWS públicos 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, você conecta vários Amazon VPC Transit Gateways em várias contas Regiões da AWS (exceto as regiões da AWS 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

AWS Direct Connect tem dois elementos de cobrança: horário portuário 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 taxas de saída de transferência de dados para interfaces privadas e interfaces virtuais de trânsito são alocadas à AWS conta responsável pela transferência de dados. Não há cobranças adicionais para usar um gateway do AWS Direct Connect de várias contas.

Para AWS recursos endereçáveis publicamente (por exemplo, buckets do Amazon S3, instâncias EC2 Classic EC2 ou tráfego que passa por um gateway da Internet), se o tráfego de saída for destinado a prefixos públicos pertencentes à AWS mesma conta pagadora e anunciado ativamente

por meio de AWS Direct Connect uma interface virtual pública, o uso da transferência de dados AWS para fora (DTO) será medido para o proprietário do recurso de acordo com a taxa de transferência de dados. AWS Direct Connect

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

Acesso a AWS Direct Connect regiões remotas

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

Depois de criar uma interface virtual pública e estabelecer uma sessão BGP nela, seu roteador aprende as rotas das outras regiões públicas. AWS Para obter mais informações sobre prefixos atualmente anunciados pela AWS, consulte Intervalos de endereços AWS IP 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 AWS Direct Connect conexão por meio de uma interface virtual privada à VPCs sua

conta localizada em diferentes regiões ou a um gateway de trânsito. Para obter mais informações, consulte AWS Direct Connect gateways.

Como alternativa, você pode criar uma interface virtual pública para sua AWS Direct Connect conexão e, em seguida, estabelecer 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.

Network-to-Amazon Opções de conectividade VPC

É possível usar a configuração a seguir para conectar redes remotas ao seu ambiente Amazon VPC. Essas opções são úteis para integrar AWS recursos aos seus serviços locais existentes:

- Opções de conectividade da Amazon Virtual Private Cloud

AWS Direct Connect políticas de roteamento e comunidades BGP

AWS Direct Connect aplica políticas de roteamento de entrada (do seu data center local) e de saída (da sua AWS região) para uma conexão pública. AWS 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 AWS 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.
- AWS 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 AWS Direct Connect se o mesmo prefixo estiver sendo anunciado na Internet e em uma interface virtual pública.
- AWS 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.

- AWS Direct Connect anuncia prefixos com um comprimento mínimo de caminho de 3.
- AWS 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 AWS 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 AWS 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.
- AWS 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 AWS 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.
  - Privado ASNs: você pode usar privado ASNs (64512-65534, 4200000000-4294967294). No entanto, AWS Direct Connect substituirá o ASN privado pelo AWS ASN (7224) ao anunciar seus prefixos para outros AWS clientes ou para a Internet.
  - ASN prependente:
    - Com um ASN público, o prefixo funcionará conforme o esperado e seu ASN prefixo ficará visível para outras redes.
    - Com um ASN privado, 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 paralelamente. AWS O ASN em seu roteador ou dispositivo de gateway do cliente deve ser diferente desse ASN.

Comunidades BGP de interface virtual pública

AWS 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 AWS Direct Connect.

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

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

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

Para interfaces virtuais públicas, todas as rotas AWS 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 conexões ativas/passivas. Para obter mais informações, consulte Influencing Traffic over Hybrid Networks using Longest Prefix Match.
- A preferência local é o atributo de BGP recomendado para usar quando os caminhos de rota desejados forem destinados a conexões ativas ou passivas e os comprimentos dos prefixos anunciados forem semelhantes. 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 or 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 AWS 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 AWS 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.

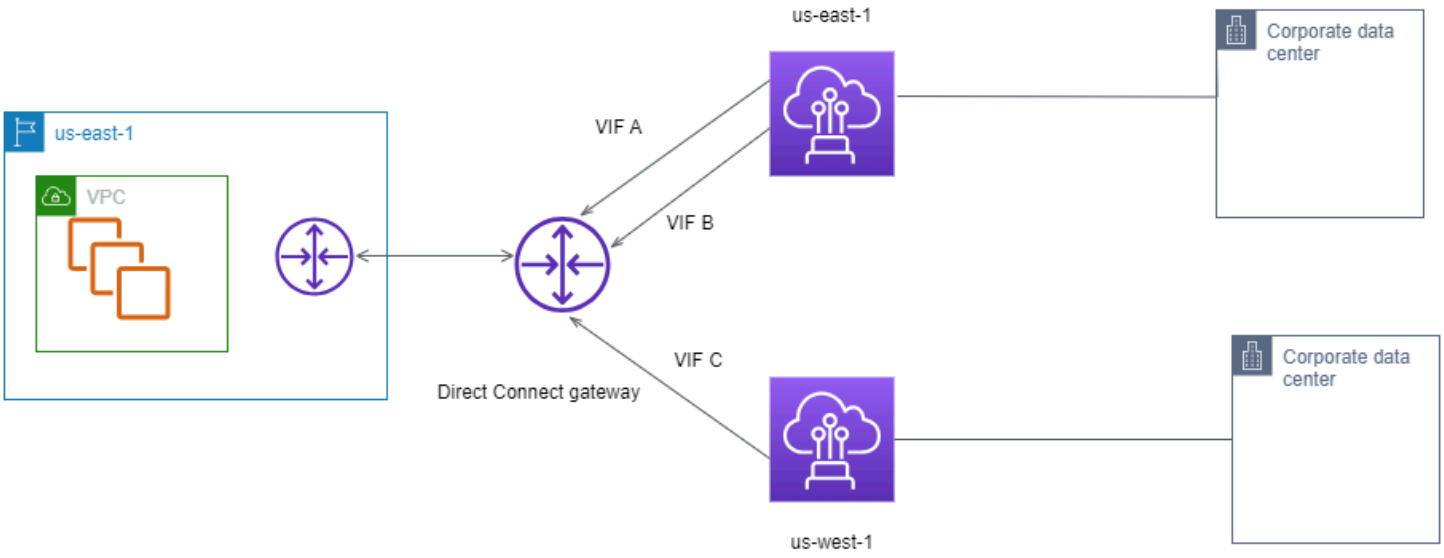
As tags de comunidade BGP de preferência local são avaliadas antes de qualquer atributo AS_PATH e da menor para a maior preferência (quando a maior preferência tiver prioridade).

AWS Direct Connect exemplo de roteamento de interface virtual privada

Considere a configuração em que a região de origem do AWS Direct Connect local 1 é igual à região de origem da VPC. Há um AWS Direct Connect local redundante em uma região diferente. Há dois locais privados VIFs (VIF A e VIF B) do local AWS Direct Connect 1 (us-east-1) até o gateway Direct Connect. Há uma VIF privada (VIF C) do AWS 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.

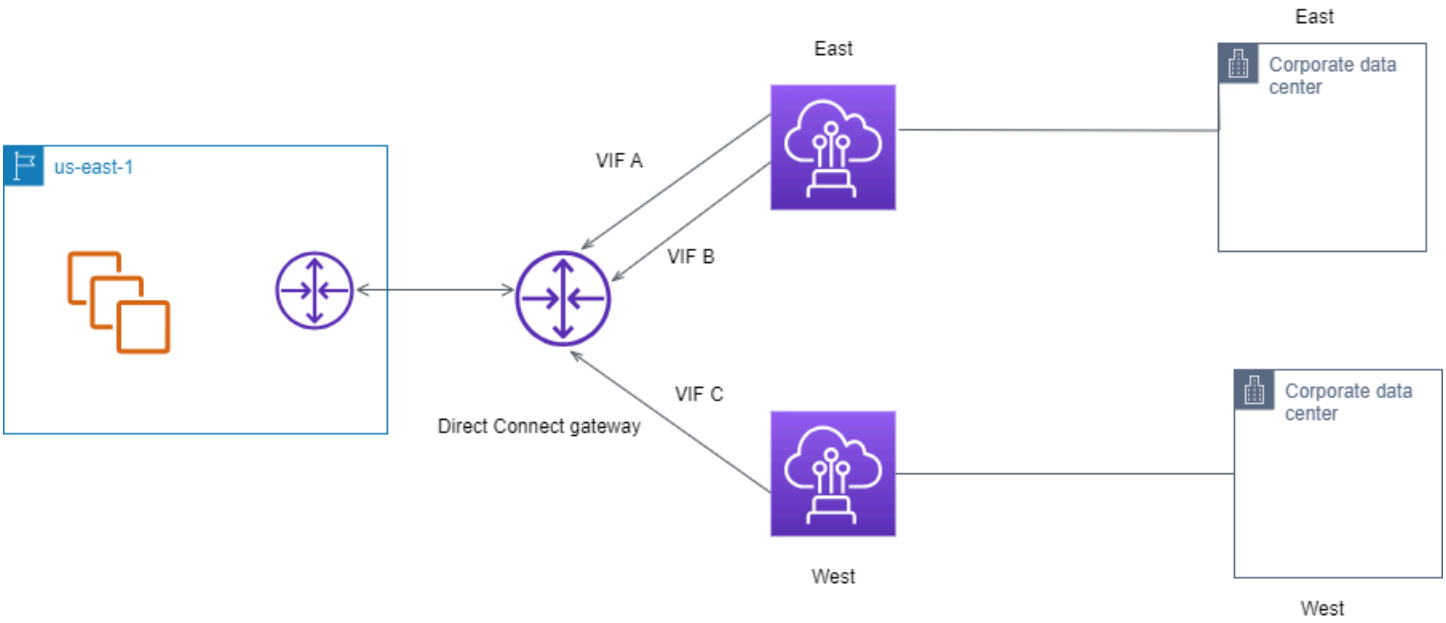
Eles VIFs têm as seguintes configurações:

- 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


East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

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 AWS 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 AWS 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.

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

- Maximum Resiliency (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 AWS Direct Connect.
- High Resiliency (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 AWS Direct Connect.
- Desenvolvimento e teste: este modelo permite que você obtenha resiliência de desenvolvimento e teste para cargas de trabalho não críticas usando conexões separadas que são encerradas em dispositivos separados em um único local.
- Classic (Clássica). Este modelo é destinado a usuários que já possuem conexões e desejam incluir conexões adicionais. Esse modelo não fornece um SLA.

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

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

Pré-requisitos

AWS 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 AWS Direct Connect conexão de uma das seguintes formas:

Modelo	Largura de banda	Método
Conexão dedicada	1 Gbps, 10 Gbps, 100 Gbps e 400 Gbps	Trabalhe com um AWS Direct Connect parceiro ou um provedor de rede para conectar um roteador do seu data center, escritório ou ambiente de colocation a um AWS Direct Connect local. O provedor de rede não precisa ser um AWS Direct Connect parceiro para conectar você a uma conexão dedicada. AWS 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, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps e 25 Gbps.	Trabalhe com um AWS Direct Connect parceiro no Programa de Parceria para conectar um roteador do seu data center, escritório ou ambiente de colocation a um AWS Direct Connect local.

Modelo	Largura de banda	Método
		Somente determinados parceiros oferecem conexões de maior capacidade.

Para conexões AWS 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 Direct Connect estiver ativa, consulteSolucionar 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. AWS 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.

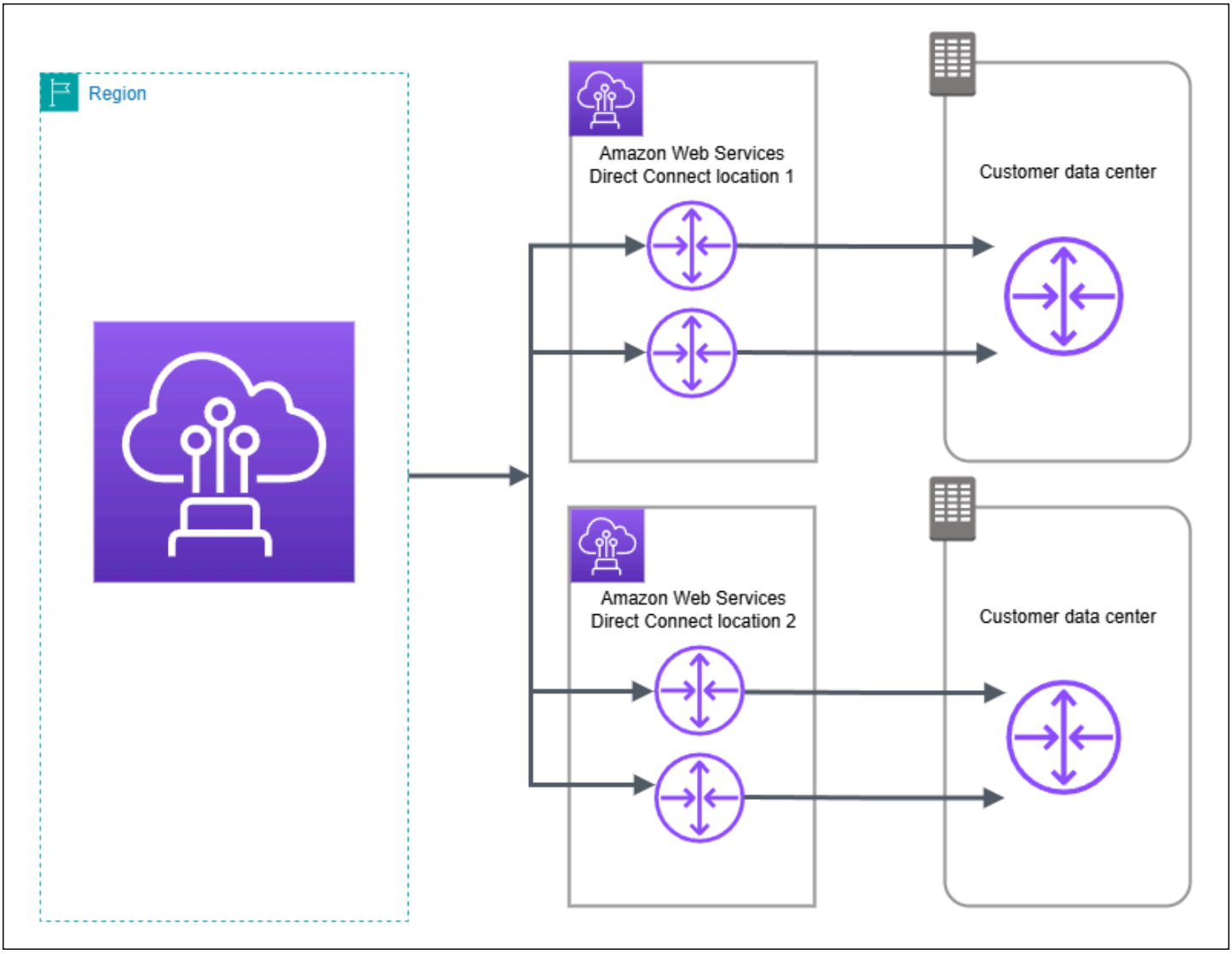
Verifique se você tem as seguintes informações antes de iniciar a configuração:

- O modelo de resiliência que você deseja usar.
- A velocidade, o local e o parceiro de todas as conexões.

  Você só precisa da velocidade para uma conexão.

Resiliência máxima

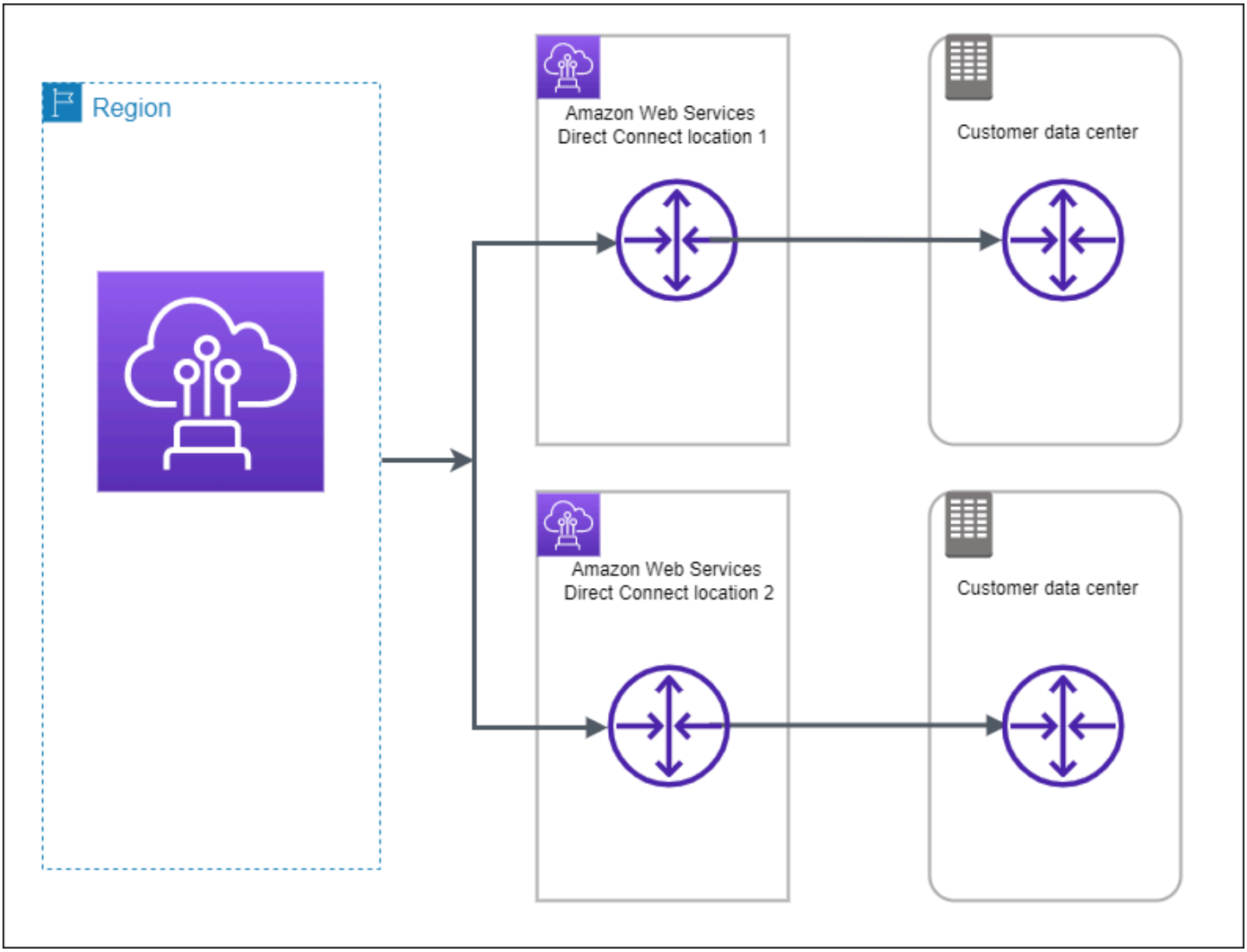
Você pode alcançar a máxima resiliência para cargas de trabalho críticas usando conexões separadas que são encerradas em dispositivos separados em mais de um local (conforme mostrado na figura). Esse modelo fornece resiliência contra falhas de dispositivo, conectividade e localização completa. A figura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

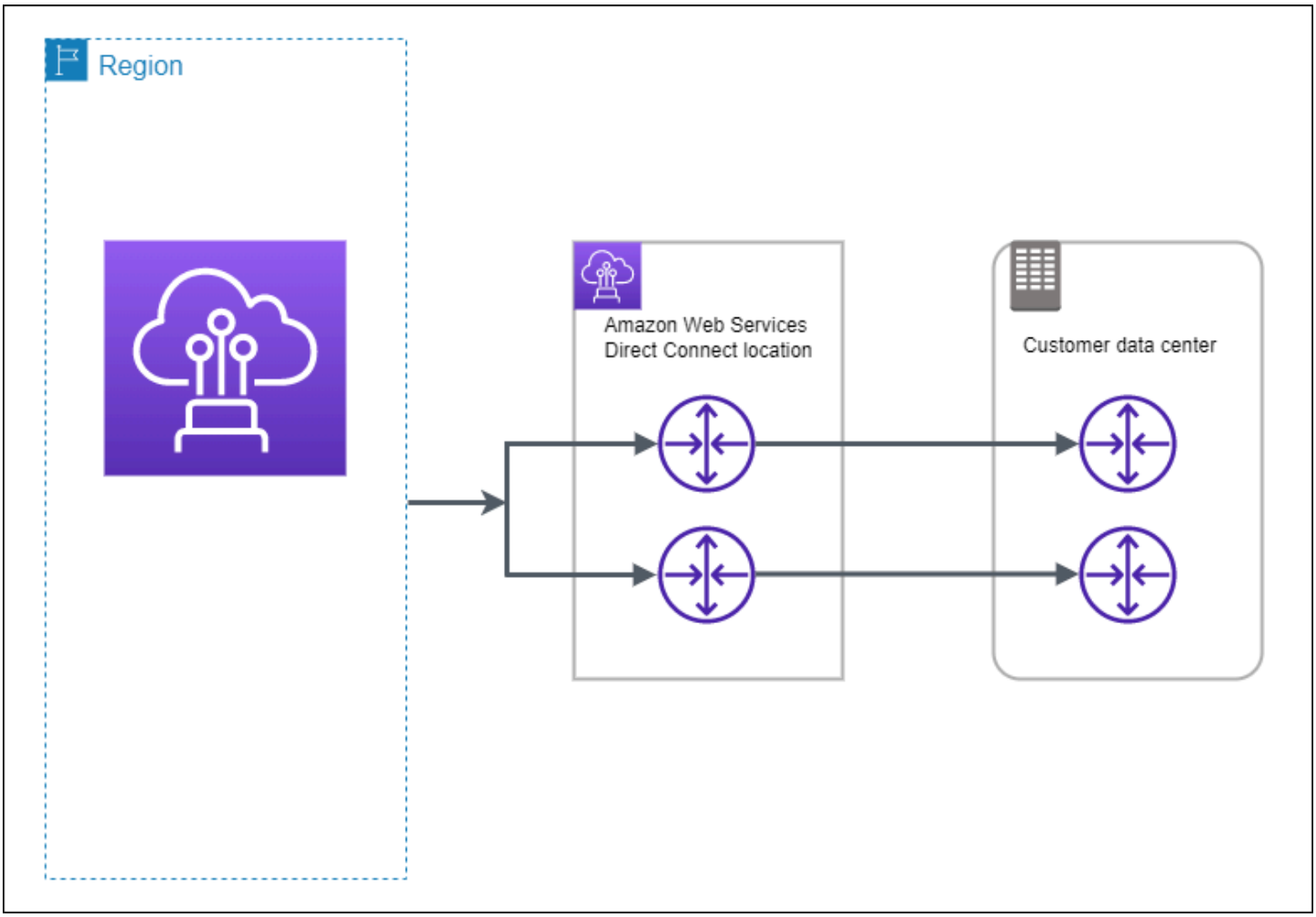


Para obter o procedimento de uso do AWS Direct Connect Resiliency Toolkit para configurar um modelo de alta resiliência, consulte. Configuração da alta resiliência

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

Clássica

Selecione Clássica quando você tiver conexões existentes.

Os procedimentos a seguir demonstram os cenários comuns a serem configurados com uma conexão do AWS Direct Connect .

Pré-requisitos

Para conexões AWS Direct Connect com velocidades de porta 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 Direct Connect estiver ativa, consulteSolucionar 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. AWS 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.

Para obter o procedimento de uso do AWS Direct Connect Resiliency Toolkit para configurar uma conexão clássica, consulte. Configuração de uma conexão Classic

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

Use o AWS Direct Connect Resiliency Toolkit AWS Direct Connect para configurar a máxima resiliência

Neste exemplo, o AWS 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 AWS 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 AWS IAM Identity Center, 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 AWS Management Consolecomo 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 AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

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 AWS IAM Identity Center 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 AWS IAM Identity Center .

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

Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Etapa 2: Configurar o modelo de resiliência

Configurar um modelo de resiliência máxima

1. Abra o AWS 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 AWS 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 AWS 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 AWS Direct Connect conexão ou o grupo de agregação de links (LAG) para o qual você está criando a interface virtual.

Recurso	Informações necessárias
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 AWS 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 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 AWS 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.

(Somente interfaces virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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. AWS 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 AWS 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 AWS 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 1-2147483647.
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 AWS 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 2147483647.

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 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 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 AWS 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.

Use o AWS Direct Connect Resiliency Toolkit para configurar AWS Direct Connect para alta resiliência

Neste exemplo, o AWS 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 AWS 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 AWS IAM Identity Center, 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 AWS Management Consolecomo 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 AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
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 AWS IAM Identity Center 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 AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Etapa 2: Configurar o modelo de resiliência

Configurar um modelo de alta resiliência

1. Abra o AWS 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 Primeiro provedor de serviços de localização, selecione o AWS 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 AWS 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 AWS 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 AWS 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 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 AWS 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.

(Somente interfaces virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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. AWS 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 AWS 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 AWS 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 1-2147483647.
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 AWS 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 2147483647.

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 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 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 AWS 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.

Use o AWS Direct Connect Resiliency Toolkit AWS Direct Connect para configurar o desenvolvimento e testar a resiliência

Neste exemplo, o AWS 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 AWS 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 AWS IAM Identity Center, 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 AWS Management Consolecomo 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 AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
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 AWS IAM Identity Center 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 AWS IAM Identity Center .

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

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Etapa 2: Configurar o modelo de resiliência

Configurar o modelo de resiliência

1. Abra o AWS 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 Primeiro provedor de serviços de localização, selecione o AWS 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 AWS 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 AWS 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.

Recurso	Informações necessárias
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 AWS 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 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 AWS 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.

(Somente interfaces virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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. AWS 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 AWS 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 AWS 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 1-2147483647.
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 AWS 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 2147483647.

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 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 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 AWS 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.

Configurar uma conexão AWS Direct Connect clássica

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

Etapa 1: inscrever-se em AWS

Para usar AWS 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 AWS IAM Identity Center, 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 AWS Management Consolecomo 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 AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

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 AWS IAM Identity Center 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 AWS IAM Identity Center .

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

Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Etapa 2: solicitar uma conexão AWS Direct Connect dedicada

Para conexões dedicadas, você pode enviar uma solicitação de conexão usando o AWS 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 AWS Direct Connect local em que a conexão deve ser encerrada.

> **Note**
>
> Você não pode usar o AWS 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 AWS Direct Connect conexão

1. Abra o AWS 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 AWS 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 AWS 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 AWS Direct Connect conexões dedicadas e hospedadas.

Aceitar a conexão hospedada

Você deve aceitar a conexão hospedada no AWS 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 AWS 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 AWS 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. Se ele ainda estiver indisponível ou se você não tiver 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. AWS 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 AWS 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.

AWS 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 AWS Direct Connect local. Para obter alta disponibilidade, configure conexões a locais diferentes do AWS 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 AWS 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 AWS 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

Recurso	Informações necessárias
	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 AWS 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 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 AWS 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.

(Somente interfaces virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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. AWS 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 AWS 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 (quadros 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 AWS 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 AWS 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 1-2147483647.
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 AWS 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 2147483647.

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 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 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 AWS 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 AWS 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 AWS Direct Connect.

Para obter mais informações sobre como configurar manualmente o roteador, consulteDownload do arquivo de configuração do roteador do .

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 AWS 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 Solucionar 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 AWS Direct Connect identificador está no rastreamento da rede.

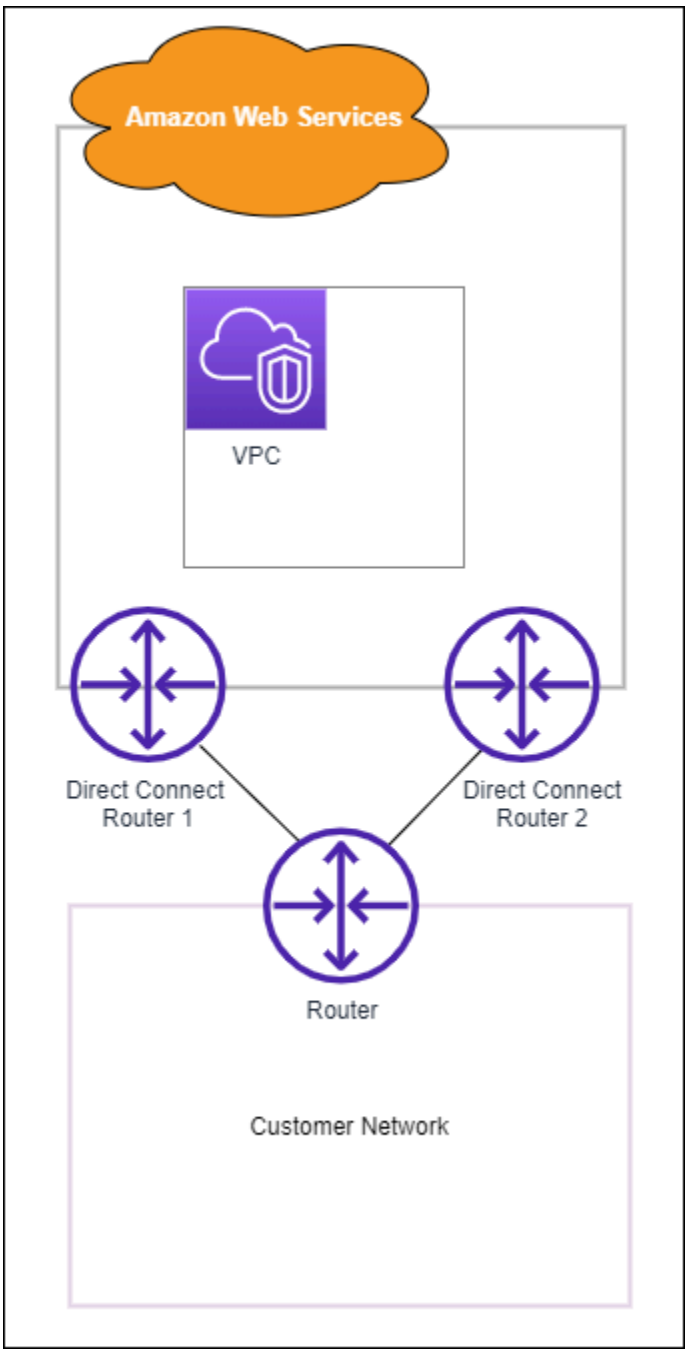
Para verificar sua conexão de interface virtual com a Amazon VPC

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. AWS 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 AWS Direct Connect locais diferentes.

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

AWS Direct Connect Teste de failover

Os modelos de AWS Direct Connect resiliência do Resiliency Toolkit foram projetados para garantir que você tenha o número adequado de conexões de interface virtual em vários locais. Depois de concluir o assistente, use o teste de failover do AWS Direct Connect Resiliency Toolkit para interromper a sessão de emparelhamento do BGP a fim de verificar se o tráfego é direcionado para uma de suas interfaces virtuais redundantes e atende aos 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

peering do BGP e por quanto tempo executar o teste. AWS coloca a sessão de emparelhamento 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 é concluído, ou você interrompe manualmente o teste, a sessão do BGP é AWS restaurada. Depois que o teste for concluído, você poderá usar o AWS Direct Connect Resiliency Toolkit para ajustar sua 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 de testes

AWS exclui o histórico do teste 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 de AWS CloudTrail que um teste foi executado em uma interface virtual.

Tópicos

- Inicie um teste de AWS Direct Connect failover da interface virtual do Resiliency Toolkit
- Veja o histórico de testes de failover da interface virtual do AWS Direct Connect Resiliency Toolkit
- Interrompa um teste de failover da interface virtual do AWS Direct Connect Resiliency Toolkit

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 AWS Direct Connect console ou o. AWS CLI

Como iniciar o teste de failover da interface virtual no console do AWS Direct Connect

1. Abra o AWS 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 comerciais).

      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 AWS Direct Connect console ou o. AWS CLI

Como visualizar o histórico de teste de failover da interface virtual no console do AWS Direct Connect

1. Abra o AWS 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 AWS Direct Connect console ou o. AWS CLI

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

1. Abra o AWS 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.

AWS Direct Connect manutenção

AWS Direct Connect está comprometida em garantir a segurança, a disponibilidade e a escalabilidade do serviço. Para manter esses padrões, é necessária manutenção periódica nos dispositivos de rede de hardware. A manutenção do Direct Connect é 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 emPreparação do evento de manutenção, você pode preparar melhor seu ambiente Direct Connect para evitar interrupções durante 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 Direct Connect ou do recurso de interface virtual. Se você estiver usando uma conexão hospedada pelo Direct Connect com um dos parceiros de entrega do Direct Connect, notificações por e-mail serão enviadas para você e para a conta do parceiro sobre o evento de manutenção. 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.

Eventos de manutenção

- Manutenção planejada do Direct Connect
- Manutenção de emergência do Direct Connect
- Manutenção de terceiros
- Preparação do evento 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 em terminais de dispositivos de hardware, necessárias para melhorar a disponibilidade e fornecer novos recursos.

Esses eventos de manutenção são programados com 14 dias de antecedência e geralmente ocorrem durante uma janela 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 a janela completa de quatro horas expire e você receberá uma notificação quando o trabalho for concluído. Em casos raros em que circunstâncias imprevistas exijam a extensão da janela 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 bilhetes por meio da integração com. 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 AWS Health Dashboard.

Em raras circunstâncias, um evento de manutenção planejado não pode acontecer conforme programado. Caso isso ocorra, enviaremos uma notificação de cancelamento e remarcaremos o evento futuramente, seguindo o mesmo processo descrito acima.

Manutenção de emergência do Direct Connect

Os eventos de manutenção de emergência são iniciados de forma crítica para evitar eventos iminentes de impacto no serviço ou resolver deficiências que já resultaram em uma interrupção na conectividade. Nesses casos, é necessário tomar medidas imediatas para restaurar o endpoint afetado a um estado saudável.

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 de emergência estiver programada ou em andamento e novamente quando for concluída.

Esses eventos geralmente ocorrem durante uma janela de duas horas no local do Direct Connect onde o endpoint do dispositivo reside. As atividades de manutenção geralmente são concluídas nessa janela. Nos casos em que circunstâncias imprevistas exijam a extensão da janela de manutenção, como a substituição 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 do evento 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, consulteResiliência 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 terminal 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 conexões redundantes durante as janelas de manutenção usando comunidades de preferência local do Border Gateway Protocol (BGP). Para obter mais informações sobre comunidades do BGP, consulte. Políticas de roteamento e comunidades BGP

Configurar seu ambiente 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 para esses eventos de manutenção.

Validação de resiliência

Se você configurou seu ambiente Direct Connect para ser resiliente, valide regularmente se seu tráfego é roteado por outras conexões redundantes quando houver conexão. out-of-service Testes proativos regulares podem ajudar a identificar e resolver possíveis problemas antes que eles afetem as cargas de trabalho de produção durante um evento real de manutenção ou cenário de falha. Isso garantirá maior confiança na 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 AWS Direct Connect failover, consulteTeste 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

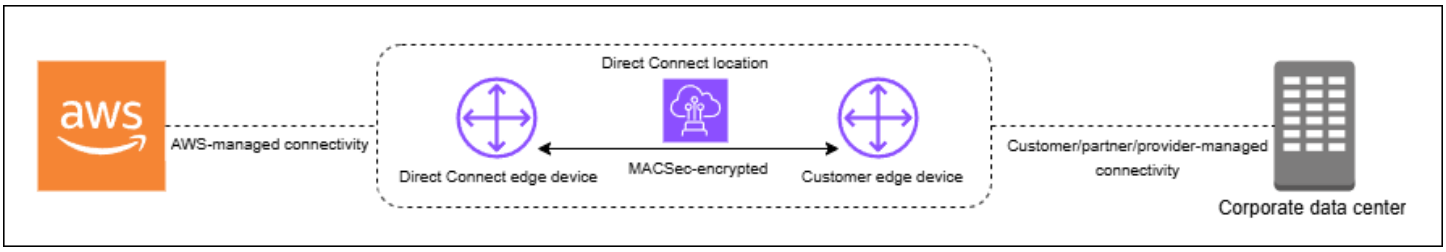
Os dispositivos Direct Connect são compartilhados entre vários clientes. Portanto, não atendemos solicitações específicas de reagendamento ou cancelamento de manutenção. Solicitações de reagendamento ou cancelamento para um cliente podem impactar negativamente outros clientes que usam esse endpoint.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

Segurança MAC em AWS 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 AWS 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 AWS 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 trocadas 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 AWS Direct Connect conexão e, em seguida, os provisiona em seu dispositivo de borda no final da AWS Direct Connect conexão. O Direct Connect suporta somente o modo CAK estático, mas não o modo CAK dinâmico. Como somente o modo CAK estático é suportado, 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, exatamente 64 caracteres de comprimento. O Direct Connect suporta 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 pode permitir tráfego não criptografado em determinados cenários de falha.

  O modo de criptografia pode ser definido durante a configuração da conexão e 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 gire manualmente essas 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 volta para a tecla de trabalho 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 da Chave de Associação Segura (SAK) (automática)

  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. O SAK nunca é armazenado de forma persistente e é regenerado por meio de um processo seguro de derivação de chaves 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**
>
> Suporte para conexões hospedadas MACsec se implementado pelo AWS Direct Connect Parceiro em suas interconexões.

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 AWS 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

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

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. AWS Direct Connect As funções vinculadas ao serviço são predefinidas AWS 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 AWS Direct Connect porque você não precisa adicionar manualmente as permissões necessárias. AWS Direct Connect define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS 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 AWS 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 MACsec considerações e Criação de um LAG.

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

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

- Associar um MACsec CKN/CAK a uma conexão
- Associar um MACsec CKN/CAK 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 AWS Direct Connect local deve corresponder. Para obter mais informações, consulte Download do arquivo de configuração do roteador do .

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

Como opção, é possível remover a associação entre as chaves CKN/CAK e a conexão ou o LAG. Se você precisar remover a associação, consulte um dos seguintes:

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

AWS Direct Connect conexões dedicadas e hospedadas

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

AWS Direct Connect Conexões dedicadas

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

AWS Direct Connect location

> Trabalhe com um AWS Direct Connect parceiro no Programa de Parceria para ajudá-lo a estabelecer circuitos de rede entre um AWS 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 AWS 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 AWS 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 AWS Direct Connect local, primeiro entre em contato com um AWS Direct Connect AWS Direct Connect parceiro no Programa de Parceria. Para obter mais informações, consulte Parceiros da APN que oferecem suporte ao AWS 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 no LoA. O documento PDF impede que uma LoA modificada ou potencialmente fraudulenta seja executada pelo provedor de instalações nos sites 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 obter mais informações sobre precificação, consulte Precificação do AWS 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 AWS Direct Connect conexão.

Tópicos

Crie uma conexão AWS 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 AWS Direct Connect dedicada”.

Para criar uma conexão usando o Assistente de conexão

1. Abra o AWS 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 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 AWS 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 AWS 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(AWS Direct Connect API)

Crie uma conexão AWS Direct Connect clássica

Para conexões dedicadas, você pode enviar uma solicitação de conexão usando o AWS 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 AWS Direct Connect local em que a conexão deve ser encerrada.

> **Note**
>
> Você não pode usar o AWS 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 AWS Direct Connect conexão

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Na tela do AWS 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 AWS 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 AWS 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 AWS Direct Connect LOA-CFA

Você pode baixar o LOA-CFA usando o AWS 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 AWS 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 Solicitando conexões cruzadas em locais AWS Direct Connect.

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

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

Associar um MACsec CKN/CAK a uma conexão AWS 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 AWS 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 AWS 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(AWS Direct Connect API)

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

Você pode remover a associação entre a conexão e a MACsec chave usando o AWS 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 AWS 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(AWS Direct Connect API)

AWS Direct Connect Conexões hospedadas

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

AWS 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 AWS 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 AWS Direct Connect.

> **Note**
>
> Você não pode solicitar uma conexão hospedada por meio do AWS 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 AWS 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 o seu parceiro oferecer suporte ao upgrade/downgrade da sua conexão, você não precisará mais excluir e recriar uma conexão para atualizar ou rebaixar a largura de banda de uma conexão hospedada existente.
- 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 AWS 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 AWS 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 Parceria. O parceiro provisiona a conexão para você. Depois que for configurada, a conexão será visualizada no painel Connections (Conexões) do console do AWS Direct Connect .

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

1. Abra o AWS 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(AWS Direct Connect API)

Excluir uma AWS 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). AWS 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 AWS Direct Connect console ou a linha de comando ou a API.

Para excluir uma conexão

1. Abra o AWS 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(AWS Direct Connect API)

Atualizar uma AWS Direct Connect conexão

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

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

> **Note**
>
> MACsec só está disponível em conexões dedicadas.

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 AWS 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(AWS Direct Connect API)

Exibir detalhes da AWS Direct Connect conexão

Você pode ver o status atual da sua conexão usando o AWS 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 AWS 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(AWS Direct Connect API)

Solicitando conexões cruzadas em locais AWS 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 um equipamento localizado em um AWS Direct Connect local, entre em contato com o fornecedor apropriado para concluir 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, você precisará 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 AWS Direct Connect console.

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

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

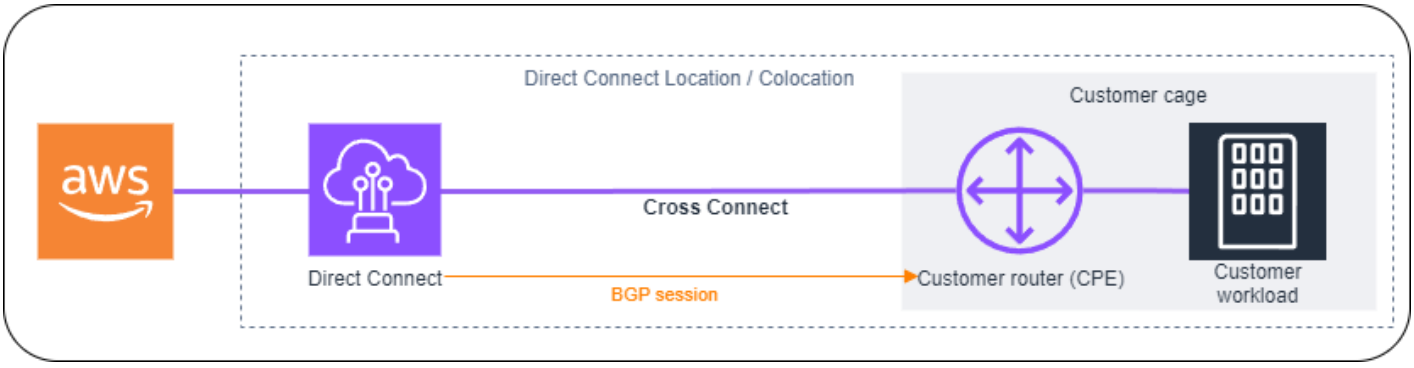
Uma AWS Direct Connect conexão pode fornecer acesso a recursos em outras regiões. Para obter mais informações, consulte Acesso a AWS Direct Connect regiões remotas.

> **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 AWS Direct Connect . Para obter mais informações, consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA).

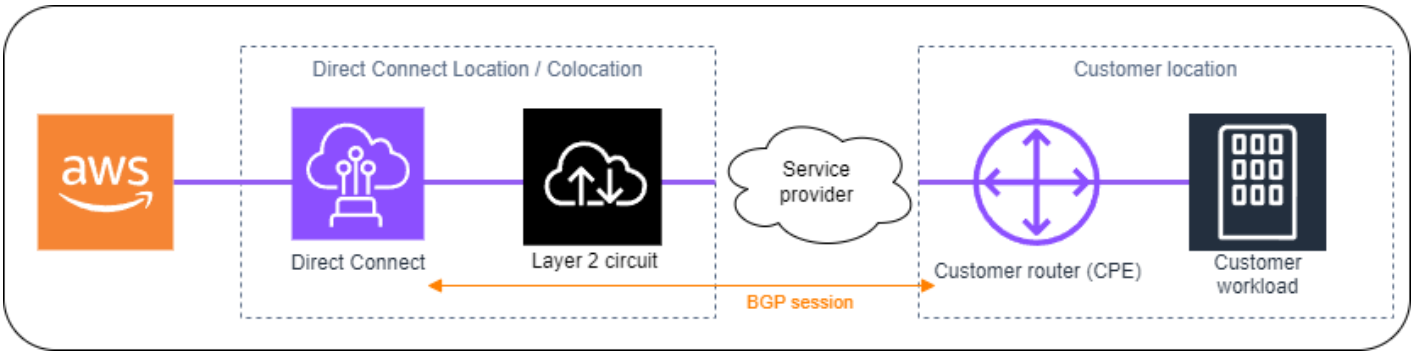
Opções de conectividade

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

- Se você tiver recursos implantados na mesma center/colocation instalação de dados que a localização do Direct Connect, a instalação pode fornecer uma conexão cruzada entre o AWS Direct Connect equipamento 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:

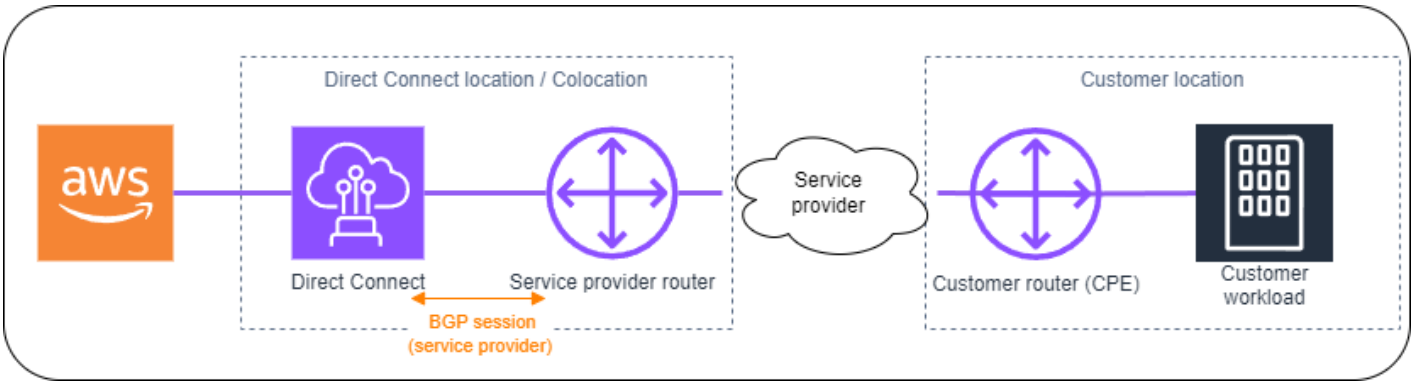


- Amplie a conexão do Direct Connect na Camada 2 (camada de enlace de dados) por meio de um “circuito” da localização do Direct Connect até a localização do cliente ao colaborar com os parceiros do Direct Connect. O roteador instalado no local do cliente formará diretamente uma sessão BGP com o AWS equipamento. 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. Para essa opção de conectividade, o Direct Connect Partner fornece um roteador dentro do local do Direct Connect

que forma uma sessão do Border Gateway Protocol (BGP) com o AWS equipamento. O parceiro Direct Connect então estabeleceu outro BGP com você; por exemplo, isso pode ser 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, Colombo	Entre em contato com a Cologix em sales@cologix.com.
Cologix MIN3, Mineápolis	Entre em contato com a Cologix em sales@cologix.com.
CyrusOne Oeste 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 o QTS em 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.
CoreSite 32k, Nova York	Faça um pedido usando o Portal CoreSite do Cliente. 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 Portal do CoreSite Cliente. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
Imóveis digitais ATL1 eATL2, Atlanta	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
Imóveis digitais IAD38, Ashburn	Entre em contato com a Digital Realty pelo e-mail amazon.orders@digitalrealty.com.
Equinix DC1 — DC6 & DC1 0-D12, Ashburn	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Equinix DAA1 - DC3 & 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, Seacaucus	Entre em contato com a Equinix pelo e-mail awsdealreg@equinix.com.
Redes KIO QRO1, Querétaro, MX	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.

Local	Como solicitar uma conexão
Netrality Data Centers, 2nd floor MMR, Philadelphia	Entre em contato com a Netrality Data Centers pelo e-mail support@netrality.com.
QTS ATL1, Atlanta	Entre em contato com o QTS em AConnect@qtsdatacenters .com.

Oeste dos EUA (Norte da Califórnia)

Local	Como solicitar uma conexão
CoreSite LA1, Los Angeles	Faça um pedido usando o Portal CoreSite do Cliente. 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 Portal CoreSite do Cliente. 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 Portal CoreSite do Cliente. Depois de preencher o formulário, analise a precisão do pedido e, em seguida, aprove-o usando o MyCoreSite site.
EdgeConneX, Fênix	Faça um pedido usando o EdgeOS Customer Portal. Depois de enviar o formulário, EdgeConne X 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 & SV5, São 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 Portal CoreSite do Cliente. Depois de preencher o formulário, analise o pedido para verificar a precisão e, em seguida, aprová-lo usando o site.
Digital Realty SEA1 0, Edifício Westin, 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 de enviar o formulário, EdgeConne X 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 TierPoint em 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 Indonésia em 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 NetMagic Vendas e Marketing gratuitamente pelo telefone 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, Délhi DC2	Entre em contato com a STT em caso de consulta. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Entre em contato com a STT em caso de consulta. AWSDX@sttelemediagdc .in.

Local	Como solicitar uma conexão
STT Hyderabad, Hyderabad DC1	Entre em contato com a STT em caso de consulta. 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, Singapura	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, Auckland DH6	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, Montréal	Entre em contato com a Cologix em sales@cologix.com.
Cologix VAN2, Vancouver	Entre em contato com a Cologix em 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 DigiPlex em helpme@digiplex.com.
Equinix AM3, Amsterdã, Países Baixos	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, Helsinque	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,, Milano ML2, 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, Oberengstringen ZRH51, Suazilândia	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 MedOne em support@Medone.co.il
EdgeConnex, Herzliya	Entre em contato EdgeConnect em info@edgeconnecx.com

Oriente Médio (Bahrein)

Local	Como solicitar uma conexão
AWS Bahrein DC53, Manama	Para concluir a conexão, é possível trabalhar com um de nossos provedores de rede parceiros no local para estabelecer conectivi

Local	Como solicitar uma conexão
	dade. Em seguida, você fornecerá uma Carta de Autorização (LOA) do provedor de rede para AWS o AWS Support Center. AWS conclui a conexão cruzada nesse local.
AWS Bahrein 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 Carta de Autorização (LOA) do provedor de rede para AWS o AWS Support Center. AWS conclui 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.
Centro de SmartHub dados da Etisalat, Fujairah, Emirados Árabes Unidos	Entre em contato com o SmartHub Data Center da Etisalat em 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.

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

AWS Direct Connect interfaces virtuais e interfaces virtuais hospedadas

Você deve criar uma das seguintes interfaces virtuais (VIFs) para começar a usar sua AWS 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 AWS 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 EC2 instâncias da Amazon, Amazon S3, endpoints de API AWS 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 em. 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 AWS 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 AWS 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 para várias interfaces virtuais. • Várias interfaces virtuais podem ter o mesmo gateway virtual/ASN do gateway Direct Connect e o ASN do gateway do cliente, desde que façam parte de diferentes conexões do Direct Connect. Por exemplo: Gateway virtual (ASN 64.496) <---Interface virtual 1 (conexão Direct Connect 1) ---> Gateway do cliente (ASN 64.511) Gateway virtual (ASN 64.496) <---Interface virtual 2 (conexão 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 AWS 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 AWS 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 virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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 oferecerão suporte a Jumbo Frames, inclusive de EC2 instância s com entradas da tabela de rotas estáticas VPC para o Transit Gateway Attachment. Para verificar se uma conexão ou interface virtual suporta quadros jumbo, selecione-a no AWS 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 AWS 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

AWS 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 (quadros 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 AWS 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 AWS 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 EC2 instância não oferecer suporte a quadros grandes, ela descarta quadros enormes do Direct Connect. Todos os tipos de EC2 instância oferecem suporte a quadros jumbo, exceto C1 CC1, T1 e M1. Para obter mais informações, consulte Unidade máxima de transmissão de rede (MTU) para sua EC2 instância no Guia do EC2 usuário da Amazon.

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.

AWS Direct Connect interfaces virtuais

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 dentro da sua AWS Organizations, ou AWS Organizations que sejam diferentes das suas, 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 AWS 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.

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 (quadros 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 AWS 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.

Crie uma interface virtual AWS Direct Connect pública

Quando você cria uma interface virtual pública, pode levar até 72 horas úteis para analisarmos e aprovarmos sua solicitação.

Como provisionar uma interface virtual pública

1. Abra o AWS 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. Para BGP ASN, insira o Número do Sistema Autônomo (ASN) do Border Gateway Protocol do seu roteador local para a nova interface virtual.

      Os valores válidos são 1-2147483647.

> **Note**
>
> Ao estabelecer uma sessão de emparelhamento de BGP com AWS uma interface virtual pública, use 7224 como ASN para estabelecer a sessão de BGP paralelamente. 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 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. 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, 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.

      > **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 Download do arquivo de configuração do roteador do .

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

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

Crie uma interface virtual AWS Direct Connect privada

Você pode provisionar uma interface virtual privada para um gateway privado virtual na mesma região da sua AWS Direct Connect conexão. Para obter mais informações sobre como provisionar uma interface virtual privada para um AWS Direct Connect gateway, consulte. AWS Direct Connect gateways

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 (quadros 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 AWS 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 AWS 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 2147483647.
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 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 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).
8. Faça download da configuração do roteador para o dispositivo. Para obter mais informações, consulte Download do arquivo de configuração do roteador do .

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

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Criação de uma interface virtual de trânsito para o gateway do AWS Direct Connect

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 AWS 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 2147483647.
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 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 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 Download do arquivo de configuração do roteador do .

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

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS 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(AWS Direct Connect API)

Baixe o arquivo de configuração do AWS Direct Connect roteador

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 que foram MACsec ativadas, criaremos automaticamente o arquivo de configuração do 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 baixar o arquivo de configuração do roteador

1. Abra o AWS 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. 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 AWS Direct Connect.

7. Se você precisar configurar manualmente seu roteador para MACsec, use a tabela a seguir como diretriz.

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 confidenc ialidade	0
Indicador ICV	Não
Tempo de rechaveamento do SAK	PN Rollover>

Interfaces AWS Direct Connect virtuais hospedadas

Para usar sua AWS Direct Connect conexão 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 AWS 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 AWS Direct Connect .

Recurso	Informações necessárias
	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 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 AWS 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 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 virtuais privadas e de trânsito) Jumbo frames	A unidade máxima de transmissão (MTU) dos pacotes acima. AWS 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. AWS 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 AWS Direct Connect console e encontre capacidade para quadros jumbo na página de configuração geral da interface virtual.

Crie uma interface virtual privada hospedada no AWS 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 AWS 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 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 1-2147483647.
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 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 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 Download do arquivo de configuração do roteador do .

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

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(AWS Direct Connect API)

Crie uma interface virtual pública hospedada no AWS 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 AWS 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 1-2147483647.
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 Download do arquivo de configuração do roteador do .

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

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct Connect API)

Crie uma interface virtual de trânsito AWS 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 AWS 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 1-2147483647.
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 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 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 Download do arquivo de configuração do roteador do .

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

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct Connect API)

Exibir detalhes da interface AWS Direct Connect virtual

Você pode ver o status atual da sua interface virtual usando o AWS Direct Connect console ou usando 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 AWS Direct Connectconsole 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(AWS Direct Connect API)

Adicionar um peer BGP a uma interface virtual AWS Direct Connect

Adicione ou exclua uma sessão de emparelhamento IPv4 ou IPv6 BGP à sua interface virtual usando o AWS Direct Connect console ou usando a linha de comando ou a API.

Uma interface virtual pode suportar uma única sessão de emparelhamento de IPv4 BGP e uma única sessão de emparelhamento de IPv6 BGP. Você não pode especificar seus próprios IPv6 endereços de peering para uma sessão de peering do IPv6 BGP. A Amazon aloca automaticamente um CIDR IPv6 /125.

O BGP multiprotocolo não é suportado. IPv4 e IPv6 opere no modo de pilha dupla para a interface virtual.

AWS ativa 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 AWS 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 Add peering (Adicionar emparelhamento).
5. (Interface virtual privada) Para adicionar pares IPv4 BGP, faça o seguinte:
   - Selecione IPv4.
   - 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
6. (Interface virtual pública) Para adicionar pares IPv4 BGP, faça o seguinte:
   - Para o IP do seu roteador, insira o endereço de destino IPv4 CIDR para o qual o tráfego deve ser enviado.
   - 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 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 locais de IPv4 link.

7. (Interface virtual privada ou pública) Para adicionar pares IPv6 BGP, escolha. IPv6 Os IPv6 endereços de pares são atribuídos automaticamente a partir do pool de IPv6 endereços da Amazon; você não pode especificar IPv6 endereços 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 1-2147483647.

   Observe que atribuiremos um valor automaticamente se você não inserir um valor.
9. Para fornecer sua própria chave BGP, para Chave de Autenticação BGP, insira sua chave BGP. MD5
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)
- Criar BGPPeer (AWS Direct Connect API)

Excluir uma interface AWS Direct Connect virtual BGP peer

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). Você pode excluir uma interface virtual BGP peer usando o AWS Direct Connect console ou usando a linha de comando ou a API.

Para excluir um BGP de mesmo nível

1. Abra o AWS 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. 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)
- Excluir BGPPeer (AWS Direct Connect API)

Definir a MTU de uma interface virtual AWS 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 AWS Direct Connect console ou usando a linha de comando ou a API.

Para definir a MTU de uma interface virtual privada

1. Abra o AWS 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 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(AWS Direct Connect API)

Adicionar ou remover tags de interface AWS Direct Connect virtual

As tags fornecem uma maneira de identificar a interface virtual. Você pode adicionar ou remover uma tag usando o AWS Direct Connect console ou a linha de comando ou a API se for o proprietário da conta da interface virtual.

Para adicionar ou remover uma tag da interface virtual

1. Abra o AWS 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. 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)

Excluir uma interface AWS Direct Connect virtual

Exclua uma ou mais interfaces virtuais. Para excluir uma conexão, você deve excluir a interface virtual. A exclusão de uma interface virtual interrompe as cobranças de transferência de AWS Direct Connect dados associadas à interface virtual.

Você pode excluir uma interface virtual usando o AWS Direct Connect console, a linha de comando ou a API.

Para excluir uma interface virtual

1. Abra o AWS Direct Connectconsole 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(AWS Direct Connect API)

Aceite uma interface AWS 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 AWS Direct Connect console, a linha de comando ou a API.

Para aceitar uma interface virtual hospedada

1. Abra o AWS 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 AWS 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(AWS 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(AWS 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(AWS Direct Connect API)

Migrar uma interface AWS Direct Connect virtual

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 VLANs IDs são exclusivas; portanto, migrar uma VIF dessa forma significaria que elas VLANs não coincidem. 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 AWS 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 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

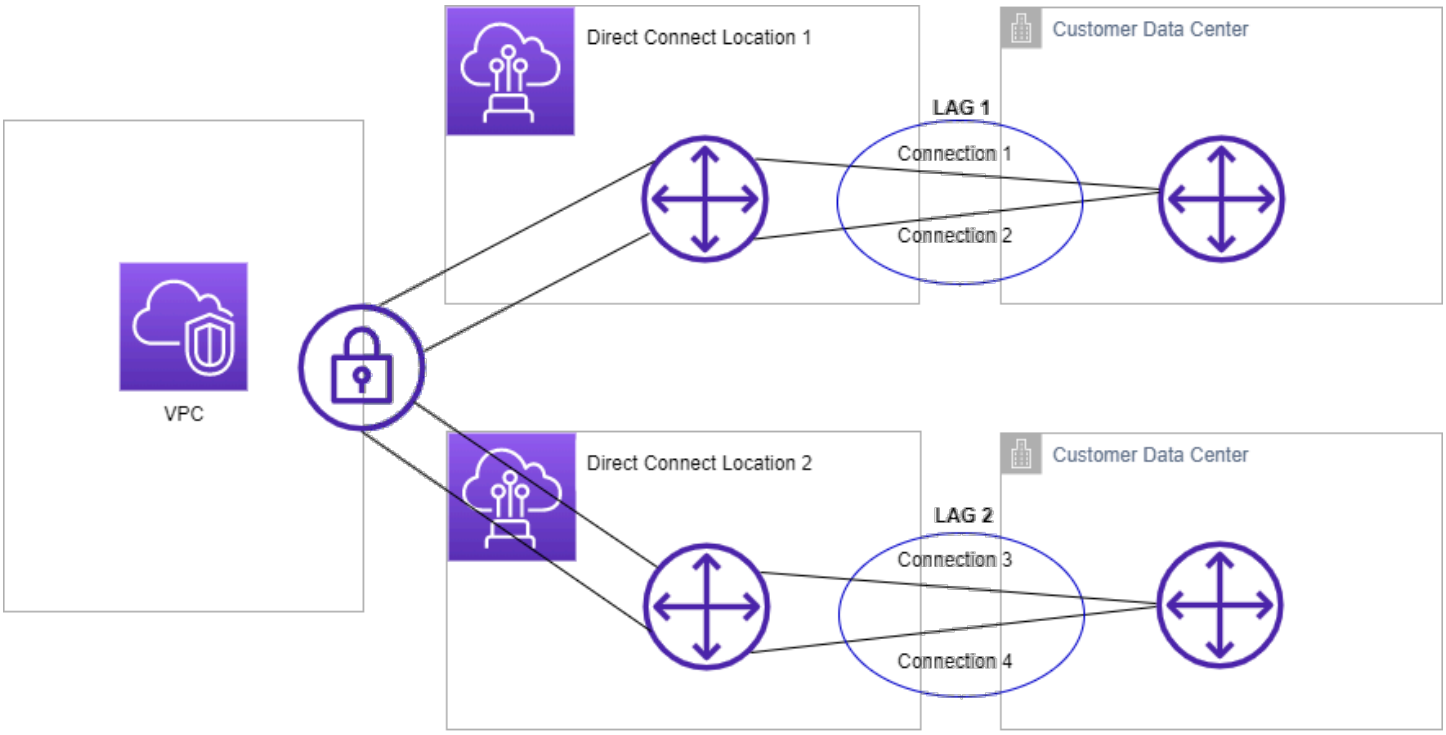
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(AWS Direct Connect API)

AWS Direct Connect grupos de agregação de links () LAGs

Você pode usar várias conexões para aumentar a largura de banda disponível. Um grupo de agregação de links (LAG) é uma interface lógica que usa o Link Aggregation Control Protocol (LACP) para agregar várias conexões em um único AWS Direct Connect endpoint, permitindo tratá-las como uma única conexão gerenciada. LAGs simplifique a configuração porque a configuração do LAG se aplica a todas as conexões no grupo.

> **Note**
>
> O LAG de vários chassis (MLAG) não é suportado pelo. AWS

No diagrama a seguir, você tem quatro conexões, com duas conexões para cada local. Você pode criar um LAG para conexões que terminam no mesmo AWS dispositivo e no mesmo local e, em seguida, usar as duas LAGs em vez das quatro conexões para configuração e 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 terminar no mesmo AWS Direct Connect endpoint.
- LAGs são compatíveis com todos os tipos de interface virtual — pública, privada e de trânsito.

Ao criar um LAG, você pode baixar a Carta de Autorização e Atribuição de Facilidade de Conexão (LOA-CFA) para uma nova conexão física individualmente a partir do console. AWS Direct Connect Para obter mais informações, consulte Carta de autorização e atribuição de instalação de conexão (LoA-CFA).

Todos LAGs têm um atributo que determina o número mínimo de conexões no LAG que devem estar operacionais para que o próprio LAG esteja operacional. Por padrão, new LAGs tem 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, talvez não possamos garantir portas disponíveis suficientes em um determinado AWS Direct Connect endpoint.

Tópicos

- Associe um MACsec CKN/CAK a um LAG de endpoint AWS Direct Connect
- Remova a associação entre uma chave MACsec secreta e um LAG de AWS Direct Connect endpoint
- Excluir um AWS Direct Connect endpoint LAG

MACsec considerações para AWS Direct Connect

Leve o seguinte em consideração quando quiser configurar MACsec emLAGs:

- Quando você cria um LAG a partir de conexões existentes, dissociamos todas as MACsec chaves das conexões. Em seguida, adicionamos as conexões ao LAG e associamos a MACsec chave LAG às conexões.
- Quando você associa uma conexão existente a um LAG, as MACsec chaves atualmente associadas ao LAG são associadas à conexão. Portanto, desassociamos as MACsec chaves da conexão, adicionamos a conexão ao LAG e, em seguida, associamos a MACsec chave LAG à conexão.

Crie um LAG em um endpoint AWS 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 a partir de conexões existentes, as conexões devem estar no mesmo AWS dispositivo (terminar no mesmo AWS Direct Connect endpoint). 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**
>
> Nas conexões existentes, a conectividade com AWS é interrompida durante a criação do LAG.

Para criar um LAG com novas conexões

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha 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 a segurança MAC (MACsec) para a conexão. Em Configurações adicionais, selecione Solicitar uma porta MACsec compatível.

     MACsec só está disponível em 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 AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha 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.
- Minimum links (Links mínimos): o número mínimo de conexões que devem funcionar para que o LAG propriamente dito esteja operacional. Caso você não especifique um valor, atribuímos um valor padrão de 0.

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(AWS Direct Connect API)

Para descrever seu LAGs uso da linha de comando ou da API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct Connect API)

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

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

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 AWS Direct Connect

Depois de criar um LAG, você pode ver seus detalhes usando o AWS Direct Connect console ou usando a linha de comando ou a API.

Para visualizar informações sobre o LAG

1. Abra o AWS 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 AWS 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(AWS Direct Connect API)

Atualizar um LAG em um endpoint AWS Direct Connect

Você pode atualizar os seguintes atributos do grupo de agregação de links (LAG) usando o AWS Direct Connect console ou usando 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 MACsec criptografia do LAG.

  MACsec só está disponível em conexões dedicadas.

  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 AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha 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 AWS Direct Connect)

Associar uma conexão a um LAG em um endpoint AWS Direct Connect

Você pode associar uma conexão existente a um LAG usando o AWS Direct Connect console 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 AWS dispositivo 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 AWS com a conexão é interrompida durante a associação.

Como associar uma conexão a um LAG

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha 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(AWS Direct Connect API)

Desassociar uma conexão de um LAG em um endpoint AWS Direct Connect

Converta uma conexão em autônoma desassociando-a de um LAG usando o AWS Direct Connect console ou usando 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 AWS é interrompida durante a dissociação.

Como desassociar uma conexão de um LAG

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel esquerdo, 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(AWS Direct Connect API)

Associe um MACsec CKN/CAK a um LAG de endpoint AWS Direct Connect

Depois de criar o LAG compatível MACsec, você pode associar um CKN/CAK à conexão usando o AWS Direct Connect console ou usando a linha de comando ou a API.

> **Note**
>
> Você não pode modificar uma chave MACsec secreta depois de 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 MACsec chave a um LAG

1. Abra o AWS 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. Escolha Associar chave.
5. Insira a MACsec chave.

   [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.

   [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 um LAG usando a linha de comando ou a API

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

Remova a associação entre uma chave MACsec secreta e um LAG de AWS Direct Connect endpoint

Você pode remover a associação entre o LAG e a MACsec chave usando o AWS 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 AWS 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(AWS Direct Connect API)

Excluir um AWS Direct Connect endpoint LAG

Se você não precisar mais LAGs, poderá excluí-los. 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.

Você pode excluir um LAG usando o AWS Direct Connect console ou a linha de comando ou a API.

Para excluir um LAG

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. No painel de navegação, escolha LAGs.
3. Selecione o e LAGs, em seguida, 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 AWS Direct Connect)

AWS Direct Connect gateways

Você pode trabalhar com AWS Direct Connect gateways usando o console Amazon VPC ou o. AWS CLI

- Gateways Direct Connect

  Usando um gateway Direct Connect, você pode associar o gateway Direct Connect a um gateway de trânsito com vários VPCs, um gateway privado virtual ou, se você usa AWS Cloud WAN, a uma rede central Cloud WAN.

- Associações de gateways privados virtuais

  Usando um gateway privado virtual, você pode associar o gateway Direct Connect por meio de uma interface virtual privada a uma ou mais VPCs contas localizadas na mesma região ou em regiões diferentes.

- Associações de gateways de trânsito

  Use um gateway Direct Connect para conectar sua conexão Direct Connect por meio de uma interface virtual de trânsito ao VPCs ou VPNs que estão conectados ao seu gateway de trânsito.

- Associações de rede principal de WAN em nuvem

  Use um gateway Direct Connect para associar um gateway Direct Connect a uma rede AWS Network Manager principal.

- Interações de prefixos permitidos

  Use os prefixos permitidos para interagir com gateways de trânsito e gateways privados virtuais.

Tópicos

AWS Direct Connect gateways

Use o AWS Direct Connect gateway para conectar seu VPCs. Você associa um AWS 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 Direct Connect é um componente virtual do Direct Connect projetado para atuar como um conjunto distribuído de refletores de rota BGP. Como opera fora do caminho do tráfego de dados, evita criar um único ponto de falha ou introduzir dependências específicas. Regiões da AWS A alta disponibilidade é inerentemente incorporada em seu design, eliminando a necessidade de vários gateways 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

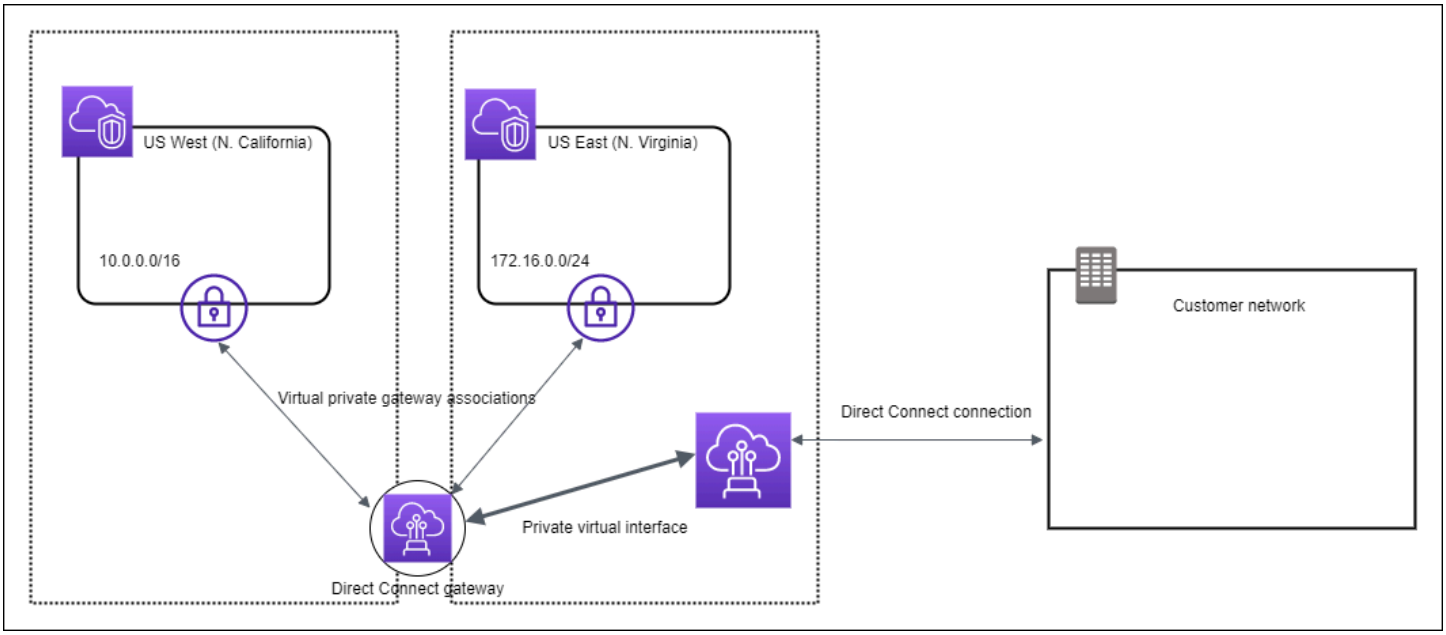
Cenários

A seguir, são descritos apenas alguns cenários para o uso de gateways do Direct Connect.

Cenário: associações de gateways privados virtuais

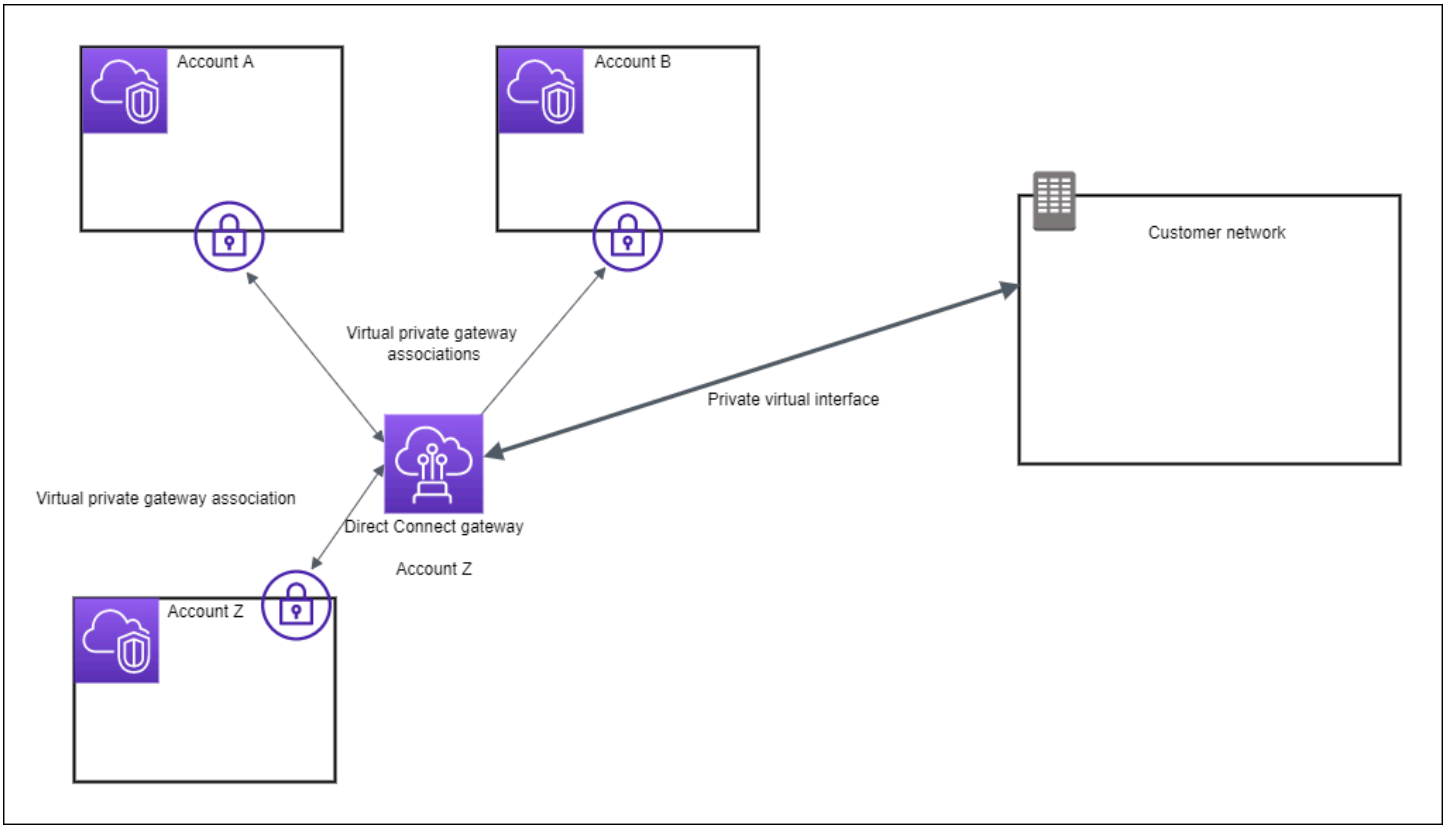
No diagrama a seguir, o gateway Direct Connect permite que você use sua AWS Direct Connect conexão na região Leste dos EUA (Norte da Virgínia) para acessar VPCs sua conta nas regiões Leste dos EUA (Norte da Virgínia) e Oeste dos EUA (Norte da Califórnia).

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 AWS Direct Connect local. Há uma conexão do AWS Direct Connect proveniente do local para o data center do cliente.



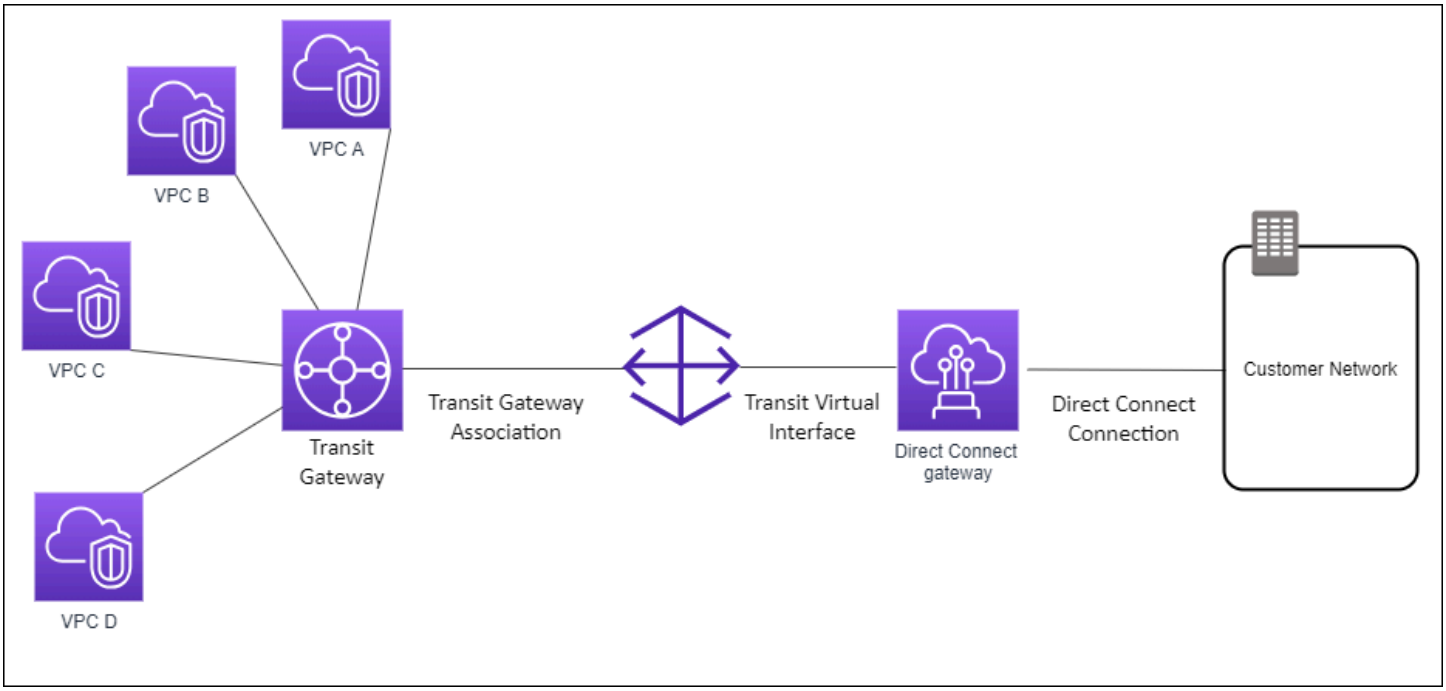
Cenário: associações de gateways privados virtuais entre contas

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.

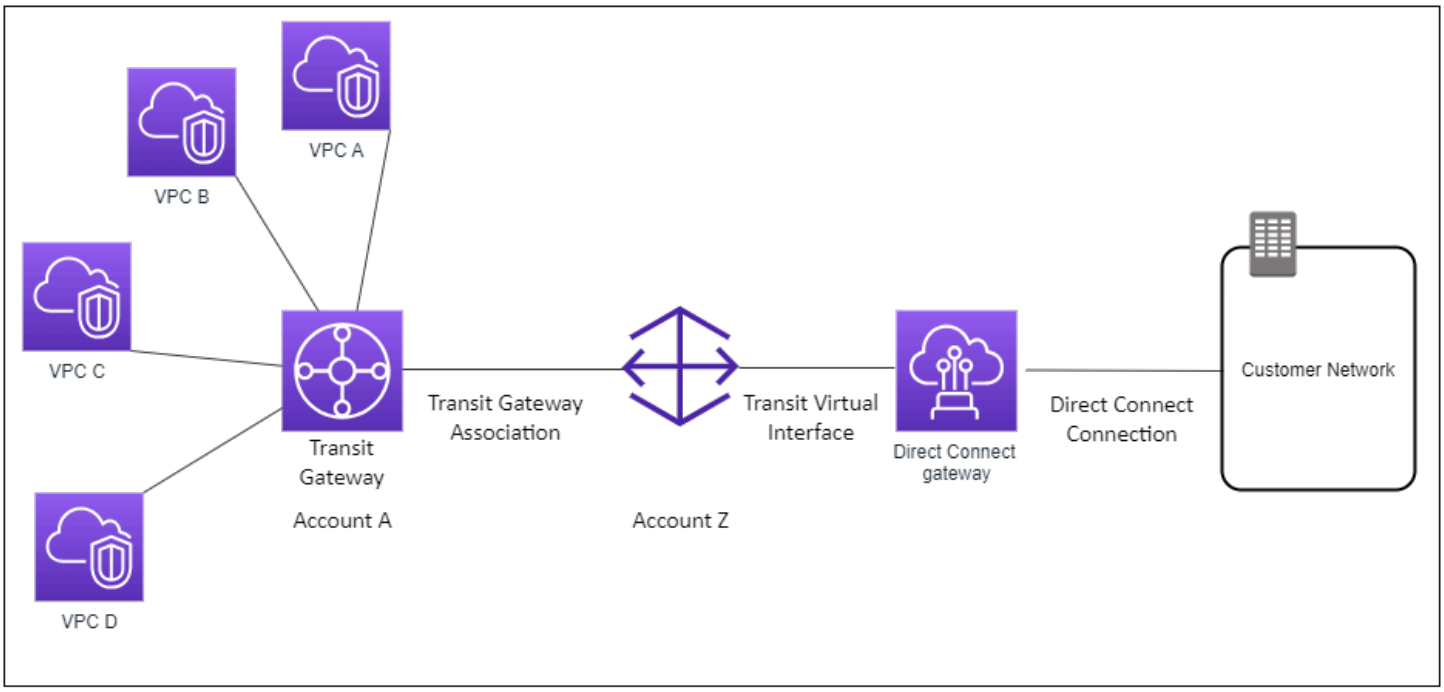
Essa configuração oferece os benefícios abaixo. É possível:

- 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.



Crie um AWS Direct Connect gateway

É possível criar um gateway do Direct Connect em qualquer região compatível usando o console do AWS Direct Connect ou a linha de comando ou a API.

Para criar um gateway Direct Connect

1. Abra o AWS Direct Connectconsole 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 Direct Connect para usar com uma rede principal 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(AWS Direct Connect API)

Migrar de um gateway privado virtual para um AWS 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, 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.

   Se o gateway Direct Connect ainda não existir, você precisará 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.

Exclusão de um gateway do AWS Direct Connect

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 AWS 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 AWS 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(AWS Direct Connect API)

AWS Direct Connect associações de gateway privado virtual

Você pode usar um AWS Direct Connect gateway para conectar sua AWS Direct Connect conexão por meio de uma interface virtual privada a uma ou mais VPCs contas localizadas na mesma região

ou em regiões diferentes. Associe o gateway Direct Connect a um gateway privado virtual para a VPC. Em seguida, você cria uma interface virtual privada para sua AWS Direct Connect conexão com o gateway Direct Connect. Você pode anexar várias interfaces virtuais privadas ao seu gateway Direct Connect.

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.
- O VPCs ao qual você se conecta por meio de um gateway Direct Connect não pode ter blocos CIDR sobrepostos. Se você adicionar um bloco IPv4 CIDR a uma VPC associada a um gateway Direct Connect, certifique-se de que o bloco CIDR não se sobreponha a um bloco CIDR existente para qualquer outra VPC associada. Para obter mais informações, consulte Adicionar blocos IPv4 CIDR 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 os VPCs que estão associados 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 todos os conectados VPCs pelo ASN atribuído a ele.

Para conectar sua AWS Direct Connect conexão a uma VPC somente na mesma região, você pode criar 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 AWS Direct Connect conexão 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

- Crie um gateway privado AWS Direct Connect virtual
- Associar ou desassociar AWS Direct Connect gateways privados virtuais
- Crie uma interface virtual privada para o AWS Direct Connect gateway
- Associe um gateway privado AWS Direct Connect virtual em todas as contas

Crie um gateway privado AWS Direct Connect virtual

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 AWS 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 todos os conectados VPCs 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 AWS Direct Connectconsole 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 do Amazon EC2 Query)
- 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 do Amazon EC2 Query)

- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Associar ou desassociar AWS Direct Connect gateways privados virtuais

Você pode associar ou desassociar um gateway privado virtual e um gateway Direct Connect usando o AWS 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 AWS 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 AWS 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(AWS 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(AWS 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(AWS Direct Connect API)

Crie uma interface virtual privada para o AWS Direct Connect gateway

Para conectar sua AWS 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 AWS 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 AWS 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 2147483647.

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 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 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 Download do arquivo de configuração do roteador do .

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

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (API do AWS 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(AWS Direct Connect API)

Associe um gateway privado AWS Direct Connect virtual em todas as contas

Você pode associar um gateway Direct Connect a um gateway privado virtual de propriedade de qualquer AWS conta. 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 a mesma CIDRs ou menor CIDRs seja anunciada 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.

AWS Direct Connect gateways e associações de gateways de trânsito

Você pode usar o AWS Direct Connect gateway para conectar sua conexão Direct Connect por meio de uma interface virtual de trânsito ao VPCs ou VPNs que estão conectados ao seu gateway de trânsito. Você associa um gateway do Direct Connect com o gateway de trânsito. Em seguida, crie uma interface virtual de trânsito para sua AWS Direct Connect conexão 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 em regiões diferentes, use um exclusivo ASNs para cada gateway de trânsito.
- Qualquer endereço de point-to-point conectividade usando um `/30` intervalo — por exemplo, `192.168.0.0/30` — não se propaga para um gateway de trânsito.

Associar um gateway de trânsito entre contas

Você pode associar um gateway Direct Connect existente ou um novo gateway Direct Connect a um gateway de trânsito de propriedade de qualquer AWS conta. 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 local AWS para o gateway de trânsito, mesmo que o VPCs anexo ao gateway de trânsito não tenha sido atribuído CIDRs. 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

- Associação ou desassociação do AWS Direct Connect com um gateway de trânsito

- Crie uma interface virtual de trânsito para o AWS Direct Connect gateway
- Crie um gateway de trânsito e uma proposta de AWS Direct Connect associação
- Aceite ou rejeite um gateway de trânsito e uma proposta de AWS Direct Connect associação
- Atualize os prefixos permitidos para um gateway de trânsito e associação AWS Direct Connect
- Excluir um gateway de trânsito e uma proposta de AWS Direct Connect associação

Associação ou desassociação do AWS Direct Connect com um gateway de trânsito

Associe ou desassocie um gateway de trânsito usando o AWS Direct Connect console ou usando a linha de comando ou a API.

Para associar um gateway de trânsito

1. Abra o AWS 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 AWS 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 AWS 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 para o qual você 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(AWS 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(AWS 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(AWS 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(AWS Direct Connect API)

Crie uma interface virtual de trânsito para o AWS Direct Connect gateway

Para conectar sua AWS 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 AWS 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 AWS 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 2147483647.

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 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 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 Download do arquivo de configuração do roteador do .

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

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface (API do AWS 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(AWS Direct Connect API)

Crie um gateway de trânsito e uma proposta de AWS 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 AWS Direct Connect. Você pode criar uma proposta de associação usando o AWS Direct Connect console ou usando a linha de comando ou a API.

Para criar uma proposta de associação

1. Abra o AWS 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(AWS Direct Connect API)

Aceite ou rejeite um gateway de trânsito e uma proposta de AWS Direct Connect associação

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. Você pode aceitar ou rejeitar a proposta de associação usando o AWS Direct Connect console ou a linha de comando ou a API.

Para aceitar uma proposta de associação

1. Abra o AWS Direct Connectconsole 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 AWS Direct Connectconsole 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-propostas de associação ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(AWS Direct Connect API)

Para aceitar uma proposta de associação usando a linha de comando ou a API

- accept-direct-connect-gateway-proposta de associação ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Para rejeitar uma proposta de associação usando a linha de comando ou a API

- delete-direct-connect-gateway-proposta de associação ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(AWS Direct Connect API)

Atualize os prefixos permitidos para um gateway de trânsito e associação AWS Direct Connect

Você pode atualizar os prefixos permitidos do gateway de trânsito pelo gateway Direct Connect usando o AWS 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 AWS 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(AWS Direct Connect API)

Excluir um gateway de trânsito e uma proposta de AWS 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 AWS Direct Connect console ou a linha de comando ou a API.

Para excluir uma proposta de associação

1. Abra o AWS 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(AWS Direct Connect API)

AWS Direct Connect associações de gateway e rede principal de AWS Cloud WAN

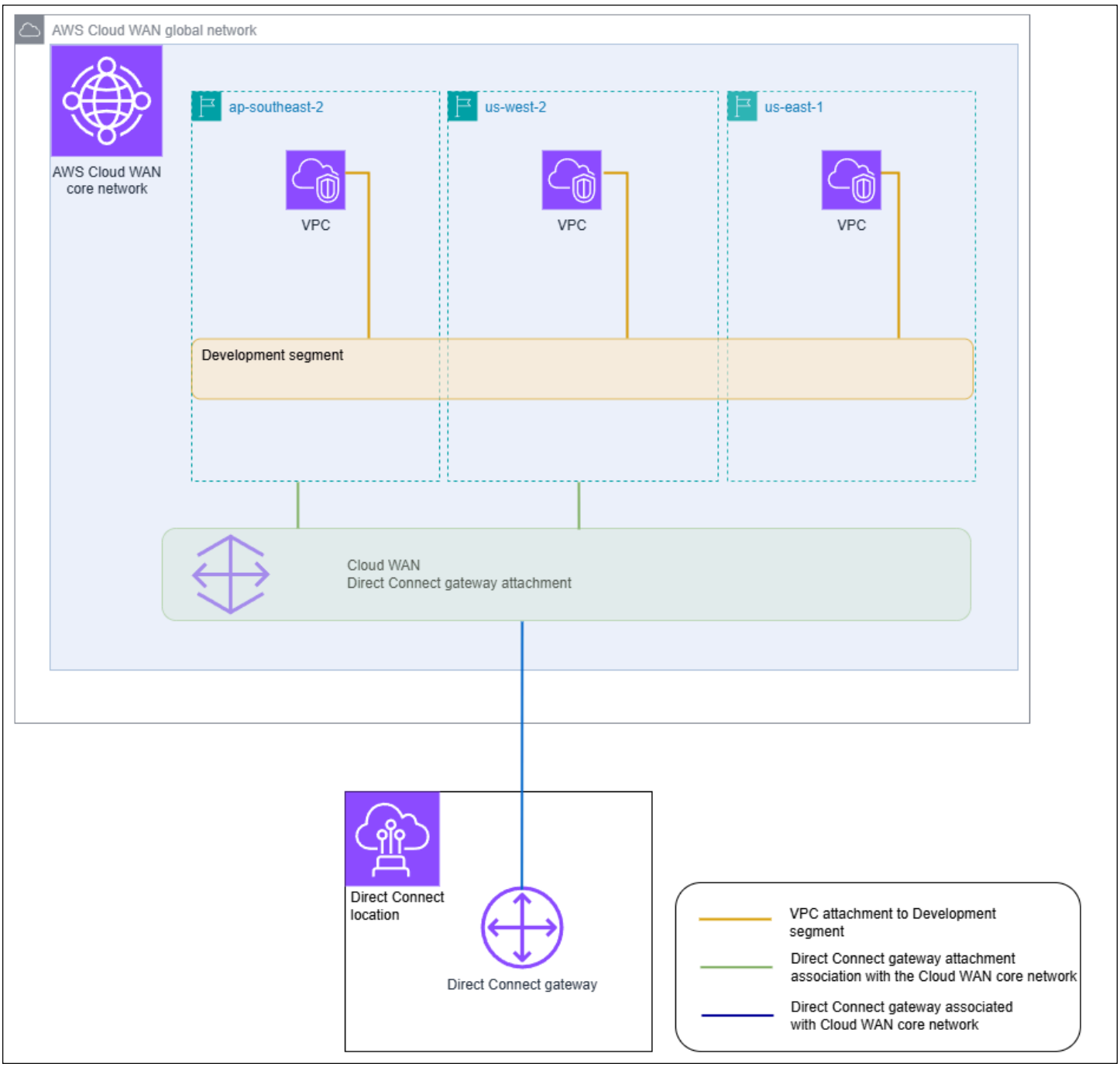
Associe um AWS Direct Connect gateway a uma rede principal do AWS Cloud WAN usando um tipo de anexo Direct Connect no Cloud WAN. Essa associação direta direciona o tráfego entre os

pontos de presença selecionados da sua rede principal e suas conexões do Direct Connect usando o caminho mais curto disponível.

O tipo de anexo do gateway Direct Connect oferece suporte ao BGP (protocolo Border Gateway) para propagação automática de informações de roteamento entre sua rede principal e locais locais. O anexo do Direct Connect também oferece suporte aos recursos padrão do Cloud WAN, como gerenciamento central baseado em políticas, automação de anexos com base em tags e segmentação para configurações avançadas de segurança.

> **Note**
>
> A associação entre uma rede principal e um gateway Direct Connect é criada, excluída e gerenciada do console Cloud WAN no Network Manager. 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 Direct Connect ou a linha de comando para verificar se uma associação foi criada.

O exemplo a seguir mostra uma rede global Cloud WAN com três regiões dentro da rede principal Cloud WAN. Cada região tem sua própria VPC conectada a um segmento de desenvolvimento de rede principal compartilhado entre essas três regiões. Usando o Cloud WAN, um anexo do gateway Direct Connect é criado dentro do Cloud WAN usando um gateway Direct Connect, que foi criado usando o Direct Connect. O anexo está associado a duas das três regiões, ap-southeast-2 e us-west-2, e tem acesso permitido ao segmento de Desenvolvimento. Embora us-east-1 compartilhe o mesmo segmento de desenvolvimento, o anexo do gateway Direct Connect não é compartilhado com essa região e, portanto, não está disponível.



Tópicos

- Pré-requisitos
- Considerações
- Associações de gateway Direct Connect a uma rede central Cloud WAN
- Verificar uma associação de AWS Direct Connect gateway a uma rede principal de WAN em AWS nuvem

Pré-requisitos

A associação do gateway Direct Connect com uma rede central Cloud WAN exige o seguinte:

- Um gateway Direct Connect existente. 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 informações sobre o Cloud WAN, consulte o Guia do usuário do AWS Cloud WAN.

Considerações

Os limites a seguir se aplicam às associações de gateway Direct Connect com uma rede central Cloud WAN:

- Um gateway Direct Connect pode ser associado a uma única rede central 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 então usar esse gateway para outros tipos de associação.
- O anexo do gateway Cloud WAN Direct Connect usa o tipo de interface virtual de trânsito para conectividade.
- O anexo do Cloud WAN não suporta listas de prefixos permitidos. Todos os prefixos em um segmento de rede principal serão anunciados no gateway Direct Connect associado a esse segmento.
- A cota para prefixos máximos que podem ser anunciados localmente ou AWS por meio de uma interface virtual de trânsito é diferente da cota para prefixos anunciados de uma rede central do Cloud WAN para o local. As cotas para outros recursos do Direct Connect usados com uma associação de Cloud WAN também são aplicáveis. Consulte Cotas do Direct Connect.
- O atributo AS-PATH BGP será mantido na rede principal, no gateway Direct Connect e na interface virtual.
- O ASN de um gateway Direct Connect deve estar fora do intervalo de ASN configurado para a rede principal do Cloud WAN. Por exemplo, se você tiver um intervalo de ASN de 64512 a 65534 para a rede principal, o ASN do gateway Direct Connect deverá usar um ASN fora desse intervalo.
- O Cloud WAN pode não oferecer suporte a tipos específicos de anexo usando o tipo de anexo 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 Network Health Indicator não é suportado. Para obter mais informações, consulte Usando o Monitor de Amazon CloudWatch Rede no Guia Amazon CloudWatch do Usuário.

Associações de gateway Direct Connect a uma rede central 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 Direct Connect existente a uma rede principal do Cloud WAN, crie um novo anexo do Direct Connect no console do Cloud WAN. Depois que o anexo do Direct Connect for criado, a associação será estabelecida. Por padrão, ao criar a associação, você pode escolher o padrão para incluir todos os pontos de borda da rede principal no segmento de rede principal escolhido. Como alternativa, você pode especificar localizações de 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 AWS Direct Connect gateway a uma rede principal de WAN em AWS nuvem

Você pode verificar a associação de um gateway Direct Connect a uma rede principal do Cloud WAN usando o console do Direct Connect, a API Direct Connect ou a linha de comando.

Para verificar a associação do gateway Direct Connect a uma rede principal do Cloud WAN usando o console

1. Abra o AWS Direct Connectconsole em https://console.aws.amazon.com/directconnect/v2/home.
2. Escolha gateways Direct Connect no painel de navegação.
3. Escolha o anexo do gateway Direct Connect para o qual você deseja visualizar a associação.
4. Escolha a guia Associações de gateway.

   - A coluna ID exibe a ID da rede principal à qual o gateway Direct Connect está associado.
   - A coluna Estado é exibida associada.
   - A coluna Tipo de associação exibe Cloud WAN Core Network.

Para verificar a associação do gateway Direct Connect a uma rede principal do Cloud WAN usando a linha de comando ou a API

- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)
- describe-direct-connect-gateway-associação ()AWS CLI

Interações de prefixos permitidos para gateways AWS 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 o mesmo CIDRs ou um intervalo menor de CIDRs sejam anunciados no gateway 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 eliminar 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 local de ou para um gateway Direct Connect para o gateway de trânsito, mesmo quando o VPCs conectado ao gateway de trânsito não está atribuído CIDRs. 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 o mesmo ou menores. CIDRs

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.

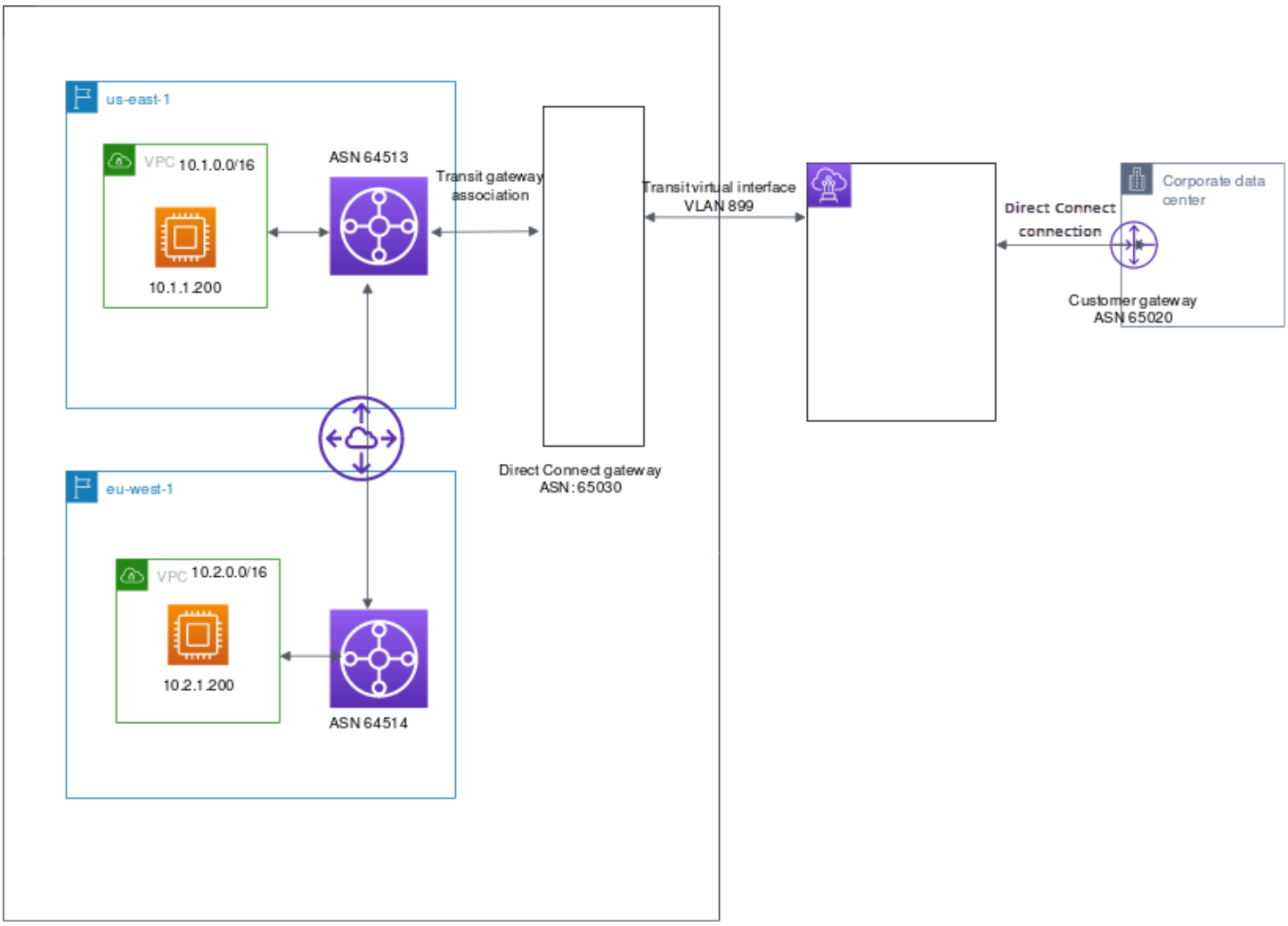
Não é permitido ter sobreposições de prefixos permitidos quando houver vários gateways de trânsito associados a um gateway do Direct Connect. Por exemplo, se você tiver um gateway de trânsito com uma lista de prefixos permitidos que inclua 10.1.0.0/16 e um segundo gateway de trânsito com uma lista de 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 a 0.0.0.0/0 inclui todas as IPv4 redes, você não pode configurar a 0.0.0.0/0 se vários gateways de trânsito estiverem associados a um gateway 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 eliminar somente o tráfego que usa esse prefixo.

Exemplo: permitido em prefixos em uma configuração de gateway de trânsito

Considere a configuração em que você tem instâncias em duas AWS regiões diferentes 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 AWS Direct Connect .



Configure as seguintes opções para os recursos:

- Gateway 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 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 Direct Connect com o gateway de trânsito: defina os prefixos permitidos como 10.0.0.0/8.

  Esse bloco CIDR abrange os dois 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 com um destino de 0.0.0.0/0 e o ID do gateway de trânsito como destino. Isso permite que

o tráfego da VPC chegue ao gateway Direct Connect. Para obter mais informações sobre o roteamento para um gateway de trânsito, consulte Roteamento para um gateway de trânsito no Guia do usuário da Amazon VPC.

AWS Direct Connect Recursos de tags

Uma tag é um rótulo que o proprietário do recurso atribui aos seus AWS Direct Connect recursos. Cada tag consiste de uma chave e um valor opcional, que podem ser definidos. As tags permitem que o proprietário do recurso categorize seus AWS Direct Connect recursos de maneiras diferentes, por exemplo, por finalidade ou 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 AWS Direct Connect conexões 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 nenhum significado semântico AWS Direct Connect e são interpretadas estritamente como uma sequência 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.

Você pode marcar os seguintes AWS Direct Connect recursos usando o AWS Direct Connect console, a AWS Direct Connect API, o AWS CLI AWS Tools for Windows PowerShell, o ou um AWS SDK. 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 Amazon Resource Names (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 tags

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 `aws:` prefixo está reservado para AWS uso. 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 suportadas somente para conexões, interconexões e. LAGs Para obter informações sobre como usar tags com o gerenciamento de custos, consulte Usando tags de alocação de custos no Guia do Gerenciamento de Faturamento e Custos da AWS usuário.

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 AWS Direct Connect. Os tópicos a seguir mostram como configurar para atender AWS Direct Connect aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Direct Connect recursos.

Tópicos

Proteção de dados em AWS Direct Connect

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Direct Connect. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os 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 Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center 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. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint 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 quando você trabalha com AWS Direct Connect ou Serviços da AWS usa o console, a API ou AWS SDKs. AWS CLI 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 na AWS Direct Connect
- Criptografia no AWS Direct Connect

Privacidade do tráfego entre redes na 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 ter 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 ter mais informações, consulte Associações de gateways privados virtuais e Associações de gateways de trânsito.

Criptografia no 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 de tráfego de EC2 instâncias, consulte Criptografia em trânsito no Guia EC2 do usuário da Amazon.

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 AWS Direct Connect conexões que oferecem suporte MACsec para criptografar seus dados do data center corporativo até o AWS 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 o AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz no Direct Connect.

Usuário do serviço: se você usar o serviço Direct Connect para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. Conforme você use mais recursos do Direct Connect para realizar seu trabalho, poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se não conseguir acessar um recurso no Direct Connect, consulte Solução de problemas de identidade e acesso do Direct Connect.

Administrador do serviço: se você for o responsável pelos recursos do Direct Connect na empresa, provavelmente terá acesso total ao Direct Connect. Cabe a você determinar quais atributos e recursos do Direct Connect os usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Direct Connect, consulte Funcionamento do Direct Connect com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode criar políticas para gerenciar o acesso ao Direct Connect. Para visualizar exemplos de políticas baseadas em identidade do Direct Connect que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Direct Connect.

Autenticação com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como usuário do Usuário raiz da conta da AWS IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações

usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, 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 de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Casos de uso para usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a

um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). 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.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um 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 obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para 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 a serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e

fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon 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 é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

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.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. 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.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política 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. 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. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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.

Listas de controle de acesso (ACLs)

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.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade.

As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, 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
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 você pode anexar 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. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. 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. Você deve 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, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em

identidade adicional será necessária. 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. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática

recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver

marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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 as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

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 obter mais informações 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 baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Direct Connect

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil do IAM (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal entre serviços para o Direct Connect

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. 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 obter mais informações, 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 presumir o perfil para 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 funções vinculadas 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. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

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
- Ações, recursos e condições do Direct Connect
- Uso do console do Direct Connect
- Permitir que os usuários visualizem suas próprias permissões
- Acesso somente leitura ao AWS Direct Connect
- Acesso total ao AWS Direct Connect
- Exemplos de política baseada em identidade do Direct Connect usando condições baseadas em tag

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 obter mais informações, 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 obter mais informações 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: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode 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 AWS CloudFormation. Para obter mais informações, 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 obter mais informações, 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 obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações 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. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não

têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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 EC2 instância da Amazon com a operação de EC2 `DescribeVpnGateways` API da Amazon, você inclui a `ec2:DescribeVpnGateways` ação na política dessa 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 AWS 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 AWS 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. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, 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}`

Tipo de recurso	ARN
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, você deve 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 AWS 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 declaração de política do IAM, o especificado `Effect` funcionará.

No exemplo a seguir, nenhum dos especificados `Effect` será bem-sucedido se a `DescribeConnections` ação for chamada sem uma `connectionId` passagem 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, a `DescribeConnections` ação `"Effect": "Allow"` será bem-sucedida, pois `*` foi fornecida para o `Resource` campo da declaração de política do IAM, independentemente de ter `connectionId` sido especificada 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` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. 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.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. 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 leitura ao AWS Direct Connect

O exemplo de política a seguir concede acesso de AWS Direct Connect leitura a.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Acesso total ao AWS Direct Connect

O exemplo de política a seguir concede acesso total AWS 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 AWS 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 AWS 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. AWS Direct Connect As funções vinculadas ao serviço são predefinidas AWS 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 AWS Direct Connect porque você não precisa adicionar manualmente as permissões necessárias. AWS Direct Connect define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma,

só AWS 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 AWS Direct Connect recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços suportados por perfis vinculados a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para AWS Direct Connect

AWS Direct Connect usa uma função vinculada ao serviço chamada. `AWSServiceRoleForDirectConnect` Isso AWS 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`.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para que o perfil vinculado a serviço `AWSServiceRoleForDirectConnect` seja criado com êxito, a identidade do IAM com a qual você usa o AWS 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 Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para AWS 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 AWS Direct Connect ao serviço que permite recuperar os MACsec segredos armazenados em AWS Secrets Manager seu nome na AWS Management Console, 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. AWS 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 obter mais informações, 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 AWS Direct Connect

AWS 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 obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para AWS 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 AWS Management Console, a AWS CLI, ou a AWS API, AWS 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 AWS 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 AWS 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 obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a AWS Direct Connect serviços

AWS 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 mais informações, consulte Políticas gerenciadas pela AWS no Manual 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 AWS Direct Connect a.

Para visualizar as permissões para esta política, consulte AWSDirectConnectFullAccess no AWS Management Console.

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. AWS Direct Connect

Para visualizar as permissões para esta política, consulte AWSDirectConnectReadOnlyAccess no AWS Management Console.

AWS política gerenciada: AWSDirect ConnectServiceRolePolicy

Essa política é anexada à função vinculada ao serviço chamada AWSServiceRoleForDirectConnectpara permitir AWS Direct Connect a recuperação de segredos de segurança MAC em seu nome. Para obter mais informações, consulte the section called “Perfis vinculados a serviço”.

Para visualizar as permissões para esta política, consulte AWSDirectConnectServiceRolePolicy no AWS Management Console.

AWS Direct Connect atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS 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 AWS 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
AWS Direct Connect começou a rastrear alterações	AWS 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

Você pode 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.

Registro e monitoramento em AWS Direct Connect

Você pode usar as seguintes ferramentas de monitoramento automatizadas para observar o AWS Direct Connect e gerar relatórios 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 mais informações, 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 Registre chamadas de AWS Direct Connect API usando AWS CloudTrail Trabalhar com arquivos de CloudTrail log no Guia AWS CloudTrail do usuário.

Para obter mais informações, consulte Monitoramento de recursos do Direct Connect.

Validação de conformidade para AWS Direct Connect

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o

Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Direct Connect

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. 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 AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, AWS Direct Connect oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Para obter informações sobre como usar a VPN com AWS Direct Connect, consulte AWS Direct Connect Plus VPN.

Failover

O AWS Direct Connect Resiliency Toolkit fornece um assistente de conexão com vários modelos de resiliência que ajudam você a solicitar conexões dedicadas para atingir seu 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.

- 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 AWS Direct Connect Kit de ferramentas de resiliência.

Segurança da infraestrutura em AWS Direct Connect

Como serviço gerenciado, AWS Direct Connect é protegido pelos procedimentos AWS globais de segurança de rede. Você usa chamadas de API AWS publicadas para acessar AWS Direct Connect pela 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 de rede, mas AWS Direct Connect oferece suporte a políticas de acesso baseadas em recursos, que podem incluir restrições com base no endereço IP de origem. Você também pode usar AWS Direct Connect políticas para controlar o acesso de endpoints específicos da Amazon Virtual Private Cloud (Amazon VPC) ou específicos. VPCs Efetivamente, isso isola o acesso à rede a um determinado AWS Direct Connect recurso somente da VPC específica dentro da AWS rede. 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 AWS funciona para proteger com mais segurança sua rede contra o sequestro do BGP, consulte Como AWS está ajudando a proteger o roteamento da Internet.

Use a AWS Direct Connect CLI

Você pode usar o AWS CLI para criar e trabalhar com AWS Direct Connect recursos.

O exemplo a seguir usa os AWS CLI comandos para criar uma AWS Direct Connect conexão. 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 saber a velocidade da porta necessária e a AWS Direct Connect localização. Para obter mais informações, consulte Conexões dedicadas e hospedadas.

Para criar uma solicitação de conexão

1. Descreva os AWS Direct Connect locais 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 fazer um pedido de AWS Direct Connect conexão, você deve criar uma interface virtual para começar a usá-la. Crie uma interface virtual privada para se conectar à VPC. Ou você pode criar uma interface virtual pública para se conectar a AWS serviços que não estão em uma VPC. Você pode criar uma interface virtual que ofereça suporte IPv4 ao IPv6 tráfego.

Antes de começar, certifique-se de que você tenha lido os pré-requisitos em the section called “Pré-requisitos para interfaces virtuais”.

Quando você cria uma interface virtual usando o AWS CLI, a saída inclui informações genéricas de configuração do roteador. Para criar uma configuração de roteador específica para seu dispositivo, use o AWS Direct Connect console. Para obter mais informações, consulte Download do arquivo de configuração do roteador do .

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 IPv4 tráfego, você precisa de IPv4 endereços privados para cada extremidade da sessão de peering do BGP. Você pode especificar seus próprios IPv4 endereços ou deixar que a Amazon gere os endereços para você. No exemplo a seguir, os IPv4 endereços 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 que ofereça suporte ao IPv6 tráfego, use o mesmo comando acima e especifique `ipv6` o `addressFamily` parâmetro. Você não pode especificar seus próprios IPv6 endereços para a sessão de emparelhamento do BGP; a Amazon aloca seus endereços. IPv6

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 IPv4 tráfego, você também deve especificar IPv4 endereços públicos para cada extremidade da sessão de emparelhamento do BGP e as IPv4 rotas públicas que você anunciará pelo BGP. O exemplo a seguir cria uma interface virtual pública para IPv4 tráfego.

```
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 que ofereça suporte ao IPv6 tráfego, você pode especificar IPv6 as rotas que serão anunciadas pelo BGP. Você não pode especificar IPv6 endereços para a sessão de emparelhamento; a Amazon aloca IPv6 endereços para você. O exemplo a seguir cria uma interface virtual pública para IPv6 tráfego.

```
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 AWS Direct Connect API usando AWS CloudTrail

AWS Direct Connect é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Direct Connect. CloudTrail captura todas as chamadas de API AWS Direct Connect como eventos. As chamadas capturadas incluem chamadas do AWS Direct Connect console e chamadas de código para as operações AWS 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. AWS 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 AWS 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.

AWS Direct Connect informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre em AWS 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 AWS 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 obter mais informações, 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 AWS Direct Connect as ações são registradas CloudTrail e documentadas na Referência da AWS 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 uma função 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 AWS 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 AWS 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 AWS Direct Connect 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 AWS 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 AWS 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 AWS 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 AWS 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

AWS Direct Connect métricas e dimensões

As métricas estão disponíveis para conexões AWS Direct Connect físicas e interfaces virtuais.

AWS Direct Connect Métricas de conexão

As métricas apresentadas a seguir estão disponíveis ao usar conexões dedicadas do Direct Connect.

Métrica	Descrição
`ConnectionState`	O estado da conexão. 1 indica ativa e 0 indica inativa. Esta métrica está disponível para conexões dedicadas e hospedadas.

Métrica	Descrição
	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	Descrição
`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	Descrição
`ConnectionErrorCount`	A contagem total de erros para todos os tipos de erros no nível de MAC no dispositivo da AWS . O total inclui erros de verificação de redundância cíclica (CRC). 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	Descrição
`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.

AWS Direct Connect métricas de interface virtual

As métricas a seguir estão disponíveis nas interfaces AWS Direct Connect virtuais.

Métrica	Descrição
`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).

Métrica	Descrição
	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

AWS Direct Connect dimensões disponíveis

Você pode filtrar os AWS Direct Connect dados usando as seguintes dimensões.

Dimensão	Descrição
`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

Exibir AWS Direct Connect CloudWatch métricas

AWS Direct Connect envia as seguintes métricas sobre suas conexões do Direct Connect. A Amazon CloudWatch então agrega esses pontos de dados em intervalos de 1 minuto ou 5 minutos. Por padrão, os dados métricos do Direct Connect são gravados CloudWatch em intervalos de 5 minutos.

> **Note**
>
> Ao monitorar o Direct Connect por meio do Direct Connect CloudWatch, você pode solicitar métricas em intervalos de 1 minuto. No entanto, a frequência real de atualização é controlada por CloudWatch. Como 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 visualizar métricas usando o CloudWatch console

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 Amazon CloudWatch para visualizar as métricas do Direct Connect, incluindo a adição de funções matemáticas ou consultas pré-criadas, consulte Como usar Amazon CloudWatch métricas no Guia CloudWatch do usuário da Amazon.

1. Abra o CloudWatch console 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 nome ConnectionIdou métrica e, em seguida, escolha qualquer uma das opções a seguir para definir melhor 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 CloudWatch métricas com o Metrics Insights no Guia CloudWatch do usuário da Amazon.

Para visualizar métricas usando o AWS Direct Connect console

1. Abra o AWS Direct Connectconsole 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 o AWS CLI

Em um prompt de comando, use o seguinte comando.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Crie CloudWatch alarmes da Amazon para monitorar conexões AWS Direct Connect

Você pode criar um CloudWatch alarme 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 AWS 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 saber para criar um alarme e obter mais informações sobre como criar um alarme, consulte Usando CloudWatch alarmes da Amazon no Guia do CloudWatch usuário da Amazon.

Para criar um CloudWatch alarme.

1. Abra o CloudWatch console 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 AWS Direct Connect conexão 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 métricas e condições específicas, consulte Usando CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.
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 CloudWatch usuário da Amazon.
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.

AWS Direct Connect cotas

A tabela a seguir lista as cotas relacionadas a. AWS Direct Connect

Componente	Quota	Comentários
Interfaces virtuais privadas ou públicas por conexão AWS Direct Connect dedicada	50	Este limite não pode ser aumentado.
Interfaces virtuais de trânsito por conexão AWS Direct Connect dedicada. As interfaces virtuais de trânsito podem ser usadas para se 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 AWS Direct Connect dedicada e interfaces virtuais de trânsito por conexão AWS Direct Connect dedicada	51	Quando o AWS Direct Connect suporte para Amazon VPC Transit Gateways foi lançado, uma cota de uma (1) interface virtual de trânsito foi 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 AWS Direct Connect hospedada	1	Este limite não pode ser aumentado.

Componente	Quota	Comentários
AWS Direct Connect Conexões ativas 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 o AWS Direct Connect suporte para Amazon VPC Transit Gateways foi lançado, uma cota de uma (1) interface virtual de trânsito foi 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 do Border Gateway Protocol (BGP) em uma interface virtual privada ou interface virtual de trânsito do local para o. AWS Se você anunciar mais de 100 rotas para IPv4 e IPv6 sobre a 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.
AWS Direct Connect gateways por conta	200	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Gateways privados virtuais por AWS Direct Connect gateway	20	Este limite não pode ser aumentado.
Gateways de trânsito por AWS Direct Connect gateway	6	Este limite não pode ser aumentado.

Componente	Quota	Comentários
Número máximo de prefixos de rota anunciados de um anexo do gateway Direct Connect da rede principal AWS Cloud WAN ao local. **Note** Todas as interfaces virtuais de trânsito conectadas a esse gateway 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 AWS Direct Connect gateway	30	Este limite não pode ser aumentado.
Número de prefixos por AWS Transit Gateway origem AWS até o local 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.
SiteLink limite de prefixo	100	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.

AWS Direct Connect suporta essas velocidades de porta em fibra monomodo: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm), 100 Gbps: 100GBASE- e 400 Gbps: 400GBASE-. LR4 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

Considerações sobre balanceamento de carga

Se você quiser usar o balanceamento de carga com vários públicos VIFs, todos VIFs devem estar na mesma região.

Solução de problemas AWS Direct Connect

As seguintes informações sobre resolução de problemas podem ajudar você a diagnosticar e corrigir problemas com sua conexão do AWS Direct Connect .

Sumário

Solucionar problemas da camada 1 (física)

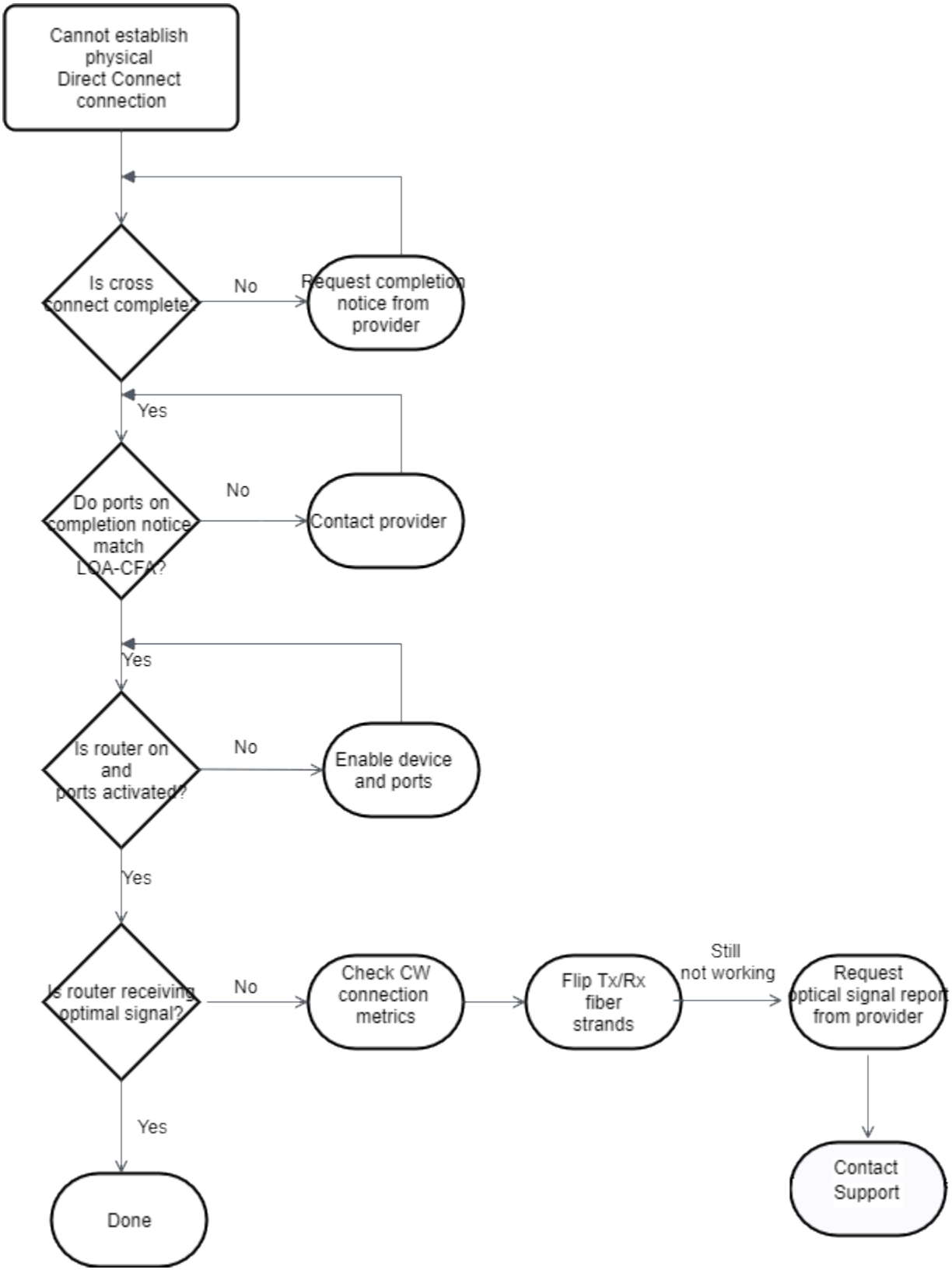
Se você ou seu provedor de rede estiverem tendo dificuldades em estabelecer conectividade física com um AWS Direct Connect dispositivo, use as etapas a seguir para solucionar o problema.

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 atende sua conexão, a negociação automática pode precisar ser ativada ou desativada 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 em que sua conexão termina, a negociação automática pode precisar ser ativada ou desativada 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 as CloudWatch métricas da Amazon para AWS Direct Connect. Você pode verificar as leituras ópticas Tx/Rx do AWS Direct Connect dispositivo (1 Gbps e 10 Gbps), a contagem de

erros físicos e o status operacional. Para obter mais informações, consulte Monitoramento com a 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.

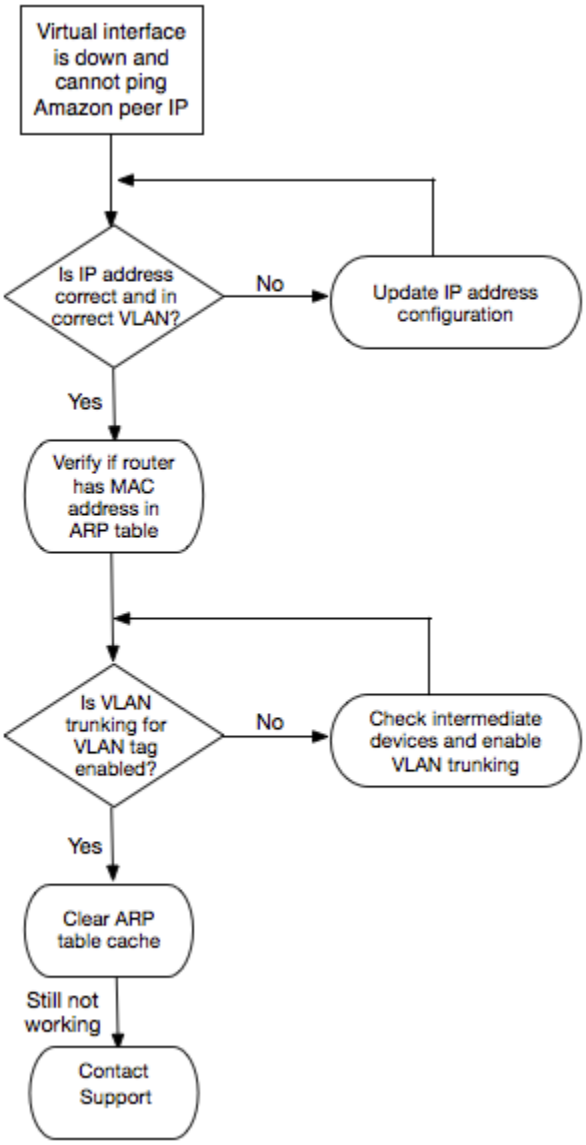

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check 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)

Se sua conexão AWS Direct Connect física estiver ativa, mas sua interface virtual estiver inativa, use as etapas a seguir para solucionar 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. Certifique-se de que o endereço IP esteja configurado na subinterface da VLAN e não na interface física (por exemplo, GigabitEthernet 0/0.123 em vez de 0/0). GigabitEthernet
2. Verifique se o roteador tem uma entrada de endereço MAC do AWS endpoint na tabela do protocolo de resolução de endereços (ARP).
3. Verifique se algum dispositivo intermediário entre endpoints tem entroncamento VLAN habilitado para a tag VLAN 802.1Q. O ARP não pode ser estabelecido na AWS lateral até AWS receber tráfego marcado.
4. Apague o cache da tabela ARP do provedor.
5. Se as etapas acima não estabelecerem o ARP ou você ainda não conseguir fazer ping no IP de mesmo nível da Amazon, entre em contato com o Support AWS.

O fluxograma a seguir contém as etapas para diagnosticar problemas com o link de dados.



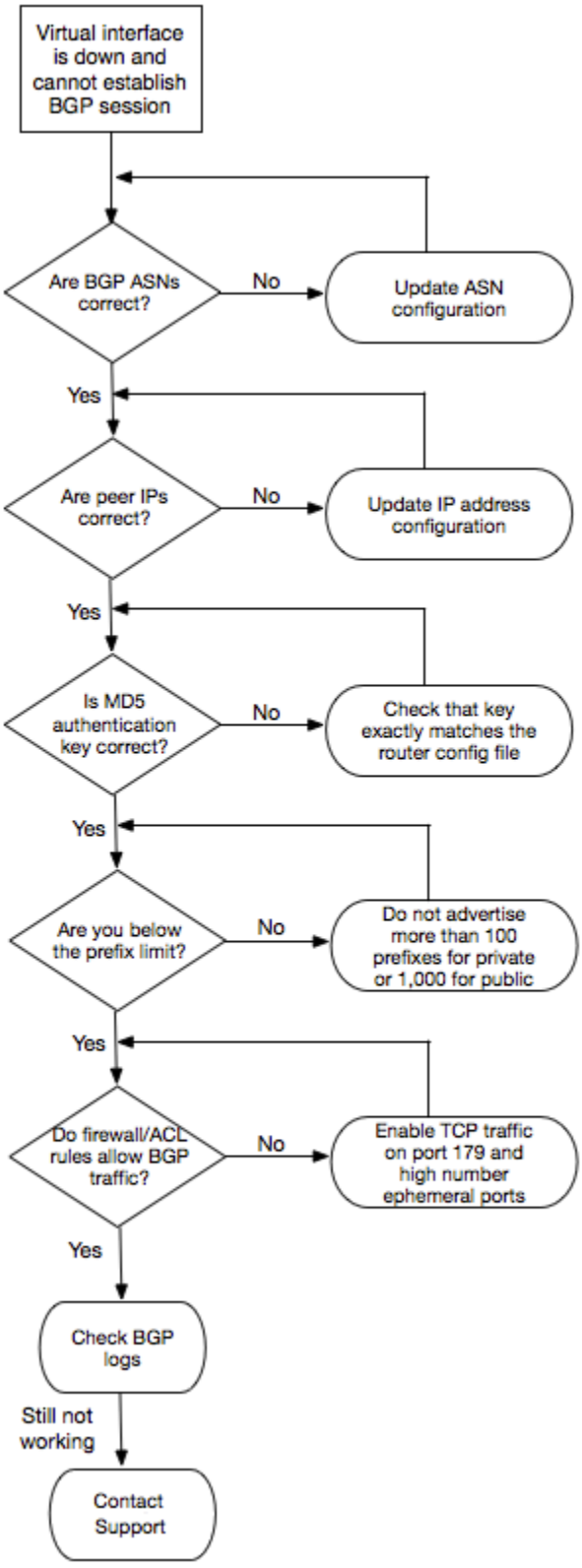
Caso a sessão BGP ainda não seja estabelecida após a verificação dessas etapas, consulte Solucionar problemas das camadas 3/4 (rede/transporte). Caso a sessão BGP seja estabelecida, mas você esteja enfrentando problemas de roteamento, consulte Solucionar problemas de roteamento.

Solucionar problemas das camadas 3/4 (rede/transporte)

Considere uma situação em que sua conexão AWS Direct Connect física esteja ativa e você possa fazer ping no endereço IP de mesmo nível 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. Certifique-se de que o peer de ambos IPs os lados da sessão de peering do BGP esteja configurado corretamente.
3. Certifique-se de que sua chave de MD5 autenticação esteja configurada e corresponda exatamente à chave no arquivo de configuração do roteador baixado. 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. Se as etapas acima não estabelecerem a sessão de emparelhamento do BGP, entre em contato com o Support. AWS

O fluxograma a seguir contém as etapas para diagnosticar problemas com a sessão de mesmo nível BGP.



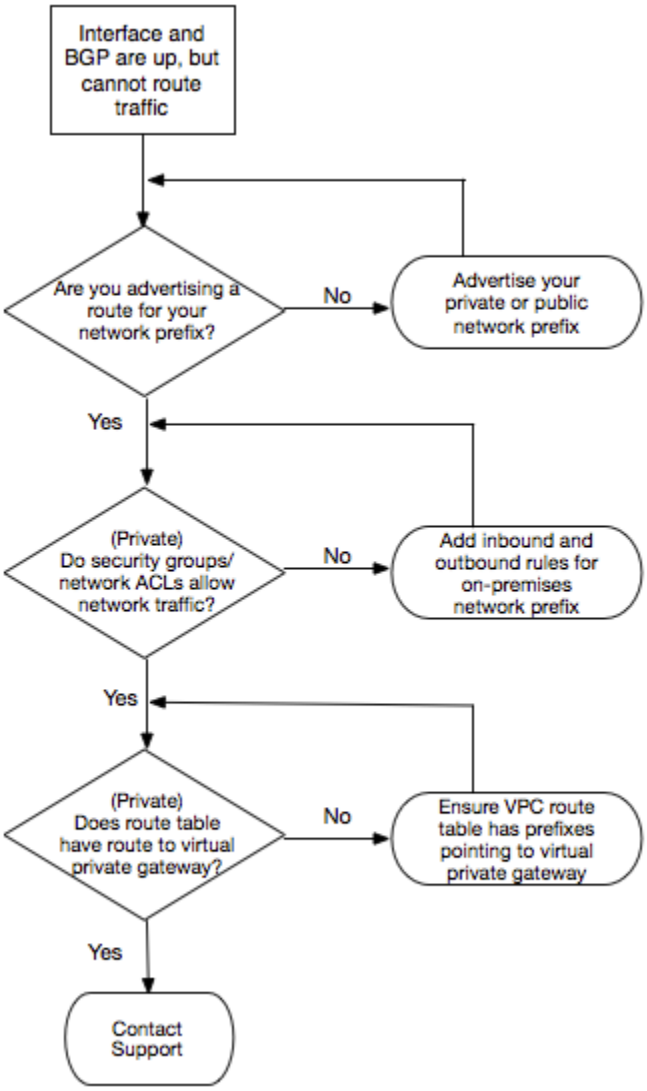
Caso a sessão de mesmo nível BGP seja estabelecida, mas você esteja enfrentando problemas de roteamento, consulte Solucionar problemas de roteamento.

Solucionar 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 uma interface virtual privada, certifique-se de que seus grupos de segurança e rede de VPC ACLs permitam tráfego de entrada e saída para seu prefixo de rede local. Para obter mais informações, consulte Security Groups and Network ACLs 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. Se as etapas acima não resolverem seus problemas 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 tabela a seguir descreve as versões do AWS Direct Connect. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Alteração	Descrição	Data
Crie uma associação entre o gateway Direct Connect e uma rede AWS Network Manager principal	Agora você pode criar uma associação de gateway do Direct Connect diretamente entre o Direct Connect e uma rede principal do AWS Cloud WAN.	25 de novembro de 2024
Support para 400G	Tópicos atualizados para incluir suporte para conexões 400G.	18 de julho de 2024
Adicionado um limite de SiteLink prefixo	Um limite de prefixo para SiteLink foi adicionado ao tópico cotas e limites.	15 de junho de 2023
Support for SiteLink	Você pode criar uma interface virtual privada que permita a conectividade entre dois pontos de presença do Direct Connect (PoPs) na mesma AWS região.	1º de dezembro de 2021
Support MAC Security	Você pode usar AWS Direct Connect conexões que oferecem suporte MACsec para criptografar seus dados do data center corporativo até o AWS Direct Connect local.	31 de março de 2021

Support para 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
Nova localização em Israel	Atualização do tópico para incluir a adição do novo local em Israel.	7 de julho de 2020
Suporte para testes de failover do Resiliency Toolkit	Use o recurso de teste de failover do Resiliency Toolkit para testar a resiliência de suas conexões.	3 de junho de 2020
CloudWatch Suporte métrico VIF	Você pode monitorar AWS Direct Connect conexões físicas e interfaces virtuais usando CloudWatch.	11 de maio de 2020
AWS Direct Connect Kit de ferramentas de resiliência	O AWS Direct Connect Resiliency Toolkit fornece um assistente de conexão com vários modelos de resiliência que ajudam você a solicitar conexões dedicadas para atingir seu objetivo de SLA.	7 de outubro de 2019
Suporte regional adicional para Support para AWS Transit Gateway várias contas	Suporte regional adicional para AWS Transit Gateway várias contas.	30 de setembro de 2019

AWS Direct Connect suporte para AWS Transit Gateway	Você pode usar um AWS Direct Connect gateway para conectar sua AWS Direct Connect conexão por meio de uma interface virtual de trânsito ao gateway de trânsito VPCs ou VPNs conectada a ele. Você associa um gateway do Direct Connect com o gateway de trânsito. Em seguida, crie uma interface virtual de trânsito para sua AWS Direct Connect conexão com o gateway Direct Connect.	27 de março de 2019
Suporte para quadros Jumbo	Você pode enviar quadros jumbo (9001 MTU). AWS 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
AWS Direct Connect porta de entrada	Você pode usar um gateway Direct Connect para conectar sua AWS Direct Connect conexão a VPCs regiões remotas.	1 de novembro de 2017
CloudWatch Métricas da Amazon	Você pode ver CloudWatch as métricas de suas AWS Direct Connect conexões.	29 de junho de 2017

Grupos de agregação de links	Você pode criar um grupo de agregação de links (LAG) para agregar várias conexões. AWS Direct Connect	13 de fevereiro de 2017
IPv6 apoio	Sua interface virtual agora pode suportar uma sessão de emparelhamento do IPv6 BGP.	1° de dezembro de 2016
Suporte a marcação	Agora você pode marcar seus AWS Direct Connect recursos.	4 de novembro de 2016
LOA-CFA de autoatendimento	Agora você pode baixar sua Carta de Autorização e Atribuição de Instalações de Conexão (LOA-CFA) usando o console ou a AWS Direct Connect API.	22 de junho de 2016
Nova localização 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
Nova localização 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

Nova localização 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	Tópicos atualizados para incluir a adição de novos locais em Dallas (região Leste dos EUA (Norte da Virgínia)), Londres (região da Europa (Irlanda)), Vale do Silício AWS GovCloud (região Oeste dos EUA) e Mumbai (região Ásia-Pacífico (Cingapura)).	27 de novembro de 2015
Nova localização na região da China (Pequim)	Atualização do tópico para incluir a adição do novo local em Pequim na região China (Pequim).	14 de abril de 2015
Nova localização em Las Vegas na região Oeste dos EUA (Oregon)	Tópicos atualizados para incluir a adição da nova localização de AWS Direct Connect Las Vegas na região Oeste dos EUA (Oregon).	10 de novembro de 2014
Nova região da UE (Frankfurt)	Tópicos atualizados para incluir a adição de novos AWS Direct Connect locais que atendem à região da UE (Frankfurt).	23 de outubro de 2014
Novos locais na região Ásia-Pacífico (Sydney)	Tópicos atualizados para incluir a adição de novos AWS Direct Connect locais que atendem à região Ásia-Pací fico (Sydney).	14 de julho de 2014

Support for AWS CloudTrail	Foi adicionado um novo tópico para explicar como você pode usar CloudTrail para registrar atividades AWS Direct Connect.	4 de abril de 2014
Support para acessar AWS regiões remotas	Adição de um novo tópico para explicar como você pode acessar recursos públicos em uma Região remota.	19 de dezembro de 2013
Support para conexões hospedadas	Tópicos atualizados para incluir suporte a conexões hospedadas.	22 de outubro de 2013
Nova localização na região da UE (Irlanda)	Tópicos atualizados para incluir a adição do novo AWS Direct Connect local que atende à região da UE (Irlanda).	24 de junho de 2013
Nova localização em Seattle na região Oeste dos EUA (Oregon)	Tópicos atualizados para incluir a adição do novo AWS Direct Connect local em Seattle, atendendo à região Oeste dos EUA (Oregon).	8 de maio de 2013
Support para usar o IAM com AWS Direct Connect	Foi adicionado um tópico sobre o uso AWS Identity and Access Management com AWS Direct Connect.	21 de dezembro de 2012
Nova região Ásia-Pacífico (Sydney)	Tópicos atualizados para incluir a adição do novo AWS Direct Connect local que atende à região Ásia-Pacífico (Sydney).	14 de dezembro de 2012

Novo AWS Direct Connect console e as regiões Leste dos EUA (Norte da Virgínia) e América do Sul (São Paulo)	Substituiu o AWS Direct Connect Guia de introdução pelo Guia AWS Direct Connect do usuário. Foram adicionad os novos tópicos para cobrir o novo AWS Direct Connect console, adicionaram um tópico de cobrança, adicionar am informações de configura ção do roteador e atualizaram tópicos para incluir a adição de dois novos AWS Direct Connect locais que atendem às regiões Leste dos EUA (Norte da Virgínia) e América do Sul (São Paulo).	13 de agosto de 2012
Support para as regiões da UE (Irlanda), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio)	Foi adicionada uma nova seção de solução de problemas e tópicos atualizad os para incluir a adição de quatro novos AWS Direct Connect locais que atendem às regiões Oeste dos EUA (Norte da Califórnia), UE (Irlanda), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Tóquio).	10 de janeiro de 2012
Support 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	O primeiro lançamento do AWS 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.