User Guide

AWS Direct Connect

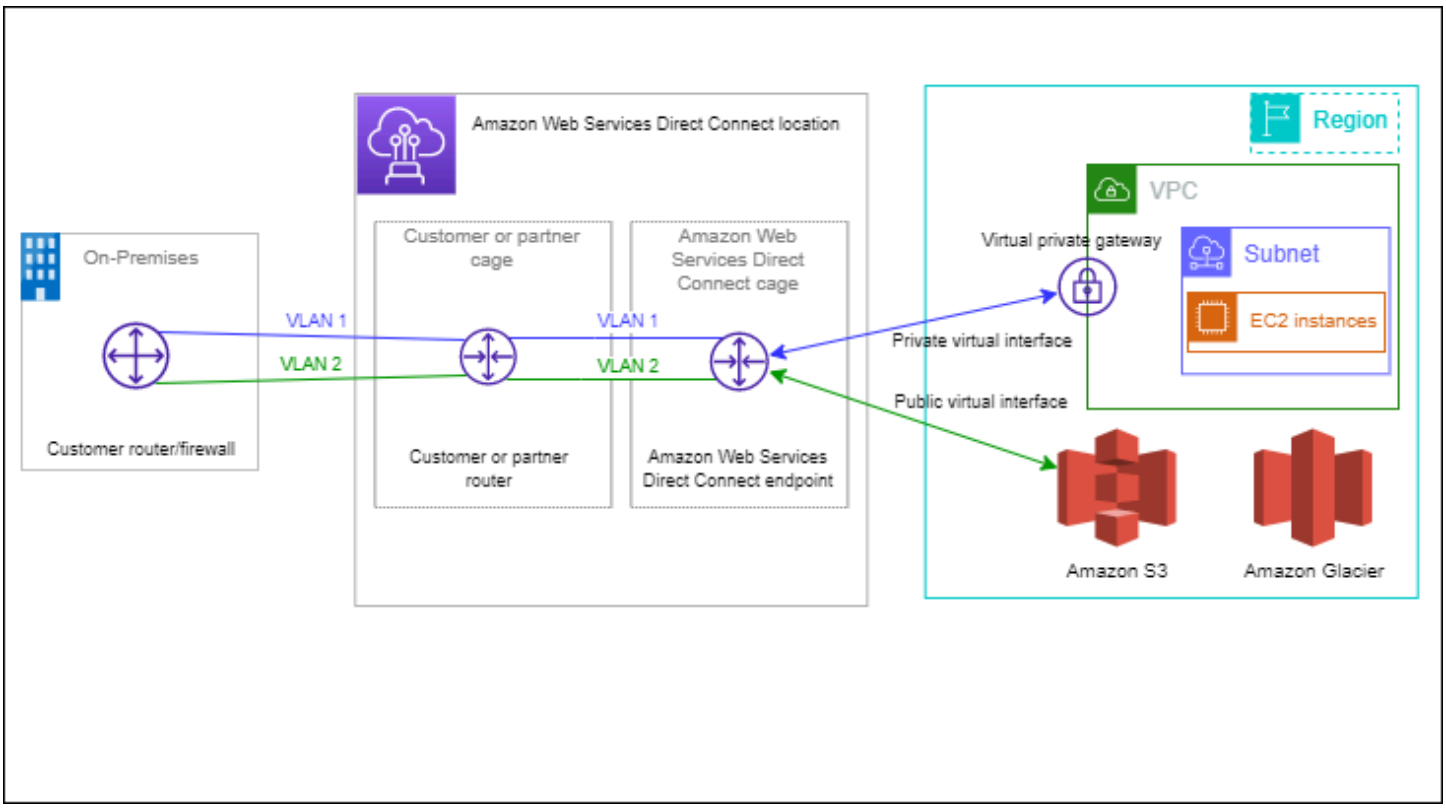
AWS Direct Connect: User Guide

Table of Contents

Was ist AWS Direct Connect?

AWS Direct Connect verbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem AWS Direct Connect Standort. Das eine Kabelende wird an Ihren Router angeschossen, das andere an einen AWS Direct Connect -Router. Mit dieser Verbindung können Sie virtuelle Schnittstellen direkt zu öffentlichen AWS Diensten (z. B. zu Amazon S3) oder zu Amazon VPC erstellen und dabei Internetdienstanbieter in Ihrem Netzwerkpfad umgehen. Ein AWS Direct Connect Standort bietet Zugriff auf die AWS Region, der er zugeordnet ist. Sie können eine einzige Verbindung in einer öffentlichen Region oder für AWS GovCloud (US) den Zugriff auf öffentliche AWS Dienste in allen anderen öffentlichen Regionen verwenden.

Das folgende Diagramm zeigt einen allgemeinen Überblick über die AWS Direct Connect Schnittstellen zu Ihrem Netzwerk.



Inhalt

- Remote-Zugriff auf eine AWS-Region
- Routing-Richtlinien und BGP-Communitys

AWS Direct Connect Komponenten

Im Folgenden sind die wichtigsten Komponenten aufgeführt, die Sie verwenden für AWS Direct Connect:

Verbindungen

Stellen Sie eine Verbindung an einem AWS Direct Connect Standort her, um eine Netzwerkverbindung von Ihren Räumlichkeiten zu einer AWS Region herzustellen. Weitere Informationen finden Sie unter AWS Direct Connect Verbindungen.

Virtuelle Schnittstellen

Erstellen Sie eine virtuelle Schnittstelle, um den Zugriff auf AWS Dienste zu ermöglichen. Eine öffentliche virtuelle Schnittstelle ermöglicht den Zugriff auf öffentliche Services wie z. B. Amazon S3. Eine private virtuelle Schnittstelle ermöglicht den Zugriff auf Ihre VPC. Weitere Informationen finden Sie unter AWS Direct Connect virtuelle Schnittstellen und Voraussetzungen für virtuelle Schnittstellen.

Netzwerkanforderungen

Um es AWS Direct Connect an einem AWS Direct Connect Standort verwenden zu können, muss Ihr Netzwerk eine der folgenden Bedingungen erfüllen:

- Ihr Netzwerk befindet sich an einem vorhandenen AWS Direct Connect Standort. Weitere Informationen zu verfügbaren AWS Direct Connect Standorten finden Sie unter AWS Direct Connect-Produktdetails.
- Sie arbeiten mit einem AWS Direct Connect Partner zusammen, der Mitglied des AWS Partnernetzwerks (APN) ist. Informationen hierzu finden Sie unter APN-Partner, die AWS Direct Connect unterstützen.
- Sie stellen über einen unabhängigen Serviceanbieter eine Verbindung mit AWS Direct Connect her.

Darüber hinaus muss Ihr Netzwerk folgende Bedingungen erfüllen:

- Ihr Netzwerk muss Singlemode-Glasfaser mit einem 1000BASE-LX-Transceiver (1310 nm) für 1-Gigabit-Ethernet, einem 10GBASE-LR-Transceiver (1310 nm) für 10 Gigabit oder einem 100GBASE-LR4 für 100-Gigabit-Ethernet verwenden.
- Die Auto-Negotiation für einen Port muss für eine Verbindung mit einer Portgeschwindigkeit von mehr als 1 Gbit/s deaktiviert sein. Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bedient, muss die automatische Absprache jedoch möglicherweise für 1-Gbit/s-Verbindungen aktiviert oder deaktiviert werden. Wenn Ihre virtuelle Schnittstelle weiterhin nicht verfügbar ist, finden Sie weitere Informationen unter Behandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss Border Gateway Protocol (BGP) und BGP-MD5-Authentifizierung unterstützen.
- (Optional) Sie können jedoch die Bidirectional Forwarding Detection (BFD) in Ihrem Netzwerk konfigurieren. Asynchrones BFD wird automatisch für jede virtuelle Schnittstelle aktiviert. AWS Direct Connect Die asynchrone BFD wird für virtuelle Direct-Connect-Schnittstellen automatisch aktiviert, aber die Aktivierung wird erst wirksam, wenn Sie sie auf Ihrem Router konfigurieren. Weitere Informationen finden Sie unter BFD für eine Direct-Connect-Verbindung aktivieren.

AWS Direct Connect unterstützt sowohl die IPv4- als auch die IPv6-Kommunikationsprotokolle. IPv6-Adressen, die von öffentlichen AWS Diensten bereitgestellt werden, sind über AWS Direct Connect öffentliche virtuelle Schnittstellen zugänglich.

AWS Direct Connect unterstützt eine Ethernet-Frame-Größe von 1 522 oder 9 023 Byte (14 Bytes Ethernet-Header + 4 Bytes VLAN-Tag + Bytes für das IP-Datagramm + 4 Bytes FCS) auf der Verbindungsschicht. Sie können die MTU für Ihre privaten virtuellen Schnittstellen festlegen. Weitere Informationen finden Sie unter Die Netzwerk-MTU für private virtuelle Schnittstellen oder virtuelle Transit-Schnittstellen festlegen.

Preisgestaltung für AWS Direct Connect

AWS Direct Connect umfasst zwei Abrechnungselemente: Portzeiten und ausgehende Datenübertragung. Die Preise für Port-Stunden hängen von der Kapazität und dem Verbindungstyp (dedizierte Verbindung oder gehostete Verbindung) ab.

Die Gebühren für ausgehende Datenübertragungen für private Schnittstellen und virtuelle Übertragungsschnittstellen werden dem AWS Konto zugewiesen, das für die Datenübertragung

verantwortlich ist. Für die Nutzung eines AWS Direct Connect -Gateways mit mehreren Konten fallen keine zusätzlichen Kosten an.

Wenn bei öffentlich adressierbaren AWS Ressourcen (z. B. Amazon S3 S3-Buckets, Classic EC2-Instances oder EC2-Verkehr, der über ein Internet-Gateway geleitet wird) der ausgehende Datenverkehr für öffentliche Präfixe bestimmt ist, die demselben AWS Zahlerkonto gehören und für die aktiv AWS über eine AWS Direct Connect öffentliche virtuelle Schnittstelle geworben wird, wird die ausgehende Datenübertragung (DTO) an den Eigentümer der Ressource mit der Datenübertragungsrate abgerechnet. AWS Direct Connect

Weitere Informationen finden Sie unter AWS Direct Connect – Preise.

AWS Direct Connect Wartung

AWS Direct Connect ist ein vollständig verwalteter Service, bei dem Direct Connect in regelmäßigen Abständen Wartungsarbeiten an einer Hardwareflotte durchführt, die den Service unterstützt. Direct Connect-Verbindungen werden auf eigenständigen Hardwaregeräten bereitgestellt, sodass Sie äußerst belastbare Netzwerkverbindungen zwischen Amazon Virtual Private Cloud und Ihrer lokalen Infrastruktur herstellen können. Diese Funktion ermöglicht Ihnen einen zuverlässigen, skalierbaren und kostengünstigen Zugriff auf Ihre AWS Ressourcen. Weitere Informationen finden Sie unter AWS Direct Connect -Resiliency-Empfehlungen.

Es gibt zwei Arten von Direct-Connect-Wartungen: geplante Wartung und Notfallwartung:

- Geplante Wartung. Geplante Wartungsarbeiten werden im Voraus geplant, um die Verfügbarkeit zu verbessern und neue Features bereitzustellen. Diese Art der Wartung wird während eines Wartungsfensters geplant, in dem wir drei Benachrichtigungen bereitstellen: 14 Kalendertage, 7 Kalendertage und 1 Kalendertag.

  > **Note**
  >
  > Zu den Kalendertagen gehören arbeitsfreie Tage und lokale Feiertage.

- Notfallwartung. Die Notfallwartung wird auf kritischer Basis eingeleitet, wenn es zu einem servicebeeinträchtigenden Ausfall kommt und AWS sofortige Maßnahmen zur Wiederherstellung der Services ergreifen muss. Diese Art der Wartung ist nicht im Voraus geplant. Betroffene Kunden werden bis zu 60 Minuten vor der Wartung über Notfallwartungsarbeiten informiert.

Wir empfehlen Ihnen, die AWS Direct Connect -Resiliency-Empfehlungen zu befolgen, damit Sie den Datenverkehr während der Wartung problemlos und proaktiv auf Ihre redundante Direct-Connect-Verbindung verlagern können. Wir empfehlen Ihnen außerdem, die Resilienz Ihrer redundanten Verbindungen regelmäßig proaktiv zu testen, um sicherzustellen, dass der Failover wie gewünscht funktioniert. Mithilfe dieser the section called “AWS Direct Connect-Failover-Test” Funktion können Sie überprüfen, ob Ihr Datenverkehr über eine Ihrer redundanten virtuellen Schnittstellen geleitet wird.

Hinweise zu den Zulassungskriterien für die Einreichung eines Antrags auf Stornierung einer geplanten Wartung finden Sie unter Wie storniere ich ein Direct-Connect-Wartungsereignis?.

> **Note**
>
> Wartungsanfragen im Notfall können nicht storniert werden, da sofort reagiert werden AWS muss, um den Service wiederherzustellen.

Weitere Informationen zu Wartungsereignissen finden Sie unter Wartungsereignisse in den AWS Direct Connect häufig gestellten Fragen.

Remote-Zugriff auf eine AWS-Region

AWS Direct Connect-Standorte in öffentlichen Regionen oder AWS GovCloud (US) können in einer beliebigen anderen Region (mit Ausnahme von China (Peking und Ningxia)) auf öffentliche Services zugreifen. Darüber hinaus können AWS Direct Connect-Verbindungen in öffentlichen Regionen oder AWS GovCloud (US) so konfiguriert werden, dass sie auf eine VPC in Ihrem Konto in jeder beliebigen anderen öffentlichen Region (abgesehen von China (Peking und Ningxia)) zugreifen. Sie können daher mit einer einzelnen AWS Direct Connect-Verbindung Services für mehrere Regionen aufbauen. Der gesamte Datenverkehrs eines Netzwerks verbleibt auf dem globalen AWS-Netzwerk-Backbone, unabhängig davon, ob Sie auf öffentliche AWS-Services oder auf eine VPC in einer anderen Region zugreifen.

Alle Datenübertragungen aus einer Remote-Region werden mit dem Datentransfertarif für die Remote-Region abgerechnet. Weitere Informationen zu den Kosten von Datenübertragungen finden Sie im Abschnitt Preise auf der Detailseite zu AWS Direct Connect.

Weitere Informationen zu den Routing-Richtlinien und zu unterstützten BGP-Communities für eine AWS Direct Connect-Verbindung finden Sie unter Routing-Richtlinien und BGP-Communitys.

Zugriff auf öffentliche Services in einer Remote-Region

Für den Zugriff auf öffentliche Ressourcen in einer Remote-Region müssen Sie eine öffentliche virtuelle Schnittstelle und eine BGP-Sitzung (Border Gateway Protocol) einrichten. Weitere Informationen finden Sie unter AWS Direct Connect virtuelle Schnittstellen.

Nachdem Sie eine öffentliche virtuelle Schnittstelle erstellt und eine BGP-Sitzung eingerichtet haben, lernt Ihr Router die Routen der anderen öffentlichen AWS-Regionen kennen. Weitere Informationen über die derzeit von AWS angekündigten Präfixe finden Sie unter AWS-IP-Adressbereiche im Allgemeine Amazon Web Services-Referenz.

Zugriff auf VPCs in einer Remote-Region

Sie können ein Direct Connect-Gateway in einer beliebigen öffentlichen Region erstellen. Mit ihm können Sie Ihre AWS Direct Connect-Verbindung über eine private virtuelle Schnittstelle mit VPCs in Ihrem Konto herstellen, die sich in derselben oder einer anderen Region befinden, oder mit einem Transit-Gateway. Weitere Informationen finden Sie unter Arbeiten mit Direct Connect-Gateways.

Alternativ können Sie eine öffentliche virtuelle Schnittstelle für Ihre AWS Direct Connect-Verbindung erstellen und anschließend eine VPN-Verbindung mit Ihrer VPC in der Remote-Region herstellen. Weitere Informationen zur Konfiguration der VPN-Konnektivität für eine VPC finden Sie unter Verwendungsszenarien für Amazon Virtual Private Cloud im Amazon-VPC-Benutzerhandbuch.

Netzwerk-zu-Amazon VPC-Anbindungsoptionen

Die folgende Konfiguration kann verwendet werden, um Remote-Netzwerke mit Ihrer Amazon-VPC-Umgebung zu verbinden. Diese Optionen sind nützlich, um AWS-Ressourcen in Ihre bestehenden Services vor Ort zu integrieren:

- Amazon Virtual Private Cloud Connectivity Options

Routing-Richtlinien und BGP-Communitys

AWS Direct Connect wendet Routing-Richtlinien für eingehende (aus Ihrem lokalen Rechenzentrum) und ausgehende (aus Ihrer AWS Region) Routing-Richtlinien für eine öffentliche Verbindung an. AWS Direct Connect Sie können auch BGP (Border Gateway Protocol)-Community-Tags auf von Amazon angekündigten Routen verwenden und BGP-Community-Tags auf die Routen anwenden, die Sie in Amazon ankündigen.

Routing-Richtlinien für öffentliche virtuelle Schnittstellen

Wenn Sie auf öffentliche AWS Dienste zugreifen, müssen Sie AWS Direct Connect die öffentlichen IPv4-Präfixe oder IPv6-Präfixe angeben, um über BGP zu werben.

Es gelten die folgenden eingehenden Routing-Richtlinien:

- Sie müssen Eigentümer der öffentlichen Präfixe sein und diese Präfixe müssen entsprechend im jeweiligen regionalen Internet Registry registriert sein.
- Der Datenverkehr muss an öffentliche Amazon-Präfixe gerichtet sein. Transitives Routing zwischen Verbindungen wird nicht unterstützt.
- AWS Direct Connect führt eine Filterung eingehender Pakete durch, um zu überprüfen, ob die Quelle des Datenverkehrs von Ihrem angekündigten Präfix stammt.

Die folgenden Richtlinien gelten für ausgehendes Routing:

- AS_PATH und Longest Prefix Match werden verwendet, um den Routingpfad zu bestimmen. AWS empfiehlt, spezifischere Routen AWS Direct Connect anzukündigen, wenn dasselbe Präfix sowohl im Internet als auch in einer öffentlichen virtuellen Schnittstelle angekündigt wird.
- AWS Direct Connect kündigt alle Präfixe für lokale und entfernte AWS Regionen an, sofern verfügbar, und schließt Netzpräfixe von anderen Points of Presence (PoP) AWS außerhalb der Region ein, sofern verfügbar, z. B. und Route 53. CloudFront

> **Note**
>
> - Präfixe, die in der JSON-Datei für AWS IP-Adressbereiche, ip-ranges.json, für die chinesischen Regionen aufgeführt sind, werden nur in den AWS chinesischen Regionen beworben. AWS
> - Präfixe, die in der JSON-Datei für AWS IP-Adressbereiche, ip-ranges.json, für die Handelsregionen aufgeführt sind, werden nur in den Handelsregionen beworben. AWS AWS
>
> Weitere Informationen zur Datei ip-ranges.json finden Sie unter AWS -IP-Adressbereiche in der Allgemeine AWS-Referenz.

- AWS Direct Connect bewirbt Präfixe mit einer Mindestpfadlänge von 3.
- AWS Direct Connect bewirbt alle öffentlichen Präfixe mit der bekannten BGP-Community. `NO_EXPORT`

- Wenn Sie dieselben Präfixe aus zwei verschiedenen Regionen über zwei verschiedene öffentliche virtuelle Schnittstellen bewerben und beide dieselben BGP-Attribute und die längste Präfixlänge haben, AWS wird die Heimatregion für ausgehenden Verkehr priorisiert.
- Wenn Sie mehrere AWS Direct Connect Verbindungen haben, können Sie die Lastverteilung des eingehenden Datenverkehrs anpassen, indem Sie Präfixe mit denselben Pfadattributen ankündigen.
- Die von beworbenen Präfixe AWS Direct Connect dürfen nicht außerhalb der Netzwerkgrenzen Ihrer Verbindung beworben werden. Diese Präfixe dürfen beispielsweise nicht in einer öffentlichen Internet-Routing-Tabelle enthalten sein.
- AWS Direct Connect speichert Präfixe, die von Kunden im Amazon-Netzwerk beworben werden. Wir kündigen Kundenpräfixe, die wir aus einer öffentlichen VIF erhalten haben, nicht erneut einer der folgenden Gruppe an:
  - Andere Kunden AWS Direct Connect
  - Netzwerke, die mit dem AWS globalen Netzwerk mithalten
  - den Transitanbietern von Amazon

Public Virtual Interface BGP-Communitys

AWS Direct Connect unterstützt BGP-Community-Tags für den Geltungsbereich, um den Umfang (regional oder global) und die bevorzugte Route des Datenverkehrs auf öffentlichen virtuellen Schnittstellen zu kontrollieren. AWS behandelt alle von einer öffentlichen VIF empfangenen Routen so, als ob sie mit dem BGP-Community-Tag NO_EXPORT gekennzeichnet wären, was bedeutet, dass nur das AWS Netzwerk diese Routing-Informationen verwendet.

BGP-Communitys für den Umfang

Sie können BGP-Community-Tags auf die öffentlichen Präfixe anwenden, die Sie in Amazon ankündigen, um anzugeben, wie weit Ihre Präfixe im Amazon-Netzwerk verbreitet werden sollen: nur innerhalb der lokalen AWS -Region, in allen Regionen eines Kontinents oder in allen öffentlichen Regionen.

AWS-Region Gemeinschaften

Sie können die folgenden BGP-Communitys für Ihre Präfixe verwenden:

- `7224:9100`—Lokal AWS-Regionen
- `7224:9200`—Alles AWS-Regionen für einen Kontinent:

  - In ganz Nordamerika
  - Asien-Pazifik
  - Europa, Naher Osten und Afrika
- `7224:9300`—Global (alle öffentlichen Regionen) AWS

> **Note**
>
> Wenn Sie keine Community-Tags verwenden, werden Präfixe standardmäßig für alle öffentlichen AWS Regionen (global) angekündigt.
> Präfixe, die mit denselben Communitys gekennzeichnet sind und identische AS_PATH-Attribute aufweisen, sind Kandidaten für Multi-Pathing.

Die Communitys `7224:1` bis `7224:65535` sind AWS Direct Connect vorbehalten.

AWS Direct Connect Wendet bei Richtlinien für ausgehendes Routing die folgenden BGP-Communities auf die beworbenen Routen an:

- `7224:8100`— Routen, die aus derselben AWS Region stammen, der der AWS Direct Connect Point of Presence zugeordnet ist.
- `7224:8200`— Routen, die von demselben Kontinent stammen, dem der AWS Direct Connect Point of Presence zugeordnet ist.
- Kein Tag – Routen, die von anderen Kontinenten stammen.

> **Note**
>
> Um alle AWS öffentlichen Präfixe zu erhalten, wenden Sie keinen Filter an.

Communities, die für eine AWS Direct Connect öffentliche Verbindung nicht unterstützt werden, werden entfernt.

`NO_EXPORT`-BGP-Community

Für Richtlinien für ausgehendes Routing wird das BGP-Community-Tag `NO_EXPORT` für öffentliche virtuelle Schnittstellen unterstützt.

AWS Direct Connect bietet auch BGP-Community-Tags auf beworbenen Amazon-Routen. Wenn Sie AWS Direct Connect auf öffentliche AWS Dienste zugreifen, können Sie Filter erstellen, die auf diesen Community-Tags basieren.

Bei öffentlichen virtuellen Schnittstellen sind alle Routen, auf denen Kunden AWS Direct Connect beworben werden, mit dem Community-Tag NO_EXPORT gekennzeichnet.

Routing-Richtlinien für Private Virtual Interface und Transit Virtual Interface

Wenn Sie für AWS Direct Connect den Zugriff auf Ihre privaten AWS Ressourcen verwenden, müssen Sie die IPv4- oder IPv6-Präfixe angeben, um über BGP zu werben. Diese Präfixe können öffentlich oder privat sein.

Basierend auf den angekündigten Präfixen gelten die folgenden Regeln für das Routing ausgehender Nachrichten:

- AWS berechnet zuerst die längste Präfixlänge. AWS empfiehlt, spezifischere Routen mithilfe mehrerer virtueller Direct Connect-Schnittstellen anzukündigen, wenn die gewünschten Routingpfade für aktive/passive Verbindungen vorgesehen sind. Weitere Informationen finden Sie unter Beeinflussung des Datenverkehrs in Hybridnetzwerken mithilfe von Longest Prefix Match.
- Lokale Präferenz ist das BGP-Attribut, das empfohlen wird, wenn die gewünschten Routingpfade für aktive/passive Verbindungen vorgesehen sind und die angegebenen Präfixlängen identisch sind. Dieser Wert wird pro Region so festgelegt, dass AWS Direct Connect Standorte bevorzugt werden, denen dieselben zugeordnet sind, wobei der Community-Wert `7224:7200` —Medium für die AWS-Region lokale Präferenz verwendet wird. Wenn die lokale Region nicht mit dem Direct Connect-Standort verknüpft ist, wird sie auf einen niedrigeren Wert gesetzt. Dies gilt nur, wenn keine Community-Tags mit lokaler Präferenz zugewiesen wurden.
- Die AS_PATH-Länge kann verwendet werden, um den Routingpfad zu bestimmen, wenn die Präfixlänge und die lokale Präferenz identisch sind.
- Der Multi-Exit Discriminator (MED) kann verwendet werden, um den Routingpfad zu bestimmen, wenn Präfixlänge, lokale Präferenz und AS_PATH identisch sind. AWS empfiehlt nicht, MED-Werte zu verwenden, da sie bei der Auswertung eine geringere Priorität haben.
- AWS verteilt die Last auf mehrere Transitschnittstellen oder private virtuelle Schnittstellen, wenn Präfixe dieselbe Länge und dieselben BGP-Attribute haben.

Private Virtual Interface und Transit Virtual Interface BGP-Communitys

Wenn ein Traffic über private Direct Connect-Schnittstellen oder virtuelle Transitschnittstellen an lokale Standorte AWS-Region weiterleitet, beeinflusst AWS-Region der zugeordnete Direct Connect-Standort die Fähigkeit, Equal-Cost Multi-Path Routing (ECMP) zu verwenden. AWS-Regionen bevorzugen standardmäßig Direct Connect-Standorte in AWS-Region derselben Verknüpfung. Unter AWS Direct Connect Standorte finden Sie die zugehörigen AWS-Region Direct Connect-Standorte.

Wenn keine Community-Tags mit lokaler Präferenz angewendet werden, unterstützt Direct Connect ECMP über private oder virtuelle Transitschnittstellen für Präfixe mit derselben Länge, AS_PATH-Länge und demselben MED-Wert über zwei oder mehr Pfade in den folgenden Szenarien:

- Der AWS-Region sendende Datenverkehr besteht aus zwei oder mehr virtuellen Schnittstellenpfaden von Standorten derselben Zuordnung AWS-Region, unabhängig davon, ob es sich um dieselben oder unterschiedliche Colocation-Einrichtungen handelt.
- Der AWS-Region sendende Verkehr hat zwei oder mehr virtuelle Schnittstellenpfade von Standorten, die sich nicht in derselben Region befinden.

Weitere Informationen finden Sie unter Wie richte ich eine Active/Active- oder Active/Passive Direct Connect-Verbindung AWS von einer privaten oder transitbasierten virtuellen Schnittstelle aus ein?

> **Note**
>
> Dies hat keine Auswirkungen auf ECMP zu und von lokalen Standorten. AWS-Region

Um die Routeneinstellungen zu steuern, unterstützt Direct Connect BGP-Community-Tags mit lokaler Präferenz für private virtuelle Schnittstellen und virtuelle Transitschnittstellen.

BGP-Communitys mit lokalen Präferenzen

Mit BGP-Community-Tags für lokale Präferenzen erreichen Sie Lastausgleich und Routing-Präferenzen für eingehenden Datenverkehr mit Ihrem Netzwerk. Bei jedem Präfix, das Sie über eine BGP-Sitzung ankündigen, können Sie einen Community-Tag anwenden, um die Priorität des zugehörigen Pfads für den rückkehrenden Datenverkehr anzugeben.

Die folgenden BGP-Community-Tags für lokale Präferenzen werden unterstützt:

- `7224:7100`: Niedrige Präferenz

- `7224:7200`: Mäßige Präferenz
- `7224:7300`: Hohe Präferenz

BGP-Community-Tags für lokale Präferenzen schließen sich gegenseitig aus. Um den Datenverkehr auf mehrere AWS Direct Connect Verbindungen (aktiv/aktiv) zu verteilen, die in derselben oder in verschiedenen AWS Regionen stationiert sind, wenden Sie dasselbe Community-Tag an, z. B. `7224:7200` (mittlere Präferenz) auf die Präfixe für die Verbindungen. Wenn eine der Verbindungen ausfällt, erfolgt der Lastenausgleich des Datenverkehrs mithilfe von ECMP für die verbleibenden aktiven Verbindungen, unabhängig von den Zuordnungen der jeweiligen Heimatregion. Um Failover bei mehreren AWS Direct Connect -Verbindungen (aktiv/passiv) zu erreichen, wenden Sie einen Community-Tag mit höher Präferenz bei Präfixen für die primäre oder aktive virtuelle Schnittstelle und eine niedrigere Präferenz bei Präfixen für die Backup- oder passive virtuelle Schnittstelle an. Legen Sie beispielsweise die BGP-Community-Tags für Ihre primären oder aktiven virtuellen Schnittstellen auf `7224:7300` (hohe Präferenz) und für Ihre passiven virtuellen Schnittstellen auf `7224:7100` (niedrige Präferenz) fest.

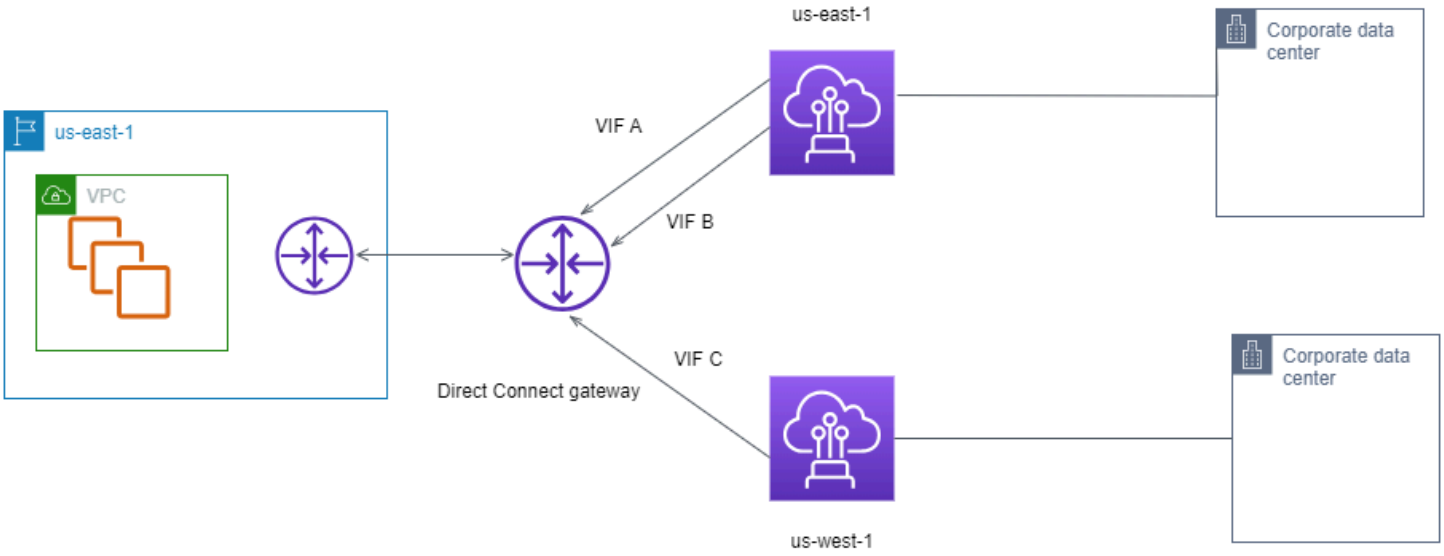
BGP-Community-Tags für lokale Präferenzen werden vor jedem AS_PATH-Attribut ausgewertet, und zwar in der Reihenfolge von der niedrigsten bis zur höchsten Präferenz (wobei die höchste Präferenz bevorzugt wird).

Beispiel für privates virtuelles Schnittstellen-Routing

Stellen Sie sich die Konfiguration vor, bei der die Heimatregion AWS Direct Connect Standort 1 mit der VPC-Heimatregion identisch ist. Es gibt einen redundanten AWS Direct Connect Standort in einer anderen Region Es gibt zwei private VIFs (VIF A und VIF B) von AWS Direct Connect Standort 1 (us-east-1) zum Direct Connect-Gateway. Es gibt eine private VIF (VIF C) vom AWS Direct Connect Standort (us-west-1) zum Direct Connect-Gateway. Um den Verkehr über VIF B vor VIF A zu AWS leiten, legen Sie das AS_PATH-Attribut von VIF B so fest, dass es kürzer ist als das AS_PATH-Attribut VIF A.

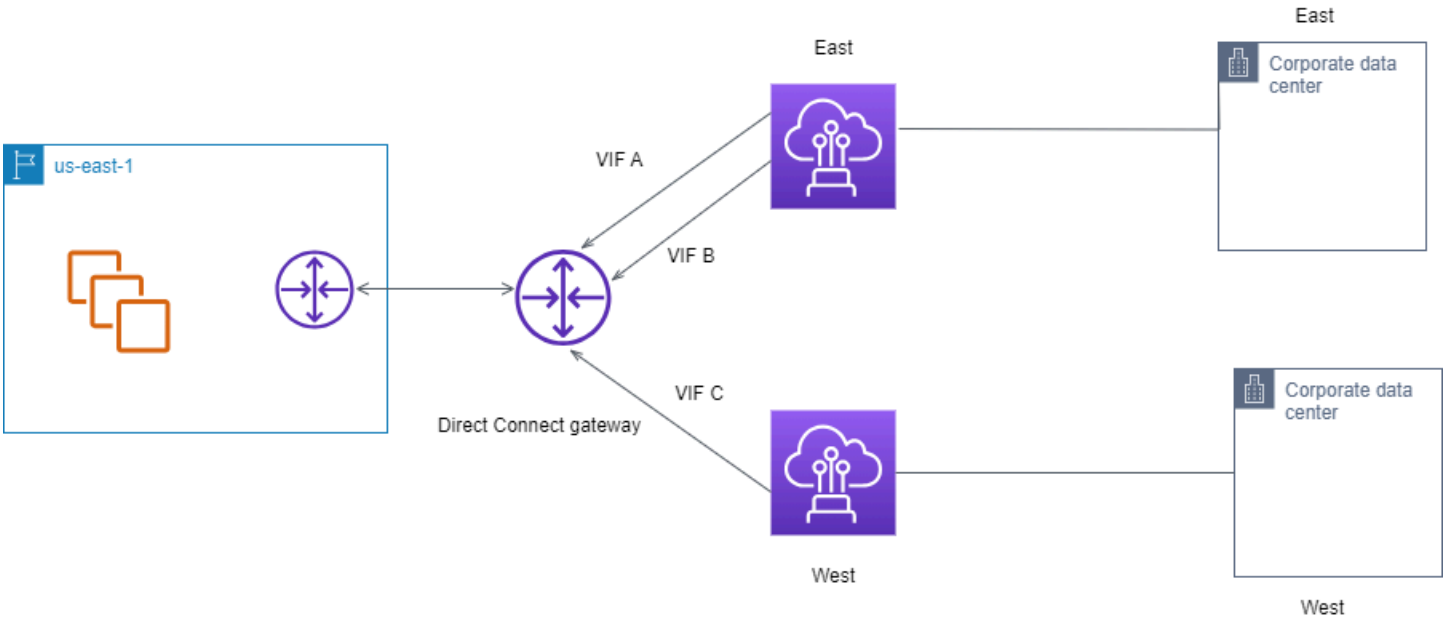
Die VIFs haben folgende Konfigurationen:

- VIF A (in us-east-1) kündigt 172.16.0.0/16 an und hat das AS_PATH-Attribut 65001, 65001, 65001
- VIF B (in us-east-1) kündigt 172.16.0.0/16 an und hat das AS_PATH-Attribut 65001, 65001
- VIF C (in us-west-1) kündigt 172.16.0.0/16 an und hat das AS_PATH-Attribut 65001



Wenn Sie die CIDR-Bereichskonfiguration von VIF C ändern, verwenden Routen, die in den CIDR-Bereich VIF C fallen, VIF C, da es die längste Präfixlänge hat.

- VIF C (in us-west-1) kündigt 172.16.0.0/24 an und hat das AS_PATH-Attribut 65001



Erste Schritte mit dem AWS Direct Connect Resiliency Toolkit

AWS bietet Kunden die Möglichkeit, hochbelastbare Netzwerkverbindungen zwischen Amazon Virtual Private Cloud (Amazon VPC) und ihrer lokalen Infrastruktur herzustellen. Das AWS Direct Connect Resiliency Toolkit bietet einen Verbindungsassistenten mit mehreren Resilienzmodellen. Diese Modelle unterstützen Sie dabei, die Anzahl der dedizierten Verbindungen festzustellen und dann eine Bestellung aufzugeben, um Ihr SLA-Ziel zu erreichen. Sie wählen ein Resilienzmodell aus, und dann führt Sie das AWS Direct Connect Resiliency Toolkit durch den speziellen Prozess zur Bestellung von Verbindungen. Die Resilienzmodelle wurden entwickelt, um sicherzustellen, dass Sie über die entsprechende Anzahl dedizierter Verbindungen an mehreren Standorten verfügen.

Das AWS Direct Connect Resiliency Toolkit bietet die folgenden Vorteile:

- Hinweise zur Bestimmung und dann Bestellung der geeigneten redundanten, dedizierten AWS Direct Connect -Verbindungen.
- Sicherstellung, dass die redundanten, dedizierten Verbindungen die gleichen Geschwindigkeiten aufweisen.
- Automatische Konfiguration der dedizierten Verbindungsnamen.
- Genehmigt automatisch Ihre dedizierten Verbindungen, wenn Sie ein bestehendes AWS Konto haben und einen bekannten Partner auswählen. AWS Direct Connect Der „Letter of Authority“ (LOA) steht sofort zum Download zur Verfügung.
- Erstellt automatisch ein Supportticket für die Genehmigung der dedizierten Verbindung, wenn Sie ein neuer AWS Kunde sind oder einen unbekannten (anderen) Partner auswählen.
- Eine Bestellübersicht für Ihre dedizierten Verbindungen mit der SLA, die Sie erreichen können, und die Port-Stunden-Kosten für die bestellten dedizierten Verbindungen.
- Erstellung von Link Aggregation Groups (LAGs) und Hinzufügung der entsprechenden Anzahl dedizierter Verbindungen zu den LAGs, wenn Sie eine andere Geschwindigkeit als 1 Gbit/s, 10 Gbit/s oder 100 Gbit/s wählen.
- Bereitstellung einer LAG-Zusammenfassung mit der dedizierten Verbindungs-SLA, die Sie erreichen können, sowie den Gesamtkosten für Port-Stunden für jede bestellte dedizierte Verbindung als Teil der LAG.
- Verhinderung, dass Sie die dedizierten Verbindungen auf demselben AWS Direct Connect -Gerät beenden.

- Bietet eine Möglichkeit, Ihre Konfiguration auf Ausfallsicherheit zu testen. Sie arbeiten mit AWS , die BGP-Peering-Sitzung herunterzufahren, um zu überprüfen, ob der Datenverkehr an eine Ihrer redundanten virtuellen Schnittstellen weitergeleitet wird. Weitere Informationen finden Sie unter the section called “AWS Direct Connect-Failover-Test”.
- Stellt CloudWatch Amazon-Metriken für Verbindungen und virtuelle Schnittstellen bereit. Weitere Informationen finden Sie unter Überwachen.

Die folgenden Resilienzmodelle sind im AWS Direct Connect Resiliency Toolkit verfügbar:

- Maximum Resiliency (Maximale Ausfallsicherheit): Dieses Modell bietet Ihnen die Möglichkeit, dedizierte Verbindungen zu bestellen, um eine SLA von 99,99 % zu erreichen. Sie müssen alle Anforderungen zum Erreichen der SLA erfüllen, die im AWS Direct Connect Service Level Agreement angegeben sind.
- High Resiliency (Hohe Ausfallsicherheit): Dieses Modell bietet Ihnen die Möglichkeit, dedizierte Verbindungen zu bestellen, um eine SLA von 99,9 % zu erreichen. Sie müssen alle Anforderungen zum Erreichen der SLA erfüllen, die im AWS Direct Connect Service Level Agreement angegeben sind.
- Entwicklung und Test: Mit diesem Modell erzielen Sie Entwicklungs- und Testausfallsicherheit für nicht kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an einem Standort beendet werden.
- Classic. Dieses klassische Modell ist für Benutzer gedacht, die bestehende Verbindungen haben und zusätzliche Verbindungen hinzufügen wollen. Dieses Modell bietet keine SLA.

Es empfiehlt sich, den Verbindungsassistenten im AWS Direct Connect Resiliency Toolkit zu verwenden, um die dedizierten Verbindungen so zu ordnen, dass Sie Ihr SLA-Ziel erreichen.

Nachdem Sie das Resilienzmodell ausgewählt haben, führt Sie das AWS Direct Connect Resiliency Toolkit durch die folgenden Verfahren:

- Auswählen der Anzahl der dedizierten Verbindungen
- Auswählen der Verbindungskapazität und des dedizierten Verbindungsstandorts
- Bestellen der dedizierten Verbindungen
- Überprüfen, ob die dedizierten Verbindungen einsatzbereit sind
- Herunterladen Ihres „Letter of Authority“ (LOA-CFA) für jede dedizierte Verbindung
- Überprüfen, ob Ihre Konfiguration Ihren Anforderungen an die Ausfallsicherheit entspricht

Voraussetzungen

AWS Direct Connect unterstützt die folgenden Portgeschwindigkeiten über Singlemode-Glasfaser: 1000BASE-LX-Transceiver (1310 nm) für 1-Gigabit-Ethernet, 10GBASE-LR-Transceiver (1310 nm) für 10 Gigabit oder 100GBASE-LR4 für 100-Gigabit-Ethernet.

Sie können eine Verbindung auf eine der folgenden Arten einrichten: AWS Direct Connect

Modell	Bandbreite	Methode
Dedizierte Verbindung	1 Gbit/s, 10 Gbit/s und 100 Gbit/s	Arbeiten Sie mit einem AWS Direct Connect Partner oder einem Netzwerkanbieter zusammen, um einen Router von Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung mit einem AWS Direct Connect Standort zu verbinden. Beim Netzanbie ter muss es sich nicht um einen AWS Direct Connect - Partner handeln, um für Sie eine dedizierte Verbindung herzustellen. Dedizierte AWS Direct Connect -Verbindungen unterstützen die folgenden Port-Geschwindigkeiten über Monomode-Glasfaser: 1 Gbit/ s: 1000BASE-LX (1310 nm), 10 Gbit/s: 10GBASE-LR (1310 nm) und 100 Gbit/s: 100GBASE-LR4.
Gehostete Verbindung	50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 300 Mbit/s, 400 Mbit/s, 500 Mbit/s, 1 Gbit/s, 2 Gbit/s, 5 Gbit/s und 10 Gbit/s	Arbeiten Sie mit einem Partner im AWS Direct Connect Partnerprogramm zusammen, um einen Router

Modell	Bandbreite	Methode
		von Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung mit einem AWS Direct Connect Standort zu verbinden. Nur bestimmte Partner bieten Verbindungen mit einer höheren Kapazität an.

Stellen Sie bei Verbindungen AWS Direct Connect mit Bandbreiten von 1 Gbit/s oder höher sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt:

- Ihr Netzwerk muss Singlemode-Glasfaser mit einem 1000BASE-LX-Transceiver (1310 nm) für 1-Gigabit-Ethernet, einem 10GBASE-LR-Transceiver (1310 nm) für 10 Gigabit oder einem 100GBASE-LR4 für 100-Gigabit-Ethernet verwenden.
- Die Auto-Negotiation für einen Port muss für eine Verbindung mit einer Portgeschwindigkeit von mehr als 1 Gbit/s deaktiviert sein. Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bedient, muss die automatische Absprache jedoch möglicherweise für 1-Gbit/s-Verbindungen aktiviert oder deaktiviert werden. Wenn Ihre virtuelle Schnittstelle weiterhin nicht verfügbar ist, finden Sie weitere Informationen unter Behandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss Border Gateway Protocol (BGP) und BGP-MD5-Authentifizierung unterstützen.
- (Optional) Sie können jedoch die Bidirectional Forwarding Detection (BFD) in Ihrem Netzwerk konfigurieren. Asynchrones BFD wird automatisch für jede virtuelle Schnittstelle aktiviert. AWS Direct Connect Die asynchrone BFD wird für virtuelle Direct-Connect-Schnittstellen automatisch aktiviert, aber die Aktivierung wird erst wirksam, wenn Sie sie auf Ihrem Router konfigurieren. Weitere Informationen finden Sie unter BFD für eine Direct-Connect-Verbindung aktivieren.

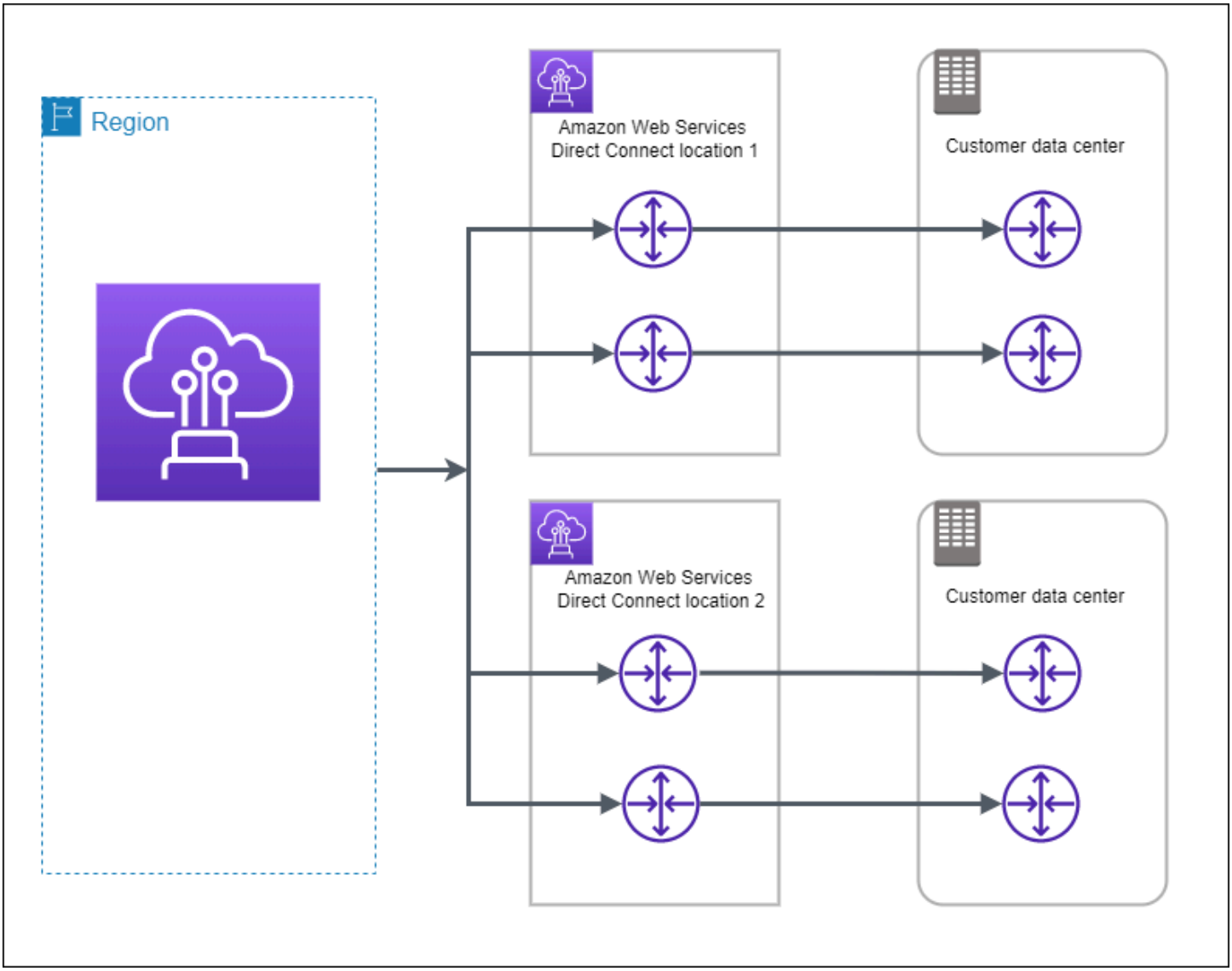
Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie mit der Konfiguration beginnen:

- Das Resilienzmodell, das Sie verwenden möchten.
- Geschwindigkeit, Standort und Partner für alle Ihre Verbindungen.

  Sie benötigen nur die Geschwindigkeit für eine Verbindung.

Maximale Ausfallsicherheit

Sie erzielen maximale Ausfallsicherheit für kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an mehreren Standorten terminiert werden (wie in der nachfolgenden Abbildung dargestellt). Dieses Modell bietet Ausfallsicherheit gegen Geräte-, Konnektivitäts- und vollständige Standortausfälle. Die folgende Abbildung zeigt, dass beide Verbindungen von jedem Kundenrechenzentrum zu denselben AWS Direct Connect Standorten führen. Sie können optional festlegen, dass jede Verbindung von einem Kundenrechenzentrum zu unterschiedlichen Standorten führt.



Die folgenden Verfahren veranschaulichen, wie das AWS Direct Connect Resiliency Toolkit verwendet wird, um ein Modell mit maximaler Ausfallsicherheit zu konfigurieren.

Themen

Schritt 1: Melden Sie sich an für AWS

Für die Nutzung benötigen Sie ein AWS Konto AWS Direct Connect, falls Sie noch keines haben.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Schritt 2: Konfigurieren des Resilienzmodells

So konfigurieren Sie ein Modell mit maximaler Ausfallsicherheit:

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections (Verbindungen) und dann Create a connection (Verbindung erstellen) aus.
3. Wählen Sie unter Connection ordering type (Art der Verbindungsbestellung) die Option Connection wizard (Verbindungsassistent)aus.
4. Wählen Sie unter Resiliency level (Ausfallsicherheitsstufe) die Option Maximum Resiliency (Maximale Ausfallsicherheit) und dann Next (Weiter)aus.
5. Führen Sie im Bereich Configure connections (Verbindungen konfigurieren) unter Connection settings (Verbindungseinstellungen) die folgenden Schritte aus:

   a. Wählen Sie für Bandwidth (Bandbreite) die dedizierte Verbindungsbandbreite aus.

      Diese Bandbreite gilt für alle erstellten Verbindungen.

   b. Wählen Sie unter First Location Service Provider den entsprechenden AWS Direct Connect Standort für die dedizierte Verbindung aus.

   c. Wählen Sie ggf. für First Sub Location (erster Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten liegt. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   d. Wenn Sie Other (Andere) für First location service provider (Serviceanbieter erster Standort) ausgewählt haben, geben Sie für Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   e. Wählen Sie für Second Location Service Provider den entsprechenden AWS Direct Connect Standort aus.

   f. Wählen Sie ggf. für Second Sub Location (zweiter Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten liegt. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   g. Wenn Sie Other (Anderer) für Second location service provider (Serviceanbieter zweiter Standort) ausgewählt haben, geben Sie unter Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   h. (Optional) Hinzufügen oder Entfernen einer Markierung.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Verbindungen, und wählen Sie dann Continue (Weiter) aus.

   Wenn Ihre LOAs bereit sind, können Sie Download LOA (LOA herunterladen) auswählen und dann auf Continue (Weiter) klicken.

   Es kann bis zu 72 Stunden dauern AWS , bis Ihre Anfrage geprüft und ein Port für Ihre Verbindung bereitgestellt ist. Während dieser Zeit erhalten Sie möglicherweise eine E-Mail-Nachricht mit der Bitte um weitere Informationen über Ihren Anwendungsfall oder den angegebenen Standort. Die E-Mail wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung verwendet haben AWS. Sie müssen innerhalb von 7 Tagen antworten, andernfalls wird die Verbindung gelöscht.

Schritt 3: Erstellen Ihrer virtuellen Schnittstellen

Sie können eine private virtuelle Schnittstelle erstellen, um eine Verbindung mit Ihrer VPC herzustellen. Oder Sie können eine öffentliche virtuelle Schnittstelle erstellen, um eine Verbindung zu öffentlichen AWS Diensten herzustellen, die sich nicht in einer VPC befinden. Wenn Sie eine private virtuelle Schnittstelle zu einer VPC erstellen, benötigen Sie eine private virtuelle Schnittstelle für jede VPC, zu der Sie eine Verbindung herstellen. Angenommen, drei private virtuelle Schnittstellen müssen eine Verbindung zu drei VPCs herstellen.

Beginnen Sie erst, wenn die folgenden Informationen vorliegen:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.

Ressource	Erforderliche Informationen
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

Wir bitten Sie um weitere Informationen, wenn Ihre öffentlichen Präfixe oder ASNs zu einem Internetdienstanbieter oder Netzanbieter gehören. Dies kann ein Dokument mit einem offiziellen

Briefkopf oder eine E-Mail-Nachricht von dem Domänennamen des Unternehmens sein, um zu belegen, dass das/der Netzwerkpräfix/ASN von Ihnen verwendet werden darf.

Wenn Sie eine öffentliche virtuelle Schnittstelle erstellen, kann es bis zu 72 Stunden dauern, bis Ihre AWS Anfrage geprüft und genehmigt ist.

So stellen Sie Nicht-VPC-Services eine öffentliche virtuelle Schnittstelle bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public virtual interface settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   d. Geben Sie unter BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) Ihres Gateways ein.

      Die gültigen Werte lauten 1-2147483647.
6. Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie Ihren BGP-MD5-Schlüssel ein.

   Wenn Sie keinen Wert eingeben, erstellen wir einen BGP-Schlüssel.

c. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

So stellen Sie eine private, virtuelle Schnittstelle zu einer VPC bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

c. Wählen Sie als Gateway type (Gateway-Typ) Virtual Private Gateway oder Direct Connect Gateway aus.

d. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus und geben Sie dann das AWS Konto ein.

e. Wählen Sie für Virtual Private Gateway das für diese Schnittstelle zu verwendende Virtual Private Gateway aus.

f. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

g. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, führen Sie einen Failover-Test für virtuelle Schnittstellen durch, um sicherzustellen, dass Ihre Konfiguration Ihren Stabilitätsanforderungen entspricht. Weitere Informationen finden Sie unter the section called “AWS Direct Connect-Failover-Test”.

Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, können Sie Ihre AWS Direct Connect Verbindung mithilfe der folgenden Verfahren überprüfen.

Um Ihre virtuelle Schnittstellenverbindung zur Cloud zu überprüfen AWS

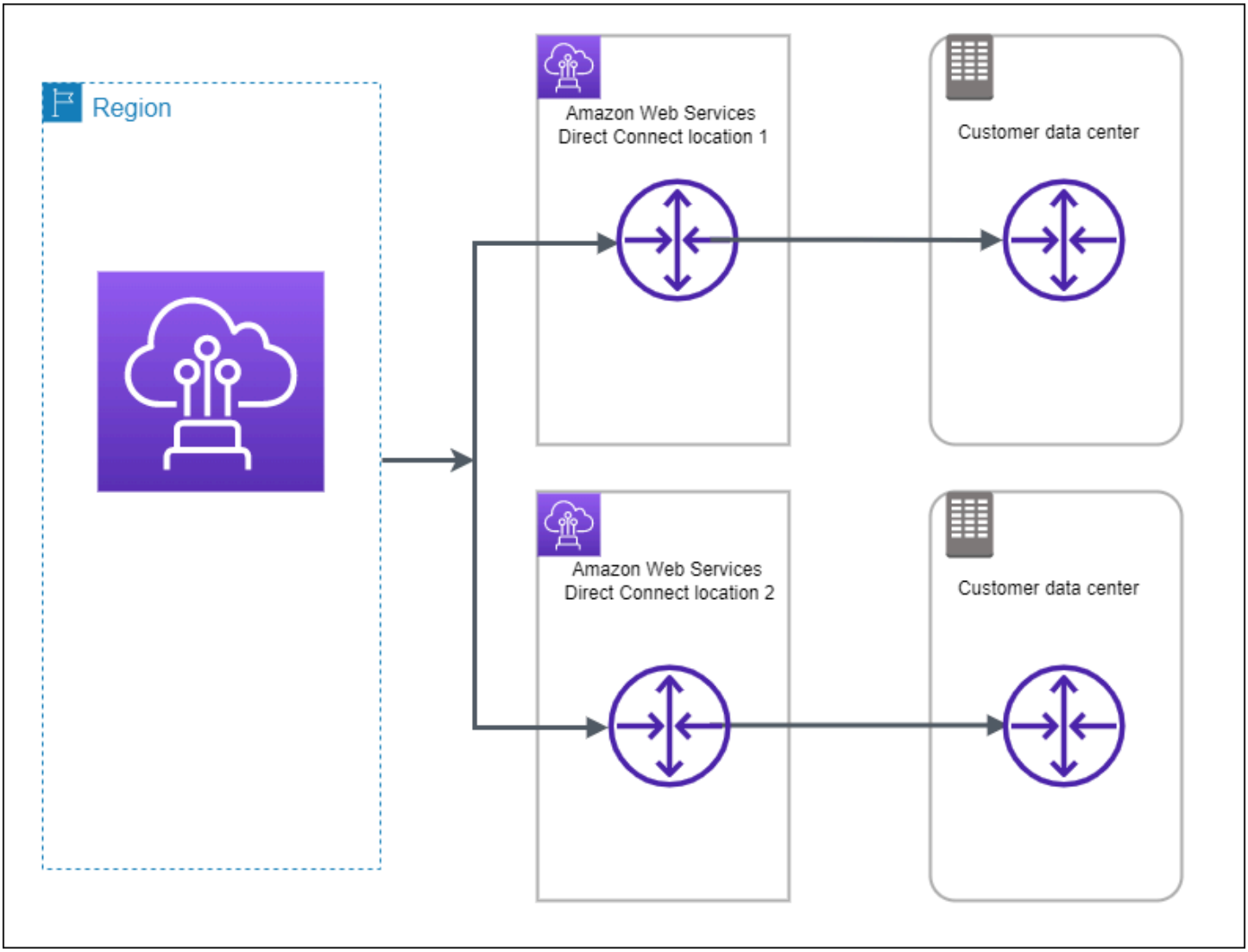
- Führen Sie den `traceroute` Vorgang aus und überprüfen Sie, ob sich der AWS Direct Connect Identifier im Netzwerk-Trace befindet.

So überprüfen Sie die Verbindung Ihrer virtuellen Schnittstelle zu Amazon VPC

1. Starten Sie unter Verwendung eines erreichbaren AMI (z. B. Amazon Linux AMI) eine EC2-Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon Linux AMIs sind auf der Registerkarte Quick Start (Schnellstart) verfügbar, wenn Sie den Startassistenten für Instances in der Amazon-EC2-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im Amazon EC2 EC2-Benutzerhandbuch. Achten Sie darauf, dass die mit der Instance verknüpfte Sicherheitsgruppe eine Regel enthält, die den eingehenden ICMP-Datenverkehr (für die Ping-Anforderung) zulässt.
2. Rufen Sie, sobald die Instance ausgeführt wird, die private IPv4-Adresse (z. B. 10.0.0.4) ab. Die Amazon-EC2-Konsole zeigt die Adresse als Teil der Instance-Details an.
3. Testen Sie mit dem Ping-Befehl die private IPv4-Adresse.

Hohe Ausfallsicherheit

Sie erzielen eine hohe Ausfallsicherheit für kritische Workloads, indem Sie zwei einzelne Verbindungen zu mehreren Standorten verwenden (wie in der folgenden Abbildung dargestellt). Dieses Modell bietet Ausfallsicherheit gegen Konnektivitätsfehler, die durch eine Unterbrechung der Glasfaserverbindung oder einen Geräteausfall verursacht werden. Außerdem werden so vollständige Standortfehler verhindert.



Die folgenden Verfahren zeigen, wie Sie das AWS Direct Connect Resiliency Toolkit verwenden, um ein Modell mit hoher Ausfallsicherheit zu konfigurieren.

Themen

Schritt 1: Melden Sie sich an für AWS

Für die Nutzung benötigen Sie ein AWS Konto AWS Direct Connect, falls Sie noch keines haben.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Schritt 2: Konfigurieren des Resilienzmodells

So konfigurieren Sie ein Modell mit hoher Ausfallsicherheit:

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections (Verbindungen) und dann Create a connection (Verbindung erstellen) aus.
3. Wählen Sie unter Connection ordering type (Art der Verbindungsbestellung) die Option Connection wizard (Verbindungsassistent)aus.
4. Wählen Sie unter Resiliency level (Ausfallsicherheitsstufe) die Option High Resiliency (Hohe Ausfallsicherheit) und dann Next (Weiter)aus.
5. Führen Sie im Bereich Configure connections (Verbindungen konfigurieren) unter Connection settings (Verbindungseinstellungen) die folgenden Schritte aus:

   a. Wählen Sie für Bandwidth (Bandbreite) die Verbindungsbandbreite aus.

      Diese Bandbreite gilt für alle erstellten Verbindungen.

   b. Wählen Sie für First Location Service Provider den entsprechenden AWS Direct Connect Standort aus.

   c. Wählen Sie ggf. für First Sub Location (erster Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten liegt. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   d. Wenn Sie Other (Andere) für First location service provider (Serviceanbieter erster Standort) ausgewählt haben, geben Sie für Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   e. Wählen Sie für Second Location Service Provider den entsprechenden AWS Direct Connect Standort aus.

   f. Wählen Sie ggf. für Second Sub Location (zweiter Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten liegt. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   g. Wenn Sie Other (Anderer) für Second location service provider (Serviceanbieter zweiter Standort) ausgewählt haben, geben Sie unter Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   h. (Optional) Hinzufügen oder Entfernen einer Markierung.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Verbindungen, und wählen Sie dann Continue (Weiter) aus.

   Wenn Ihre LOAs bereit sind, können Sie Download LOA (LOA herunterladen) auswählen und dann auf Continue (Weiter) klicken.

   Es kann bis zu 72 Stunden dauern AWS , bis Ihre Anfrage geprüft und ein Port für Ihre Verbindung bereitgestellt ist. Während dieser Zeit erhalten Sie möglicherweise eine E-Mail-Nachricht mit der Bitte um weitere Informationen über Ihren Anwendungsfall oder den angegebenen Standort. Die E-Mail wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung verwendet haben AWS. Sie müssen innerhalb von 7 Tagen antworten, andernfalls wird die Verbindung gelöscht.

Schritt 3: Erstellen Ihrer virtuellen Schnittstellen

Sie können eine private virtuelle Schnittstelle erstellen, um eine Verbindung mit Ihrer VPC herzustellen. Oder Sie können eine öffentliche virtuelle Schnittstelle erstellen, um eine Verbindung zu öffentlichen AWS Diensten herzustellen, die sich nicht in einer VPC befinden. Wenn Sie eine private virtuelle Schnittstelle zu einer VPC erstellen, benötigen Sie eine private virtuelle Schnittstelle für jede VPC, zu der Sie eine Verbindung herstellen. Angenommen, drei private virtuelle Schnittstellen müssen eine Verbindung zu drei VPCs herstellen.

Beginnen Sie erst, wenn die folgenden Informationen vorliegen:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.

Ressource	Erforderliche Informationen
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

Wenn Ihre öffentlichen Präfixe oder ASNs einem ISP oder Netzbetreiber gehören, AWS fordert Sie zusätzliche Informationen an. Dies kann ein Dokument mit einem offiziellen Briefkopf oder eine E-

Mail-Nachricht von dem Domänennamen des Unternehmens sein, um zu belegen, dass das/der Netzwerkpräfix/ASN von Ihnen verwendet werden darf.

Wenn Sie eine öffentliche virtuelle Schnittstelle einrichten, kann es bis zu 72 Stunden dauern, bis Ihre Anfrage AWS geprüft und genehmigt ist.

So stellen Sie Nicht-VPC-Services eine öffentliche virtuelle Schnittstelle bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public virtual interface settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   d. Geben Sie unter BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) Ihres Gateways ein.

      Die gültigen Werte lauten 1-2147483647.
6. Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie Ihren BGP-MD5-Schlüssel ein.

   Wenn Sie keinen Wert eingeben, erstellen wir einen BGP-Schlüssel.

c. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

So stellen Sie eine private, virtuelle Schnittstelle zu einer VPC bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

c. Wählen Sie als Gateway type (Gateway-Typ) Virtual Private Gateway oder Direct Connect Gateway aus.

d. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus und geben Sie dann das AWS Konto ein.

e. Wählen Sie für Virtual Private Gateway das für diese Schnittstelle zu verwendende Virtual Private Gateway aus.

f. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

g. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, führen Sie einen Failover-Test für virtuelle Schnittstellen durch, um sicherzustellen, dass Ihre Konfiguration Ihren Stabilitätsanforderungen entspricht. Weitere Informationen finden Sie unter the section called “AWS Direct Connect-Failover-Test”.

Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, können Sie Ihre AWS Direct Connect Verbindung mithilfe der folgenden Verfahren überprüfen.

Um Ihre virtuelle Schnittstellenverbindung zur Cloud zu überprüfen AWS

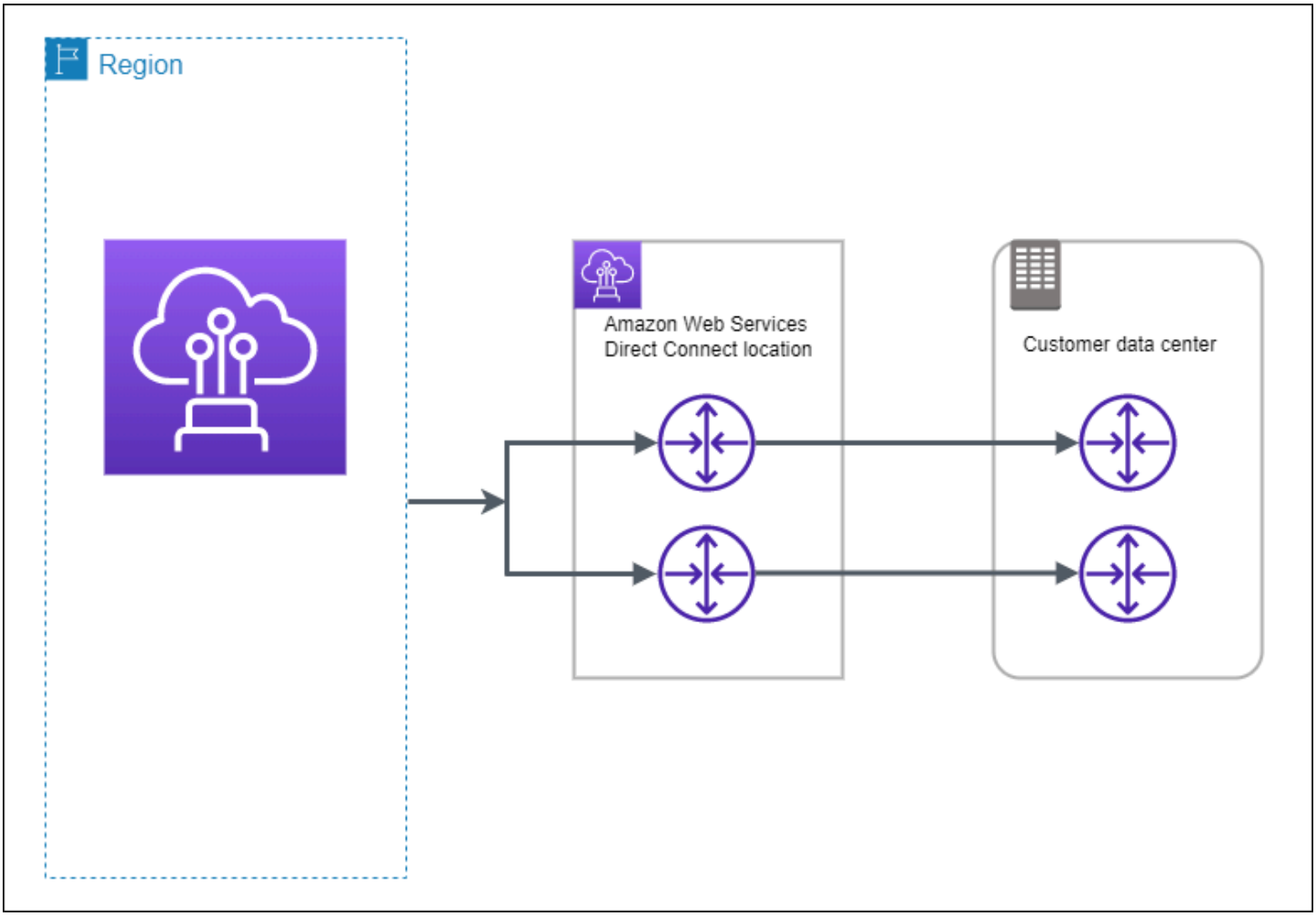
- Führen Sie den `traceroute` Vorgang aus und überprüfen Sie, ob sich der AWS Direct Connect Identifier im Netzwerk-Trace befindet.

So überprüfen Sie die Verbindung Ihrer virtuellen Schnittstelle zu Amazon VPC

1. Starten Sie unter Verwendung eines erreichbaren AMI (z. B. Amazon Linux AMI) eine EC2-Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon Linux AMIs sind auf der Registerkarte Quick Start (Schnellstart) verfügbar, wenn Sie den Startassistenten für Instances in der Amazon-EC2-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im Amazon EC2 EC2-Benutzerhandbuch. Achten Sie darauf, dass die mit der Instance verknüpfte Sicherheitsgruppe eine Regel enthält, die den eingehenden ICMP-Datenverkehr (für die Ping-Anforderung) zulässt.
2. Rufen Sie, sobald die Instance ausgeführt wird, die private IPv4-Adresse (z. B. 10.0.0.4) ab. Die Amazon-EC2-Konsole zeigt die Adresse als Teil der Instance-Details an.
3. Testen Sie mit dem Ping-Befehl die private IPv4-Adresse.

Entwicklung und Test

Sie erzielen Entwicklungs- und Testausfallsicherheit für nicht kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an einem Standort beendet werden (wie in der folgenden Abbildung dargestellt). Dieses Modell bietet Ausfallsicherheit bei Geräteausfällen, jedoch nicht bei Standortfehlern.



Die folgenden Verfahren zeigen, wie Sie mit dem AWS Direct Connect Resiliency Toolkit ein Resilienzmodell für Entwicklung und Test konfigurieren.

Themen

Schritt 1: Melden Sie sich an für AWS

Für die Nutzung benötigen Sie ein AWS Konto AWS Direct Connect, falls Sie noch keines haben.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Schritt 2: Konfigurieren des Resilienzmodells

So konfigurieren Sie das Resilienzmodell:

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections (Verbindungen) und dann Create a connection (Verbindung erstellen) aus.
3. Wählen Sie unter Connection ordering type (Art der Verbindungsbestellung) die Option Connection wizard (Verbindungsassistent)aus.
4. Wählen Sie unter Resiliency level (Ausfallsicherheitsstufe) die Option Development and test (Entwicklung und Test) und dann Next (Weiter)aus.
5. Führen Sie im Bereich Configure connections (Verbindungen konfigurieren) unter Connection settings (Verbindungseinstellungen) die folgenden Schritte aus:

   a. Wählen Sie für Bandwidth (Bandbreite) die Verbindungsbandbreite aus.

      Diese Bandbreite gilt für alle erstellten Verbindungen.

   b. Wählen Sie für First Location Service Provider den entsprechenden AWS Direct Connect Standort aus.

   c. Wählen Sie ggf. für First Sub Location (erster Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten liegt. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   d. Wenn Sie Other (Andere) für First location service provider (Serviceanbieter erster Standort) ausgewählt haben, geben Sie für Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   e. (Optional) Hinzufügen oder Entfernen einer Markierung.

      [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

      - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
      - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

      [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.
6. Wählen Sie Weiter aus.
7. Überprüfen Sie Ihre Verbindungen, und wählen Sie dann Continue (Weiter) aus.

Wenn Ihre LOAs bereit sind, können Sie Download LOA (LOA herunterladen) auswählen und dann auf Continue (Weiter) klicken.

Es kann bis zu 72 Stunden dauern AWS , bis Ihre Anfrage geprüft und ein Port für Ihre Verbindung bereitgestellt ist. Während dieser Zeit erhalten Sie möglicherweise eine E-Mail-Nachricht mit der Bitte um weitere Informationen über Ihren Anwendungsfall oder den angegebenen Standort. Die E-Mail wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung verwendet haben AWS. Sie müssen innerhalb von 7 Tagen antworten, andernfalls wird die Verbindung gelöscht.

Schritt 3: Erstellen einer virtuellen Schnittstelle

Um Ihre AWS Direct Connect Verbindung nutzen zu können, müssen Sie eine virtuelle Schnittstelle erstellen. Sie können eine private virtuelle Schnittstelle erstellen, um eine Verbindung mit Ihrer VPC herzustellen. Oder Sie können eine öffentliche virtuelle Schnittstelle erstellen, um eine Verbindung zu öffentlichen AWS Diensten herzustellen, die sich nicht in einer VPC befinden. Wenn Sie eine private virtuelle Schnittstelle zu einer VPC erstellen, benötigen Sie eine private virtuelle Schnittstelle für jede VPC, zu der Sie eine Verbindung herstellen. Angenommen, drei private virtuelle Schnittstellen müssen eine Verbindung zu drei VPCs herstellen.

Beginnen Sie erst, wenn die folgenden Informationen vorliegen:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

Wir bitten Sie um weitere Informationen, wenn Ihre öffentlichen Präfixe oder ASNs zu einem Internetdienstanbieter oder Netzanbieter gehören. Dies kann ein Dokument mit einem offiziellen

Briefkopf oder eine E-Mail-Nachricht von dem Domänennamen des Unternehmens sein, um zu belegen, dass das/der Netzwerkpräfix/ASN von Ihnen verwendet werden darf.

Wenn Sie eine öffentliche virtuelle Schnittstelle erstellen, kann es bis zu 72 Stunden dauern, bis AWS Ihre Anforderung überprüft und genehmigt.

So stellen Sie Nicht-VPC-Services eine öffentliche virtuelle Schnittstelle bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public virtual interface settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   d. Geben Sie unter BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) Ihres Gateways ein.

      Die gültigen Werte lauten 1-2147483647.
6. Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie Ihren BGP-MD5-Schlüssel ein.

   Wenn Sie keinen Wert eingeben, erstellen wir einen BGP-Schlüssel.

c. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

So stellen Sie eine private, virtuelle Schnittstelle zu einer VPC bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

c. Wählen Sie als Gateway type (Gateway-Typ) Virtual Private Gateway oder Direct Connect Gateway aus.

d. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus und geben Sie dann das AWS Konto ein.

e. Wählen Sie für Virtual Private Gateway das für diese Schnittstelle zu verwendende Virtual Private Gateway aus.

f. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

g. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, führen Sie einen Failover-Test für virtuelle Schnittstellen durch, um sicherzustellen, dass Ihre Konfiguration Ihren Stabilitätsanforderungen entspricht. Weitere Informationen finden Sie unter the section called “AWS Direct Connect-Failover-Test”.

Schritt 5: Überprüfen Ihrer virtuellen Schnittstelle

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, können Sie Ihre AWS Direct Connect Verbindung mithilfe der folgenden Verfahren überprüfen.

Um Ihre virtuelle Schnittstellenverbindung zur Cloud zu überprüfen AWS

- Führen Sie den `traceroute` Vorgang aus und überprüfen Sie, ob sich der AWS Direct Connect Identifier im Netzwerk-Trace befindet.

So überprüfen Sie die Verbindung Ihrer virtuellen Schnittstelle zu Amazon VPC

1. Starten Sie unter Verwendung eines erreichbaren AMI (z. B. Amazon Linux AMI) eine EC2-Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon Linux AMIs sind auf der Registerkarte Quick Start (Schnellstart) verfügbar, wenn Sie den Startassistenten für Instances in der Amazon-EC2-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im Amazon EC2 EC2-Benutzerhandbuch. Achten Sie darauf, dass die mit der Instance verknüpfte Sicherheitsgruppe eine Regel enthält, die den eingehenden ICMP-Datenverkehr (für die Ping-Anforderung) zulässt.
2. Rufen Sie, sobald die Instance ausgeführt wird, die private IPv4-Adresse (z. B. 10.0.0.4) ab. Die Amazon-EC2-Konsole zeigt die Adresse als Teil der Instance-Details an.
3. Testen Sie mit dem Ping-Befehl die private IPv4-Adresse.

Classic

Wählen Sie Classic aus, wenn bestehende Verbindungen vorhanden sind.

Die folgenden Verfahren zeigen die gängigen Szenarien zur Einrichtung einer AWS Direct Connect - Verbindung.

Inhalt

Voraussetzungen

Stellen Sie bei Verbindungen AWS Direct Connect mit Portgeschwindigkeiten von 1 Gbit/s oder höher sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt:

- Ihr Netzwerk muss Singlemode-Glasfaser mit einem 1000BASE-LX-Transceiver (1310 nm) für 1-Gigabit-Ethernet, einem 10GBASE-LR-Transceiver (1310 nm) für 10 Gigabit oder einem 100GBASE-LR4 für 100-Gigabit-Ethernet verwenden.
- Die Auto-Negotiation für einen Port muss für eine Verbindung mit einer Portgeschwindigkeit von mehr als 1 Gbit/s deaktiviert sein. Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bedient, muss die automatische Absprache jedoch möglicherweise für 1-Gbit/s-Verbindungen aktiviert oder deaktiviert werden. Wenn Ihre virtuelle Schnittstelle weiterhin nicht verfügbar ist, finden Sie weitere Informationen unter Behandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss Border Gateway Protocol (BGP) und BGP-MD5-Authentifizierung unterstützen.
- (Optional) Sie können jedoch die Bidirectional Forwarding Detection (BFD) in Ihrem Netzwerk konfigurieren. Asynchrones BFD wird automatisch für jede virtuelle Schnittstelle aktiviert. AWS Direct Connect Die asynchrone BFD wird für virtuelle Direct-Connect-Schnittstellen automatisch aktiviert, aber die Aktivierung wird erst wirksam, wenn Sie sie auf Ihrem Router konfigurieren. Weitere Informationen finden Sie unter BFD für eine Direct-Connect-Verbindung aktivieren.

Schritt 1: Melden Sie sich an für AWS

Für die Nutzung benötigen Sie ein Konto AWS Direct Connect, falls Sie noch keines haben.

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Schritt 2: Fordern Sie eine AWS Direct Connect dedizierte Verbindung an

Für dedizierte Verbindungen können Sie über die AWS Direct Connect Konsole eine Verbindungsanfrage stellen. Bei gehosteten Verbindungen wenden Sie sich an einen AWS Direct Connect Partner, um eine gehostete Verbindung anzufordern. Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen:

- Die Portgeschwindigkeit, die Sie benötigen. Sie können die Portgeschwindigkeit nach dem Erstellen der Verbindungsanforderung nicht ändern.
- Der AWS Direct Connect Ort, an dem die Verbindung beendet werden soll.

> **Note**
>
> Sie können die AWS Direct Connect Konsole nicht verwenden, um eine gehostete Verbindung anzufordern. Wenden Sie sich stattdessen an einen AWS Direct Connect

Partner, der eine gehostete Verbindung für Sie herstellen kann, die Sie dann akzeptieren. Überspringen Sie die folgenden Schritte und gehen Sie zu Akzeptieren Ihrer gehosteten Verbindung.

Um eine neue AWS Direct Connect Verbindung herzustellen

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections (Verbindungen) und dann Create a connection (Verbindung erstellen) aus.
3. Wählen Sie Classicaus.
4. Gehen Sie im Bereich Create connection (Verbindung erstellen) unter Connection settings (Verbindungseinstellungen) wie folgt vor:

   a. Geben Sie unter Name einen Namen für die Verbindung ein.

   b. Wählen Sie unter Location (Standort) den entsprechenden AWS Direct Connect -Standort aus.

   c. Wählen Sie ggf. für Sub Location (Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten ist. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.

   d. Wählen Sie für Port Speed (Portgeschwindigkeit) die Verbindungsbandbreite aus.

   e. Wählen Sie für On-premises die Option Über einen AWS Direct Connect Partner Connect aus, wenn Sie diese Verbindung verwenden, um eine Verbindung zu Ihrem Rechenzentrum herzustellen.

   f. Wählen Sie als Dienstanbieter den AWS Direct Connect Partner aus. Wenn Sie einen Partner verwenden, der nicht in der Liste enthalten ist, wählen Sie Other (Anderer) aus.

   g. Wenn Sie Other (Anderer) für Service provider (Serviceanbieter) ausgewählt haben, geben Sie unter Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.

   h. (Optional) Hinzufügen oder Entfernen einer Markierung.

      [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

      - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.

- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

5. Wählen Sie Create Connection (Verbindung erstellen) aus.

Es kann bis zu 72 Stunden dauern AWS , bis Ihre Anfrage geprüft und ein Port für Ihre Verbindung bereitgestellt ist. Während dieser Zeit erhalten Sie möglicherweise eine E-Mail-Nachricht mit der Bitte um weitere Informationen über Ihren Anwendungsfall oder den angegebenen Standort. Die E-Mail wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung verwendet haben AWS. Sie müssen innerhalb von 7 Tagen antworten, andernfalls wird die Verbindung gelöscht.

Weitere Informationen finden Sie unter AWS Direct Connect Verbindungen.

Akzeptieren Ihrer gehosteten Verbindung

Sie müssen die gehostete Verbindung in der AWS Direct Connect Konsole akzeptieren, bevor Sie eine virtuelle Schnittstelle erstellen können. Dieser Schritt gilt nur für gehostete Verbindungen.

So akzeptieren Sie eine gehostete virtuelle Schnittstelle

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die gehostete Verbindung aus und klicken Sie dann auf Accept (Akzeptieren).

   Wählen Sie Accept (Akzeptieren) aus.

(Dedizierte Verbindung) Schritt 3: Herunterladen des LOA-CFA

Nachdem Sie die Verbindung angefordert haben, stellen wir Ihnen einen „Letter of Authorization and Connecting Facility Assignment“ (LOA-CFA) zum Download zur Verfügung oder senden Ihnen nach der Erstellung der Verbindungsanforderung eine E-Mail zu, in der Sie gebeten werden, weitere Informationen anzugeben. Die LOA-CFA ist die Autorisierung für die Verbindung und wird vom Colocation-Anbieter oder Ihrem Netzwerkanbieter benötigt AWS, um die netzwerkübergreifende Verbindung (Cross-Connect) herzustellen.

So laden Sie das LOA-CFA-Dokument herunter

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/directconnect/v2/home. AWS Direct Connect
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die Verbindung und View details (Details ansehen) aus.
4. Wählen Sie Download LOA-CFA aus.

   Das LOA-CFA-Dokument wird als PDF-Datei auf Ihren Computer heruntergeladen.

   > **Note**
   >
   > Wenn der Link nicht aktiviert ist, steht das LOA-CFA-Dokument noch nicht zum Download bereit. Überprüfen Sie, ob sich in Ihrem E-Mail-Posteingang eine Bitte um weitere Informationen befindet. Wenn die Autorisierung immer noch nicht verfügbar ist und Sie auch nach 72 Stunden keine E-Mail erhalten haben, wenden Sie sich an den AWS Support.

5. Führen Sie nach dem Download des LOA-CFA einen der folgenden Schritte aus:

   - Wenn Sie mit einem AWS Direct Connect Partner oder Netzwerkanbieter zusammenarbeiten, senden Sie ihm den LOA-CFA, damit er vor Ort eine Cross-Connect-Verbindung für Sie bestellen kann. AWS Direct Connect Wenn er keine Querverbindung für Sie bestellen kann, wenden Sie sich ggf. direkt an den Co-Location-Anbieter.
   - Wenn Sie am AWS Direct Connect Standort über Geräte verfügen, wenden Sie sich an den Colocation-Anbieter, um eine netzwerkübergreifende Verbindung anzufordern. Sie müssen ein Kunde des Co-Location-Anbieters sein. Sie müssen ihnen auch den LOA-CFA vorlegen, der die Verbindung zum AWS Router autorisiert, sowie die erforderlichen Informationen, um eine Verbindung zu Ihrem Netzwerk herzustellen.

AWS Direct Connect Standorte, die als mehrere Standorte aufgeführt sind (z. B. Equinix DC1-DC6 und DC10-DC11), werden als Campus eingerichtet. Wenn sich Ihre Ausrüstung oder die Ihres Netzanbieters an einem dieser Standorte befindet, können Sie eine Querverbindung zu dem Ihnen zugewiesenen Port anfordern, auch wenn sich dieser in einem anderen Gebäude auf dem Campus befindet.

> **Important**
>
> Ein Campus wird als ein einziger Standort behandelt. AWS Direct Connect Um hohe Verfügbarkeit zu erzielen, konfigurieren Sie Verbindungen zu anderen AWS Direct Connect - Standorten.

Wenn Sie oder Ihr Netzanbieter Probleme bei der Herstellung einer physischen Verbindung haben, lesen Sie Behandlung von Problemen auf Ebene 1 (physisch).

Schritt 4: Erstellen einer virtuellen Schnittstelle

Um Ihre AWS Direct Connect Verbindung nutzen zu können, müssen Sie eine virtuelle Schnittstelle erstellen. Sie können eine private virtuelle Schnittstelle erstellen, um eine Verbindung mit Ihrer VPC herzustellen. Oder Sie können eine öffentliche virtuelle Schnittstelle erstellen, um eine Verbindung zu öffentlichen AWS Diensten herzustellen, die sich nicht in einer VPC befinden. Wenn Sie eine private virtuelle Schnittstelle zu einer VPC erstellen, benötigen Sie eine private virtuelle Schnittstelle für jede VPC, zu der Sie eine Verbindung herstellen. Angenommen, drei private virtuelle Schnittstellen müssen eine Verbindung zu drei VPCs herstellen.

Beginnen Sie erst, wenn die folgenden Informationen vorliegen:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private

Ressource	Erforderliche Informationen
	ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

Wir bitten Sie um weitere Informationen, wenn Ihre öffentlichen Präfixe oder ASNs zu einem Internetdienstanbieter oder Netzanbieter gehören. Dies kann ein Dokument mit einem offiziellen

Briefkopf oder eine E-Mail von dem Domänennamen des Unternehmens sein, um zu belegen, dass der Netzwerkpräfix/ASN von Ihnen verwendet werden darf.

Für private virtuelle Schnittstellen und öffentliche virtuelle Schnittstellen ist die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung die Größe des größten zulässigen Pakets, das über die Verbindung übergeben werden kann, in Byte. Der MTU-Wert einer virtuellen privaten Schnittstelle kann entweder 1 500 oder 9 001 (Jumbo-Frames) sein. Der MTU-Wert einer virtuellen Transit-Schnittstelle kann entweder 1500 oder 8500 (Jumbo-Frames) sein. Sie können die MTU angeben, wenn Sie die Schnittstelle erstellen oder eine erstellte Schnittstelle aktualisieren. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8500 (Jumbo-Frames) oder 9001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Registerkarte Zusammenfassung nach Jumbo Frame-fähig.

Wenn Sie eine öffentliche virtuelle Schnittstelle erstellen, kann es bis zu 72 Stunden dauern, bis Ihre AWS Anfrage geprüft und genehmigt ist.

So stellen Sie Nicht-VPC-Services eine öffentliche virtuelle Schnittstelle bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public virtual interface settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

d. Geben Sie für BGP ASN die Border Gateway Protocol Autonomous System Number des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1-2147483647.

6. Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

   b. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie Ihren BGP-MD5-Schlüssel ein.

      Wenn Sie keinen Wert eingeben, erstellen wir einen BGP-Schlüssel.

   c. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

   d. (Optional) Hinzufügen oder Entfernen einer Markierung.

      [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

      - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
      - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

      [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

So stellen Sie eine private, virtuelle Schnittstelle zu einer VPC bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.
   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.
   c. Wählen Sie als Gateway type (Gateway-Typ) Virtual Private Gateway oder Direct Connect Gateway aus.
   d. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus und geben Sie dann das AWS Konto ein.
   e. Wählen Sie für Virtual Private Gateway das für diese Schnittstelle zu verwendende Virtual Private Gateway aus.
   f. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.
   g. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1 bis 2147483647.
6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

> **Important**
>
> Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben.
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
8. Sie müssen Ihr BGP-Gerät verwenden, um das Netzwerk anzukündigen, das Sie für die öffentliche VIF-Verbindung verwenden.

Schritt 5: Herunterladen der Routerkonfiguration

Nachdem Sie eine virtuelle Schnittstelle für Ihre AWS Direct Connect Verbindung erstellt haben, können Sie die Router-Konfigurationsdatei herunterladen. Die Datei enthält die erforderlichen Befehle zum Konfigurieren Ihres Routers für die Verwendung mit Ihrer privaten oder öffentlichen virtuellen Schnittstelle.

So laden Sie eine Router-Konfiguration herunter

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die Verbindung und View details (Details ansehen) aus.
4. Wählen Sie Download router configuration (Router-Konfiguration herunterladen) aus.
5. Führen Sie unterDownload router configuration (Router-Konfiguration herunterladen) die folgenden Schritte aus:
   a. Wählen Sie unter Vendor den Hersteller Ihres Routers aus.
   b. Wählen Sie unter Platform das Modell Ihres Routers aus.
   c. Wählen Sie unter Software die Softwareversion Ihres Routers aus.
6. Wählen Sie Download (Herunterladen) und verwenden Sie anschließend die entsprechende Konfiguration für Ihren Router, damit Sie eine Verbindung zu AWS Direct Connect herstellen können.

Beispiel-Konfigurationsdateien finden Sie unter Beispiel für Router-Konfigurationsdateien.

Nach der Konfiguration Ihres Routers wechselt der Status der virtuellen Schnittstelle zu UP. Wenn die virtuelle Schnittstelle weiterhin nicht verfügbar ist und Sie die Peer-IP-Adresse des AWS Direct Connect Geräts nicht pingen können, finden Sie weitere Informationen unterBehandlung von Problemen auf Ebene 2 (Datenverbindung). Wenn Sie die Peer-IP-Adresse anpingen können, lesen Sie Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport). Wenn die BGP-Peering-Sitzung hergestellt wurde, Sie den Datenverkehr aber nicht weiterleiten können, lesen Sie Beheben von Routing-Problemen.

Schritt 6: Überprüfen der virtuellen Schnittstelle

Nachdem Sie virtuelle Schnittstellen zur AWS Cloud oder zu Amazon VPC eingerichtet haben, können Sie Ihre AWS Direct Connect Verbindung mithilfe der folgenden Verfahren überprüfen.

Um Ihre virtuelle Schnittstellenverbindung zur Cloud zu überprüfen AWS

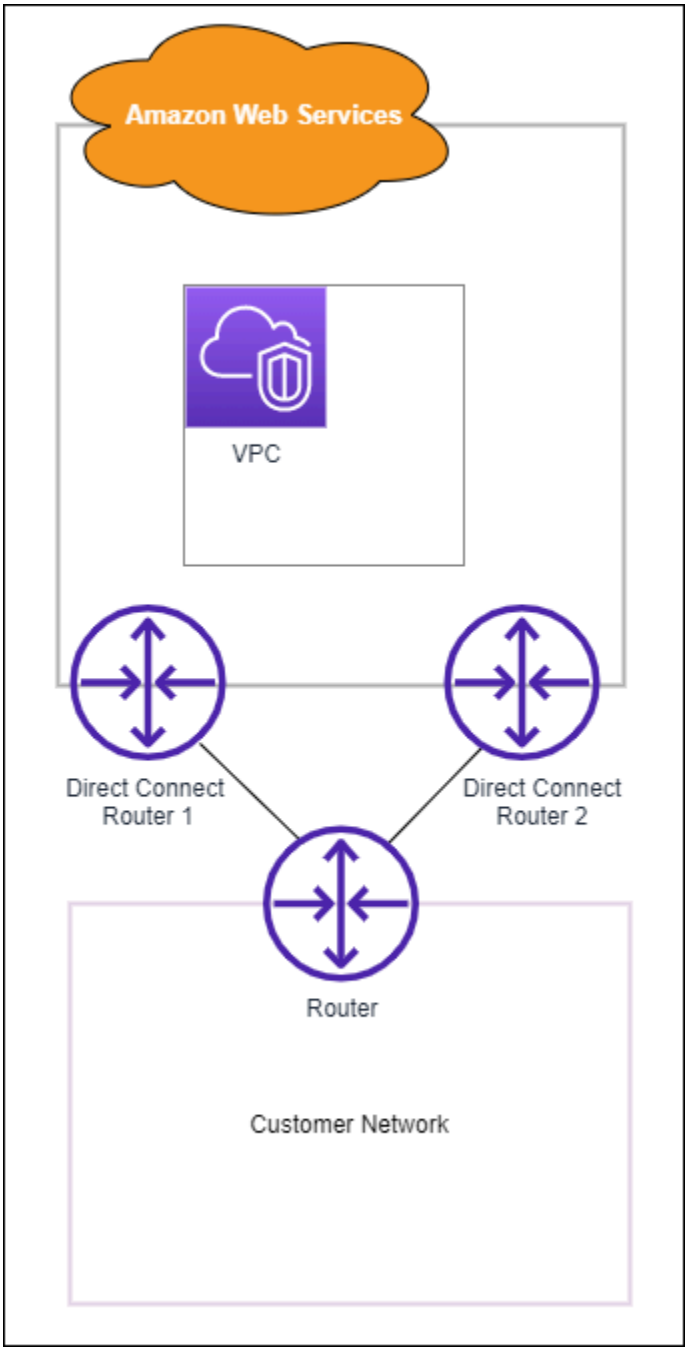
- Führen Sie den `traceroute` Vorgang aus und überprüfen Sie, ob sich der AWS Direct Connect Identifier im Netzwerk-Trace befindet.

So überprüfen Sie die Verbindung Ihrer virtuellen Schnittstelle zu Amazon VPC

1. Starten Sie unter Verwendung eines erreichbaren AMI (z. B. Amazon Linux AMI) eine EC2-Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon Linux AMIs sind auf der Registerkarte Quick Start (Schnellstart) verfügbar, wenn Sie den Startassistenten für Instances in der Amazon-EC2-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im Amazon EC2 EC2-Benutzerhandbuch. Achten Sie darauf, dass die mit der Instance verknüpfte Sicherheitsgruppe eine Regel enthält, die den eingehenden ICMP-Datenverkehr (für die Ping-Anforderung) zulässt.
2. Rufen Sie, sobald die Instance ausgeführt wird, die private IPv4-Adresse (z. B. 10.0.0.4) ab. Die Amazon-EC2-Konsole zeigt die Adresse als Teil der Instance-Details an.
3. Testen Sie mit dem Ping-Befehl die private IPv4-Adresse.

(Empfohlen) Schritt 7: Konfigurieren redundanter Verbindungen

Um ein Failover zu gewährleisten, empfehlen wir, dass Sie zwei dedizierte Verbindungen für anfordern und konfigurieren AWS, wie in der folgenden Abbildung dargestellt. Diese Verbindungen können auf ein oder zwei Routern in Ihrem Netzwerk auflaufen.



Es sind verschiedene Konfigurationsoptionen verfügbar, wenn Sie zwei dedizierte Verbindungen bereitstellen:

- Aktiv/Aktiv (BGP Multipath). Dies ist die Standardkonfiguration, bei der beide Verbindungen aktiv sind. AWS Direct Connect unterstützt Multipathing zu mehreren virtuellen Schnittstellen am selben Standort, und der Datenverkehr wird auf der Grundlage des Datenflusses auf die Schnittstellen verteilt. Wenn eine Verbindung ausfällt, wird der gesamte Datenverkehr über die andere Verbindung geleitet.

- Aktiv/Passiv (Failover). Eine Verbindung dient zur Verarbeitung des Datenverkehrs, die andere befindet sich im Standby-Modus. Wenn die aktive Verbindung ausfällt, wird der gesamte Datenverkehr über die passive Verbindung geleitet. Sie müssen einem Link (dem passiven) den AS-Pfad voranstellen.

Die Konfiguration der Verbindungen hat keine Auswirkungen auf die Redundanz, aber auf die Richtlinien für das Routing der Daten über beide Verbindungen. Wir empfehlen, beide Verbindungen als aktiv zu konfigurieren.

Wenn Sie eine VPN-Verbindung für Redundanz verwenden, stellen Sie sicher, dass Sie eine Zustandsprüfung und einen Failover-Mechanismus implementieren. Wenn Sie eine der folgenden Konfigurationen verwenden, müssen Sie das Routing Ihrer Routing-Tabelle überprüfen, um an die neue Netzwerkschnittstelle weiterzuleiten.

- Sie verwenden Ihre eigenen Instances für das Routing, z. B. kann die Firewall die Instance sein.
- Sie verwenden Ihre eigene Instance, die eine VPN-Verbindung beendet.

Um eine hohe Verfügbarkeit zu erreichen, empfehlen wir dringend, Verbindungen zu verschiedenen Standorten zu konfigurieren. AWS Direct Connect

Weitere Informationen zur AWS Direct Connect Resilienz finden Sie unter AWS Direct Connect Resilienz-Empfehlungen.

AWS Direct Connect-Failover-Test

Die Modelle des AWS Direct Connect Resiliency Toolkit wurden entwickelt, um sicherzustellen, dass Sie über die angemessene Anzahl virtueller Schnittstellenverbindungen an mehreren Standorten verfügen. Nachdem Sie den Assistenten abgeschlossen haben, beenden Sie mit dem Failover-Test des AWS Direct Connect Resiliency Toolkit die BGP-Peering-Sitzung, um zu überprüfen, ob die Datenverkehrsrouten zu einer Ihrer redundanten virtuellen Schnittstellen Ihre Anforderungen an die Ausfallsicherheit erfüllen.

Stellen Sie mithilfe des Tests sicher, dass Datenverkehr über redundante virtuelle Schnittstellen weitergeleitet wird, wenn eine virtuelle Schnittstelle außer Betrieb ist. Sie starten den Test, indem Sie eine virtuelle Schnittstelle, eine BGP-Peering-Sitzung und die gewünschte Dauer für die Testausführung auswählen. AWS platziert die BGP-Peering-Sitzung der ausgewählten Schnittstelle in den heruntergefahrenen Zustand. Wenn sich die Schnittstelle in diesem Zustand befindet, sollte der Datenverkehr über eine redundante virtuelle Schnittstelle gehen. Wenn Ihre Konfiguration nicht

die entsprechenden redundanten Verbindungen enthält, schlägt die BGP-Peeringsitzung fehl, und der Datenverkehr wird nicht weitergeleitet. Wenn der Test abgeschlossen wird oder Sie ihn manuell beenden, stellt AWS die BGP-Sitzung wieder her. Nachdem der Test abgeschlossen wurde, können Sie Ihre Konfiguration mit dem AWS Direct Connect Resiliency Toolkit anpassen.

> **Note**
>
> Verwenden Sie diese Funktion nicht während eines Direct Connect-Wartungszeitraums, da die BGP-Sitzung während oder nach der Wartung möglicherweise vorzeitig wiederhergestellt wird.

Testverlauf

AWS löscht den Testverlauf nach 365 Tagen. Der Testverlauf enthält den Status für Tests, die auf allen BGP-Peers ausgeführt wurden. Der Verlauf enthält, welche BGP-Peering-Sitzungen getestet wurden, die Start- und Endzeiten sowie den Teststatus, bei dem es sich um einen der folgenden Werte handeln kann:

- In Bearbeitung – Der Test wird derzeit ausgeführt.
- Abgeschlossen – Der Test wurde für die angegebene Zeit ausgeführt.
- Abgebrochen – Der Test wurde vor der angegebenen Zeit abgebrochen.
- Fehlgeschlagen – Der Test wurde zu dem von Ihnen angegebenen Zeitpunkt nicht ausgeführt. Dies kann passieren, wenn ein Problem mit dem Router vorliegt.

Weitere Informationen finden Sie unter the section called “Anzeigen des Failover-Testverlaufs der virtuellen Schnittstelle”.

Validierungsberechtigungen

Das einzige Konto, das zum Ausführen des Failovertests berechtigt ist, ist das Konto, das die virtuelle Schnittstelle besitzt. Der Kontoinhaber erhält einen Hinweis über AWS CloudTrail darauf, dass ein Test auf einer virtuellen Schnittstelle ausgeführt wurde.

Starten des Failover-Tests für die virtuelle Schnittstelle

Sie können den Failover-Test für die virtuelle Schnittstelle über die AWS Direct Connect-Konsole oder über die AWS CLI starten.

So starten Sie den Failover-Test für die virtuelle Schnittstelle von der AWS Direct Connect-Konsole aus

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie Virtuelle Schnittstellen.
3. Wählen Sie die virtuellen Schnittstellen und dann Aktionen, BGP herunterfahren aus.

   Sie können den Test auf einer öffentlichen oder einer privaten Schnittstelle oder auf einer virtuellen Transitschnittstelle ausführen.
4. Führen Sie im Dialogfeld Fehlertest starten die folgenden Schritte aus:

   a. Wählen Sie für Peering-Sitzungen, die zum Testen deaktiviert werden müssen, welche Peering-Sitzungen getestet werden sollen, z. B. IPv4.

   b. Geben Sie für die Maximale Testzeit die Anzahl der Minuten ein, die der Test dauern soll.

      Der Maximalwert beträgt 4 320 Minuten (72 Stunden).

      Der Standardwert ist 180 Minuten (3 Stunden).

   c. Geben Sie für Um den Test zu bestätigen Bestätigen ein.

   d. Wählen Sie Bestätigen aus.

   Die BGP-Peering-Sitzung wird in den Zustand DOWN versetzt. Sie können Datenverkehr senden, um sicherzustellen, dass keine Ausfälle vorliegen. Bei Bedarf können Sie den Test sofort beenden.

So starten Sie den Failover-Test für die virtuelle Schnittstelle mit der AWS CLI

Verwenden Sie StartBgpFailoverTest.

Anzeigen des Failover-Testverlaufs der virtuellen Schnittstelle

Sie können den Failover-Testverlauf der virtuellen Schnittstelle über die AWS Direct Connect-Konsole oder über die AWS CLI anzeigen.

So zeigen Sie den Failover-Testverlauf der virtuellen Schnittstelle über die AWS Direct Connect-Konsole an

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie Virtuelle Schnittstellen.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).
4. Wählen Sie Testverlauf aus.

   Die Konsole zeigt die Tests der virtuellen Schnittstelle an, die Sie für die virtuelle Schnittstelle durchgeführt haben.
5. Um die Details für einen bestimmten Test anzuzeigen, wählen Sie die Test-ID aus.

So zeigen Sie den Failover-Testverlauf der virtuellen Schnittstelle mit der AWS CLI an

Verwenden Sie ListVirtualInterfaceTestHistory.

Beenden des Failover-Tests für die virtuelle Schnittstelle

Sie können den Failover-Test der virtuellen Schnittstelle über die AWS Direct Connect-Konsole oder die AWS CLI beenden.

So beenden Sie den Failover-Test für die virtuelle Schnittstelle von der AWS Direct Connect-Konsole aus

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie Virtuelle Schnittstellen.
3. Wählen Sie die virtuelle Schnittstelle und dann Aktionen, Test abbrechen aus.
4. Wählen Sie Bestätigen aus.

AWS stellt die BGP-Peering-Sitzung wieder her. Der Testverlauf zeigt für den Test „abgebrochen“ an.

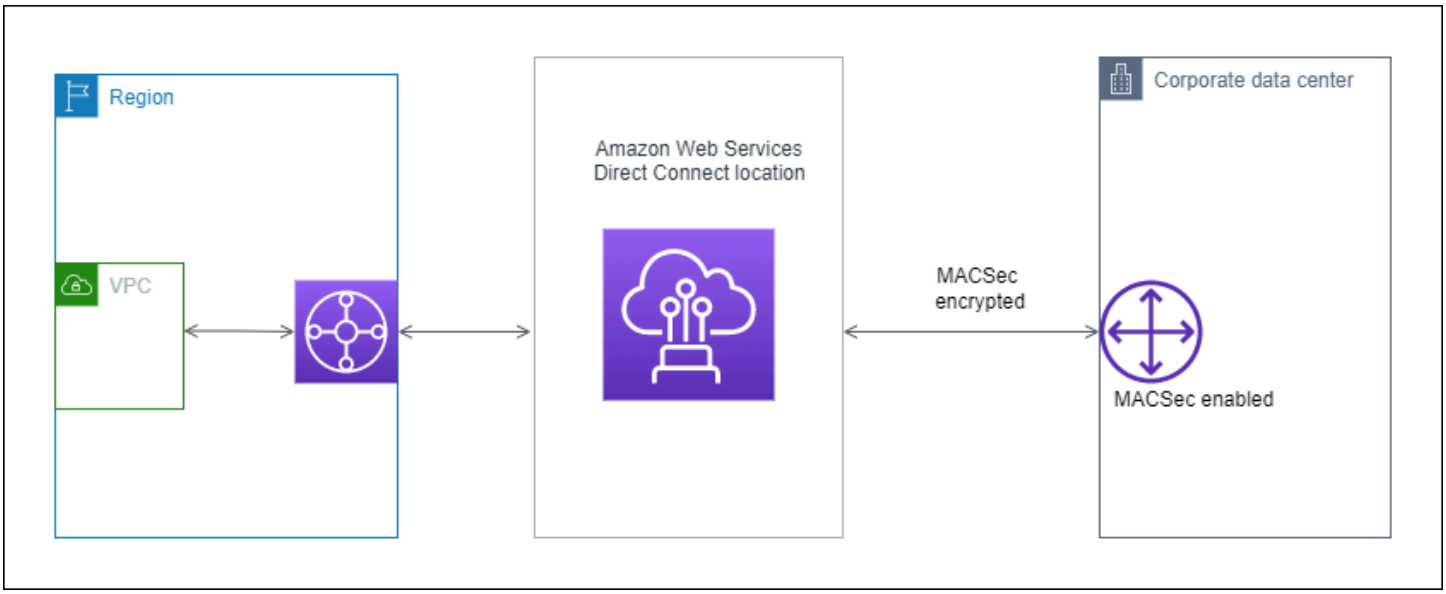
So beenden Sie den Failover-Test der virtuellen Schnittstelle mit der AWS CLI

Verwenden Sie StopBgpFailoverTest.

MAC Security

MAC Security (MACsec) ist ein IEEE-Standard, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. MACSec bietet point-to-point Layer-2-Verschlüsselung über die Querverbindung zu. AWS MACSec arbeitet auf Layer 2 zwischen zwei Layer-3-Routern und sorgt für Verschlüsselung in der Layer-2-Domäne. Alle Daten, die über das AWS globale Netzwerk fließen, das sich mit Rechenzentren und Regionen verbindet, werden auf der physischen Ebene automatisch verschlüsselt, bevor sie das Rechenzentrum verlassen.

In der folgenden Abbildung müssen sowohl die dedizierte Verbindung als auch Ihre lokalen Ressourcen MACsec unterstützen. Datenverkehr auf Ebene 2, der über die dedizierte Verbindung zum oder vom Rechenzentrum übertragen wird, ist verschlüsselt.



MACsec-Konzepte

Die wichtigsten Komponenten für MACsec sind folgende:

- MAC Security (MACsec) – Ein IEEE-802.1-Standard der Layer 2, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. Weitere Informationen zum Protokoll finden Sie unter 802.1AE: MAC Security (MACsec).
- Geheimer MACSec-Schlüssel — Ein vorab gemeinsam genutzter Schlüssel, der die MACSec-Konnektivität zwischen dem lokalen Router des Kunden und dem Verbindungsport am Standort herstellt. AWS Direct Connect Der Schlüssel wird von den Geräten an den Enden der Verbindung

mithilfe des CKN/CAK-Paars generiert, das Sie für Ihr Gerät bereitstellen AWS und das Sie auch auf Ihrem Gerät bereitgestellt haben.

- Connection Key Name (CKN) und Connectivity Association Key (CAK)) – Die Werte in diesem Paar werden zum Generieren des geheimen MACsec-Schlüssels verwendet. Sie generieren die Paarwerte, ordnen sie einer AWS Direct Connect Verbindung zu und stellen sie am Ende der Verbindung auf Ihrem Edge-Gerät bereit. AWS Direct Connect

Unterstützte Verbindungen

MACsec ist auf dedizierten Verbindungen verfügbar. Informationen zum Bestellen von Verbindungen, die MACsec unterstützen, finden Sie unter AWS Direct Connect.

Erste Schritte mit MACsec auf dedizierten Verbindungen

Die folgenden Aufgaben helfen Ihnen, sich mit MACsec auf AWS Direct Connect dedizierten Verbindungen vertraut zu machen. Für die Nutzung von MACsec fallen keine zusätzlichen Gebühren an.

Beachten Sie Folgendes, bevor Sie MACsec für eine dedizierte Verbindung konfigurieren:

- MACsec wird auf dedizierten Direct-Connect-Verbindungen mit 10 Gbit/s und 100 Gbit/s an ausgewählten Points of Presence unterstützt. Für diese Verbindungen werden die folgenden MACsec-Cipher-Suites unterstützt:
  - Für 10Gbps-Verbindungen GCM-AES-256 und GCM-AES-XPN-256.
  - Für 100-Gbit/s-Verbindungen GCM-AES-XPN-256.
- Es werden nur 256-Bit-MACsec-Schlüssel unterstützt.
- Extended Packet Numbering (XPN) ist für 100Gbps-Verbindungen erforderlich. Für 10Gbps-Verbindungen unterstützt Direct Connect sowohl GCM-AES-256 als auch GCM-AES-XPN-256. Hochgeschwindigkeitsverbindungen, wie z. B. dedizierte Verbindungen mit 100 Gbit/s, können den ursprünglichen 32-Bit-Paketnummerierungsraum von MACsec schnell erschöpfen, sodass Sie Ihre Verschlüsselungsschlüssel alle paar Minuten rotieren müssten, um eine neue Connectivity Association einzurichten. Um diese Situation zu vermeiden, führte das IEEE Std 802.1AEbw -2013-Gleitkommazahl eine erweiterte Paketnummerierung ein, wodurch der Nummernraum auf 64 Bit erhöht wurde, wodurch die Rechtzeitigkeit für die Schlüsselrotation erleichtert wurde.

- Secure Channel Identifier (SCI) ist erforderlich und muss aktiviert sein. Diese Einstellung kann nicht angepasst werden.
- IEEE 802.1Q (Dot1q/VLAN) Tag offset/dot1 q-in-clear wird nicht unterstützt, um ein VLAN-Tag außerhalb einer verschlüsselten Nutzlast zu verschieben.

Weitere Informationen zu Direct Connect und MACsec finden Sie im Abschnitt MACsec der AWS Direct Connect FAQs .

Themen

MACsec-Voraussetzungen

Schließen Sie die folgenden Aufgaben ab, bevor Sie MACsec für eine dedizierte Verbindung konfigurieren.

- Erstellen Sie ein CKN/CAK-Paar für den geheimen MACsec-Schlüssel.

  Sie können das Paar mit einem offenen Standardtool erstellen. Das Paar muss die Anforderungen unter the section called “Schritt 4: On-Premises-Router konfigurieren” erfüllen.
- Es muss ein Gerät an Ihrem Ende der Verbindung vorhanden sein, das MACsec unterstützt.
- Secure Channel Identifier (SCI) muss aktiviert sein.
- Es werden nur 256-Bit-MACsec-Schlüssel unterstützt, die den neuesten erweiterten Datenschutz bieten.

Serviceverknüpfte Rollen

AWS Direct Connect verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen . Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit verknüpft ist AWS Direct Connect. Serviceverknüpfte Rollen werden von vordefiniert AWS Direct Connect und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert. Eine serviceverknüpfte Rolle AWS Direct Connect vereinfacht die Einrichtung von , da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Direct Connect definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, AWS Direct Connect kann nur die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden. Weitere Informationen finden Sie unter the section called “Serviceverknüpfte Rollen”.

Wichtige Überlegungen zu vorinstalliertem MACsec CKN/CAK

AWS Direct Connect verwendet AWS verwaltete CMKs für die vorinstallierten Schlüssel, die Sie Verbindungen oder LAGs zuordnen. Secrets Manager speichert Ihre vorab gemeinsam genutzten CKN- und CAK-Paare als Secret, das der Root-Schlüssel des Secrets Manager verschlüsselt. Weitere Informationen finden Sie unter AWS -verwaltete CMKs im AWS Key Management Service - Entwicklerhandbuch.

Der gespeicherte Schlüssel ist standardmäßig schreibgeschützt, aber Sie können eine Löschung nach sieben bis dreißig Tagen über die AWS Secrets-Manager-Konsole oder API planen.
Wenn Sie einen Löschvorgang planen, kann das CKN nicht gelesen werden, was sich auf Ihre Netzwerkkonnektivität auswirken kann. In diesem Fall wenden wir die folgenden Regeln an:

- Wenn sich die Verbindung im Status „Pending“ (Ausstehend) befindet, trennen wir den CKN von der Verbindung.
- Wenn sich die Verbindung im Status „Available“ (Verfügbar) befindet, benachrichtigen wir den Eigentümer der Verbindung per E-Mail. Wenn Sie innerhalb von 30 Tagen keine Maßnahmen ergreifen, trennen wir den CKN von Ihrer Verbindung.

Wenn wir den letzten CKN von Ihrer Verbindung trennen und der Verbindungsverschlüsselungsmodus auf „must encrypt“ (muss verschlüsseln) gesetzt ist, setzen wir den Modus auf „should_encrypt“, um einen plötzlichen Paketverlust zu verhindern.

Schritt 1: Erstellen einer Verbindung

Um mit der Verwendung von MACsec zu beginnen, müssen Sie ds Feature aktivieren, wenn Sie eine dedizierte Verbindung herstellen. Weitere Informationen finden Sie unter the section called “Eine Verbindung mit dem Verbindungsassistenten erstellen”.

(Optional) Schritt 2: Erstellen einer Link Aggregation Group (LAG)

Wenn Sie aus Redundanzgründen mehrere Verbindungen verwenden, können Sie eine LAG erstellen, die MACsec unterstützt. Weitere Informationen finden Sie unter the section called “Überlegungen zu MACsec” und the section called “Eine LAG erstellen”.

Schritt 3: Den CKN/CAK der Verbindung oder LAG zuordnen

Nachdem Sie die Verbindung oder LAG erstellt haben, die MACsec unterstützt, müssen Sie der Verbindung ein CKN/CAK zuordnen. Weitere Informationen finden Sie unter einem der folgenden Themen:

- the section called “Einer Verbindung ein MACsec CKN/CAK zuordnen”
- the section called “Ein MACsec CKN/CAK einer LAG zuordnen”

Schritt 4: On-Premises-Router konfigurieren

Aktualisieren Sie Ihren lokalen Router mit dem geheimen MACsec-Schlüssel. Der geheime MACsec-Schlüssel auf dem lokalen Router und am - AWS Direct Connect Standort muss übereinstimmen. Weitere Informationen finden Sie unter the section called “Routerkonfigurationsdatei herunterladen”.

Schritt 5: (Optional) Die Zuordnung zwischen dem CKN/CAK und der Verbindung oder LAG entfernen

Wenn Sie die Verknüpfung zwischen dem MACsec-Schlüssel und der Verbindung oder LAG entfernen möchten, beachten Sie Folgendes:

- the section called “Die Zuordnung zwischen einem geheimen MACsec-Schlüssel und einer Verbindung entfernen”
- the section called “Die Zuordnung zwischen allen MACsec-Schlüsseln und LAGs entfernen”

AWS Direct Connect Verbindungen

AWS Direct Connect ermöglicht es Ihnen, eine dedizierte Netzwerkverbindung zwischen Ihrem Netzwerk und einem der AWS Direct Connect Standorte herzustellen.

Es gibt zwei Arten von Verbindungen:

- Dedizierte Verbindung: eine physische Ethernet-Verbindung für einen einzelnen Kunden. Kunden können über die AWS Direct Connect Konsole, die CLI oder die API eine dedizierte Verbindung anfordern. Weitere Informationen finden Sie unter the section called “Dedizierte Verbindungen”.
- Gehostete Verbindung: Eine physische Ethernet-Verbindung, die ein AWS Direct Connect Partner im Namen eines Kunden bereitstellt. Kunden fordern eine gehostete Verbindung an, indem sie einen Partner im AWS Direct Connect -Partnerprogramm kontaktieren, der die Verbindung bereitstellt. Weitere Informationen finden Sie unter the section called “Gehostete Verbindungen”.

Dedizierte Verbindungen

Um eine dedizierte AWS Direct Connect -Verbindung herzustellen, benötigen Sie folgende Informationen:

AWS Direct Connect location

Arbeiten Sie mit einem Partner im AWS Direct Connect Partnerprogramm zusammen, der Sie beim Aufbau von Netzwerkverbindungen zwischen einem AWS Direct Connect Standort und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung unterstützt. Dieser Partner kann Ihnen auch dabei behilflich sein, einen Co-Location-Raum innerhalb der gleichen Einrichtung wie der Standort bereitzustellen. Weitere Informationen finden Sie unter APN-Partner, die AWS Direct Connect unterstützen.

Port speed (Port-Geschwindigkeit)

Die möglichen Werte sind 1 Gbit/s, 10 Gbit/s und 100 Gbit/s.

Sie können die Portgeschwindigkeit nach dem Erstellen der Verbindungsanforderung nicht ändern. Wenn die Port-Geschwindigkeit geändert werden soll, müssen Sie eine neue Verbindung erstellen und konfigurieren.

Sie können eine Verbindung entweder mit dem Verbindungsassistenten oder mit einer klassischen Verbindung herstellen. Mit dem Verbindungsassistenten können Sie Verbindungen anhand von Empfehlungen zur Ausfallsicherheit einrichten. Der Assistent wird empfohlen, wenn Sie Verbindungen zum ersten Mal einrichten. Wenn Sie möchten, können Sie Classic verwenden, um Verbindungen one-at-a-time herzustellen. Classic wird empfohlen, wenn Sie bereits über ein bestehendes Setup verfügen, zu dem Sie Verbindungen hinzufügen möchten. Sie können eine eigenständige Verbindung erstellen, oder Sie können eine Verbindung herstellen, um sie mit einer LAG in Ihrem Konto zu verknüpfen. Wenn Sie eine Verbindung mit einer LAG verknüpfen, wird sie mit der gleichen Port-Geschwindigkeit und demselben Standort erstellt, wie in der LAG angegeben.

Nachdem Sie die Verbindung angefordert haben, stellen wir Ihnen einen „Letter of Authorization and Connecting Facility Assignment“ (LOA-CFA) zum Download zur Verfügung oder senden Ihnen nach der Erstellung der Verbindungsanforderung eine E-Mail zu, in der Sie gebeten werden, weitere Informationen anzugeben. Wenn Sie diese Bitte um weitere Informationen nicht innerhalb von 7 Tagen beantworten, wird die Verbindung gelöscht. Die LOA-CFA ist die Autorisierung, mit der Sie eine Verbindung herstellen können AWS, und wird von Ihrem Netzwerkanbieter benötigt, um eine Cross-Connect-Verbindung für Sie zu bestellen. Wenn Sie vor AWS Direct Connect Ort keine Geräte haben, können Sie dort keine Cross-Connect-Verbindung für sich selbst bestellen.

Es sind folgende Operationen für dedizierte Verbindungen verfügbar:

- the section called “Eine Verbindung mit dem Verbindungsassistenten erstellen”
- the section called “Eine Classic-Verbindung erstellen”
- the section called “Ihre Verbindungsdetails anzeigen”
- the section called “Aktualisieren einer Verbindung”
- the section called “Einer Verbindung ein MACsec CKN/CAK zuordnen”
- the section called “Die Zuordnung zwischen einem geheimen MACsec-Schlüssel und einer Verbindung entfernen”
- the section called “Verbindungen löschen”

Sie können eine dedizierte Verbindung einer Link Aggregation Group (LAG) hinzufügen. Auf diese Weise können Sie mehrere Verbindungen wie eine einzige behandeln. Weitere Informationen finden Sie unter Eine Verbindung mit einer LAG verknüpfen.

Nachdem Sie eine Verbindung eingerichtet haben, erstellen Sie eine virtuelle Schnittstelle, um eine Verbindung mit öffentlichen und privaten AWS -Ressourcen herzustellen. Weitere Informationen finden Sie unter AWS Direct Connect virtuelle Schnittstellen.

Wenn Sie an einem AWS Direct Connect Standort keine Ausrüstung haben, wenden Sie sich zunächst an einen AWS Direct Connect Partner des AWS Direct Connect Partnerprogramms. Weitere Informationen finden Sie unter APN-Partner, die AWS Direct Connect unterstützen.

Wenn Sie eine Verbindung herstellen möchten, die MAC Security (MACsec) verwendet, überprüfen Sie vorher die Voraussetzungen. Weitere Informationen finden Sie unter the section called “MACsec-Voraussetzungen ”.

Eine Verbindung mit dem Verbindungsassistenten erstellen

In diesem Abschnitt wird das Erstellen einer Verbindung mithilfe des Verbindungsassistenten beschrieben. Wenn Sie es vorziehen, eine Classic-Verbindung herzustellen, finden Sie die zugehörigen Schritte unter the section called “Schritt 2: Fordern Sie eine AWS Direct Connect dedizierte Verbindung an”.

So erstellen Sie eine Verbindung mit dem Verbindungsassistenten

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections (Verbindungen) und dann Create connection (Verbindung erstellen) aus.
3. Wählen Sie auf der Seite Create connection (Verbindung erstellen) unter Connection ordering type (Art der Verbindungsreihenfolge) die Option Connection wizard (Verbindungsassistent) aus.
4. Wählen Sie eine Resilienzstufe für Ihre Netzwerkverbindungen. Die Resilienzstufe kann einer der folgenden sein:

   - Maximale Ausfallsicherheit
   - Hohe Ausfallsicherheit
   - Entwicklung und Test

   Beschreibungen und detailliertere Informationen zu diesen Resilienzstufen finden Sie unter Verwenden Sie das AWS Direct Connect Resiliency Toolkit für den Einstieg.
5. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Configure connections (Verbindungen konfigurieren) die folgenden Informationen an.

a. Wählen Sie aus der Dropdown-Liste Bandwidth (Bandbreite) die für die Verbindung erforderliche Bandbreite aus. Dies kann zwischen 1 Gbit/s und 100 Gbit/s liegen.

b. Wählen Sie für Standort den entsprechenden AWS Direct Connect Standort und dann den Ersten Standortdienstanbieter aus. Wählen Sie den Dienstanbieter aus, der die Konnektivität für die Verbindung an diesem Standort bereitstellt.

c. Wählen Sie für Zweiter Standort den entsprechenden AWS Direct Connect am zweiten Standort aus, und wählen Sie dann den Dienstanbieter für den zweiten Standort aus. Wählen Sie den Dienstanbieter aus, der die Konnektivität für die Verbindung an diesem zweiten Standort bereitstellt.

d. (Optional) Konfigurieren Sie MAC Security (MACsec) für die Verbindung. Wählen Sie unter Additional Settings (Zusätzliche Einstellungen) die Option Request a MACsec capable port (Einen MACsec-fähigen Port anfordern) aus.

   MACsec ist nur auf dedizierten Verbindungen verfügbar.

e. (Optional) Wählen Sie Add tag (Tag hinzufügen) aus, um Schlüssel/Wert-Paare hinzuzufügen, mit denen Sie diese Verbindung besser identifizieren können.

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   Um ein vorhandenes Tag zu entfernen, wählen Sie das Tag und dann Remove tag (Tag entfernen) aus. Sie können keine leeren Tags haben.

7. Wählen Sie Weiter aus.
8. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die Verbindung. Auf dieser Seite werden auch die geschätzten Kosten für die Portnutzung und zusätzliche Datenübertragungsgebühren angezeigt.
9. Wählen Sie Erstellen.
10. Laden Sie Ihr LOA-CFA (Letter of Authorization and Connecting Facility Assignment) herunter. Weitere Informationen finden Sie unter the section called “Das LOA-CFA-Dokument herunterladen”.

Verwenden Sie einen der folgenden Befehle.

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

Eine Classic-Verbindung erstellen

Für dedizierte Verbindungen können Sie über die AWS Direct Connect Konsole eine Verbindungsanfrage stellen. Bei gehosteten Verbindungen wenden Sie sich an einen AWS Direct Connect Partner, um eine gehostete Verbindung anzufordern. Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen:

- Die Portgeschwindigkeit, die Sie benötigen. Bei dedizierten Verbindungen können Sie die Portgeschwindigkeit nach dem Erstellen der Verbindungsanforderung nicht ändern. Bei gehosteten Verbindungen kann Ihr AWS Direct Connect -Partner die Geschwindigkeit ändern.
- Der AWS Direct Connect Ort, an dem die Verbindung beendet werden soll.

> **Note**
>
> Sie können die AWS Direct Connect Konsole nicht verwenden, um eine gehostete Verbindung anzufordern. Wenden Sie sich stattdessen an einen AWS Direct Connect Partner, der eine gehostete Verbindung für Sie herstellen kann, die Sie dann akzeptieren. Überspringen Sie die folgenden Schritte und gehen Sie zu Akzeptieren Ihrer gehosteten Verbindung.

Um eine neue AWS Direct Connect Verbindung herzustellen

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie auf dem AWS Direct Connect-Bildschirm unter Get started (Erste Schritte) die Option Create a connection (Verbindung erstellen) aus.
3. Wählen Sie Classicaus.
4. Geben Sie unter Name einen Namen für die Verbindung ein.
5. Wählen Sie unter Location (Standort) den entsprechenden AWS Direct Connect -Standort aus.
6. Wählen Sie ggf. für Sub Location (Unterstandort) das Stockwerk aus, das Ihnen oder dem Netzanbieter am nächsten ist. Diese Option ist nur verfügbar, wenn der Standort über Meet-Me-Räume (MMRs) auf mehreren Stockwerken des Gebäudes verfügt.
7. Wählen Sie für Port Speed (Portgeschwindigkeit) die Verbindungsbandbreite aus.

8. Wählen Sie für On-premises (Lokal) die Option Connect through an AWS Direct Connect partner (Über einen -Partner verbinden) aus, wenn Sie über diese Verbindung eine Verbindung mit Ihrem Rechenzentrum herstellen.
9. Wählen Sie als Dienstanbieter den AWS Direct Connect Partner aus. Wenn Sie einen Partner verwenden, der nicht in der Liste enthalten ist, wählen Sie Other (Anderer) aus.
10. Wenn Sie Other (Anderer) für Service provider (Serviceanbieter) ausgewählt haben, geben Sie unter Name of other provider (Name des anderen Anbieters) den Namen des Partners ein, den Sie verwenden.
11. (Optional) Wählen Sie Add tag (Tag hinzufügen) aus, um Schlüssel/Wert-Paare hinzuzufügen, mit denen Sie diese Verbindung besser identifizieren können.

    - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
    - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

    Um ein vorhandenes Tag zu entfernen, wählen Sie das Tag und dann Remove tag (Tag entfernen) aus. Sie können keine leeren Tags haben.
12. Wählen Sie Create Connection (Verbindung erstellen) aus.

Es kann bis zu 72 Stunden dauern AWS , bis Ihre Anfrage geprüft und ein Port für Ihre Verbindung bereitgestellt ist. Während dieser Zeit erhalten Sie möglicherweise eine E-Mail-Nachricht mit der Bitte um weitere Informationen über Ihren Anwendungsfall oder den angegebenen Standort. Die E-Mail wird an die E-Mail-Adresse gesendet, die Sie bei der Registrierung verwendet haben AWS. Sie müssen innerhalb von 7 Tagen antworten, andernfalls wird die Verbindung gelöscht.

Weitere Informationen finden Sie unter AWS Direct Connect Verbindungen.

Das LOA-CFA-Dokument herunterladen

Nachdem wir Ihre Verbindungsanforderung verarbeitet haben, können Sie das LOA-CFA-Dokument herunterladen. Wenn der Link nicht aktiviert ist, steht das LOA-CFA-Dokument noch nicht zum Download bereit. Überprüfen Sie, ob sich in Ihrem E-Mail-Posteingang eine Anfrage nach weiteren Informationen befindet.

Die Abrechnung beginnt automatisch, wenn der Port aktiv ist oder 90 Tage nach Ausstellung der LOA, je nachdem, was zuerst eintritt. Sie können Abrechnungsgebühren vermeiden, indem Sie den Port vor der Aktivierung oder innerhalb von 90 Tagen nach Ausstellung der LOA löschen.

Wenn Ihre Verbindung nach 90 Tagen nicht verfügbar ist und der LOA-CFA noch nicht ausgestellt wurde, senden wir Ihnen eine E-Mail, in der Sie darüber informiert werden, dass der Port innerhalb von 10 Tagen gelöscht wird. Wenn Sie den Port nicht innerhalb der zusätzlichen 10 Tage aktivieren, wird der Port automatisch gelöscht und Sie müssen den Porterstellungsprozess erneut starten.

> **Note**
>
> Weitere Informationen über die Preise finden Sie unter AWS Direct Connect – Preise. Wenn Sie die Verbindung nicht mehr benötigen, nachdem Sie das LOA-CFA neu ausgestellt haben, müssen Sie die Verbindung selbst löschen. Weitere Informationen finden Sie unter Verbindungen löschen.

Console

So laden Sie das LOA-CFA-Dokument herunter

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die Verbindung und View details (Details ansehen) aus.
4. Wählen Sie Download LOA-CFA aus.

   > **Note**
   >
   > Wenn der Link nicht aktiviert ist, steht das LOA-CFA-Dokument noch nicht zum Download bereit. Es wird ein Support-Fall erstellt, in dem zusätzliche Informationen angefordert werden. Sobald Sie auf die Anfrage geantwortet und die Anfrage bearbeitet haben, steht das LOA-CFA zum Herunterladen zur Verfügung. Wenn es immer noch nicht verfügbar sein sollte, wenden Sie sich an den AWS Support.

5. Schicken Sie die LOA-CFA an Ihren Netzbetreiber oder Co-Location-Anbieter, damit sie eine Querverbindung für Sie bestellen können. Das Kontaktverfahren kann bei jedem Co-Location-Anbieter variieren. Weitere Informationen finden Sie unter Anfordern von Querverbindungen an - AWS Direct Connect Standorten.

Command line

So laden Sie das LOA-CFA über die Befehlszeile oder API herunter

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

Aktualisieren einer Verbindung

Sie können die folgenden Verbindungsattribute aktualisieren:

- Der Name der Verbindung.
- Den MACsec-Verschlüsselungsmodus der Verbindung.

> **Note**
> MACsec ist nur auf dedizierten Verbindungen verfügbar.

Die gültigen Werte sind:

- `should_encrypt`
- `must_encrypt`

  Wenn Sie den Verschlüsselungsmodus auf diesen Wert einstellen, wird die Verbindung unterbrochen, wenn die Verschlüsselung unterbrochen ist.
- `no_encrypt`

Console

So aktualisieren Sie eine Verbindung

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die Verbindung und anschließend Edit (Bearbeiten) aus.
4. Modifizieren der Verbindung:

[Namen ändern] Geben Sie unter Name einen neuen Verbindungsnamen ein.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

5. Wählen Sie Edit connection (Verbindung bearbeiten) aus.

Command line

So fügen Sie Tags über die Befehlszeile hinzu und entfernen sie

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

So aktualisieren Sie eine Verbindung über die Befehlszeile oder API

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

Einer Verbindung ein MACsec CKN/CAK zuordnen

Nachdem Sie die Verbindung hergestellt haben, die MACsec unterstützt, können Sie der Verbindung ein CKN/CAK zuordnen.

> **Note**
>
> Sie können einen geheimen MACsec-Schlüssel nicht ändern, nachdem Sie ihn einer Verbindung zugeordnet haben. Wenn Sie den Schlüssel ändern müssen, trennen Sie den Schlüssel von der Verbindung und ordnen Sie der Verbindung dann einen neuen Schlüssel zu. Informationen zum Entfernen einer Zuordnung finden Sie unter the section called “Die Zuordnung zwischen einem geheimen MACsec-Schlüssel und einer Verbindung entfernen”.

Console

So ordnen Sie einen MACsec-Schlüssel einer Verbindung zu

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Bereich Connections (Verbindungen) aus.
3. Wählen Sie eine Verbindung und View details (Details ansehen) aus.
4. Wählen Sie Associate key (Schlüssel zuordnen) aus.
5. Geben Sie den MACsec-Schlüssel ein.

   [Das CAK/CKN-Paar verwenden] Wählen Sie Key Pair (Schlüsselpaar) aus und gehen Sie dann wie folgt vor:

   - Geben Sie für Connectivity Association Key (CAK) den CAK ein.
   - Geben Sie für Connectivity Association Key Name (CKN) den CKN ein.

   [Den geheimen Schlüssel verwenden] Wählen Sie Existing Secret Manager Secret (Vorhandenes Secret-Manager-Secret) dann für Secret den geheimen MACsec-Schlüssel aus.
6. Wählen Sie Associate key (Schlüssel zuordnen) aus.

Command line

So ordnen Sie einen MACsec-Schlüssel einer Verbindung zu

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

Die Zuordnung zwischen einem geheimen MACsec-Schlüssel und einer Verbindung entfernen

Sie können die Zuordnung zwischen der Verbindung und dem MACsec-Schlüssel entfernen.

Console

So entfernen Sie eine Zuordnung zwischen einer Verbindung und einem MACsec-Schlüssel

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2.
3. Wählen Sie im linken Bereich Connections (Verbindungen) aus.
4. Wählen Sie eine Verbindung und View details (Details ansehen) aus.
5. Wählen Sie das zu entfernende MACsec-Secret aus, und klicken Sie dann auf Disassociate key (Schlüssel trennen).
6. Geben Sie im Bestätigungsdialogfeld disassociate (Trennen) ein und wählen Sie dann Disassociate (Trennen) aus.

Command line

So entfernen Sie eine Zuordnung zwischen einer Verbindung und einem MACsec-Schlüssel

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

Gehostete Verbindungen

Um eine AWS Direct Connect gehostete Verbindung herzustellen, benötigen Sie die folgenden Informationen:

AWS Direct Connect location

Arbeiten Sie mit einem AWS Direct Connect Partner im AWS Direct Connect Partnerprogramm zusammen, der Sie beim Aufbau von Netzwerkverbindungen zwischen einem AWS Direct Connect Standort und Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung unterstützt. Dieser Partner kann Ihnen auch dabei behilflich sein, einen Co-Location-Raum innerhalb der gleichen Einrichtung wie der Standort bereitzustellen. Weitere Informationen finden Sie unter AWS Direct Connect -Lieferpartner.

> **Note**
>
> Sie können keine gehostete Verbindung über die AWS Direct Connect Konsole anfordern. Ein AWS Direct Connect Partner kann jedoch eine gehostete Verbindung für Sie erstellen und konfigurieren. Nachdem die Verbindung konfiguriert ist, erscheint sie im Bereich Connections (Verbindungen) in der Konsole.
> Sie müssen die gehostete Verbindung akzeptieren, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter the section called “Eine gehostete Verbindung akzeptieren”.

Port speed (Port-Geschwindigkeit)

Für gehostete Verbindungen sind die möglichen Werte 50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 300 Mbit/s, 400 Mbit/s, 500 Mbit/s, 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s und 25 Gbit/s. Beachten Sie, dass nur AWS Direct Connect Partner, die bestimmte Anforderungen erfüllen, eine gehostete Verbindung mit 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s oder 25 Gbit/s einrichten dürfen. 25-Gbit/s-Verbindungen sind nur an Direct Connect-Standorten verfügbar, an denen Portgeschwindigkeiten von 100 Gbit/s verfügbar sind.

Beachten Sie Folgendes:

- Die Verbindungsgeschwindigkeiten können nur von Ihrem AWS Direct Connect Partner geändert werden. Sie müssen eine Verbindung nicht mehr löschen und dann neu erstellen, um die Bandbreite einer vorhandenen gehosteten Verbindung zu erhöhen oder herabzusetzen. Um Ihre Portgeschwindigkeit zu ändern, wenden Sie sich bitte an den AWS Direct Connect Partner, der Ihre gehostete Verbindung verwaltet.
- AWS verwendet Traffic Policing für gehostete Verbindungen, d. h., wenn die Datenverkehrsrate die konfigurierte Höchstrate erreicht, wird überschüssiger Verkehr gelöscht. Dies kann dazu führen, dass der Datenverkehr einen geringeren Durchsatz hat als nicht stoßweiser Datenverkehr.
- Jumbo-Frames können nur dann an Verbindungen aktiviert werden, wenn sie ursprünglich für die gehostete übergeordnete AWS Direct Connect -Verbindung aktiviert waren. Wenn Jumbo-Frames auf dieser übergeordneten Verbindung nicht aktiviert sind, können sie auf keiner Verbindung aktiviert werden.

Die folgenden Konsolenoperationen sind verfügbar, nachdem Sie eine gehostete Verbindung angefordert und akzeptiert haben:

- the section called “Ihre Verbindungsdetails anzeigen”
- the section called “Aktualisieren einer Verbindung”
- the section called “Verbindungen löschen”

Nachdem Sie eine Verbindung akzeptiert haben, erstellen Sie eine virtuelle Schnittstelle, um eine Verbindung mit öffentlichen und privaten AWS -Ressourcen herzustellen. Weitere Informationen finden Sie unter AWS Direct Connect virtuelle Schnittstellen.

Eine gehostete Verbindung akzeptieren

Wenn Sie am Kauf einer gehosteten Verbindung interessiert sind, müssen Sie sich an einen AWS Direct Connect Partner des AWS Direct Connect Partnerprogramms wenden. Der Partner stellt die Verbindung für Sie bereit. Nachdem die Verbindung konfiguriert ist, erscheint sie im Bereich Connections (Verbindungen) in der AWS Direct Connect -Konsole.

Bevor Sie eine gehostete Verbindung verwenden können, müssen Sie die Verbindung akzeptieren.

Console

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die gehostete Verbindung und View details (Details ansehen) aus.
4. Aktivieren Sie das Bestätigungs-Kontrollkästchen und wählen Sie Accept (Akzeptieren) aus.

Command line

So akzeptieren Sie eine gehostete Verbindung mit der Befehlszeile oder API

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

Ihre Verbindungsdetails anzeigen

Sie können den aktuellen Status Ihrer Verbindung ansehen. Sie können auch die Verbindungs-ID (z. B. `dxcon-12nikabc`) anzeigen und sicherstellen, dass sie mit der Verbindungs-ID auf dem LOA-CFA übereinstimmt, das Sie empfangen oder heruntergeladen haben.

Hinweise zur Überwachung von Verbindungen finden Sie unter Überwachen.

Console

So zeigen Sie Informationen über eine Verbindung an

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Bereich Connections (Verbindungen) aus.
3. Wählen Sie eine Verbindung und View details (Details ansehen) aus.

Command line

So beschreiben Sie eine Verbindung mit der Befehlszeile oder API

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

Verbindungen löschen

Sie können eine Verbindung löschen, solange keine virtuellen Schnittstellen damit verknüpft sind. Wenn Sie Ihre Verbindung löschen, werden alle Port-Stunden-Gebühren für diese Verbindung gelöscht, es können jedoch weiterhin Cross-Connect- oder Netzwerkverbindungsgebühren anfallen (siehe unten). AWS Direct Connect Datenübertragungsgebühren fallen im Zusammenhang mit virtuellen Schnittstellen an. Weitere Informationen zum Löschen einer virtuellen Schnittstelle finden Sie unter Virtuelle Schnittstellen entfernen.

Laden Sie vor dem Löschen einer Verbindung die LOA für die Verbindung herunter, die die kontoübergreifenden Informationen enthält, sodass Sie über die relevanten Informationen zu den Verbindungen verfügen, die unterbrochen werden. Die Schritte zum Herunterladen des Verbindungs-LOA finden Sie unter the section called “Das LOA-CFA-Dokument herunterladen”.

Wenn Sie eine Verbindung löschen, AWS wird der Colocation-Anbieter angewiesen, Ihr Netzwerkgerät vom Direct Connect-Router zu trennen, indem Sie das Glasfaser-Querverbindungskabel vom entsprechenden Patchpanel entfernen. AWS Ihr Colocation- oder Circuit-Anbieter kann Ihnen jedoch weiterhin Cross-Connect- oder Netzwerkverbindungsgebühren berechnen, da das Cross-Connect-Kabel möglicherweise immer noch mit Ihrem Netzwerkgerät verbunden ist. Diese Gebühren für den Cross-Connect sind unabhängig von Direct Connect und müssen mit dem Colocation- oder Circuit-Anbieter unter Verwendung der Informationen der LOA storniert werden.

Verbindungen, die Teil einer Link Aggregation Group (LAG) sind, können nicht gelöscht werden, wenn die LAG dadurch die minimale Anzahl der operativen Verbindungen unterschreiten würde.

Console

So löschen Sie eine Verbindung

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie die Verbindungen aus und klicken Sie auf Delete (Löschen).
4. Wählen Sie im Bestätigungsdialogfeld Delete (Löschen) die Option Delete (Löschen) aus.

Command line

So löschen Sie eine Verbindung über die Befehlszeile oder API

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

Anfordern von Querverbindungen an - AWS Direct Connect Standorten

Nachdem Sie Ihr "Letter of Authorization and Connecting Facility Assignment (LOA-CFA)"-Dokument heruntergeladen haben, müssen Sie die Cross-Netzwerkverbindung, auch bekannt als Querverbindung, herstellen. Wenn Sie bereits über Ausrüstung an einem - AWS Direct Connect Standort verfügen, wenden Sie sich an den entsprechenden Anbieter, um die Querverbindung abzuschließen. Spezifische Anweisungen für die einzelnen Anbieter finden Sie in der folgenden Tabelle. Wenden Sie sich an Ihren Anbieter für die Preise der Querverbindung. Nachdem die Querverbindung hergestellt wurde, können Sie die virtuellen Schnittstellen mithilfe der AWS Direct Connect -Konsole erstellen.

Einige Speicherorte werden als Campus eingerichtet. Weitere Informationen, einschließlich zu den an den einzelnen Standorten verfügbaren Geschwindigkeiten, finden Sie unter AWS Direct Connect - Standorte.

Wenn Sie noch keine Ausrüstung an einem - AWS Direct Connect Standort haben, können Sie mit einem der Partner im - AWS Partnernetzwerk (APN) zusammenarbeiten. Diese Geräte helfen Ihnen beim Herstellen einer Verbindung mit einem AWS Direct Connect -Standort. Weitere Informationen finden Sie unter APN-Partner, die unterstützen AWS Direct Connect. Sie müssen das LOA-CFA-Dokument mit dem von Ihnen gewählten Anbieter teilen, um Ihre Querverbindungsanfrage zu vereinfachen.

Eine - AWS Direct Connect Verbindung kann Zugriff auf Ressourcen in anderen Regionen gewähren. Weitere Informationen finden Sie unter Remote-Zugriff auf eine AWS-Region.

> **Note**
>
> Wenn die Querverbindung nicht innerhalb von 90 Tagen abgeschlossen ist, erlischt die vom LOA-CFA erteilte Befugnis. Um ein LOA-CFA zu erneuern, das abgelaufen ist, können Sie es wieder von der AWS Direct Connect -Konsole herunterladen. Weitere Informationen finden Sie unter Das LOA-CFA-Dokument herunterladen.

Co-Locations

- USA Ost (Ohio)
- USA Ost (Nord-Virginia)

- USA West (Nordkalifornien)
- USA West (Oregon)
- Afrika (Kapstadt)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Kanada (Zentral)
- China (Peking)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Irland)
- Europa (Milan)
- Europa (London)
- Europa (Paris)
- Europa (Stockholm)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (USA-Ost)
- AWS GovCloud (USA-West)

USA Ost (Ohio)

Ort	Anfordern einer Verbindung
Cologix COL2, Columbus	Wenden Sie sich an Cologix unter sales@cologix.com.

Ort	Anfordern einer Verbindung
Cologix MIN3, Minneapolis	Wenden Sie sich an Cologix unter sales@cologix.com.
CyrusOne West III, Puerto	Übermitteln Sie über das Customer Portal eine Anfrage.
Equinix CH2, Chicago	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
S, Chicago	Kontaktieren Sie QTS unter AConnect@qtsdatacenters.com.
Netrality Data Centers, 1102 Grand, Kansas City	Kontaktieren Sie Netrality Data Centers unter support@netrality.com.

USA Ost (Nord-Virginia)

Ort	Anfordern einer Verbindung
165 Halsey Street, Newark	Wenden Sie sich an operations@165halsey.com.
CoreSite 32 000, New York	Bestellen Sie über das CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite VA1-VA2, Reston	Bestellen Sie im CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
Digitale Realty ATL1 &ATL2, Bol	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
Digitale Realty IAD38, Ashburn	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
Eaffinix DC1-DC6 und DC10-D12, Ashburn	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Eaffinix DAA1-DC3 und DC6, Dallas	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Ort	Anfordern einer Verbindung
Equinix MI1, Miami	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Echinix NY5, Seeaukus	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
KIO Networks QRO1, Queretaro, MX	Wenden Sie sich an KIO Networks ".
Markley, One Summer Street, Boston	Erstellen Sie für aktuelle Kunden eine -Anfrage über das Kundenportal . Für neue Anfragen kontaktieren Sie sales@markleygroup.com.
Netrality-Rechenzentren, MMR auf der 2. Ebene, Bol	Kontaktieren Sie Netrality Data Centers unter support@netrality.com.
S ATL1,	Kontaktieren Sie QTS unter AConnect@qtsdatacenters.com.

USA West (Nordkalifornien)

Ort	Anfordern einer Verbindung
CoreSite, LA1, Los Angeles	Bestellen Sie über das CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite SV2, Mailpitas	Bestellen Sie über das CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite SV4, Clara	Bestellen Sie über das CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Reihenfolge auf Genauigkeit und genehmigen Sie es dann auf der MyCoreSite Website.
EdgeConneX, Phoenix	Geben Sie über das EdgeOS Customer Portal eine Bestellung auf. Nachdem Sie das Formular eingereicht haben, stellt EdgeConneX ein Service-Auftragsformular zur Genehmigung

Ort	Anfordern einer Verbindung
	bereit. Sie können Fragen an cloudaccess@edgeconnex.com senden.
Equinix LA3, El Segundo	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
E Bolix SV1 und SV5, San Bol	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Kontaktieren Sie phoenixNAP Provisioning unter provisioning@phoenixnap.com.

USA West (Oregon)

Ort	Anfordern einer Verbindung
CoreSite DE1, Denver	Bestellen Sie über das CoreSite Kundenportal . Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
Digital Realty SEA10, Westin Building, Phoenix	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Geben Sie über das EdgeOS Customer Portal eine Bestellung auf. Nachdem Sie das Formular eingereicht haben, stellt EdgeConneX ein Service-Auftragsformular zur Genehmigung bereit. Sie können Fragen an cloudaccess@edgeconnex.com senden.
Equinix SE2, Seattle	Kontaktieren Sie Equinix unter support@equinix.com.
Pittock Block, Portland	Richten Sie Anfragen per E-Mail an crossconnect@pittock.com oder per Telefon an+1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Kontaktieren Sie Switch SUPERNAP unter orders@supernap.com.
TierPoint Singapur	Wenden Sie sich TierPoint an sales@tierpoint.com.

Afrika (Kapstadt)

Ort	Anfordern einer Verbindung
Internetknoten Kapstadt/ Teraco-Rechenzentren	Kontaktieren Sie Teraco unter support@teraco.co.za (für bestehende Teraco-Kunden) oder connect@teraco.co.za (für neue Kunden).
Teraco JB1, Johannesburg, Südafrika	Kontaktieren Sie Teraco unter support@teraco.co.za (für bestehende Teraco-Kunden) oder connect@teraco.co.za (für neue Kunden).

Asien-Pazifik (Jakarta)

Ort	Anfordern einer Verbindung
DCI JK3, Jakarta	Kontaktieren Sie DCI Indonesia unter jessie.w@dci-indonesia.com.com.
NTT 2 Data Center, Jakarta	Kontaktieren Sie NTT unter tps.cms.presales@global.ntt.

Asien-Pazifik (Mumbai)

Ort	Anfordern einer Verbindung
Equinix, Mumbai	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Wenden Sie sich an den gebührenfreien - NetMagic Vertrieb und das Marketing unter 18001033130 oder unter marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Kontaktieren Sie Sify unter aws.directconnect@sifycorp.com .
STT-Delhi DC2, Delhi	Wenden Sie sich an STT unter enquiry.AWSDX@sttelemediagdc.in .

Ort	Anfordern einer Verbindung
STT GDC Pvt. Ltd. VSB, Chennai	Wenden Sie sich an STT unter enquiry.AWSDX@sttelemediagdc.in .
STT Hyderabad DC1, Hyderabad	Wenden Sie sich an STT unter enquiry.AWSDX@sttelemediagdc.in .

Asien-Pazifik (Seoul)

Ort	Anfordern einer Verbindung
Digitale Realty ICN1, Seoul	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
KINX Gasan Data Center, Seoul	Kontaktieren Sie KINX unter sales@kinx.net.
LG U+ Pyeong-Chon Mega Center, Seoul	Senden Sie das LOA-Dokument an kidcadmin@lguplus.co.kr und center8@kidc.net.

Asien-Pazifik (Singapur)

Ort	Anfordern einer Verbindung
Equinix HK1, Tsuen Wan N.T., Hong Kong SAR	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix SG2, Singapur	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Global Switch, Singapur	Kontaktieren Sie Global Switch unter salessingapore@globalswitch.com.
GPX, Mumbai	Kontaktieren Sie GPX (Equinix) unter awsdealreg@equinix.com.

Ort	Anfordern einer Verbindung
iAdvantage Mega-i, Hongkong	Kontaktieren Sie iAdvantage unter cs@iadvantage.net oder geben Sie eine Bestellung über iAdvantage Cabling Order e-Form auf.
Menara AIMS, Kuala Lumpur	AIMS-Bestandskunden können eine X-Connect-Bestellung über das Kundendienstportal anfordern, indem sie ein Formular zur Anforderung eines Technik-Arbeitsauftrags ausfüllen. Sie können eine E-Mail an service.delivery@aims.com.my senden, falls beim Einreichen der Anforderung Probleme auftreten.
TCC Data Center, Bangkok	Kontaktieren Sie TCC Technology Co., Ltd unter gateway.ne@tcc-technology.com.

Asien-Pazifik (Sydney)

Ort	Anfordern einer Verbindung
CDC Bole 2, Canberra	Melden Sie sich beim Kundenportal unter CDC-Kundenportal an.
Datacom DH6, Auckland	Wenden Sie sich an Datacom unter Datacom Orbit – Auckland .
Erigix ME2, Bol	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix SY3, Sydney	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Global Switch, Sydney	Kontaktieren Sie Global Switch unter salessydney@globalswitch.com.
NEXTDC C1, Canberra	Kontaktieren Sie NEXTDC unter nxtops@nextdc.com.
NEXTDC M1, Melbourne	Kontaktieren Sie NEXTDC unter nxtops@nextdc.com.
NEXTDC P1, Perth	Kontaktieren Sie NEXTDC unter nxtops@nextdc.com.
NEXTDC S2, Sydney	Kontaktieren Sie NEXTDC unter nxtops@nextdc.com.

Asien-Pazifik (Tokio)

Ort	Anfordern einer Verbindung
AT Tokyo Chuo Rechenzentrum, Tokyo	Kontaktieren Sie AT TOKYO unter at-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Kontaktieren Sie Chief Telecom unter vicky_chan@chief.com.tw.
Chungwa Telecom, Taipei	Kontaktieren Sie CHT Taipei IDC NOC unter taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix TY2, Tokio	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
NEC Inzai, Inzai	Kontaktieren Sie NEC Inzai unter connection_support@ices.jp.nec.com.

Kanada (Zentral)

Ort	Anfordern einer Verbindung
Allied 250 Front St W, Toronto	Kontaktieren Sie driches@alliedreit.com.
Cologix MTL3, Montreal	Wenden Sie sich an Cologix unter sales@cologix.com.
Cologix VAN2, Vancouver	Wenden Sie sich an Cologix unter sales@cologix.com.
eStruxture, Montreal	Kontaktieren Sie eStruxture unter directconnect@estruxture.com.

China (Peking)

Ort	Anfordern einer Verbindung
CIDS Jiachuang IDC, Peking	Kontaktieren Sie dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao IDC, Peking	Kontaktieren Sie dx-order@sinnet.com.cn.
Rechenzentrum GDS Nr. 3, Shanghai	Kontaktieren Sie dx@nwcdcloud.cn.
Rechenzentrum GDS Nr. 3, Shenzhen	Kontaktieren Sie dx@nwcdcloud.cn.

China (Ningxia)

Ort	Anfordern einer Verbindung
Industrial Park IDC, Ningxia	Kontaktieren Sie dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Kontaktieren Sie dx@nwcdcloud.cn.

Europa (Frankfurt)

Ort	Anfordern einer Verbindung
CE Colo, Prag, Tschechien	Kontaktieren Sie CE Colo unter info@cecolo.com.
DigiPlex ven,, Norwegen	Wenden Sie sich DigiPlex an helpme@digiplex.com.
Equinix AM3, Amsterdam, Niederlande	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix FR5, Frankfurt	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Ort	Anfordern einer Verbindung
Equinix HE6, Helsinki	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix MU1, München	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix WA1, Warschau	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Interxion AMS7, Amsterdam	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion CPH2, Kopenhagen	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion FRA6, Frankfurt	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion MAD2, Madrid	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion VIE2, Wien	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion ZUR1, Zürich	Kontaktieren Sie Interxion unter customer.services@interxion.com.
IPB, Berlin	Kontaktieren Sie IPB unter kontakt@ipb.de.
Equinix ITConic MD2, Madrid	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Europa (Irland)

Ort	Anfordern einer Verbindung
Digital Realty (UK), Docklands	Kontaktieren Sie Digital Realty (UK) unter amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Kontaktieren Sie Eircom unter awsorders@eircom.ie.

Ort	Anfordern einer Verbindung
Equinix DX1, Dubai	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix LD5, London (Slough)	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Interxion DUB2, Dublin	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion MRS1, Marseille	Kontaktieren Sie Interxion unter customer.services@interxion.com.

Europa (Milan)

Ort	Anfordern einer Verbindung
CDLAN srl Via Caldera 21, Milano	Wenden Sie sich an CDLAN per E-Mail an sales@cdlan.it.
Equinix, ML2, Mailand, Italien	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Europa (London)

Ort	Anfordern einer Verbindung
Digital Realty (UK), Docklands	Kontaktieren Sie Digital Realty (UK) unter amazon.orders@digitalrealty.com.
Equinix LD5, London (Slough)	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix MA3, Manchester	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Telehouse West, London	Kontaktieren Sie Telehouse UK unter sales.support@uk.telehouse.net.

Europa (Paris)

Ort	Anfordern einer Verbindung
Equinix PA3, Paris	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Interxion PAR7, Paris	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Telehouse Voltaire, Paris	Wenden Sie sich auf der Seite Kontaktieren Sie uns an Telehouse Paris Bol.

Europa (Stockholm)

Ort	Anfordern einer Verbindung
Interxion STO1, Stockholm	Kontaktieren Sie Interxion unter customer.services@interxion.com.

Europa (Zürich)

Ort	Anfordern einer Verbindung
Equinix ZRH51, Oberengstringen, Schweiz	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Israel (Tel Aviv)

Ort	Anfordern einer Verbindung
MedOne, Haifa	Kontaktieren Sie MedOne unter support@Medone.co.il
EdgeConnex, Bolliya	Kontaktieren Sie EdgeConnect unter info@edgeconnecx.com

Naher Osten (Bahrain)

Ort	Anfordern einer Verbindung
AWS Bahrain DC53, Manama	Um die Verbindung herzustellen, können Sie mit einem unserer Netzwerkanbieter-Partner vor Ort bei der Einrichtung der Konnektivität zusammenarbeiten. Anschließend stellen Sie ein Letter of Authorization (LOA) vom Netzwerkanbieter an AWS über das AWS Support Center bereit. AWS schließt die Querverbindung an diesem Standort ab.
AWS Bahrain DC52, Manama	Um die Verbindung herzustellen, können Sie mit einem unserer Netzwerkanbieter-Partner vor Ort bei der Einrichtung der Konnektivität zusammenarbeiten. Anschließend stellen Sie ein Letter of Authorization (LOA) vom Netzwerkanbieter an AWS über das AWS Support Center bereit. AWS schließt die Querverbindung an diesem Standort ab.

Naher Osten (VAE)

Ort	Anfordern einer Verbindung
Equinix DX1, Dubai, VAE	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Etisalat SmartHub Data Centre, Fujatsch, VAE	Wenden Sie sich an das Etisalat SmartHub Data Centre unter IntlSales-C&WS@etisalat.ae.

Südamerika (São Paulo)

Ort	Anfordern einer Verbindung
Equinix RJ2, Rio de Janeiro	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix SP4, São Paulo	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Ort	Anfordern einer Verbindung
Tivit	Kontaktieren Sie Tivit unter aws@tivit.com.br.

AWS GovCloud (USA-Ost)

Sie können in dieser Region keine Verbindungen anfordern.

AWS GovCloud (USA-West)

Ort	Anfordern einer Verbindung
Equinix SV5, San Jose	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

AWS Direct Connect virtuelle Schnittstellen

Sie müssen eine der folgenden virtuellen Schnittstellen (VIFs) erstellen, um Ihre AWS Direct Connect Verbindung nutzen zu können.

- Private virtuelle Schnittstelle: Eine private virtuelle Schnittstelle sollte für den Zugriff auf eine Amazon VPC über private IP-Adressen verwendet werden.
- Öffentliche virtuelle Schnittstelle: Eine öffentliche virtuelle Schnittstelle kann über AWS öffentliche IP-Adressen auf alle öffentlichen Dienste zugreifen.
- Virtuelle Transit-Schnittstelle: Eine virtuelle Transit-Schnittstelle sollte für den Zugriff auf ein oder mehrere Transit Gateways von Amazon VPC verwendet werden, die Direct-Connect-Gateways zugeordnet sind. Sie können virtuelle Transitschnittstellen mit jeder AWS Direct Connect dedizierten oder gehosteten Verbindung beliebiger Geschwindigkeit verwenden. Hinweise zu Direct Connect-Gatewaykonfigurationen finden Sie unter the section called “Direct Connect-Gateways”.

Um mithilfe von IPv6-Adressen eine Verbindung zu anderen AWS Diensten herzustellen, überprüfen Sie in der Servicedokumentation, ob die IPv6-Adressierung unterstützt wird.

Werberegeln für das Public Virtual Interface-Präfix

Wir machen Ihnen entsprechende Amazon-Präfixe bekannt, damit Sie entweder Ihre VPCs oder andere AWS Dienste erreichen können. Sie können über diese Verbindung auf alle AWS Präfixe zugreifen, z. B. Amazon EC2, Amazon S3 und Amazon.com. Sie haben keinen Zugriff auf Präfixe, die nicht von Amazon stammen. Eine aktuelle Liste der von beworbenen Präfixen finden Sie unter AWSAWS IP-Adressbereiche in der. Allgemeine Amazon Web Services-Referenz AWS gibt Kundenpräfixe, die über öffentliche virtuelle Schnittstellen von AWS Direct Connect empfangen wurden, nicht erneut an andere Kunden weiter. Weitere Informationen zu öffentlichen virtuellen Schnittstellen und Routing-Richtlinien finden Sie unter the section called “Routing-Richtlinien für öffentliche virtuelle Schnittstellen”.

> **Note**
>
> Wir empfehlen, einen Firewall-Filter (basierend auf der Quell/Ziel-Adresse von Paketen) zu verwenden, um den Datenverkehr zu und von einigen Präfixen zu kontrollieren. Wenn Sie einen Präfixfilter (Routing-Map) verwenden, stellen Sie sicher, dass er Präfixe mit einer bestimmten Länge oder längere Präfixe akzeptiert. Präfixe, von denen aus geworben wird,

AWS Direct Connect können aggregiert sein und sich von den in Ihrem Präfixfilter definierten Präfixen unterscheiden.

Gehostete virtuelle Schnittstellen

Um Ihre AWS Direct Connect Verbindung mit einem anderen Konto zu verwenden, können Sie eine gehostete virtuelle Schnittstelle für dieses Konto erstellen. Der Eigentümer des anderen Kontos muss die gehostete virtuelle Schnittstelle akzeptieren, um sie verwenden zu können. Eine gehostete virtuelle Schnittstelle funktioniert genauso wie eine standardmäßige virtuelle Schnittstelle und kann eine Verbindung mit öffentlichen Ressourcen oder einer VPC herstellen.

Sie können virtuelle Transitschnittstellen mit dedizierten oder gehosteten Direct Connect-Verbindungen beliebiger Geschwindigkeit verwenden. Gehostete Verbindungen unterstützen nur eine virtuelle Schnittstelle.

Zur Erstellung einer virtuelle Schnittstelle sind folgende Informationen erforderlich:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit

Ressource	Erforderliche Informationen
	einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

SiteLink

Wenn Sie eine private oder virtuelle Transitschnittstelle erstellen, können Sie Folgendes verwenden. SiteLink

SiteLink ist eine optionale Direct Connect-Funktion für virtuelle private Schnittstellen, die Konnektivität zwischen zwei beliebigen Direct Connect-Points of Presence (PoPs) in derselben AWS Partition über den kürzesten verfügbaren Pfad über das AWS Netzwerk ermöglicht. Auf diese Weise können Sie Ihr lokales Netzwerk über das AWS Global Network verbinden, ohne Ihren Datenverkehr durch eine Region leiten zu müssen. Weitere Informationen dazu finden SiteLink Sie unter Einführung AWS Direct Connect SiteLink.

> **Note**
>
> SiteLink ist in AWS GovCloud (US) und in den Regionen China nicht verfügbar.

Für die Nutzung fällt eine separate Preisgebühr an SiteLink. Weitere Informationen finden Sie unter AWS Direct Connect – Preise.

SiteLink unterstützt nicht alle virtuellen Schnittstellentypen. Die folgende Tabelle zeigt den Schnittstellentyp und ob er unterstützt wird.

Name der virtuellen Schnittstelle	Unterstützt/Nicht unterstützt
Virtuelle Transit-Schnittstelle	Unterstützt
Private virtuelle Schnittstelle, die an einen Direct-Connect-Gateway mit einem virtuellen Gateway angehängt ist.	Unterstützt
Private virtuelle Schnittstelle, die an einen Direct-Connect-Gateway angehängt ist, der keinem virtuelle	Unterstützt

Name der virtuellen Schnittstelle	Unterstützt/Nicht unterstützt
n Gateway oder Transit Gateway zugeordnet ist.	
Private virtuelle Schnittstelle, die an einen virtuellen Gateway angehängt ist.	Nicht unterstützt
Öffentliche virtuelle Schnittstelle	Nicht unterstützt

Das Verhalten beim Routing des Datenverkehrs von AWS-Regionen (virtuellen Gateways oder Transit-Gateways) zu lokalen Standorten über eine SiteLink aktivierte virtuelle Schnittstelle unterscheidet sich geringfügig vom Standardverhalten der virtuellen Direct Connect-Schnittstelle mit einem vorangestellten AWS Pfad. Wenn SiteLink aktiviert, AWS-Region bevorzugen virtuelle Schnittstellen von einem BGP-Pfad mit einer geringeren AS-Pfadlänge von einem Direct Connect-Standort aus, unabhängig von der zugehörigen Region. Beispielsweise wird für jeden Direct-Connect-Standort eine zugehörige Region angekündigt. Wenn SiteLink deaktiviert, bevorzugt der Datenverkehr, der von einem virtuellen Gateway oder einem Transit-Gateway kommt, standardmäßig einen Direct Connect-Standort, der diesem zugeordnet ist AWS-Region, auch wenn der Router von Direct Connect-Standorten, die verschiedenen Regionen zugeordnet sind, einen Pfad mit einer kürzeren AS-Pfadlänge ankündigt. Das virtuelle Gateway oder das Transit Gateway bevorzugt weiterhin den Pfad von lokalen Direct-Connect-Standorten vor den zugeordneten AWS-Region.

SiteLink unterstützt je nach Art der virtuellen Schnittstelle eine maximale Jumbo-Frame-MTU-Größe von entweder 8500 oder 9001. Weitere Informationen finden Sie unter the section called “Die Netzwerk-MTU für private virtuelle Schnittstellen oder virtuelle Transit-Schnittstellen festlegen”.

Voraussetzungen für virtuelle Schnittstellen

Tun Sie Folgendes, bevor Sie eine virtuelle Schnittstelle erstellen:

- Verbindung erstellen Weitere Informationen finden Sie unter the section called “Eine Verbindung mit dem Verbindungsassistenten erstellen”.

- Erstellen Sie eine Link Aggregation Group (LAG), wenn Sie mehrere Verbindungen haben, die Sie wie eine einzige behandeln möchten. Weitere Informationen finden Sie unter Eine Verbindung mit einer LAG verknüpfen.

Zur Erstellung einer virtuelle Schnittstelle sind folgende Informationen erforderlich:

Ressource	Erforderliche Informationen
Connection (Verbindung)	Die AWS Direct Connect Verbindungs- oder Linkaggregationsgruppe (LAG), für die Sie die virtuelle Schnittstelle erstellen.
Name der virtuellen Schnittstelle	Ein Namen für die virtuelle Schnittstelle.
Besitzer der virtuellen Schnittstelle	Wenn Sie die virtuelle Schnittstelle für ein anderes Konto erstellen, benötigen Sie die AWS Konto-ID des anderen Kontos.
(Nur private virtuelle Schnittstelle) Verbindung	Um eine Verbindung zu einer VPC in derselben AWS Region herzustellen, benötigen Sie das Virtual Private Gateway für Ihre VPC. Die ASN für die Amazon-Seite der BGP-Sitzung wird vom Virtual Private Gateway geerbt. Bei der Erstellung eines Virtual Private Gateway können Sie Ihre eigene private ASN angeben. Andernfalls stellt Amazon eine Standard-ASN bereit. Weitere Informationen finden Sie unter Erstellen eines Virtual Private Gateway im Amazon-VPC-Benutzerhandbuch. Für das Herstellen einer Verbindung mit einer VPC über ein Direct-Connect-Gateway ist das Direct-Connect-Gateway erforderlich. Weitere Informationen finden Sie unter Direct Connect-Gateways.
VLAN	Ein eindeutiges VLAN (Virtual Local Area Network; virtuelles lokales Netzwerk)-Tag, das noch nicht auf Ihrer Verbindung verwendet wird. Der Wert muss zwischen 1 und 4094 liegen und dem Ethernet-802.1Q-Standard entsprechen. Dieses Tag ist für jeglichen Datenverkehr über die AWS Direct Connect -Verbindung erforderlich. Wenn Sie über eine gehostete Verbindung verfügen, bietet Ihnen Ihr AWS Direct Connect Partner diesen Wert. Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen

Peer-IP-Adressen	Eine virtuelle Schnittstelle unterstützt eine BGP-Peering-Sitzung für IPv4, IPv6 oder eine von jedem (Dual-Stack). Verwenden Sie keine Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon Pool, um eine öffentliche virtuelle Schnittstelle zu erstellen. Sie können nicht mehrere BGP-Sitzungen für dieselbe IP-Adressierungsfamilie für die gleiche virtuelle Schnittstelle erstellen. Die IP-Adressbereiche, die jedem Ende der virtuellen Schnittstelle für die BGP-Peering-Sitzung zugewiesen sind.
	
	• IPv4:
	  • (Nur bei öffentlichen virtuellen Schnittstellen) Sie müssen eigene einmalige öffentliche IPv4-Adressen angeben. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigenes IPv4-CIDR
	
	  Dabei kann es sich um beliebige öffentliche IP-Adressen handeln (die dem Kunden gehören oder von ihm bereitgestellt werden AWS), es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die Peer-IP des Routers verwendet werden. AWS Wenn Sie beispielsweise einen `/31` Bereich zuweisen, den Sie `203.0.113.0` für Ihre Peer-IP und `203.0.113.1` für die AWS Peer-IP verwenden könnten. `203.0.113.0/31` Oder, wenn Sie einen `/24` Bereich zuweisen, den Sie z. B. `198.51.100.0/24` `198.51.100.10` für Ihre Peer-IP und `198.51.100.20` für die AWS Peer-IP verwenden könnten.
	  • Ein IP-Bereich, der Ihrem AWS Direct Connect Partner oder ISP gehört, zusammen mit einer LOA-CFA-Autorisierung
	  • Ein AWS von -bereitgestellter /31-CIDR. Wenden Sie sich an den AWS Support, um eine öffentliche IPv4 CIDR anzufordern (und einen Anwendungsfall in Ihrer Anfrage anzugeben)

Ressource	Erforderliche Informationen
	> **Note** > Wir können nicht garantieren, dass wir alle Anfragen nach von ihnen AWS bereitgestellten öffentlichen IPv4-Adressen erfüllen können. • (Nur bei privaten virtuellen Schnittstellen) Amazon kann private IPv4-Adressen für Sie generieren. Wenn Sie Ihre eigenen angeben, stellen Sie sicher, dass Sie private CIDRs nur für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispiels weise keine anderen IP-Adressen aus Ihrem lokalen Netzwerk an. Ähnlich wie bei einer öffentlichen virtuellen Schnittstelle muss dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Pe er-IP verwendet werden. Wenn Sie beispielsweise einen `/30` Bereich zuweisen, den Sie `192.168.0.1` für Ihre Peer-IP und `192.168.0.2` für die AWS Peer-IP verwenden könnten. `192.168.0.0/30` • IPv6: Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu. Sie können nicht Ihre eigenen Peer-IPv6-Adressen angeben.
Adress-Familie	Ob die BGP-Peering-Sitzung über IPv4 oder IPv6 erfolgen soll.
BGP-Infor mationen	• Eine öffentliche oder private autonome Systemnnummer (ASN) des Border Gateway Protocol (BGP) für Ihre Seite der BGP-Sitzung. Wenn Sie eine öffentliche ASN verwenden, müssen Sie der ASN-Eigentümer sein. Wenn Sie eine private ASN verwenden, können Sie einen benutzerdefinierte n ASN-Wert festlegen. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 1 und 2147483647 liegen. Das Voranstellen eines autonomen Systems (AS) funktioniert nicht, wenn Sie eine private ASN für eine öffentliche virtuelle Schnittstelle verwenden. • AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern. • Ein MD5-BGP-Authentifizierungsschlüssel. Sie können Ihren eigenen angeben oder Amazon einen Schlüssel generieren lassen.

Ressource	Erforderliche Informationen

(Nur öffentliche virtuelle Schnittstelle) Präfixe, die Sie ankündigen möchten	Öffentliche IPv4-Routen oder IPv6-Routen, die über BGP angekündigt werden sollen. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Das IPv4-CIDR kann sich mit einem anderen öffentlichen IPv4-CIDR überschneiden, das verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Die CIDRs stammen aus verschiedenen Regionen. AWS Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer aktiven/passiven Konfiguration haben.
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• IPv6: Geben Sie eine Präfixlänge von /64 oder kürzer an.
	• Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS -Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.
	• Sie können eine beliebige Präfixlänge über eine öffentliche virtuelle Direct-Connect-Schnittstelle angeben. IPv4 sollte alles von /1 bis /32 unterstützen, und IPv6 sollte alles von /1 bis /64 unterstützen.

Ressource	Erforderliche Informationen
(Nur private virtuelle Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 9 001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames gelten nur für weitergeleitete Routen von. AWS Direct Connect Wenn Sie statische Routen zu einer Routing-Tabelle hinzufügen, die auf Ihr virtuelles privates Gateway verweisen, wird der über die statischen Routen weitergeleitete Verkehr mit 1.500 MTU gesendet. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo Frame-fähig.
(Nur virtuelle Transit-Schnittstelle) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) der übermittelten Pakete. AWS Direct Connect Der Standardwert ist 1500. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8 500 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Jumbo-Frames werden mit bis zu 8500 MTU für Direct Connect unterstützt. Statische Routen und propagierte Routen, die in der Routing-Tabelle von Transit Gateway konfiguriert sind, unterstützen Jumbo-Frames, darunter von EC2-Instances mit statischen VPC-Routing-Tabelleneinträgen zum Transit-Gateway-Anhang. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Seite Allgemeine Konfiguration der virtuellen Schnittstelle nach Jumbo-Frame-fähig.

Wenn Sie eine virtuelle Schnittstelle erstellen, können Sie angeben, welches Konto Eigentümer der virtuellen Schnittstelle ist. Wenn Sie ein AWS Konto wählen, das nicht Ihr Konto ist, gelten die folgenden Regeln:

- Bei privaten VIFs und Transit-VIFs gilt das Konto für die virtuelle Schnittstelle und das Virtual Private Gateway-/Direct Connect-Gateway-Ziel.
- Bei öffentlichen VIFs wird das Konto für die Fakturierung virtueller Schnittstellen verwendet. Die Nutzung ausgehender Daten (Data Transfer Out, DTO) wird dem Eigentümer der Ressource anhand der AWS Direct Connect Datenübertragungsrate berechnet.

> **Note**
>
> 31-Bit-Präfixe werden auf allen virtuellen Direct-Connect-Schnittstellentypen unterstützt. Weitere Informationen finden Sie unter RFC 3021: Verwendung von 31-Bit-Präfixen für IPv4-Punkt-zu-Punkt-Links.

Eine virtuelle Schnittstelle erstellen

Sie können eine virtuelle Transit-Schnittstelle für eine Verbindung mit einem Transit-Gateway, eine öffentliche virtuelle Schnittstelle für eine Verbindung mit öffentlichen Ressourcen (Nicht-VPC-Services) oder eine private virtuelle Schnittstelle für die Verbindung mit einer VPC erstellen.

Um eine virtuelle Schnittstelle für Konten innerhalb Ihres Kontos oder Konten AWS Organizations, die sich von Ihrem unterscheiden AWS Organizations , zu erstellen, erstellen Sie eine gehostete virtuelle Schnittstelle. Weitere Informationen finden Sie unter the section called “Eine gehostete virtuelle Schnittstelle erstellen”.

Voraussetzungen

Bevor Sie beginnen, sollten Sie die Informationen unter Voraussetzungen für virtuelle Schnittstellen lesen.

Eine öffentliche virtuelle Schnittstelle erstellen

Wenn Sie eine öffentliche virtuelle Schnittstelle erstellen, kann es bis zu 72 Stunden dauern, bis wir Ihre Anforderung überprüfen und genehmigen.

So stellen Sie eine öffentliche virtuelle Schnittstelle bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.

3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public virtual interface settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   d. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1-2147483647.
6. Gehen Sie unter Additional settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

   b. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie Ihren BGP-MD5-Schlüssel ein.

      Wenn Sie keinen Wert eingeben, erstellen wir einen BGP-Schlüssel. Wenn Sie Ihren eigenen Schlüssel angegeben oder wir den Schlüssel für Sie generiert haben, wird dieser Wert in der Spalte BGP authentication key (BGP-Authentifizierungsschlüssel) auf der Detailseite zu virtuellen Schnittstellen von Virtual interfaces (Virtuelle Schnittstellen) angezeigt.

c. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

> **Important**
>
> Sie können einer vorhandenen öffentlichen VIF zusätzliche Präfixe hinzufügen und diese bekannt geben, indem Sie sich an den AWS Support wenden. Stellen Sie in Ihrem Support-Fall eine Liste zusätzlicher CIDR-Präfixe bereit, die Sie der öffentlichen VIF hinzufügen und ankündigen möchten.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
8. Laden Sie die Routerkonfiguration für Ihr Gerät herunter. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine öffentliche virtuelle Schnittstelle über die Befehlszeile oder API

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

Eine private virtuelle Schnittstelle erstellen

Sie können eine private virtuelle Schnittstelle für ein virtuelles privates Gateway in derselben Region wie Ihre AWS Direct Connect Verbindung bereitstellen. Weitere Informationen zur Bereitstellung einer privaten virtuellen Schnittstelle für ein AWS Direct Connect Gateway finden Sie unterArbeiten mit Direct Connect-Gateways.

Wenn Sie eine VPC mithilfe des VPC-Assistenten erstellen, ist die Routing-Verbreitung automatisch für Sie aktiviert. Bei aktivierter Routing-Verbreitung werden Routen automatisch in die Routing-

Tabellen in Ihrer VPC eingefügt. Wenn Sie möchten, können Sie die Funktion deaktivieren. Weitere Informationen finden Sie unter Aktivieren der Routing-Verbreitung in Ihrer Routing-Tabelle im Amazon-VPC-Benutzerhandbuch.

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Der MTU-Wert einer virtuellen privaten Schnittstelle kann entweder 1 500 oder 9 001 (Jumbo-Frames) sein. Der MTU-Wert einer virtuellen Transit-Schnittstelle kann entweder 1500 oder 8500 (Jumbo-Frames) sein. Sie können die MTU angeben, wenn Sie die Schnittstelle erstellen oder eine erstellte Schnittstelle aktualisieren. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8500 (Jumbo-Frames) oder 9001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Um zu prüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect -Konsole aus und suchen Sie den Punkt Jumbo Frame Capable (Jumbo-Frame-fähig) auf der Registerkarte Summary (Übersicht).

So stellen Sie eine private, virtuelle Schnittstelle zu einer VPC bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Wählen Sie unter Besitzer der virtuellen Schnittstelle Mein AWS Konto aus, wenn die virtuelle Schnittstelle für Ihr AWS Konto bestimmt ist.

   d. Wählen Sie für Direct Connect Gateway das Direct Connect-Gateway aus.

   e. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

f. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung (nicht RFC 1918) verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

      [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

   b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

   c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
8. Laden Sie die Routerkonfiguration für Ihr Gerät herunter. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine private virtuelle Schnittstelle über die Befehlszeile oder API

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

Eine virtuelle Transit-Schnittstelle für das Direct-Connect-Gateway erstellen

Um Ihre AWS Direct Connect Verbindung mit dem Transit-Gateway zu verbinden, müssen Sie eine Transitschnittstelle für Ihre Verbindung erstellen. Geben Sie das Direct Connect-Gateway an, mit dem die Verbindung hergestellt wird.

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Der MTU-Wert einer virtuellen privaten Schnittstelle kann entweder 1 500 oder 9 001 (Jumbo-Frames) sein. Der MTU-Wert einer virtuellen Transit-Schnittstelle kann entweder 1500 oder 8500 (Jumbo-Frames) sein. Sie können die MTU angeben, wenn Sie die Schnittstelle erstellen oder eine erstellte Schnittstelle aktualisieren. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8500 (Jumbo-Frames) oder 9001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Um zu prüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo-Frames unterstützt, wählen Sie sie in der AWS Direct Connect -Konsole aus und suchen Sie den Punkt Jumbo Frame Capable (Jumbo-Frame-fähig) auf der Registerkarte Summary (Übersicht).

> **Important**
>
> Wenn Sie Ihr Transit Gateway einem oder mehreren Direct-Connect-Gateways zuordnen, muss die vom Transit Gateway und dem Direct-Connect-Gateway verwendete autonome Systemnummer (ASN) unterschiedlich sein. Wenn Sie beispielsweise die Standard-ASN 64512 sowohl für das Transit Gateway als auch für das Direct-Connect-Gateway verwenden, schlägt die Zuordnungsanfrage fehl.

So stellen Sie eine virtuelle Transit-Schnittstelle für ein Direct Connect-Gateway bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Transit aus.
5. Führen Sie unter Transit virtual interface settings (Einstellungen für virtuelle Transit-Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Wählen Sie unter Besitzer der virtuellen Schnittstelle Mein AWS Konto aus, wenn die virtuelle Schnittstelle für Ihr AWS Konto bestimmt ist.

   d. Wählen Sie für Direct Connect Gateway das Direct Connect-Gateway aus.

   e. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   f. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1 bis 2147483647.
6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

[IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

- Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
- Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

> **Important**
>
> Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung (nicht RFC 1918) verwenden und die Adresse selbst angeben.
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU-Wert (Maximum Transmission Unit, maximale Größe für Übertragungseinheiten) von 1500 (Standard) in 8500 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 8500) (Jumbo-MTU (MTU-Größe 8500)) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Nachdem Sie die virtuelle Schnittstelle erstellt haben, können Sie die Router-Konfiguration für Ihr Gerät herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine virtuelle Transit-Schnittstelle über die Befehlszeile oder API

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

So zeigen Sie die virtuellen Schnittstellen an, die einem Direct Connect-Gateway über die Befehlszeile oder API angefügt sind

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAnlagen (AWS Direct Connect API)

Routerkonfigurationsdatei herunterladen

Nachdem Sie die virtuelle Schnittstelle erstellt haben und der Schnittstellenstatus „aktiv“ ist, können Sie die Router-Konfigurationsdatei für Ihren Router herunterladen.

Wenn Sie einen der folgenden Router für virtuelle Schnittstellen verwenden, für die MACsec aktiviert ist, erstellen wir automatisch die Konfigurationsdatei für Ihren Router:

- Cisco Nexus Switches der Serie 9K+, auf denen Software NX-OS 9.3 oder höher ausgeführt wird
- Router von Juniper Networks der Serie M/MX mit Software von JunOS 9.5 oder höher

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).
4. Wählen Sie Download router configuration (Router-Konfiguration herunterladen) aus.
5. Führen Sie unterDownload router configuration (Router-Konfiguration herunterladen) die folgenden Schritte aus:

a. Wählen Sie unter Vendor den Hersteller Ihres Routers aus.

b. Wählen Sie unter Platform das Modell Ihres Routers aus.

c. Wählen Sie unter Software die Softwareversion Ihres Routers aus.

6. Wählen Sie Download (Herunterladen) und verwenden Sie anschließend die entsprechende Konfiguration für Ihren Router, damit Sie eine Verbindung zu AWS Direct Connect herstellen können.

Überlegungen zu MACsec

Wenn Sie Ihren Router manuell für MACsec konfigurieren müssen, orientieren Sie sich an der folgenden Tabelle.

Parameter	Beschreibung
CKN-Länge	Dies ist eine Zeichenfolge mit 64 Hexadezimalzeichen (0–9, A–E). Verwenden Sie die volle Länge, um eine maximale plattformübergreifende Kompatibilität zu erreichen.
CAK-Länge	Dies ist eine Zeichenfolge mit 64 Hexadezimalzeichen (0–9, A–E). Verwenden Sie die volle Länge, um eine maximale plattformübergreifende Kompatibilität zu erreichen.
Kryptografischer Algorithmus	AES_256_CMAC
SAK Cipher Suite	• Für 100-Gbit/s-Verbindungen: GCM_AES_XPN_256 • Für 10-Gbit/s-Verbindungen: GCM_AES_XPN_256 oder GCM_AES _256
Key Cipher Suite	16
Vertraulichkeits-Offset	0

Parameter	Beschreibung
ICV-Indikator	Nein
SAK-Rekey-Zeit	PN Rollover>

Details der virtuellen Schnittstelle anzeigen

Sie können den aktuellen Status Ihrer virtuellen Schnittstelle anzeigen. Zu den Details gehören:

- Verbindungsstatus
- Name
- Ort
- VLAN
- BGP-Details
- Peer-IP-Adressen

So zeigen Sie Details zu einer virtuellen Schnittstelle an

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Bereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).

So beschreiben Sie virtuelle Schnittstellen über die Befehlszeile oder API

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualSchnittstellen (AWS Direct Connect API)

Einen BGP-Peer hinzufügen oder löschen

Fügen Sie eine IPv4- oder IPv6-BGP-Peering-Sitzung zu Ihrer virtuellen Schnittstelle hinzu oder löschen Sie die Sitzung.

Eine virtuelle Schnittstelle unterstützt jeweils eine IPv4-BGP-Peering-Sitzung und eine IPv6-BGP-Peering-Sitzung.

Sie können nicht Ihre eigenen Peer-IPv6-Adressen für eine IPv6-BGP-Peering-Sitzung angeben. Amazon weist Ihnen automatisch eine /125 IPv6 CIDR zu.

BGP mit mehreren Protokollen wird nicht unterstützt. IPv4 und IPv6 arbeiten für die virtuelle Schnittstelle im Dual-Stack-Modus.

AWS aktiviert standardmäßig MD5. Sie können diese Option nicht ändern.

Ein BGP-Peer hinzufügen

Gehen Sie wie folgt vor, um einen BGP-Peer hinzuzufügen.

So fügen Sie einen BGP-Peer hinzu

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).
4. Wählen Sie Add peering (Peering hinzufügen) aus.
5. (Private virtuelle Schnittstelle) Um IPv4-BGP-Peers hinzuzufügen, führen Sie die folgenden Schritte aus:
   - Wählen Sie IPv4 aus.
   - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll. Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.
6. (Öffentliche virtuelle Schnittstelle) Um IPv4-BGP-Peers hinzuzufügen, führen Sie die folgenden Schritte aus:
   - Geben Sie unter Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die der Datenverkehr gesendet werden soll.
   - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

> **Important**
>
> Wenn Sie die AWS automatische Zuweisung von IP-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 zugewiesen. AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und Ziel für den Datenverkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben. Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

7. (Private oder öffentliche virtuelle Schnittstelle) Wählen Sie zum Hinzufügen von IPv6-BGP-Peers IPv6 aus. Die Peer-IPv6-Adressen werden automatisch aus dem IPv6-Adresspool von Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.
8. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Für eine öffentliche virtuelle Schnittstelle muss die ASN privat oder für die virtuelle Schnittstelle bereits auf der Genehmigungsliste freigegeben sein.

   Die gültigen Werte lauten 1-2147483647.

   Beachten Sie, dass wir automatisch einen Wert zuweisen, wenn Sie keinen Wert eingeben.
9. Wenn Sie Ihren eigenen BGP-Schlüssel bereitstellen möchten, geben Sie unter BGP Authentication Key (BGP-Authentifizierungsschlüssel) Ihren eigenen BGP-MD5-Schlüssel ein.
10. Wählen Sie Add peering (Peering hinzufügen) aus.

So erstellen Sie einen BGP-Peer über die Befehlszeile oder API

- create-bgp-peer (AWS CLI)
- BGP Peer (API) erstellenAWS Direct Connect

Ein BGP-Peer löschen

Wenn Ihre virtuelle Schnittstelle sowohl über eine IPv4- als auch eine IPv6-BGP-Peering-Sitzung verfügt, können Sie eine der BGP-Peering-Sitzungen löschen (nicht aber beide).

So löschen Sie einen BGP-Peer

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).
4. Wählen Sie unter Peerings das zu löschende Peering und danach Delete (Löschen) aus.
5. Klicken Sie im Dialogfeld Remove peering from virtual interface (Peering von virtueller Schnittstelle entfernen) auf Delete (Löschen).

So löschen Sie einen BGP-Peer über die Befehlszeile oder API

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (API)AWS Direct Connect

Die Netzwerk-MTU für private virtuelle Schnittstellen oder virtuelle Transit-Schnittstellen festlegen

AWS Direct Connect unterstützt eine Ethernet-Framegröße von 1522 oder 9023 Byte (14 Byte Ethernet-Header + 4 Byte VLAN-Tag + Byte für das IP-Datagramm + 4 Byte FCS) auf der Verbindungsschicht.

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Der MTU-Wert einer virtuellen privaten Schnittstelle kann entweder 1 500 oder 9 001 (Jumbo-Frames) sein. Der MTU-Wert einer virtuellen Transit-Schnittstelle kann entweder 1500 oder 8500 (Jumbo-Frames) sein. Sie können die MTU angeben, wenn Sie die Schnittstelle erstellen oder eine erstellte Schnittstelle aktualisieren. Das Festlegen der MTU einer virtuellen Schnittstelle auf 8500 (Jumbo-Frames) oder 9001 (Jumbo-Frames) kann zu einem Update der zugrunde liegenden physischen Verbindung führen, wenn diese noch nicht aktualisiert wurde, um Jumbo-Frames zu unterstützen. Das Aktualisieren der Verbindung unterbricht die Netzwerkkonnektivität für alle virtuellen Schnittstellen der Verbindung für bis zu 30 Sekunden. Um zu überprüfen, ob eine Verbindung oder virtuelle Schnittstelle Jumbo Frames unterstützt, wählen Sie sie in der AWS Direct Connect Konsole aus und suchen Sie auf der Registerkarte Zusammenfassung nach Jumbo Frame Capable.

Wenn Sie Jumbo-Frames für Ihre private virtuelle Schnittstelle oder virtuelle Transit-Schnittstelle aktiviert haben, können Sie sie nur mit einer Verbindung oder LAG verknüpfen, die Jumbo-Frames unterstützt. Jumbo-Frames werden von privaten virtuellen Schnittstellen unterstützt, die entweder einem Virtual Private Gateway oder einem Direct-Connect-Gateway zugewiesen sind, sowie von virtuellen Transit-Schnittstellen, die einem Direct-Connect-Gateway zugewiesen sind. Wenn Sie zwei private virtuelle Schnittstellen haben, die dieselbe Route vorschlagen, aber unterschiedliche MTU-Werte verwenden, oder wenn Sie eine Site-to-Site-VPN haben, die dieselbe Route ankündigt, wird der Wert 1 500 MTU genutzt.

> **Important**
>
> Jumbo Frames gelten nur für übertragene Routen AWS Direct Connect und für statische Routen über Transit-Gateways. Jumbo-Frames auf Transit Gateways unterstützen nur 8 500 Byte.
> Wenn eine EC2-Instance keine Jumbo-Frames unterstützt, lässt sie Jumbo-Frames von Direct Connect fallen. Alle EC2-Instance-Typen unterstützen Jumbo-Frames, mit Ausnahme von C1, CC1, T1 und M1. Weitere Informationen finden Sie unter Network Maximum Transmission Unit (MTU) für Ihre EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.
> Für gehostete Verbindungen können Jumbo-Frames nur aktiviert werden, wenn sie ursprünglich für die gehostete übergeordnete Direct-Connect-Verbindung aktiviert waren. Wenn Jumbo-Frames auf dieser übergeordneten Verbindung nicht aktiviert sind, können sie auf keiner Verbindung aktiviert werden.

So legen Sie die MTU für eine private virtuelle Schnittstelle fest

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle und danach Edit (Bearbeiten) aus.
4. Wählen Sie unter Jumbo MTU (MTU size 9001) (Jumbo-MTU (MTU-Größe 9001)) oder Jumbo MTU (MTU size 8500) (Jumbo-MTU (MTU-Größe 8500)) die Option Enabled (Aktiviert) aus.
5. Wählen Sie unter Acknowledge (Bestätigen) die Option I understand the selected connection(s) will go down for a brief period (Ich verstehe, dass die ausgewählte(n) Verbindung(en) für einen kurzen Zeitraum ausfallen) aus. Der Status der virtuellen Schnittstelle lautet `pending`, bis die Aktualisierung abgeschlossen ist.

So legen Sie die MTU einer privaten virtuellen Schnittstelle über die Befehlszeile oder API fest

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct Connect API)

Tags für virtuelle Schnittstellen hinzufügen oder entfernen

Tags bieten eine Möglichkeit zur Identifizierung der virtuellen Schnittstelle. Sie können ein Tag hinzufügen oder entfernen, wenn Sie der Kontoinhaber der virtuellen Schnittstelle sind.

So fügen Sie Tags für virtuelle Schnittstellen hinzu oder entfernen sie

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle und danach Edit (Bearbeiten) aus.
4. Hinzufügen oder Entfernen eines Tag.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.
5. Klicken Sie auf Edit virtual interface (Virtuelle Schnittstelle bearbeiten).

So fügen Sie Tags über die Befehlszeile hinzu und entfernen sie

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Virtuelle Schnittstellen entfernen

Löschen Sie eine oder mehrere virtuelle Schnittstellen. Bevor Sie eine Verbindung löschen können, müssen Sie die zugehörige virtuelle Schnittstelle löschen. Durch das Löschen einer

virtuellen Schnittstelle fallen keine mit der virtuellen Schnittstelle verbundenen AWS Direct Connect Datenübertragungsgebühren an.

So löschen Sie eine virtuelle Schnittstelle

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Bereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuellen Schnittstellen und danach Delete (Löschen) aus.
4. Wählen Sie im Bestätigungsdialogfeld Delete (Löschen) die Option Delete (Löschen) aus.

So löschen Sie eine virtuelle Schnittstelle über die Befehlszeile oder API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualSchnittstelle (AWS Direct Connect API)

Eine gehostete virtuelle Schnittstelle erstellen

Sie können eine öffentliche, Transit- oder private gehostete virtuelle Schnittstelle erstellen. Bevor Sie beginnen, sollten Sie die Informationen unter Voraussetzungen für virtuelle Schnittstellen lesen.

Eine gehostete private virtuelle Schnittstelle erstellen

So erstellen Sie eine gehostete private, virtuelle Schnittstelle

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

c. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Ein weiteres AWS -Konto aus, und geben Sie dann für Besitzer der virtuellen Schnittstelle die ID des Kontos ein, dem diese virtuelle Schnittstelle gehört.

d. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

e. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1-2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IP-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 zugewiesen. AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und Ziel für den Datenverkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung (nicht RFC 1918) verwenden und die Adresse selbst angeben. Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

      [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Nachdem die gehostete virtuelle Schnittstelle vom Eigentümer des anderen AWS -Kontos akzeptiert wurde, können Sie die Router-Konfigurationsdatei herunterladen.

So erstellen Sie eine gehostete private virtuelle Schnittstelle über die Befehlszeile oder API

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

Eine gehostete öffentliche virtuelle Schnittstelle erstellen

So erstellen Sie eine gehostete öffentliche, virtuelle Schnittstelle

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Public (Öffentlich).
5. Führen Sie unter Public Virtual Interface Settings (Einstellungen für öffentliche virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

c. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus, und geben Sie dann für Besitzer der virtuellen Schnittstelle die ID des Kontos ein, dem diese virtuelle Schnittstelle gehört.

d. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

e. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1-2147483647.

6. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

   [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

   - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
   - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

   > **Important**
   >
   > Wenn Sie die AWS automatische Zuweisung von IP-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 zugewiesen. AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und Ziel für den Datenverkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung verwenden und die Adresse selbst angeben. Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

   [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

7. Um Präfixe für Amazon anzukündigen, geben Sie bei Prefixes you want to advertise (Präfixe, die Sie ankündigen möchten) die IPv4-CIDR-Zieladressen an (getrennt durch Kommas), an die Datenverkehr über die virtuelle Schnittstelle weitergeleitet werden soll.

8. Wenn Sie zur Authentifizierung der BGP-Sitzung einen eigenen Schlüssel bereitstellen möchten, geben Sie den Schlüssel in den Additional Settings (Weitere Einstellungen) im Feld BGP Authentication Key (BGP-Authentifizierungsschlüssel) ein.

   Wenn Sie keinen Wert eingeben, generieren wir einen BGP-Schlüssel.
9. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:
   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.
10. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
11. Nachdem die gehostete virtuelle Schnittstelle vom Eigentümer des anderen AWS -Kontos akzeptiert wurde, können Sie die Router-Konfigurationsdatei herunterladen.

So erstellen Sie eine gehostete öffentliche virtuelle Schnittstelle über die Befehlszeile oder API

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

Eine gehostete virtuelle Transit-Schnittstelle erstellen

So erstellen Sie eine gehostete virtuelle Transit-Schnittstelle

> **Important**
>
> Wenn Sie Ihr Transit Gateway einem oder mehreren Direct-Connect-Gateways zuordnen, muss die vom Transit Gateway und dem Direct-Connect-Gateway verwendete autonome Systemnummer (ASN) unterschiedlich sein. Wenn Sie beispielsweise die Standard-ASN 64512 sowohl für das Transit Gateway als auch für das Direct-Connect-Gateway verwenden, schlägt die Zuordnungsanfrage fehl.

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.

2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Transit aus.
5. Führen Sie unter Transit virtual interface settings (Einstellungen für virtuelle Transit-Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Wählen Sie für Besitzer der virtuellen Schnittstelle die Option Anderes AWS Konto aus, und geben Sie dann für Besitzer der virtuellen Schnittstelle die ID des Kontos ein, dem diese virtuelle Schnittstelle gehört.

   d. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   e. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1-2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IP-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 zugewiesen. AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und Ziel für den Datenverkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder

eine andere Adressierung verwenden und die Adresse selbst angeben. Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU-Wert (Maximum Transmission Unit, maximale Größe für Übertragungseinheiten) von 1500 (Standard) in 8500 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 8500) (Jumbo-MTU (MTU-Größe 8500)) aus.

c. [Optional] Hinzufügen eines Tags. Gehen Sie wie folgt vor:

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
8. Nachdem die gehostete virtuelle Schnittstelle vom Eigentümer des anderen AWS -Kontos akzeptiert wurde, können Sie die Router-Konfigurationsdatei herunterladen.

So erstellen Sie eine gehostete virtuelle Transit-Schnittstelle über die Befehlszeile oder API

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

Eine gehostete virtuelle Schnittstelle akzeptieren

Bevor Sie eine gehostete virtuelle Schnittstelle verwenden können, müssen Sie sie akzeptieren. Für eine private virtuelle Schnittstelle müssen Sie auch über ein vorhandenes Virtual Private Gateway oder Direct Connect-Gateway verfügen. Für eine virtuelle Transit-Schnittstelle müssen Sie auch über ein vorhandenes Transit-Gateway oder Direct Connect-Gateway verfügen.

So akzeptieren Sie eine gehostete virtuelle Schnittstelle

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle aus und wählen Sie View details (Details anzeigen).
4. Wählen Sie Accept (Akzeptieren) aus.
5. Dies gilt für private virtuelle Schnittstellen und virtuelle Transitschnittstellen.

   (Private virtuelle Schnittstelle) Wählen Sie im Dialogfeld Accept virtual interface (Virtuelle Schnittstelle akzeptieren) ein Direct Connect-Gateway aus und klicken Sie anschließend auf Accept virtual interface (Virtuelle Schnittstelle akzeptieren).

   (Private virtuelle Schnittstelle) Wählen Sie im Dialogfeld Accept virtual interface (Virtuelle Schnittstelle akzeptieren) ein Virtual Private Gateway oder Direct Connect-Gateway aus und klicken Sie anschließend auf Accept virtual interface (Virtuelle Schnittstelle akzeptieren).
6. Nachdem Sie die gehostete virtuelle Schnittstelle akzeptiert haben, kann der Eigentümer der AWS Direct Connect -Verbindung die Router-Konfigurationsdatei herunterladen. Die Option Download router configuration (Router-Konfiguration herunterladen) ist für das Konto, das die gehostete virtuelle Schnittstelle akzeptiert, nicht verfügbar.

So akzeptieren Sie eine gehostete private virtuelle Schnittstelle über die Befehlszeile oder API

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct Connect API)

So akzeptieren Sie eine gehostete öffentliche virtuelle Schnittstelle über die Befehlszeile oder API

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct Connect API)

So akzeptieren Sie eine gehostete virtuelle Transit-Schnittstelle über die Befehlszeile oder API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct Connect API)

Eine virtuelle Schnittstelle migrieren

Verwenden Sie dieses Verfahren, wenn Sie eine der folgenden Migrationsoperationen für virtuelle Schnittstellen ausführen möchten:

- Migrieren Sie eine vorhandene virtuelle Schnittstelle, die einer Verbindung zugeordnet ist, zu einer anderen LAG.
- Migrieren Sie eine vorhandene virtuelle Schnittstelle, die einer vorhandenen LAG zugeordnet ist, zu einer neuen LAG.
- Migrieren Sie eine vorhandene virtuelle Schnittstelle, die einer Verbindung zugeordnet ist, zu einer anderen Verbindung.

> **Note**
>
> - Sie können eine virtuelle Schnittstelle zu einer neuen Verbindung innerhalb derselben Region migrieren, aber Sie können sie nicht von einer Region in eine andere migrieren. Wenn Sie eine vorhandene virtuelle Schnittstelle zu einer neuen Verbindung migrieren oder dieser zuordnen, sind die Konfigurationsparameter, die den virtuellen Schnittstellen zugeordnet sind, identisch. Sie können dies umgehen, indem Sie die Konfiguration für die Verbindung vorbereiten und dann die BGP-Konfiguration aktualisieren.
> - Sie können eine VIF nicht von einer gehosteten Verbindung zu einer anderen gehosteten Verbindung migrieren. VLAN-IDs sind eindeutig. Daher würde eine Migration einer VIF auf diese Weise bedeuten, dass die VLANs nicht übereinstimmen. Sie müssen entweder die Verbindung oder die VIF löschen und diese dann mithilfe eines VLAN neu erstellen, das sowohl für die Verbindung als auch für die VIF identisch ist.

> **Important**
>
> Die virtuelle Schnittstelle fällt für einen kurzen Zeitraum aus. Wir empfehlen Ihnen, dieses Verfahren während eines Wartungsfensters durchzuführen.

So migrieren Sie eine virtuelle Schnittstelle:

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie die virtuelle Schnittstelle und danach Edit (Bearbeiten) aus.
4. Wählen Sie unter Connection (Verbindung) die LAG oder Verbindung aus.
5. Klicken Sie auf Edit virtual interface (Virtuelle Schnittstelle bearbeiten).

So löschen Sie eine virtuelle Schnittstelle über die Befehlszeile oder API:

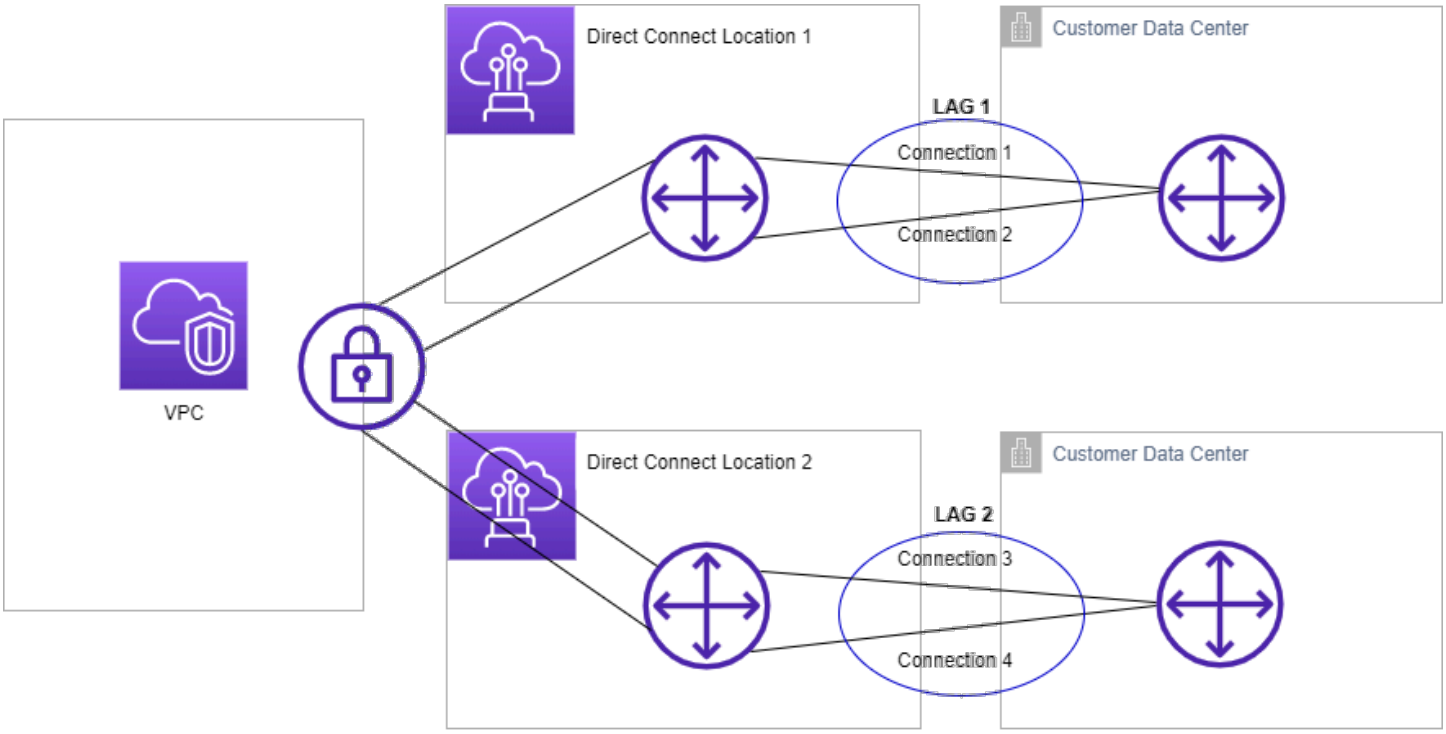
- associate-virtual-interface (AWS CLI)
- AssociateVirtualSchnittstelle (AWS Direct Connect API)

Link Aggregation Groups (LAG)

Sie können mehrere Verbindungen verwenden, um die verfügbare Bandbreite zu erhöhen. Eine Link Aggregation Group (LAG) ist eine logische Schnittstelle, die über das Link Aggregation Control Protocol (LACP) mehrere Verbindungen zu einem einzigen AWS Direct Connect-Endpunkt zusammenfasst, sodass sie als eine einzelne verwaltete Verbindung behandelt werden können. LAGs optimieren die Konfiguration, da die LAG-Konfiguration für alle Verbindungen in der Gruppe gilt.

> **Note**
>
> Multi-Chassis LAG (MLAG) wird von AWS nicht unterstützt.

Im folgenden Diagramm sehen Sie vier Verbindungen (zwei Verbindungen zu jedem Standort). Sie können eine LAG für Verbindungen erstellen, die auf demselben AWS Gerät und am selben Ort enden, und dann die beiden LAGs anstelle der vier Verbindungen für Konfiguration und Verwaltung verwenden.



Sie können eine LAG aus vorhandenen Verbindungen erstellen oder neue Verbindungen bereitstellen. Nach der Erstellung der LAG können Sie ihr bestehende Verbindungen zuordnen (eigenständige ebenso wie Verbindungen, die Teil einer anderen LAG sind).

Die folgenden Regeln gelten:

- Alle Verbindungen müssen dedizierte Verbindungen sein und eine Portgeschwindigkeit von 1 Gbit/s, 10 Gbit/s oder 100 Gbit/s haben.
- Alle Verbindungen in der LAG müssen dieselbe Bandbreite aufweisen.
- Sie können maximal zwei 100G-Verbindungen oder vier Verbindungen mit einer Portgeschwindigkeit von weniger als 100 G in einer LAG haben. Jede Verbindung in der LAG muss einzeln beim Gesamt-Verbindungslimit für die Region berücksichtigt werden.
- Alle Verbindungen in der LAG müssen an demselben AWS Direct Connect-Endpunkt auflaufen.
- LAGs werden für alle virtuellen Schnittstellentypen unterstützt – öffentlichen, privaten und Transit-Schittstellen.

Beim Erstellen einer LAG können Sie den "Letter of Authorization and Connecting Facility Assignment" (LOA-CFA) für jede neue physische Verbindung einzeln von der AWS Direct Connect-Konsole herunterladen. Weitere Informationen finden Sie unter Das LOA-CFA-Dokument herunterladen.

Alle LAGs verfügen über ein Attribut, in dem die Mindestanzahl der aktiven Verbindungen festgelegt ist, die für den Betrieb in der LAG selbst erforderlich sind. Der Standardwert dieses Attributs für neue LAGs lautet 0. Sie können einen anderen Wert für die LAG festlegen. In diesem Fall fällt die gesamte LAG aus, wenn die Anzahl der aktiven Verbindungen diesen Grenzwert unterschreitet. Mit diesem Attribut kann eine Überlastung der verbleibenden Verbindungen verhindert werden.

Alle Verbindungen in einer LAG befinden sich im Aktiv/Aktiv-Modus.

> **Note**
>
> Wenn Sie eine LAG erstellen oder mehrere Verbindungen der LAG zuordnen, können wir nicht garantieren, dass genügend Ports an einem bestimmten AWS Direct Connect-Endpunkt verfügbar sind.

Überlegungen zu MACsec

Berücksichtigen Sie Folgendes, wenn Sie MACsec auf LAGs konfigurieren möchten:

- Wenn Sie eine LAG aus bestehenden Verbindungen erstellen, trennen wir alle MACsec-Schlüssel von den Verbindungen. Dann fügen wir die Verbindungen zur LAG hinzu und ordnen den LAG-MACsec-Schlüssel den Verbindungen zu.
- Wenn Sie einer LAG eine bestehende Verbindung zuordnen, werden die MACsec-Schlüssel, die derzeit der LAG zugeordnet sind, der Verbindung zugeordnet. Daher trennen wir die MACsec-Schlüssel von der Verbindung, fügen die Verbindung zur LAG hinzu und ordnen dann den LAG-MACsec-Schlüssel der Verbindung zu.

Eine LAG erstellen

Sie können eine LAG durch Bereitstellung neuer Verbindungen oder durch Zusammenfassung vorhandener Verbindungen erstellen.

Sie können keine LAG mit neuen Verbindungen erstellen, wenn Sie damit das Gesamt-Verbindungslimit für die Region überschreiten.

Wenn Sie eine LAG auf der Grundlage vorhandener Verbindungen erstellen möchten, müssen sich die Verbindungen auf demselben AWS-Gerät befinden (an demselben AWS Direct Connect-Endpunkt auflaufen) und dieselbe Bandbreite aufweisen. Sie müssen auch dieselbe Bandbreite aufweisen. Eine Migration der Verbindung von einer vorhandenen LAG ist nicht möglich, wenn dies dazu führt, dass die ursprüngliche LAG unter den eingestellten Mindestwert für funktionierende Verbindungen fällt.

> **Important**
>
> Bei bestehenden Verbindungen wird die Konnektivität mit AWS während der Erstellung der LAG unterbrochen.

Create a LAG with new connections using the console

So erstellen Sie eine LAG mit neuen Verbindungen

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie Create LAG aus.

4. Wählen Sie unter Lag creation type (LAG-Erstellungstyp) die Option Request new connections (Neue Verbindungen anfordern) aus, und geben Sie die folgenden Informationen an:

   - LAG name (LAG-Name): ein Name für die LAG
   - Location (Standort): der Standort der LAG
   - Port speed (Portgeschwindigkeit): die Portgeschwindigkeit für die Verbindungen
   - Number of new connections (Anzahl neuer Verbindungen): die Anzahl der neuen zu erstellenden Verbindungen. Sie können maximal vier Verbindungen haben, wenn die Portgeschwindigkeit 1G oder 10G ist, oder zwei, wenn die Portgeschwindigkeit 100G beträgt.
   - (Optional) Konfigurieren Sie MAC Security (MACsec) für die Verbindung. Wählen Sie unter Additional Settings (Zusätzliche Einstellungen) die Option Request a MACsec capable port (Einen MACsec-fähigen Port anfordern) aus.

     MACsec ist nur auf dedizierten Verbindungen verfügbar.
   - (Optional) Hinzufügen oder Entfernen einer Markierung.

     [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

     - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
     - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

     [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.
5. Wählen Sie Create LAG aus.

Create a LAG with existing connections using the console

So erstellen Sie eine LAG auf der Grundlage vorhandener Verbindungen

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie Create LAG aus.
4. Wählen Sie unter Lag creation type (LAG-Erstellungstyp) die Option Use existing connections (Vorhandene Verbindungen verwenden) aus, und geben Sie die folgenden Informationen an:

- LAG name (LAG-Name): ein Name für die LAG
- Existing connections (Bestehende Verbindungen): Die Direct-Connect-Verbindung, die für die LAG verwendet werden soll.
- (Optional) Number of new connections (Anzahl neuer Verbindungen): die Anzahl der neuen zu erstellenden Verbindungen. Sie können maximal vier Verbindungen haben, wenn die Portgeschwindigkeit 1G oder 10G ist, oder zwei, wenn die Portgeschwindigkeit 100G beträgt.
- Minimum links (Min. Verbindungen): die Mindestanzahl an Verbindungen, die für den Betrieb der LAG selbst erforderlich sind. Wenn Sie keinen Wert angeben, wird der Standardwert 0 zugewiesen.

5. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

6. Wählen Sie Create LAG aus.

Command line

So erstellen Sie eine LAG über die Befehlszeile oder API

- create-lag (AWS CLI)
- CreateLag (AWS Direct Connect-API)

So beschreiben Sie Ihre LAGs über die Befehlszeile oder API

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

So laden Sie das LOA-CFA über die Befehlszeile oder API herunter

- describe-loa (AWS CLI)

- DescribeLoa (AWS Direct Connect-API)

Nachdem Sie eine LAG erstellt haben, können Sie dieser Verbindungen zuzuordnen oder Verbindungen von dieser LAG trennen. Weitere Informationen finden Sie unter Eine Verbindung mit einer LAG verknüpfen und Die Verknüpfung einer Verbindung mit einer LAG aufheben.

Ihre LAG-Daten anzeigen

Nachdem Sie eine LAG erstellt haben, können Sie ihre Details anzeigen.

Console

So zeigen Sie Informationen über Ihre LAG an

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAG aus, und klicken Sie auf View details (Details anzeigen).
4. Sie können Informationen zur LAG anzeigen, wie z. B. die ID und der AWS Direct Connect-Endpunkt, an dem die Verbindungen enden.

Command line

Anzeigen von Informationen zu Ihrer LAG Volume mithilfe der Befehlszeile oder API

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

Eine LAG aktualisieren

Sie können die folgenden Link Aggregation Group (LAG)-Attribute aktualisieren:

- Den Namen der LAG.
- Den Wert der Mindestanzahl an Verbindungen, die für den Betrieb der LAG selbst erforderlich sind.
- Den MACsec-Verschlüsselungsmodus der LAG.

  MACsec ist nur auf dedizierten Verbindungen verfügbar.

AWS weist diesen Wert jeder Verbindung zu, die Teil der LAG ist.

Die gültigen Werte sind:

- `should_encrypt`
- `must_encrypt`

  Wenn Sie den Verschlüsselungsmodus auf diesen Wert einstellen, werden die Verbindungen unterbrochen, wenn die Verschlüsselung unterbrochen ist.
- `no_encrypt`

- Die Tags.

> **Note**
>
> Wenn Sie den Schwellenwert für die Mindestanzahl funktionierender Verbindungen anpassen, müssen Sie darauf achten, dass die LAG unter den neuen Wert fällt und nicht mehr betriebsbereit ist.

Console

So aktualisieren Sie eine LAG

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAG aus und klicken Sie dann auf Edit (Bearbeiten).
4. Ändern der LAG

   [Namen ändern] Geben Sie unter LAG Name (LAG-Name) einen neuen LAG-Namen ein.

   [Anpassen der Mindestanzahl an Verbindungen] Geben Sie bei Minimum Links (Min. Verbindungen) die Mindestanzahl funktionierender Verbindungen ein.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.

- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

5. Wählen Sie Edit LAG (LAG bearbeiten) aus.

Command line

So aktualisieren Sie eine LAG über die Befehlszeile oder API

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect-API)

So fügen Sie Tags über die Befehlszeile hinzu und entfernen sie

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Eine Verbindung mit einer LAG verknüpfen

Sie können eine vorhandene Verbindung mit einer LAG verknüpfen. Die Verbindung kann eigenständig oder Bestandteil einer anderen LAG sein. Die Verbindung muss sich auf demselben AWS-Gerät befinden und dieselbe Bandbreite wie die LAG aufweisen. Wenn die Verbindung bereits mit einer anderen LAG verknüpft ist, können Sie keine Neuzuweisung vornehmen, wenn dadurch die ursprüngliche LAG unter den Mindestwert für funktionierende Verbindungen fällt.

Durch die Verknüpfung einer Verbindung mit einer LAG werden die virtuellen Schnittstellen automatisch neu mit der LAG verknüpft.

> **Important**
>
> Die Konnektivität zu AWS über die Verbindung wird während der Verknüpfung unterbrochen.

Console

So verknüpfen Sie eine Verbindung mit einer LAG

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAG aus, und klicken Sie auf View details (Details anzeigen).
4. Wählen Sie unter Connections (Verbindungen) die Option Associate connection (Verbindung zuweisen) aus.
5. Wählen Sie für Connection (Verbindung) die Direct Connect-Verbindung aus, die für die LAG verwendet werden soll.
6. Wählen Sie Associate Connection (Verbindung zuweisen) aus.

Command line

So verknüpfen Sie eine Verbindung über die Befehlszeile oder API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (AWS Direct Connect-API)

Die Verknüpfung einer Verbindung mit einer LAG aufheben

Konvertieren einer Verbindung zu Standalone durch Trennen von einer LAG. Sie können die Verknüpfung nicht aufheben, wenn dies dazu führen würde, dass die LAG unter den Mindestwert funktionierender Verbindungen fallen würde.

Die Aufhebung einer Verknüpfung zwischen Verbindung und LAG führt nicht automatisch zur Aufhebung der Verknüpfungen von virtuellen Schnittstellen.

> **Important**
>
> Ihre Verbindung mit AWS wird während der Aufhebung der Verknüpfung unterbrochen.

Console

So heben Sie die Verknüpfung einer Verbindung mit einer LAG auf

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Bereich LAGs aus.
3. Wählen Sie die LAG aus, und klicken Sie auf View details (Details anzeigen).
4. Wählen Sie unter Connections (Verbindungen) die Verbindung aus der Liste der verfügbaren Verbindungen aus, und klicken Sie auf Disassociate (Verknüpfung aufheben).
5. Wählen Sie im Bestätigungsdialogfeld Disassociate (Aufheben) aus.

Command line

So heben Sie die Verknüpfung einer Verbindung über die Befehlszeile oder API auf

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (AWS Direct Connect-API)

Ein MACsec CKN/CAK einer LAG zuordnen

Nachdem Sie die LAG erstellt haben, die MACsec unterstützt, können Sie der Verbindung ein CKN/CAK zuordnen.

> **Note**
>
> Sie können einen geheimen MACsec-Schlüssel nicht ändern, nachdem Sie ihn einer LAG zugeordnet haben. Wenn Sie den Schlüssel ändern müssen, trennen Sie den Schlüssel von der Verbindung und ordnen Sie der Verbindung dann einen neuen Schlüssel zu. Informationen zum Entfernen einer Zuordnung finden Sie unter the section called “Die Zuordnung zwischen allen MACsec-Schlüsseln und LAGs entfernen”.

Console

So ordnen Sie einen MACsec-Schlüssel einer LAG zu

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAG aus, und klicken Sie auf View details (Details anzeigen).
4. Wählen Sie Associate key (Schlüssel zuordnen) aus.
5. Geben Sie den MACsec-Schlüssel ein.

   [Das CAK/CKN-Paar verwenden] Wählen Sie Key Pair (Schlüsselpaar) aus und gehen Sie dann wie folgt vor:

   - Geben Sie für Connectivity Association Key (CAK) den CAK ein.
   - Geben Sie für Connectivity Association Key Name (CKN) den CKN ein.

   [Den geheimen Schlüssel verwenden] Wählen Sie Existing Secret Manager Secret (Vorhandenes Secret-Manager-Secret) dann für Secret den geheimen MACsec-Schlüssel aus.
6. Wählen Sie Associate key (Schlüssel zuordnen) aus.

Command line

So ordnen Sie einen MACsec-Schlüssel einer LAG zu

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

Die Zuordnung zwischen allen MACsec-Schlüsseln und LAGs entfernen

Sie können die Zuordnung zwischen der LAG und dem MACsec-Schlüssel entfernen.

Console

So entfernen Sie eine Zuordnung zwischen einer LAG und einem MACsec-Schlüssel

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAG aus, und klicken Sie auf View details (Details anzeigen).
4. Wählen Sie das zu entfernende MACsec-Secret aus, und klicken Sie dann auf Disassociate key (Schlüssel trennen).
5. Geben Sie im Bestätigungsdialogfeld disassociate (Trennen) ein und wählen Sie dann Disassociate (Trennen) aus.

Command line

So entfernen Sie eine Zuordnung zwischen einer LAG und einem MACsec-Schlüssel

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

LAGs löschen

Wenn Sie LAGs nicht mehr benötigen, können Sie sie löschen. Eine LAG kann nicht gelöscht werden, wenn virtuelle Schnittstellen mit ihr verknüpft sind. Sie müssen zuerst die virtuellen Schnittstellen löschen oder diese einer anderen LAG oder Verbindung zuweisen. Das Löschen einer LAG heißt nicht, dass die Verbindungen in der LAG gelöscht werden. Dies müssen Sie selbst erledigen. Weitere Informationen finden Sie unter Verbindungen löschen.

Console

So löschen Sie eine LAG

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich LAGs aus.
3. Wählen Sie die LAGs aus, und klicken Sie auf Delete (Löschen).
4. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).

Command line

So löschen Sie eine LAG über die Befehlszeile oder API

- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect-API)

Arbeiten mit Direct Connect-Gateways

Sie können mit AWS Direct Connect Gateways über die Amazon VPC-Konsole oder die arbeiten. AWS CLI

Inhalt

Direct Connect-Gateways

Verwenden Sie AWS Direct Connect das Gateway, um Ihre VPCs zu verbinden. Sie ordnen ein AWS Direct Connect -Gateway einem der folgenden Gateways zu:

- Einem Transit Gateway, wenn sich mehrere VPCs in derselben Region befinden
- Ein Virtual Private Gateway

Sie können auch ein Virtual Private Gateway verwenden, um Ihre Local Zone zu erweitern. Diese Konfiguration ermöglicht es der VPC, die mit der Local Zone verknüpft ist, eine Verbindung zu einem Direct-Connect-Gateway herzustellen. Das Direct-Connect-Gateway verbindet sich mit einem Direct-Connect-Standort in einer Region. Das lokale Rechenzentrum verfügt über eine Direct-Connect-Verbindung mit dem Direct-Connect-Standort. Weitere Informationen finden Sie unter Zugreifen auf Local Zones mithilfe eines Direct-Connect-Gateways im Amazon-VPC-Benutzerhandbuch.

Ein Direct Connect-Gateway ist eine global verfügbare Ressource. Sie können mit einem Direct-Connect-Gateway eine Verbindung zu jeder Region weltweit herstellen. Dies schließt die Regionen AWS Chinas ein, schließt sie AWS GovCloud (US) jedoch nicht ein.

Kunden, die Direct Connect mit VPCs verwenden, die derzeit eine übergeordnete Availability Zone umgehen, können ihre Direct-Connect-Verbindungen oder virtuellen Schnittstellen nicht migrieren.

Im Folgenden werden Szenarien beschrieben, in denen Sie ein Direct-Connect-Gateway verwenden können.

Ein Direct Connect-Gateway lässt nicht zu, dass Gateway-Zuordnungen, die sich auf demselben Direct Connect-Gateway befinden, einander Datenverkehr senden (z. B. ein Virtual Private Gateway an ein anderes Virtual Private Gateway). Eine Ausnahme von dieser Regel, die im November 2021 eingeführt wurde, ist, wenn ein Supernet über zwei oder mehr VPCs angekündigt wird, deren angeschlossene Virtual Private Gateways (VGW) demselben Direct-Connect-Gateway und derselben virtuellen Schnittstelle zugeordnet sind. In diesem Fall können VPCs über den Direct-Connect-Endpunkt miteinander kommunizieren. Wenn Sie beispielsweise ein Supernet (z. B. 10.0.0.0/8 oder 0.0.0.0/0) ankündigen, das sich mit den an ein Direct-Connect-Gateway angeschlossenen VPCs (z. B. 10.0.0.0/24 und 10.0.1.0/24) überschneidet und sich auf derselben virtuellen Schnittstelle befindet, können die VPCs von Ihrem lokalen Netzwerk aus miteinander kommunizieren.

Wenn Sie die VPC-zu-VPC-Kommunikation innerhalb eines Direct-Connect-Gateways blockieren möchten, gehen Sie wie folgt vor:

1. Richten Sie Sicherheitsgruppen auf den Instances und anderen Ressourcen in der VPC ein, um den Verkehr zwischen VPCs zu blockieren, und verwenden Sie diese auch als Teil der Standardsicherheitsgruppe in der VPC.
2. Vermeiden Sie es, in Ihrem lokalen Netzwerk ein Supernet anzukündigen, das sich mit Ihren VPCs überschneidet. Stattdessen können Sie spezifischere Routen in Ihrem On-Premises-Netzwerk ankündigen, die sich nicht mit Ihren VPCs überschneiden.
3. Stellen Sie für jede VPC, die Sie mit Ihrem On-Premises-Netzwerk verbinden möchten, ein einzelnes Direct-Connect-Gateway bereit, anstatt dasselbe Direct-Connect-Gateway für mehrere VPCs zu verwenden. Anstatt beispielsweise ein einziges Direct-Connect-Gateway für Ihre Entwicklungs- und Produktions-VPCs zu verwenden, verwenden Sie separate Direct-Connect-Gateways für jede dieser VPCs.

Ein Direct-Connect-Gateway verhindert nicht, dass Datenverkehr von einer Gateway-Zuordnung zurück an die Gateway-Zuordnung selbst gesendet wird, wenn es beispielsweise eine On-Premise-Supernetroute gibt, die die Präfixe der Gateway-Zuordnung enthält. Wenn Sie eine Konfiguration mit mehreren VPCs haben, die mit Transit Gateways verbunden sind, die demselben Direct-Connect-Gateway zugeordnet sind, können die VPCs kommunizieren. Um zu verhindern, dass die VPCs kommunizieren, ordnen Sie den VPC-Anhängen, für die die Blackhole-Option aktiviert ist, eine Routing-Tabelle zu.

Im Folgenden werden Szenarien beschrieben, in denen Sie ein Direct-Connect-Gateway verwenden können.

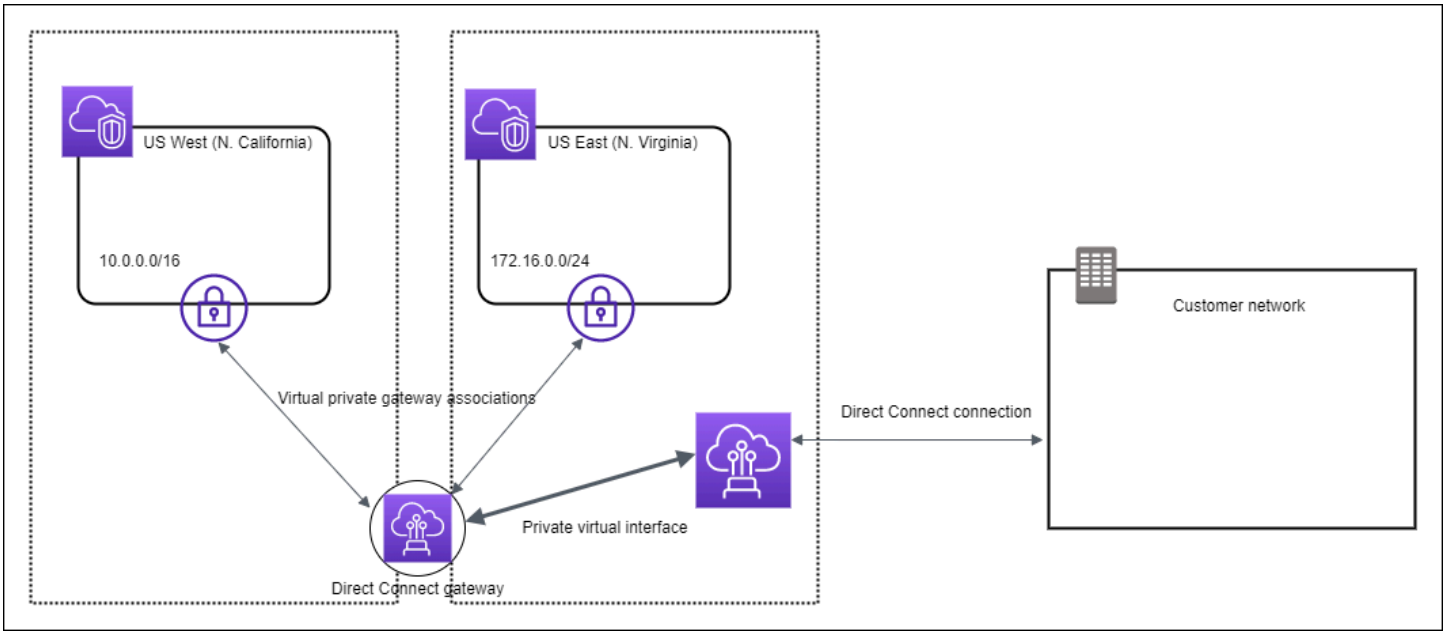
Szenarien

- Virtual Private Gateway-Zuordnungen
- Kontenübergreifende Virtual Private Gateway-Zuordnungen
- Transit-Gateway-Zuordnungen
- Kontenübergreifende Transit Gateway-Zuordnungen
- Erstellen eines Direct Connect-Gateways
- Löschen von Direct Connect-Gateways
- Migrieren von einem Virtual Private Gateway zu einem Direct Connect-Gateway

Virtual Private Gateway-Zuordnungen

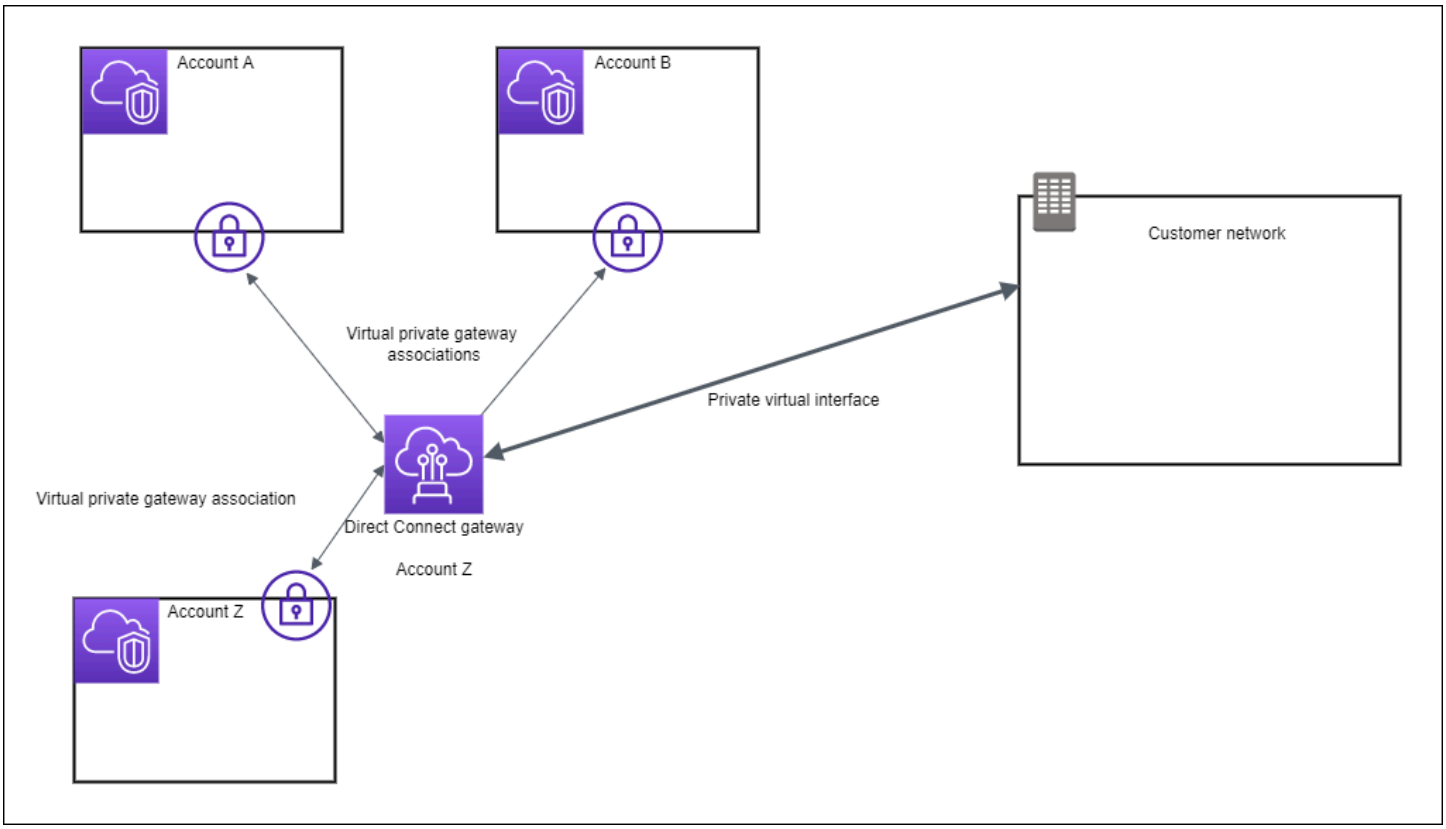
In der folgenden Abbildung können Sie mit dem Direct-Connect-Gateway Ihre AWS Direct Connect -Verbindung in der Region USA Ost (Nord-Virginia) verwenden, um auf VPCs in Ihrem Konto sowohl in den Regionen USA Ost (Nord-Virginia) als auch USA West (Nordkalifornien) zuzugreifen.

Jede VPC verfügt über ein Virtual Private Gateway, das über eine Virtual-Private-Gateway-Zuordnung eine Verbindung zum Direct-Connect-Gateway herstellt. Das Direct Connect-Gateway verwendet eine private virtuelle Schnittstelle für die Verbindung zum AWS Direct Connect Standort. Es besteht eine AWS Direct Connect -Verbindung vom Standort zum Kunden-Rechenzentrum.



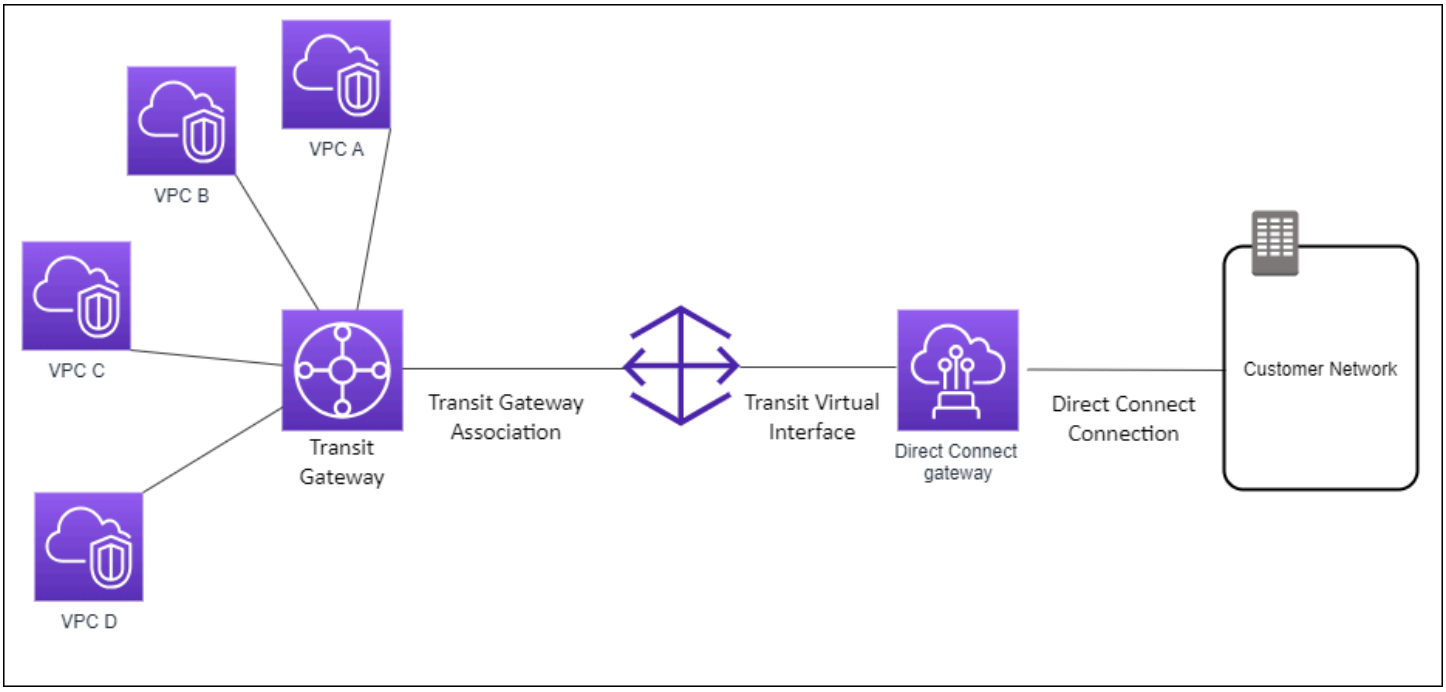
Kontenübergreifende Virtual Private Gateway-Zuordnungen

Beispiel: Szenario mit einem Direct Connect-Gateway-Eigentümer (Konto Z), dem das Direct Connect-Gateway gehört. Konto A und Konto B möchten das Direct Connect-Gateway verwenden. Konto A und Konto B senden jeweils einen Verknüpfungsvorschlag an Konto Z. Dieses akzeptiert die Verknüpfungsvorschläge und kann optional auch die Präfixe aktualisieren, die vom Virtual Private Gateway von Konto A oder Konto B erlaubt werden. Nachdem Konto Z die Vorschläge akzeptiert hat, können Konto A und Konto B den Datenverkehr aus ihrem Virtual Private Gateway zum Direct Connect-Gateway leiten. Konto Z ist auch für das Routing an die Kunden verantwortlich, da Konto Z das Gateway gehört.



Transit-Gateway-Zuordnungen

In der folgenden Grafik ist dargestellt, wie das Direct-Connect-Gateway es Ihnen ermöglicht, eine einzige Verbindung zu Ihrer Direct-Connect-Verbindung zu erstellen, die dann von allen Ihren VPCs genutzt werden kann.



Die Lösung umfasst die folgenden Komponenten:

- Das Transit Gateway hat drei VPC-Anhänge.
- Ein Direct-Connect-Gateway
- Eine Zuordnung zwischen dem Direct-Connect-Gateway und dem Transit Gateway.
- Eine dem Direct-Connect-Gateway angefügte virtuelle Transit-Schnittstelle

Diese Konfiguration bietet die folgenden Vorteile. Sie haben folgende Möglichkeiten:

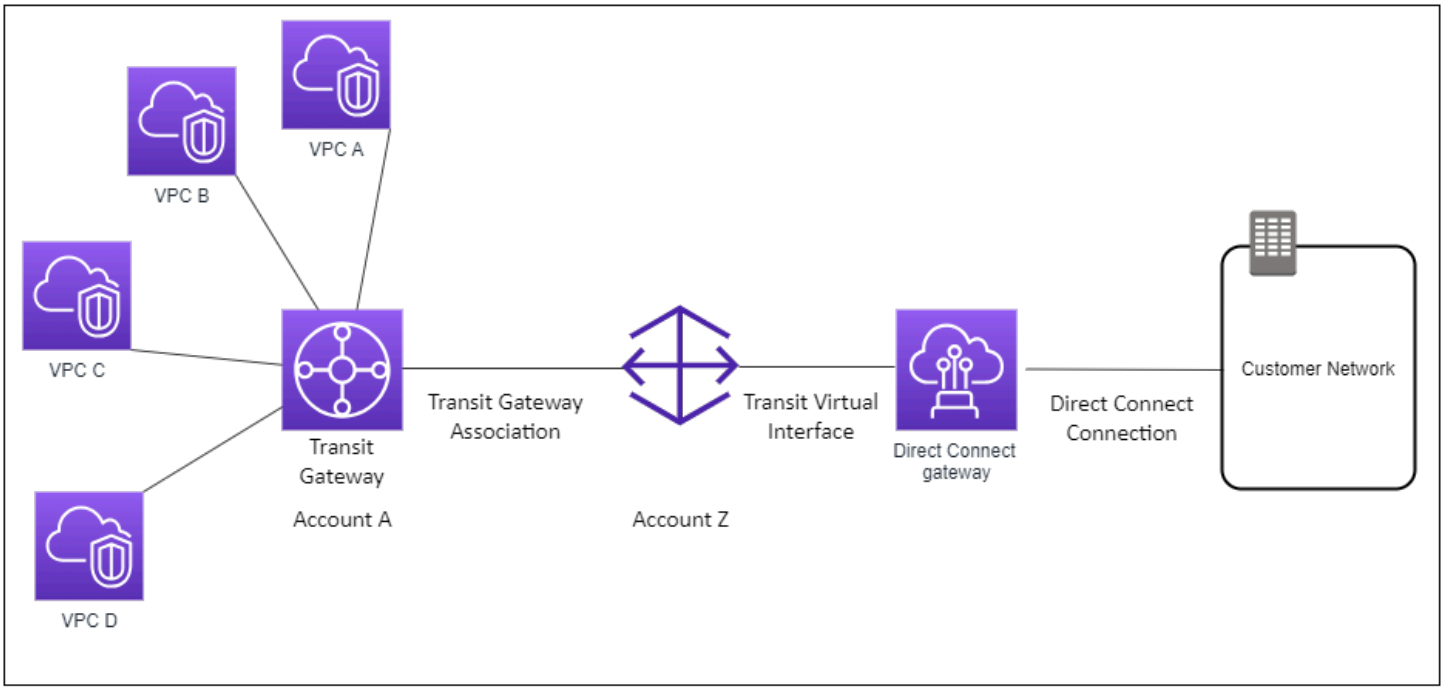
- Verwaltung einer einzigen Verbindung für mehrere VPCs oder VPNs, die sich in der gleichen Region befinden
- Kündigen Sie Präfixe von lokal zu AWS und von AWS zu lokal an.

Weitere Informationen zur Konfiguration von Transit Gateways finden Sie unter Arbeiten mit Transit Gateways im Handbuch zu Transit Gateways von Amazon VPC.

Kontenübergreifende Transit Gateway-Zuordnungen

Beispiel: Szenario mit einem Direct Connect-Gateway-Eigentümer (Konto Z), dem das Direct Connect-Gateway gehört. Konto A ist Eigentümer des Transit Gateways und möchte das Direct-Connect-Gateway verwenden. Konto Z akzeptiert die Zuordnungsvorschläge und kann optional

aktualisieren, welche Präfixe vom Transit Gateway von Konto A zulässig sind. Nachdem Konto Z die Vorschläge akzeptiert hat, können die dem Transit Gateway zugeordneten VPCs den Datenverkehr vom Transit Gateway zum Direct-Connect-Gateway weiterleiten. Konto Z ist auch für das Routing an die Kunden verantwortlich, da Konto Z das Gateway gehört.



Inhalt

- Erstellen eines Direct Connect-Gateways
- Löschen von Direct Connect-Gateways
- Migrieren von einem Virtual Private Gateway zu einem Direct Connect-Gateway

Erstellen eines Direct Connect-Gateways

Sie können ein Direct-Connect-Gateway in einer beliebigen unterstützten Region erstellen.

So erstellen Sie ein Direct Connect-Gateway

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect Gateways aus.
3. Wählen Sie Create Direct Connect gateway (Direct Connect-Gateway erstellen) aus.

4. Geben Sie die folgenden Informationen ein und wählen Sie Create Direct Connect gateway (Direct Connect-Gateway erstellen).
   - Name: Geben Sie einen Namen ein, der Ihnen bei der Identifizierung des Direct Connect-Gateways hilft.
   - ASN der Amazon-Seite: Geben Sie die ASN für die Amazon-Seite der BGP-Sitzung an. Die ASN muss zwischen 64.512 und 65.534 oder 4.200.000.000 und 4.294.967.294 liegen.
   - Virtual private Gateway (Virtual Private Gateway): Um ein Virtual Private Gateway zu verknüpfen, wählen Sie es aus.

So erstellen Sie ein Direct Connect-Gateway über die Befehlszeile oder API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Löschen von Direct Connect-Gateways

Wenn Sie ein Direct Connect-Gateway nicht mehr benötigen, können Sie es löschen. Sie müssen zunächst die Zuordnung aller Virtual Private Gateways aufheben und die angefügte private virtuelle Schnittstelle löschen.

So löschen Sie ein Direct Connect-Gateway

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect Gateways aus.
3. Wählen Sie die Gateways aus und klicken Sie auf Delete (Löschen).

So löschen Sie ein Direct Connect-Gateway über die Befehlszeile oder API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

Migrieren von einem Virtual Private Gateway zu einem Direct Connect-Gateway

Wenn Sie ein Virtual Private Gateway an eine virtuelle Schnittstelle angefügt haben und zu einem Direct Connect-Gateway migrieren möchten, führen Sie die folgenden Schritte aus:

So migrieren Sie zu einem Direct Connect-Gateway

1. Erstellen Sie ein Direct Connect-Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Direct Connect-Gateways”.
2. Erstellen Sie eine virtuelle Schnittstelle für das Direct Connect-Gateway. Weitere Informationen finden Sie unter the section called “Eine virtuelle Schnittstelle erstellen”.
3. Verknüpfen Sie jedes Virtual Private Gateway mit dem Direct Connect-Gateway. Weitere Informationen finden Sie unter the section called “Zuordnen und Aufheben der Zuordnung von Virtual Private Gateways”.
4. Löschen Sie die virtuelle Schnittstelle, die dem Virtual Private Gateway zugeordnet war. Weitere Informationen finden Sie unter the section called “Virtuelle Schnittstellen entfernen”.

Virtual Private Gateway-Zuordnungen

Mit einem AWS Direct Connect -Gateway können Sie Ihre AWS Direct Connect -Verbindung über eine private virtuelle Schnittstelle mit mindestens einer VPC in einem beliebigen Konto in derselben oder einer anderen Region herstellen. Sie ordnen ein Direct Connect-Gateway dem Virtual Private Gateway für die VPC zu. Anschließend erstellen Sie eine private virtuelle Schnittstelle für Ihre AWS Direct Connect Verbindung zum Direct Connect-Gateway. Sie können Ihrem Direct Connect-Gateway mehrere private virtuelle Schnittstellen anfügen.

Die folgenden Regeln gelten für Virtual-Private-Gateway-Zuordnungen:

- Aktivieren Sie Route Propagation erst, nachdem Sie ein virtuelles Gateway mit einem Direct Connect-Gateway verknüpft haben. Wenn Sie die Route-Propagierung aktivieren, bevor Sie die Gateways zugeordnet haben, werden Routen möglicherweise falsch weitergegeben.
- Bei der Erstellung und Verwendung von Direct Connect-Gateways gibt es Grenzen. Weitere Informationen finden Sie unter Kontingente.
- Sie können ein Direct-Connect-Gateway an ein Virtual Private Gateway anfügen, wenn das Direct-Connect-Gateway bereits einem Transit Gateway zugeordnet ist.

- Die VPCs, mit denen Sie über ein Direct Connect-Gateway eine Verbindung herstellen, dürfen über keine überlappenden CIDR-Blöcke verfügen. Wenn Sie einer VPC, die einem Direct Connect-Gateway zugewiesen ist, ein IPv4-CIDR-Block hinzufügen, vergewissern Sie sich, dass der CIDR-Block nicht mit einem bestehenden CIDR-Block für eine andere VPC überlappt. Weitere Informationen finden Sie unter Hinzufügen von IPv4 CIDR-Blöcken zu einer VPC in Amazon VPC-Benutzerhandbuch.
- Sie können keine öffentliche virtuelle Schnittstelle für ein Direct Connect-Gateway erstellen.
- Ein Direct-Connect-Gateway unterstützt nur die Kommunikation zwischen angefügten privaten virtuellen Schnittstellen und den zugehörigen Virtual Private Gateways, und kann ein Virtual Private Gateway in einem anderen privaten Gateway aktivieren. Folgender Datenverkehr wird nicht unterstützt:
  - Die direkte Kommunikation zwischen den VPCs, die einem einzelnen Direct Connect-Gateway zugewiesen sind. Dies umfasst Datenverkehr von einer VPC zu einer anderen, indem ein Hairpin über ein On-Premises-Netzwerk über einen einzelnen Direct-Connect-Gateway verwendet wird.
  - Die direkte Kommunikation zwischen den virtuellen Schnittstellen, die einem einzelnen Direct Connect-Gateway angefügt sind.
  - Die direkte Kommunikation zwischen einer virtuellen Schnittstelle, die einem einzelnen Direct Connect-Gateway angefügt ist, und einer VPN-Verbindung auf einem Virtual Private Gateway, das demselben Direct Connect-Gateway zugewiesen ist.
- Sie können ein Virtual Private Gateway höchstens einem Direct Connect-Gateway zuweisen und maximal einem Direct Connect-Gateway eine private virtuelle Schnittstelle anfügen.
- Ein Virtual Private Gateway, das Sie einem Direct Connect-Gateway zuweisen, muss einer VPC angefügt werden.
- Ein Zuordnungsvorschlag für ein Virtual Private Gateway läuft 7 Tage nach seiner Erstellung ab.
- Ein angenommener Vorschlag für ein Virtual Private Gateway oder ein gelöschter Vorschlag für ein Virtual Private Gateway bleibt 3 Tage lang sichtbar.
- Ein Virtual Private Gateway kann einem Direct Connect-Gateway und einer virtuellen Schnittstelle zugewiesen werden.
- Wenn Sie ein Virtual Private Gateway von einer VPC trennen, wird das virtuelle private Gateway auch von einem Direct-Connect-Gateway getrennt.

Um Ihre AWS Direct Connect Verbindung nur mit einer VPC in derselben Region zu verbinden, können Sie ein Direct Connect-Gateway erstellen. Alternativ können Sie eine private virtuelle

Schnittstelle erstellen und diese dem Virtual Private Gateway für die VPC anfügen. Weitere Informationen finden Sie unter Eine private virtuelle Schnittstelle erstellen und VPN CloudHub.

Um Ihre AWS Direct Connect Verbindung mit einer VPC in einem anderen Konto zu verwenden, können Sie eine gehostete private virtuelle Schnittstelle für dieses Konto erstellen. Wenn der Eigentümer des anderen Kontos die gehostete virtuelle Schnittstelle akzeptiert, kann er diese entweder an ein Virtual Private Gateway oder an ein Direct Connect-Gateway in seinem Konto anhängen. Weitere Informationen finden Sie unter AWS Direct Connect virtuelle Schnittstellen.

Inhalt

Erstellen eines Virtual Private Gateway

Das Virtual Private Gateway muss der VPC angefügt sein, mit der eine Verbindung hergestellt werden soll.

> **Note**
>
> Wenn Sie planen, das Virtual Private Gateway für eine Direct-Connect-Gateway- und eine dynamische VPN-Verbindung zu nutzen, legen Sie Sie für den ASN auf dem Virtual Private Gateway auf den Wert fest, den Sie für die VPN-Verbindung benötigen. Andernfalls kann der ASN auf dem virtuellen privaten Gateway auf einen beliebigen zulässigen Wert gesetzt werden. Der Direct Connect-Gateway bewirbt alle verbundenen VPCs über den ihm zugewiesenen ASN.

Nachdem Sie das Virtual Private Gateway erstellt haben, müssen Sie es Ihrer VPC zuweisen.

So erstellen Sie ein Virtual Private Gateway und weisen Sie es Ihrer VPC zu

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.

2. Wählen Sie im Navigationsbereich Virtual Private Gateways und anschließend Create Virtual Private Gateway (Virtual Private Gateway erstellen) aus.
3. (Optional) Geben Sie einen Namen für Ihr Virtual Private Gateway ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
4. Übernehmen Sie für ASN die Standardeinstellung, um die standardmäßige Amazon ASN zu verwenden. Andernfalls wählen Sie Custom ASN (Benutzerdefinierte ASN) und geben Sie einen Wert ein. Für eine 16-Bit-ASN muss der Wert im Bereich zwischen 64512 und 65534 liegen. Für eine 32-Bit-ASN muss der Wert im Bereich zwischen 4200000000 und 4294967294 liegen.
5. Wählen Sie Create Virtual Private Gateway.
6. Wählen Sie das Virtual Private Gateway aus, das Sie eben erstellt haben, und wählen Sie anschließend Actions, Attach to VPC.
7. Markieren Sie Ihr VPC in der Liste, und wählen Sie Yes, Attach.

So erstellen Sie ein Virtual Private Gateway über die Befehlszeile oder API

- CreateVpnGateway(Amazon EC2 EC2-Abfrage-API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

So fügen Sie ein Virtual Private Gateway unter Verwendung der Befehlszeile oder API einer VPC an

- AttachVpnGateway(Amazon EC2 EC2-Abfrage-API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Zuordnen und Aufheben der Zuordnung von Virtual Private Gateways

Sie können ein Virtual Private Gateway mit einem Direct-Connect-Gateway verknüpfen oder die Verknüpfung aufheben. Der Kontoinhaber des Virtual Private Gateway führt diese Vorgänge durch.

So ordnen Sie ein Virtual Private Gateway zu

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.

2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct-Connect-Gateways) und anschließend das Direct-Connect-Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Gateway associations (Gateway-Zuordnungen) und dann Associate gateway (Gateway zuordnen) aus.
5. Wählen Sie bei Gateways die zuzuordnenden Virtual Private Gateways und anschließend Associate gateway (Gateway zuordnen) aus.

Sie können alle Virtual Private Gateways, die dem Direct Connect-Gateway zugeordnet sind, anzeigen, indem Sie Gateway associations (Gateway-Zuordnungen) auswählen.

So heben Sie die Zuordnung eines Virtual Private Gateways auf

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) und anschließend das Direct Connect-Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Gateway associations (Gateway-Zuordnungen) und wählen Sie dann das Virtual Private Gateway aus.
5. Wählen Sie Disassociate (Zuordnung aufheben) aus.

So weisen Sie ein Virtual Private Gateway über die Befehlszeile oder API zu

- create-direct-connect-gateway-association ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

So zeigen Sie die Virtual Private Gateways mit einem Direct Connect-Gateway über die Befehlszeile oder API an

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

So trennen Sie ein Virtual Private Gateway über die Befehlszeile oder API

- delete-direct-connect-gateway-Assoziation ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Erstellen einer privaten virtuellen Schnittstelle für das Direct Connect-Gateway

Um Ihre AWS Direct Connect Verbindung mit der Remote-VPC zu verbinden, müssen Sie eine private virtuelle Schnittstelle für Ihre Verbindung erstellen. Geben Sie das Direct Connect-Gateway an, mit dem die Verbindung hergestellt wird.

> **Note**
>
> Wenn Sie eine gehostete private virtuelle Schnittstelle akzeptieren, können Sie sie mit einem Direct Connect-Gateway in Ihrem Konto verknüpfen. Weitere Informationen finden Sie unter Eine gehostete virtuelle Schnittstelle akzeptieren.

So stellen Sie eine private virtuelle Schnittstelle für ein Direct Connect-Gateway bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) die Option Private (Privat) aus.
5. Führen Sie unter Private virtual interface settings (Einstellungen für private virtuelle Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Wählen Sie unter Besitzer der virtuellen Schnittstelle die Option Mein AWS Konto aus, wenn die virtuelle Schnittstelle für Ihr AWS Konto bestimmt ist.

d. Wählen Sie für Direct Connect Gateway das Direct Connect-Gateway aus.

e. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

f. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

   Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung (nicht RFC 1918) verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

      [IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

   b. Um den MTU (maximale Übertragungseinheit)-Wert von 1 500 (Standard) in 9 001 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 9 001) (Jumbo-MTU [MTU-Größe 9 001]) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

   [Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Nachdem Sie die virtuelle Schnittstelle erstellt haben, können Sie die Router-Konfiguration für Ihr Gerät herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine private virtuelle Schnittstelle über die Befehlszeile oder API

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

So zeigen Sie die virtuellen Schnittstellen an, die einem Direct Connect-Gateway über die Befehlszeile oder API angefügt sind

- describe-direct-connect-gateway-anhänge ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Kontoübergreifendes Zuordnen eines Virtual Private Gateway

Sie können ein Direct Connect-Gateway einem virtuellen privaten Gateway zuordnen, das einem beliebigen AWS Konto gehört. Das Direct Connect-Gateway kann ein vorhandenes Gateway sein oder Sie können ein neues Gateway erstellen. Der Eigentümer des Virtual Private Gateway erstellt einen Verknüpfungsvorschlag, den der Eigner des Direct Connect-Gateway akzeptieren muss.

Ein Verknüpfungsvorschlag kann Präfixe enthalten, die vom Virtual Private Gateway erlaubt werden. Der Eigentümer des Direct Connect-Gateway kann optional angeforderte Präfixe im Verknüpfungsvorschlag aufheben.

Zulässige Präfixe

Wenn Sie ein Virtual Private Gateway mit einem Direct Connect-Gateway verknüpfen, geben Sie eine Liste mit Amazon VPC-Präfixen zur Ankündigung beim Direct Connect-Gateway an. Die Präfixliste fungiert als Filter, der die Ankündigung der gleichen oder kleineren CIDRs beim Direct Connect-Gateway erlaubt. Sie müssen Allowed prefixes (Zulässige Präfixe) auf einen Bereich festlegen, der mindestens genauso groß wie der VPC-CIDR ist, da wir den gesamten VPC-CIDR auf dem Virtual Private Gateway bereitstellen.

Beispiel: Fall, bei dem der VPC-CIDR 10.0.0.0/16 lautet. Sie können für Allowed prefixes (Zulässige Präfixe) 10.0.0.0/16 (der VPC-CIDR-Wert) oder 10.0.0.0/15 (ein größerer Wert als der VPC-CIDR) festlegen.

Alle virtuellen Schnittstellen innerhalb von Netzwerkpräfixen, die über Direct Connect angekündigt werden, werden nur an Transit-Gateways in verschiedenen Regionen weitergegeben, nicht innerhalb derselben Region. Weitere Informationen dazu, wie zulässige Präfixe mit Virtual Private Gateways und Transit Gateways interagieren, finden Sie unter the section called “Interaktionen zulässiger Präfixe”.

Aufgaben

- Erstellen eines Verknüpfungsvorschlags
- Akzeptieren oder Ablehnen eines Verknüpfungsvorschlags
- Aktualisieren der zulässigen Präfixe für eine Zuordnung
- Löschen eines Verknüpfungsvorschlags

Erstellen eines Verknüpfungsvorschlags

Wenn Sie der Eigentümer des Virtual Private Gateway sind, müssen Sie einen Verknüpfungsvorschlag erstellen. Das Virtual Private Gateway muss mit einer VPC in Ihrem AWS Konto verbunden sein. Der Besitzer des Direct Connect-Gateways muss die ID des Direct Connect-Gateways und die ID seines AWS Kontos teilen. Nachdem Sie den Vorschlag erstellt haben, muss der Eigentümer des Direct Connect-Gateway ihn akzeptieren, damit Sie Zugriff auf das lokale Netzwerk über AWS Direct Connect erhalten.

So erstellen Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.

2. Wählen Sie im Navigationsbereich Virtual private gateways (Virtual Private Gateways) und anschließend das Virtual Private Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Direct Connect gateway associations (Direct Connect-Gateway-Verknüpfungen) und Associate Direct Connect gateway (Direct Connect-Gateway verknüpfen).
5. Wählen Sie unter Association account type (Zuordnungskontotyp) fürAccount owner (Konto-Eigentümer) die Option Another account (Anderes Konto).
6. Geben Sie für Direct Connect gateway owner (Eigentümer des Direct-Connect-Gateways) die ID des AWS -Kontos ein, das der Eigentümer des Direct-Connect-Gateways ist.
7. Gehen Sie unter Association settings (Zuordnungseinstellungen) wie folgt vor:
   a. Geben Sie für Direct Connect gateway ID (Direct Connect-Gateway-ID) die ID des Direct Connect-Gateway ein.
   b. Geben Sie als Besitzer des Direct Connect-Gateways die ID des AWS Kontos ein, dem das Direct Connect-Gateway für die Zuordnung gehört.
   c. (Optional) Um eine Liste mit Präfixen festzulegen, die vom Virtual Private Gateway erlaubt werden, fügen Sie die Präfixe unter Allowed prefixes (Zulässige Präfixe) durch Kommas getrennt hinzu oder geben diese in separaten Zeilen ein.
8. Wählen Sie Associate Direct Connect gateway (Direct Connect-Gateway zuordnen).

So erstellen Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API

- create-direct-connect-gateway-assoziation-propos ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Akzeptieren oder Ablehnen eines Verknüpfungsvorschlags

Wenn Sie Eigentümer des Direct Connect-Gateway sind, müssen Sie den Zuordnungsvorschlag akzeptieren, um die Zuordnung zu erstellen. Ansonsten können Sie den Verknüpfungsvorschlag ablehnen.

So akzeptieren Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.

2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) aus.
3. Wählen Sie das Direct Connect-Gateway mit den ausstehenden Vorschlägen aus, und klicken Sie dann auf View details (Details anzeigen).
4. Wählen Sie auf der Registerkarte Pending proposals (Ausstehende Vorschläge) den Vorschlag aus, und klicken Sie auf Accept proposal (Vorschlag akzeptieren).
5. (Optional) Um eine Liste mit Präfixen festzulegen, die vom Virtual Private Gateway erlaubt werden, fügen Sie die Präfixe unter Allowed prefixes (Zulässige Präfixe) durch Kommas getrennt hinzu oder geben diese in separaten Zeilen ein.
6. Wählen Sie Accept proposal (Vorschlag akzeptieren).

So lehnen Sie einen Zuordnungsvorschlag ab

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) aus.
3. Wählen Sie das Direct Connect-Gateway mit den ausstehenden Vorschlägen aus, und klicken Sie dann auf View details (Details anzeigen).
4. Wählen Sie auf der Registerkarte Pending proposals (Ausstehende Vorschläge) das Virtual Private Gateway aus, und klicken Sie auf Reject proposal (Vorschlag ablehnen).
5. Geben Sie im Dialogfeld Reject proposal (Vorschlag ablehnen) „Delete“ (Löschen) ein, und klicken Sie auf Reject proposal (Vorschlag ablehnen).

So zeigen Sie Zuordnungsvorschläge mithilfe der Befehlszeile oder API an

- describe-direct-connect-gateway-association-proposals ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(API)AWS Direct Connect

So akzeptieren Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API

- accept-direct-connect-gateway-assoziationsvorschlag ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

So lehnen Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API ab

- delete-direct-connect-gateway-assoziationsvorschlag ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Aktualisieren der zulässigen Präfixe für eine Zuordnung

Sie können die Präfixe aktualisieren, die vom Virtual Private Gateway über das Direct Connect-Gateway erlaubt sind.

Wenn Sie Eigentümer des Virtual Private Gateway sind, erstellen Sie einen neuen Verknüpfungsvorschlag für das gleiche Direct Connect-Gateway und virtuelle private Gateway; geben Sie dabei die zulässigen Präfixe an.

Wenn Sie Eigentümer des Direct Connect-Gateway sind, aktualisieren Sie die zulässigen Präfixe, wenn Sie den Zuordnungsvorschlag akzeptieren, oder aktualisieren Sie die zulässigen Präfixe für eine vorhandene Zuordnung wie folgt.

So aktualisieren Sie die zulässigen Präfixe für eine vorhandene Zuordnung über die Befehlszeile oder API

- update-direct-connect-gateway-Assoziation ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Löschen eines Verknüpfungsvorschlags

Der Eigentümer des Virtual Private Gateway kann den Verknüpfungsvorschlag für das Direct Connect-Gateway löschen, wenn dieser erst noch akzeptiert werden muss. Nach dem Akzeptieren eines Verknüpfungsvorschlags kann dieser zwar nicht mehr gelöscht werden, Sie können jedoch die Verknüpfung des Virtual Private Gateway vom Direct Connect-Gateway aufheben. Weitere Informationen finden Sie unter the section called “Zuordnen und Aufheben der Zuordnung von Virtual Private Gateways”.

So löschen Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Virtual private gateways (Virtual Private Gateways) und anschließend das Virtual Private Gateway aus.

3. Wählen Sie die Option View details aus.
4. Klicken Sie auf Pending Direct Connect gateway associations (Ausstehende Direct Connect-Gateway-Zuordnungen), wählen Sie die Zuordnung aus, und klicken Sie auf Delete association (Verknüpfung löschen).
5. Geben Sie im Dialogfeld Delete association proposal (Verknüpfungsvorschlag löschen) „Delete“ (Löschen) ein, und klicken Sie auf Delete (Löschen).

So löschen Sie einen ausstehenden Zuordnungsvorschlag mithilfe der Befehlszeile oder API

- delete-direct-connect-gateway-association-propos ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Transit-Gateway-Zuordnungen

Sie können ein AWS Direct Connect -Gateway verwenden, um Ihre AWS Direct Connect -Verbindung über eine virtuelle Transit-Schnittstelle mit den VPCs oder VPNs zu verbinden, die an das Transit Gateway angefügt sind. Sie ordnen ein Direct-Connect-Gateway dem Transit Gateway zu. Erstellen Sie anschließend eine virtuelle Transitschnittstelle für Ihre AWS Direct Connect Verbindung zum Direct Connect-Gateway.

Die folgenden Regeln gelten für Transit-Gateway-Zuordnungen:

- Sie können ein Direct-Connect-Gateway an ein Transit Gateway anfügen, wenn das Direct-Connect-Gateway bereits einem Virtual Private Gateway zugeordnet oder an eine private virtuelle Schnittstelle angefügt ist.
- Bei der Erstellung und Verwendung von Direct Connect-Gateways gibt es Grenzen. Weitere Informationen finden Sie unter Kontingente.
- Ein Direct Connect-Gateway unterstützt die Kommunikation zwischen angeschlossenen virtuellen Transitschnittstellen und zugehörigen Transit-Gateways.
- Wenn Sie eine Verbindung zu mehreren Transit Gateways herstellen, die sich in verschiedenen Regionen befinden, verwenden Sie für jedes Transit Gateway jeweils eindeutige ASNs.
- Alle virtuellen Schnittstellen innerhalb von Netzwerkpräfixen, die über Direct Connect angekündigt werden, werden nur an Transit-Gateways in verschiedenen Regionen, aber nicht innerhalb derselben Region weitergegeben

Zuordnen und Aufheben der Zuordnung von Transit-Gateways

So verknüpfen Sie ein Transit Gateway

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/directconnect/v2/home AWS Direct Connect.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) und anschließend das Direct Connect-Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Gateway associations (Gateway-Zuordnungen) und dann Associate gateway (Gateway zuordnen).
5. Wählen Sie bei Gateways das Transit Gateway aus, das Sie zuordnen möchten.
6. Geben Sie im Feld Allowed prefixes (Zulässige Präfixe) die Präfixe ein (durch ein Komma getrennt oder in einer neuen Zeile), die das Direct-Connect-Gateway dem lokalen Rechenzentrum bekannt gibt. Weitere Informationen zu zulässigen Präfixen finden Sie unter the section called “Interaktionen zulässiger Präfixe”.
7. Associate gateway (Gateway zuordnen) auswählen

Sie können alle Gateways, die dem Direct Connect-Gateway zugeordnet sind, anzeigen, indem Sie Gateway associations (Gateway-Zuordnungen) auswählen.

So verknüpfen Sie ein Transit Gateway

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) und anschließend das Direct Connect-Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Gateway associations (Gateway-Zuordnungen) und danach das Transit-Gateway aus.
5. Wählen Sie Disassociate (Zuordnung aufheben) aus.

So aktualisieren Sie zulässige Präfixe für ein Transit Gateway

Sie können dem Transit Gateway zulässige Präfixe hinzufügen oder entfernen.

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways und dann das Direct-Connect-Gateway aus, für das Sie zulässige Präfixe hinzufügen oder entfernen möchten.
3. Wählen Sie die Registerkarte Gateway assocations (Gateway-Zuordnungen) aus.
4. Wählen Sie das Gateway aus, das Sie ändern möchten, und wählen Sie anschließend Edit (Bearbeiten) aus.
5. Geben Sie im Feld Allowed prefixes (Zulässige Präfixe) die Präfixe ein, die das Direct-Connect-Gateway dem lokalen Rechenzentrum bekannt gibt. Bei mehreren Präfixen trennen Sie jedes Präfix durch ein Komma oder setzen jedes Präfix in eine neue Zeile. Die Präfixe, die Sie hinzufügen, sollten mit den Amazon-VPC-CIDRs für alle Virtual Private Gateway übereinstimmen. Weitere Informationen zu zulässigen Präfixen finden Sie unter the section called “Interaktionen zulässiger Präfixe”.
6. Wählen Sie Edit association.

   Im Bereich Gateway association (Gateway-Zuordnung) wird unter State (Status) die Meldung updating (Aktualisierung läuft) angezeigt. Wenn der Vorgang abgeschlossen ist, wechselt der State (Status) zu associated (Zugeordnet).
7. Wählen Sie Disassociate (Zuordnung aufheben) aus.
8. Wählen Sie erneut Disassociate (Trennen), um zu bestätigen, dass Sie die Verbindung zum Gateway aufheben möchten.

   Im Bereich Gateway association (Gateway-Zuordnung) wird unter State (Status) die Meldung disassociating (Trennung läuft) angezeigt. Wenn der Vorgang abgeschlossen ist, wird eine Bestätigungsmeldung angezeigt und das Gateway wird aus dem Abschnitt entfernt. Dieser Vorgang kann mehrere Minuten oder länger dauern.

So erstellen Sie ein Transit Gateway über die Befehlszeile oder die API

- create-direct-connect-gateway-association ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

So zeigen Sie die einem Direct-Connect-Gateway zugeordneten Transit Gateways über die Befehlszeile oder API an

- describe-direct-connect-gateway-Verbände ()AWS CLI

- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

So trennen Sie ein Transit Gateway über die Befehlszeile oder die API

- delete-direct-connect-gateway-Assoziation ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

So aktualisieren Sie die zulässigen Präfixe für ein Transit Gateway über die Befehlszeile oder die API

- update-direct-connect-gateway-Assoziation ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Erstellen einer virtuellen Transit-Schnittstelle für das Direct Connect-Gateway

Um Ihre AWS Direct Connect Verbindung mit dem Transit-Gateway zu verbinden, müssen Sie eine Transitschnittstelle für Ihre Verbindung erstellen. Geben Sie das Direct Connect-Gateway an, mit dem die Verbindung hergestellt wird.

> **Important**
>
> Wenn Sie Ihr Transit Gateway einem oder mehreren Direct-Connect-Gateways zuordnen, muss die vom Transit Gateway und dem Direct-Connect-Gateway verwendete autonome Systemnummer (ASN) unterschiedlich sein. Wenn Sie beispielsweise die Standard-ASN 64512 sowohl für das Transit Gateway als auch für das Direct-Connect-Gateway verwenden, schlägt die Zuordnungsanfrage fehl.

So stellen Sie eine virtuelle Transit-Schnittstelle für ein Direct Connect-Gateway bereit

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im linken Navigationsbereich Virtual Interfaces (Virtuelle Schnittstellen) aus.
3. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.
4. Wählen Sie unter Virtual interface type (Virtueller Schnittstellentyp) bei Type (Typ) die Option Transit aus.

5. Führen Sie unter Transit virtual interface settings (Einstellungen für virtuelle Transit-Schnittstelle) die folgenden Schritte aus:

   a. Geben Sie unter Virtual interface name (Name der virtuellen Schnittstelle) einen Namen für die virtuelle Schnittstelle ein.

   b. Wählen Sie bei Connection (Verbindung) die Direct Connect-Verbindung, die Sie für diese Schnittstelle verwenden möchten.

   c. Wählen Sie unter Besitzer der virtuellen Schnittstelle die Option Mein AWS Konto aus, wenn die virtuelle Schnittstelle für Ihr AWS Konto bestimmt ist.

   d. Wählen Sie für Direct Connect Gateway das Direct Connect-Gateway aus.

   e. Geben Sie unter VLAN die ID-Nummer für Ihr virtuelles LAN (VLAN) ein.

   f. Geben Sie für BGP ASN die autonome Systenummer des Border Gateway Protocol des lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1 bis 2147483647.

6. Gehen Sie unter Additional Settings (Weitere Einstellungen) wie folgt vor:

   a. Um einen IPv4-BGP- oder IPv6-Peer zu konfigurieren, gehen Sie wie folgt vor:

      [IPv4] Wenn Sie einen IPv4-BGP-Peer konfigurieren, wählen Sie IPv4 und führen Sie einen der folgenden Schritte aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie bei Your router peer IP (Ihre Router-Peer-IP) die IPv4-CIDR-Zieladresse ein, an die Amazon Datenverkehr senden soll.
      - Geben Sie unter Amazon router peer IP (Router-Peer-IP von Amazon) die IPv4-CIDR-Adresse ein, die zum Senden von Datenverkehr an AWS verwendet werden soll.

      > **Important**
      >
      > Wenn Sie die AWS automatische Zuweisung von IPv4-Adressen zulassen, wird ein /29 CIDR von 169.254.0.0/16 IPv4 Link-Local gemäß RFC 3927 für Konnektivität zugewiesen. point-to-point AWS empfiehlt diese Option nicht, wenn Sie die Peer-IP-Adresse des Kundenrouters als Quelle und/oder Ziel für VPC-Verkehr verwenden möchten. Stattdessen sollten Sie RFC 1918 oder eine andere Adressierung (nicht RFC 1918) verwenden und die Adresse selbst angeben.
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

- Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von IPv4-Link-Local-Adressen.

[IPv6] Wenn Sie einen IPv6-BGP-Peer konfigurieren, wählen Sie IPv6. Die Peer-IPv6-Adressen werden automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen. Sie können keine benutzerdefinierten IPv6-Adressen angeben.

b. Um den MTU-Wert (Maximum Transmission Unit, maximale Größe für Übertragungseinheiten) von 1500 (Standard) in 8500 (Jumbo-Frames) zu ändern, wählen Sie Jumbo MTU (MTU size 8500) (Jumbo-MTU (MTU-Größe 8500)) aus.

c. (Optional) Wählen Sie unter Aktivieren die Option Aktiviert aus SiteLink, um direkte Konnektivität zwischen Direct Connect-Points of Presence zu aktivieren.

d. (Optional) Hinzufügen oder Entfernen einer Markierung.

[Markierung hinzufügen] Wählen Sie Add tag (Markierung hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie neben dem Tag die Option Remove tag (Tag löschen) aus.

7. Wählen Sie Create virtual interface (Virtuelle Schnittstelle erstellen) aus.

Nachdem Sie die virtuelle Schnittstelle erstellt haben, können Sie die Router-Konfiguration für Ihr Gerät herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine virtuelle Transit-Schnittstelle über die Befehlszeile oder API

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

So zeigen Sie die virtuellen Schnittstellen an, die einem Direct Connect-Gateway über die Befehlszeile oder API angefügt sind

- describe-direct-connect-gateway-anhänge ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Zuordnen eines Transit-Gateways über Konten hinweg

Sie können ein vorhandenes Direct Connect-Gateway oder ein neues Direct Connect-Gateway einem Transit-Gateway zuordnen, das einem beliebigen AWS Konto gehört. Der Eigentümer des Transit Gateways erstellt einen Zuordnungsvorschlag, den der Eigentümer des Direct-Connect-Gateway akzeptieren muss.

Ein Zuordnungsvorschlag kann Präfixe enthalten, die vom Transit Gateway erlaubt werden. Der Eigentümer des Direct Connect-Gateway kann optional angeforderte Präfixe im Verknüpfungsvorschlag aufheben.

Zulässige Präfixe

Für eine Transit-Gateway-Zuordnung stellen Sie die Liste zulässiger Präfixe auf dem Direct-Connect-Gateway bereit. Die Liste wird verwendet, um den Verkehr vom lokalen Standort zum Transit-Gateway AWS weiterzuleiten, auch wenn den an das Transit-Gateway angeschlossenen VPCs keine zugewiesenen CIDRs zugewiesen wurden. Die Präfixe in der Liste der für das Direct Connect-Gateway zulässigen Präfixe stammen vom Direct Connect-Gateway und werden im lokalen Netzwerk angekündigt. Weitere Informationen dazu, wie zulässige Präfixe mit Transit Gateways und Virtual Private Gateways interagieren, finden Sie unter the section called “Interaktionen zulässiger Präfixe”.

Aufgaben

- Erstellen eines Transit-Gateway-Zuordnungsvorschlags
- Akzeptieren oder Ablehnen eines Transit-Gateway-Zuordnungsvorschlags
- Aktualisieren der zulässigen Präfixe für eine Transit Gateway-Zuordnung
- Löschen eines Transit-Gateway-Zuordnungsvorschlags

Erstellen eines Transit-Gateway-Zuordnungsvorschlags

Wenn Sie das Transit Gateway besitzen, müssen Sie den Zuordnungsvorschlag erstellen. Das Transit-Gateway muss mit einer VPC oder einem VPN in Ihrem AWS Konto verbunden sein. Der Eigentümer des Direct-Connect-Gateways muss die ID des Direct-Connect-Gateways und die ID des AWS -Kontos freigeben. Nachdem Sie den Vorschlag erstellt haben, muss der Eigentümer des Direct Connect-Gateway ihn akzeptieren, damit Sie Zugriff auf das lokale Netzwerk über AWS Direct Connect erhalten.

So erstellen Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Transit Gateway Attachments (Transit-Gateway-Anhänge) aus. Wählen Sie das Transit Gateway aus.
3. Wählen Sie die Option View details aus.
4. Wählen Sie Direct Connect gateway associations (Direct Connect-Gateway-Zuordnungen) und Associate Direct Connect gateway (Direct Connect-Gateway zuordnen).
5. Wählen Sie unter Association account type (Zuordnungskontotyp) fürAccount owner (Konto-Eigentümer) die Option Another account (Anderes Konto).
6. Geben Sie für Direct Connect gateway owner (Rigentümer des Direct-Connect-Gateways) die ID des Kontos ein, das der Eigentümer des Direct-Connect-Gateway ist.
7. Gehen Sie unter Association settings (Zuordnungseinstellungen) wie folgt vor:
   a. Geben Sie für Direct Connect gateway ID (Direct Connect-Gateway-ID) die ID des Direct Connect-Gateway ein.
   b. Geben Sie für Virtual interface owner (Besitzer der virtuellen Schnittstelle die ID des Kontos ein, das Eigentümer der virtuellen Schnittstelle für die Zuordnung ist.
   c. (Optional) Um eine Liste mit Präfixen festzulegen, die vom Transit Gateway erlaubt werden, fügen Sie die Präfixe unter Allowed prefixes (Zulässige Präfixe) durch Kommata getrennt hinzu oder geben diese in separaten Zeilen ein.
8. Wählen Sie Associate Direct Connect gateway (Direct Connect-Gateway zuordnen).

So erstellen Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API

- create-direct-connect-gateway-association-propos ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Akzeptieren oder Ablehnen eines Transit-Gateway-Zuordnungsvorschlags

Wenn Sie Eigentümer des Direct Connect-Gateway sind, müssen Sie den Zuordnungsvorschlag akzeptieren, um die Zuordnung zu erstellen. Sie haben auch die Möglichkeit, den Zuordnungsvorschlag abzulehnen.

So akzeptieren Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) aus.
3. Wählen Sie das Direct Connect-Gateway mit den ausstehenden Vorschlägen aus und klicken Sie dann auf View details (Details anzeigen).
4. Wählen Sie auf der Registerkarte Pending proposals (Ausstehende Vorschläge) den Vorschlag aus und klicken Sie auf Accept proposal (Vorschlag akzeptieren).
5. (Optional) Um eine Liste mit Präfixen festzulegen, die vom Transit Gateway erlaubt werden, fügen Sie die Präfixe unter Allowed prefixes (Zulässige Präfixe) durch Kommata getrennt hinzu oder geben diese in separaten Zeilen ein.
6. Wählen Sie Accept proposal (Vorschlag akzeptieren).

So lehnen Sie einen Zuordnungsvorschlag ab

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) aus.
3. Wählen Sie das Direct Connect-Gateway mit den ausstehenden Vorschlägen aus und klicken Sie dann auf View details (Details anzeigen).
4. Wählen Sie auf der Registerkarte Pending proposals (Ausstehende Vorschläge) das Transit-Gateway aus und klicken Sie auf Reject proposal (Vorschlag ablehnen).
5. Geben Sie im Dialogfeld Reject proposal (Vorschlag ablehnen) „Delete (Löschen)“ ein und klicken Sie auf Reject proposal (Vorschlag ablehnen).

So zeigen Sie Zuordnungsvorschläge mithilfe der Befehlszeile oder API an

- describe-direct-connect-gateway-association-proposals ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(API)AWS Direct Connect

So akzeptieren Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API

- accept-direct-connect-gateway-assoziationsvorschlag ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

So lehnen Sie einen Verknüpfungsvorschlag mithilfe der Befehlszeile oder API ab

- delete-direct-connect-gateway-assoziationsvorschlag ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Aktualisieren der zulässigen Präfixe für eine Transit Gateway-Zuordnung

Sie können aktualisieren, welche Präfixe vom Transit Gateway über das Direct-Connect-Gateway zulässig sind.

Wenn Sie Eigentümer des Transit Gateways sind, erstellen Sie einen neuen Zuordnungsvorschlag für das gleiche Direct-Connect-Gateway und Virtual Private Gateway; geben Sie dabei die zulässigen Präfixe an.

Wenn Sie Eigentümer des Direct Connect-Gateway sind, aktualisieren Sie die zulässigen Präfixe, wenn Sie den Zuordnungsvorschlag akzeptieren, oder aktualisieren Sie die zulässigen Präfixe für eine vorhandene Zuordnung wie folgt.

So aktualisieren Sie die zulässigen Präfixe für eine vorhandene Zuordnung über die Befehlszeile oder API

- update-direct-connect-gateway-Assoziation ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Löschen eines Transit-Gateway-Zuordnungsvorschlags

Der Eigentümer des Transit Gateway kann den Zuordnungsvorschlag für das Direct-Connect-Gateway löschen, wenn dieser erst noch akzeptiert werden muss. Nach dem Akzeptieren eines Zuordnungsvorschlags kann dieser zwar nicht mehr gelöscht werden, Sie können jedoch die Zuordnung des Transit-Gateways zum Direct Connect-Gateway aufheben. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Zuordnungsvorschlags”.

So löschen Sie einen Zuordnungsvorschlag

1. Öffnen Sie die AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Transit Gateway Attachments (Transit-Gateway-Anhänge) aus. Wählen Sie das Transit Gateway aus.

3. Wählen Sie die Option View details aus.
4. Wählen Sie Pending gateway associations (Ausstehende Gateway-Zuordnungen), wählen Sie die Zuordnung aus und klicken Sie auf Delete association (Zuordnung löschen).
5. Geben Sie im Dialogfeld Delete association proposal (Zuordnungsvorschlag löschen) Delete (Löschen) ein und klicken Sie auf Delete (Löschen).

So löschen Sie einen ausstehenden Zuordnungsvorschlag mithilfe der Befehlszeile oder API

- delete-direct-connect-gateway-association-propos ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Interaktionen zulässiger Präfixe

Hier erfahren Sie, wie zulässige Präfixe mit Transit Gateways und Virtual Private Gateways interagieren. Weitere Informationen finden Sie unter the section called “Routing-Richtlinien und BGP-Communitys”.

Virtual Private Gateway-Zuordnungen

Die Präfixliste (IPv4 und IPv6) fungiert als Filter, der die Ankündigung der gleichen oder einer kleineren Auswahl von CIDRs beim Direct Connect-Gateway erlaubt. Sie müssen die Präfixe auf einen Bereich festlegen, der identisch mit dem VPC-CIDR-Block oder breiter ist.

> **Note**
>
> Die Genehmigungsliste dient nur als Filter, und nur die zugehörige VPC-CIDR wird dem Kunden-Gateway bekannt gegeben.

Betrachten Sie das Szenario, bei dem VPC mit CIDR 10.0.0.0/16 einem Virtual Private Gateway angefügt ist.

- Wenn die Liste zulässiger Präfixe auf 22.0.0.0/24 eingestellt ist, erhalten Sie keine Route, da 22.0.0.0/24 ist nicht gleich oder größer als 10.0.0.0/16 ist.
- Wenn die Liste zulässiger Präfixe auf 10.0.0.0/24 eingestellt ist, erhalten Sie keine Route, da 10.0.0.0/24 nicht gleich 10.0.0.0/16 ist.

- Wenn die Liste zulässiger Präfixe auf 10.0.0.0/15 eingestellt ist, erhalten Sie 10.0.0.0/16, da die IP-Adresse größer als 10.0.0.0/16 ist.

Wenn Sie ein zulässiges Präfix entfernen oder hinzufügen, wird der Datenverkehr, der dieses Präfix nicht verwendet, nicht beeinträchtigt. Bei Aktualisierungen ändert sich der Status von `associated` zu `updating`. Durch das Ändern eines vorhandenen Präfixes kann nur der Datenverkehr verzögert werden, der dieses Präfix verwendet.

Transit-Gateway-Zuordnungen

Für eine Transit-Gateway-Zuordnung stellen Sie die Liste zulässiger Präfixe auf dem Direct-Connect-Gateway bereit. Die Liste leitet den lokalen Datenverkehr von oder zum Direct-Connect-Gateway an das Transit Gateway, selbst wenn den mit dem Transit Gateway verbundenen VPCs keine CIDRs zugewiesen wurden. Zulässige Präfixe funktionieren je nach Gateway-Typ unterschiedlich:

- Bei Transit-Gateway-Zuordnungen werden nur die eingegebenen zulässigen Präfixe lokal angekündigt. Diese werden als von der Direct-Connect-Gateway-ASN stammend angezeigt.
- Bei Virtual Private Gateways dienen die eingegebenen zulässigen Präfixe als Filter, um dieselben oder kleinere CIDRs zuzulassen.

Betrachten Sie das Szenario, in dem Sie eine VPC mit CIDR 10.0.0.0/16 an ein Transit Gateway angefügt haben.

- Wenn die Liste der zulässigen Präfixe auf 22.0.0.0/24 eingestellt ist, erhalten Sie auf Ihrer virtuellen Transit-Schnittstelle 22.0.0.0/24 über BGP. Sie erhalten nicht 10.0.0.0/16, da wir die Präfixe, die in der Liste zulässiger Präfixe enthalten sind, direkt bereitstellen.
- Wenn die Liste der zulässigen Präfixe auf 10.0.0.0/24 eingestellt ist, erhalten Sie auf Ihrer virtuellen Transit-Schnittstelle 10.0.0.0/24 über BGP. Sie erhalten nicht 10.0.0.0/16, da wir die Präfixe, die in der Liste zulässiger Präfixe enthalten sind, direkt bereitstellen.
- Wenn die Liste der zulässigen Präfixe auf 10.0.0.0/8 eingestellt ist, erhalten Sie auf Ihrer virtuellen Transit-Schnittstelle 10.0.0.0/8 über BGP.

Überschneidungen von zulässigen Präfixen sind nicht zulässig, wenn mehrere Transit Gateways einem Direct-Connect-Gateway zugeordnet sind. Wenn Sie beispielsweise ein Transit Gateway mit einer Liste zulässiger Präfixe haben, die 10.1.0.0/16 enthält, und ein zweites Transit Gateway mit einer Liste zulässiger Präfixe, die 10.2.0.0/16 und 0.0.0.0/0 enthält, können Sie die Zuordnungen

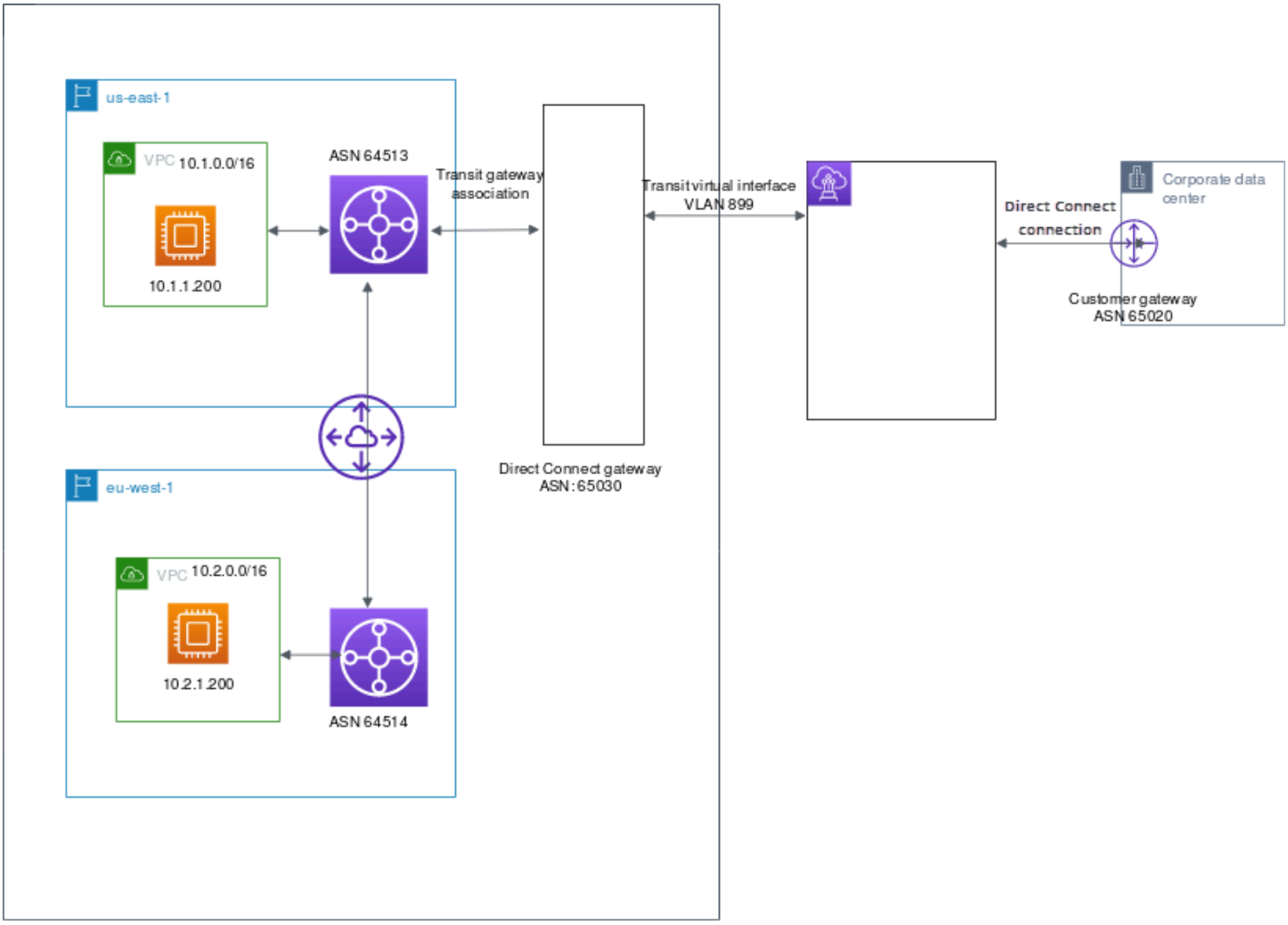
des zweiten Transit Gateways nicht auf 0.0.0.0/0 setzen. Da 0.0.0.0/0 alle IPv4-Netzwerke umfasst, können Sie 0.0.0.0/0 nicht konfigurieren, wenn mehrere Transit Gateways mit einem Direct-Connect-Gateway verknüpft sind. Es wird ein Fehler zurückgegeben, der darauf hinweist, dass sich die zulässigen Routen mit einer oder mehreren vorhandenen zulässigen Routen auf dem Direct-Connect-Gateway überschneiden.

Wenn Sie ein zulässiges Präfix entfernen oder hinzufügen, wird der Datenverkehr, der dieses Präfix nicht verwendet, nicht beeinträchtigt. Bei Aktualisierungen ändert sich der Status von `associated` zu `updating`. Durch das Ändern eines vorhandenen Präfixes kann nur der Datenverkehr verzögert werden, der dieses Präfix verwendet.

Beispiel: Zulässig für Präfixe in einer Transit-Gateway-Konfiguration

Stellen Sie sich die Konfiguration vor, in der Sie Instancs in zwei verschiedenen AWS-Regionen haben, die auf das Unternehmensrechenzentrum zugreifen müssen. Sie konfigurieren die folgenden Ressourcen für diese Konfiguration:

- Ein Transit Gateway in jeder Region.
- Transit-Gateway-Peering-Verbindungen.
- Ein Direct-Connect-Gateway.
- Eine Transit-Gateway-Zuordnung zwischen einem der Transit Gateways (dem in us-east-1) und dem Direct-Connect-Gateway.
- Eine virtuelle Transit-Schnittstelle zwischen dem lokalen Standort und dem AWS Direct Connect-Standort.



Konfigurieren Sie die folgenden Optionen für die Ressourcen.

- Direct-Connect-Gateway: Stellen Sie die ASN auf 65030 ein. Weitere Informationen finden Sie unter the section called “Erstellen eines Direct Connect-Gateways”.
- Virtuelle Transit-Schnittstelle: Stellen Sie das VLAN auf 899 und die ASN auf 65020 ein. Weitere Informationen finden Sie unter the section called “Eine virtuelle Transit-Schnittstelle für das Direct-Connect-Gateway erstellen”.
- Direct-Connect-Gateway-Zuordnung zum Transit Gateway: Stellen Sie die zulässigen Präfixe auf 10.0.0.0/8 ein.

  Dieser CIDR-Block deckt beide VPC-CIDR-Blöcke ab. Weitere Informationen finden Sie unter the section called “Zuordnen und Aufheben der Zuordnung von Transit-Gateways”.
- VPC-Route: Um den Verkehr von der VPC 10.2.0.0 weiterzuleiten, erstellen Sie in der VPC-Routing-Tabelle eine Route mit dem Ziel 0.0.0.0/0 und der Transit-Gateway-ID als Ziel. Weitere

Informationen über das Rotuing zu einem Transit Gateway finden Sie unter Routing für ein Transit Gateway im Amazon-VPC-Benutzerhandbuch.

Markieren von AWS Direct Connect-Ressourcen

Ein Tag ist eine Markierung, die den AWS Direct Connect-Ressourcen von ihrem Eigentümer zugewiesen wird. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Mit Tags können Sie Ihre AWS Direct Connect-Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck oder Umgebung. Dies ist hilfreich, wenn Sie viele Ressourcen desselben Typs haben. In diesem Fall können Sie basierend auf den zugewiesenen Tags schnell bestimmte Ressourcen identifizieren.

Zum Beispiel haben Sie zwei AWS Direct Connect-Verbindungen in einer Region, jede davon an unterschiedlichen Standorten. Verbindung `dxcon-11aa22bb` ist eine Verbindung, die dem Produktionsverkehr dient und mit der virtuellen Schnittstelle verknüpft ist `dxvif-33cc44dd`. Verbindung `dxcon-abcabcab` ist eine redundante (backup) Verbindung und ist der virtuellen Schnittstelle zugeordnet `dxvif-12312312`. Sie können Ihre Verbindungen und virtuellen Schnittstellen wie folgt markieren, um sie zu unterscheiden:

Ressourcen-ID	Tag-Schlüssel	Tag-Wert
`dxcon-11aa22bb`	Zweck	Produktion
	Ort	Amsterdam
`dxvif-33cc44dd`	Zweck	Produktion
`dxcon-abcabcab`	Zweck	Backup
	Ort	Frankfurt
`dxvif-12312312`	Zweck	Backup

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Eine Anzahl einheitlicher Tag (Markierung)-Schlüssel vereinfacht das Verwalten der Ressourcen. Tags haben keine semantische Bedeutung für AWS Direct Connect und werden ausschließlich als Zeichenfolgen interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht Null

festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Sie können die folgenden AWS Direct Connect-Ressourcen über die AWS Direct Connect-Konsole, die AWS Direct Connect-API, die AWS CLI, die AWS Tools for Windows PowerShell oder ein AWS SDK markieren. Wenn Sie die diese Tools für die Verwaltung von Tags verwenden, müssen Sie den Amazon-Ressourcennamen (ARN) für die Ressource angeben. Weitere Informationen zur Verwendung von ARNs finden Sie unter Amazon-Ressourcennamen (ARN) im Allgemeine Amazon Web Services-Referenz.

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Tags bei der Erstellung	Unterstützt Tags bei der Steuerung von Zugriff und Ressourcenzuordnung	Unterstützt die Kostenzuordnung
Verbindungen	Ja	Ja	Ja	Ja
Virtuelle Schnittstellen	Ja	Ja	Ja	Nein
Link Aggregation Groups (LAG)	Ja	Ja	Ja	Ja
Interconnects	Ja	Ja	Ja	Ja
Direct Connect-Gateways	Nein	Nein	Nein	Nein

Tag (Markierung)-Einschränkungen

Folgende Regeln und Einschränkungen gelten für die Tags:

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 128 Unicode-Zeichen
- Maximale Wertlänge: 265 Unicode-Zeichen

- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das Präfix `aws:` ist zur Verwendung in AWS reserviert. Sie können den Schlüssel oder Wert eines Tags nicht bearbeiten oder löschen, wenn das Tag über einen Tag-Schlüssel mit dem `aws:`-Präfix verfügt. Tags mit einem Tag-Schlüssel und dem `aws:`-Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.
- Erlaubte Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = . _ : / @.
- Nur der Ressourceneigentümer kann Tags hinzufügen oder entfernen. Wenn zum Beispiel eine gehostete Verbindung vorliegt, kann der Partner die Tags nicht hinzufügen, entfernen oder anzeigen.
- Kostenzuordnungs-Tags werden nur für Verbindungen, Interconnects und LAGs unterstützt. Weitere Informationen zur Verwendung von Tags beim Kostenmanagement finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS Billing and Cost Management-Benutzerhandbuch.

Arbeiten mit Tags mittels CLI oder API

Mit den folgenden Befehlen können Sie Tags für Ihre Ressourcen hinzufügen, aktualisieren, auflisten und löschen.

Aufgabe	API	CLI
Fügen Sie einen oder mehrere Tags hinzu oder überschre iben Sie sie.	TagResource	tag-resource
Löschen Sie ein oder mehrere Tags.	UntagResource	untag-resource
Beschreiben Sie ein oder mehrere Tags.	DescribeTags	describe-tags

Beispiele

Verwenden Sie den Befehl tag-resource , um die Verbindung `dxcon-11aa22bb` zu markieren.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Verwenden Sie den Befehl describe-tags , um die-Tags der Verbindung `dxcon-11aa22bb` zu beschreiben.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Verwenden Sie den Befehl untag-resource, um ein Tag aus der Verbindung `dxcon-11aa22bb` zu entfernen.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Sicherheit in AWS Direct Connect

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen für AWS Direct Connect finden Sie unter Durch das Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von AWS Direct Connect einsetzen können. Die folgenden Themen veranschaulichen, wie Sie AWS Direct Connect zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre AWS Direct Connect-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz in AWS Direct Connect

Das Modell der geteilten Verantwortung von AWS gilt für den Datenschutz in AWS Direct Connect. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie unter Verwendung der Konsole, der API, AWS CLI oder AWS SDKs mit AWS Direct Connect oder anderen AWS-Services arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag AWS Shared Responsibility Model and GDPR im AWS-Sicherheitsblog.

Themen

Richtlinie für den Datenverkehr zwischen Netzwerken in AWS Direct Connect

Datenverkehr zwischen Service und On-Premises-Clients und -Anwendungen

Sie haben zwei Verbindungsoptionen zwischen Ihrem privaten Netzwerk und AWS:

- Eine Zuordnung zu einer AWS Site-to-Site VPN. Weitere Informationen finden Sie unter the section called “Sicherheit der Infrastruktur”.
- Eine Zuordnung zu VPCs. Weitere Informationen finden Sie unter the section called “Virtual Private Gateway-Zuordnungen” und the section called “Transit-Gateway-Zuordnungen”.

Datenverkehr zwischen AWS-Ressourcen in derselben Region

Sie haben zwei Konnektivitätsoptionen:

- Eine Zuordnung zu einer AWS Site-to-Site VPN. Weitere Informationen finden Sie unter the section called “Sicherheit der Infrastruktur”.
- Eine Zuordnung zu VPCs. Weitere Informationen finden Sie unter the section called “Virtual Private Gateway-Zuordnungen” und the section called “Transit-Gateway-Zuordnungen”.

Verschlüsselung in der AWS Direct ConnectÜbertragung

AWS Direct Connect verschlüsselt standardmäßig nicht Ihren Datenverkehr, der übertragen wird. Um die übertragenen Daten zu verschlüsseln, müssen Sie die AWS Direct ConnectÜbertragungsverschlüsselungsoptionen für diesen Dienst verwenden. Weitere Informationen

zur Verschlüsselung des EC2-Instance-Datenverkehrs finden Sie unter Verschlüsselung bei der Übertragung im Amazon EC2-Benutzerhandbuch.

Mit AWS Direct Connect und AWS Site-to-Site VPN können Sie eine oder mehrere AWS Direct Connect dedizierte Netzwerkverbindungen mit dem Amazon VPC-VPN kombinieren. Diese Kombination bietet eine IPSec-verschlüsselte private Verbindung, die auch die Netzwerkkosten senkt, den Bandbreitendurchsatz erhöht und ein konsistenteres Netzwerkerlebnis bietet als internetbasierte VPN-Verbindungen. Weitere Informationen finden Sie unter Verbindungsoptionen zwischen Amazon VPC und Amazon VPC.

MAC Security (MACsec) ist ein IEEE-Standard, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. Sie können AWS Direct Connect Verbindungen verwenden, die MACSec unterstützen, um Ihre Daten von Ihrem Unternehmensrechenzentrum bis zum Standort zu verschlüsseln. AWS Direct Connect Weitere Informationen finden Sie unter MAC Security.

Identity and Access Management für Direct Connect

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzend) ist, um Direct-Connect-Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Direct Connect.

Service-Benutzer – Wenn Sie den Direct-Connect-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Direct-Connect-Features ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für Direct-Connect-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf ein Feature in Direct Connect haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für Direct-Connect-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Direct Connect. Es ist Ihre Aufgabe, zu bestimmen, auf welche Direct-Connect-Features und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Direct Connect verwenden kann, finden Sie unter Funktionsweise von Direct Connect mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Direct Connect verfassen können. Beispiele für identitätsbasierte Direct-Connect-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Direct Connect.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center. (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services

zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation

aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in Amazon Managed Service for Prometheus verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden

zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen

in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Funktionsweise von Direct Connect mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Direct Connect verwenden, erfahren Sie, welche IAM-Funktionen Sie mit Direct Connect verwenden können.

IAM-Funktionen, die Sie mit Direct Connect verwenden können

IAM-Funktion	Unterstützung von Direct Connect
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja

IAM-Funktion	Unterstützung von Direct Connect
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen Überblick über das Zusammenwirken von Direct Connect und anderen AWS-Services mit den meisten IAM-Features finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Direct Connect

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Direct Connect

Beispiele für identitätsbasierte Direct-Connect-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Direct Connect.

Ressourcenbasierte Richtlinien in Direct Connect

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienmaßnahmen für Direct Connect

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Direct Connect-Aktionen finden Sie unter Von Direct Connect definierte Aktionen in der Serviceautorisierungsreferenz.

Richtlinienaktionen in Direct Connect verwenden das folgende Präfix vor der Aktion:

```
Direct Connect
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Richtlinienressourcen für Direct Connect

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der Direct-Connect-Ressourcentypen und ihrer ARNs finden Sie unter Ressourcentypen, die von Direct Connect definiert werden in der AWS Direct Connect-API-Referenz. Informationen zu

den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Direct Connect definierte Aktionen.

Beispiele für identitätsbasierte Direct-Connect-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Direct Connect.

Beispiele für ressourcenbasierte Direct-Connect-Richtlinien finden Sie unter Beispiele für identitätsbasierte Direct-Connect-Richtlinien mit tagbasierten Bedingungen.

Richtlinienbedingungsschlüssel für Direct Connect

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Direct-Connect-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Direct Connect in der AWS Direct Connect-API-Referenz. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Direct Connect in der Serviceautorisierungsreferenz.

Beispiele für identitätsbasierte Direct-Connect-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Direct Connect.

ACLs in Direct Connect

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Direct Connect

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder `aws:TagKeys`Bedingung verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Direct Connect

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen Featureieren, finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Hauptberechtigungen für Direct Connect

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein

Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Direct Connect

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Dienstrolle könnte die Direct-Connect-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Direct Connect dazu Anleitungen gibt.

Servicerollen für Direct Connect

Unterstützt serviceverknüpfte Rollen	Nein

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Direct Connect

Standardmäßig besitzen Benutzer und Rollen keine Berechtigungen zum Erstellen oder Ändern von Direct-Connect-Ressourcen. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von Direct Connect definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Direct Connect in der Service-Authorization-Referenz.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Direct-Connect-Ressourcen in Ihrem Konto erstellen, aufrufen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine

Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für AuftragsFeatureen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Aktionen, Ressourcen und Bedingungen für Direct Connect

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Direct Connect unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Direct Connect verwenden das folgende Präfix vor der Aktion: `directconnect:`. Um einem Benutzer beispielsweise die Berechtigung zum Ausführen einer Amazon-EC2-Instance mit der Amazon-EC2-`DescribeVpnGateways`-API-Operation zu erteilen, fügen Sie die Aktion `ec2:DescribeVpnGateways` in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Direct Connect definiert eine eigene Gruppe von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Die folgende Beispielrichtlinie erteilt Lesezugriff auf AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Die folgende Beispielrichtlinie erteilt vollständigen Zugriff auf AWS Direct Connect.

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

Eine Liste der Direct-Connect-Aktionen finden Sie im IAM-Benutzerhandbuch unter Von Direct Connect definierte Aktionen.

Ressourcen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Direct Connect verwendet die folgenden ARNs:

Direct Connect-Ressourcen-ARNs

Ressourcentyp	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Weitere Informationen zum Format von ARNs finden Sie unter Amazon-Ressourcennamen (ARNs) und AWS-Service-Namespaces.

Um beispielsweise die `dxcon-11aa22bb`-Schnittstelle in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Um alle virtuellen Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Einige Direct-Connect-Aktionen, z. B. zum Erstellen von Ressourcen, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Eine Liste der Direct-Connect-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Direct Connect definierte Ressourcentypen im IAM-Benutzerhandbuch. Informationen dazu, mit welchen Aktionen Sie den ARN der einzelnen Ressourcen angeben können, finden Sie unter SERVICE-ACTIONS-URL;.

Bedingungsschlüssel

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Direct Connect definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Sie können Bedingungsschlüssel mit der Tag-Ressource verwenden. Weitere Informationen finden Sie unter Beispiel: Einschränken des Zugriffs auf eine bestimmte Region.

Eine Liste der Direct-Connect-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Direct Connect im IAM-Benutzerhandbuch. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter SERVICE-ACTIONS-URL;.

Verwenden der Direct-Connect-Konsole

Um auf die Direct-Connect-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und Anzeigen von Details zu den Direct-Connect-Ressourcen in Ihrem AWS-Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (oder Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten dennoch Direct-Connect-Konsole verwenden können, fügen Sie den Entitäten auch die folgende von AWS verwaltete Richtlinie an. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch:

```
directconnect
```

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "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": "*"
        }
    ]
}
```

Schreibgeschützter Zugriff auf AWS Direct Connect

Die folgende Beispielrichtlinie erteilt Lesezugriff auf AWS Direct Connect.

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

```
}
```

Vollzugriff auf AWS Direct Connect

Die folgende Beispielrichtlinie erteilt vollständigen Zugriff auf AWS Direct Connect.

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

Beispiele für identitätsbasierte Direct-Connect-Richtlinien mit tagbasierten Bedingungen

Sie können den Zugriff auf Ressourcen und Anfragen anhand von Tag-Schlüsselbedingungen steuern. Sie können außerdem über eine Bedingung in Ihren IAM-Richtlinien steuern, ob spezifische Tag-Schlüssel an einer Ressource oder in einer Anfrage verwendet werden können.

Informationen zum Verwenden von Tags mit IAM-Richtlinien finden Sie unter Zugriffssteuerung mithilfe von Tags im IAM-Benutzerhandbuch.

Verknüpfen von virtuellen Direct-Connect-Schnittstellen basierend auf Tags

Im folgenden Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, über die die Zuordnung einer virtuellen Schnittstelle nur dann möglich ist, wenn das Tag den Umgebungsschlüssel und die preprod- oder Produktionswerte enthält.

```
       {
      "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": "*"
        }
      ]
    }
```

Steuern des Zugriffs auf Anforderungen basierend auf Tags

Sie können Bedingungen in Ihren IAM-Richtlinien verwenden, um zu steuern, welche Tag-Schlüsselwert-Paare in einer Anforderung weitergeleitet werden können, die eine AWS-Ressource markieren. Das folgende Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es erlaubt, die AWS Direct Connect TagResource Aktion nur dann zu verwenden, um Tags an eine virtuelle Schnittstelle anzuhängen, wenn das Tag den Umgebungsschlüssel und die Preprod- oder Produktionswerte enthält. Als bewährte Methode verwenden Sie den Modifikator `ForAllValues` mit dem Bedingungsschlüssel `aws:TagKeys`, um anzugeben, dass in der Anfrage nur die Schlüsselumgebung zulässig ist.

```
    {
        "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"}
            }
        }
    }
```

Steuern von Tag-Schlüsseln

Sie können eine Bedingung in Ihren IAM-Richtlinien verwenden, um zu steuern, ob spezifische Tag-Schlüssel an einer Ressource oder in einer Anforderung verwendet werden können.

Im folgenden Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die es Ihnen ermöglicht, Ressourcen zu markieren, jedoch nur mit der Tag-Schlüssel-Umgebung

```
    {
     "Version": "2012-10-17",
     "Statement": {
       "Effect": "Allow",
       "Action": "directconnect:TagResource",
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringEquals": {
           "aws:TagKeys": [
             "environment"
           ]
         }
       }
     }
    }
```

Serviceverknüpfte Rollen für AWS Direct Connect

AWS Direct Connect verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit AWS Direct Connect verknüpft ist. Serviceverknüpfte Rollen werden von AWS Direct Connect vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von AWS Direct Connect, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Direct Connect definiert die

Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur AWS Direct Connect die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre AWS Direct Connect-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AWS Direct Connect

AWS Direct Connect verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForDirectConnect`. Auf diese Weise kann AWS Direct Connect die in AWS Secrets Manager in Ihrem Namen gespeicherten MACsec-Secrets abrufen.

Die serviceverknüpfte Rolle `AWSServiceRoleForDirectConnect` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `directconnect.amazonaws.com`

Die serviceverknüpfte Rolle `AWSServiceRoleForDirectConnect` verwendet die verwaltete Richtlinie `AWSDirectConnectServiceRolePolicy`.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Damit die serviceverknüpfte Rolle namens `AWSServiceRoleForDirectConnect` erfolgreich erstellt wird, benötigt die IAM-Identität, mit der Sie AWS Direct Connect verwenden, die erforderlichen Berechtigungen. Um die erforderlichen Berechtigungen zu erteilen, fügen Sie die folgende Richtlinie an die IAM-Identität an.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS Direct Connect

Sie müssen die serviceverknüpfte Rolle nicht manuell erstellen. AWS Direct Connect legt für Sie die entsprechende serviceverknüpfte Rolle an. Wenn Sie den `associate-mac-sec-key`-Befehl ausführen, erstellt AWS eine serviceverknüpfte Rolle, mit der AWS Direct Connect die MACsec-Secrets abrufen kann, die in AWS Secrets Manager in Ihrem Namen in der AWS Management Console, der AWS CLI oder der AWS-API gespeichert sind.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. AWS Direct Connect erstellt erneut die serviceverknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall AWS Direct Connect zu erstellen. Erstellen Sie in der AWS CLI oder der AWS-API

eine servicegebundene Rolle mit dem Servicenamen `directconnect.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese servicegebundene Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für AWS Direct Connect

AWS Direct Connect verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForDirectConnect`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Direct Connect

Sie müssen die Rolle `AWSServiceRoleForDirectConnect` nicht manuell löschen. Wenn Sie Ihre serviceverknüpfte Rolle löschen, müssen Sie alle zugehörigen Ressourcen löschen, die im AWS Secrets Manager-Webservice gespeichert sind. Bei der AWS Management Console, der AWS CLI oder der AWS-API bereinigt AWS Direct Connect die Ressourcen und löscht die serviceverknüpfte Rolle für Sie.

Sie können die IAM-Konsole auch für das Löschen einer serviceverknüpften Rolle verwenden. Sie müssen dafür zuerst die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen und können sie dann löschen.

> **Note**
>
> Wenn der AWS Direct Connect-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Löschen Sie die von **`AWSServiceRoleForDirectConnect`** verwendeten AWS Direct Connect-Ressourcen wie folgt:

1. Entfernen Sie die Zuordnung zwischen allen MACsec-Schlüsseln und Verbindungen. Weitere Informationen finden Sie unter the section called “Die Zuordnung zwischen einem geheimen MACsec-Schlüssel und einer Verbindung entfernen”.

2. Entfernen Sie die Zuordnung zwischen allen MACsec-Schlüsseln und LAGs. Weitere Informationen finden Sie unter the section called “Die Zuordnung zwischen allen MACsec-Schlüsseln und LAGs entfernen”.

To manually delete the service-linked role using IAM (So löschen Sie die servicegebundene Rolle mit IAM)

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die `AWSServiceRoleForDirectConnect` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte AWS Direct Connect-Rollen

AWS Direct Connect unterstützt die Verwendung von serviceverknüpften Rollen in allen AWS-Regionen, in denen das MAC-Security-Feature verfügbar ist. Weitere Informationen finden Sie unter AWS Direct Connect-Standorte.

AWS Von verwaltete Richtlinien für AWS Direct Connect

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWSverwaltete Richtlinie: AWSDirectConnectFullAccess

Sie können die `AWSDirectConnectFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die vollen Zugriff auf AWS Direct Connect ermöglichen.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectFullAccess im AWS Management Console.

AWSverwaltete Richtlinie: AWSDirectConnectReadOnlyAccess

Sie können die `AWSDirectConnectReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf AWS Direct Connect erlauben.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectReadOnlyAccess im AWS Management Console.

AWSverwaltete Richtlinie: AWSDirectConnectServiceRolePolicy

Diese Richtlinie ist der dienstbezogenen Rolle zugeordnet, die den Namen trägt AWSServiceRoleForDirectConnect, AWS Direct Connect damit MAC-Sicherheitsgeheimnisse in Ihrem Namen abgerufen werden können. Weitere Informationen finden Sie unter the section called “Serviceverknüpfte Rollen”.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectServiceRolePolicy im AWS Management Console.

AWS Direct Connect-Aktualisierungen für AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für AWS Direct Connect, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS Direct Connect-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWSDirectConnectServiceRolePolicy – Neue Richtlinie	Zur Unterstützung von MAC Security wurde die AWSServiceRoleForD	31. März 2021

Änderung	Beschreibung	Datum
	irectConnectdienstbezogene Rolle hinzugefügt.	
AWS Direct Connect hat die Änderungsverfolgung gestartet	AWS Direct Connect hat mit der Verfolgung von Änderungen an seinen AWS-verwalteten Richtlinien begonnen.	31. März 2021

Fehlerbehebung für Direct-Connect-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Direct Connect und IAM auftreten könnten.

Themen

Ich bin nicht autorisiert, eine Aktion in Direct Connect auszuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `directconnect:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `directconnect:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der Aktion `iam:PassRole` autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Direct Connect übergeben können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Direct Connect auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Direct-Connect-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Direct Connect diese Features unterstützt, finden Sie unter Funktionsweise von Direct Connect mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollieren und Überwachen in AWS Direct Connect

Sie können die folgenden automatisierten Tools zur Überwachung von AWS Direct Connect verwenden und möglicherweise auftretende Probleme melden:

- Amazon-CloudWatch-Alarme – Überwachen eine Metrik über einen von Ihnen definierten Zeitraum. Führen Sie eine oder mehrere Aktionen durch, die vom Wert der Metrik im Vergleich zu einem festgelegten Schwellenwert in einer Reihe von Zeiträumen abhängen. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema gesendet wird. CloudWatch-Alarme rufen keine Aktionen auf, nur weil sie einen bestimmten Status aufweisen. Der Status muss geändert und für eine bestimmte Anzahl an Zeiträumen aufrechterhalten worden sein. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.
- AWS CloudTrail-Protokollüberwachung – Teilt Protokolldateien zwischen Konten und überwacht CloudTrail-Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden. Sie können außerdem Anwendungen zur Protokollverarbeitung in Java schreiben und sich vergewissern, dass nach der Lieferung durch CloudTrail keine Änderungen an den Protokolldaten vorgenommen wurden. Weitere Informationen finden Sie unter Protokollieren von AWS Direct Connect-API-Aufrufen mithilfe von AWS CloudTrail sowie unter Arbeiten mit CloudTrail-Protokolldateien im AWS CloudTrail-Benutzerhandbuch.

Weitere Informationen finden Sie unter Überwachen.

Konformitätsvalidierung für AWS Direct Connect

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services

unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten

Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit in AWS Direct Connect

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones. AWS Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die mit Netzwerken mit geringer Latenz, hohem Durchsatz und hochredundanten Vernetzungen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur globalen AWS-Infrastruktur stellt AWS Direct Connect verschiedene Funktionen bereit, um Ihren Anforderungen in Bezug auf Ausfallsicherheit und Datensicherung zu erfüllen.

Weitere Informationen zur Verwendung von VPN mit AWS Direct Connect, finden Sie unter AWS Direct Connect Plus VPN.

Failover

Das AWS Direct Connect Resiliency Toolkit bietet einen Verbindungsassistenten mit mehreren Resilienzmodellen, mit denen Sie dedizierte Verbindungen bestellen können, um Ihr SLA-Ziel zu erreichen. Sie wählen ein Resilienzmodell aus, und AWS Direct Connect führt Sie dann durch den dedizierten Verbindungsbestellungsprozess. Die Resilienzmodelle wurden entwickelt, um sicherzustellen, dass Sie über die entsprechende Anzahl dedizierter Verbindungen an mehreren Standorten verfügen.

- Maximum Resiliency (Maximale Ausfallsicherheit): Sie erzielen eine maximale Ausfallsicherheit für kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an mehreren Standorten beendet werden. Dieses Modell bietet Ausfallsicherheit gegen Geräte-, Konnektivitäts- und vollständige Standortausfälle.
- High Resiliency (Hohe Ausfallsicherheit): Sie erzielen eine hohe Ausfallsicherheit für kritische Workloads, indem Sie zwei einzelne Verbindungen zu mehreren Standorten verwenden. Dieses Modell bietet Ausfallsicherheit gegen Konnektivitätsfehler, die durch eine Unterbrechung der Glasfaserverbindung oder einen Geräteausfall verursacht werden. Außerdem werden so vollständige Standortfehler verhindert.
- Development and Test (Entwicklung und Test): Sie erzielen Entwicklungs- und Testausfallsicherheit für nicht kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an einem Standort beendet werden. Dieses Modell bietet Ausfallsicherheit bei Geräteausfällen, jedoch nicht bei Standortfehlern.

Weitere Informationen finden Sie unter Verwenden Sie das AWS Direct Connect Resiliency Toolkit für den Einstieg.

Sicherheit der Infrastruktur in AWS Direct Connect

Als verwalteter Service ist AWS Direct Connect durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS Direct Connect zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Wir empfehlen TLS 1.3. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Sie können API-Operationen von jedem Netzwerkstandort aus aufrufen. AWS Direct Connect unterstützt ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Basis der Quell-IP-Adresse enthalten können. Sie können auch AWS Direct Connect-Richtlinien verwenden, um den Zugriff über bestimmte Amazon Virtual Private Cloud (Amazon VPC)-Endpunkte oder bestimmte VPCs zu steuern. Tatsächlich wird der Netzwerkzugriff hierdurch auf eine bestimmte AWS Direct

Connect-Ressource eingeschränkt, sodass er ausschließlich über eine bestimmte VPC innerhalb des AWS-Netzwerks ausgeführt werden kann. Für Beispiele vgl. the section called “Beispiele für identitätsbasierte Richtlinien”.

Border Gateway Protocol (BGP)-Sicherheit

Das Internet stützt sich zum großen Teil auf BGP, um Informationen zwischen Netzwerksystemen weiterzuleiten. BGP-Routing kann manchmal anfällig für böswillige Angriffe oder BGP-Hijacking sein. Informationen darüber, wie AWS Ihr Netzwerk sicherer vor BGP-Hijacking schützt, finden Sie unter So trägt AWS zur Sicherung des Internet-Routing bei.

Verwendung von AWS CLI

Sie können die AWS CLI verwenden, um AWS Direct Connect-Ressourcen zu erstellen und zu bearbeiten.

In folgendem Beispiel wird die AWS CLI-Befehle zum Erstellen einer AWS Direct Connect-Verbindung verwendet. Außerdem können Sie das Dokument "Letter of Authorization and Connecting Facility Assignment (LOA-CFA)" oder eine private oder öffentliche virtuelle Schnittstelle bereitzustellen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die AWS CLI installiert und konfiguriert haben. Weitere Informationen finden Sie im AWS Command Line Interface-Benutzerhandbuch.

Inhalt

Schritt 1: Erstellen einer Verbindung

Im ersten Schritt senden Sie eine Verbindungsanforderung. Vergewissern Sie sich, dass Sie die benötigte Portgeschwindigkeit und den AWS Direct Connect-Standort kennen. Weitere Informationen finden Sie unter AWS Direct Connect Verbindungen.

So erstellen Sie eine Verbindungsanforderung

1. Beschreiben Sie die AWS Direct Connect-Standorte für Ihre aktuelle Region. Beachten Sie in der Ausgabe, die zurückgeschickt wird den Standortcode für den Ort, in dem Sie die Verbindung herstellen möchten.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
```

```
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
    ]
}
```

2. Erstellen Sie die Verbindung und geben Sie einen Namen, die Portgeschwindigkeit und den Standortcode an. Beachten Sie die Verbindung-ID in der Ausgabe die zurückgeschickt wird. Sie brauchen die ID, um das LOA-CFA im nächsten Schritt zu bekommen.

```
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"
}
```

Schritt 2: Herunterladen des LOA-CFA-Dokuments

Nachdem Sie eine Verbindung angefordert haben, können Sie das LOA-CFA-Dokument mit dem Befehl `describe-loa` erhalten. Die Ausgabe ist base64-kodiert. Sie müssen die relevanten LOA-Inhalte extrahieren, entschlüsseln und eine PDF-Datei erstellen.

So fordern Sie das LOA-CFA-Dokument mit Linux oder macOS an

In diesem Beispiel decodiert der letzte Teil des Befehls den Inhalt mit dem base64-Dienstprogramm und sendet die Ausgabe an eine PDF-Datei.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

So bekommen Sie das LOA-CFA mit Windows

In diesem Beispiel wird die Ausgabe in eine Datei mit dem Namen myLoaCfa.base64 extrahiert. Der zweite Befehl verwendet das `certutil` Dienstprogramm um die Datei zu dekodieren und die Ausgabe an eine PDF-Datei zu senden.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Nachdem Sie das LOA-CFA-Dokument heruntergeladen haben, senden Sie es Ihrem Netzwerk-Anbieter oder Ihrem Co-Location-Anbieter.

Schritt 3: Erstellen einer virtuellen Schnittstelle und Abrufen der Router-Konfiguration

Nach der Beantragung einer AWS Direct Connect-Verbindung müssen Sie zuerst eine virtuelle Schnittstelle erstellen. Sie können eine private virtuelle Schnittstelle erstellen, um eine Verbindung mit Ihrer VPC herzustellen. Alternativ können Sie eine öffentliche virtuelle Schnittstelle erstellen, um eine Verbindung zu den AWS-Services herzustellen, die sich nicht in einer VPC befinden. Sie können eine virtuelle Schnittstelle erstellen, die den IPv4- oder IPv6-Traffic unterstützt.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Voraussetzungen in Voraussetzungen für virtuelle Schnittstellen gelesen haben.

Wenn Sie eine virtuelle Schnittstelle mit der AWS CLI erstellen, enthält die Ausgabe allgemeine Router-Konfigurationsinformationen. Wenn Sie eine Router-Konfiguration erstellen möchten, die für Ihr Gerät spezifisch ist, verwenden Sie die AWS Direct Connect-Konsole. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

So erstellen Sie eine private, virtuelle Schnittstelle

1. Holen Sie sich die ID des Virtual Private Gateway (vgw-xxxxxxxx) die an Ihre VPC angehängt ist. Sie benötigen die ID, um die virtuelle Schnittstelle im nächsten Schritt zu erstellen.

   ```
   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. Erstellen Sie eine private virtuelle Schnittstelle. Geben Sie einen Namen, eine VLAN-ID und eine BGP Autonomous System Number (ASN) an.

   Für den IPv4-Traffic benötigen Sie private IPv4-Adressen für jedes Ende der BGP-Peering-Session. Sie können Ihre eigenen IPv4-Adressen angeben, oder Sie können Amazon die Adressen für Sie generieren lassen. Im folgenden Beispiel werden die IPv4-Adressen für Sie generiert.

```
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"
}
```

Um eine private virtuelle Schnittstelle zu erstellen, die den IPv6-Traffic unterstützt, verwenden Sie denselben Befehl wie oben und geben Sie `ipv6` für die `addressFamily` Parameter an. Sie können keine eigenen IPv6-Adressen für die BGP-Peering-Session angeben. Amazon weist Ihnen IPv6-Adressen zu.

3. Um die Router-Konfigurationsinformationen im XML-Format anzuzeigen, beschreiben Sie die virtuelle Schnittstelle, die Sie erstellt haben. Verwenden Sie den `--query` Parameter um die `customerRouterConfig` Information zu extrahieren und den `--output` Parameter um den Text in tabulatorgetrennten Zeilen auszurichten.

```
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>
```

So erstellen Sie eine öffentliche virtuelle Schnittstelle

1. Um eine öffentliche virtuelle Schnittstelle zu erstellen, müssen Sie einen Namen, eine VLAN ID und eine BGP Autonome System Number (ASN) angeben.

   Für den IPv4-Traffic müssen Sie auch öffentliche IPv4-Adressen für jedes Ende der BGP-Peering-Session und öffentliche IPv4-Routen angeben, die Sie über BGP bewerben werden. Das folgende Beispiel erstellt eine öffentliche virtuelle Schnittstelle für den IPv4-Traffic.

```
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"
}
```

Um eine öffentliche virtuelle Schnittstelle zu erstellen, die IPv6-Traffic unterstützt, können Sie IPv6-Routen angeben, die Sie über BGP bewerben werden. Sie können keine IPv6-Adressen für die Peering-Session angeben. Amazon weist Ihnen IPv6-Adressen zu. Das folgende Beispiel erstellt eine öffentliche virtuelle Schnittstelle für den IPv6-Traffic.

```
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. Um die Router-Konfigurationsinformationen im XML-Format anzuzeigen, beschreiben Sie die virtuelle Schnittstelle, die Sie erstellt haben. Verwenden Sie den `--query` Parameter um die `customerRouterConfig` Information zu extrahieren und den `--output` Parameter um den Text in tabulatorgetrennten Zeilen auszurichten.

```
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>
```

Protokollieren von AWS Direct Connect-API-Aufrufen mithilfe von AWS CloudTrail

AWS Direct Connect ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in AWS Direct Connect protokolliert. CloudTrail erfasst alle API-Aufrufe für AWS Direct Connect als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Direct Connect-Konsole und Code-Aufrufe der AWS Direct Connect-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignisse für AWS Direct Connect aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail erfassten Informationen können Sie die an AWS Direct Connect gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS Direct Connect-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in AWS Direct Connect auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen in Event History (Ereignisverlauf). aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Direct Connect, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen

- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle AWS Direct Connect-Aktionen werden von CloudTrail protokolliert und sind in der AWS Direct Connect-API-Referenz dokumentiert. Zum Beispiel generieren Aufrufe der Aktionen `CreateConnection` und `CreatePrivateVirtualInterface` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit den Anmeldeinformationen des Root-Benutzers oder AWS Identity and Access Management (IAM-Benutzer) ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie im CloudTrail `userIdentity` Element.

Grundlagen zu AWS Direct Connect-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt CloudTrail-Protokolleinträge für AWS Direct Connect.

Example Beispiel: 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 Beispiel: 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 Beispiel: 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 Beispiel: 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
    },
    ...
  ]
}
```

Überwachen von - AWS Direct Connect Ressourcen

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Direct-Connect-Ressourcen aufrechtzuerhalten. Sie sollten Überwachungsdaten von allen Teilen Ihrer - AWS Lösung sammeln, damit Sie Ausfälle an mehreren Punkten leichter debuggen können. Bevor Sie mit der Überwachung von Direct Connect beginnen, sollten Sie jedoch einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Überwachungsziele?
- Welche Ressourcen sollten überwacht werden?
- Wie oft sollten Sie diese Ressourcen überwachen?
- Welche Überwachungstools können Sie verwenden?
- Wer führt die Überwachungsaufgaben aus?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Der nächste Schritt besteht darin, eine Grundlage für die normale Direct-Connect-Leistung in Ihrer Umgebung zu schaffen, indem Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen messen. Speichern Sie bei der Überwachung von Direct Connect historische Überwachungsdaten. Diese gespeicherten Daten bieten dann eine Basis für den Vergleich mit aktuellen Leistungsdaten, zur Identifikation normaler Leistungsmuster und von Leistungsanomalien sowie zur Entwicklung von Verfahren für den Umgang mit Problemen.

Um eine Baseline einzurichten, sollten Sie die Nutzung, den Status und den Zustand Ihrer physischen Direct-Connect-Verbindungen überwachen.

Inhalt

Überwachungstools

AWS bietet verschiedene Tools, mit denen Sie eine - AWS Direct Connect Verbindung überwachen können. Sie können einige dieser Tools so konfigurieren, dass diese die Überwachung für Sie übernehmen, während bei anderen Tools ein manuelles Eingreifen nötig ist. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Automatisierte Überwachungstools

Sie können die folgenden automatisierten Tools zur Überwachung von Direct Connect verwenden und Missstände melden:

- Amazon- CloudWatch Alarme – Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum. Führen Sie eine oder mehrere Aktionen durch, die vom Wert der Metrik im Vergleich zu einem festgelegten Schwellenwert in einer Reihe von Zeiträumen abhängen. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema gesendet wird. CloudWatch Alarme rufen keine Aktionen auf, nur weil sie sich in einem bestimmten Status befinden. Der Status muss geändert und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Informationen zu den verfügbaren Metriken und Dimensionen finden Sie unter Überwachung mit Amazon CloudWatch.
- AWS CloudTrail Protokollüberwachung – Teilen Sie Protokolldateien zwischen Konten und überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an - CloudWatch Protokolle senden. Sie können außerdem Anwendungen zur Protokollverarbeitung in Java schreiben und sich vergewissern, dass nach der Lieferung durch CloudTrail keine Änderungen an den Protokolldaten vorgenommen wurden. Weitere Informationen finden Sie unter Protokollieren von AWS Direct Connect-API-Aufrufen mithilfe von AWS CloudTrail und Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail -Benutzerhandbuch.

Manuelle Überwachungstools

Ein weiterer wichtiger Bestandteil der Überwachung einer - AWS Direct Connect Verbindung ist die manuelle Überwachung derjenigen Elemente, die die CloudWatch Alarme nicht abdecken. Die Direct Connect- und CloudWatch Konsolen-Dashboards bieten eine at-a-glance Ansicht des Zustands Ihrer AWS Umgebung.

- Die AWS Direct Connect Konsole zeigt:
  - Verbindungsstatus (siehe Spalte State)
  - Status der virtuellen Schnittstelle (siehe Spalte State)
- Die - CloudWatch Startseite zeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

Darüber hinaus können Sie mit Folgendes CloudWatch tun:

- Erstellen von benutzerdefinierten Dashboards zur Überwachung des gewünschten Services.
- Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen.
- Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken.
- Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden.

Überwachung mit Amazon CloudWatch

Sie können physische AWS Direct Connect Verbindungen und virtuelle Schnittstellen mit überwachen CloudWatch. CloudWatch sammelt Rohdaten von Direct Connect und verarbeitet sie zu lesbaren Metriken. Standardmäßig CloudWatch stellt Direct-Connect-Metrikdaten in 5-Minuten-Intervallen bereit.

Ausführliche Informationen zu CloudWatchfinden Sie im Amazon CloudWatch -Benutzerhandbuch. Sie können Ihre Services auch überwachen, CloudWatch um zu sehen, welche Ressourcen verwenden. Weitere Informationen finden Sie unter AWS -Services, die CloudWatch Metriken veröffentlichen.

Inhalt

AWS Direct Connect -Metriken und -Dimensionen

Metriken sind für AWS Direct Connect physische Verbindungen und virtuelle Schnittstellen verfügbar.

AWS Direct Connect Verbindungsmetriken

Die folgenden Metriken sind über dedizierte Direct Connect-Verbindungen verfügbar.

Metrik	Beschreibung
`ConnectionState`	Der Zustand der Verbindung.1 zeigt nach oben und 0 nach unten.

Metrik	Beschreibung
	Diese Metrik ist für dedizierte und gehostete Verbindungen verfügbar. **Note** Diese Metrik ist zusätzlich zu den Konten der Verbindungsbesitzer auch in Eigentüme rkonten für gehostete virtuelle Schnittstellen verfügbar. Einheiten: boolescher Wert
`ConnectionBpsEgress`	Die Bitrate für ausgehende Daten von der - AWS Seite der Verbindung. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten, mindestens 1 Minute). Sie können das Standardaggregat ändern. Diese Metrik ist möglicherweise für eine neue Verbindung oder beim Neustart eines Geräts nicht verfügbar. Die Metrik wird gestartet, wenn die Verbindung zum Senden oder Empfangen von Datenverkehr verwendet wird. Einheiten: Bits pro Sekunde

Metrik	Beschreibung
`ConnectionBpsIngress`	Die Bitrate für eingehende Daten zur - AWS Seite der Verbindung. Diese Metrik ist möglicherweise für eine neue Verbindung oder beim Neustart eines Geräts nicht verfügbar. Die Metrik wird gestartet, wenn die Verbindung zum Senden oder Empfangen von Datenverkehr verwendet wird. Einheiten: Bits pro Sekunde
`ConnectionPpsEgress`	Die Paketrate für ausgehende Daten von der - AWS Seite der Verbindung. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten, mindestens 1 Minute). Sie können das Standardaggregat ändern. Diese Metrik ist möglicherweise für eine neue Verbindung oder beim Neustart eines Geräts nicht verfügbar. Die Metrik wird gestartet, wenn die Verbindung zum Senden oder Empfangen von Datenverkehr verwendet wird. Einheiten: Pakete pro Sekunde

Metrik	Beschreibung
`ConnectionPpsIngress`	Die Paketrate für eingehende Daten zur - AWS Seite der Verbindung. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten, mindestens 1 Minute). Sie können das Standardaggregat ändern. Diese Metrik ist möglicherweise für eine neue Verbindung oder beim Neustart eines Geräts nicht verfügbar. Die Metrik wird gestartet, wenn die Verbindung zum Senden oder Empfangen von Datenverkehr verwendet wird. Einheiten: Pakete pro Sekunde
`ConnectionCRCErrorCount`	Dieser Wert wird nicht mehr verwendet. Verwenden Sie stattdessen `ConnectionErrorCount` .

Metrik	Beschreibung
`ConnectionErrorCount`	Die Gesamtanzahl der Fehler für alle Arten von Fehlern auf MAC-Ebene auf dem AWS -Gerät. Die Summe beinhaltet zyklische Redundanzprüfungsf ehler (CRC). Diese Metrik gibt die Anzahl der Fehler an, die seit dem letzten gemeldeten Datenpunkt aufgetreten sind. Wenn auf der Schnittstelle Fehler auftreten , meldet die Metrik Werte ungleich Null. Um die Gesamtzahl aller Fehler für das ausgewählte Intervall in zu erhalten, CloudWatchz. B. 5 Minuten, wenden Sie die Statistik „Summe“ an. Weitere Informationen zum Abrufen der Summenstatistik finden Sie unter Abrufen von Statistiken für eine Metrik im Amazon-CloudWatch Benutzerhandbuch. Der Metrikwert wird auf 0 gesetzt, wenn die Fehler auf der Schnittstelle aufhören. **Note** Diese Metrik ersetzt `ConnectionCRCErrorCount` , das nicht mehr verwendet wird. Einheiten: Anzahl

Metrik	Beschreibung
`ConnectionLightLevelTx`	Gibt den Zustand der Glasfaserverbindung für ausgehenden (ausgehenden) Datenverkehr von der - AWS Seite der Verbindung an. Es gibt zwei Dimensionen für diese Metrik. Weitere Informationen finden Sie unter the section called “AWS Direct Connect Verfügbare Dimensionen”. Einheiten: dBm
`ConnectionLightLevelRx`	Gibt den Zustand der Glasfaserverbindung für eingehenden (eingehenden) Datenverkehr zur - AWS Seite der Verbindung an. Es gibt zwei Dimensionen für diese Metrik. Weitere Informationen finden Sie unter the section called “AWS Direct Connect Verfügbare Dimensionen”. Einheiten: dBm
`ConnectionEncryptionState`	Gibt den Verschlüsselungsstatus der Verbindung an. 1 gibt an, dass die Verbindungsverschlüsselung up ist, und 0 gibt an, dass die Verbindungsverschl üsselung down ist. Wenn diese Metrik auf eine LAG angewendet wird, bedeutet 1, dass für alle Verbindun gen in der LAG die Verschlüsselung up ist. 0 gibt an, dass mindestens eine LAG-Verbindungsverschlüssel ung down ist.

AWS Direct Connect Metriken für virtuelle Schnittstellen

Die folgenden Metriken sind über AWS Direct Connect virtuelle Schnittstellen verfügbar.

Metrik	Beschreibung
`VirtualInterfaceBpsEgress`	Die Bitrate für ausgehende Daten von der - AWS Seite der virtuellen Schnittstelle. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten). Einheiten: Bits pro Sekunde
`VirtualInterfaceBpsIngress`	Die Bitrate für eingehende Daten an der - AWS Seite der virtuellen Schnittstelle. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten). Einheiten: Bits pro Sekunde
`VirtualInterfacePpsEgress`	Die Paketrate für ausgehende Daten von der - AWS Seite der virtuellen Schnittstelle. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten). Einheiten: Pakete pro Sekunde
`VirtualInterfacePpsIngress`	Die Paketrate für eingehende Daten an die - AWS Seite der virtuellen Schnittstelle. Der registrierte Wert ist der (durchschnittliche) aggregierte Wert in einem bestimmten Zeitraum (standardmäßig 5 Minuten). Einheiten: Pakete pro Sekunde

AWS Direct Connect Verfügbare Dimensionen

Sie können die AWS Direct Connect Daten anhand der folgenden Dimensionen filtern.

Dimension	Beschreibung
`ConnectionId`	Diese Dimension ist für die Metriken für Direct Connect-V erbindung und virtuelle Schnittstelle verfügbar. Diese Dimension filtert die Daten nach Verbindung.
`OpticalLaneNumber`	Diese Dimension filtert die `ConnectionLightLevelTx` Daten und die `ConnectionLightLevelRx` Daten und filtert die Daten nach der Nummer der -Direct-Connect-Verbindung.
`VirtualInterfaceId`	Diese Dimension ist auf den Metriken für die virtuelle Direct Connect-Schnittstelle verfügbar und filtert die Daten nach der virtuellen Schnittstelle.

Anzeigen von AWS Direct Connect CloudWatch Metriken

AWS Direct Connect sendet die folgenden Metriken zu Ihren Direct-Connect-Verbindungen. Amazon CloudWatch aggregiert diese Datenpunkte dann in Intervallen von 1 oder 5 Minuten. Standardmäßig werden Direct-Connect-Metrikdaten CloudWatch in 5-Minuten-Intervallen in geschrieben.

> **Note**
>
> Wenn Sie ein 1-Minuten-Intervall festlegen, versucht Direct Connect, die Metriken CloudWatch mit diesem Intervall in zu schreiben, kann jedoch nicht immer garantiert werden.

Sie können die folgenden Verfahren verwenden, um die Metriken für Direct-Connect-Verbindungen anzuzeigen.

So zeigen Sie Metriken mit der CloudWatch Konsole an

Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert. Weitere Informationen zur Verwendung von Amazon CloudWatch zum Anzeigen von Direct-Connect-Metriken, einschließlich

des Hinzufügens von mathematischen Funktionen oder vorgefertigten Abfragen, finden Sie unter Verwenden von Amazon CloudWatch Metriken im Amazon- CloudWatch Benutzerhandbuch.

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metrics (Metriken) und dann All metrics (Alle Metriken) aus.
3. Wählen Sie im Abschnitt Metrics (Metriken) die Option DX aus.
4. Wählen Sie einen ConnectionId oder Metriknamen und dann eine der folgenden Optionen aus, um die Metrik weiter zu definieren:
   - Add to search (Zur Suche hinzufügen) – Fügt diese Metrik zu Ihren Suchergebnissen hinzu.
   - Search for this only (Nur danach suchen) – Sucht nur nach dieser Metrik.
   - Remove from graph (Aus Diagramm entfernen) – Löscht diese Metrik aus dem Diagramm.
   - Graph this metric only (Nur diese Metrik grafisch darstellen) – Stellt nur diese Metrik grafisch dar.
   - Graph all search results (Alle Suchergebnisse grafisch darstellen) – Stellt alle Metriken grafisch dar.
   - Graph with SQL query (Diagramm mit SQL-Abfrage) – Öffnet den Metric-Insights-Abfragegenerator, mit dem Sie auswählen können, was Sie grafisch darstellen möchten, indem Sie eine SQL-Abfrage erstellen. Weitere Informationen zur Verwendung von Metric Insights finden Sie unter Abfragen Ihrer Metriken mit CloudWatch Metrics Insights im Amazon-CloudWatch Benutzerhandbuch.

So zeigen Sie Metriken mit der AWS Direct Connect Konsole an

1. Öffnen Sie die -AWS Direct ConnectKonsole unter https://console.aws.amazon.com/directconnect/v2/home.
2. Wählen Sie im Navigationsbereich Connections aus.
3. Wählen Sie Ihre Verbindung aus.
4. Auf der Registerkarte Monitoring (Überwachung) werden die Metriken für Ihre Verbindung angezeigt.

So zeigen Sie Metriken mit der an AWS CLI

Geben Sie als Eingabeaufforderung den folgenden Befehl ein.

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

Erstellen von CloudWatch Alarmen zur Überwachung von AWS Direct Connect Verbindungen

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum. Er sendet eine Benachrichtigung an ein Amazon SNS-Thema basierend auf dem Wert der Metrik im Hinblick auf einen Schwellenwert über verschiedene Zeiträume.

Sie können beispielsweise einen Alarm einrichten, der den Status einer AWS Direct Connect - Verbindung überwacht. Er sendet eine Benachrichtigung, wenn der Verbindungsstatus in fünf aufeinanderfolgenden Zeiträumen von 1 Minute ausgefallen ist. Einzelheiten zum Erstellen eines Alarms und weitere Informationen zum Erstellen eines Alarms finden Sie unter Verwenden von Amazon- CloudWatch Alarmen im Amazon- CloudWatch Benutzerhandbuch.

So erstellen Sie einen CloudWatch Alarm.

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Alarme und dann Alle Alarme aus.
3. Wählen Sie Alarm erstellen aus.
4. Wählen Sie Select metric (Metrik auswählen) und anschließend DX aus.
5. Wählen Sie die Metrik Connection Metrics (Verbindungsmetriken) aus.
6. Wählen Sie die AWS Direct Connect Verbindung und dann die Metrik auswählen aus.
7. Konfigurieren Sie auf der Seite Specify metric and conditions (Metrik und Bedingungen angeben) die Parameter für den Alarm. Weitere Informationen zur Angabe von Metriken und Bedingungen finden Sie unter Verwenden von Amazon CloudWatch-Alarmen im Amazon- CloudWatch Benutzerhandbuch.
8. Wählen Sie Weiter aus.
9. Konfigurieren Sie die Alarmaktionen auf der Seite Configure actions (Aktionen konfigurieren). Weitere Informationen zum Konfigurieren von Alarmaktionen finden Sie unter Alarmaktionen im Amazon- CloudWatch Benutzerhandbuch.
10. Wählen Sie Weiter aus.
11. Geben Sie auf der Seite Add name and description (Name und Beschreibung hinzufügen) den Name und die Alarm description (Alarmbeschreibung) ein und wählen Sie Next (Weiter) aus.

12. Überprüfen Sie den vorgeschlagenen Alarm auf der Seite Preview and create (Vorschau und Erstellung).
13. Wählen Sie bei Bedarf Edit (Bearbeiten) aus, um Informationen zu ändern, und wählen Sie dann Create alarm (Alarm erstellen) aus.

    Auf der Seite Alarms (Alarme) wird eine neue Zeile mit Informationen über den neuen Alarm angezeigt. Der Status Actions (Aktionen) zeigt Actions enabled (Aktionen aktiviert) an, was darauf hinweist, dass der Alarm aktiv ist.

AWS Direct Connect -Kontingente

In der folgenden Tabelle sind die Kontingente im Zusammenhang mit aufgeführt AWS Direct Connect.

Komponente	Kontingent	Kommentare
Private oder öffentliche virtuelle Schnittstellen pro AWS Direct Connect dedizierter Verbindung	50	Dieses Limit kann nicht erhöht werden.
Virtuelle Transit-Schnittstellen pro AWS Direct Connect dedizierter Verbindung	4	Dieses Limit kann nicht erhöht werden.
Private oder öffentliche virtuelle Schnittstellen pro AWS Direct Connect dedizierter Verbindung und virtuelle Transitschnittstellen pro AWS Direct Connect dedizierter Verbindung	51	Als die AWS Direct Connect Unterstützung für Amazon VPC Transit Gateways eingeführt wurde, wurde dem Kontingent von 50 privaten oder öffentlichen virtuellen Schnittstellen pro dedizierter Verbindung ein Kontingent von einer (1) virtuellen Transit-Schnittstelle hinzugefügt. Die Anzahl der zulässigen virtuellen Transit-Schnittstellen beträgt jetzt vier (4) und wird auf das Maximum von 51 virtuellen Schnittstellen pro dedizierter Verbindung angerechnet. Dieses Limit kann nicht erhöht werden.
Virtuelle private, öffentliche oder Transit-Schnittstellen pro AWS Direct Connect gehosteter Verbindung	1	Dieses Limit kann nicht erhöht werden.
Aktive AWS Direct Connect Verbindungen pro Direct-Connect-Standort pro Region und Konto	10	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).

Komponente	Kontingent	Kommentare
Anzahl der virtuellen Schnittstellen pro Link Aggregation Group (LAG)	51	Als die AWS Direct Connect Unterstützung für Amazon VPC Transit Gateways eingeführt wurde, wurde dem Kontingent von 50 privaten oder öffentlichen virtuellen Schnittstellen pro LAG ein Kontingent von einer (1) virtuellen Transit-Schnittstelle hinzugefügt. Die Anzahl der zulässigen virtuellen Transit-Schnittstellen beträgt jetzt vier (4) und wird auf das Maximum von 51 virtuellen Schnittstellen pro LAG angerechnet. Dieses Limit kann nicht erhöht werden.
Routen pro Border Gateway Protocol (BGP)-Sitzung auf einer privaten virtuellen Schnittstelle oder virtuellen Transitschnittstelle von On-Premises zu AWS. Wenn Sie für IPv4 und IPv6 je mehr als 100 Routen über die BGP-Sitzung ankündigen, wird die BGP-Sitzung in einen Ruhezustand (mit BGP-Sitzung DOWN) versetzt.	Jeweils 100 für IPv4 und IPv6	Dieses Limit kann nicht erhöht werden.
Routes pro Border Gateway Protocol (BGP)-Sitzung bei einer öffentlichen virtuellen Schnittstelle	1.000	Dieses Limit kann nicht erhöht werden.

Komponente	Kontingent	Kommentare
Dedizierte Verbindungen pro Link Aggregation Group (LAG)	4, wenn die Portgeschwindigkeit weniger als 100G beträgt 2, wenn die Portgeschwindigkeit 100G beträgt	
Link Aggregation Groups (LAGs) pro Region	10	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
AWS Direct Connect -Gateways pro Konto	200	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Virtual Private Gateways pro AWS Direct Connect Gateway	20	Dieses Limit kann nicht erhöht werden.
Transit-Gateways pro AWS Direct Connect Gateway	6	Dieses Limit kann nicht erhöht werden.
Virtuelle Schnittstellen (privat oder Transit) pro AWS Direct Connect Gateway	30	Dieses Limit kann nicht erhöht werden.

Komponente	Kontingent	Kommentare
Anzahl der Präfixe pro AWS Transit Gateway von AWS bis On-Premise auf einer virtuellen Transit-Schnittstelle	Insgesamt 200 für IPv4 und IPv6	Dieses Limit kann nicht erhöht werden.
Anzahl der virtuellen Schnittstellen pro Virtual Private Gateway	Es gibt kein Limit.	
Anzahl der einem Transit Gateway zugeordneten Direct-Connect-Gateways.	20	Dieses Limit kann nicht erhöht werden.
SiteLink Präfix-Limit	100	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).

AWS Direct Connect unterstützt diese Portgeschwindigkeiten über Singlemode-Glasfaser: 1 Gbit/s: 1000BASE-LX (1310 microSD), 10 Gbit/s: 10GBASE-LR (1310 microSD) und 100Gbps/s: 100GBASE-LR4.

BGP-Kontingente

Die folgenden sind BGP-Kontingente. Die BGP-Timer werden bis zum niedrigsten Wert zwischen den Routern ausgehandelt. Die BFD-Intervalle werden durch das langsamste Gerät definiert.

- Standard-Wartetimer: 90 Sekunden
- Mindest-Wartetimer: 3 Sekunden

  Ein Wartewert von 0 wird nicht unterstützt.
- Standard-Keepalive-Timer: 30 Sekunden
- Mindest-Keepalive-Timer: 1 Sekunde
- Timer für einen ordnungsgemäßen Neustart: 120 Sekunden

Es wird empfohlen, dass Sie nicht gleichzeitig den ordnungsgemäßen Neustart und den BFD-Modus konfigurieren.

- Mindestintervall für die Erkennung der BFD-Liveness: 300 ms
- BFD-Mindestmultiplikator: 3

Überlegungen zu Load Balancing

Wenn Sie Load Balancing mit mehreren öffentlichen VIFs verwenden möchten, müssen sich alle VIFs in derselben Region befinden.

Fehlerbehebung AWS Direct Connect

Die folgenden Fehlerbehebungsinformationen können Ihnen helfen, Probleme bei Ihrer AWS Direct Connect -Verbindung zu erkennen und zu beheben.

Inhalt

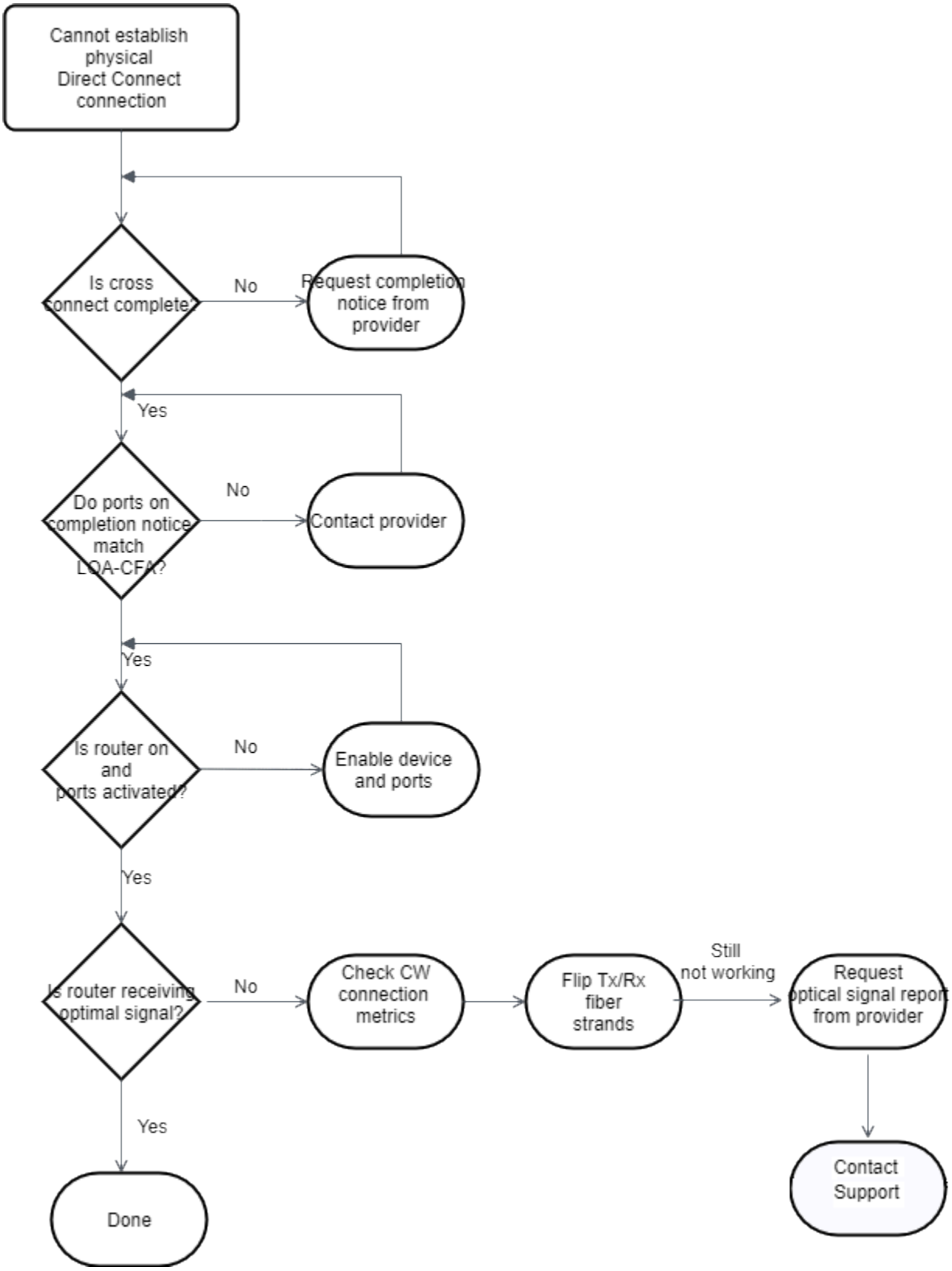
Behandlung von Problemen auf Ebene 1 (physisch)

Wenn Sie oder Ihr Netzwerkanbieter Schwierigkeiten haben, eine physische Konnektivität zu einem - AWS Direct Connect Gerät herzustellen, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

1. Überprüfen Sie beim Co-Location-Anbieter, dass die Querverbindung abgeschlossen ist. Bitten Sie den Co-Location-Anbieter oder Ihren Netzanbieter, Ihnen eine Abschlussbenachrichtigung über die Querverbindung bereitzustellen und vergleichen Sie die Ports mit denen in Ihrem LOA-CFA-Dokument.
2. Stellen Sie sicher, dass Ihr Router bzw. der Router Ihres Anbieters eingeschaltet ist und dass die Ports aktiviert wurden.
3. Stellen Sie sicher, dass die Router den richtigen optischen Transceiver verwenden. Die Auto-Negotiation für den Port muss deaktiviert sein, wenn Sie eine Verbindung mit einer Portgeschwindigkeit von mehr als 1 Gbit/s haben. Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bedient, muss die automatische Aushandlung jedoch möglicherweise für 1-Gbit/s-Verbindungen aktiviert oder deaktiviert werden. Wenn die Auto-Negotiation für Ihre Verbindungen deaktiviert werden muss, müssen die Portgeschwindigkeit und der Vollduplexmodus manuell konfiguriert werden. Wenn Ihre virtuelle Schnittstelle weiterhin nicht verfügbar ist, finden Sie weitere Informationen unter Behandlung von Problemen auf Ebene 2 (Datenverbindung).
4. Überprüfen Sie, ob der Router ein akzeptables optisches Signal über die Querverbindung erhält.
5. Versuchen Sie, die Tx/Rx-Faserstränge umzudrehen bzw. zu wenden.

6. Überprüfen Sie die Amazon- CloudWatch Metriken für AWS Direct Connect. Sie können die visuellen Tx/Rx-Messungen des AWS Direct Connect Geräts (1 Gbit/s und 10 Gbit/s), die physische Fehleranzahl und den Betriebsstatus überprüfen. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.
7. Wenden Sie sich an den Co-Location-Anbieter und fordern Sie einen schriftlichen Bericht über das optische Tx/Rx-Signal über die Querverbindung an.
8. Wenn sich die Probleme mit der physischen Verbindung nicht mit den oben genannten Schritten lösen lassen, wenden Sie sich an den AWS Support. Stellen Sie die Abschlussbenachrichtigung über die Querverbindung und den Bericht über das optische Signal des Co-Location-Anbieters bereit.

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Problemen mit der physischen Verbindung.

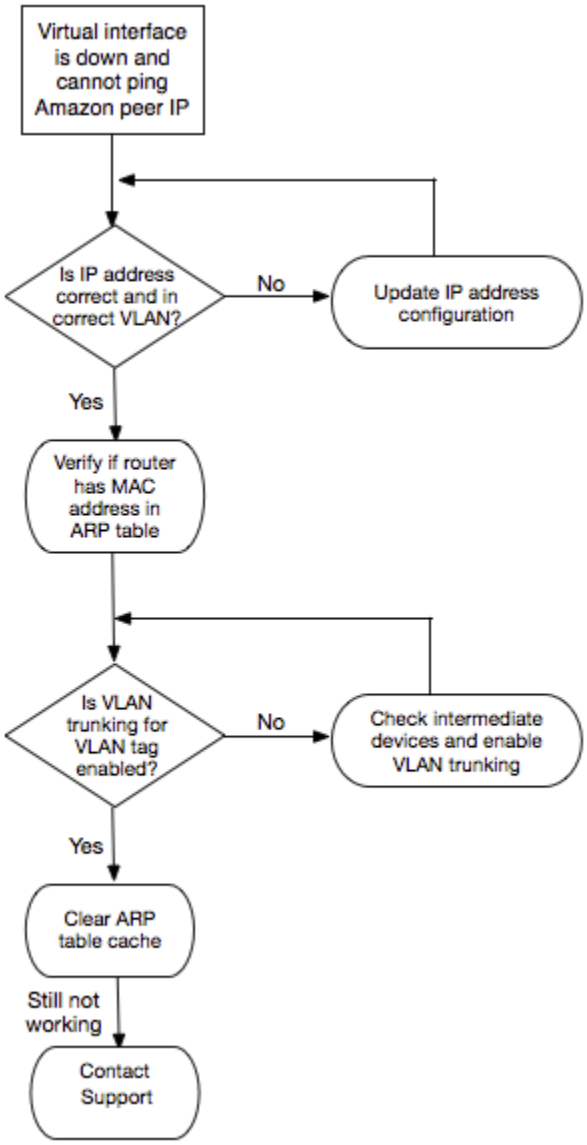

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Behandlung von Problemen auf Ebene 2 (Datenverbindung)

Wenn Ihre AWS Direct Connect physische Verbindung aktiv ist, Ihre virtuelle Schnittstelle jedoch ausgefallen ist, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

1. Wenn Sie die Amazon-Peer-IP-Adresse nicht anpingen können, vergewissern Sie sich, dass Ihre Peer-IP-Adresse korrekt und im richtigen VLAN konfiguriert ist. Stellen Sie sicher, dass die IP-Adresse in der VLAN-Subschnittstelle und nicht in der physischen Schnittstelle konfiguriert ist (z. B. GigabitEthernet0/0.123 anstelle von GigabitEthernet0/0).
2. Überprüfen Sie, ob der Router über einen MAC-Adresseintrag vom AWS Endpunkt in Ihrer ARP-Tabelle (Address Resolution Protocol) verfügt.
3. Stellen Sie sicher, dass für alle zwischengeschalteten Geräte zwischen Endpunkten für Ihren 802.1Q VLAN-Tag VLAN-Trunking aktiviert ist. ARP kann auf der - AWS Seite erst eingerichtet werden, wenn markierten Datenverkehr AWS empfängt.
4. Löschen Sie den Cache Ihrer ARP-Tabelle oder der Ihres Anbieters.
5. Wenn die obigen Schritte keine ARP einrichten oder Sie immer noch keinen Ping an die Amazon-Peer-IP senden können, wenden Sie sich an AWS den Support .

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Problemen mit der Datenverbindung.



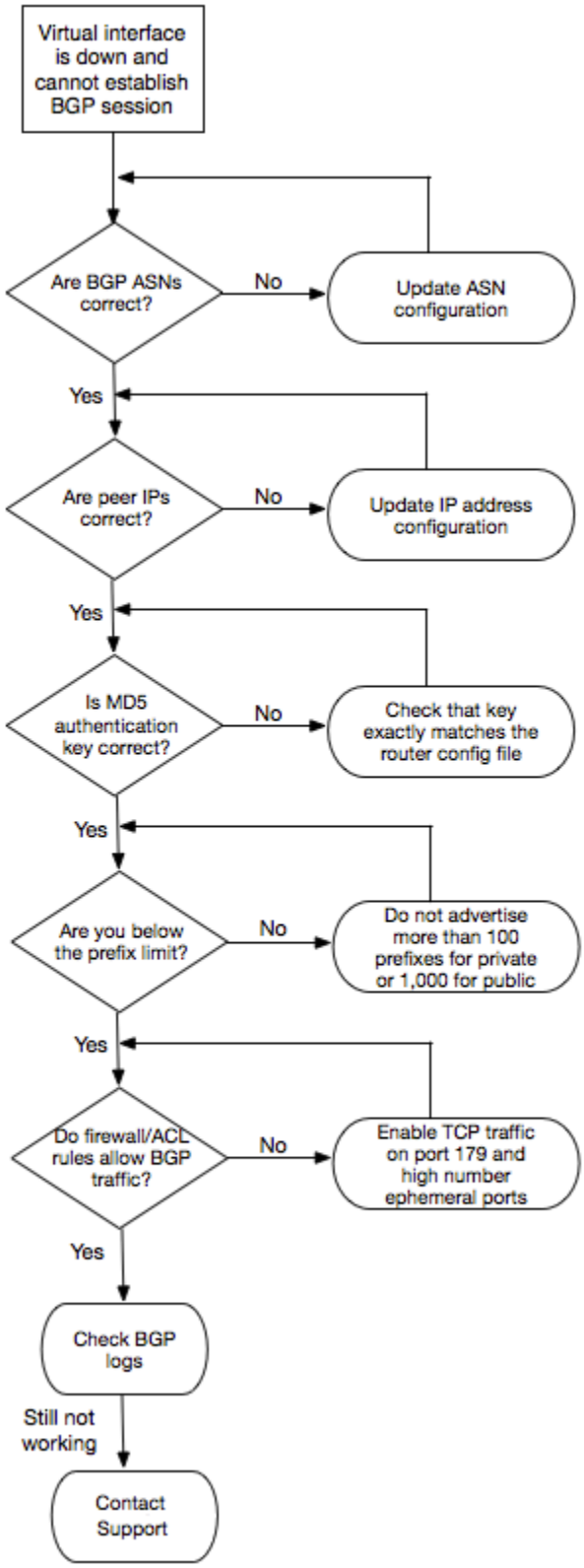
Wenn die BGP-Sitzung auch nach Überprüfen dieser Schritte nicht hergestellt werden kann, lesen Sie Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport). Wenn die BGP-Sitzung zwar hergestellt wurde, Sie aber Probleme mit dem Routing haben, lesen Sie Beheben von Routing-Problemen.

Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport)

Stellen Sie sich eine Situation vor, in der Ihre AWS Direct Connect physische Verbindung aktiv ist und Sie die Amazon-Peer-IP-Adresse pingen können. Wenn Ihre virtuelle Schnittstelle ausgefallen ist und die BGP-Peering-Sitzung nicht hergestellt werden kann, führen Sie die folgenden Schritte aus, um das Problem zu beheben:

1. Stellen Sie sicher, dass Ihre lokale BGP-ASN (Autonomous System Number) und die Amazon-ASN korrekt konfiguriert sind.
2. Stellen Sie sicher, dass die Peer-IPs für beide Seiten der BGP-Peering-Sitzung korrekt konfiguriert sind.
3. Stellen Sie sicher, dass der MD5-Authentifizierungsschlüssel konfiguriert ist und genau mit dem Schlüssel in der heruntergeladenen Router-Konfigurationsdatei übereinstimmt. Stellen Sie außerdem sicher, dass keine zusätzlichen Leerzeichen oder Zeichen vorhanden sind.
4. Vergewissern Sie sich, dass Sie bzw. Ihr Anbieter nicht mehr als 100 Präfixe für private virtuelle Schnittstellen bzw. 1.000 Präfixe für öffentliche virtuelle Schnittstellen ankündigen. Dies sind feste Grenzen, die nicht überschritten werden dürfen.
5. Stellen Sie sicher, dass keine Firewall oder ACL-Regeln den TCP-Port 179 oder flüchtige TCP-Ports mit hohen Nummern blockieren. Diese Ports sind erforderlich, damit BGP eine TCP-Verbindung zwischen den Peers herstellen kann.
6. Überprüfen Sie Ihre BGP-Protokolle auf Fehler oder Warnmeldungen.
7. Wenn die BGP-Peering-Sitzung mit den obigen Schritten nicht eingerichtet wird, wenden Sie sich an den - AWS Support.

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Problemen mit der BGP-Peering-Sitzung.



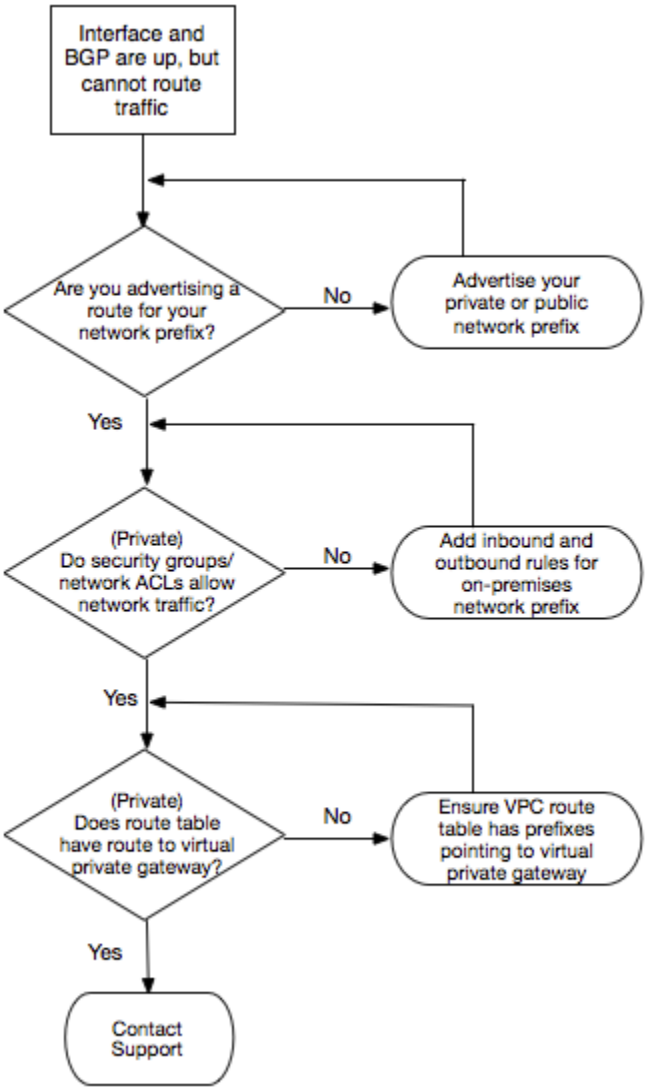
Wenn die BGP-Peering-Sitzung hergestellt wurde, Sie aber Probleme mit dem Routing haben, lesen Sie Beheben von Routing-Problemen.

Beheben von Routing-Problemen

Angenommen, Ihre virtuelle Schnittstelle ist betriebsbereit und Sie haben eine BGP-Peering-Sitzung hergestellt. Wenn Sie keinen Datenverkehr über die virtuelle Schnittstelle leiten können, führen Sie die folgenden Schritte aus, um das Problem zu beheben:

1. Stellen Sie sicher, dass Sie für Ihren lokalen Netzwerkpräfix über die BGP-Sitzung eine Route ankündigen. Bei einer privaten virtuellen Schnittstelle kann es sich dabei um einen privaten oder öffentlichen Netzwerkpräfix handeln. Bei einer öffentlichen virtuellen Schnittstelle muss dies Ihr öffentlich routingfähiger Netzwerkpräfix sein.
2. Stellen Sie bei einer privaten virtuellen Schnittstelle sicher, dass Ihre VPC-Sicherheitsgruppen und Netzwerk-ACLs ein- und ausgehenden Datenverkehr für Ihren lokalen Netzwerkpräfix zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen und Netzwerk-ACLs im Amazon-VPC-Benutzerhandbuch.
3. Stellen Sie bei einer privaten virtuellen Schnittstelle sicher, dass die Präfixe in Ihren VPC-Routing-Tabellen auf das virtuelle private Gateway verweisen, mit dem Ihre private virtuelle Schnittstelle verbunden ist. Wenn Sie zum Beispiel möchten, dass der gesamte Datenverkehr standardmäßig an Ihr lokales Netzwerk weitergeleitet wird, können Sie die Standardroute (0.0.0.0/0 oder ::/0) mit dem Virtual Private Gateway als Ziel in Ihren VPC-Routing-Tabellen hinzufügen.
   - Alternativ können Sie die Routing-Verbreitung aktivieren, um Routen in den Routing-Tabellen automatisch basierend auf Ihrer dynamischen BGP-Routing-Ankündigung zu aktualisieren. Es können bis zu 100 propagierte Routen pro Routing-Tabelle vorhanden sein. Dieses Limit kann nicht erhöht werden. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren der Routing-Verbreitung im Amazon-VPC-Benutzerhandbuch.
4. Wenn die obigen Schritte Ihre Routing-Probleme nicht beheben, wenden Sie sich an den - AWS Support.

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Routing-Problemen.


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

Dokumentverlauf

In der folgenden Tabelle werden die Veröffentlichungen für AWS Direct Connect beschrieben.

Funktion	Beschreibung	Datum
Support für SiteLink	Sie können eine virtuelle private Schnittstelle erstellen, die Konnektivität zwischen zwei Direct Connect-Points of Presence (PoPs) in derselben AWS Region ermöglicht. Weitere Informati onen finden Sie unter Gehostete virtuelle Schnittstellen.	2021-12-01
Support für MAC Security	Sie können AWS Direct Connect-Verbindungen verwenden, die MACsec unterstützen, um Ihre Daten von Ihrem Unternehm ensrechenzentrum zum AWS Direct Connect-Standort zu verschlüsseln. Weitere Informationen finden Sie unter MAC Security.	31.03.2021
Unterstüt zung für 100G	Aktualisierte Inhalte um Support für dedizierte 100G-Verb indungen mit einzubeziehen.	12.02.2021
Neuer Standort in Italien	Thema wurde aktualisiert, um das Hinzufügen des neuen Standorts in Italien einzuschließen. Weitere Informationen finden Sie unter the section called “Europa (Milan)”.	22.01.2021
Neuer Standort in Israel	Thema wurde aktualisiert, um das Hinzufügen des neuen Standorts in Israel einzuschließen. Weitere Informationen finden Sie unter the section called “Israel (Tel Aviv)”.	07.07.2020
Unterstüt zung für Failover-Test des Resilienz -Toolkits	Verwenden Sie die Funktion „Failover-Test des Resilienz-Toolkits“, um die Ausfallsicherheit Ihrer Verbindungen zu testen. Weitere Informationen finden Sie unter the section called “AWS Direct Connect-Failover-Test”.	2020-06-03
CloudWatc h Unterstüt	Sie können physische AWS Direct Connect Verbindungen und virtuelle Schnittstellen mithilfe von CloudWatch überwache	11.05.2020

Funktion	Beschreibung	Datum
zung von VIF-Metriken	n. Weitere Informationen finden Sie unter the section called “Überwachung mit Amazon CloudWatch”.	
AWS Direct Connect Resiliency Toolkit	Das AWS Direct Connect Resiliency Toolkit bietet einen Verbindungsassistenten mit mehreren Resilienzmodellen, mit denen Sie dedizierte Verbindungen bestellen können, um Ihr SLA-Ziel zu erreichen. Weitere Informationen finden Sie unter Verwenden Sie das AWS Direct Connect Resiliency Toolkit für den Einstieg.	07.10.2019
Zusätzliche Regionsunterstützung zur kontenübergreifenden Unterstützung von AWS Transit Gateway	Weitere Informationen finden Sie unter the section called “Transit-Gateway-Zuordnungen”.	30.09.2019
AWS Direct Connect-Unterstützung für AWS Transit Gateway	Sie können ein AWS Direct Connect-Gateway verwenden, um Ihre AWS Direct Connect-Verbindung über eine virtuelle Transit-Schnittstelle mit den VPCs oder VPNs zu verbinden, die Ihrem Transit Gateway angefügt sind. Dann erstellen Sie eine virtuelle Transit-Schnittstelle für Ihre AWS Direct Connect-Verbindung zum Direct Connect-Gateway. Weitere Informationen finden Sie unter the section called “Transit-Gateway-Zuordnungen”.	2019-03-27
Unterstützung von Jumbo-Frames	Sie können Jumbo-Frames (9 001 MTU) über AWS Direct Connect senden. Weitere Informationen finden Sie unter Die Netzwerk-MTU für private virtuelle Schnittstellen oder virtuelle Transit-Schnittstellen festlegen.	11.10.2018

Funktion	Beschreibung	Datum
BGP-Communitys mit lokalen Präferenzen	Mit BGP-Community-Tags für lokale Präferenzen erreichen Sie Lastausgleich und Routing-Präferenzen für eingehenden Datenverkehr mit Ihrem Netzwerk. Weitere Informationen finden Sie unter BGP-Communitys mit lokalen Präferenzen.	06.02.2018
AWS Direct Connect-Gateway	Mit einem Direct Connect-Gateway können Sie eine AWS Direct Connect-Verbindung mit VPCs in abgelegenen Regionen herstellen. Weitere Informationen finden Sie unter Arbeiten mit Direct Connect-Gateways.	01.11.2017
CloudWatch Amazon-Metriken	Sie können CloudWatch Metriken für Ihre AWS Direct Connect Verbindungen einsehen. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.	29.06.2017
Link Aggregation Groups (LAG)	Sie können eine Link Aggregation Group (LAG) erstellen, um mehrere AWS Direct Connect-Verbindungen zu aggregieren. Weitere Informationen finden Sie unter Link Aggregation Groups (LAG).	13.02.2017
IPv6-Support	Ihre virtuelle Schnittstelle unterstützt nun eine IPv6-BGP-Peering-Session. Weitere Informationen finden Sie unter Einen BGP-Peer hinzufügen oder löschen.	01.12.2016
Unterstütze Markierungen	Sie können nun Ihre AWS Direct Connect-Ressourcen taggen. Weitere Informationen finden Sie unter Markieren von AWS Direct Connect-Ressourcen.	04.11.2016
Self-Service-LOA-CFA	Sie können jetzt Ihr "Letter of Authorization and Connecting Facility Assignment" (LOA-CFA) mithilfe der AWS Direct ConnectKonsole oder der API herunterladen.	22.06.2016
Neuer Standort in Silicon Valley	Thema wurde aktualisiert, um den neuen Standort Silicon Valley in die Region USA West (Nordkalifornien) mit einzubeziehen.	03.06.2016

Funktion	Beschreibung	Datum
Neuer Standort in Amsterdam	Thema wurde aktualisiert, um den neuen Standort Amsterdam in die Region Europa (Frankfurt) mit einzubeziehen.	19.05.2016
Neue Standorte in Portland, Oregon und Singapur	Thema wurde aktualisiert, um die neuen Standorte Portland, Oregon und Singapur in die Regionen USA West (Oregon) und Asien-Pazifik (Singapur) mit einzubeziehen.	27.04.2016
Neuer Standort in Sao Paulo, Brasilien	Thema wurde aktualisiert, um den neuen Standort Sao Paulo in die Region Südamerika (São Paulo) mit einzubeziehen.	09.12.2015
Neue Standorte in Dallas, London, Silicon Valley und Mumbai	Die Themen wurden aktualisiert und beinhalten nun die Hinzufügung der neuen Standorte in Dallas (Region USA Ost (Nord-Virginia)), London (Region Europa (Irland)), Silicon Valley AWS GovCloud (Region US-West)) und Mumbai (Region Asien-Pazifik (Singapur)).	27.11.2015
Neuer Standort in der Region China (Peking)	Themen wurden aktualisiert, um den neuen Standort Peking in die Region China (Peking) mit einzubeziehen.	14.04.2015
Neuer Las Vegas-Standort in der Region USA West (Oregon)	Themen wurden aktualisiert, um den neuen AWS Direct Connect-Standort Las Vegas in die Region USA West (Oregon) mit einzubeziehen.	10.11.2014

Funktion	Beschreibung	Datum
Neue Region EU (Frankfurt)	Themen wurden aktualisiert, um die neuen AWS Direct Connect-Standorte für die Region EU (Frankfurt) mit einzubeziehen.	23.10.2014
Neue Standorte in der Region Asien-Pazifik (Sydney)	Themen wurden aktualisiert, um die neuen AWS Direct Connect-Standorte für die Region Asien-Pazifik (Sydney) mit einzubeziehen.	14.07.2014
Unterstützung fü AWS CloudTrail	Es wurde ein neues Thema hinzugefügt, das erklärt, wie Sie CloudTrail damit Aktivitäten protokollieren können. AWS Direct Connect Weitere Informationen finden Sie unter Protokollieren von AWS Direct Connect-API-Aufrufen mithilfe von AWS CloudTrail.	04.04.2014
Support für den Zugriff auf entfernte AWS-Regionen	Neues Thema hinzugefügt, um zu erklären, wie Sie Zugriff auf öffentliche Ressourcen in einer entfernten Region erhalten. Weitere Informationen finden Sie unter Remote-Zugriff auf eine AWS-Region.	19.12.2013
Support für gehostete Verbindungen	Aktualisierte Inhalte um Support für gehostete Verbindungen mit einzubeziehen.	22.10.2013
Neuer Standort in der Region EU (Irland)	Themen wurden aktualisiert, um den neuen AWS Direct Connect-Standort für die Region EU (Irland) mit einzubeziehen.	24.06.2013

Funktion	Beschreibung	Datum
Neuer Seattle-Standort in der Region USA West (Oregon)	Themen wurden aktualisiert, um den neuen AWS Direct Connect-Standort in Seattle für die Region USA West (Oregon) mit einzubeziehen.	08.05.2013
Unterstützung der Nutzung von IAM mit AWS Direct Connect	Neuer Inhalt über die Verwendung von AWS Identity and Access Management mit AWS Direct Connect hinzugefügt. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.	21.12.2012
Neue Region Asien-Pazifik (Sydney)	Themen wurden aktualisiert, um den neuen AWS Direct Connect-Standort für die Region Asien-Pazifik (Sydney) mit einzubeziehen.	14.12.2012
Neue AWS Direct Connect-Konsole und die Regionen USA Ost (Nord-Virginia) und Südamerika (São Paulo).	Das AWS Direct Connect-Handbuch "Erste Schritte" wurde durch das AWS Direct Connect-Benutzerhandbuch ersetzt. Es wurden neue Themen hinzugefügt, um die neue AWS Direct Connect-Konsole abzudecken, und Fakturierungsinhalte, Router-Konfigurationsinformationen und aktualisierte Themen hinzugefügt, um die beiden neuen AWS Direct Connect-Standorte für die Region USA Ost (Nord-Virginia) und Südamerika (São Paulo) mit einzubeziehen.	13.08.2012

Funktion	Beschreibung	Datum
Support für die Regionen EU (Irland), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio)	Abschnitt zur Fehlerbehebung hinzugefügt und Themen aktualisiert, um vier neue AWS Direct Connect-Standorte für die Region USA West (Nordkalifornien), EU (Irland), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) mit einzubeziehen.	10.01.2012
Support für die Region USA West (Nordkalifornien)	Themen wurden aktualisiert, um die Region USA West (Nordkalifornien) mit einzubeziehen.	08.09.2011
Öffentliche Freigabe	Die erste Veröffentlichung von AWS Direct Connect.	03.08.2011

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.