User Guide

AWS Direct Connect

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Direct Connect: User Guide

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Direct Connect? ... 1
Direct Connect-Komponenten ... 2
Netzwerkanforderungen ... 2
Unterstützte virtuelle Direct Connect-Schnittstellentypen ... 3
Preise für Direct Connect ... 4
Zugang zu abgelegenen AWS Regionen ... 5
Zugriff auf öffentliche Dienste in einer abgelegenen Region ... 5
Zugriff auf VPCs in einer entfernten Region ... 6
Network-to-Amazon VPC-Konnektivitätsoptionen ... 6
Routing policies and BGP communities ... 6
Routing-Richtlinien für öffentliche virtuelle Schnittstellen ... 6
Public Virtual Interface BGP-Communitys ... 8
Routing-Richtlinien für Private Virtual Interface und Transit Virtual Interface ... 10
Beispiel für privates virtuelles Schnittstellen-Routing ... 12
AWS Direct Connect Toolkit für Resilienz ... 15
Voraussetzungen ... 17
Maximale Ausfallsicherheit ... 19
Hohe Ausfallsicherheit ... 20
Entwicklung und Test ... 21
Classic ... 22
Voraussetzungen ... 22
Failover-Test ... 23
Konfigurieren Sie maximale Resilienz ... 23
Schritt 1: Melden Sie sich an für AWS ... 24
Schritt 2: Konfigurieren des Resilienzmodells ... 26
Schritt 3: Erstellen Ihrer virtuellen Schnittstellen ... 27
Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle ... 36
Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen ... 36
Konfigurieren Sie eine hohe Ausfallsicherheit ... 37
Schritt 1: Melden Sie sich an für AWS ... 37
Schritt 2: Konfigurieren des Resilienzmodells ... 39
Schritt 3: Erstellen Ihrer virtuellen Schnittstellen ... 41
Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle ... 50
Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen ... 50

Konfigurieren Sie die Entwicklungs- und Testausfallsicherheit 51
Schritt 1: Melden Sie sich an für AWS 51
Schritt 2: Konfigurieren des Resilienzmodells 53
Schritt 3: Erstellen einer virtuellen Schnittstelle 54
Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle 64
Schritt 5: Überprüfen Ihrer virtuellen Schnittstelle 64
Konfigurieren Sie eine Classic-Verbindung 65
Schritt 1: Melden Sie sich an für AWS 65
Schritt 2: Fordern Sie eine AWS Direct Connect dedizierte Verbindung an 67
(Dedizierte Verbindung) Schritt 3: Herunterladen des LOA-CFA 69
Schritt 4: Erstellen einer virtuellen Schnittstelle 70
Schritt 5: Herunterladen der Routerkonfiguration 79
Schritt 6: Überprüfen der virtuellen Schnittstelle 80
(Empfohlen) Schritt 7: Konfigurieren redundanter Verbindungen 81
Direct Connect-Failovertest 83
Verlauf des Tests 84
Validierungsberechtigungen 84
Starten Sie einen Failover-Test für virtuelle Schnittstellen 85
Den Failover-Testverlauf einer virtuellen Schnittstelle anzeigen 86
Beenden Sie einen Failover-Test für virtuelle Schnittstellen 86
Direct Connect-Wartung 88
Geplante Wartung 88
..... 88
Wartung im Notfall 89
Wartung durch Dritte 90
Vorbereitung von Wartungsereignissen 90
Validierung der Resilienz 91
Verschiebung der Wartungsveranstaltung 91
MAC-Sicherheit (MACsec) 92
MACsec Konzepte 92
MACsec Schlüsselrotation 94
Unterstützte Verbindungen 94
Dedizierte Verbindungen 95
LAGs 96
Serviceverknüpfte Rollen 96
MACsec Wichtige Überlegungen zu vorab geteilten CKN/CAKs 97

Beginnen Sie mit MACsec einer dedizierten Verbindung 97
Eine Verbindung erstellen 98
(Optional) Erstellen Sie eine LAG 98
Ordnen Sie das CKN/CAK der Verbindung oder LAG zu 98
Konfigurieren Sie Ihren lokalen Router 98
Entfernen Sie die Zuordnung zwischen dem CKN/CAK und der Verbindung oder LAG 98
Dedizierte und gehostete Verbindungen 99
Dedizierte Verbindungen 99
Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA) 101
Eine Verbindung mit dem Verbindungsassistenten erstellen 102
Eine Classic-Verbindung erstellen 104
Das LOA-CFA-Dokument herunterladen 106
Ordnen Sie ein MACsec CKN/CAK einer Verbindung zu 107
Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer Verbindung 108
Gehostete Verbindungen 108
Eine gehostete Verbindung akzeptieren 110
Eine Verbindung löschen 111
Aktualisieren einer Verbindung 112
Anzeigen von Verbindungsdetails 113
Querverbindungen 115
Verbindungsoptionen 116
USA Ost (Ohio) 117
USA Ost (Nord-Virginia) 117
USA West (Nordkalifornien) 119
USA West (Oregon) 120
Afrika (Kapstadt) 120
Asien-Pazifik (Jakarta) 121
Asien-Pazifik (Mumbai) 121
Asien-Pazifik (Seoul) 122
Asien-Pazifik (Singapur) 122
Asien-Pazifik (Sydney) 123
Asien-Pazifik (Tokio) 123
Kanada (Zentral) 124
China (Peking) 124
China (Ningxia) 125

Europa (Frankfurt) ... 125
Europa (Irland) ... 126
Europa (Milan) ... 127
Europa (London) ... 127
Europa (Paris) ... 128
Europa (Stockholm) ... 128
Europa (Zürich) ... 128
Israel (Tel Aviv) ... 128
Naher Osten (Bahrain) ... 129
Naher Osten (VAE) ... 129
Südamerika (São Paulo) ... 130
AWS GovCloud (US-Ost) ... 130
AWS GovCloud (US-West) ... 130
Virtuelle Schnittstellen und gehostete virtuelle Schnittstellen ... 131
Werberegeln für das Public Virtual Interface-Präfix ... 131
SiteLink ... 132
Voraussetzungen für virtuelle Schnittstellen ... 134
MTUs für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen ... 141
Virtuelle Schnittstellen ... 142
Voraussetzungen für die Übertragung virtueller Schnittstellen zu einem Direct Connect-Gateway ... 143
Eine öffentliche virtuelle Schnittstelle erstellen ... 143
Eine private virtuelle Schnittstelle erstellen ... 146
Eine virtuelle Transit-Schnittstelle für das Direct-Connect-Gateway erstellen ... 149
Routerkonfigurationsdatei herunterladen ... 151
Gehostete virtuelle Schnittstellen ... 153
Eine gehostete private virtuelle Schnittstelle erstellen ... 158
Eine gehostete öffentliche virtuelle Schnittstelle erstellen ... 161
Eine gehostete virtuelle Transit-Schnittstelle erstellen ... 163
Details der virtuellen Schnittstelle anzeigen ... 165
Ein BGP-Peer hinzufügen ... 166
Ein BGP-Peer löschen ... 168
Legen Sie die MTU einer privaten virtuellen Schnittstelle fest ... 169
Tags für virtuelle Schnittstellen hinzufügen oder entfernen ... 169
Löschen Sie eine virtuelle Schnittstelle ... 170
Eine gehostete virtuelle Schnittstelle akzeptieren ... 171

Eine virtuelle Schnittstelle migrieren ... 172
Aggregationsgruppen verknüpfen () LAGs ... 174
MACsec Überlegungen ... 176
Eine LAG erstellen ... 176
LAG-Details anzeigen ... 179
Eine LAG aktualisieren ... 180
Eine Verbindung mit einer LAG verknüpfen ... 181
Die Verknüpfung einer Verbindung mit einer LAG aufheben ... 182
Ordnen Sie ein MACsec CKN/CAK einer LAG zu ... 183
Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer LAG ... 184
Löschen Sie eine LAG ... 185
Gateways ... 186
Direct Connect-Gateways ... 187
Szenarien ... 189
Erstellen Sie ein Direct Connect-Gateway ... 192
Migrieren Sie von einem Virtual Private Gateway zu einem Direct Connect Gateway ... 193
Löschen Sie ein Direct Connect-Gateway ... 194
Virtual Private Gateway-Zuordnungen ... 195
Erstellen eines Virtual Private Gateways ... 197
Ordnen Sie virtuelle private Gateways zu oder trennen Sie die Zuordnung ... 198
Erstellen Sie eine private virtuelle Schnittstelle zum Direct Connect-Gateway ... 199
Ordnen Sie ein virtuelles privates Gateway kontenübergreifend zu ... 202
Transit-Gateway-Zuordnungen ... 203
Zuordnen eines Transit-Gateways über Konten hinweg ... 204
Ordnen Sie Direct Connect ein Transit-Gateway zu oder trennen Sie die Verknüpfung. ... 205
Eine virtuelle Transit-Schnittstelle für das Direct-Connect-Gateway erstellen ... 207
Erstellen Sie einen Vorschlag für die Zuordnung eines Transit-Gateways ... 210
Akzeptieren oder lehnen Sie einen Vorschlag zur Verknüpfung eines Transit-Gateways ab . 211
Aktualisieren Sie die zulässigen Präfixe für eine Transit-Gateway-Verknüpfung ... 212
Löschen Sie einen Vorschlag für eine Transit-Gateway-Verbindung ... 213
Zuordnungen zu Cloud-WAN-Kernnetzwerken ... 214
Voraussetzungen ... 216
Überlegungen ... 216
Direct Connect-Gateway-Zuordnungen zu einem Cloud-WAN-Kernnetzwerk ... 217
Überprüfen Sie eine Direct Connect-Gateway-Zuordnung ... 218
Interaktionen zulässiger Präfixe ... 218

Virtual Private Gateway-Zuordnungen 219
Transit-Gateway-Zuordnungen 219
Beispiel: Zulässig für Präfixe in einer Transit-Gateway-Konfiguration 220
Markieren von Ressourcen 223
Tag-Einschränkungen 224
Arbeiten mit Tags mittels CLI oder API 225
Beispiele 225
Sicherheit 227
Datenschutz 228
Richtlinie für den Datenverkehr zwischen Netzwerken 229
Verschlüsselung 229
Identitäts- und Zugriffsverwaltung 230
Zielgruppe 231
Authentifizierung mit Identitäten 231
Verwalten des Zugriffs mit Richtlinien 235
Funktionsweise von Direct Connect mit IAM 238
Beispiele für identitätsbasierte Richtlinien für Direct Connect 245
Service-verknüpfte Rollen 257
AWS verwaltete Richtlinien 261
Fehlerbehebung 263
Protokollierung und Überwachung 265
Compliance-Validierung 265
Resilienz bei Direct Connect 266
Failover 267
Sicherheit der Infrastruktur 268
Border Gateway Protocol 268
Verwenden Sie die AWS CLI 269
Schritt 1: Erstellen einer Verbindung 269
Schritt 2: Herunterladen des LOA-CFA-Dokuments 270
Schritt 3: Erstellen einer virtuellen Schnittstelle und Abrufen der Router-Konfiguration 271
Protokollieren von -API-Aufrufen 277
AWS Direct Connect Informationen in CloudTrail 277
AWS Direct Connect Logdateieinträge verstehen 278
Direct Connect-Ressourcen überwachen 283
Überwachungstools 283
Automatisierte Überwachungstools 284

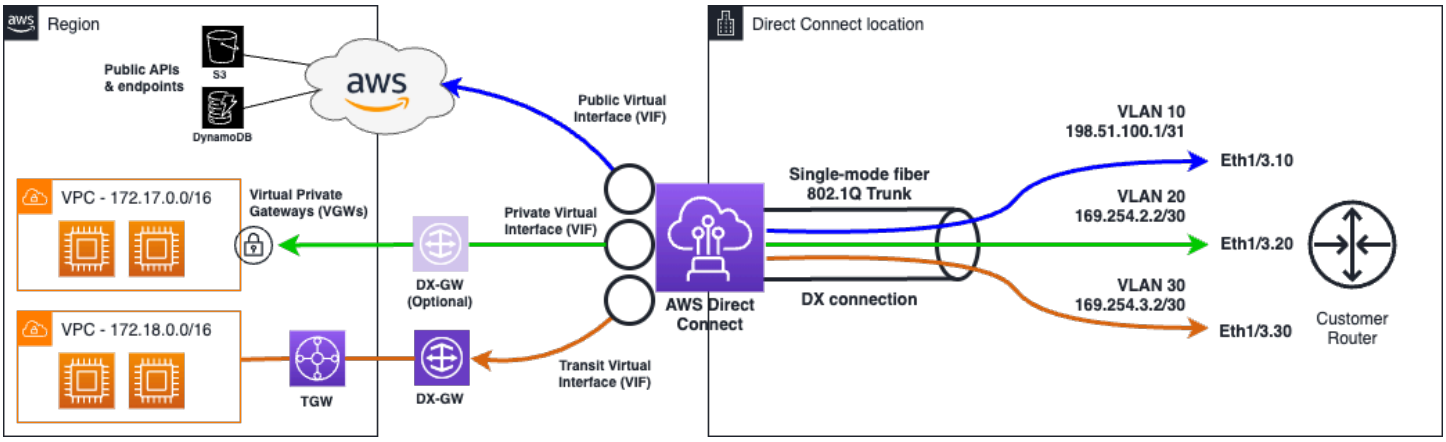
Manuelle Überwachungstools 284
Überwachen Sie mit Amazon CloudWatch 285
AWS Direct Connect Metriken und Dimensionen 285
Direct CloudWatch Connect-Kennzahlen anzeigen 292
Erstellen Sie Alarme zur Überwachung von Verbindungen 294
Direct Connect-Kontingente 296
BGP-Kontingente 300
Überlegungen zu Load Balancing 300
Fehlerbehebung 301
Probleme auf Ebene 1 (physisch) 301
Probleme auf Ebene 2 (Datenverbindung) 304
Probleme auf Ebene 3/4 (Netzwerk/Transport) 305
Routing-Probleme 308
Dokumentverlauf 310
..... cccxviii

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.

- Eine Liste der Direct Connect-Standorte, mit denen Sie eine Connect können, finden Sie unter AWS Direct Connect-Standorte.
- Antworten auf Fragen zu Direct Connect finden Sie in den häufig gestellten Fragen zu Direct Connect.

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



Inhalt

- AWS Direct Connect Komponenten
- Netzwerkanforderungen
- Unterstützte virtuelle Direct Connect-Schnittstellentypen
- Preise für Direct Connect
- Zugang zu abgelegenen AWS Direct Connect Regionen

- AWS Direct Connect Routing-Richtlinien und BGP-Communities

AWS Direct Connect Komponenten

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

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 dedizierte und gehostete 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. Die unterstützten Schnittstellentypen werden weiter unten unter beschriebenthe section called “Unterstützte virtuelle Direct Connect-Schnittstellentypen”. Weitere Informationen zu den unterstützten Schnittstellen finden Sie unter AWS Direct Connect virtuelle Schnittstellen und gehostete virtuelle Schnittstellen undVoraussetzungen 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, einem 100GBASE- für 100-Gigabit-Ethernet oder einem 400GBASE- für 400-Gbit/s-Ethernet verwenden. LR4 LR4
- Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bereitstellt, muss die automatische Aushandlung von lokalen Geräten möglicherweise für jede dedizierte Verbindung aktiviert oder deaktiviert werden. Wenn eine virtuelle Schnittstelle ausgefallen bleibt, während eine Direct Connect-Verbindung besteht, finden Sie weitere Informationen unterBehandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss das Border Gateway Protocol (BGP) und die BGP-Authentifizierung MD5 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 als auch die IPv4 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 MTUs für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen.

Unterstützte virtuelle Direct Connect-Schnittstellentypen

AWS Direct Connect unterstützt die folgenden drei Typen virtueller Schnittstellen (VIF):

- Private virtuelle Schnittstelle

  Diese Art von Schnittstelle wird verwendet, um über private IP-Adressen auf eine Amazon Virtual Private Cloud (VPC) zuzugreifen. Mit einer privaten virtuellen Schnittstelle können Sie

  - Stellen Sie über eine private virtuelle Schnittstelle eine direkte Connect zu einer einzelnen VPC her, um über Private IPs in derselben Region auf diese Ressourcen zuzugreifen.
  - Connect eine private virtuelle Schnittstelle mit einem Direct Connect-Gateway, um auf mehrere virtuelle private Gateways in jedem Konto und jeder AWS Region (außer den Regionen in AWS China) zuzugreifen.
- Öffentliche virtuelle Schnittstelle

  Diese Art von virtueller Schnittstelle wird für den Zugriff auf alle AWS öffentlichen Dienste über öffentliche IP-Adressen verwendet. Mit einer öffentlichen virtuellen Schnittstelle können Sie eine Verbindung zu allen AWS öffentlichen IP-Adressen und Diensten weltweit herstellen.
- Virtuelle Schnittstelle für den Transit

  Dieser Schnittstellentyp wird für den Zugriff auf ein oder mehrere Amazon VPC Transit Gateways verwendet, die Direct Connect-Gateways zugeordnet sind. Mit einer virtuellen Transitschnittstelle verbinden Sie mehrere Amazon VPC Transit Gateways über mehrere Konten und AWS-Regionen (mit Ausnahme der Regionen AWS China).

  > **Note**
  >
  > Die Anzahl der verschiedenen Zuordnungstypen zwischen einem Direct Connect-Gateway und einer virtuellen Schnittstelle ist begrenzt. Weitere Informationen zu bestimmten Grenzwerten finden Sie Direct Connect-Kontingente auf der Seite.

Weitere Informationen zu virtuellen Schnittstellen finden Sie unterVirtuelle Schnittstellen und gehostete virtuelle Schnittstellen.

Preise für Direct Connect

AWS Direct Connect beinhaltet 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, EC2 Classic-Instances oder EC2 Datenverkehr, der über ein Internet-Gateway läuft) 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.

Zugang zu abgelegenen AWS Direct Connect Regionen

AWS Direct Connect Standorte in öffentlichen Regionen oder AWS GovCloud (US) Zugang zu öffentlichen Diensten in jeder anderen öffentlichen Region (außer China (Peking und Ningxia)). Darüber hinaus AWS GovCloud (US) können AWS Direct Connect Verbindungen in öffentlichen Regionen oder für den Zugriff auf eine VPC in Ihrem Konto in einer anderen öffentlichen Region (außer China) (Peking und Ningxia) konfiguriert werden. Sie können daher mit einer einzelnen AWS Direct Connect -Verbindung Services für mehrere Regionen aufbauen. Der gesamte Netzwerkverkehr verbleibt auf dem AWS globalen Netzwerk-Backbone, unabhängig davon, ob Sie auf öffentliche AWS Dienste oder 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 policies and BGP communities.

Zugriff auf öffentliche Dienste in einer abgelegenen 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 Virtuelle Schnittstellen und gehostete virtuelle Schnittstellen.

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

Zugriff auf VPCs in einer entfernten Region

Sie können ein Direct Connect-Gateway in einer beliebigen öffentlichen Region erstellen. Verwenden Sie es, um Ihre AWS Direct Connect Verbindung über eine private virtuelle Schnittstelle mit Ihrem Konto, das sich VPCs in verschiedenen Regionen befindet, oder mit einem Transit-Gateway zu verbinden. Weitere Informationen finden Sie unter AWS Direct Connect Gateways.

Alternativ können Sie eine öffentliche virtuelle Schnittstelle für Ihre AWS Direct Connect Verbindung erstellen und dann eine VPN-Verbindung zu 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.

Network-to-Amazon VPC-Konnektivitätsoptionen

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

AWS Direct Connect Routing-Richtlinien und BGP-Communities

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 die öffentlichen IPv4 Präfixe oder IPv6 Präfixe angeben, AWS Direct Connect 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 Regionen China aufgeführt sind, werden nur AWS in den China 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
- Wenn Sie eine öffentliche Schnittstelle verwenden, können Sie entweder eine öffentliche oder eine private ASN verwenden. Es gibt jedoch wichtige Überlegungen:
  - Öffentlich ASNs: Sie müssen Eigentümer der ASN sein und das Recht haben, sie bekannt zu geben. AWS wird überprüfen, ob Sie der Eigentümer der ASN sind.
  - Privat ASNs: Sie können private ASNs (64512-65534, 4200000000-4294967294) verwenden. Ersetzt jedoch die private ASN durch AWS Direct Connect die ASN (7224), wenn Sie anderen Kunden oder im Internet Werbung für Ihre Präfixe AWS machen. AWS
  - ASN vorangestellt:
    - Bei einer öffentlichen ASN funktioniert das Vorabsenden erwartungsgemäß, und Ihre vorausgestellte ASN ist für andere Netzwerke sichtbar.
    - Bei einer privaten ASN werden alle von Ihnen vorgenommenen Benachrichtigungen entfernt, wenn Ihre private ASN durch 7224 ersetzt wird. AWS Das bedeutet, dass ASN-Präsent nicht effektiv ist, um Routing-Entscheidungen zu beeinflussen, es sei denn, AWS wenn Sie eine private ASN auf einer öffentlichen virtuellen Schnittstelle verwenden.
- Wenn Sie eine BGP-Peering-Sitzung AWS über eine öffentliche virtuelle Schnittstelle einrichten, verwenden Sie 7224 für die autonomen Systemnummern (ASN), um die BGP-Sitzung nebenbei einzurichten. AWS Die ASN auf Ihrem Router oder Kunden-Gateway-Gerät sollte sich von dieser ASN unterscheiden.

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:
  - Nordamerikaweit
  - 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 IPv6 Präfixe IPv4 oder 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 wertet zuerst die längste Präfixlänge aus. 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 verwendet ECMP-Routing (Equal-Cost Multi-Path) über mehrere Transit- oder private virtuelle Schnittstellen, wenn Präfixe dieselbe AS_PATH-Länge und dieselben BGP-Attribute haben. Die Angaben ASNs in AS_PATH der Präfixe müssen nicht übereinstimmen.

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, ECMP zu verwenden. AWS-Regionen bevorzugen standardmäßig Direct Connect-Standorte in demselben AWS-Region verknüpften Ordner. Unter AWS Direct Connect Standorte finden Sie die zugehörigen AWS-Region Direct Connect-Standorte.

Wenn keine Community-Tags mit lokalen Einstellungen angewendet werden, unterstützt Direct Connect ECMP über private oder virtuelle Transitschnittstellen für Präfixe mit derselben 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 or Active/Passive Direct Connect-Verbindung AWS von einer privaten oder virtuellen Transitschnittstelle aus ein?

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

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).

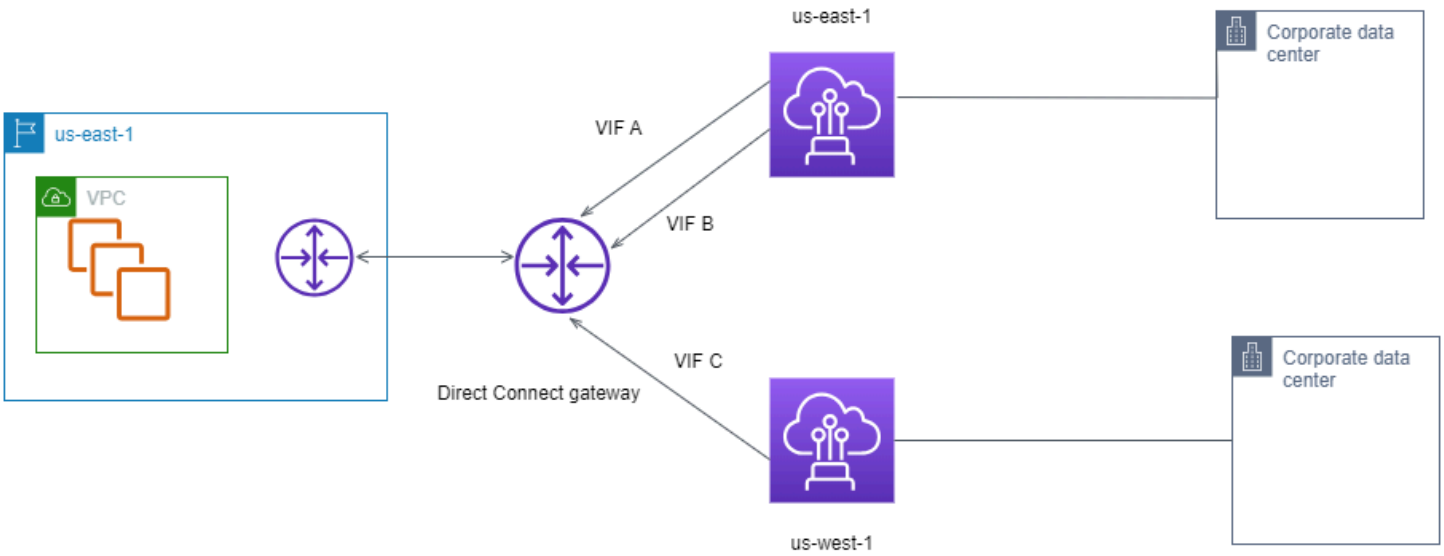
AWS Direct Connect Beispiel für das Routing einer privaten virtuellen Schnittstelle

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 Standorte 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.

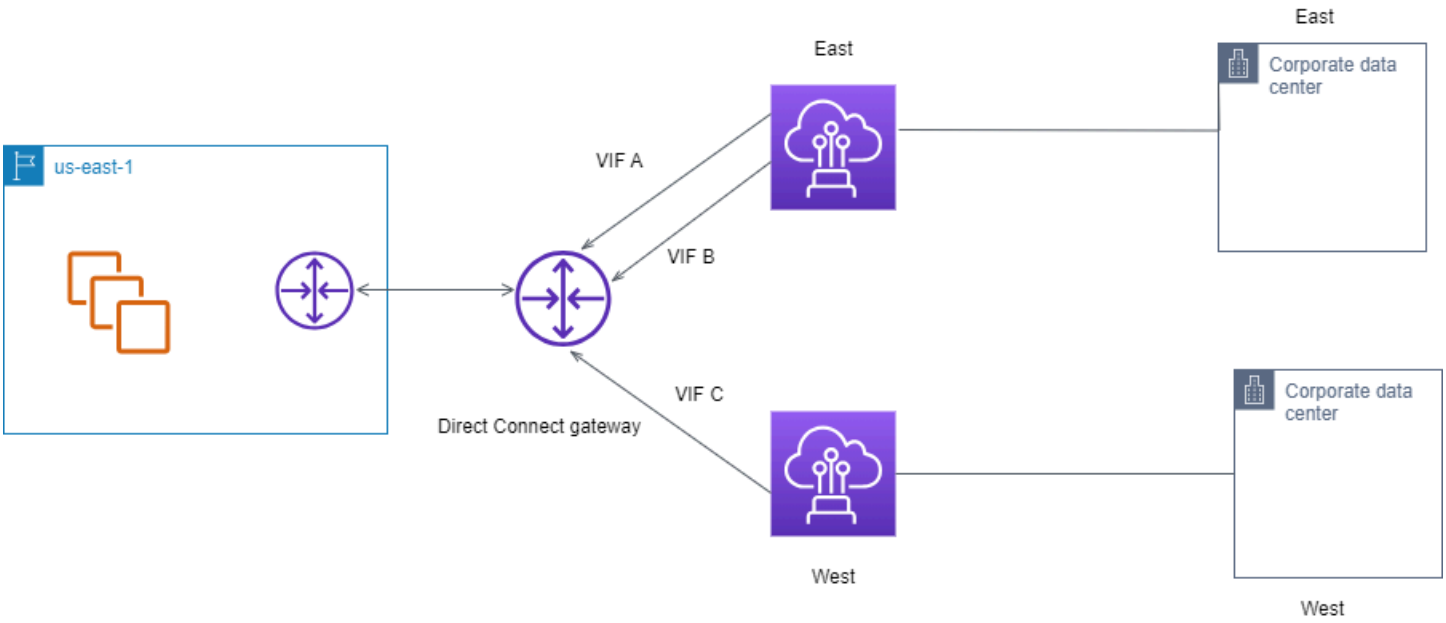
Sie VIFs haben die folgenden Konfigurationen:

- 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


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

AWS Direct Connect Resilienz-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.
- Erstellt Link-Aggregationsgruppen (LAGs) und fügt die entsprechende Anzahl von dedizierten Verbindungen hinzu, LAGs wenn Sie eine andere Geschwindigkeit als 1 Gbit/s, 10 Gbit/s, 100 Gbit/s oder 400 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 “Direct Connect-Failovertest”.

- Stellt CloudWatch Amazon-Metriken für Verbindungen und virtuelle Schnittstellen bereit. Weitere Informationen finden Sie unter Direct Connect-Ressourcen 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, 100GBASE- für 100-Gigabit-Ethernet oder 400GBASE- für 400-Gbit/s-Ethernet. LR4 LR4

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

Modell	Bandbreite	Methode
Dedizierte Verbindung	1 Gbit/s, 10 Gbit/s, 100 Gbit/s und 400 Gbit/s	Arbeiten Sie mit einem AWS Direct Connect Partner oder Netzwerkanbieter zusammen, um einen Router von Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebun g mit einem Standort zu verbinden. AWS Direct Connect Der Netzwerka nbieter muss kein AWS Direct Connect Partner sein, um Sie mit einer dedizierten Verbindung zu verbinden. AWS Direct Connect dediziert e Verbindungen unterstützen diese Portgeschwindigkeiten über Singlemode-Glasfaser: 1 Gbit/s: 1000BASE-LX (1310 nm), 10 Gbit/s: 10GBASE-LR (1310 nm), 100 Gbit/s: 100GBASE- oder 400GBASE- für 400-Gbit/s-Ethernet. LR4 LR4
Gehostete Verbindung	50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 300 Mbit/s, 400 Mbit/	Arbeiten Sie mit einem Partner im AWS Direct Connect

Modell	Bandbreite	Methode
	s, 500 Mbit/s, 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s und 25 Gbit/s.	Partnerprogramm zusammen, um einen Router von Ihrem Rechenzentrum, Büro oder Ihrer Colocation-Umgebung mit einem Standort zu verbinden. AWS Direct Connect 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, einem 100GBASE- für 100-Gigabit-Ethernet oder einem 400GBASE- für 400-Gbit/s-Ethernet verwenden. LR4 LR4
- Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bereitstellt, muss die automatische Aushandlung von lokalen Geräten möglicherweise für jede dedizierte Verbindung aktiviert oder deaktiviert werden. Wenn eine virtuelle Schnittstelle ausgefallen bleibt, während eine Direct Connect-Verbindung besteht, finden Sie weitere Informationen unterBehandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss das Border Gateway Protocol (BGP) und die BGP-Authentifizierung MD5 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.

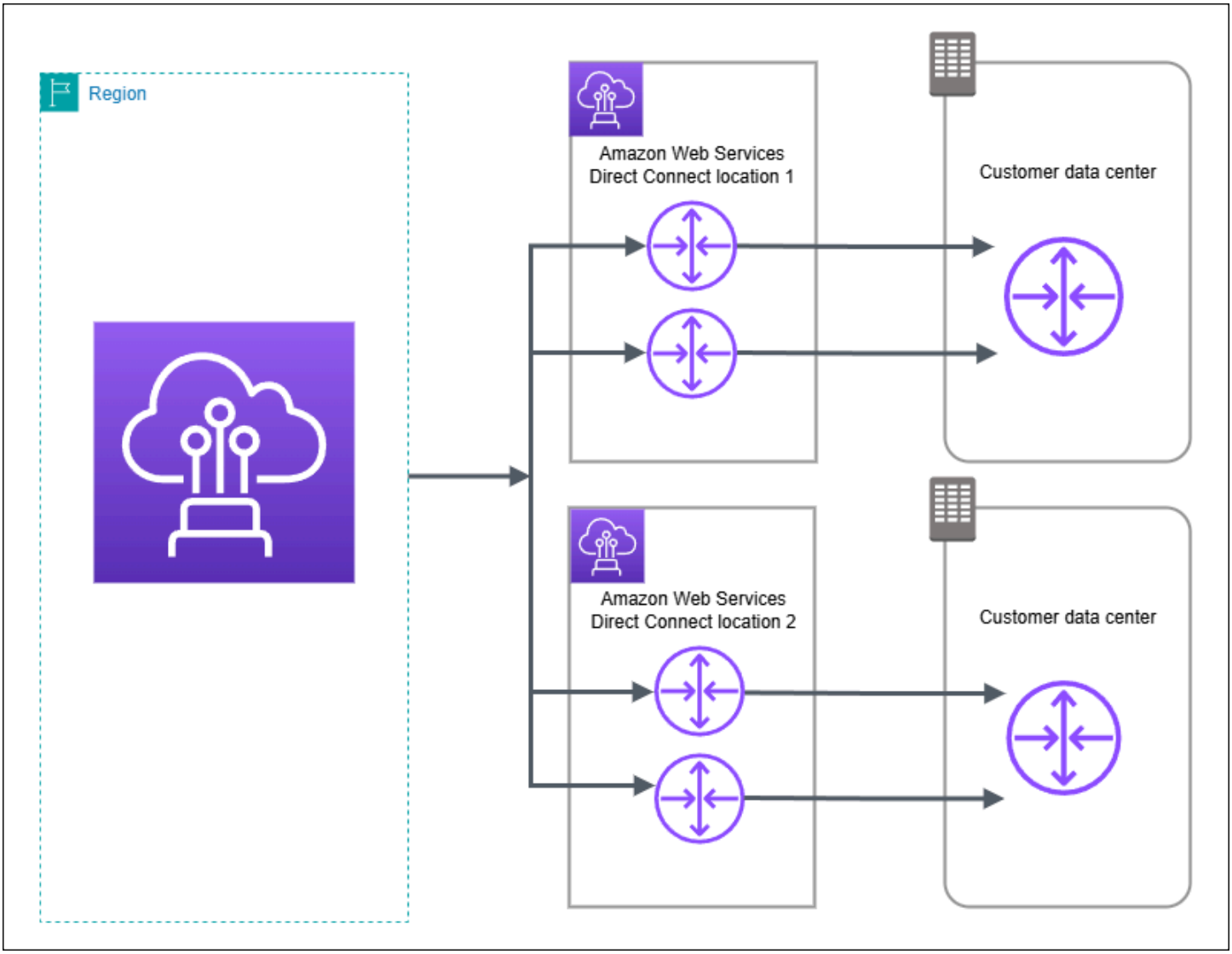
Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie mit der Konfiguration beginnen:

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

  Sie benötigen nur die Geschwindigkeit für eine Verbindung.

Maximale Ausfallsicherheit

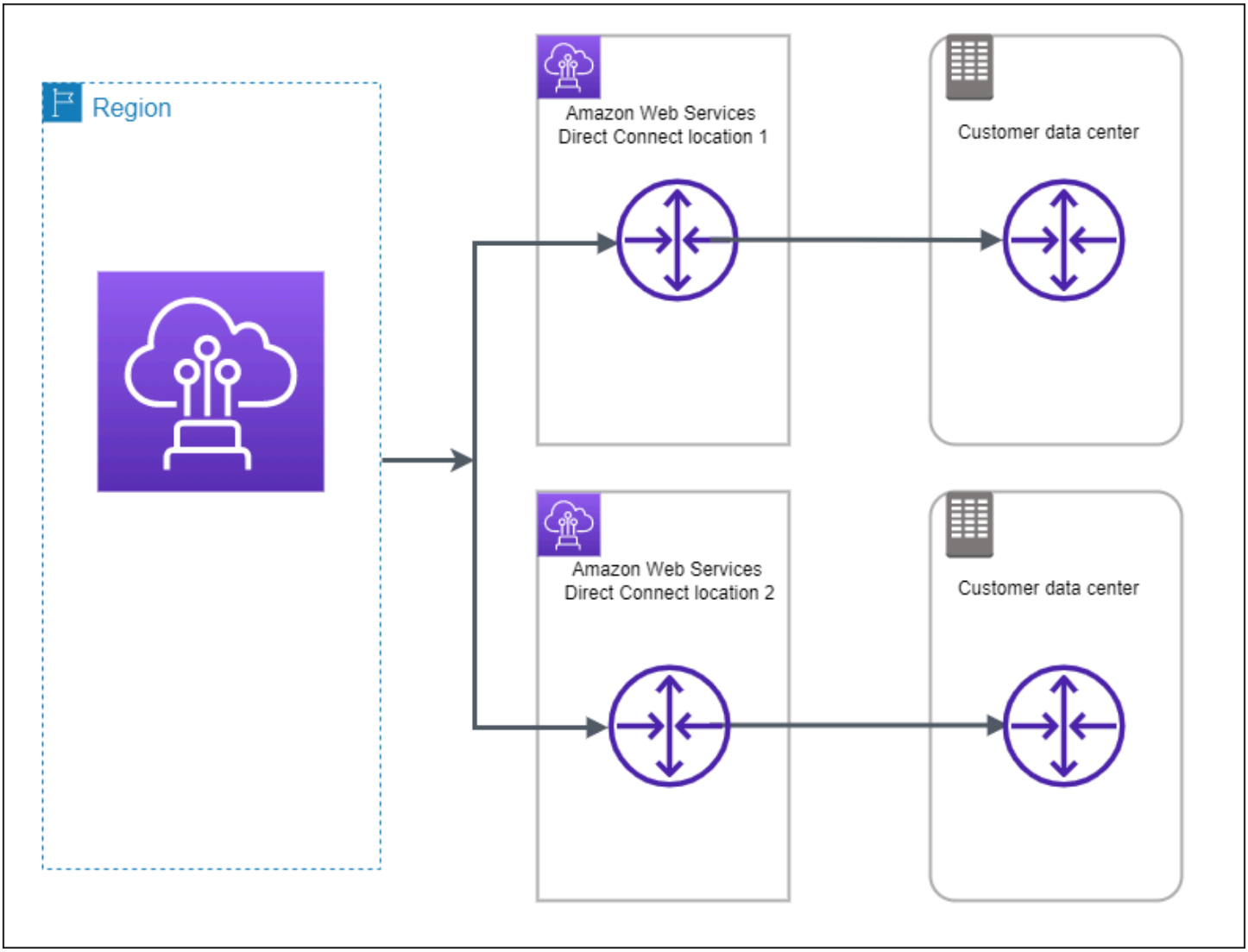
Sie erzielen maximale Ausfallsicherheit für kritische Workloads, indem Sie separate Verbindungen verwenden, die auf separaten Geräten an mehreren Standorten terminiert werden (wie in der nachfolgenden Abbildung dargestellt). Dieses Modell bietet Ausfallsicherheit gegen Geräte-, Konnektivitäts- und vollständige 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.



Das Verfahren zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Konfiguration eines Modells mit maximaler Ausfallsicherheit finden Sie unter. Konfigurieren Sie maximale Resilienz

Hohe Ausfallsicherheit

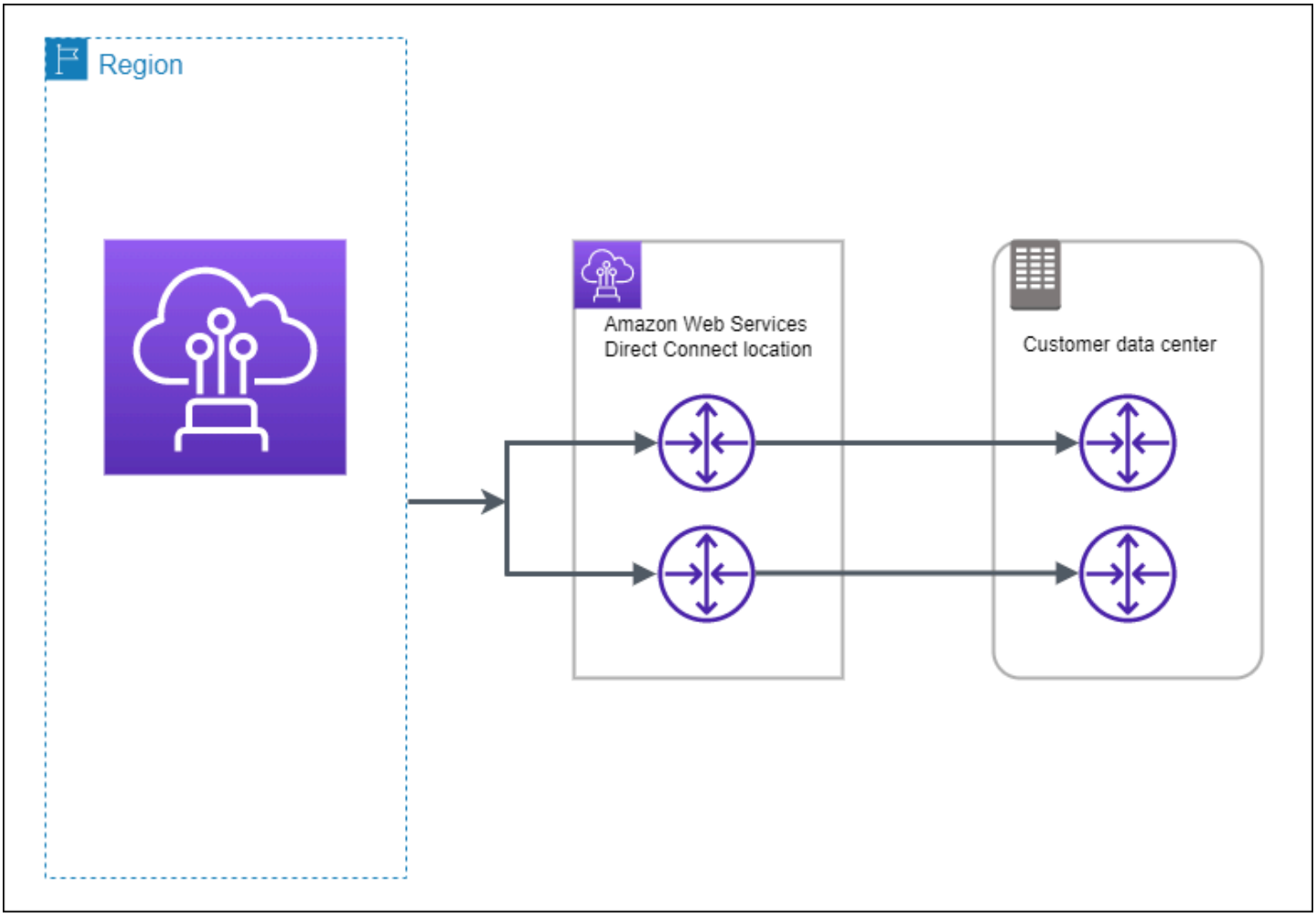
Sie erzielen eine hohe Ausfallsicherheit für kritische Workloads, indem Sie zwei einzelne Verbindungen zu mehreren Standorten verwenden (wie in der folgenden Abbildung dargestellt). Dieses Modell bietet Ausfallsicherheit gegen Konnektivitätsfehler, die durch eine Unterbrechung der Glasfaserverbindung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



Das Verfahren zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Konfiguration eines Modells mit hoher Ausfallsicherheit finden Sie unter. Konfigurieren Sie eine hohe Ausfallsicherheit

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.



Das Verfahren zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Konfiguration eines Modells mit maximaler Ausfallsicherheit finden Sie unter. Konfigurieren Sie die Entwicklungs- und Testausfallsicherheit

Classic

Wählen Sie Classic aus, wenn bestehende Verbindungen vorhanden sind.

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

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, einem 100GBASE- für 100-Gigabit-Ethernet oder einem 400GBASE- für 400-Gbit/s-Ethernet verwenden. LR4 LR4
- Abhängig vom AWS Direct Connect-Endpunkt, der Ihre Verbindung bereitstellt, muss die automatische Aushandlung von lokalen Geräten möglicherweise für jede dedizierte Verbindung aktiviert oder deaktiviert werden. Wenn eine virtuelle Schnittstelle ausgefallen bleibt, während eine Direct Connect-Verbindung besteht, finden Sie weitere Informationen unterBehandlung von Problemen auf Ebene 2 (Datenverbindung).
- Die 802.1Q-VLAN-Kapselung muss für die gesamte Verbindung unterstützt werden, einschließlich zwischengeschalteter Geräte.
- Ihr Gerät muss das Border Gateway Protocol (BGP) und die BGP-Authentifizierung MD5 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.

Das Verfahren zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Konfiguration einer Classic-Verbindung finden Sie unter. Konfigurieren Sie eine Classic-Verbindung

AWS Direct Connect FailoverTest

Verwenden Sie das AWS Direct Connect Resiliency Toolkit, um Verkehrswege zu überprüfen und zu überprüfen, ob diese Routen Ihren Stabilitätsanforderungen entsprechen.

Die Verfahren zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Durchführung von Failover-Tests finden Sie unter. Direct Connect-Failovertest

Verwenden Sie das AWS Direct Connect Resiliency Toolkit, um maximale Ausfallsicherheit AWS Direct Connect zu konfigurieren

In diesem Beispiel wird das AWS Direct Connect Resiliency Toolkit verwendet, um ein Modell mit maximaler Ausfallsicherheit zu konfigurieren

Aufgaben

- Schritt 1: Melden Sie sich an für AWS
- Schritt 2: Konfigurieren des Resilienzmodells
- Schritt 3: Erstellen Ihrer virtuellen Schnittstellen
- Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle
- Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

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

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

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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-Rooms (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 Sie bereit LOAs sind, können Sie LOA herunterladen auswählen und dann auf 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. Sie benötigen beispielsweise drei private virtuelle Schnittstellen, um eine Verbindung zu drei VPCs herzustellen.

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 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 kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein CIDR, das sich im Besitz IPv4 eines Kunden befindet
	
	Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP verwendet werden. 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 ein öffentliches IPv4 CIDR anzufordern (und geben Sie in Ihrer Anfrage einen Anwendungsfall an)
	
	Note
	Wir können nicht garantieren, dass wir in der Lage sein werden, alle Anfragen für von uns AWS bereitgestellte öffentliche IPv4 Adressen zu erfüllen.

Ressource	Erforderliche Informationen
	• (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6
BGP-Informationen	• 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 benutzerdefinierten 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 MD5 standardmäßig. 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 zur Werbung über BGP. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer Konfiguration haben. active/passive
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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.

Wenn Sie öffentliche Präfixe haben oder zu einem ISP oder Netzbetreiber ASNs gehören, bitten wir Sie um zusätzliche Informationen. Dabei kann es sich um ein Dokument mit einem offiziellen Firmenbriefkopf oder um eine E-Mail vom Domainnamen des Unternehmens handeln, mit der bestätigt wird, dass das Netzwerk von Ihnen genutzt werden prefix/ASN kann.

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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

   b. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie Ihren MD5 BGP-Schlüssel ein.

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

   c. Um Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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 Konsole unter v2/home. AWS Direct Connecthttps://console.aws.amazon.com/directconnect/
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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

- Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

> **Important**
>
> Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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 “Direct Connect-Failovertest”.

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 mit einem pingbaren AMI, z. B. einem Amazon Linux AMI, eine EC2 Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon AMIs Linux-Versionen sind auf der Registerkarte Schnellstart verfügbar, wenn Sie den Instance-Startassistenten in der EC2 Amazon-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im EC2 Amazon-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. Nachdem die Instance ausgeführt wurde, rufen Sie ihre private IPv4 Adresse ab (z. B. 10.0.0.4). Die EC2 Amazon-Konsole zeigt die Adresse als Teil der Instanzdetails an.
3. Pingen Sie die private IPv4 Adresse an und erhalten Sie eine Antwort.

Verwenden Sie das AWS Direct Connect Resiliency Toolkit, um eine hohe Ausfallsicherheit AWS Direct Connect zu konfigurieren

In diesem Beispiel wird das AWS Direct Connect Resiliency Toolkit verwendet, um ein Modell mit hoher Ausfallsicherheit zu konfigurieren

Aufgaben

- Schritt 1: Melden Sie sich an für AWS
- Schritt 2: Konfigurieren des Resilienzmodells
- Schritt 3: Erstellen Ihrer virtuellen Schnittstellen
- Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle
- Schritt 5: Überprüfen der Konnektivität Ihrer virtuellen Schnittstellen

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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-Rooms (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 Sie bereit LOAs sind, können Sie LOA herunterladen auswählen und dann auf 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. Sie benötigen beispielsweise drei private virtuelle Schnittstellen, um eine Verbindung zu drei VPCs herzustellen.

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 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 kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein CIDR, das sich im Besitz IPv4 eines Kunden befindet
	
	Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP verwendet werden. 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 ein öffentliches IPv4 CIDR anzufordern (und geben Sie in Ihrer Anfrage einen Anwendungsfall an)
	
	Note
	Wir können nicht garantieren, dass wir alle Anfragen für von Ihnen AWS bereitgestellte öffentliche IPv4 Adressen erfüllen können.

Ressource	Erforderliche Informationen
	• (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6
BGP-Informationen	• 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 benutzerdefinierten 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 MD5 standardmäßig. 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 zur Werbung über BGP. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer Konfiguration haben. active/passive
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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.

Wenn Sie öffentliche Präfixe haben oder zu einem ISP oder Netzbetreiber ASNs gehören, AWS fordert er zusätzliche Informationen von Ihnen an. Dabei kann es sich um ein Dokument mit einem offiziellen Firmenbriefkopf oder um eine E-Mail vom Domainnamen des Unternehmens handeln, in der bestätigt wird, dass das Netzwerk von Ihnen genutzt werden prefix/ASN kann.

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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

   b. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie Ihren MD5 BGP-Schlüssel ein.

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

   c. Um Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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 Konsole unter v2/home. AWS Direct Connecthttps://console.aws.amazon.com/directconnect/
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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

- Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

> **Important**
>
> Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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 “Direct Connect-Failovertest”.

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 mit einem pingbaren AMI, z. B. einem Amazon Linux AMI, eine EC2 Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon AMIs Linux-Versionen sind auf der Registerkarte „Schnellstart“ verfügbar, wenn Sie den Instance-Startassistenten in der EC2 Amazon-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im EC2 Amazon-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. Nachdem die Instance ausgeführt wurde, rufen Sie ihre private IPv4 Adresse ab (z. B. 10.0.0.4). Die EC2 Amazon-Konsole zeigt die Adresse als Teil der Instanzdetails an.
3. Pingen Sie die private IPv4 Adresse an und erhalten Sie eine Antwort.

Verwenden Sie das AWS Direct Connect Resiliency Toolkit, um die Ausfallsicherheit AWS Direct Connect für Entwicklung zu konfigurieren und zu testen

In diesem Beispiel wird das AWS Direct Connect Resiliency Toolkit verwendet, um ein Resilienzmodell für Entwicklung und Test zu konfigurieren

Aufgaben

- Schritt 1: Melden Sie sich an für AWS
- Schritt 2: Konfigurieren des Resilienzmodells
- Schritt 3: Erstellen einer virtuellen Schnittstelle
- Schritt 4: Überprüfen der Resilienzkonfiguration Ihrer virtuellen Schnittstelle
- Schritt 5: Überprüfen Ihrer virtuellen Schnittstelle

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können Ihre aktuellen Kontoaktivitäten jederzeit einsehen und Ihr Konto verwalten, indem Sie zu https://aws.amazon.com/gehen und Mein Konto auswählen.

Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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 Sie bereit LOAs sind, können Sie LOA herunterladen auswählen und dann auf 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. Sie benötigen beispielsweise drei private virtuelle Schnittstellen, um eine Verbindung zu drei VPCs herzustellen.

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 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.

Ressource	Erforderliche Informationen
	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 kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein CIDR, das sich im Besitz IPv4 eines Kunden befindet
	
	Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP verwendet werden. 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 ein öffentliches IPv4 CIDR anzufordern (und geben Sie in Ihrer Anfrage einen Anwendungsfall an)
	
	Note
	Wir können nicht garantieren, dass wir alle Anfragen für von Ihnen AWS bereitgestellte öffentliche IPv4 Adressen erfüllen können.

Ressource	Erforderliche Informationen
	• (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6
BGP-Informationen	• 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 MD5 standardmäßig. 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 zur Werbung über BGP. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer Konfiguration haben. active/passive
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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.

Wenn Sie öffentliche Präfixe haben oder zu einem ISP oder Netzbetreiber ASNs gehören, bitten wir Sie um zusätzliche Informationen. Dabei kann es sich um ein Dokument mit einem offiziellen Firmenbriefkopf oder um eine E-Mail vom Domainnamen des Unternehmens handeln, die bestätigt, dass das Netzwerk von Ihnen genutzt werden prefix/ASN kann.

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 v2/home. https://console.aws.amazon.com/directconnect/
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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

   b. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie Ihren MD5 BGP-Schlüssel ein.

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

   c. Um Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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 Konsole unter v2/home. AWS Direct Connecthttps://console.aws.amazon.com/directconnect/
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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

- Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

> **Important**
>
> Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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 “Direct Connect-Failovertest”.

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 mit einem pingbaren AMI, z. B. einem Amazon Linux AMI, eine EC2 Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon AMIs Linux-Versionen sind auf der Registerkarte Schnellstart verfügbar, wenn Sie den Instance-Startassistenten in der EC2 Amazon-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im EC2 Amazon-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. Nachdem die Instance ausgeführt wurde, rufen Sie ihre private IPv4 Adresse ab (z. B. 10.0.0.4). Die EC2 Amazon-Konsole zeigt die Adresse als Teil der Instanzdetails an.
3. Pingen Sie die private IPv4 Adresse an und erhalten Sie eine Antwort.

Eine AWS Direct Connect klassische Verbindung konfigurieren

Konfigurieren Sie eine Classic-Verbindung, wenn Sie bereits Direct Connect-Verbindungen haben.

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

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

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

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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) in 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 dedizierte und gehostete 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 v2/home. AWS Direct Connecthttps://console.aws.amazon.com/directconnect/
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 & DC1 0-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 AWS Direct Connect Standort behandelt. 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. Sie benötigen beispielsweise drei private virtuelle Schnittstellen, um eine Verbindung zu drei VPCs herzustellen.

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 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 kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein kundeneigener CIDR IPv4
	
	Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP verwendet werden. 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 ein öffentliches IPv4 CIDR anzufordern (und in Ihrer Anfrage einen Anwendungsfall anzugeben)
	
	Note
	Wir können nicht garantieren, dass wir alle Anfragen für von Ihnen AWS bereitgestellte öffentliche IPv4 Adressen erfüllen können.

Ressource	Erforderliche Informationen
	• (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6
BGP-Informationen	• 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 benutzerdefinierten 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 MD5 standardmäßig. 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 zur Werbung über BGP. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer Konfiguration haben. active/passive
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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.

Wir bitten Sie um zusätzliche Informationen, wenn Sie öffentliche Präfixe verwenden oder zu einem ISP oder Netzbetreiber ASNs gehören. Dabei kann es sich um ein Dokument mit einem offiziellen Firmenbriefkopf oder um eine E-Mail vom Domainnamen des Unternehmens handeln, in der bestätigt wird, dass das Netzwerk von Ihnen genutzt werden prefix/ASN kann.

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. Die MTU einer privaten virtuellen Schnittstelle kann entweder 1500 oder 9001 (Jumbo Frames) betragen. 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 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

b. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie Ihren MD5 BGP-Schlüssel ein.

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

c. Um Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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 Konsole unter v2/home. AWS Direct Connecthttps://console.aws.amazon.com/directconnect/
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 Systemnummer 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      > **Important**
      >
      > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
      > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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.

Weitere Informationen zur manuellen Konfiguration Ihres Routers finden Sie unter. Routerkonfigurationsdatei herunterladen

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.

Um Ihre virtuelle Schnittstelle+Schnittstellenverbindung zu Amazon VPC zu verifizieren

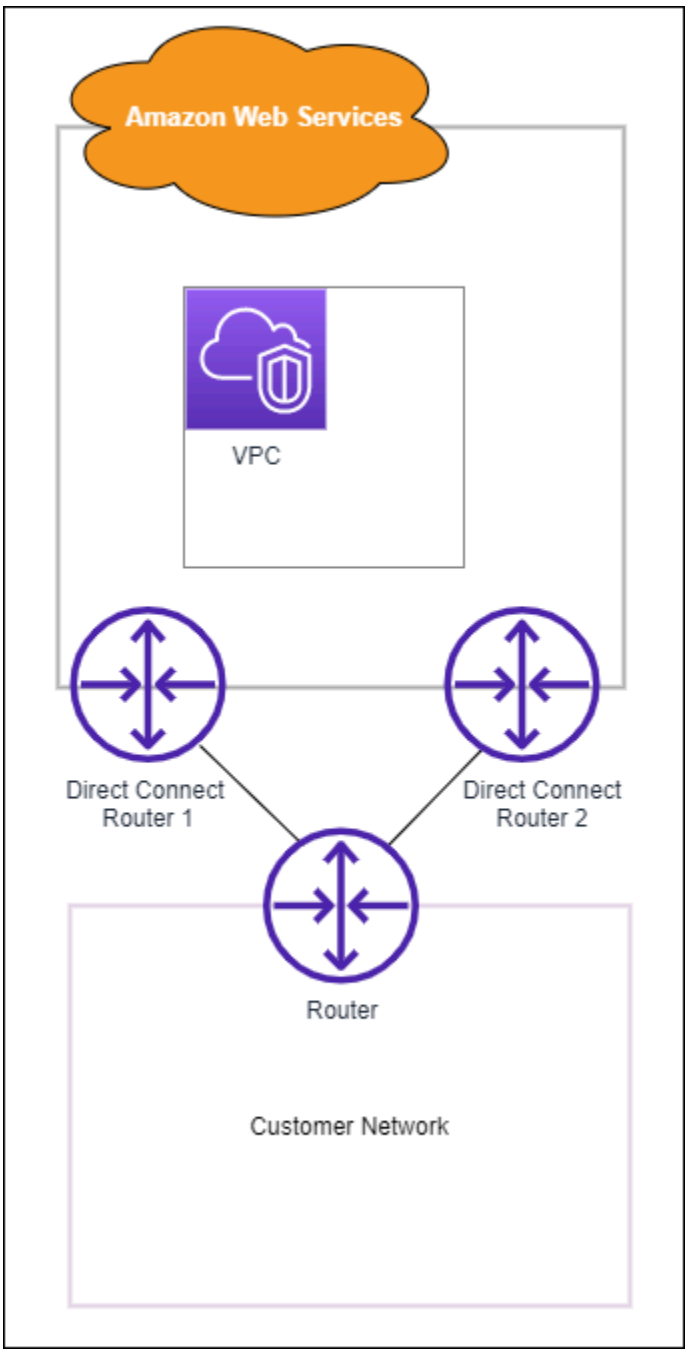
1. Starten Sie mit einem pingbaren AMI, z. B. einem Amazon Linux AMI, eine EC2 Instance in der VPC, die mit Ihrem Virtual Private Gateway verbunden ist. Die Amazon AMIs Linux-Versionen sind auf der Registerkarte „Schnellstart“ verfügbar, wenn Sie den Instance-Startassistenten in der EC2 Amazon-Konsole verwenden. Weitere Informationen finden Sie unter Launch an Instance im EC2 Amazon-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. Nachdem die Instance ausgeführt wurde, rufen Sie ihre private IPv4 Adresse ab (z. B. 10.0.0.4). Die EC2 Amazon-Konsole zeigt die Adresse als Teil der Instanzdetails an.
3. Pingen Sie die private IPv4 Adresse an und erhalten Sie eine Antwort.

(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 AWS Direct Connect Resilienzmodelle des Resiliency Toolkit wurden entwickelt, um sicherzustellen, dass Sie über die entsprechende Anzahl virtueller Schnittstellenverbindungen an mehreren Standorten verfügen. Nachdem Sie den Assistenten abgeschlossen haben, verwenden Sie den AWS Direct Connect Resiliency Toolkit-Failover-Test, um die BGP-Peering-Sitzung zu beenden und zu überprüfen, ob der Datenverkehr zu einer Ihrer redundanten virtuellen Schnittstellen geleitet wird und Ihre Resilienzanforderungen erfüllt.

Stellen Sie mithilfe des Tests sicher, dass Datenverkehr über redundante virtuelle Schnittstellen weitergeleitet wird, wenn eine virtuelle Schnittstelle außer Betrieb ist. Sie beginnen den Test, indem Sie eine virtuelle Schnittstelle, eine BGP-Peering-Sitzung und die Dauer der Testausführung auswählen. AWS versetzt die ausgewählte BGP-Peering-Sitzung mit virtueller Schnittstelle in den Status „Inaktiv“. 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 ist oder Sie den Test manuell beenden, wird die AWS BGP-Sitzung wiederhergestellt. Nach Abschluss des Tests können Sie das AWS Direct Connect Resiliency Toolkit verwenden, um Ihre Konfiguration anzupassen.

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

Verlauf des Tests

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 “Den Failover-Testverlauf einer virtuellen Schnittstelle anzeigen”.

Validierungsberechtigungen

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

Themen

- Starten Sie einen AWS Direct Connect Failover-Test für die virtuelle Schnittstelle des Resiliency Toolkit

- Den Failover-Testverlauf der virtuellen Schnittstelle des AWS Direct Connect Resiliency Toolkit anzeigen
- Beenden Sie einen AWS Direct Connect Failover-Test für die virtuelle Schnittstelle des Resiliency Toolkit

Starten Sie einen AWS Direct Connect Failover-Test für die virtuelle Schnittstelle des Resiliency Toolkit

Sie können den Failover-Test für virtuelle Schnittstellen mit der AWS Direct Connect Konsole oder dem starten. AWS CLI

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 zum Beispiel aus, welche Peering-Sitzungen getestet werden sollen, damit Peerings zum Testen heruntergefahren werden. 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.

Um den Failover-Test der virtuellen Schnittstelle mit dem zu starten AWS CLI

Verwenden Sie StartBgpFailoverTest.

Den Failover-Testverlauf der virtuellen Schnittstelle des AWS Direct Connect Resiliency Toolkit anzeigen

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

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.

Um den Failover-Testverlauf der virtuellen Schnittstelle mit dem AWS CLI

Verwenden Sie ListVirtualInterfaceTestHistory.

Beenden Sie einen AWS Direct Connect Failover-Test für die virtuelle Schnittstelle des Resiliency Toolkit

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

Um den Failover-Test der virtuellen Schnittstelle von der Konsole aus zu beenden AWS Direct Connect

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.

Um den Failover-Test der virtuellen Schnittstelle mit dem zu beenden AWS CLI

Verwenden Sie StopBgpFailoverTest.

AWS Direct Connect Wartung

AWS Direct Connect setzt sich dafür ein, die Sicherheit, Verfügbarkeit und Skalierbarkeit von Diensten zu gewährleisten. Um diese Standards aufrechtzuerhalten, ist eine regelmäßige Wartung der Hardware-Netzwerkgeräte erforderlich. Die Direct Connect-Wartung ist in zwei Typen unterteilt: geplante Wartung und Notfallwartung.

Zu diesen Wartungsmaßnahmen gehören die Behebung von Sicherheitslücken und Hardwareproblemen, die Durchführung von Gerätemigrationen zur Einhaltung von Standards, die Behebung von Fehlern und die Bereitstellung neuer Funktionen. Wenn Sie die unter beschriebenen Methoden befolgenVorbereitung von Wartungsereignissen, können Sie Ihre Direct Connect-Umgebung besser vorbereiten, um Unterbrechungen bei Wartungsereignissen zu vermeiden. Wenn Sie über eine nicht stabile Netzwerkkonfiguration oder eine einzelne Verbindung verfügen, kommt es zu einer Unterbrechung der Konnektivität zwischen Ihrem lokalen Netzwerk und den Ressourcen. AWS

Direct Connect sendet E-Mail-Benachrichtigungen über geplante und dringende Wartungsereignisse an die E-Mail-Adresse, die dem AWS Konto zugeordnet ist, dem die Direct Connect-Verbindung oder die virtuelle Schnittstellenressource gehört. Wenn Sie eine von Direct Connect gehostete Verbindung mit einem der Direct Connect-Lieferpartner verwenden, werden E-Mail-Benachrichtigungen über das Wartungsereignis sowohl an Sie als auch an das Partnerkonto gesendet. Sie können auch zusätzliche E-Mail-Adressen oder Verteilerlisten hinzufügen, um Benachrichtigungen zu erhalten. Weitere Informationen finden Sie unter Alternative Kontakte für Ihr AWS Konto aktualisieren.

Wartungsereignisse

- Geplante Wartung mit Direct Connect
- Direct Connect-Notfallwartung
- Wartung durch Dritte
- Vorbereitung von Wartungsereignissen
- Anfragen zur Verschiebung oder Absage von Wartungsveranstaltungen

Geplante Wartung mit Direct Connect

Geplante Wartungsereignisse beinhalten Netzwerk-Upgrades wie Betriebssystem-Patches und Konfigurationsupdates auf Hardware-Endpunkten, die zur Verbesserung der Verfügbarkeit und Bereitstellung neuer Funktionen erforderlich sind.

Diese Wartungsereignisse werden 14 Tage im Voraus geplant und finden in der Regel innerhalb eines Zeitfensters von vier Stunden zu Zeiten mit geringem Datenverkehr am Direct Connect-Standort statt, an dem sich der Geräteendpunkt befindet. Wartungsarbeiten werden in der Regel abgeschlossen, bevor das volle Zeitfenster von vier Stunden abläuft, und Sie erhalten eine Benachrichtigung, sobald die Arbeiten abgeschlossen sind. In seltenen Fällen, in denen unvorhergesehene Umstände eine Verlängerung des Wartungsfensters erforderlich machen, senden wir Ihnen eine separate Benachrichtigung mit der überarbeiteten Schätzung der Fertigstellung.

Gemäß dem folgenden Zeitplan werden die ersten Benachrichtigungen und Erinnerungsbenachrichtigungen an das AWS Konto gesendet, dem die Ressource gehört:

- 14 Kalendertage vor dem geplanten Wartungsereignis,
- 7 Kalendertage vor dem geplanten Wartungsereignis und
- 1 Tag vor dem geplanten Wartungsereignis.

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

Darüber hinaus

- Erhalten Sie Benachrichtigungen in Ihrem Überwachungs- oder Ticketsystem, indem Sie es mit AWS Health integrieren. Informationen zur Integration AWS Health finden Sie unter Überwachung von Ereignissen AWS Health mit Amazon EventBridge im AWS Health Benutzerhandbuch.
- Sehen Sie sich geplante Wartungspläne auf Ihrem an AWS Health Dashboard.

In seltenen Fällen kann ein geplantes Wartungsereignis nicht wie geplant stattfinden. Sollte dies der Fall sein, senden wir eine Stornierungsbenachrichtigung und werden die Veranstaltung in future nach dem gleichen Verfahren wie oben verschieben.

Direct Connect-Notfallwartung

Notfallwartungsmaßnahmen werden auf kritischer Basis eingeleitet, um drohende Ereignisse zu verhindern, die sich auf den Betrieb auswirken, oder um Störungen zu beheben, die bereits zu einer Unterbrechung der Konnektivität geführt haben. In solchen Fällen müssen sofortige Maßnahmen ergriffen werden, um den fehlerfreien Zustand des betroffenen Endgeräts wiederherzustellen.

Wir bemühen uns zwar, Sie nach Möglichkeit im Voraus zu informieren, in einigen Situationen kann es jedoch erforderlich sein, dass die Wartung sofort beginnt. Sie erhalten Benachrichtigungen, wenn eine Notfallwartung geplant ist oder im Gange ist, und erneut, wenn sie abgeschlossen ist.

Diese Ereignisse treten in der Regel innerhalb eines zweistündigen Zeitfensters am Direct Connect-Standort auf, an dem sich der Geräteendpunkt befindet. Wartungsarbeiten werden normalerweise innerhalb dieses Zeitfensters abgeschlossen. In Fällen, in denen unvorhergesehene Umstände eine Verlängerung des Wartungsfensters erforderlich machen, z. B. beim Austausch von Hardware, senden wir eine separate Benachrichtigung mit der überarbeiteten Schätzung der Fertigstellung.

Wartung durch Dritte

Neben AWS eingeleiteten Wartungsereignissen kann Ihr Direct Connect Delivery-Partner oder Netzwerkdienstanbieter, der die Netzwerkkonnektivität von Ihrem Standort zum Direct Connect-Standort bereitstellt, Wartungsarbeiten durchführen. Direct Connect Delivery-Partner erhalten Benachrichtigungen über Wartungsereignisse von, AWS sodass sie ihre eigenen Wartungspläne planen können, um Überschneidungen zu vermeiden. AWS hat keinen Einblick in die Wartungsaktivitäten eines Partners, daher müssen Sie sich bei ihm nach dem Planungsprozess, den Benachrichtigungsmethoden und den bewährten Verfahren erkundigen.

Vorbereitung von Wartungsereignissen

Um sicherzustellen, dass Produktionsworkloads während eines Wartungsereignisses weiterhin funktionieren, empfiehlt Direct Connect, dass Sie das AWS Direct Connect Resiliency Toolkit verwenden, um Ihre Netzwerkverbindungen für maximale Ausfallsicherheit zu konfigurieren. Ein Beispielmodell für maximale Ausfallsicherheit finden Sie unter. Maximale Ausfallsicherheit

Bei maximaler Ausfallsicherheit werden Verbindungen auf mindestens zwei Direct Connect-Standorte verteilt, wobei die Terminierung an zwei eindeutigen Geräteendpunkten innerhalb jedes Direct Connect-Standorts erfolgt. Dies bietet mehrere Redundanzschichten, wodurch das Risiko eines Ausfalls eines einzelnen Endgeräts reduziert wird und die Konnektivität bei Wartungsarbeiten aufrechterhalten wird. Direct Connect plant niemals eine geplante Wartung, bei der gleichzeitig Ihre redundanten Verbindungen unterbrochen werden. Die Schritte zur Verwendung des AWS Direct Connect Resiliency Toolkits zur Konfiguration maximaler Ausfallsicherheit finden Sie unter. Konfigurieren Sie maximale Resilienz

Während eines geplanten Wartungsereignisses leitet Direct Connect den Datenverkehr zum und vom Verbindungsendpunkt ab, der gerade gewartet wird, und zwingt den Datenverkehr, Ihre redundanten

Verbindungen zu nutzen. Dies ermöglicht eine nahtlosere Umleitung des Netzwerkverkehrs, ohne dass manuelles Eingreifen erforderlich ist, wenn die maximale Ausfallsicherheit nicht konfiguriert wurde. Alternativ können Sie die Umleitung des Datenverkehrs zwischen redundanten Verbindungen während der Wartungsfenster steuern, indem Sie lokale Border Gateway Protocol (BGP) - Communities verwenden. Weitere Informationen zu BGP-Communities finden Sie unter. Routing policies and BGP communities

Durch die Konfiguration Ihrer Direct Connect-Umgebung mit dem Modell der maximalen Ausfallsicherheit können Sie sicherstellen, dass Ihr Unternehmen nicht durch Wartungsereignisse und Infrastrukturausfälle beeinträchtigt wird. Bei ordnungsgemäßer Implementierung und Prüfung müssen Sie in der Regel keine Maßnahmen für diese Wartungsereignisse ergreifen.

Validierung der Resilienz

Wenn Sie Ihre Direct Connect-Umgebung so konfiguriert haben, dass sie robust ist, überprüfen Sie regelmäßig, ob Ihr Datenverkehr über andere redundante Verbindungen geleitet wird, wenn eine Verbindung bestehtout-of-service. Regelmäßige proaktive Tests können dabei helfen, potenzielle Probleme zu identifizieren und zu beheben, bevor sie sich auf die Produktionsauslastung auswirken, und zwar während eines echten Wartungsereignisses oder eines Ausfallszenarios. Dadurch wird ein größeres Vertrauen in die Zuverlässigkeit Ihres Netzwerks während eines Wartungsereignisses gewährleistet. Verwenden Sie den Direct Connect Failover-Test, um die Resilienz Ihrer redundanten Verbindungen zu überprüfen. Die Schritte zur Verwendung des AWS Direct Connect Failover-Tests finden Sie unter. Direct Connect-Failovertest

Sie können Amazon CloudWatch Network Monitor auch nutzen, um Ihre Direct Connect-Verbindungen aktiv zu überwachen. Weitere Informationen finden Sie unter Überwachen der Hybridkonnektivität mit Amazon CloudWatch Network Synthetic Monitor.

Anfragen zur Verschiebung oder Absage von Wartungsveranstaltungen

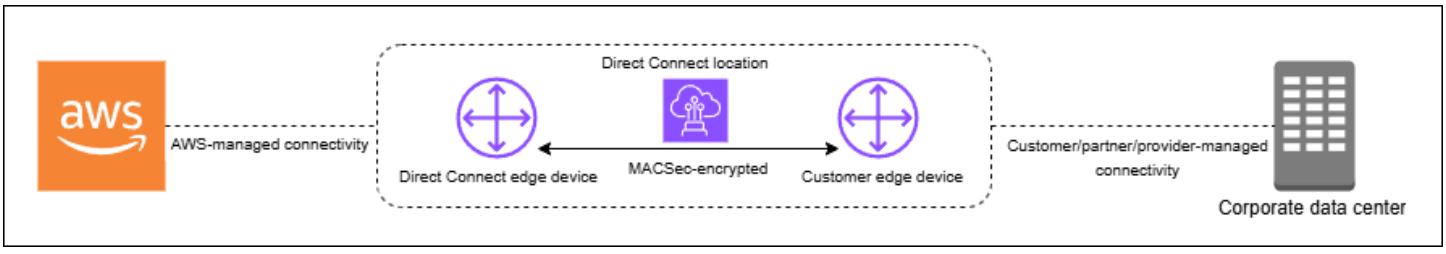
Direct Connect-Geräte werden von mehreren Kunden gemeinsam genutzt. Daher gehen wir nicht auf spezielle Anfragen zur Verschiebung oder Stornierung von Wartungsarbeiten ein. Anfragen zur Verschiebung oder Stornierung eines Kunden können sich negativ auf andere Kunden auswirken, die diesen Endpunkt nutzen. Dies kann auch ein Risiko für die rechtzeitige Behebung von Verfügbarkeits- oder Sicherheitsproblemen darstellen.

MAC-Sicherheit in AWS Direct Connect

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 und funktioniert zwischen zwei Layer-3-Routern. MACsec Sichert zwar die Verbindung zwischen Ihrem Router und dem Direct Connect-Standort auf Layer 2, AWS bietet jedoch zusätzliche Sicherheit, indem alle Daten auf der physischen Ebene verschlüsselt werden, während sie über das Netzwerk zwischen AWS Direct Connect Standorten und AWS Regionen fließen. Dadurch entsteht ein mehrschichtiger Sicherheitsansatz, bei dem Ihr Datenverkehr sowohl beim ersten Eintritt in AWS das Netzwerk als auch bei der Übertragung durch das AWS Netzwerk geschützt ist.

In der folgenden Abbildung muss die AWS Direct Connect Cross-Connect-Verbindung mit einer MACsec -fähigen Schnittstelle auf dem Edge-Gerät des Kunden verbunden werden. MACsec over Direct Connect bietet Layer-2-Verschlüsselung für den point-to-point Datenverkehr zwischen dem Direct Connect-Edge-Gerät und dem Edge-Gerät des Kunden. Diese Verschlüsselung erfolgt, nachdem Sicherheitsschlüssel zwischen den Schnittstellen an beiden Enden der Cross-Connect-Verbindung ausgetauscht und verifiziert wurden.

> **Note**
>
> MACsec bietet point-to-point Sicherheit für Ethernet-Verbindungen. Daher bietet sie keine end-to-end Verschlüsselung für mehrere sequentielle Ethernet- oder andere Netzwerksegmente.



MACsec Konzepte

Im Folgenden sind die wichtigsten Konzepte aufgeführt für MACsec:

- MAC Security (MACsec) — Ein IEEE 802.1 Layer-2-Standard, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. Weitere Informationen zum Protokoll finden Sie unter 802.1AE: MAC-Sicherheit (). MACsec
- Secure Association Key (SAK) — Ein Sitzungsschlüssel, der die MACsec Konnektivität zwischen dem lokalen Kundenrouter und dem Verbindungsport am Direct Connect-Standort herstellt. Der SAK wird nicht vorab gemeinsam genutzt, sondern automatisch aus dem Paar abgeleitet. CKN/CAK pair through a cryptographic key generation process. This derivation happens at both ends of the connection after you provide and provision the CKN/CAK Der SAK wird aus Sicherheitsgründen und immer dann, wenn eine MACsec Sitzung eingerichtet wird, regelmäßig neu generiert.
- Connectivity Association Key Name (CKN) und Connectivity Association Key (CAK) — Die Werte in diesem Paar werden zur Generierung des Schlüssels verwendet. MACsec Sie generieren die Paarwerte, ordnen sie einer AWS Direct Connect Verbindung zu und stellen sie dann am Ende der AWS Direct Connect Verbindung auf Ihrem Edge-Gerät bereit. Direct Connect unterstützt nur den statischen CAK-Modus, nicht aber den dynamischen CAK-Modus. Da nur der statische CAK-Modus unterstützt wird, wird empfohlen, dass Sie Ihre eigenen Schlüsselverwaltungsrichtlinien für die Schlüsselgenerierung, -verteilung und -rotation befolgen.
- Schlüsselformat — Das Schlüsselformat sollte Hexadezimalzeichen mit einer Länge von genau 64 Zeichen verwenden. Direct Connect unterstützt nur 256-Bit-Schlüssel des Advanced Encryption Standard (AES) für dedizierte Verbindungen, was einer 64-stelligen Hexadezimalzeichenfolge entspricht.
- Verschlüsselungsmodi — Direct Connect unterstützt zwei MACsec Verschlüsselungsmodi:
  - must_encrypt — In diesem Modus erfordert die Verbindung eine MACsec Verschlüsselung des gesamten Datenverkehrs. Wenn die MACsec Verhandlung fehlschlägt oder die Verschlüsselung nicht hergestellt werden kann, überträgt die Verbindung keinen Verkehr. Dieser Modus bietet die höchste Sicherheitsgarantie, kann sich jedoch auf die Verfügbarkeit auswirken, wenn damit MACsec verbundene Probleme auftreten.
  - should_encrypt — In diesem Modus versucht die Verbindung, eine MACsec Verschlüsselung herzustellen, greift aber auf unverschlüsselte Kommunikation zurück, falls die Verhandlung fehlschlägt. MACsec Dieser Modus bietet mehr Flexibilität und höhere Verfügbarkeit, kann jedoch in bestimmten Ausfallszenarien unverschlüsselten Datenverkehr zulassen.

  Der Verschlüsselungsmodus kann während der Verbindungskonfiguration festgelegt und später geändert werden. Standardmäßig sind neu MACsec aktivierte Verbindungen auf den Modus „should_encrypt“ gesetzt, um mögliche Verbindungsprobleme bei der Ersteinrichtung zu vermeiden.

MACsec Schlüsselrotation

- CNN/CAK-Rotation (manuell)

  Direct Connect MACsec unterstützt MACsec Schlüsselanhänger mit einer Kapazität zum Speichern von bis zu drei CKN/CAK pairs. This allows you to manually rotate these long-term keys without connection disruption. When you associate a new CKN/CAK Paaren. Verwenden Sie den `associate-mac-sec-key` Befehl. Sie müssen dasselbe Paar auf Ihrem Gerät konfigurieren. Das Direct Connect-Gerät versucht, den zuletzt hinzugefügten Schlüssel zu verwenden. Wenn diese Taste nicht mit der Taste Ihres Geräts übereinstimmt, wird sie auf die vorherige funktionierende Taste zurückgesetzt, sodass die Verbindungsstabilität während der Rotation gewährleistet ist.

  Informationen zur Verwendung finden `associate-mac-sec-key` Sie unter associate-mac-sec-key.
- Rotation des Secure Association Key (SAK) (automatisch)

  Das SAK, das vom aktiven CKN/CAK-Paar abgeleitet wird, wird auf der Grundlage der folgenden Kriterien automatisch rotiert:

  - Zeitintervalle
  - Volumen des verschlüsselten Datenverkehrs
  - MACsec Einrichtung einer Sitzung

  Diese Rotation wird automatisch vom Protokoll abgewickelt, erfolgt transparent, ohne die Verbindung zu unterbrechen, und erfordert kein manuelles Eingreifen. Das SAK wird niemals dauerhaft gespeichert und wird durch einen sicheren Schlüsselableitungsprozess regeneriert, der dem IEEE 802.1X-Standard entspricht.

Unterstützte Verbindungen

MACsec ist auf dedizierten Direct Connect-Verbindungen und Link-Aggregationsgruppen verfügbar:

Unterstützte Verbindungen MACsec

- Dedizierte Verbindungen
- LAGs

> **Note**
>
> Gehostete Verbindungen und Direct Connect Gateway-Verknüpfungen unterstützen keine MACsec Verschlüsselung.

Informationen zur Bestellung von Verbindungen, die diese Unterstützung bieten MACsec, finden Sie unter AWS Direct Connect.

Dedizierte Verbindungen

Im Folgenden können Sie sich mit MACsec AWS Direct Connect dedizierten Verbindungen vertraut machen. Für die Nutzung fallen keine zusätzlichen Gebühren an MACsec. Die Schritte MACsec zur Konfiguration für eine dedizierte Verbindung finden Sie unterBeginnen Sie mit MACsec einer dedizierten Verbindung.

MACsec Voraussetzungen für dedizierte Verbindungen

Beachten Sie die folgenden Anforderungen für MACsec keine dedizierten Verbindungen:

- MACsec wird auf dedizierten Direct Connect-Verbindungen mit 10 Gbit/s, 100 Gbit/s und 400 Gbit/s an ausgewählten Präsenzpunkten unterstützt. Für diese Verbindungen werden die folgenden MACsec Cipher Suites unterstützt:
  - Für 10-Gbit/s-Verbindungen GCM-AES-256 und GCM-AES-XPN-256.
  - Für 100-Gbit/s- und 400-Gbit/s-Verbindungen, -256. GCM-AES-XPN
- Es werden nur 256-Bit-Schlüssel unterstützt MACsec .
- Extended Packet Numbering (XPN) ist für Verbindungen mit 100 Gbit/s und 400 Gbit/s erforderlich. Für 10-Gbit/s-Verbindungen unterstützt Direct Connect sowohl GCM-AES-256 als auch -256. GCM-AES-XPN Hochgeschwindigkeitsverbindungen, wie z. B. dedizierte Verbindungen mit 100 Gbit/s und 400 Gbit/s, können den ursprünglichen 32-Bit-Paketnummerierungsspeicher schnell erschöpfen MACsec, sodass Sie Ihre Verschlüsselungsschlüssel alle paar Minuten wechseln müssten, um eine neue Connectivity Association einzurichten. Um diese Situation zu vermeiden, wurde mit der Änderung IEEE Std 802.1 AEbw -2013 eine erweiterte Paketnummerierung eingeführt, wodurch der Nummerierungsraum auf 64 Bit erhöht wurde, wodurch die Anforderung an 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.

Darüber hinaus sollten Sie die folgenden Aufgaben ausführen, bevor Sie eine dedizierte Verbindung konfigurieren. MACsec

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

  Sie können das Paar mit einem offenen Standardtool erstellen. Das Paar muss die Anforderungen unter the section called “Konfigurieren Sie Ihren lokalen Router” erfüllen.
- Stellen Sie sicher, dass Sie an Ihrem Ende der Verbindung ein Gerät haben, das unterstützt. MACsec
- Secure Channel Identifier (SCI) muss aktiviert sein.
- Es werden nur MACsec 256-Bit-Schlüssel unterstützt, wodurch der neueste erweiterte Datenschutz gewährleistet ist.

LAGs

Die folgenden Anforderungen helfen Ihnen, sich mit MACsec Direct Connect-Link-Aggregationsgruppen (LAGs) vertraut zu machen:

- LAGs muss aus MACsec -fähigen dedizierten Verbindungen bestehen, unterstützt Verschlüsselung MACsec
- Alle Verbindungen innerhalb einer LAG müssen dieselbe Bandbreite und Unterstützung haben MACsec
- MACsec Die Konfiguration gilt einheitlich für alle Verbindungen in der LAG
- Die Erstellung und MACsec Aktivierung von LAG können gleichzeitig erfolgen

Serviceverknüpfte Rollen

AWS Direct Connect verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Direct Connect Mit Diensten verknüpfte Rollen sind vordefiniert AWS Direct Connect und

enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Eine dienstbezogene Rolle AWS Direct Connect erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Direct Connect definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Direct Connect kann, sofern nicht anders definiert, nur ihre 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 “Service-verknüpfte Rollen”.

MACsec Wichtige Überlegungen zu vorab geteilten CKN/CAKs

AWS Direct Connect verwendet AWS verwaltete Schlüssel CMKs für die vorinstallierten Schlüssel, die Sie Verbindungen zuordnen, oder. LAGs 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 verwaltet CMKs im AWS Key Management Service Entwicklerhandbuch.

Der gespeicherte Schlüssel ist standardmäßig schreibgeschützt, aber Sie können mithilfe der AWS Secrets Manager Manager-Konsole oder der API eine Löschung von sieben bis dreißig Tagen 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.

Erste Schritte mit der Nutzung MACsec über eine dedizierte AWS Direct Connect Verbindung

Mit der folgenden Aufgabe können Sie mit der Einrichtung für MACsec die Verwendung auf einer dedizierten Direct Connect-Verbindung beginnen.

Schritt 1: Erstellen einer Verbindung

Um mit der Nutzung zu beginnen MACsec, müssen Sie die Funktion aktivieren, wenn Sie eine dedizierte Verbindung herstellen.

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

Wenn Sie aus Redundanzgründen mehrere Verbindungen verwenden, können Sie eine LAG erstellen, die Folgendes unterstützt MACsec. Weitere Informationen finden Sie unter MACsec Überlegungen LAG erstellen.

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

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

- Ordnen Sie ein MACsec CKN/CAK einer Verbindung zu
- Ordnen Sie ein MACsec CKN/CAK einer LAG zu

Schritt 4: On-Premises-Router konfigurieren

Aktualisieren Sie Ihren lokalen Router mit dem MACsec geheimen Schlüssel. Der MACsec geheime Schlüssel auf dem lokalen Router und am AWS Direct Connect Standort müssen übereinstimmen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

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

Sie können optional die Zuordnung zwischen dem CKN/CAK und der Verbindung oder LAG entfernen. Wenn Sie die Zuordnung entfernen müssen, finden Sie einen der folgenden Hinweise:

- Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer Verbindung
- Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer LAG

AWS Direct Connect dedizierte und gehostete 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, die einem einzelnen Kunden zugeordnet ist. Kunden können über die AWS Direct Connect Konsole, die CLI oder die API eine dedizierte Verbindung anfordern. Weitere Informationen finden Sie unter 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 Gehostete Verbindungen.

Themen

- Dedizierte AWS Direct Connect Verbindungen
- Gehostete AWS Direct Connect Verbindungen
- Löscht eine AWS Direct Connect Verbindung
- Eine AWS Direct Connect Verbindung aktualisieren
- AWS Direct Connect Verbindungsdetails anzeigen

Dedizierte AWS Direct Connect 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, 100 Gbit/s und 400 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 herzustellen. one-at-a-time 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 ein Letter of Authorization and Connecting Facility Assignment (LOA-CFA) zur Verfügung, das Sie herunterladen oder Ihnen per E-Mail mit der Bitte um weitere Informationen zusenden können. Wenn Sie diese Bitte um weitere Informationen nicht innerhalb von 7 Tagen beantworten, wird die Verbindung gelöscht. Der 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:

- Eine Verbindung mit dem Verbindungsassistenten erstellen
- Eine Classic-Verbindung erstellen
- the section called “Anzeigen von Verbindungsdetails”
- the section called “Aktualisieren einer Verbindung”
- Ordnen Sie ein MACsec CKN/CAK einer Verbindung zu
- the section called “Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer Verbindung”
- the section called “Eine Verbindung 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 Virtuelle Schnittstellen und gehostete 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 die Voraussetzungen, bevor Sie die Verbindung herstellen. Weitere Informationen finden Sie unter the section called “MACsec Voraussetzungen für dedizierte Verbindungen”.

Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA)

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.

Das heruntergeladene LoA ist digital signiert und mit einem Wasserzeichen versehen, um die Echtheit des von ausgestellten LoA zu bestätigen. AWS Die digitale Signatur und das Wasserzeichen in der LoA. Das PDF-Dokument verhindert, dass der Anbieter von Einrichtungen an Direct Connect-Standorten auf eine modifizierte oder potenziell betrügerische LoA reagiert. Die digitale Signatur kann authentifiziert werden, indem die PDF-Datei geöffnet und das Signaturfeld überprüft wird. In einem gültigen Dokument werden „Signatur ist gültig“ und „Dokument wurde seit dem Anwenden der Signatur nicht geändert“ angezeigt. Das Wasserzeichen wiederholt das Patchpanel und die Stränge, die dem LoA zugewiesen sind, und dient als optischer, aber nicht sicherer Indikator für die Echtheit.

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.

Die Schritte zum Herunterladen des LoA-CFA finden Sie unter. Das LOA-CFA-Dokument herunterladen

> **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 Löscht eine AWS Direct Connect Verbindung.

Themen

- Erstellen Sie mit AWS Direct Connect dem Verbindungsassistenten eine dedizierte Verbindung
- Erstellen Sie eine AWS Direct Connect klassische Verbindung
- Laden Sie den AWS Direct Connect LOA-CFA herunter
- Ordnen Sie einer Verbindung ein MACsec CKN/CAK zu AWS Direct Connect
- Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer AWS Direct Connect Verbindung

Erstellen Sie mit AWS Direct Connect dem Verbindungsassistenten eine dedizierte Verbindung

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 AWS Direct Connect Toolkit für Resilienz.
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 400 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 die MAC-Sicherheit (MACsec) für die Verbindung. Wählen Sie unter Zusätzliche Einstellungen die Option Einen MACsec fähigen Port anfordern aus.

      MACsec ist nur für dedizierte Verbindungen verfügbar.

   e. (Optional) Wählen Sie Tag hinzufügen, um key/value Paare hinzuzufügen, um diese Verbindung besser identifizieren zu 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 aus.
10. Laden Sie Ihr LOA-CFA (Letter of Authorization and Connecting Facility Assignment) herunter. Weitere Informationen finden Sie unter the section called “Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA)”.

Verwenden Sie einen der folgenden Befehle.

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

Erstellen Sie eine AWS Direct Connect klassische Verbindung

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) in 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 Tag hinzufügen, um key/value Paare hinzuzufügen, um diese Verbindung besser identifizieren zu 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 Dedizierte und gehostete Verbindungen.

Laden Sie den AWS Direct Connect LOA-CFA herunter

Sie können den LOA-CFA entweder über die Konsole oder über die Befehlszeile herunterladen. AWS Direct Connect Sobald Sie den LOA-CFA heruntergeladen und Ihrem Netzwerk- oder Colocation-Anbieter zur Verfügung gestellt haben, kann dieser Anbieter das Cross-Connect für Sie bestellen.

So laden Sie das LOA-CFA-Dokument herunter

1. AWS Direct ConnectÖffnen Sie https://console.aws.amazon.com/directconnect/die Konsole unter 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 Cross-Connects an AWS Direct Connect Standorten anfordern.

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

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

Ordnen Sie einer Verbindung ein MACsec CKN/CAK zu AWS Direct Connect

Nachdem Sie die unterstützende Verbindung erstellt haben MACsec, können Sie der CKN/CAK Verbindung eine zuordnen. Sie können die Zuordnung entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API erstellen.

> **Note**
>
> Sie können einen MACsec geheimen 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 Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer Verbindung.

Um einen MACsec Schlüssel mit einer Verbindung zu verknüpfen

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 Schlüssel ein. MACsec

   [Das CAK/CKN Paar verwenden] Wählen Sie Schlüsselpaar 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 und dann für Secret den MACsec geheimen Schlüssel aus.
6. Wählen Sie Associate key (Schlüssel zuordnen) aus.

Um einen MACsec Schlüssel über die Befehlszeile oder API einer Verbindung zuzuordnen

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

Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer AWS Direct Connect Verbindung

Sie können die Verknüpfung zwischen der Verbindung und dem MACsec Schlüssel entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API entfernen.

Um eine Zuordnung zwischen einer Verbindung und einem Schlüssel zu entfernen MACsec

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 MACsec Geheimnis aus, das Sie entfernen möchten, und klicken Sie dann auf Schlüssel trennen.
6. Geben Sie im Bestätigungsdialogfeld disassociate (Trennen) ein und wählen Sie dann Disassociate (Trennen) aus.

Um eine Zuordnung zwischen einer Verbindung und einem MACsec Schlüssel mithilfe der Befehlszeile oder API zu entfernen

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

Gehostete AWS Direct Connect 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 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. Bitte erkundigen Sie sich bei Ihrem AWS Direct Connect-Partner, ob er das Upgrade oder Downgrade einer bestehenden Verbindung unterstützt. Wenn Ihr Partner das Upgrade/Downgrade Ihrer Verbindung unterstützt, müssen Sie eine Verbindung nicht mehr löschen und anschließend neu erstellen, um die Bandbreite einer vorhandenen gehosteten Verbindung zu aktualisieren oder herabzustufen.

- 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:

- Eine Verbindung löschen
- Aktualisieren einer Verbindung
- Anzeigen von Verbindungsdetails

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 Virtuelle Schnittstellen und gehostete virtuelle Schnittstellen.

Akzeptieren Sie eine AWS Direct Connect gehostete Verbindung

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. Sie können eine gehostete Verbindung entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder die API akzeptieren.

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.

So akzeptieren Sie eine gehostete Verbindung mit der Befehlszeile oder API

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

Löscht eine AWS Direct Connect Verbindung

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 Löschen Sie eine virtuelle Schnittstelle.

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 Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA).

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.

Sie können eine Verbindung entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder die API löschen.

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.

So löschen Sie eine Verbindung über die Befehlszeile oder API

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

Eine AWS Direct Connect Verbindung aktualisieren

Sie können das folgende Verbindungsattribut entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API aktualisieren.

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

> **Note**
>
> MACsec ist nur für dedizierte 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`

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.

So aktualisieren Sie eine Verbindung über die Befehlszeile oder API

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

AWS Direct Connect Verbindungsdetails anzeigen

Sie können den aktuellen Status Ihrer Verbindung entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API einsehen. 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 Direct Connect-Ressourcen überwachen.

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.

So beschreiben Sie eine Verbindung mit der Befehlszeile oder API

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

Cross-Connects an AWS Direct Connect Standorten anfordern

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 Geräte an einem AWS Direct Connect Standort haben, wenden Sie sich an den entsprechenden Anbieter, um die Cross-Connect-Verbindung abzuschließen. Spezifische Anweisungen für jeden Anbieter finden Sie in den folgenden Tabellen. Partner und Kontaktinformationen sind nach Regionen geordnet. Für spezifische Cross-Connect-Preise müssen Sie sich direkt an den Direct Connect-Partner wenden. Nachdem die Cross-Connect eingerichtet 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 Geräte 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 Unterstützung durch APN-Partner. AWS Direct Connect Sie müssen das LOA-CFA-Dokument mit dem von Ihnen gewählten Anbieter teilen, um Ihre Querverbindungsanfrage zu vereinfachen.

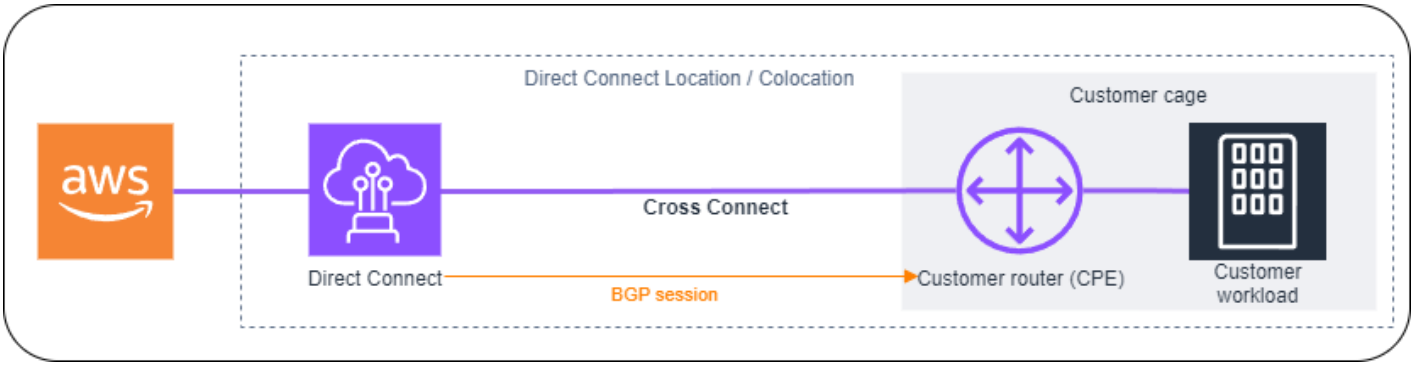
Eine AWS Direct Connect Verbindung kann den Zugriff auf Ressourcen in anderen Regionen ermöglichen. Weitere Informationen finden Sie unter Zugang zu abgelegenen AWS Direct Connect Regionen.

> **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 Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA).

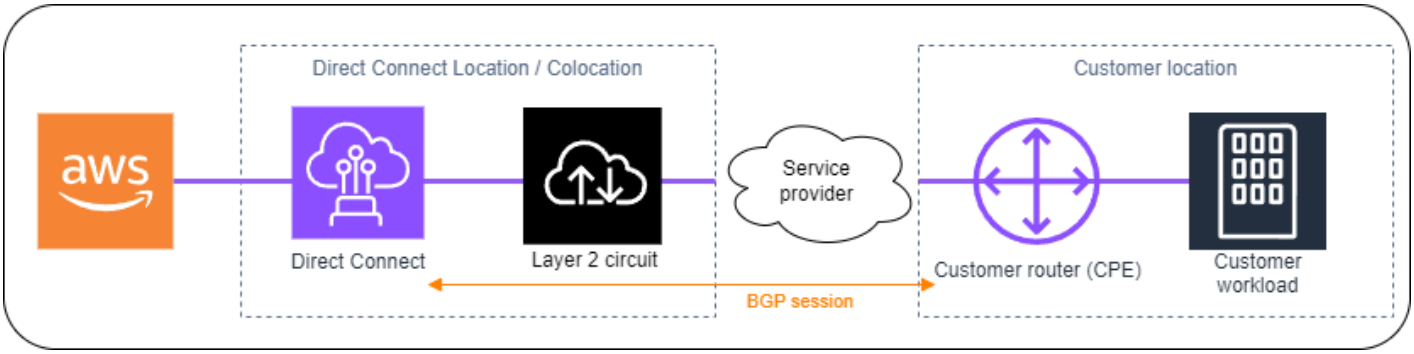
Konnektivitätsoptionen

Die verfügbaren Optionen für die Connect einem Direct Connect-Standort können je nach Partner und AWS Region variieren. Sie können mit einem der Partner im AWS Partnernetzwerk (APN) zusammenarbeiten, der eine oder mehrere der folgenden Verbindungsoptionen anbieten kann:

- Wenn Sie Ressourcen in derselben center/colocation Dateneinrichtung wie der Direct Connect-Standort bereitgestellt haben, kann die Einrichtung eine Querverbindung zwischen den AWS Direct Connect Geräten und Ihren Ressourcen herstellen. Dazu müssen Sie der Einrichtung zunächst LOA-CFA zur Verfügung stellen. Weitere Informationen finden Sie unter Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA). Im Folgenden finden Sie ein Beispiel für diese Direct Connect-Konnektivitätsoption:

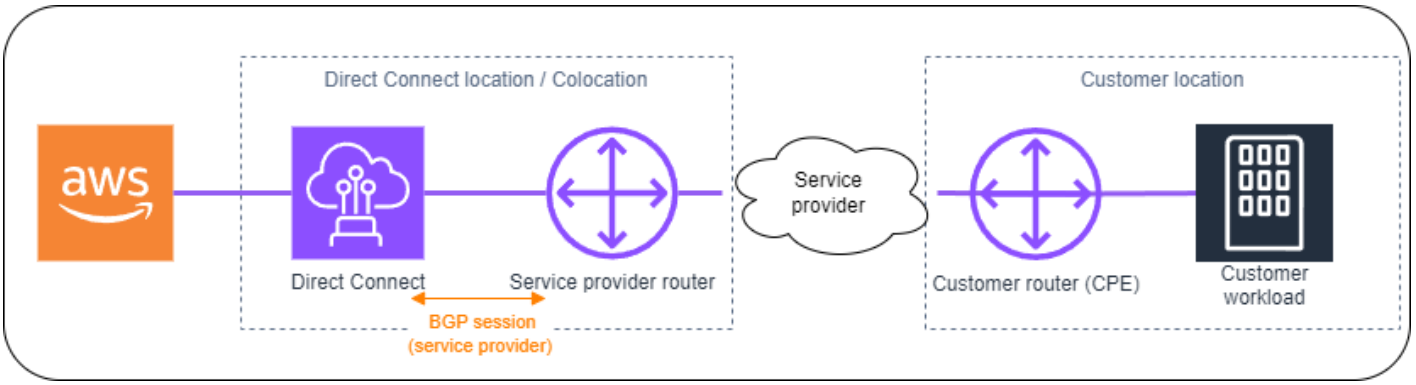


- Erweitern Sie die Direct Connect-Verbindung auf Ebene 2 (Datenverbindungsebene) über eine „Verbindung“ vom Direct Connect-Standort zum Kundenstandort, indem Sie mit Direct Connect-Partnern zusammenarbeiten. Der am Kundenstandort installierte Router bildet direkt eine BGP-Sitzung mit dem AWS Gerät. Zu den Technologien, die verwendet werden können, gehören beispielsweise Metro Ethernet, Dark Fibre oder Wavelength. Im Folgenden finden Sie ein Beispiel für diese Direct Connect-Konnektivitätsoption.



- Erweitern Sie die Direct Connect-Verbindung auf Ebene 3 (Netzwerkschicht) vom Direct Connect-Standort zu Ihrem Standort, indem Sie mit Direct Connect-Partnern zusammenarbeiten. Für diese Konnektivitätsoption stellt der Direct Connect-Partner einen Router am Direct Connect-Standort

bereit, der eine Border Gateway Protocol (BGP) -Sitzung mit den AWS Geräten bildet. Der Direct Connect-Partner hat dann ein weiteres BGP mit Ihnen eingerichtet. Dies kann beispielsweise über Multiprotocol Label Switching (MPLS) erfolgen. Im Folgenden finden Sie ein Beispiel für diese Direct Connect-Konnektivitätsoption.



USA Ost (Ohio)

Ort	Anfordern einer Verbindung
Cologix, Kolumbus COL2	Kontaktieren Sie Cologix unter sales@cologix.com.
Cologix, Minneapolis MIN3	Kontaktieren Sie Cologix unter sales@cologix.com.
CyrusOne West III, Houston	Reichen Sie eine Anfrage über das Kundenkontaktformular ein.
Equinix CH2, Chicago	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
QTS, 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.

Ort	Anfordern einer Verbindung
CoreSite 32k, New York	Geben Sie eine Bestellung über das CoreSite Kundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite VA1-VA2, Reston	Geben Sie eine Bestellung im CoreSite Kundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
Digital Realty ATL1 &ATL2, Atlanta	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
Digitale Immobilien IAD38, Ashburn	Kontaktieren Sie Digital Realty unter amazon.orders@digitalrealty.com.
Equinix DC1 - DC6 & 0-D12, Ashburn DC1	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix - und, Dallas DAA1 DC3 DC6	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix MI1, Miami	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
KIO Networks, Querétaro, MX QRO1	Wenden Sie sich an KIO Networks“.
Markley, One Summer Street, Boston	Für Bestandskunden erstellen Sie eine Anfrage über das Kundenportal. Für neue Anfragen kontaktieren Sie sales@markleygroup.com.
Netrality Data Centers, 2. Stock MMR, Philadelphia	Kontaktieren Sie Netrality Data Centers unter support@netrality.com.
QTS, Atlanta ATL1	Kontaktieren Sie QTS unter AConnect@qtsdatacenters .com.

USA West (Nordkalifornien)

Ort	Anfordern einer Verbindung
CoreSite, LA1, Los Angeles	Geben Sie eine Bestellung über das CoreSite Kundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite SV2, Milpitas	Geben Sie eine Bestellung über das CoreSiteKundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
CoreSite SV4, Santa Clara	Geben Sie eine Bestellung über das CoreSite Kundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf ihre Richtigkeit und genehmigen Sie sie dann über die MyCoreSite Website.
EdgeConneX, Phönix	Geben Sie über das EdgeOS Customer Portal eine Bestellun g auf. Nachdem Sie das Formular abgeschickt haben, stellt EdgeConne X Ihnen ein Serviceauftragsformular zur Genehmigu ng zur Verfügung. Sie können Fragen an cloudaccess@edgeco nnex.com senden.
Equinix LA3, El Segundo	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix & SV1 , San José SV5	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Kontaktieren Sie phoenixNAP Provisioning unter provision ing@phoenixnap.com.

USA West (Oregon)

Ort	Anfordern einer Verbindung
CoreSite DE1, Denver	Geben Sie eine Bestellung über das CoreSite Kundenportal auf. Nachdem Sie das Formular ausgefüllt haben, überprüfen Sie die Bestellung auf Genauigkeit und bestätigen Sie sie über die Website.
Digital Realty SEA1 0, Westin Building, Seattle	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 abgeschickt haben, stellt EdgeConne X Ihnen ein Serviceauftragsformular zur Genehmigung zur Verfügung. 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 Seattle	Kontaktieren Sie uns TierPoint unter 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).

Ort	Anfordern einer Verbindung
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 Indonesien unter awsdx@dci-indonesia.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	Kontaktieren Sie NetMagic Vertrieb und Marketing gebührenfrei unter 18001033130 oder unter marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Kontaktieren Sie Sify unter aws.directconnect@sifycorp.com .
STT Delhi, Delhi DC2	Wenden Sie sich auf Anfrage an STT. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Kontaktieren Sie STT auf Anfrage. AWSDX@sttelemediagdc .in.
STT Hyderabad, Hyderabad DC1	Wenden Sie sich auf Anfrage an STT. AWSDX@sttelemediagdc .in.

Asien-Pazifik (Seoul)

Ort	Anfordern einer Verbindung
Digitale Immobilien 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 NT, Sonderverwaltungszone Hongkong	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.
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.

Ort	Anfordern einer Verbindung
TCC Data Center, Bangkok	Kontaktieren Sie TCC Technology Co., Ltd unter gateway.ne@tcc-technology.com.

Asien-Pazifik (Sydney)

Ort	Anfordern einer Verbindung
CDC Hume 2, Canberra	Melden Sie sich im Kundenportal unter CDC Customer Portal an.
Datacom DH6, Auckland	Wenden Sie sich an Datacom bei Datacom Orbit — Auckland.
Equinix, Melbourne ME2	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.

Ort	Anfordern einer Verbindung
Chungwa Telecom, Taipei	Kontaktieren Sie CHT Taipei IDC NOC unter taipei_idc@cht.com.tw.
Equinix OS1, Ōsaka	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
Telehouse, 250 Front Street W, Toronto	Wenden Sie sich an product@ca.telehouse.com.
Cologix MTL3, Montréal	Kontaktieren Sie Cologix unter sales@cologix.com.
Cologix, Vancouver VAN2	Kontaktieren Sie 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.

Ort	Anfordern einer Verbindung
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 Ulven, Oslo, Norwegen	Kontaktieren Sie uns DigiPlex unter helpme@digiplex.com.
Equinix AM3, Amsterdam, Niederlande	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix FR5, Frankfurt	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
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.

Ort	Anfordern einer Verbindung
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 datacentre@eirevo.ie.
Equinix DX1, Dublin	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix LD5, London (Slough)	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.

Ort	Anfordern einer Verbindung
Interxion, Dublín DUB2	Kontaktieren Sie Interxion unter customer.services@interxion.com.
Interxion MRS1, Marseilles	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, Mailand ML2, 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, Manchester MA3	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	Kontaktieren Sie Telehouse Paris Voltaire über die Kontaktseite.

Europa (Stockholm)

Ort	Anfordern einer Verbindung
Interxion, Stockholm STO1	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 uns MedOne unter support@Medone.co.il
EdgeConnex, Herzlia	Kontaktieren Sie uns unter info@edgeconnecx.com EdgeConnect

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 dem AWS Support Center eine Autorisierungsbescheinigung (Letter of Authorization, LOA) des Netzwerkanbieters zur AWS Verfügung. AWS schließt die Querverbindung an dieser Stelle 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 dem AWS Support Center eine Autorisierungsbescheinigung (Letter of Authorization, LOA) des Netzwerkanbieters zur AWS Verfügung. AWS schließt die Querverbindung an dieser Stelle ab.

Naher Osten (VAE)

Ort	Anfordern einer Verbindung
Equinix DX1, Dubai, Vereinigte Arabische Emirate	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
SmartHub Rechenzentrum Etisalat, Fujairah, Vereinigte Arabische Emirate	Kontaktieren Sie das Rechenzentrum von Etisalat unter -C& SmartHub WS@etisalat.ae. IntlSales

Südamerika (São Paulo)

Ort	Anfordern einer Verbindung
Cirion BNARAGMS, Buenos Aires	Kontaktieren Sie Cirion unter cloud.connect@ciriontechnologies.com.
Equinix RJ2, Rio de Janeiro	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Equinix SP4, São Paulo	Kontaktieren Sie Equinix unter awsdealreg@equinix.com.
Tivit	Kontaktieren Sie Tivit unter aws@tivit.com.br.

AWS GovCloud (US-Ost)

Sie können in dieser Region keine Verbindungen anfordern.

AWS GovCloud (US-West)

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

AWS Direct Connect virtuelle Schnittstellen und gehostete 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 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 geben Ihnen die entsprechenden Amazon-Präfixe bekannt, damit Sie die öffentlichen IP-Adressen der Workloads in Ihren VPCs und anderen AWS Diensten erreichen können. Sie können über diese Verbindung auf alle AWS Präfixe zugreifen, z. B. auf öffentliche IP-Adressen, die von EC2 Amazon-Instances verwendet werden, Amazon S3, API-Endpunkte für AWS Dienste und Amazon.com. Sie haben keinen Zugriff auf Präfixe, die nicht von Amazon stammen. Eine aktuelle Liste der von AWS verwendeten Präfixe finden Sie unter AWS IP-Adressbereiche im Amazon VPC-Benutzerhandbuch. Auf dieser Seite können Sie eine `.json` Datei mit den aktuell veröffentlichten AWS IP-Bereichen herunterladen. Beachten Sie, dass für veröffentlichte IP-Adressbereiche:

- Präfixe, die über BGP über eine öffentliche virtuelle Schnittstelle angekündigt werden, können im Vergleich zu den in der Liste der IP-Adressbereiche aufgeführten Präfixe aggregiert oder deaggregiert sein. AWS

- Alle IP-Adressbereiche, auf die Sie AWS über Ihre eigenen IP-Adressen (BYOIP) zugreifen, sind nicht in der `.json` Datei enthalten, aber diese BYOIP-Adressen werden AWS dennoch über eine öffentliche virtuelle Schnittstelle beworben.
- AWS bewirbt Kundenpräfixe, die über öffentliche virtuelle Direct Connect-Schnittstellen empfangen wurden, nicht erneut mit Netzwerken außerhalb von. AWS Präfixe, die auf einer öffentlichen virtuellen Schnittstelle beworben werden, sind für alle Kunden unter sichtbar. AWS

> **Note**
>
> Wir empfehlen die Verwendung eines Firewallfilters (basierend auf der source/destination Adresse von Paketen), um den Verkehr zu und von einigen Präfixen zu kontrollieren.

Weitere Informationen zu öffentlichen virtuellen Schnittstellen und Routing-Richtlinien finden Sie unter the section called “Routing-Richtlinien für öffentliche virtuelle Schnittstellen”.

SiteLink

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

SiteLink ist eine optionale Direct Connect-Funktion für private virtuelle 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.
> - SiteLink funktioniert nicht, wenn ein lokaler Router dieselbe Route AWS auf mehreren virtuellen Schnittstellen ankündigt.

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 virtuellen Gateway oder Transit Gateway zugeordnet ist.	Unterstützt
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 MTUs für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen.

Voraussetzungen für virtuelle Schnittstellen

Tun Sie Folgendes, bevor Sie eine virtuelle Schnittstelle erstellen:

- Verbindung erstellen Weitere Informationen finden Sie unter 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

Ressource	Erforderliche Informationen
	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. **Note** • Sie können nicht dieselbe ASN für das Kunden-Gateway und das Virtual gateway/Direct Connect-Gateway auf der virtuellen Schnittst elle verwenden. • Sie können dieselbe Kunden-Gateway-ASN für mehrere virtuelle Schnittstellen verwenden. • Mehrere virtuelle Schnittstellen können dieselbe ASN für virtuelle s Gateway/Direct Connect-Gateway und dieselbe Kunden-Ga teway-ASN haben, sofern sie Teil verschiedener Direct Connect-V erbindungen sind. Zum Beispiel: Virtuelles Gateway (ASN 64.496) <---Virtuelle Schnittstelle 1 (Direct Connect-Verbindung 1) ---> Kunden-Gateway (ASN 64.511) Virtuelles Gateway (ASN 64.496) <---Virtuelle Schnittstelle 2 (Direct Connect-Verbindung 2) ---> Kunden-Gateway (ASN 64.511)
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 Partner diesen Wert. AWS Direct Connect Sie können den Wert nicht ändern, nachdem Sie die virtuelle Schnittstelle erstellt haben.

Ressource	Erforderliche Informationen
Peer-IP-Adressen	Eine virtuelle Schnittstelle kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. **Note** • Das Peering IPs für private und virtuelle Transitschnittstellen kann aus jedem gültigen IP-Bereich erfolgen. Dazu können auch kundeneigene öffentliche IP-Adressen gehören, sofern diese nur für die Erstellung der BGP-Peering-Sitzung verwendet werden und nicht über die virtuelle Schnittstelle angekündigt oder für NAT verwendet werden. • Wir können nicht garantieren, dass wir alle Anfragen nach bereitgestellten öffentlichen Adressen erfüllen können. AWS IPv4 Der Wert kann eine der folgenden Formen annehmen: • Ein kundeneigener CIDR IPv4 Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP

Ressource	Erforderliche Informationen
	verwendet werden. 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 bereitgestellter 3/1-CIDR. Wenden Sie sich an den AWS Support, um ein öffentliches IPv4 CIDR anzufordern (und geben Sie in Ihrer Anfrage einen Anwendungsfall an) • (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6

Ressource	Erforderliche Informationen
BGP-Informationen	• 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 benutzerdefinierten 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 MD5 standardmäßig. 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 zur Werbung über BGP. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. Stellen Sie sicher, dass Sie auf die öffentlichen Präfixe BGP-Community-Tags anwenden.
	  • Sie verwenden AS_PATH, wenn Sie eine öffentliche ASN in einer Konfiguration haben. active/passive
	  Weitere Informationen finden Sie unter Routing-Richtlinien und BGP-Communities.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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 Transit Gateway Gateway-Routentabelle konfiguriert sind, unterstützen Jumbo Frames, auch von EC2 Instances mit statischen VPC-Routentabelleneinträgen zum Transit Gateway 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:

- Für Privat VIFs - und VIFs Transitdienste gilt das Konto für die virtuelle Schnittstelle und das Virtual Private gateway/Direct Connect-Gateway-Ziel.
- Im öffentlichen Bereich VIFs wird das Konto für die Abrechnung über virtuelle Schnittstellen verwendet. Die Nutzung ausgehender Daten (Data Transfer Out, DTO) wird anhand der AWS Direct Connect Datenübertragungsrate an den Eigentümer der Ressource abgerechnet.

> **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 Links. IPv4 Point-to-Point

MTUs für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen

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. Die MTU einer privaten virtuellen Schnittstelle kann entweder 1500 oder 9001 (Jumbo-Frames) betragen. 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 über zwei private virtuelle Schnittstellen verfügen, die dieselbe Route ankündigen, aber unterschiedliche MTU-Werte verwenden, oder wenn Sie über ein Site-to-Site VPN verfügen, das dieselbe Route ankündigt, wird eine MTU von 1500 verwendet.

> **Important**
>
> Jumbo-Frames gelten nur für weitergeleitete 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 Jumbo Frames nicht unterstützt, löscht sie Jumbo Frames aus Direct Connect. Alle EC2 Instance-Typen außer C1, CC1 T1 und M1 unterstützen Jumbo-

Frames. Weitere Informationen finden Sie unter Network Maximum Transmission Unit (MTU) für Ihre EC2 Instance im EC2 Amazon-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.
MTUs for Private VIFs ist auf 8500 standardisiert. 9001 wird weiterhin akzeptiert, bis es entfernt wird.

Die Schritte zum Einstellen der MTU für eine private virtuelle Schnittstelle finden Sie unter. Legen Sie die MTU einer privaten virtuellen Schnittstelle fest

AWS Direct Connect virtuelle Schnittstellen

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, AWS Organizations die sich von Ihrem unterscheiden, zu erstellen, erstellen Sie eine gehostete virtuelle Schnittstelle.

Gehen Sie wie folgt vor, um eine virtuelle Schnittstelle zu erstellen:

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

Voraussetzungen

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

Voraussetzungen für die Übertragung virtueller Schnittstellen zu einem 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.

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Die MTU einer privaten virtuellen Schnittstelle kann entweder 1500 oder 9001 (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.

Erstellen Sie eine AWS Direct Connect öffentliche virtuelle Schnittstelle

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 Border Gateway Protocol Autonomous System Number (ASN) Ihres lokalen Peer-Routers für die neue virtuelle Schnittstelle ein.

      Die gültigen Werte lauten 1-2147483647.

      > **Note**
      >
      > Wenn Sie eine BGP-Peering-Sitzung AWS über eine öffentliche virtuelle Schnittstelle einrichten, verwenden Sie 7224 als ASN, um die BGP-Sitzung nebenbei einzurichten. AWS Die ASN auf Ihrem Router oder Kunden-Gateway-Gerät sollte sich von dieser ASN unterscheiden.

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

   a. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

b. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie Ihren MD5 BGP-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 Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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(API)AWS Direct Connect

Erstellen Sie eine AWS Direct Connect private virtuelle Schnittstelle

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 unterAWS 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. Die MTU einer privaten virtuellen Schnittstelle kann entweder 1500 oder 9001 (Jumbo-Frames) betragen. 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).

> **Note**
>
> Die MTU für private virtuelle Schnittstellen ist auf 8500 standardisiert. 9100 wird jedoch weiterhin unterstützt, bis sie entfernt wird.

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

1. Öffnen Sie die Konsole unter v2/home AWS Direct Connect. https://console.aws.amazon.com/directconnect/
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 Systemnummer 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      > **Important**
      >
      > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem

Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point

- Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
- Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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.

> **Note**
>
> Die MTU für private virtuelle Schnittstellen ist auf 8500 standardisiert. 9100 wird jedoch weiterhin unterstützt, bis sie entfernt wird.

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)

Erstellen Sie eine virtuelle Transitschnittstelle zum AWS Direct Connect Gateway

Machen Sie sich mit dem Text vertraut, bevor Sie eine virtuelle Transitschnittstelle mit dem Direct Connect-Gateway verbinden.

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 Systemnummer 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

   [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

   - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
   - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

   > **Important**
   >
   > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
   >
   > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
   > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

   [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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)

Laden Sie die AWS Direct Connect Router-Konfigurationsdatei herunter

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, die MACsec aktiviert wurden, 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

Um die Router-Konfigurationsdatei herunterzuladen

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.
7. Wenn Sie Ihren Router für manuell konfigurieren müssen MACsec, 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

Parameter	Beschreibung
Key Cipher Suite	16
Vertraulichkeits-Offset	0
ICV-Indikator	Nein
SAK-Rekey-Zeit	PN Rollover>

Gehostete AWS Direct Connect 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.

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 kann eine BGP-Peering-Sitzung für IPv4 IPv6, oder eine von beiden (Dual-Stack) unterstützen. Verwenden Sie Elastic IPs (EIPs) oder Bring Your Own IP Addresses (BYOIP) aus dem Amazon-Pool nicht, 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 öffentliche virtuelle Schnittstelle) Sie müssen eindeutige öffentliche IPv4 Adressen angeben, deren Eigentümer Sie sind. Der Wert kann eine der folgenden Formen annehmen:
	  • Ein CIDR, das sich im Besitz IPv4 eines Kunden befindet
	
	Dabei kann es sich um beliebige öffentliche IPs (kundeneigene oder von bereitgestellte AWS) handeln, es muss jedoch dieselbe Subnetzmaske sowohl für Ihre Peer-IP als auch für die AWS Router-Peer-IP verwendet werden. 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 ein öffentliches IPv4 CIDR anzufordern (und geben Sie in Ihrer Anfrage einen Anwendungsfall an)
	
	Note
	Wir können nicht garantieren, dass wir in der Lage sein werden, alle Anfragen für von uns AWS bereitgestellte öffentliche IPv4 Adressen zu erfüllen.

Ressource	Erforderliche Informationen
	• (Nur private virtuelle Schnittstelle) Amazon kann private IPv4 Adressen für Sie generieren. Wenn Sie Ihre eigene angeben, stellen Sie sicher, dass Sie privat nur CIDRs für Ihre Router-Schnittstelle und die AWS Direct Connect-Schnittstelle angeben. Geben Sie beispielsweise 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-Peer-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 IPv6 /125 CIDR zu. Sie können Ihre eigenen Peer-Adressen nicht angeben. IPv6
Adress-Familie	Ob die BGP-Peering-Sitzung beendet IPv4 sein wird oder. IPv6
BGP-Informationen	• 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 benutzerdefinierten 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 MD5 standardmäßig. 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, um über BGP zu werben. Sie müssen mindestens einen Präfix über BGP ankündigen (bis maximal 1.000 Präfixe).
	• IPv4: Der IPv4 CIDR kann sich mit einem anderen öffentlichen IPv4 CIDR überschneiden, der verwendet wurde, AWS Direct Connect wenn eine der folgenden Bedingungen zutrifft:
	  • Sie CIDRs kommen aus verschiedenen AWS Regionen. 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.
	• Über eine öffentliche virtuelle Direct Connect-Schnittstelle können Sie eine beliebige Präfixlänge von /1 bis /32 für IPv4 und von /1 bis /64 für angeben. IPv6
	• 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.

Ressource	Erforderliche Informationen
(Nur private und virtuelle Transitschnittstellen) Jumbo-Frames	Die maximale Übertragungseinheit (MTU) von Paketen über. 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.

Erstellen Sie eine gehostete private virtuelle Schnittstelle in AWS Direct Connect

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

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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      > **Important**
      >
      > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
      >
      > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.

- Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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.

> **Note**
>
> Die MTU für private virtuelle Schnittstellen ist auf 8500 standardisiert. 9100 wird jedoch weiterhin unterstützt, bis sie entfernt wird.

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 Besitzer des anderen AWS Kontos akzeptiert wurde, können Sie die Konfigurationsdatei herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei herunterladen.

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

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

Erstellen Sie eine gehostete öffentliche virtuelle Schnittstelle in AWS Direct Connect

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

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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

   [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

   - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.

- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

  [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.

7. Um Amazon Präfixe anzukündigen, geben Sie für Präfixe, die Sie bewerben möchten, die IPv4 CIDR-Zieladressen (durch Kommas getrennt) ein, an die der 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 Besitzer des anderen AWS Kontos akzeptiert wurde, können Sie die Konfigurationsdatei herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei 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)

Erstellen Sie eine AWS Direct Connect gehostete virtuelle Transitschnittstelle

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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

   [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

   - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
   - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

   > **Important**
   >
   > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
   >
   > - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
   > - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

   [IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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 Besitzer des anderen AWS Kontos akzeptiert wurde, können Sie die Router-Konfigurationsdatei für Ihr Gerät herunterladen. Weitere Informationen finden Sie unter Routerkonfigurationsdatei 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)

Details zur AWS Direct Connect virtuellen Schnittstelle anzeigen

Sie können den aktuellen Status Ihrer virtuellen Schnittstelle entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API einsehen. 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)
- DescribeVirtualInterfaces(API)AWS Direct Connect

Fügen Sie einer AWS Direct Connect virtuellen Schnittstelle einen BGP-Peer hinzu

Fügen Sie Ihrer virtuellen Schnittstelle mithilfe der AWS Direct Connect Konsole, der Befehlszeile IPv4 oder der API eine oder eine IPv6 BGP-Peering-Sitzung hinzu oder löschen Sie sie.

Eine virtuelle Schnittstelle kann eine einzelne BGP-Peering-Sitzung und eine einzelne IPv4 IPv6 BGP-Peering-Sitzung unterstützen. Sie können keine eigenen IPv6 Peer-Adressen für eine IPv6 BGP-Peering-Sitzung angeben. Amazon weist Ihnen automatisch eine IPv6 /125 CIDR zu.

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

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

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) Gehen Sie wie folgt vor, um IPv4 BGP-Peers hinzuzufügen:
   - Wählen Sie IPv4.
   - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll. Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.
6. (Öffentliche virtuelle Schnittstelle) Gehen Sie wie folgt vor, um IPv4 BGP-Peers hinzuzufügen:

- Geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die der Datenverkehr gesendet werden soll.
- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

> **Important**
>
> Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

7. (Private oder öffentliche virtuelle Schnittstelle) Um IPv6 BGP-Peers hinzuzufügen, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon zugewiesen. Sie können keine benutzerdefinierten IPv6 Adressen angeben.
8. Geben Sie für BGP ASN die autonome Systemnummer 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. Um Ihren eigenen BGP-Schlüssel bereitzustellen, geben Sie für den BGP-Authentifizierungsschlüssel Ihren MD5 BGP-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)
- Erstellen BGPPeer (API)AWS Direct Connect

Löschen Sie eine AWS Direct Connect virtuelle Schnittstelle (BGP-Peer)

Wenn Ihre virtuelle Schnittstelle sowohl über eine als auch über eine IPv4 IPv6 BGP-Peering-Sitzung verfügt, können Sie eine der BGP-Peering-Sitzungen löschen (aber nicht beide). Sie können einen BGP-Peer mit virtueller Schnittstelle entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API löschen.

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)
- Löschen BGPPeer (API)AWS Direct Connect

Stellen Sie die MTU einer AWS Direct Connect privaten virtuellen Schnittstelle ein

Wenn Ihre virtuelle Schnittstelle sowohl über eine als auch über eine IPv4 IPv6 BGP-Peering-Sitzung verfügt, können Sie eine der BGP-Peering-Sitzungen löschen (aber nicht beide). Weitere Informationen zu MTUs privaten virtuellen Schnittstellen finden Sie unter MTUs Für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen.

Sie können die MTU einer privaten virtuellen Schnittstelle entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API festlegen.

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-Größe 8500) die Option 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)
- UpdateVirtualInterfaceAttributesAWS Direct Connect (API)

AWS Direct Connect Virtuelle Schnittstellen-Tags hinzufügen oder entfernen

Tags bieten eine Möglichkeit zur Identifizierung der virtuellen Schnittstelle. Sie können ein Tag entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder die API hinzufügen oder entfernen, wenn Sie der Kontoinhaber für die virtuelle 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)

Löschen Sie eine AWS Direct Connect virtuelle Schnittstelle

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.

Sie können eine virtuelle Schnittstelle entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API löschen.

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)
- DeleteVirtualInterface(API)AWS Direct Connect

Akzeptieren Sie eine gehostete AWS Direct Connect virtuelle Schnittstelle

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.

Sie können eine gehostete virtuelle Schnittstelle entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API akzeptieren.

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(API)AWS Direct Connect

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)

Migrieren Sie eine AWS Direct Connect virtuelle Schnittstelle

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. VLANs IDs sind einzigartig. Daher würde die Migration einer VIF auf diese Weise bedeuten, dass sie nicht übereinstimmen. VLANs 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 v2/home. https://console.aws.amazon.com/directconnect/
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:

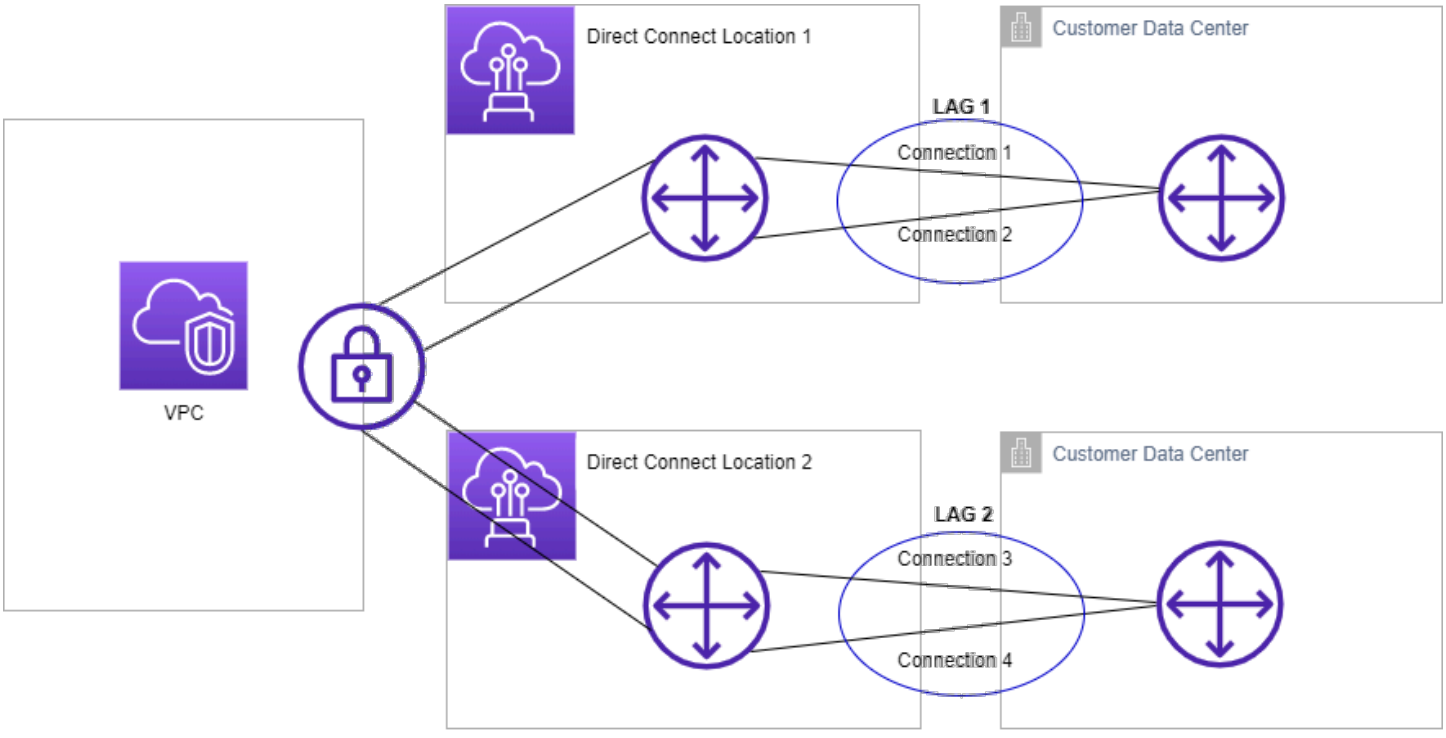
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface(API)AWS Direct Connect

AWS Direct Connect Link-Aggregationsgruppen () LAGs

Sie können mehrere Verbindungen verwenden, um die verfügbare Bandbreite zu erhöhen. Eine Link Aggregation Group (LAG) ist eine logische Schnittstelle, die das Link Aggregation Control Protocol (LACP) verwendet, um mehrere Verbindungen an einem einzigen AWS Direct Connect Endpunkt zu aggregieren, sodass Sie sie als eine einzige, verwaltete Verbindung behandeln können. LAGs Optimieren Sie die Konfiguration, da die LAG-Konfiguration für alle Verbindungen in der Gruppe gilt.

> **Note**
>
> Multi-Chassis LAG (MLAG) wird von nicht unterstützt. AWS

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 Standort enden, und dann die beiden LAGs statt 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, 100 Gbit/s oder 400 Gbit/s haben.
- Alle Verbindungen in der LAG müssen dieselbe Bandbreite aufweisen.
- Sie können maximal zwei 100-Gbit/s- oder 400-Gbit/s-Verbindungen oder vier Verbindungen mit einer Portgeschwindigkeit von weniger als 100 Gbit/s 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 am selben Endpunkt enden. AWS Direct Connect
- LAGs werden für alle virtuellen Schnittstellentypen unterstützt — öffentlich, privat und transitweit.

Wenn Sie eine LAG erstellen, können Sie den Letter of Authorization and Connecting Facility Assignment (LOA-CFA) für eine neue physische Verbindung einzeln von der Konsole herunterladen. AWS Direct Connect Weitere Informationen finden Sie unter Autorisierungsschreiben und Zuweisung von Verbindungseinrichtungen (LOA-CFA).

Alle LAGs haben ein Attribut, das die Mindestanzahl von Verbindungen in der LAG bestimmt, die betriebsbereit sein müssen, damit die LAG selbst betriebsbereit ist. Bei neuen LAGs ist dieses Attribut standardmäßig auf 0 gesetzt. 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 der LAG mehr Verbindungen zuordnen, können wir möglicherweise nicht garantieren, dass genügend Ports auf einem bestimmten AWS Direct Connect Endpunkt verfügbar sind.

Themen

- MACsec Überlegungen für AWS Direct Connect
- Erstellen Sie eine LAG an einem AWS Direct Connect Endpunkt
- LAG-Details an einem AWS Direct Connect Endpunkt anzeigen

- Eine LAG an einem AWS Direct Connect Endpunkt aktualisieren
- Eine Verbindung mit einer LAG an einem AWS Direct Connect Endpunkt verknüpfen
- Verbindung an einem Endpunkt von einer LAG trennen AWS Direct Connect
- Ordnen Sie ein MACsec CKN/CAK einer Endpunkt-LAG zu AWS Direct Connect
- Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer AWS Direct Connect Endpunkt-LAG
- Löschen Sie eine AWS Direct Connect Endpunkt-LAG

MACsec Überlegungen für AWS Direct Connect

Beachten Sie Folgendes, wenn Sie ein konfigurieren MACsec möchtenLAGs:

- 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 MACsec LAG-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 MACsec LAG-Schlüssel der Verbindung zu.

Erstellen Sie eine LAG an einem AWS Direct Connect Endpunkt

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.

Um aus bestehenden Verbindungen eine LAG zu erstellen, müssen sich die Verbindungen auf demselben AWS Gerät befinden (am selben AWS Direct Connect Endpunkt enden). 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 AWS wird die Konnektivität zu während der Erstellung der LAG unterbrochen.

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 100 Gbit/s oder 400 Gbit/s beträgt.
   - (Optional) Konfigurieren Sie die MAC-Sicherheit (MACsec) für die Verbindung. Wählen Sie unter Zusätzliche Einstellungen die Option Einen MACsec fähigen Port anfordern aus.

     MACsec ist nur für dedizierte 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.

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 100 Gbit/s oder 400 Gbit/s ist.
   - 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.

So erstellen Sie eine LAG über die Befehlszeile oder API

- create-lag (AWS CLI)
- CreateLag(API)AWS Direct Connect

Um zu beschreiben, wie Sie die LAGs Befehlszeile oder API verwenden

- 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 Verbindung einer LAG zuordnen und Verbindung von einer LAG trennen.

LAG-Details an einem AWS Direct Connect Endpunkt anzeigen

Nachdem Sie eine LAG erstellt haben, können Sie ihre Details entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API anzeigen.

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 über die LAG anzeigen, einschließlich ihrer ID und des AWS Direct Connect Endpunkts, an dem die Verbindungen beendet werden.

Anzeigen von Informationen zu Ihrer LAG Volume mithilfe der Befehlszeile oder API

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

Eine LAG an einem AWS Direct Connect Endpunkt aktualisieren

Sie können die folgenden Link-Aggregationsgruppen-Attribute (LAG) entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API aktualisieren:

- Den Namen der LAG.
- Den Wert der Mindestanzahl an Verbindungen, die für den Betrieb der LAG selbst erforderlich sind.
- Der MACsec Verschlüsselungsmodus der LAG.

  MACsec ist nur für dedizierte 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.

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.

So aktualisieren Sie eine LAG über die Befehlszeile oder API

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

Eine Verbindung mit einer LAG an einem AWS Direct Connect Endpunkt verknüpfen

Sie können eine bestehende Verbindung mit einer LAG entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API 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 verwenden. 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 Verbindung AWS über die Verbindung wird während der Zuordnung unterbrochen.

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.

So verknüpfen Sie eine Verbindung über die Befehlszeile oder API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(API)AWS Direct Connect

Verbindung an einem Endpunkt von einer LAG trennen AWS Direct Connect

Wandeln Sie eine Verbindung in eine eigenständige Verbindung um, indem Sie sie entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API von einer LAG trennen. 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 zu wurde während AWS der Trennung unterbrochen.

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.

So heben Sie die Verknüpfung einer Verbindung über die Befehlszeile oder API auf

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag(API)AWS Direct Connect

Ordnen Sie ein MACsec CKN/CAK einer Endpunkt-LAG zu AWS Direct Connect

Nachdem Sie die LAG erstellt haben, die Unterstützung MACsec bietet, können Sie der Verbindung entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API eine CKN/CAK zuordnen.

> **Note**
>
> Sie können einen MACsec geheimen 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 “Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer LAG”.

Um einen MACsec Schlüssel einer LAG zuzuordnen

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 Schlüssel ein. MACsec

   [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 und dann für Secret den MACsec geheimen Schlüssel aus.
6. Wählen Sie Associate key (Schlüssel zuordnen) aus.

Um einen MACsec Schlüssel über die Befehlszeile oder API einer LAG zuzuordnen

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

Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer AWS Direct Connect Endpunkt-LAG

Sie können die Zuordnung zwischen der LAG und dem MACsec Schlüssel entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API entfernen.

Um eine Zuordnung zwischen einer LAG und einem MACsec Schlüssel zu entfernen

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 MACsec Geheimnis aus, das Sie entfernen möchten, und klicken Sie dann auf Schlüssel trennen.
5. Geben Sie im Bestätigungsdialogfeld disassociate (Trennen) ein und wählen Sie dann Disassociate (Trennen) aus.

Um eine Zuordnung zwischen einer LAG und einem MACsec Schlüssel mithilfe der Befehlszeile oder API zu entfernen

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

Löschen Sie eine AWS Direct Connect Endpunkt-LAG

Wenn Sie sie nicht mehr benötigen LAGs, 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 Eine Verbindung löschen.

Sie können eine LAG entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API löschen.

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 und dann Löschen aus.
4. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).

So löschen Sie eine LAG über die Befehlszeile oder API

- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect API)

AWS Direct Connect Gateways

Sie können mit AWS Direct Connect Gateways über die Amazon VPC-Konsole oder die arbeiten. AWS CLI

- Direct Connect-Gateways

  Mithilfe eines Direct Connect-Gateways können Sie das Direct Connect-Gateway einem Transit-Gateway mit mehreren VPCs, einem virtuellen privaten Gateway oder, wenn Sie AWS Cloud WAN verwenden, einem Cloud WAN-Kernnetzwerk zuordnen.
- Virtual Private Gateway-Zuordnungen

  Mithilfe eines virtuellen privaten Gateways können Sie das Direct Connect-Gateway über eine private virtuelle Schnittstelle einem oder mehreren VPCs Konten zuordnen, die sich in derselben oder verschiedenen Regionen befinden.
- Transit-Gateway-Zuordnungen

  Verwenden Sie ein Direct Connect-Gateway, um Ihre Direct Connect-Verbindung über eine virtuelle Transitschnittstelle mit den VPCs oder zu verbinden VPNs , die an Ihr Transit-Gateway angeschlossen sind.
- Zuordnungen zu Cloud-WAN-Kernnetzwerken

  Verwenden Sie ein Direct Connect-Gateway, um ein Direct Connect-Gateway einem AWS Network Manager Kernnetzwerk zuzuordnen.
- Interaktionen zulässiger Präfixe

  Verwenden Sie zulässige Präfixe, um mit Transit-Gateways und virtuellen privaten Gateways zu interagieren.

Themen

- AWS Direct Connect Gateways
- AWS Direct Connect virtuelle private Gateway-Verknüpfungen
- AWS Direct Connect Gateways und Transit-Gateway-Verknüpfungen
- AWS Direct Connect Gateway- und AWS Cloud-WAN-Kernnetzwerkzuordnungen
- Zulässige Präfixe, Interaktionen für Gateways AWS Direct Connect

AWS Direct Connect Gateways

Verwenden Sie AWS Direct Connect das Gateway, um Ihre zu verbinden VPCs. Sie verknüpfen ein AWS Direct Connect Gateway mit einem der folgenden Elemente:

- Ein Transit-Gateway, wenn Sie mehrere VPCs in derselben Region haben
- Ein Virtual Private Gateway
- Ein AWS Cloud-WAN-Kernnetzwerk

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 AWS GovCloud (US) die Regionen AWS China ein, schließt sie jedoch nicht ein. Ein Direct Connect-Gateway ist eine virtuelle Komponente von Direct Connect, die als verteilter Satz von BGP-Routenreflektoren konzipiert ist. Da es außerhalb des Datenverkehrspfads betrieben wird, wird vermieden, dass ein einziger Fehlerpunkt entsteht oder Abhängigkeiten von bestimmten Faktoren entstehen. AWS-Regionen Hochverfügbarkeit ist von Haus aus in das Design integriert, sodass nicht mehrere Direct Connect-Gateways erforderlich sind.

Kunden VPCs , die Direct Connect verwenden und dabei 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 für ein Supernet über zwei oder mehr Kanäle geworben wird VPCs, deren angeschlossene virtuelle private Gateways (VGWs) demselben Direct Connect-Gateway und derselben virtuellen Schnittstelle zugeordnet sind. In diesem Fall VPCs können

sie 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 dem VPCs an ein Direct Connect angeschlossenen Gateway (z. B. 10.0.0.0/24 und 10.0.1.0/24) überschneidet und sich auf derselben virtuellen Schnittstelle befindet, können sie von Ihrem lokalen Netzwerk aus miteinander kommunizieren. VPCs

Wenn Sie die VPC-to-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 VPCs, um den Verkehr zwischen ihnen zu blockieren. Verwenden Sie diese Gruppen auch als Teil der Standardsicherheitsgruppe in der VPC.
2. Vermeiden Sie es, in Ihrem lokalen Netzwerk für ein Supernet zu werben, das sich mit Ihrem überschneidet. VPCs Stattdessen können Sie für spezifischere Routen aus Ihrem lokalen Netzwerk werben, die sich nicht mit Ihrem überschneiden. VPCs
3. Stellen Sie für jede VPC, die Sie mit Ihrem lokalen Netzwerk verbinden möchten, ein einzelnes Direct Connect Gateway bereit, anstatt dasselbe Direct Connect Gateway für mehrere zu verwenden. VPCs Anstatt beispielsweise ein einziges Direct Connect Gateway für Ihre Entwicklung und Produktion zu verwenden VPCs, verwenden Sie separate Direct Connect Gateways für jedes dieser VPCs Gateways.

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 über eine Konfiguration mit mehreren VPCs verbundenen Transit-Gateways verfügen, die demselben Direct Connect-Gateway zugeordnet sind, VPCs können diese miteinander kommunizieren. Um zu verhindern, dass die VPCs kommunizieren, ordnen Sie den VPC-Anhängen, für die die Blackhole-Option aktiviert ist, eine Routing-Tabelle zu.

Themen

- Szenarien
- Ein AWS Direct Connect Gateway erstellen
- Migrieren Sie von einem virtuellen privaten Gateway zu einem AWS Direct Connect Gateway
- Ein AWS Direct Connect Gateway löschen

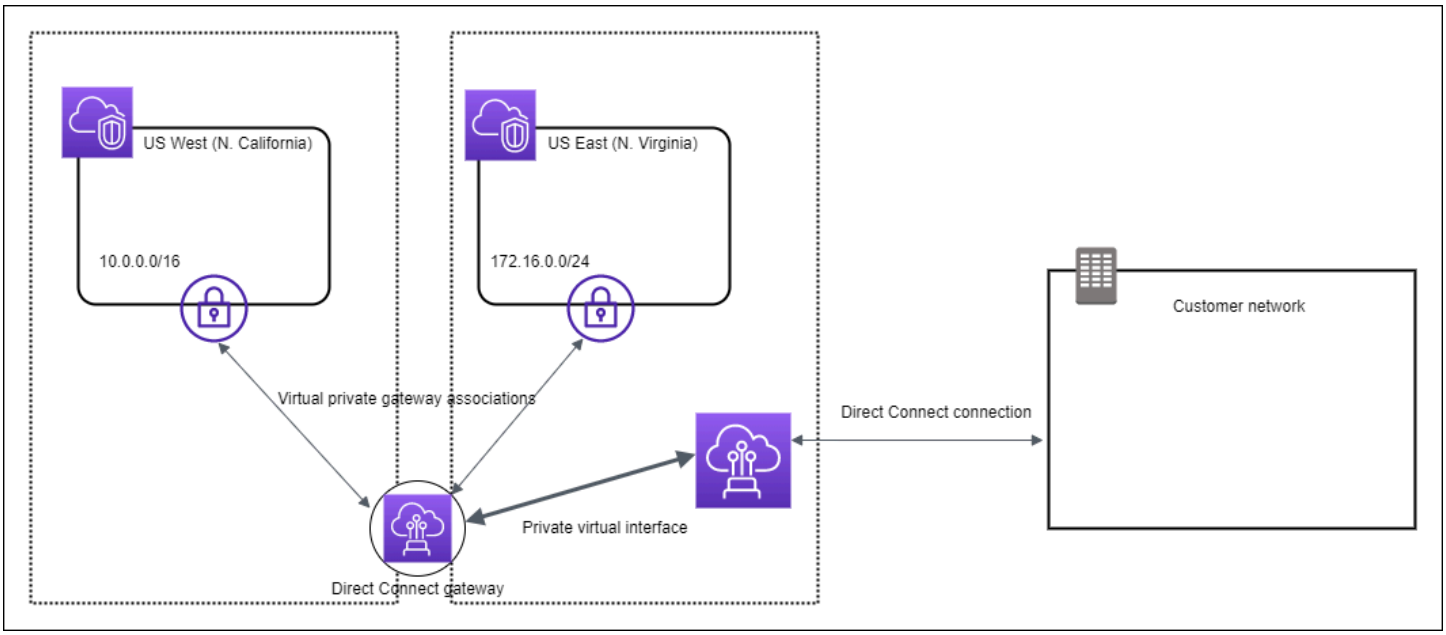
Szenarien

Im Folgenden werden nur einige Szenarien für die Verwendung von Direct Connect-Gateways beschrieben.

Szenario: Virtuelle private Gateway-Verknüpfungen

In der folgenden Abbildung ermöglicht Ihnen das Direct Connect-Gateway, Ihre AWS Direct Connect Verbindung in der Region USA Ost (Nord-Virginia) für den Zugriff über Ihr Konto sowohl VPCs in den Regionen USA Ost (Nord-Virginia) als auch USA West (Nordkalifornien) zu verwenden.

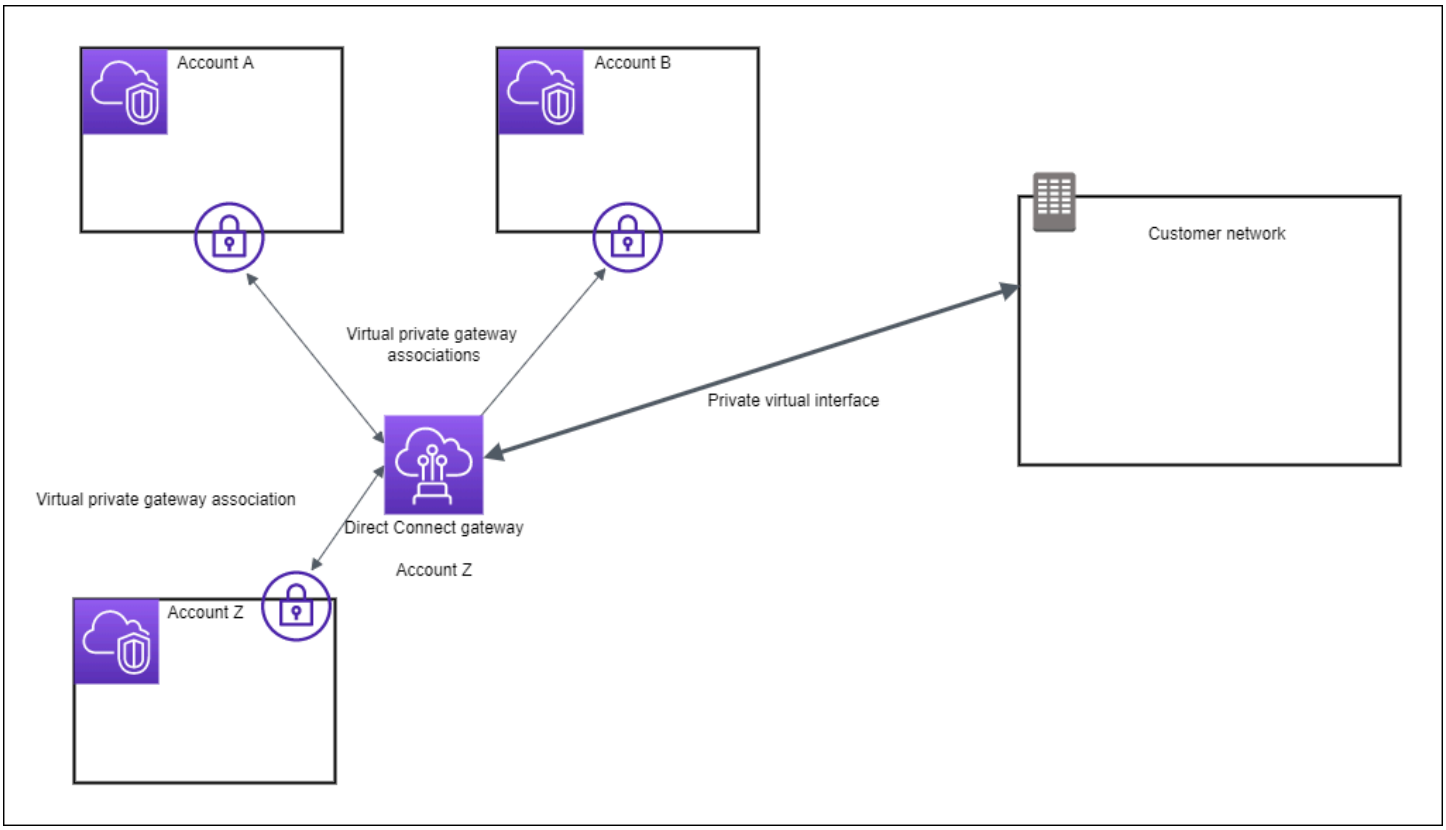
Jede VPC verfügt über ein Virtual Private Gateway, das über eine Virtual-Private-Gateway-Zuordnung eine Verbindung zum Direct-Connect-Gateway herstellt. Das Direct Connect-Gateway verwendet eine private virtuelle Schnittstelle für die Verbindung zum AWS Direct Connect Standort. Es besteht eine AWS Direct Connect -Verbindung vom Standort zum Kunden-Rechenzentrum.



Szenario: Kontenübergreifende virtuelle private Gateway-Verknüpfungen

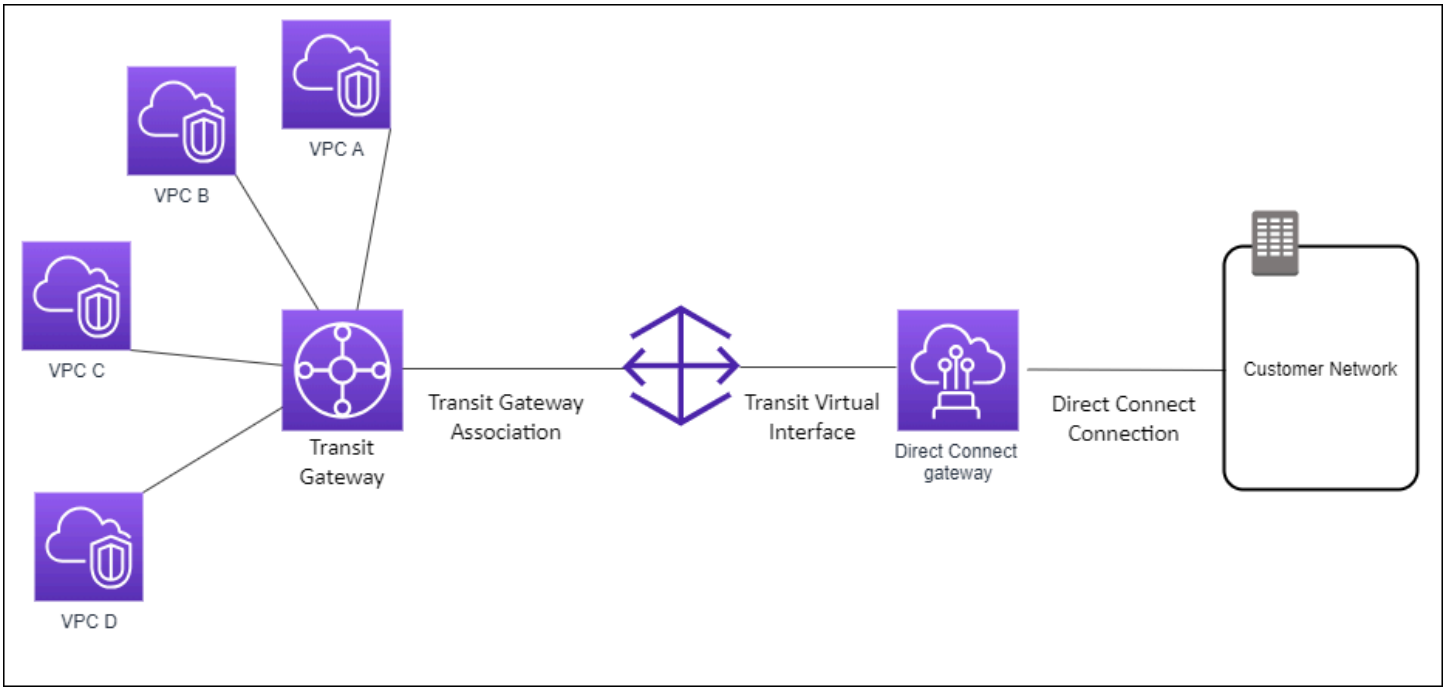
Beispiel: Szenario mit einem Direct Connect-Gateway-Eigentümer (Konto Z), dem das Direct Connect-Gateway gehört. Konto A und Konto B möchten das Direct Connect-Gateway verwenden. Konto A und Konto B senden jeweils einen Verknüpfungsvorschlag an Konto Z. Dieses akzeptiert die Verknüpfungsvorschläge und 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.



Szenario: Transit-Gateway-Verknüpfungen

Das folgende Diagramm zeigt, wie Sie mit dem Direct Connect-Gateway eine einzige Verbindung zu Ihrer Direct Connect-Verbindung herstellen können, die alle verwenden VPCs können.



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:

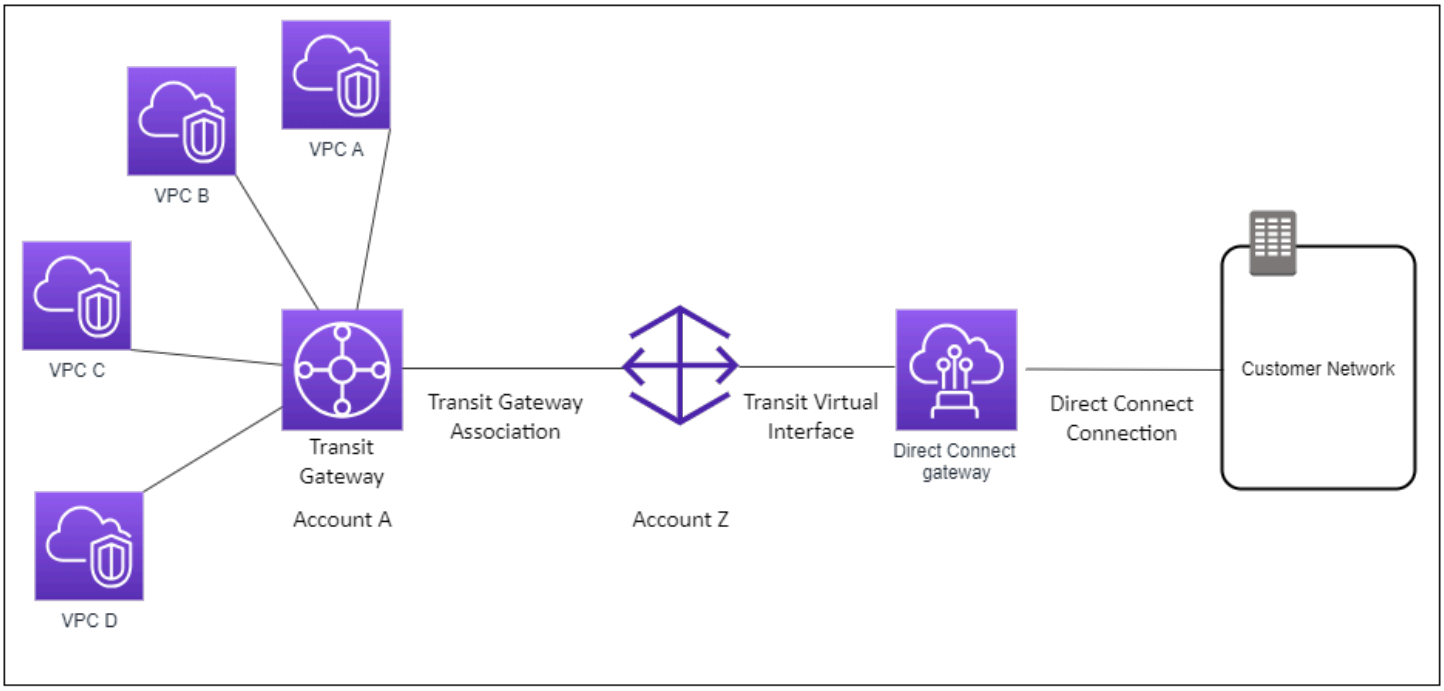
- Verwaltet eine einzelne Verbindung für mehrere Verbindungen VPCs oder Verbindungen VPNs , die sich in derselben Region befinden.
- Kündigen Sie Präfixe von lokal zu AWS und von zu lokal AWS an.

Weitere Informationen zur Konfiguration von Transit Gateways finden Sie unter Arbeiten mit Transit Gateways im Handbuch zu Transit Gateways von Amazon VPC.

Szenario: Kontenübergreifende Transit-Gateway-Verknüpfungen

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, kann das VPCs an das Transit-Gateway angeschlossene Gateway den Verkehr 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.



Ein AWS Direct Connect Gateway erstellen

Sie können ein Direct Connect-Gateway in jeder unterstützten Region entweder über die AWS Direct Connect Konsole, die Befehlszeile oder die API 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.

> **Note**
>
> Wenn Sie ein Direct Connect-Gateway für die Verwendung mit einem AWS Cloud-WAN-Kernnetzwerk erstellen möchten. Die ASN darf sich nicht im gleichen Bereich wie die ASN des Kernnetzwerks befinden.

So erstellen Sie ein Direct Connect-Gateway über die Befehlszeile oder API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(API)AWS Direct Connect

Migrieren Sie von einem virtuellen privaten Gateway zu einem AWS Direct Connect Gateway

Sie können ein virtuelles privates Gateway, das an eine virtuelle Schnittstelle angeschlossen ist, auf ein Direct Connect-Gateway migrieren.

Wenn Sie Direct Connect verwenden und VPCs dabei derzeit eine übergeordnete Availability Zone umgehen, können Sie Ihre Direct Connect-Verbindungen oder virtuellen Schnittstellen nicht migrieren.

In den folgenden Schritten werden die Schritte beschrieben, die Sie ausführen müssen, um ein Virtual Private Gateway auf ein Direct Connect Gateway zu migrieren.

So migrieren Sie zu einem Direct Connect-Gateway

1. Erstellen Sie ein Direct Connect-Gateway.

   Wenn das Direct Connect-Gateway noch nicht existiert, müssen Sie es erstellen. Die Schritte zum Erstellen eines Direct Connect-Gateways finden Sie unterErstellen Sie ein Direct Connect-Gateway.
2. Erstellen Sie eine virtuelle Schnittstelle für das Direct Connect-Gateway.

Für die Migration ist eine virtuelle Schnittstelle erforderlich. Wenn die Schnittstelle nicht existiert, müssen Sie sie erstellen. Die Schritte zum Erstellen der virtuellen Schnittstelle finden Sie unterVirtuelle Schnittstellen.

3. Verknüpfen Sie jedes Virtual Private Gateway mit dem Direct Connect-Gateway.

   Sowohl das Direct Connect-Gateway als auch ein Virtual Private Gateway müssen verknüpft werden. Die Schritte zum Erstellen der Zuordnung finden Sie unterOrdnen Sie virtuelle private Gateways zu oder trennen Sie die Zuordnung.

4. Löschen Sie die virtuelle Schnittstelle, die dem Virtual Private Gateway zugeordnet war. Weitere Informationen finden Sie unter Löschen Sie eine virtuelle Schnittstelle.

Ein AWS Direct Connect Gateway löschen

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. Nachdem Sie alle zugehörigen virtuellen privaten Gateways getrennt und alle angeschlossenen privaten virtuellen Schnittstellen gelöscht haben, können Sie das Direct Connect-Gateway entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder die API löschen.

- Die Schritte zum Trennen der Zuordnung eines virtuellen privaten Gateways finden Sie unter. Ordnen Sie virtuelle private Gateways zu oder trennen Sie die Zuordnung
- Die Schritte zum Löschen einer virtuellen Schnittstelle finden Sie unter. Löschen Sie eine virtuelle Schnittstelle

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(API)AWS Direct Connect

AWS Direct Connect virtuelle private Gateway-Verknüpfungen

Sie können ein AWS Direct Connect Gateway verwenden, um Ihre AWS Direct Connect Verbindung über eine private virtuelle Schnittstelle mit einem oder mehreren VPCs Konten zu verbinden, die sich in derselben oder verschiedenen Regionen befinden. 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 Direct Connect-Kontingente.
- Sie können ein Direct-Connect-Gateway an ein Virtual Private Gateway anfügen, wenn das Direct-Connect-Gateway bereits einem Transit Gateway zugeordnet ist.
- Das, VPCs zu dem Sie über ein Direct Connect-Gateway eine Verbindung herstellen, darf keine überlappenden CIDR-Blöcke haben. Wenn Sie einer VPC, die einem Direct Connect-Gateway zugeordnet ist, einen IPv4 CIDR-Block hinzufügen, stellen Sie sicher, dass sich der CIDR-Block nicht mit einem vorhandenen CIDR-Block für eine andere zugeordnete VPC überschneidet. Weitere Informationen finden Sie unter Hinzufügen von IPv4 CIDR-Blöcken zu einer VPC im 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:
  - Direkte Kommunikation zwischen VPCs denen, die einem einzigen Direct Connect-Gateway zugeordnet 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.
- 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. Das Direct Connect-Gateway kündigt alle Verbindungen an, die VPCs über die ihm zugewiesene ASN verbunden sind.

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 Virtuelle Schnittstellen und gehostete virtuelle Schnittstellen.

Themen

- Erstellen Sie ein AWS Direct Connect virtuelles privates Gateway

- AWS Direct Connect Virtuelle private Gateways zuordnen oder trennen
- Erstellen Sie eine private virtuelle Schnittstelle zum AWS Direct Connect Gateway
- Kontenübergreifend ein AWS Direct Connect virtuelles privates Gateway zuordnen

Erstellen Sie ein AWS Direct Connect virtuelles privates Gateway

Das Virtual Private Gateway muss der VPC angefügt sein, mit der eine Verbindung hergestellt werden soll. Sie können ein Virtual Private Gateway erstellen und es entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API an eine VPC anhängen.

> **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. Das Direct Connect-Gateway kündigt alle Verbindungen an, die VPCs über die ihm zugewiesene ASN verbunden sind.

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 v2/home. https://console.aws.amazon.com/directconnect/
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 Query 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 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

AWS Direct Connect Virtuelle private Gateways zuordnen oder trennen

Sie können ein Virtual Private Gateway und ein Direct Connect Gateway entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API zuordnen oder trennen. 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 Details anzeigen 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 v2/home. https://console.aws.amazon.com/directconnect/
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) und anschließend das Direct Connect-Gateway aus.
3. Wählen Sie die Option Details anzeigen 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-Assoziation ()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 Sie eine private virtuelle Schnittstelle zum AWS 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. Sie können eine private virtuelle Schnittstelle entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API erstellen.

> **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 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 Systemnummer 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

[IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

- Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
- Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

> **Important**
>
> Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point
>
> - Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
> - Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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-Anlagen ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Kontenübergreifend ein AWS Direct Connect virtuelles privates Gateway zuordnen

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 dient als Filter, mit dem dasselbe CIDRs oder ein kleineres CIDRs Präfix am Direct Connect-Gateway angekündigt werden kann. 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 Interaktionen zulässiger Präfixe.

AWS Direct Connect Gateways und Transit-Gateway-Verknüpfungen

Sie können AWS Direct Connect das Gateway verwenden, um Ihre Direct Connect-Verbindung über eine virtuelle Transitschnittstelle mit den VPCs oder zu verbinden VPNs , die an Ihr Transit-Gateway angeschlossen 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 Direct Connect-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 ASNs für jedes Transit-Gateway eine eindeutige Option.

- Jede point-to-point Verbindungsadresse, die einen `/30` Bereich verwendet, z. B., `192.168.0.0/30` wird nicht an ein Transit-Gateway weitergegeben.

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 AWS Transit-Gateway weiterzuleiten, auch wenn die VPCs an das Transit-Gateway angeschlossenen Verbindungen keine Zuweisung CIDRs haben. 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 darüber, wie zulässige Präfixe mit Transit-Gateways und virtuellen privaten Gateways interagieren, finden Sie unter. Interaktionen zulässiger Präfixe

Themen

- Zuordnen oder Aufheben der Verbindung zu AWS Direct Connect einem Transit-Gateway
- Erstellen Sie eine virtuelle Transitschnittstelle zum AWS Direct Connect Gateway
- Erstellen Sie ein Transit-Gateway und einen AWS Direct Connect Assoziationsvorschlag
- Einen Transit-Gateway- und AWS Direct Connect Assoziationsvorschlag annehmen oder ablehnen
- Aktualisieren Sie die zulässigen Präfixe für ein Transit-Gateway und AWS Direct Connect eine Zuordnung
- Löschen eines Transit-Gateways und eines AWS Direct Connect Assoziationsvorschlags

Zuordnen oder Aufheben der Verbindung zu AWS Direct Connect einem Transit-Gateway

Ordnen Sie ein Transit-Gateway entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder die API zu oder trennen Sie die Zuordnung.

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 Details anzeigen 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 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 v2/home. https://console.aws.amazon.com/directconnect/
2. Wählen Sie im Navigationsbereich Direct Connect gateways (Direct Connect-Gateways) und anschließend das Direct Connect-Gateway aus.
3. Wählen Sie die Option Details anzeigen 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 v2/home. https://console.aws.amazon.com/directconnect/
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, für das Sie zulässige Präfixe ändern möchten, und klicken Sie dann auf Bearbeiten.
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 der Amazon VPC CIDRs für alle virtuellen privaten Gateways übereinstimmen. Weitere Informationen zu zulässigen Präfixen finden Sie unter 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). Dieser Vorgang kann mehrere Minuten oder länger dauern.

So erstellen Sie ein Transit Gateway über die Befehlszeile oder die API

- create-direct-connect-gateway-Assoziation ()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 Sie eine virtuelle Transitschnittstelle zum AWS 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. Sie können entweder die AWS Direct Connect Konsole oder die Befehlszeile oder API verwenden.

> **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 Systemnummer 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. Gehen Sie wie folgt vor, um ein IPv4 BGP oder einen IPv6 Peer zu konfigurieren:

      [IPv4] Um einen IPv4 BGP-Peer zu konfigurieren, wählen Sie einen der folgenden IPv4Schritte aus und führen Sie ihn aus:

      - Um diese IP-Adressen selbst anzugeben, geben Sie für Ihre Router-Peer-IP die IPv4 CIDR-Zieladresse ein, an die Amazon Traffic senden soll.
      - Geben Sie für die Peer-IP des Amazon-Routers die IPv4 CIDR-Adresse ein, an die der Datenverkehr gesendet werden soll AWS.

      > **Important**
      >
      > Bei der Konfiguration virtueller AWS Direct Connect-Schnittstellen können Sie Ihre eigenen IP-Adressen mithilfe von RFC 1918 angeben, andere Adressierungsschemata verwenden oder sich für AWS zugewiesene IPv4 /29 CIDR-Adressen entscheiden, die aus dem RFC 3927 IPv4 169.254.0.0/16 Link-Local-Bereich für die Konnektivität zugewiesen wurden. point-to-point Diese point-to-point Verbindungen sollten ausschließlich für das eBGP-Peering zwischen Ihrem Kunden-Gateway-Router und dem Direct Connect-Endpunkt verwendet werden. Für VPC-Verkehr oder Tunneling-Zwecke, wie AWS Site-to-Site Private IP VPN oder Transit Gateway Connect, AWS empfiehlt es sich, anstelle der Verbindungen eine

Loopback- oder LAN-Schnittstelle auf Ihrem Kunden-Gateway-Router als Quell- oder Zieladresse zu verwenden. point-to-point

- Weitere Informationen zu RFC 1918 finden Sie unter Adresszuweisung für private Internets.
- Weitere Informationen zu RFC 3927 finden Sie unter Dynamische Konfiguration von Link-Local-Adressen. IPv4

[IPv6] Um einen IPv6 BGP-Peer zu konfigurieren, wählen Sie. IPv6 Die IPv6 Peer-Adressen werden automatisch aus dem Adresspool von IPv6 Amazon 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-Anlagen ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Erstellen Sie ein Transit-Gateway und einen AWS Direct Connect Assoziationsvorschlag

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. Sie können einen Zuordnungsvorschlag entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API erstellen.

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 Details anzeigen 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-assoziationsvorschlag ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Einen Transit-Gateway- und AWS Direct Connect Assoziationsvorschlag annehmen oder ablehnen

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. Sie können den Zuordnungsvorschlag entweder über die AWS Direct Connect Konsole, über die Befehlszeile oder die API annehmen oder 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 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 v2/home. https://console.aws.amazon.com/directconnect/
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-assoziationsvorschläge ()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 Sie die zulässigen Präfixe für ein Transit-Gateway und AWS Direct Connect eine Zuordnung

Sie können die Präfixe, die vom Transit-Gateway über das Direct Connect-Gateway zulässig sind, entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API aktualisieren. Um die zulässigen Präfixe für ein Transit-Gateway und eine Direct Connect-Verknüpfung mithilfe der AWS Direct Connect Konsole zu aktualisieren,

- Wenn Sie der Besitzer des Transit-Gateways sind, müssen Sie einen neuen Zuordnungsvorschlag für dieses Direct Connect-Gateway erstellen und die zulässigen Präfixe angeben. Die Schritte zum Erstellen eines neuen Zuordnungsvorschlags finden Sie unterErstellen Sie einen Vorschlag für die Zuordnung eines Transit-Gateways.
- Wenn Sie der Besitzer des Direct Connect-Gateways sind, können Sie die zulässigen Präfixe aktualisieren, wenn Sie den Zuordnungsvorschlag akzeptieren, oder wenn Sie die zulässigen Präfixe für eine bestehende Zuordnung aktualisieren. Die Schritte zum Aktualisieren der zulässigen Präfixe, wenn Sie die Zuordnung akzeptieren, finden Sie unter. Akzeptieren oder lehnen Sie einen Vorschlag zur Verknüpfung eines Transit-Gateways ab

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-Gateways und eines AWS Direct Connect Assoziationsvorschlags

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 Erstellen Sie einen Vorschlag für die Zuordnung eines Transit-Gateways.

Sie können ein Transit-Gateway und einen Direct Connect-Zuordnungsvorschlag entweder über die AWS Direct Connect Konsole oder über die Befehlszeile oder API löschen.

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 Details anzeigen 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-assoziationsvorschlag ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

AWS Direct Connect Gateway- und AWS Cloud-WAN-Kernnetzwerkzuordnungen

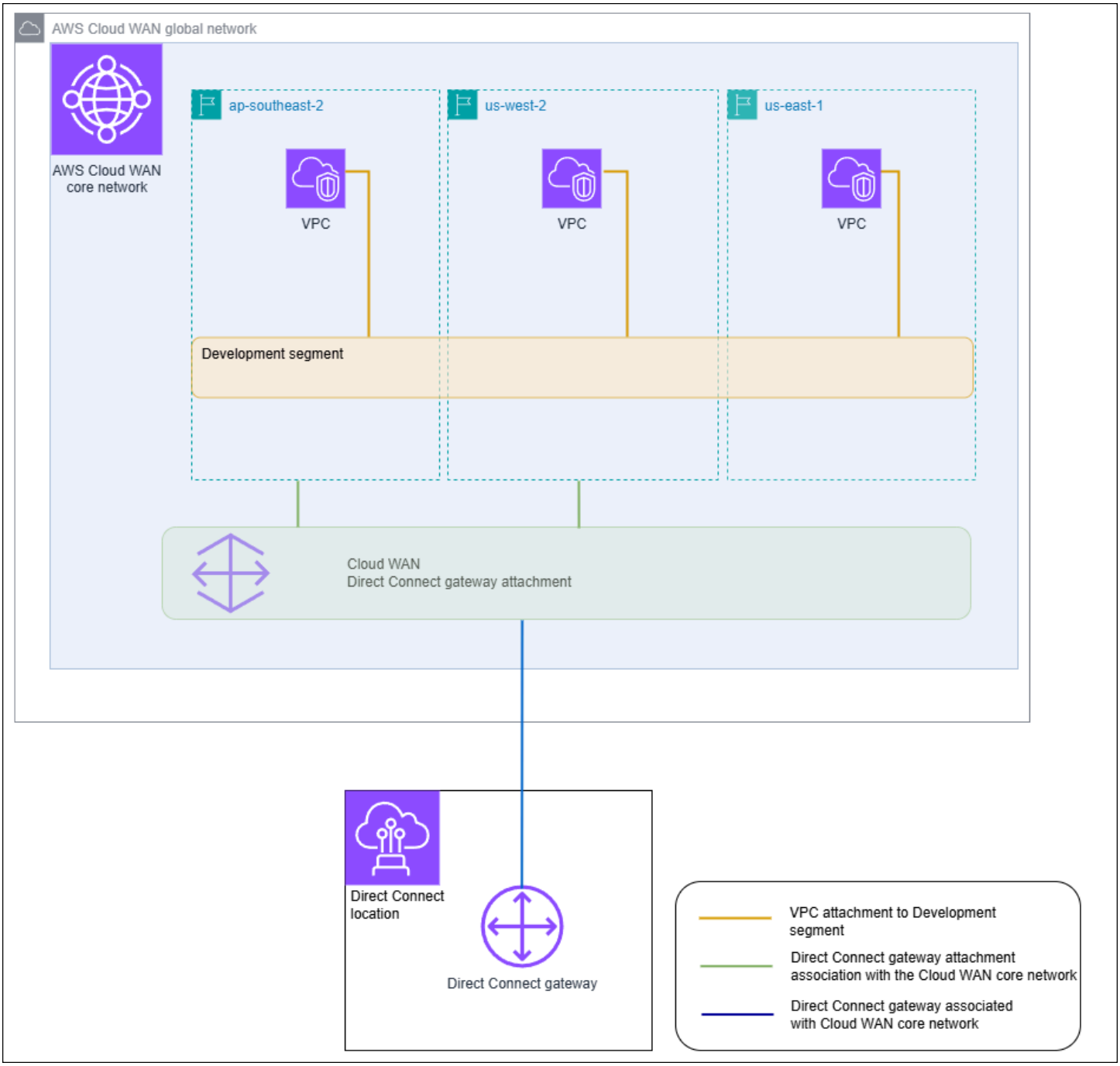
Ordnen Sie mithilfe eines Direct Connect-Anhangstyps in AWS Cloud WAN ein AWS Direct Connect Gateway einem Cloud-WAN-Kernnetzwerk zu. Diese direkte Verbindung leitet den Verkehr zwischen den ausgewählten Edge-Standorten Ihres Kernnetzwerks und Ihren Direct Connect-Verbindungen über den kürzesten verfügbaren Pfad weiter.

Der Direct Connect-Gateway-Anhangstyp unterstützt BGP (Border Gateway Protocol) für die automatische Weitergabe von Routing-Informationen zwischen Ihrem Kernnetzwerk und lokalen Standorten. Der Direct Connect-Anhang unterstützt auch die standardmäßigen Cloud-WAN-Funktionen wie zentrales richtlinienbasiertes Management, Tag-basierte Automatisierung von Anhängen und Segmentierung für erweiterte Sicherheitskonfigurationen.

> **Note**
>
> Die Zuordnung zwischen einem Kernnetzwerk und einem Direct Connect-Gateway wird über die Cloud WAN-Konsole im Network Manager erstellt, gelöscht und verwaltet. Wenn Sie ein Direct Connect-Gateway mit Cloud WAN verwenden, spiegeln die Direct Connect-Konsole APIs und die CLI die Zuordnung wider, können jedoch nicht verwendet werden, um sie zu ändern. Sie können jedoch die Direct Connect-API oder die Befehlszeile verwenden, um zu überprüfen, ob eine Zuordnung erstellt wurde.

Das folgende Beispiel zeigt ein globales Cloud-WAN-Netzwerk mit drei Regionen innerhalb des Cloud-WAN-Kernnetzwerks. Jede Region verfügt über eine eigene VPC, die mit einem

Kernnetzentwicklungssegment verbunden ist, das von diesen drei Regionen gemeinsam genutzt wird. Mithilfe von Cloud WAN wird ein Direct Connect-Gateway-Anhang innerhalb von Cloud WAN mithilfe eines Direct Connect-Gateways erstellt, das mit Direct Connect erstellt wurde. Der Anhang ist zwei der drei Regionen, ap-Southeast-2 und us-west-2, zugeordnet und hat Zugriff auf das Development-Segment. Obwohl us-east-1 dasselbe Development-Segment nutzt, wird der Direct Connect-Gateway-Anhang nicht mit dieser Region geteilt und ist daher nicht verfügbar.



Themen

- Voraussetzungen
- Überlegungen
- Direct Connect-Gateway-Zuordnungen zu einem Cloud-WAN-Kernnetzwerk
- Überprüfen Sie eine AWS Direct Connect Gateway-Zuordnung zu einem AWS Cloud-WAN-Kernnetzwerk

Voraussetzungen

Für eine Direct Connect-Gateway-Zuordnung zu einem Cloud-WAN-Kernnetzwerk ist Folgendes erforderlich:

- Ein vorhandenes Direct Connect-Gateway. Die Schritte zum Erstellen eines Direct Connect-Gateways finden Sie unterErstellen Sie ein Direct Connect-Gateway.
- Ein AWS Cloud-WAN-Kernnetzwerk. Informationen zu Cloud WAN finden Sie im AWS Cloud WAN-Benutzerhandbuch.

Überlegungen

Die folgenden Grenzwerte gelten für Direct Connect-Gateway-Verknüpfungen mit einem Cloud WAN-Kernnetzwerk:

- Ein Direct Connect-Gateway kann einem einzelnen Cloud-WAN-Kernnetzwerk und einem einzelnen Segment dieses Kernnetzwerks zugeordnet werden. Sobald eine Zuordnung erstellt wurde, kann dieses Gateway nicht mit anderen Ressourcen in AWS Regionen verknüpft werden. Wenn Sie das Gateway vom Kernnetzwerk trennen, können Sie dieses Gateway für andere Zuordnungstypen verwenden.
- Der Cloud WAN Direct Connect-Gateway-Anhang verwendet den virtuellen Transit-Schnittstellentyp für die Konnektivität.
- Der Cloud-WAN-Anhang unterstützt keine Listen mit zulässigen Präfixen. Alle Präfixe in einem Kernnetzwerksegment werden dem Direct Connect-Gateway bekannt gegeben, das diesem Segment zugeordnet ist.
- Das Kontingent für die maximale Anzahl von Präfixen, die lokal oder AWS über eine virtuelle Transitschnittstelle angekündigt werden können, unterscheidet sich von dem Kontingent für Präfixe, die von einem Cloud-WAN-Kernnetzwerk zu einem lokalen Netzwerk angekündigt

werden. Kontingente für andere Direct Connect-Ressourcen, die mit einer Cloud-WAN-Verbindung verwendet werden, gelten ebenfalls. Siehe Direct Connect-Kontingente.

- Das AS-PATH BGP-Attribut wird im gesamten Kernnetzwerk, im Direct Connect-Gateway und in der virtuellen Schnittstelle beibehalten.
- Die ASN eines Direct Connect-Gateways muss außerhalb des für das Cloud WAN-Kernnetzwerk konfigurierten ASN-Bereichs liegen. Wenn Sie beispielsweise einen ASN-Bereich von 64512 — 65534 für das Kernnetzwerk haben, muss die ASN des Direct Connect-Gateways eine ASN außerhalb dieses Bereichs verwenden.
- Cloud WAN unterstützt möglicherweise keine bestimmten Anhangstypen, die den Direct Connect-Anhangstyp für den Transport verwenden. Weitere Informationen zu Direct Connect-Gateway-Anhängen an ein Cloud WAN-Kernnetzwerk finden Sie unter Direct Connect-Gateway-Anlagen in AWS Cloud WAN im AWS Cloud WAN-Benutzerhandbuch.
- CloudWatch Network Monitor unterstützt Metriken für Latenz und Paketverlust, wenn es mit einem Cloud WAN Direct Connect-Gateway-Anhangstyp verwendet wird. Die Funktion Network Health Indicator wird nicht unterstützt. Weitere Informationen finden Sie im Amazon CloudWatch Benutzerhandbuch unter Verwenden von Amazon CloudWatch Network Monitor.

Direct Connect-Gateway-Zuordnungen zu einem Cloud-WAN-Kernnetzwerk

Die Zuordnung eines Direct Connect-Gateways zu einem AWS Cloud-WAN-Kernnetzwerk erfolgt entweder über die AWS Cloud-WAN-Konsole oder das Cloud-WAN APIs oder die Befehlszeile.

Um ein vorhandenes Direct Connect-Gateway einem Cloud WAN-Kernnetzwerk zuzuordnen, erstellen Sie einen neuen Direct Connect-Anhang in der Cloud WAN Console. Nachdem der Direct Connect-Anhang erstellt wurde, wird die Verbindung hergestellt. Standardmäßig können Sie bei der Erstellung der Zuordnung die Standardeinstellung so wählen, dass alle Edge-Standorte des Kernnetzwerks in das gewählte Kernnetzsegment aufgenommen werden. Alternativ können Sie einzelne Kantenstandorte angeben.

Weitere Informationen zu Direct Connect-Gateway-Anhängen an ein Cloud WAN-Kernnetzwerk finden Sie unter Direct Connect-Gateway-Anlagen in AWS Cloud WAN im AWS Cloud WAN-Benutzerhandbuch.

Überprüfen Sie eine AWS Direct Connect Gateway-Zuordnung zu einem AWS Cloud-WAN-Kernnetzwerk

Sie können die Zuordnung eines Direct Connect-Gateways zu einem Cloud-WAN-Kernnetzwerk mithilfe der Direct Connect-Konsole, der Direct Connect-API oder der Befehlszeile überprüfen.

So überprüfen Sie mithilfe der Konsole eine Direct Connect-Gateway-Zuordnung zu einem Cloud WAN-Kernnetzwerk

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 den Direct Connect-Gateway-Anhang aus, für den Sie die Zuordnung anzeigen möchten.
4. Wählen Sie die Registerkarte Gateway assocations (Gateway-Zuordnungen) aus.
   - In der ID-Spalte wird die Kernnetzwerk-ID angezeigt, der das Direct Connect-Gateway zugeordnet ist.
   - In der Spalte Status wird „Zugeordnet“ angezeigt.
   - In der Spalte Zuordnungstyp wird Cloud WAN Core Network angezeigt.

So überprüfen Sie die Zuordnung eines Direct Connect-Gateways zu einem Cloud WAN-Kernnetzwerk mithilfe der Befehlszeile oder API

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

Zulässige Präfixe, Interaktionen für Gateways AWS Direct Connect

Hier erfahren Sie, wie zulässige Präfixe mit Transit Gateways und Virtual Private Gateways interagieren. Weitere Informationen finden Sie unter Routing policies and BGP communities.

Virtual Private Gateway-Zuordnungen

Die Präfixliste (IPv4 und IPv6) dient als Filter, mit dem dasselbe CIDRs oder ein kleinerer Bereich von Präfixen CIDRs für das Direct Connect-Gateway angekündigt werden kann. 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 die Änderung eines vorhandenen Präfixes kann nur der Verkehr verzögert oder unterbrochen 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 lokalen Datenverkehr zu oder von einem Direct Connect-Gateway zum Transit-Gateway weiter, auch wenn die VPCs an das Transit-Gateway angeschlossenen Gateways keine Zuweisung CIDRs haben. 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 virtuellen privaten Gateways dienen die eingegebenen zulässigen Präfixe als Filter, um dieselben oder kleinere Präfixe zuzulassen. CIDRs

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 einem Direct Connect-Gateway zugeordnet 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.

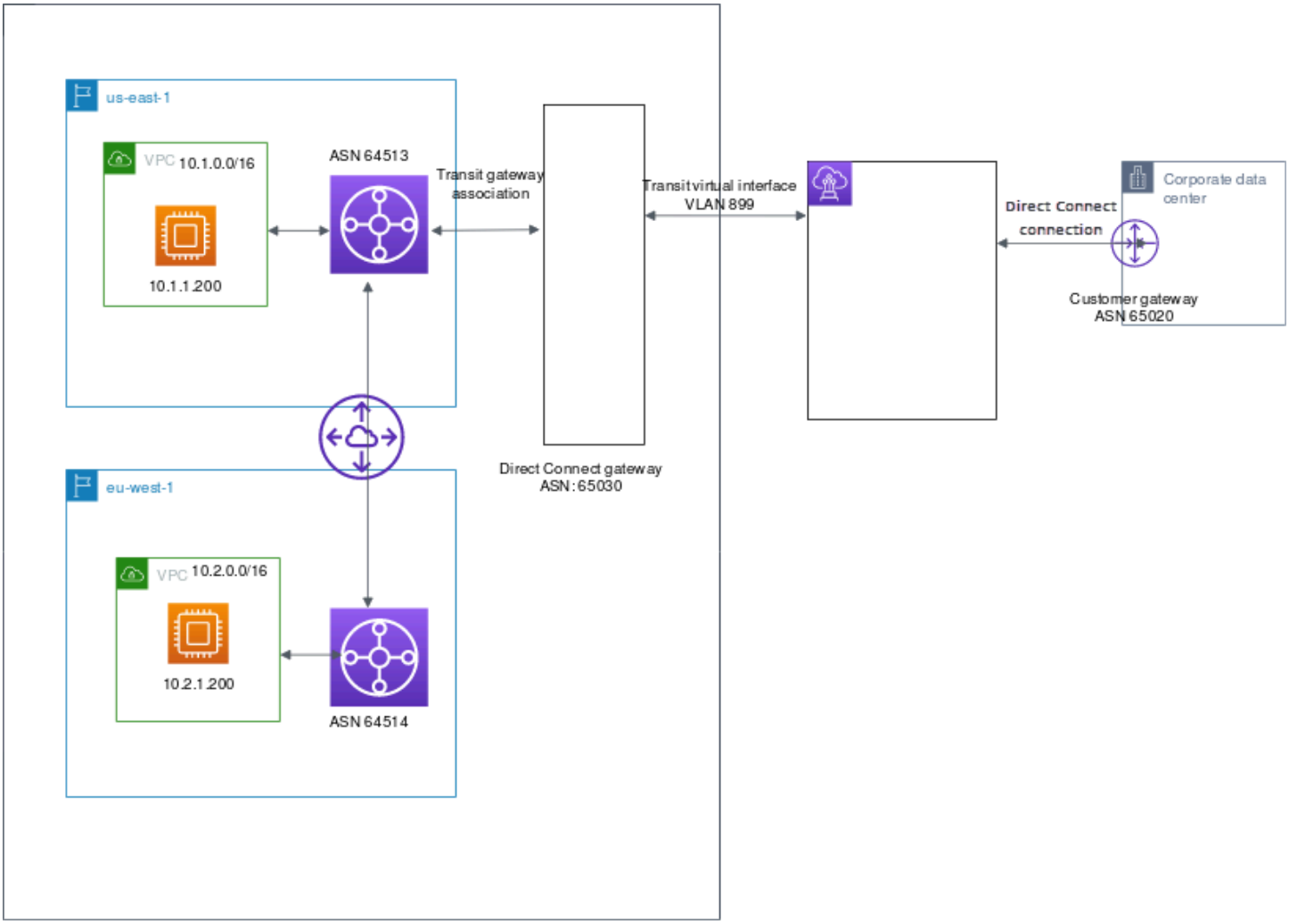
Wenn Sie ein zulässiges Präfix entfernen oder hinzufügen, wird der Datenverkehr, der dieses Präfix nicht verwendet, nicht beeinträchtigt. Bei Aktualisierungen ändert sich der Status von `associated` zu `updating`. Wenn Sie ein vorhandenes Präfix ändern, kann dies nur den Datenverkehr verzögern oder unterbrechen, der dieses Präfix verwendet.

Beispiel: Zulässig für Präfixe in einer Transit-Gateway-Konfiguration

Stellen Sie sich die Konfiguration vor, in der Sie Instanzen 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 Erstellen Sie ein Direct Connect-Gateway.

- Virtuelle Transit-Schnittstelle: Stellen Sie das VLAN auf 899 und die ASN auf 65020 ein. Weitere Informationen finden Sie unter 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 Ordnen Sie Direct Connect ein Transit-Gateway zu oder trennen Sie die Verknüpfung..
- 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.

AWS Direct Connect Ressourcen taggen

Ein Tag ist eine Bezeichnung, die ein Ressourcenbesitzer seinen AWS Direct Connect Ressourcen zuweist. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Mithilfe von Tags kann der Ressourcenbesitzer 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.

Sie haben beispielsweise zwei AWS Direct Connect Verbindungen in einer Region, die sich jeweils an unterschiedlichen Standorten befinden. 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. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen. Tags haben keine semantische Bedeutung AWS Direct Connect und werden ausschließlich als Zeichenfolge 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 mit der AWS Direct Connect Konsole, der AWS Direct Connect API, dem AWS CLI AWS Tools for Windows PowerShell, dem oder einem AWS SDK taggen. Wenn Sie die diese Tools für die Verwaltung von Tags verwenden, müssen Sie den Amazon-Ressourcennamen (ARN) für die Ressource angeben. Weitere Informationen zu finden Sie ARNs unter Amazon Resource Names (ARNs) in der 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	Ja	Ja	Ja	Nein

Tag-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 `aws:` Präfix ist für die AWS Verwendung 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.
- Tags zur Kostenzuweisung werden nur für Verbindungen, Verbindungen und LAGs unterstützt. Informationen zur Verwendung von Tags im Rahmen des Kostenmanagements finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Fakturierung und Kostenmanagement 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 überschreiben 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

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, 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, die für gelten AWS Direct Connect, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. 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 gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Direct Connect. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Direct Connect , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Direct Connect Ressourcen unterstützen.

Themen

- Datenschutz in AWS Direct Connect
- Identity and Access Management für Direct Connect
- Einloggen und Überwachen AWS Direct Connect
- Konformitätsvalidierung für AWS Direct Connect
- Resilienz in AWS Direct Connect
- Infrastruktursicherheit in AWS Direct Connect

Datenschutz in AWS Direct Connect

Das AWS Modell der gilt für den Datenschutz in AWS Direct Connect. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. 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, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. 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, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen 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 AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 mit der Konsole, der AWS Direct Connect API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs 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
- Verschlüsselung in der AWS Direct ConnectÜbertragung

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 Sicherheit der Infrastruktur.
- Eine Assoziation zu VPCs. Weitere Informationen erhalten Sie unter Virtual Private Gateway-Zuordnungen und Transit-Gateway-Zuordnungen.

Verkehr zwischen AWS Ressourcen in derselben Region

Sie haben zwei Konnektivitätsoptionen:

- Eine Zuordnung zu einer AWS Site-to-Site VPN. Weitere Informationen finden Sie unter Sicherheit der Infrastruktur.
- Eine Assoziation zu VPCs. Weitere Informationen erhalten Sie unter Virtual Private Gateway-Zuordnungen und Transit-Gateway-Zuordnungen.

Verschlüsselung in der AWS Direct ConnectÜbertragung

AWS Direct Connect verschlüsselt Ihren Datenverkehr, der übertragen wird, standardmäßig nicht. 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 EC2 Amazon-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 Amazon VPC-to-Amazon VPC-Konnektivitätsoptionen.

MAC Security (MACsec) ist ein IEEE-Standard, der Datenvertraulichkeit, Datenintegrität und Authentizität der Datenherkunft gewährleistet. Sie können AWS Direct Connect Verbindungen verwenden, die MACsec die Verschlüsselung Ihrer Daten von Ihrem Unternehmensrechenzentrum zum AWS Direct Connect Standort unterstützen. Weitere Informationen finden Sie unter MAC-Sicherheit (MACsec).

Identity and Access Management für Direct Connect

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzend) ist, um Direct-Connect-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Funktionsweise von Direct Connect mit IAM
- Beispiele für identitätsbasierte Richtlinien für Direct Connect
- Serviceverknüpfte Rollen für AWS Direct Connect
- AWS verwaltete Richtlinien für AWS Direct Connect
- Fehlerbehebung für Direct-Connect-Identität und -Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Direct Connect ausführen.

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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern 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. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer 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 und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen

Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, 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 sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem

beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, 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 in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management

Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. 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 aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen

mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 Rolleninformationen von der AWS Management Console AWS CLI, der oder der 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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen

zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

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-Feature	Unterstützung von Direct Connect
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein

IAM-Feature	Unterstützung von Direct Connect
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Direct Connect und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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 unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienmaßnahmen für Direct Connect

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang 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": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Richtlinienressourcen für Direct Connect

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Eigenschaften ARNs finden Sie unter Von Direct Connect definierte Ressourcen 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 angeben, wer auf was Zugriff hat. 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, AWS wertet die Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen 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

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten 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 an viele AWS Ressourcen anhängen. 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 Bedingung `aws:TagKeys` 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 Definieren von Berechtigungen mit ABAC-Autorisierung 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 funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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 von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu 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 verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. 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 aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte 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 mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Direct Connect definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Direct Connect in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Aktionen, Ressourcen und Bedingungen für Direct Connect
- Verwenden der Direct-Connect-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Schreibgeschützter Zugriff auf AWS Direct Connect
- Vollzugriff auf AWS Direct Connect
- Beispiele für identitätsbasierte Direct-Connect-Richtlinien mit tagbasierten Bedingungen

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 verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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 mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, 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 Sicherer API-Zugriff mit MFA 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang 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 beispielsweise jemandem die Erlaubnis zu erteilen, eine EC2 Amazon-Instance mit dem EC2 `DescribeVpnGateways` Amazon-API-Vorgang auszuführen, nehmen Sie die `ec2:DescribeVpnGateways` Aktion in seine Richtlinie auf. 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 gewährt Lesezugriff auf AWS Direct Connect.

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

Die folgende Beispielrichtlinie gewährt vollen 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Folgendes ARNs:

Direct Connect-Ressource 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 Resource Names (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 Eigenschaften finden Sie unter Ressourcentypen ARNs, die von definiert wurden AWS Direct Connect im IAM-Benutzerhandbuch. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Direct Connect definierte Aktionen.

Wenn ein Ressourcen-ARN oder ein anderes Ressourcen-ARN-Muster als im `Resource` Feld der IAM-Richtlinienanweisung für DescribeConnections,, DescribeVirtualInterfaces, oder angegeben * ist DescribeDirectConnectGateways DescribeInterconnects, tritt der angegebene Wert nicht auf DescribeLags, es sei denn, die entsprechende Ressourcen-ID `Effect` wird auch im API-Aufruf übergeben. Wenn Sie jedoch die Ressource anstelle einer bestimmten Ressourcen-ID in der IAM-Richtlinienanweisung angeben*, funktioniert die angegebene`Effect`.

Im folgenden Beispiel sind keine der angegebenen Optionen `Effect` erfolgreich, wenn die `DescribeConnections` Aktion aufgerufen wird, ohne dass die Anforderung `connectionId` übergeben wurde.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

Im folgenden Beispiel ist die `DescribeConnections` Aktion jedoch erfolgreich, `"Effect": "Allow"` da sie für das `Resource` Feld der IAM-Richtlinienanweisung angegeben * wurde, unabhängig davon, ob die in der Anforderung angegeben `connectionId` wurde.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

Bedingungsschlüssel

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. 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, AWS wertet die Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Direct Connect definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale 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 Von Direct Connect definierte Aktionen.

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 es Ihnen ermöglichen, Details zu den Direct Connect-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. 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 weiterhin die Direct Connect-Konsole verwenden können, fügen Sie den Entitäten außerdem die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch:

```
directconnect
```

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Schreibgeschützter Zugriff auf AWS Direct Connect

Die folgende Beispielrichtlinie gewährt 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 gewährt vollen 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-Schlüssel-Wert-Paare in einer Anfrage übergeben werden können, die eine Ressource kennzeichnet. AWS Das folgende Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, mit der die AWS Direct Connect TagResource Aktion nur dann Tags an eine virtuelle Schnittstelle angehängt werden kann, wenn das Tag den Umgebungsschlüssel und die Preprod- oder Production-Werte 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 AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Direct Connect Mit Diensten verknüpfte Rollen sind vordefiniert AWS Direct Connect und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Direct Connect erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Direct Connect definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Direct Connect kann, sofern nicht anders definiert, nur ihre 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. Dadurch werden Ihre AWS Direct Connect Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpften 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 serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Direct Connect

AWS Direct Connect verwendet eine dienstverknüpfte Rolle mit dem Namen. `AWSServiceRoleForDirectConnect` Auf diese Weise können AWS Direct Connect Sie das in AWS Secrets Manager Ihrem Namen gespeicherte MACSec Geheimnis 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 serviceverknüpfte 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 eine serviceverknüpfte Rolle nicht manuell erstellen. AWS Direct Connect erstellt die serviceverknüpfte Rolle für Sie. Wenn Sie den `associate-mac-sec-key` Befehl ausführen, AWS wird eine dienstbezogene Rolle erstellt, mit der Sie die MACsec Geheimnisse abrufen können AWS Direct Connect , die in AWS Secrets Manager Ihrem Namen in der AWS Management Console 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 Features verwendet. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese dienstverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dieselbe Methode verwenden, um die Rolle in Ihrem Konto neu zu erstellen. AWS Direct Connect erstellt die dienstbezogene Rolle erneut 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 dienstverknüpfte Rolle mit dem `directconnect.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer dienstbezogenen Rolle für AWS Direct Connect

AWS Direct Connect erlaubt es Ihnen nicht, die `AWSServiceRoleForDirectConnect` dienstbezogene Rolle zu bearbeiten. 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 dienstbezogenen Rolle für AWS Direct Connect

Sie müssen die Rolle `AWSServiceRoleForDirectConnect` nicht manuell löschen. Wenn Sie Ihre dienstverknüpfte Rolle löschen, müssen Sie alle zugehörigen Ressourcen löschen, die im AWS Secrets Manager Webdienst gespeichert sind. Die AWS Management Console AWS CLI, die oder die AWS API AWS Direct Connect bereinigt die Ressourcen und löscht die dienstverknüpfte 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 Dienst 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.

Um AWS Direct Connect Ressourcen zu löschen, die verwendet werden von **`AWSServiceRoleForDirectConnect`**

1. Entfernen Sie die Zuordnung zwischen allen MACsec Schlüsseln und Verbindungen. Weitere Informationen finden Sie unter the section called “Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer Verbindung”

2. Löscht die Zuordnung zwischen allen MACsec Schlüsseln und LAGs. Weitere Informationen finden Sie unter the section called “Entfernen Sie die Zuordnung zwischen einem MACsec geheimen Schlüssel und einer LAG”

So löschen Sie die -servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForDirectConnect` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Rollen AWS Direct Connect

AWS Direct Connect unterstützt die Verwendung von dienstbezogenen Rollen in allen Bereichen, in AWS-Regionen denen die MAC-Sicherheitsfunktion verfügbar ist. Weitere Informationen finden Sie unter AWS Direct Connect -Standorte.

AWS verwaltete Richtlinien für AWS Direct Connect

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSDirect ConnectFullAccess

Sie können die `AWSDirectConnectFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die vollen Zugriff auf ermöglichen AWS Direct Connect.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectFullAccess im AWS Management Console.

AWS verwaltete Richtlinie: AWSDirect ConnectReadOnlyAccess

Sie können die `AWSDirectConnectReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff auf ermöglichen. AWS Direct Connect

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectReadOnlyAccess im AWS Management Console.

AWS verwaltete Richtlinie: AWSDirect ConnectServiceRolePolicy

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 “Service-verknüpfte Rollen”.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSDirectConnectServiceRolePolicy im AWS Management Console.

AWS Direct Connect Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien AWS Direct Connect seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst. Abonnieren Sie den RSS-Feed auf der Seite AWS Direct Connect Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSDirectConnectServiceRolePolicy – Neue Richtlinie	Zur Unterstützung von MAC Security wurde die AWSServiceRoleForDirectConnectserviceverknüpfte Rolle hinzugefügt.	31. März 2021
AWS Direct Connect hat begonnen, Änderungen zu verfolgen	AWS Direct Connect hat begonnen, Änderungen an den AWS verwalteten Richtlinien zu verfolgen.	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.
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Direct Connect-Ressourcen ermöglichen

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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. 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 ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Direct Connect-Ressourcen ermöglichen

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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, 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 dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie gehören.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Einloggen und Überwachen AWS Direct Connect

Sie können die folgenden automatisierten Tools zur Überwachung von AWS Direct Connect verwenden und möglicherweise auftretende Probleme melden:

- Amazon CloudWatch Alarms — 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 SNS-Thema gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter Überwachen Sie mit Amazon CloudWatch.
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten und überwachen CloudTrail Sie 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 AWS Direct Connect API-Aufrufe protokollieren mit AWS CloudTrail und Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail Benutzerhandbuch.

Weitere Informationen finden Sie unter Direct Connect-Ressourcen überwachen.

Konformitätsvalidierung für AWS Direct Connect

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services 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:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- 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— Dies AWS-Service bietet 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. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- 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.

Resilienz in AWS Direct Connect

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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 zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Neben der AWS globalen Infrastruktur AWS Direct Connect bietet es mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

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, der Ihnen hilft, dedizierte Verbindungen zu bestellen, 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.

- 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 AWS Direct Connect Toolkit für Resilienz.

Infrastruktursicherheit in AWS Direct Connect

Als verwalteter Dienst AWS Direct Connect wird er durch die AWS globalen Netzwerksicherheitsverfahren geschützt. Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Direct Connect über das Netzwerk. 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 diese API-Operationen von jedem Netzwerkstandort aus aufrufen, AWS Direct Connect unterstützt jedoch ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Grundlage der Quell-IP-Adresse beinhalten können. Sie können auch AWS Direct Connect Richtlinien verwenden, um den Zugriff von bestimmten Amazon Virtual Private Cloud (Amazon VPC) -Endpunkten oder bestimmten zu kontrollieren. VPCs Dadurch wird der Netzwerkzugriff auf eine bestimmte AWS Direct Connect Ressource effektiv nur von der spezifischen VPC innerhalb des AWS Netzwerks isoliert. Für Beispiele vgl. the section called “Beispiele für identitätsbasierte Richtlinien für Direct Connect”.

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 Sie Ihr Netzwerk sicherer vor BGP-Hijacking schützen können, finden Sie unter So tragen Sie zum sicheren AWS Internet-Routing bei.

Verwenden Sie die AWS Direct Connect CLI

Sie können den verwenden AWS CLI , um AWS Direct Connect Ressourcen zu erstellen und mit ihnen zu arbeiten.

Im folgenden Beispiel AWS CLI werden die Befehle verwendet, um eine AWS Direct Connect Verbindung herzustellen. 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
- Schritt 2: Herunterladen des LOA-CFA-Dokuments
- Schritt 3: Erstellen einer virtuellen Schnittstelle und Abrufen der Router-Konfiguration

Schritt 1: Erstellen einer Verbindung

Im ersten Schritt senden Sie eine Verbindungsanforderung. Stellen Sie sicher, dass Sie die benötigte Portgeschwindigkeit und den AWS Direct Connect Standort kennen. Weitere Informationen finden Sie unter Dedizierte und gehostete 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 namens 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

Nachdem Sie eine AWS Direct Connect Verbindung bestellt haben, müssen Sie eine virtuelle Schnittstelle erstellen, um sie verwenden zu können. 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 AWS Diensten herzustellen, die sich nicht in einer VPC befinden. Sie können eine virtuelle Schnittstelle erstellen, die unseren IPv6 Datenverkehr unterstützt IPv4 .

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Voraussetzungen in the section called “Voraussetzungen für virtuelle Schnittstellen” gelesen haben.

Wenn Sie mit dem eine virtuelle Schnittstelle erstellen AWS CLI, enthält die Ausgabe allgemeine Informationen zur Router-Konfiguration. Verwenden Sie die AWS Direct Connect Konsole, um eine Router-Konfiguration zu erstellen, die für Ihr Gerät spezifisch ist. 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 IPv4 den Datenverkehr benötigen Sie private IPv4 Adressen für jedes Ende der BGP-Peering-Sitzung. Sie können Ihre eigenen IPv4 Adressen angeben oder 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 IPv6 Datenverkehr unterstützt, verwenden Sie denselben Befehl wie oben und geben Sie `ipv6` für den `addressFamily` Parameter Folgendes an. Sie können Ihre eigenen IPv6 Adressen für die BGP-Peering-Sitzung nicht angeben. Amazon weist Ihnen Adressen zu. IPv6

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 Datenverkehr müssen Sie außerdem öffentliche IPv4 Adressen für jedes Ende der BGP-Peering-Sitzung sowie öffentliche IPv4 Routen angeben, für die Sie über BGP werben. Im folgenden Beispiel wird eine öffentliche virtuelle Schnittstelle für den Datenverkehr erstellt. IPv4

   ```
   aws directconnect create-public-virtual-interface --
   connection-id dxcon-fg31dyv6 --new-public-virtual-interface
    virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
   {cidr=203.0.113.4/30}]
   ```

   ```
   {
       "virtualInterfaceState": "verifying",
       "asn": 65000,
       "vlan": 2000,
       "customerAddress": "203.0.113.2/30",
       "ownerAccount": "123456789012",
       "connectionId": "dxcon-fg31dyv6",
       "addressFamily": "ipv4",
       "virtualGatewayId": "",
       "virtualInterfaceId": "dxvif-fgh0hcrk",
       "authKey": "asdf34example",
       "routeFilterPrefixes": [
           {
               "cidr": "203.0.113.0/30"
           },
           {
               "cidr": "203.0.113.4/30"
   ```

```
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Um eine öffentliche virtuelle Schnittstelle zu erstellen, die IPv6 Datenverkehr unterstützt, können Sie IPv6 Routen angeben, für die Sie über BGP werben. Sie können keine IPv6 Adressen für die Peering-Sitzung angeben. Amazon weist Ihnen IPv6 Adressen zu. Das folgende Beispiel erstellt eine öffentliche virtuelle Schnittstelle für den Datenverkehr. IPv6

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. 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>
```

AWS Direct Connect API-Aufrufe protokollieren mit AWS CloudTrail

AWS Direct Connect ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS Direct Connect. CloudTrail erfasst alle API-Aufrufe AWS Direct Connect als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Direct Connect Konsole und Codeaufrufen für die AWS Direct Connect API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Direct Connect. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Direct Connect, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS Direct Connect Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn Aktivitäten in auftreten AWS Direct Connect, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Direct Connect, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen

- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Direct Connect Aktionen werden von der AWS Direct Connect API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von `CreateConnection` und `CreatePrivateVirtualInterface` Aktionen 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 Root- oder AWS Identity and Access Management (IAM-Benutzer-) Anmeldeinformationen gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen hierzu finden Sie unter dem CloudTrail-Element `userIdentity`.

AWS Direct Connect Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Im Folgenden finden CloudTrail Sie Beispiele für Protokolldatensätze 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
    },
    ...
  ]
}
```

AWS Direct Connect Ressourcen überwachen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Direct Connect-Ressourcen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen 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 Ausgangsbasis für die normale Direct Connect-Leistung in Ihrer Umgebung festzulegen, indem die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen gemessen wird. 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 einen Basiswert festzulegen, sollten Sie die Nutzung, den Zustand und den Zustand Ihrer physischen Direct Connect-Verbindungen überwachen.

Inhalt

- Überwachungstools
- Überwachen Sie mit Amazon CloudWatch

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 Überwachungstools verwenden, um Direct Connect zu beobachten und zu melden, wenn etwas nicht stimmt:

- Amazon CloudWatch Alarms — 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 SNS-Thema gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Informationen zu den verfügbaren Metriken und Dimensionen finden Sie unter Überwachen Sie mit Amazon CloudWatch.
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten und überwachen CloudTrail Sie 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 -API-Aufrufen und Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail Benutzerhandbuch.

Manuelle Überwachungstools

Ein weiterer wichtiger Teil der AWS Direct Connect Verbindungsüberwachung ist die manuelle Überwachung der Elemente, die von den CloudWatch Alarmen nicht abgedeckt werden. Die Direct Connect- und CloudWatch Konsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand 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 CloudWatch Sie Folgendes verwenden:

- 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.

Überwachen Sie mit Amazon CloudWatch

Sie können physische AWS Direct Connect Verbindungen und virtuelle Schnittstellen überwachen mit CloudWatch. CloudWatch sammelt Rohdaten aus Direct Connect und verarbeitet sie zu lesbaren Metriken. Standardmäßig werden Direct Connect-Metrikdaten in 5-Minuten-Intervallen bereitgestellt. CloudWatch Die metrischen Daten in jedem Intervall sind eine Aggregation von mindestens zwei Stichproben, die in diesem Intervall gesammelt wurden.

Ausführliche Informationen dazu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch. Sie können Ihre Dienste auch überwachen CloudWatch , um zu sehen, welche Dienste Ressourcen verbrauchen. Weitere Informationen finden Sie unter AWS Dienste, die CloudWatch Metriken veröffentlichen.

Inhalt

- AWS Direct Connect Metriken und Dimensionen
- AWS Direct Connect CloudWatch Metriken anzeigen
- CloudWatch Amazon-Alarme erstellen, um AWS Direct Connect Verbindungen zu überwachen

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 Eigentümerkonten für gehostete virtuelle Schnittstellen verfügbar. Einheiten: Für diese Metrik wurden keine Einheiten zurückgegeben.
`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 auf der 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 an die 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 Redundanzprüfungsfehler (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 CloudWatch beispielsweise 5 Minuten zu ermitteln, wenden Sie die Statistik „Summe“ an. 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
`ConnectionLightLevelTx`	Zeigt den Zustand der Glasfaserverbindung für ausgehenden (ausgehenden) Verkehr von der AWS Seite der Verbindung an. Es gibt zwei Dimensionen für diese Metrik. Weitere Informationen finden Sie unter Verfügbare Abmessungen von Direct Connect. Einheiten: dBm

Metrik	Beschreibung
`ConnectionLightLevelRx`	Zeigt den Zustand der Glasfaserverbindung für eingehenden (eingehenden) Verkehr zur AWS Seite der Verbindung an. Es gibt zwei Dimensionen für diese Metrik. Weitere Informationen finden Sie unter Verfügbare Abmessungen von Direct Connect. Einheiten: dBm
`ConnectionEncryptionState`	Gibt den Verschlüsselungsstatus der Verbindung an. 1 gibt an, dass die Verbindungsverschlüsselung up ist, und 0 gibt an, dass die Verbindungsverschlüsselung down ist. Wenn diese Metrik auf eine LAG angewendet wird, bedeutet 1, dass für alle Verbindungen in der LAG die Verschlüsselung up ist. 0 gibt an, dass mindestens eine LAG-Verbindungsverschlüsselung 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.

Metrik	Beschreibung
	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 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

AWS Direct Connect verfügbare Abmessungen

Sie können die AWS Direct Connect Daten anhand der folgenden Dimensionen filtern.

Dimension	Beschreibung
`ConnectionId`	Diese Dimension ist in den 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

Dimension	Beschreibung
	die Daten nach der optischen Spurnummer der Direct Connect-V erbindung.
`VirtualInterfaceId`	Diese Dimension ist in den Metriken für die virtuelle Direct Connect-Schnittstelle verfügbar und filtert die Daten nach der virtuellen Schnittstelle.

Themen

- AWS Direct Connect CloudWatch Metriken anzeigen
- CloudWatch Amazon-Alarme erstellen, um AWS Direct Connect Verbindungen zu überwachen

AWS Direct Connect CloudWatch Metriken anzeigen

AWS Direct Connect sendet die folgenden Messwerte zu Ihren Direct Connect-Verbindungen. Amazon aggregiert diese Datenpunkte CloudWatch dann in Intervallen von 1 Minute oder 5 Minuten. Standardmäßig werden Direct Connect-Metrikdaten in CloudWatch 5-Minuten-Intervallen geschrieben.

> **Note**
>
> Bei der Überwachung von Direct Connect können CloudWatch Sie Metriken in Intervallen von 1 Minute anfordern. Die tatsächliche Aktualisierungshäufigkeit wird jedoch von CloudWatch gesteuert. Da Direct Connect das Intervall CloudWatch steuert, kann es nicht immer garantieren, dass Intervalle kürzer als fünf Minuten sind.

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 Amazon CloudWatch zur Anzeige von Direct Connect-Kennzahlen, einschließlich des Hinzufügens

mathematischer Funktionen oder vorgefertigter Abfragen, finden Sie unter Verwenden von Amazon CloudWatch Metriken im CloudWatch Amazon-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 ConnectionIdoder Metriknamen und wählen Sie dann eine der folgenden Optionen, 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 CloudWatch Metriken mit Metrics Insights im CloudWatch Amazon-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.

Um Metriken mit dem anzuzeigen AWS CLI

Geben Sie als Eingabeaufforderung den folgenden Befehl ein.

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

CloudWatch Amazon-Alarme erstellen, um AWS Direct Connect Verbindungen zu überwachen

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS 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 dazu, was Sie zum Erstellen eines Alarms wissen sollten, und weitere Informationen zum Erstellen eines Alarms finden Sie unter Verwenden von Amazon CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.

Um einen CloudWatch Alarm zu erstellen.

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 Using Amazon CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.
8. Wählen Sie Weiter.
9. Konfigurieren Sie die Alarmaktionen auf der Seite Configure actions (Aktionen konfigurieren). Weitere Informationen zur Konfiguration von Alarmaktionen finden Sie unter Alarmaktionen im CloudWatch Amazon-Benutzerhandbuch.
10. Wählen Sie Weiter.
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 aufgeführt, die sich auf AWS Direct Connect.

Komponente	Kontingent	Kommentare
Private oder öffentliche virtuelle Schnittstellen pro AWS Direct Connect dedizierter Verbindung	50	Dieses Limit kann nicht erhöht werden.
Übertragung virtueller Schnittstellen pro AWS Direct Connect dedizierter Verbindung. Virtuelle Transitschnittstellen können verwendet werden, um eine Verbindung zu einem Transit Gateway oder einem AWS Cloud-WAN-Kernnetzwerk herzustellen. Weitere Informationen finden Sie unter Gateways.	4	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
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 Transitschnittstelle 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.

Komponente	Kontingent	Kommentare
Private, öffentliche oder virtuelle Transitschnittstellen pro gehosteter Verbindung AWS Direct Connect	1	Dieses Limit kann nicht erhöht werden.
Aktive AWS Direct Connect Verbindungen pro Direct Connect-Standort pro Region pro Konto	10	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Anzahl der virtuellen Schnittstellen pro Link Aggregation Group (LAG)	54	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 Transitschnittstelle 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 einer virtuellen Transitschnittstelle von lokal zu. AWS Wenn Sie für IPv4 und während der BGP-Sitzung jeweils mehr als 100 Routen ankündigen, geht die BGP-Sitzung in einen Ruhezustand IPv6 über, sodass die BGP-Sitzung AUSGEFALLEN ist.	Jeweils 100 für und IPv4 IPv6	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
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-Aggregationsgruppen (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).
Virtuelle private Gateways pro Gateway AWS Direct Connect	20	Dieses Limit kann nicht erhöht werden.
Transit-Gateways pro Gateway AWS Direct Connect	6	Dieses Limit kann nicht erhöht werden.

Komponente	Kontingent	Kommentare
Maximale Anzahl angekündigter Routenpräfixe von einem Direct Connect-Gateway-Anschluss eines AWS Cloud WAN-Kernnetzwerks an den Standort. **Note** Alle virtuellen Transitschnittstellen, die an dieses Direct Connect-Gateway angeschlossen sind, erhalten alle vom Kernnetzwerk angekündigten Routenpräfixe.	5,000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Virtuelle Schnittstellen (privat oder Transit) pro Gateway AWS Direct Connect	30	Dieses Limit kann nicht erhöht werden.
Anzahl der Präfixe pro AWS Transit Gateway von AWS bis vor Ort auf einer virtuellen Transitschnittstelle	Insgesamt 200 für und IPv4 IPv6	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
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 nm), 10 Gbit/s: 10GBASE-LR (1310 nm), 100 Gbit/s: 100GBASE- und 400 Gbit/s: 400GBASE-. LR4 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 den Lastenausgleich mit mehreren öffentlichen Geräten verwenden möchten, müssen sich alle in derselben Region befinden. VIFs VIFs

Problembehebung 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)
- Behandlung von Problemen auf Ebene 2 (Datenverbindung)
- Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport)
- Beheben von Routing-Problemen

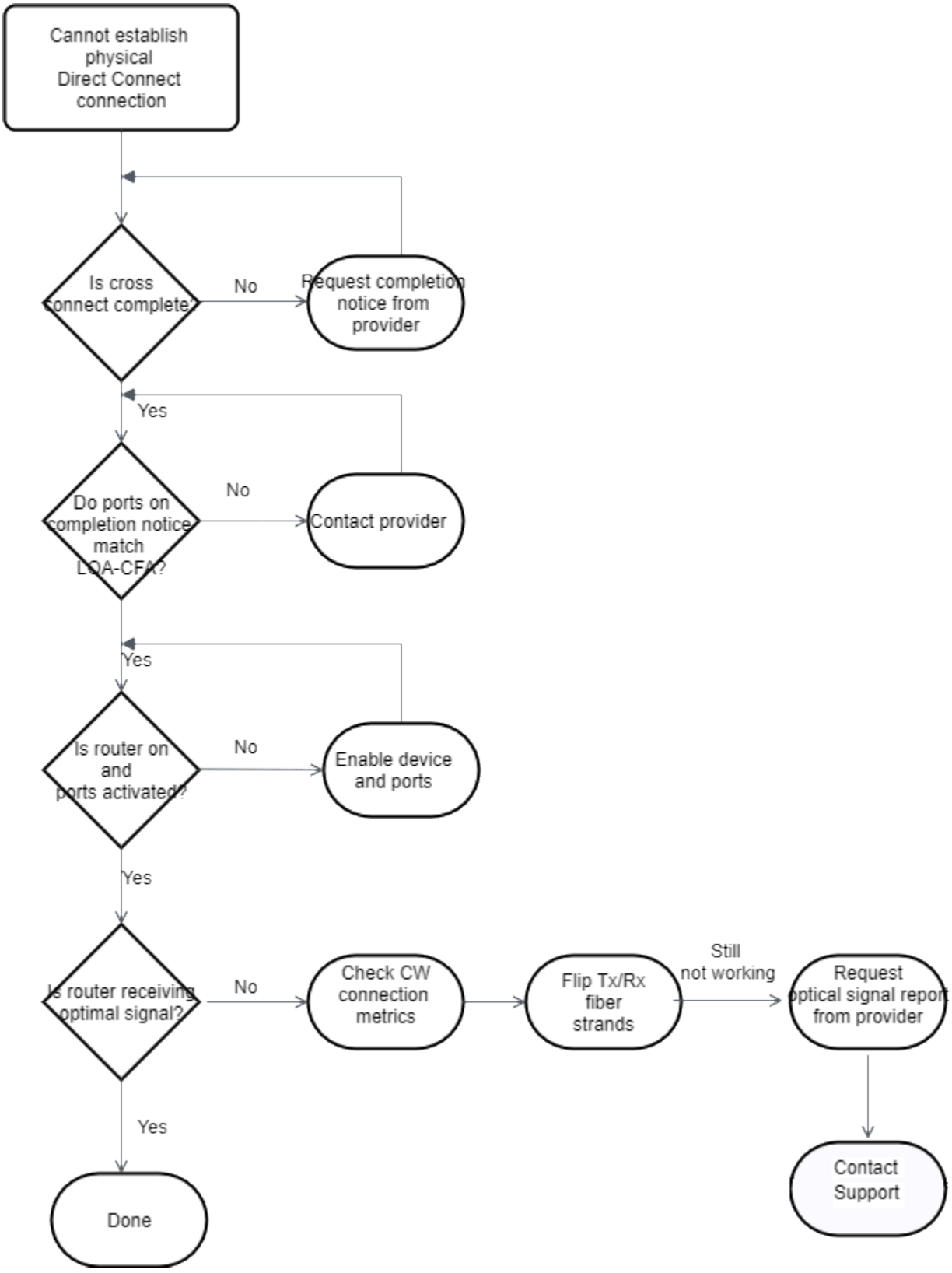
Behandlung von Problemen auf Ebene 1 (physisch)

Wenn Sie oder Ihr Netzwerkanbieter Schwierigkeiten haben, eine physische Verbindung zu einem AWS Direct Connect Gerät herzustellen, gehen Sie wie folgt vor, 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 Absprache 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). Abhängig vom Direct Connect-Endpunkt, über den Ihre Verbindung beendet wird, muss die automatische Absprache möglicherweise entsprechend aktiviert oder deaktiviert werden.
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 CloudWatch Amazon-Metriken für AWS Direct Connect. Sie können die optischen Tx/Rx-Werte des AWS Direct Connect Geräts (sowohl 1 Gbit/s als auch 10 Gbit/s), die Anzahl der physischen Fehler 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.

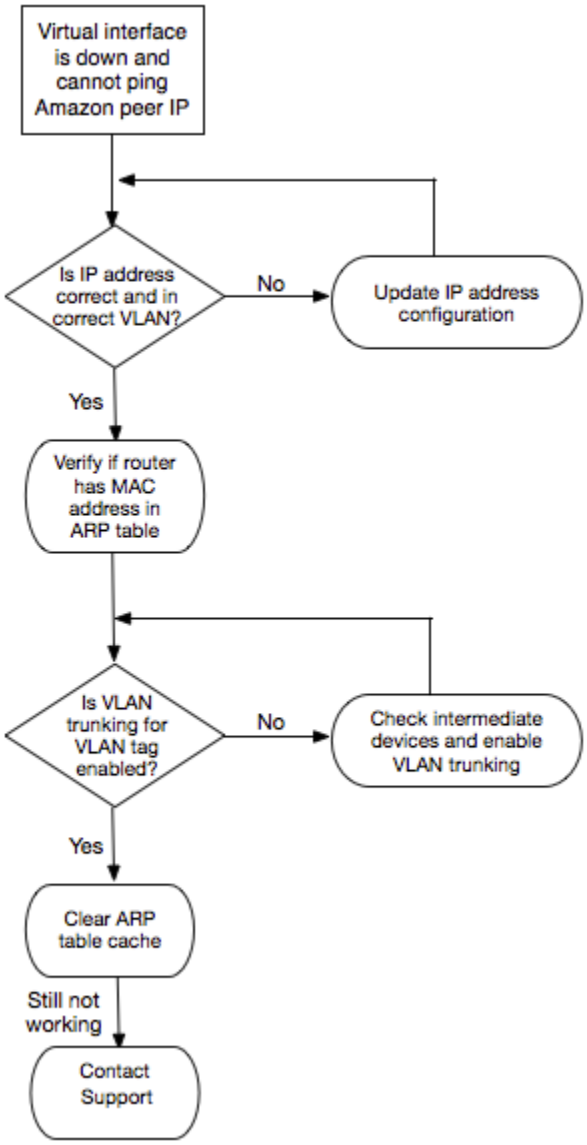

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check 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 besteht, Ihre virtuelle Schnittstelle jedoch ausgefallen ist, gehen Sie wie folgt vor, 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. GigabitEthernet 0/0.123 statt 0/0). GigabitEthernet
2. Überprüfen Sie, ob der Router in Ihrer ARP-Tabelle (Address Resolution Protocol) über einen MAC-Adresseintrag vom AWS Endpunkt verfügt.
3. Stellen Sie sicher, dass für alle zwischengeschalteten Geräte zwischen Endpunkten für Ihren 802.1Q VLAN-Tag VLAN-Trunking aktiviert ist. ARP kann nicht AWS nebenbei eingerichtet werden, bis markierter Datenverkehr AWS empfangen wird.
4. Löschen Sie den Cache Ihrer ARP-Tabelle oder der Ihres Anbieters.
5. Wenn mit den oben genannten Schritten kein ARP eingerichtet wird oder Sie die Amazon-Peer-IP immer noch nicht pingen können, wenden Sie sich an den AWS Support.

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Problemen mit der Datenverbindung.



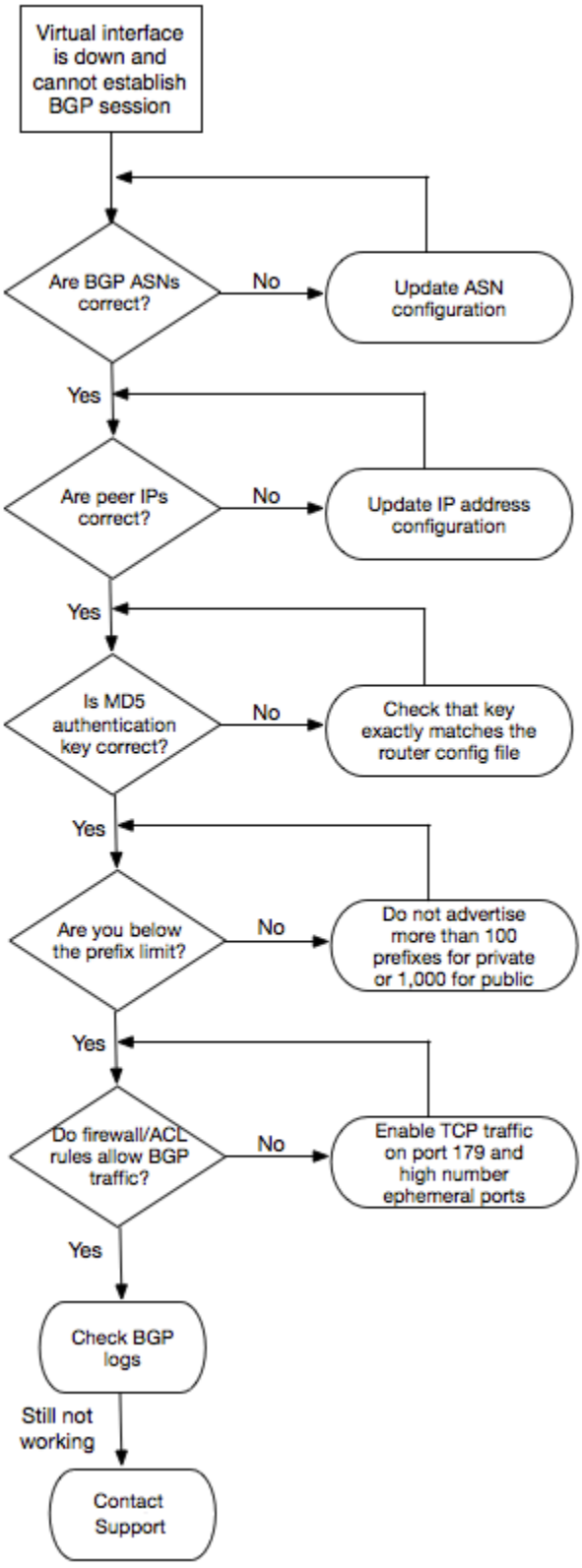
Wenn die BGP-Sitzung auch nach Überprüfen dieser Schritte nicht hergestellt werden kann, lesen Sie Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport). Wenn die BGP-Sitzung zwar hergestellt wurde, Sie aber Probleme mit dem Routing haben, lesen Sie Beheben von Routing-Problemen.

Behandlung von Problemen auf Ebene 3/4 (Netzwerk/Transport)

Stellen Sie sich eine Situation vor, in der Ihre AWS Direct Connect physische Verbindung besteht und Sie die Amazon-Peer-IP-Adresse pingen können. Wenn Ihre virtuelle Schnittstelle aktiv ist und die BGP-Peering-Sitzung nicht eingerichtet werden kann, gehen Sie wie folgt vor, 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 der Peer IPs für beide Seiten der BGP-Peering-Sitzung korrekt konfiguriert ist.
3. Stellen Sie sicher, dass Ihr 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 obigen Schritte die BGP-Peering-Sitzung nicht einrichten, wenden Sie sich an AWS den Support.

Das folgende Flussdiagramm enthält die Schritte zum Diagnostizieren von Problemen mit der BGP-Peering-Sitzung.



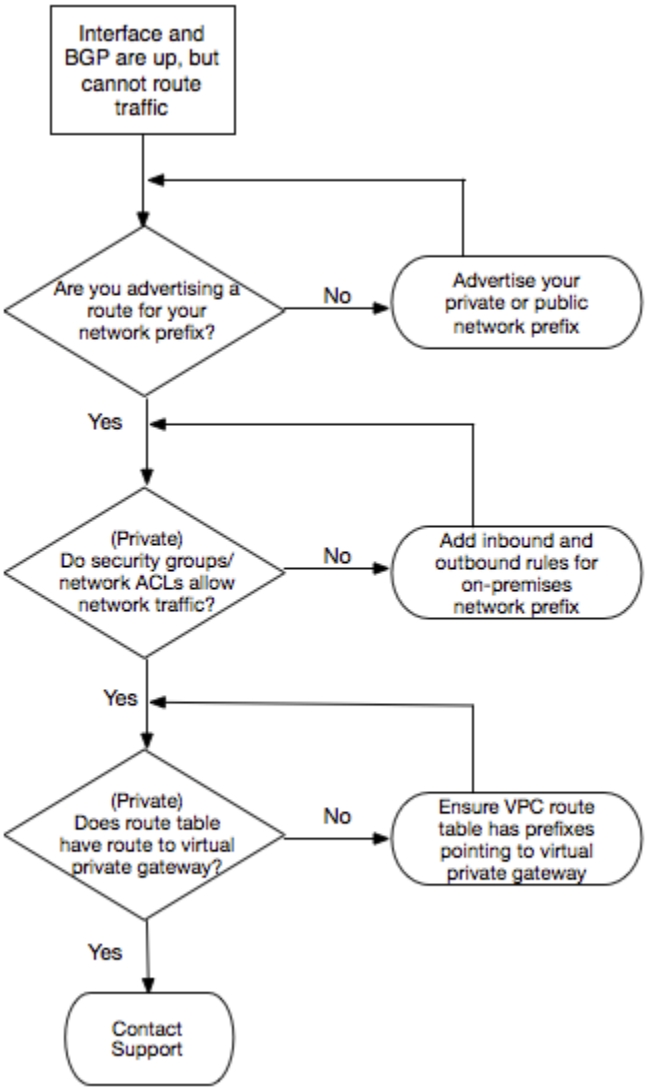
Wenn die BGP-Peering-Sitzung hergestellt wurde, Sie aber Probleme mit dem Routing haben, lesen Sie Beheben von Routing-Problemen.

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 für eine private virtuelle Schnittstelle sicher, dass Ihre VPC-Sicherheitsgruppen und Ihr Netzwerk eingehenden und ausgehenden Datenverkehr für Ihr lokales Netzwerkpräfix ACLs 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 oben genannten Schritte Ihre Routing-Probleme nicht lösen, 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 Versionen für beschrieben AWS Direct Connect. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erstellen Sie eine Verbindung zwischen dem Direct Connect-Gateway und einem AWS Network Manager Kernnetzwerk	Sie können jetzt eine Direct Connect-Gateway-Zuordnung direkt zwischen Direct Connect und einem AWS Cloud-WAN-Kernnetzwerk erstellen.	25. November 2024
Support für 400G	Die Themen wurden aktualisiert und umfassen nun Unterstützung für 400G-Verbindungen.	18. Juli 2024
Ein SiteLink Präfix-Limit wurde hinzugefügt	Dem Thema Kontingente und Limits SiteLink wurde ein Präfixlimit für hinzugefügt.	15. Juni 2023
Support für SiteLink	Sie können eine private virtuelle Schnittstelle erstellen, die Konnektivität zwischen zwei Direct Connect-Präsenzpunkten (PoPs) in derselben AWS Region ermöglicht.	1. Dezember 2021
Support Sie MAC-Sicherheit	Sie können AWS Direct Connect Verbindungen verwenden, die MACsec die Verschlüsselung Ihrer Daten von Ihrem Unternehmensrechenzentrum zum AWS	31. März 2021

	Direct Connect Standort unterstützen.	
Support für 100G	Aktualisierte Inhalte um Support für dedizierte 100G-Verbindungen mit einzubezi ehen.	12. Februar 2021
Neuer Standort in Italien	Thema wurde aktualisiert, um das Hinzufügen des neuen Standorts in Italien einzuschl ießen.	22. Januar 2021
Neuer Standort in Israel	Thema wurde aktualisiert, um das Hinzufügen des neuen Standorts in Israel einzuschl ießen.	7. Juli 2020
Unterstützung für Failover-Tests im Resiliency Toolkit	Verwenden Sie die Failover-Testfunktion des Resiliency Toolkit, um die Resilienz Ihrer Verbindungen zu testen.	3. Juni 2020
CloudWatch Unterstützung von VIF-Metriken	Sie können physische AWS Direct Connect Verbindungen und virtuelle Schnittstellen überwachen mit CloudWatch.	11. Mai 2020
AWS Direct Connect Resilienz -Toolkit	Das AWS Direct Connect Resiliency Toolkit bietet einen Verbindungsassiste nten mit mehreren Resilienz modellen, mit dem Sie spezielle Verbindungen bestellen können, um Ihr SLA-Ziel zu erreichen.	7. Oktober 2019

Zusätzliche regionale Unterstützung für Support für AWS Transit Gateway Accounts	Zusätzliche regionale Unterstützung für AWS Transit Gateway alle Konten.	30. September 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 Transitschnittstelle mit Ihrem Transit-Gateway VPCs oder einem Anschluss VPNs an Ihr Transit-Gateway zu verbinden. 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.	27. März 2019
Unterstützung für Jumbo-Frames	Sie können Jumbo-Frames (9001 MTU) darüber senden. AWS Direct Connect	11. Oktober 2018
BGP-Gemeinschaften mit lokaler Präferenz	Mit BGP-Community-Tags für lokale Präferenzen erreichen Sie Lastausgleich und Routing-Präferenzen für eingehenden Datenverkehr mit Ihrem Netzwerk.	6. Februar 2018

AWS Direct Connect Gateway	Sie können ein Direct Connect-Gateway verwenden, um Ihre AWS Direct Connect Verbindung zu VPCs abgelegenen Regionen herzustellen.	1. November 2017
CloudWatch Amazon-Metriken	Sie können CloudWatch Metriken für Ihre AWS Direct Connect Verbindungen einsehen.	29. Juni 2017
Link-Aggregationsgruppen	Sie können eine Linkaggregationsgruppe (LAG) erstellen, um mehrere AWS Direct Connect Verbindungen zu aggregieren.	13. Februar 2017
IPv6 Unterstützung	Ihre virtuelle Schnittstelle kann jetzt eine IPv6 BGP-Peering-Sitzung unterstützen.	1. Dezember 2016
Unterstützung für Tagging	Sie können Ihre AWS Direct Connect Ressourcen jetzt taggen.	4. November 2016
Self-Service LOA-CFA	Sie können Ihr LOA-CFA (Letter of Authorization and Connecting Facility Assignment) jetzt über die Konsole oder API herunterladen. AWS Direct Connect	22. Juni 2016
Neuer Standort im Silicon Valley	Thema wurde aktualisiert, um den neuen Standort Silicon Valley in die Region USA West (Nordkalifornien) mit einzubeziehen.	3. Juni 2016

Neuer Standort in Amsterdam	Thema wurde aktualisiert, um den neuen Standort Amsterdam in die Region Europa (Frankfurt) mit einzubeziehen.	19. Mai 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. April 2016
Neuer Standort in Sao Paulo, Brasilien	Thema wurde aktualisiert, um den neuen Standort Sao Paulo in die Region Südamerika (São Paulo) mit einzubeziehen.	9. Dezember 2015
Neue Standorte in Dallas, London, Silicon Valley und Mumbai	Die Themen wurden aktualisiert und umfassen 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. November 2015
Neuer Standort in der Region China (Peking)	Themen wurden aktualisiert, um den neuen Standort Peking in die Region China (Peking) mit einzubeziehen.	14. April 2015

Neuer Standort in Las Vegas in der Region USA West (Oregon)	Die Themen wurden aktualisiert und beinhalten nun auch die Hinzufügung des neuen Standorts AWS Direct Connect Las Vegas in der Region USA West (Oregon).	10. November 2014
Neue Region EU (Frankfurt)	Die Themen wurden aktualisiert und beinhalten nun auch die AWS Direct Connect Hinzufügung neuer Standorte für die Region EU (Frankfurt).	23. Oktober 2014
Neue Standorte in der Region Asien-Pazifik (Sydney)	Die Themen wurden aktualisiert und beinhalten nun die Hinzufügung neuer AWS Direct Connect Standorte für die Region Asien-Pazifik (Sydney).	14. Juli 2014
Support für AWS CloudTrail	Es wurde ein neues Thema hinzugefügt, in dem erklärt wird CloudTrail , wie Sie Aktivitäten anmelden können AWS Direct Connect.	4. April 2014
Support für den Zugriff auf abgelegene AWS Regionen	Neues Thema hinzugefügt, um zu erklären, wie Sie Zugriff auf öffentliche Ressourcen in einer entfernten Region erhalten.	19. Dezember 2013
Support für gehostete Verbindungen	Aktualisierte Inhalte um Support für gehostete Verbindungen mit einzubeziehen.	22. Oktober 2013

Neuer Standort in der Region EU (Irland)	Die Themen wurden aktualisiert und beinhalten nun auch den neuen AWS Direct Connect Standort für die Region EU (Irland).	24. Juni 2013
Neuer Standort in Seattle in der Region USA West (Oregon)	Die Themen wurden aktualisiert und beinhalten nun auch den neuen AWS Direct Connect Standort in Seattle, der die Region USA West (Oregon) bedient.	8. Mai 2013
Support für die Verwendung von IAM mit AWS Direct Connect	Es wurde ein Thema zur Verwendung von AWS Identity and Access Management mit AWS Direct Connect hinzugefügt.	21. Dezember 2012
Neue Region Asien-Pazifik (Sydney)	Die Themen wurden aktualisiert und beinhalten nun auch den neuen AWS Direct Connect Standort für die Region Asien-Pazifik (Sydney).	14. Dezember 2012

Neue AWS Direct Connect Konsole und die Regionen USA Ost (Nord-Virginia) und Südamerika (Sao Paulo)	Das Handbuch „ AWS Direct Connect Erste Schritte“ wurde durch das AWS Direct Connect Benutzerhandbuch ersetzt. Es wurden neue Themen zur neuen AWS Direct Connect Konsole hinzugefügt, ein Thema zur Abrechnung hinzugefügt, Informationen zur Router-Konfiguration hinzugefügt und die Themen um zwei neue AWS Direct Connect Standorte für die Regionen USA Ost (Nord-Virginia) und Südamerika (Sao Paulo) erweitert.	13. August 2012
Support für die Regionen EU (Irland), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio)	Es wurde ein neuer Abschnitt zur Fehlerbehebung hinzugefügt und die Themen wurden um vier neue AWS Direct Connect Standorte für die Regionen USA West (Nordkalifornien), EU (Irland), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) erweitert.	10. Januar 2012
Support für die Region USA West (Nordkalifornien)	Themen wurden aktualisiert, um die Region USA West (Nordkalifornien) mit einzubeziehen.	8. September 2011
Öffentliche Veröffentlichung	Die erste Version von AWS Direct Connect.	3. August 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.