AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Was ist ein Transit Gateway? ... 1
Transit-Gateway-Konzepte ... 1
Erste Schritte mit Transit Gateways ... 2
Arbeiten mit Transit Gateways ... 2
Preisgestaltung ... 3
Funktionsweise von Transit Gateways ... 4
Architekturdiagramm ... 4
Ressourcen-Anhänge ... 5
Mehrpfad-Routing zu gleichen Kosten ... 6
Availability Zones ... 7
Routing ... 8
Routing-Tabellen ... 8
Routing-Tabellenzuordnung ... 9
Routing-Propagierung ... 9
Routen für Peering-Anhänge ... 10
Reihenfolge der Routenauswertung ... 10
Erste Schritte ... 13
Voraussetzungen ... 13
Schritt 1: Erstellen des Transit Gateway ... 14
Schritt 2: Anhängen Ihrer VPCs an Ihre Transit Gateways ... 15
Schritt 3: Hinzufügen von Routen zwischen dem Transit Gateway und Ihren VPCs ... 16
Schritt 4: Testen des Transit Gateways ... 16
Schritt 5: Löschen des Transit Gateway ... 16
Bewährte Methoden für das Design ... 18
Beispielanwendungsfälle ... 20
Zentralisierter Router ... 20
Übersicht ... 20
Ressourcen ... 21
Routing ... 22
Isolierte VPCs ... 23
Übersicht ... 23
Ressourcen ... 24
Routing ... 25
Isolierte VPCs mit freigegeben Services ... 26

Übersicht ... 27
Ressourcen ... 27
Routing ... 28
Peering ... 29
Übersicht ... 30
Ressourcen ... 30
Routing ... 31
Zentralisiertes Outbound-Routing ... 32
Übersicht ... 33
Ressourcen ... 33
Routing ... 34
Appliance-VPC ... 37
Übersicht ... 38
Statusbehaftete Appliances und Appliance-Modus ... 39
Routing ... 41
Arbeiten mit Transit Gateways ... 43
Transit Gateways ... 43
Erstellen eines Transit Gateways ... 44
Anzeigen Ihrer Transit Gateways ... 46
Hinzufügen oder Bearbeiten von Tags für ein Transit Gateway ... 47
Ändern eines Transit Gateways ... 47
Freigabe eines Transit Gateways ... 48
Akzeptieren einer Ressourcenfreigabe ... 49
Akzeptieren eines freigegebenen Anhangs ... 49
Löschen eines Transit Gateways ... 50
VPC-Anhänge ... 50
Lebenszyklus von VPC-Anhängen ... 51
Erstellen eines Transit-Gateway-Anhangs an eine VPC ... 54
Ändern des VPC-Anhangs ... 55
Ändern der VPC-Anhang-Tags ... 56
Anzeigen Ihrer VPC-Anhänge ... 56
Löschen eines VPC-Anhangs ... 57
Problembehandlung bei VPC-Anhängen ... 57
VPN-Anhänge ... 58
Erstellen eines Transit-Gateway-Anhangs an ein VPN ... 58
Anzeigen Ihrer VPN-Anhänge ... 59

Anhänge an ein Direct-Connect-Gateway ... 60
Peering-Anhänge ... 61
Erstellen eines Peering-Anhangs ... 62
Annehmen oder Ablehnen einer Peering-Anhangs-Anforderung ... 63
Hinzufügen einer Route zur Routing-Tabelle des Transit Gateways ... 63
Anzeigen Ihrer Transit-Gateway-Peering-Verbindungs-Anhängen ... 64
Löschen eines Peering-Anhangs ... 65
Überlegungen zu Opt-inAWS-Regionen ... 65
Connect-Anfügungen und Connect-Peers ... 66
Connect-Peers ... 67
Anforderungen und Überlegungen ... 70
Erstellen Sie einen Connect-Anhang ... 71
Erstellen Sie einen Connect-Peer (GRE-Tunnel) ... 72
So können Sie sich Ihre Connect-Anfügungen und Connect-Peers anzeigen lassen ... 73
Ändern Ihrer Connect-Anfügung und Connect Peer-Tags ... 74
Löschen eines Connect-Peers ... 74
Löschen Sie einen Connect-Anhang ... 75
Transit-Gateway-Routing-Tabellen ... 75
Erstellen einer Transit-Gateway-Routing-Tabelle ... 76
Anzeigen von Transit-Gateway-Routing-Tabellen ... 76
Zuordnen einer Transit-Gateway-Routing-Tabelle ... 77
Löschen einer Zuordnung für eine Transit-Gateway-Routing-Tabelle ... 77
Verbreiten einer Route an eine Transit-Gateway-Routing-Tabelle ... 78
Deaktivieren der Route-Propagierung ... 78
Erstellen einer statischen Route ... 79
Löschen einer statischen Route ... 80
Eine statische Route ersetzen ... 81
Exportieren von Routing-Tabellen zu Amazon S3 ... 81
Löschen einer Transit-Gateway-Routing-Tabelle ... 83
Präfixlisten-Verweise ... 83
Transit-Gateway-Richtlinientabellen ... 86
Erstellen einer Transit-Gateway-Richtlinientabelle ... 87
Löschen einer Transit-Gateway-Richtlinientabelle ... 87
Multicast auf Transit Gateways ... 88
Multicast-Konzepte ... 1
Überlegungen ... 89

Multicast mit Windows Server ... 91
Multicast-Routing ... 92
Arbeiten mit Multicast ... 93
Anzeigen Ihrer Transit Gateways ... 114
Aufheben der Freigabe eines Transit Gateways ... 115
Gemeinsame Subnetze ... 116
Flow-Protokolle für Transit-Gateway ... 117
Flow-Protokolldatensätze für Transit-Gateway ... 118
Standardformat ... 119
Benutzerdefiniertes Format ... 119
Verfügbare Felder ... 119
Flow-Protokolle für Transit-Gateway – Preise ... 125
In CloudWatch Logs veröffentlichen ... 125
IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs ... 126
Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle ... 129
Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch ... 129
Prozessflussprotokolldatensätze in Logs CloudWatch ... 130
Auf Amazon S3 veröffentlichen ... 132
Flow-Protokolldateien ... 133
IAM-Richtlinie für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen ... 135
Amazon S3-Bucket-Berechtigungen für Flow-Protokolle ... 136
Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS ... 137
Amazon S3-Protokolldateiberechtigungen ... 138
Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht ... 139
Verarbeiten von Flow-Protokolldatensätzen in Amazon S3 ... 141
Veröffentlichen in Amazon Kinesis Data Firehose ... 141
IAM-Rollen für die kontoübergreifende Bereitstellung ... 141
Erstellen Sie ein Flow-Protokoll, das in Firehose veröffentlicht wird ... 146
Arbeiten mit Flow-Protokollen ... 148
Kontrollieren der Nutzung von Flow-Protokollen ... 148
Erstellen eines Flow-Protokolls ... 149
Anzeigen von Flow-Protokollen ... 149
Hinzufügen oder Entfernen von Tags für Flow-Protokolle ... 150
Anzeigen von Flow-Protokolldatensätzen ... 150
Suche nach Flow-Protokoll-Datensätzen ... 151
Löschen eines Flow-Protokolls ... 152

API- und CLI-Übersicht und -Einschränkungen 153
Überwachen Ihrer Transit Gateways 155
CloudWatch-Metriken 156
Transit-Gateway-Metriken 156
Metrik-Dimensionen für Transit Gateways 158
CloudTrail-Protokolle 158
Transit-Gateway-Informationen in CloudTrail 159
Informationen zu Transit-Gateway-Protokolldatei-Einträgen 160
Identity and Access Management 163
Beispielrichtlinien für die Verwaltung von Transit Gateways 163
Beispielrichtlinien für die Verwaltung von AWS-Network Manager 165
Serviceverknüpfte Rollen 166
Transit Gateway 166
Von AWS verwaltete Richtlinien 167
AWSVPCTransitGatewayServiceRolePolicy 168
Richtlinienaktualisierungen 168
Netzwerk-ACLs 169
Gleiches Subnetz für EC2-Instances und Transit-Gateway-Zuordnung 169
Verschiedene Subnetze für EC2-Instances und Transit-Gateway-Zuordnung 170
Bewährte Methoden 170
Kontingente 172
Allgemeines 172
Routing 172
Transit-Gateway-Anhänge 173
Bandbreite 174
AWS Direct Connect Gateways 175
Maximum Transmission Unit (MTU) 176
Multicast 176
Network Manager 177
Zusätzliche Kontingentressourcen 177
Dokumentverlauf 178
..... clxxxi

Was ist ein Transit Gateway?

Ein Transit Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre Virtual Private Clouds (VPCs) und On-Premises-Netzwerke miteinander verbinden können. Wenn sich Ihre Cloud-Infrastruktur global ausdehnt, verbindet das interregionale Peering Transit Gateways mithilfe der AWS globalen Infrastruktur Der gesamte Netzwerkverkehr zwischen AWS-Rechenzentren wird automatisch auf der physischen Ebene verschlüsselt.

Weitere Informationen finden Sie unter AWS Transit Gateway.

Transit-Gateway-Konzepte

Die wichtigsten Konzepte für Transit Gateways sind folgende:

- Anhänge – Sie können Folgendes anhängen:
  - Eine oder mehrere VPCs
  - Eine Connect-SD-WAN/Drittanbieter-Netzwerk-Appliance
  - Ein AWS Direct Connect Gateway
  - Eine Peering-Verbindung zu einem anderen Transit Gateway
  - Eine VPN-Verbindung zu einem Transit Gateway
- Maximale Transit-Gateway-Übertragungseinheit (MTU) – Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übermittelt werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein Transit Gateway unterstützt eine MTU von 8500 Byte für den Datenverkehr zwischen VPCs, AWS Direct Connect, Transit-Gateway-Connect und Peering-Anlagen. Datenverkehr über VPN-Verbindungen kann eine MTU von 1 500 Byte haben.
- Transit-Gateway-Routing-Tabelle – Ein Transit Gateway verfügt über eine Standard-Routing-Tabelle und optional über zusätzliche Routing-Tabellen. Eine Routing-Tabelle umfasst dynamische und statische Routen, die den nächsten Hop basierend auf der Ziel-IP-Adresse des Pakets bestimmen. Das Ziel dieser Routen kann ein beliebiger Transit-Gateway-Anhang sein. Standardmäßig sind Transit-Gateway-Anhänge mit der standardmäßigen Transit-Gateway-Routing-Tabelle verknüpft.
- Zuordnungen: Jeder Anhang ist immer genau einer Routing-Tabelle zugeordnet. Routing-Tabellen können keiner, aber auch mehreren Anhängen zugeordnet sein.

- Routing-Verteilung – Eine VPC oder VPN-Verbindung oder ein Direct-Connect-Gateway kann Routen dynamisch auf eine Transit-Gateway-Routing-Tabelle übertragen. Bei einem Connect-Anhang werden die Routen standardmäßig an eine Transit-Gateway-Routing-Tabelle weitergegeben. Im Falle einer VPC müssen Sie statische Routen erstellen, um Datenverkehr an das Transit-Gateway zu senden. Im Falle einer VPN-Verbindung werden Routen unter Verwendung des Border Gateway Protocol (BGP) vom Transit-Gateway auf Ihren On-Premises-Router übertragen. Bei einem Direct-Connect-Gateway werden die zulässigen Präfixe mithilfe von BGP auf Ihren On-Premises-Router übertragen. Bei einem Peering-Anhang müssen Sie in der Routing-Tabelle des Transit Gateways eine statische Route erstellen, um auf den Peering-Anhang zu verweisen.

Erste Schritte mit Transit Gateways

Verwenden Sie die folgenden Ressourcen, um ein Transit Gateway zu erstellen und zu verwenden.

- Funktionsweise von Transit Gateways
- Erste Schritte
- Bewährte Methoden für das Design

Arbeiten mit Transit Gateways

Sie können Ihre Transit-Gateway-Ressourcen über die folgenden Schnittstellen erstellen und verwalten:

- AWS Management Console – Bietet eine Webschnittstelle für den Zugriff auf Ihre Transit Gateways.
- AWS-Befehlszeilenschnittstelle (AWS CLI) – Bietet Befehle für eine breite Palette von AWS-Services, einschließlich Amazon VPC, und wird auf Windows, macOS und Linux unterstützt. Weitere Informationen finden Sie unter AWS Command Line Interface.
- AWS SDKs– Bieten sprachspezifische API-Operationen und übernehmen viele der Verbindungsdetails, wie zum Beispiel die Berechnung der Signaturen, die Verarbeitung des erneuten Absendens von Anforderungen und die Fehlerbehandlung. Weitere Informationen finden Sie unter AWS-SDKs.
- Abfrage-API – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf die

Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und die Fehlerbehandlung in der Anwendung durchgeführt werden. Weitere Informationen finden Sie in der Amazon-EC2-API-Referenz.

Preisgestaltung

Jeder Anhang an ein Transit Gateway wird Ihnen stündlich berechnet, und Ihnen wird der auf dem Transit Gateway verarbeitete Datenverkehr in Rechnung gestellt. Weitere Informationen finden Sie unter AWS-Transit-Gateway-Preise.

Funktionsweise von Transit Gateways

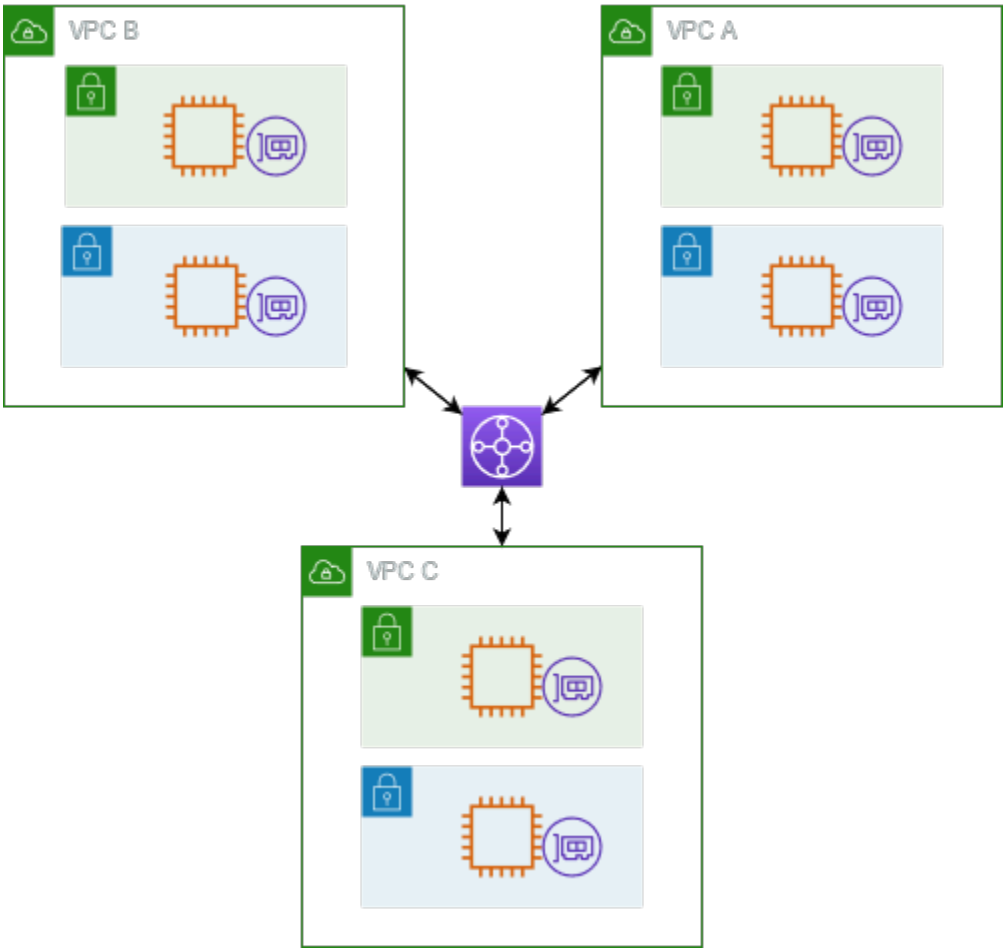
Ein Transit Gateway fungiert als regionaler virtueller Router für Datenverkehr zwischen Ihren Virtual Private Clouds (VPCs) und On-Premises-Netzwerken. Ein Transit Gateway wird basierend auf dem Volumen an Netzwerkdatenverkehr elastisch skaliert. Die Weiterleitung über ein Transit Gateway erfolgt auf Schicht 3, wo Pakete basierend auf ihren Ziel-IP-Adressen an einen bestimmten Next-Hop-Anhang gesendet werden.

Inhalt

- Architekturdiagramm
- Ressourcen-Anhänge
- Mehrpfad-Routing zu gleichen Kosten
- Availability Zones
- Routing

Architekturdiagramm

Im folgenden Diagramm ist ein Transit Gateway mit drei VPC-Anhängen abgebildet. Die Routentabelle für jede dieser VPCs enthält die lokale Route und Routen, die den für die anderen beiden VPCs bestimmten Datenverkehr an das Transit-Gateway senden.



Im Folgenden finden Sie ein Beispiel für eine Standard-Transit-Gateway-Routing-Tabelle für die im vorherigen Diagramm gezeigten Anhänge. Die CIDR-Blöcke für jede VPC werden an die Routing-Tabelle übertragen. Daher kann jeder Anhang Pakete an die beiden anderen Anhänge weiterleiten.

Bestimmungsort	Ziel	Routing-Typ
VPC A CIDR	*Anfügung für VPC A*	propagiert
VPC B CIDR	*Anfügung für VPC B*	propagiert
VPC C CIDR	*Anfügung für VPC C*	verbreitet

Ressourcen-Anhänge

Ein Transit-Gateway-Anhang ist sowohl eine Quelle als auch ein Ziel für Pakete. Sie können die folgenden Ressourcen an Ihr Transit-Gateway anhängen:

- Eine oder mehrere VPCs. AWS Transit Gateway stellt eine elastic network interface innerhalb von VPC-Subnetzen bereit, die dann vom Transit-Gateway verwendet wird, um den Verkehr zu und von den ausgewählten Subnetzen weiterzuleiten. Sie müssen mindestens ein Subnetz für jede Availability Zone haben, das es dann ermöglicht, Datenverkehr an Ressourcen in jedem Subnetz dieser Zone weiterzuleiten. Während der Anhangserstellung können Ressourcen innerhalb einer bestimmten Availability Zone nur dann ein Transit Gateway erreichen, wenn ein Subnetz innerhalb derselben Zone aktiviert ist. Wenn eine Subnetz-Routing-Tabelle eine Route zum Transit Gateway enthält, wird der Datenverkehr nur dann an das Transit Gateway weitergeleitet, wenn das Transit Gateway einen Anhang im Subnetz derselben Availability Zone hat.
- Eine oder mehrere VPN-Verbindungen
- Ein oder mehrere Gateways AWS Direct Connect
- Eine oder mehrere Transit-Gateway-Connect-Anhänge
- Eine oder mehrere Transit-Gateway-Peering-Verbindungen
- Ein Transit-Gateway-Anhang kann sowohl eine Quelle als auch ein Ziel für Pakete sein.

Mehrpfad-Routing zu gleichen Kosten

AWS Transit Gateway unterstützt Equal Cost Multipath (ECMP) -Routing für die meisten Anlagen. Für einen VPN-Anhang können Sie die ECMP-Unterstützung mithilfe der Konsole aktivieren oder deaktivieren, wenn Sie ein Transit Gateway erstellen oder ändern. Für alle anderen Anhangstypen gelten die folgenden ECMP-Einschränkungen:

- VPC – VPC unterstützt ECMP nicht, da sich CIDR-Blöcke nicht überschneiden können. Sie können beispielsweise keine VPC mit einem CIDR 10.1.0.0/16 mit einer zweiten VPC, die denselben CIDR verwendet, an ein Transit Gateway anhängen und dann ein Routing einrichten, um den Datenverkehr zwischen ihnen zu verteilen.
- VPN – Wenn die Option VPN-ECMP-Unterstützung deaktiviert ist, verwendet ein Transit Gateway interne Metriken, um den bevorzugten Pfad zu ermitteln, falls gleiche Präfixe über mehrere Pfade verteilt sind. Weitere Informationen zum Aktivieren oder Deaktivieren von ECMP für einen VPN-Anhang finden Sie unter the section called “Transit Gateways”.
- AWS Transit Gateway AWS Transit Gateway Connect — Connect-Anlagen unterstützen automatisch ECMP.
- AWS Direct Connect AWS Direct Connect Gateway — Gateway-Anhänge unterstützen ECMP automatisch für mehrere Direct Connect Gateway-Anhänge, wenn Netzwerkpräfix, Präfixlänge und AS_PATH exakt identisch sind.

- Transit-Gateway-Peering – Transit-Gateway-Peering unterstützt ECMP nicht, da es weder dynamisches Routing unterstützt noch Sie dieselbe statische Route für zwei verschiedene Ziele konfigurieren können.

> **Note**
>
> - BGP Multipath AS-Path Relax wird nicht unterstützt, daher können Sie ECMP nicht für verschiedene autonome Systemnummern (ASNs) verwenden.
> - ECMP wird zwischen verschiedenen Anhangstypen nicht unterstützt. Beispielsweise können Sie ECMP nicht zwischen einer VPN und einem VPC-Anhang aktivieren. Stattdessen werden Transit-Gateway-Routen ausgewertet und der Datenverkehr entsprechend der ausgewerteten Route weitergeleitet. Weitere Informationen finden Sie unter the section called “Reihenfolge der Routenauswertung”.
> - Ein einziges Direct Connect-Gateway unterstützt ECMP über mehrere virtuelle Transitschnittstellen. Daher empfehlen wir, nur ein einziges Direct Connect-Gateway einzurichten und zu verwenden und nicht mehrere Gateways einzurichten und zu verwenden, um ECMP nutzen zu können. Weitere Informationen zu Direct Connect-Gateways und öffentlichen virtuellen Schnittstellen finden Sie unter Wie richte ich eine aktive/aktive oder aktive/passive Direct Connect-Verbindung von einer öffentlichen virtuellen Schnittstelle AWS aus ein? .

Availability Zones

Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie eine oder mehrere Availability Zones aktivieren, die das Transit Gateway für die Weiterleitung des Datenverkehrs zu Ressourcen in den VPC-Subnetzen verwenden wird. Zur Aktivierung der einzelnen Availability Zones geben Sie genau ein Subnetz an. Das Transit Gateway platziert unter Verwendung einer IP-Adresse aus dem Subnetz eine Netzwerkschnittstelle in diesem Subnetz. Nach der Aktivierung einer Availability Zone kann Datenverkehr an alle Subnetze in der VPC geleitet werden, nicht nur an das angegebene Subnetz oder die Availability Zone. Allerdings können nur Ressourcen in Availability Zones mit Transit-Gateway-Anhang das Transit Gateway erreichen.

Wenn der Verkehr aus einer Availability Zone stammt, in der sich der Zielanhang nicht befindet, leitet AWS Transit Gateway diesen Datenverkehr intern an eine zufällige Availability Zone weiter, in der

der Anhang vorhanden ist. Für diese Art von Verkehr in der gesamten Availability Zone fallen keine zusätzlichen Transit-Gateway-Gebühren an.

Zur Sicherstellung der Verfügbarkeit sollten Sie mehrere Availability Zones aktivieren.

Verwenden des Applicance-Modus-Supports

Wenn Sie eine zustandsbehaftete Netzwerk-Appliance in Ihrer VPC konfigurieren möchten, können Sie die Unterstützung des Appliance-Modus für diese VPC-Anhänge, in welcher sich die Appliance befindet, aktivieren. Dadurch wird sichergestellt, dass das Transit Gateway während der gesamten Lebensdauer eines Verkehrsflusses zwischen Quelle und Ziel dieselbe Availability Zone für diese VPC-Anhänge verwendet. Dies ermöglicht dem Transit Gateway auch, Datenverkehr an jede Availability Zone in der VPC zu senden, solange in dieser Availability Zone eine Subnetz-Zuordnung vorhanden ist. Weitere Informationen finden Sie unter Beispiel: Appliance in einer VPC mit freigegeben Services.

Routing

Ihr Transit Gateway leitet IPv4- und IPv6-Pakete mithilfe von Transit-Gateway-Routing-Tabellen zwischen Anhängen weiter. Sie können diese Routing-Tabellen konfigurieren, damit Routen aus den Routing-Tabellen für die angehängten VPCs, VPN-Verbindungen und Direct Connect-Gateways propagiert werden. Sie können den Transit-Gateway-Routing-Tabellen auch statische Routen hinzufügen. Wenn ein Paket von einem Anhang ankommt, wird es anhand der Route, die seiner Ziel-IP-Adresse entspricht, an einen anderen Anhang weitergeleitet.

Für Transit-Gateway-Peering-Anhänge werden nur statische Routen unterstützt.

Inhalt

- Routing-Tabellen
- Routing-Tabellenzuordnung
- Routing-Propagierung
- Routen für Peering-Anhänge
- Reihenfolge der Routenauswertung

Routing-Tabellen

Ihr Transit Gateway verfügt automatisch über eine Standard-Routing-Tabelle. Diese Routing-Tabelle wird standardmäßig als Standard-Zuordnungs-Routing-Tabelle und standardmäßige Route-

Propagierung-Tabelle verwendet. Bei Deaktivierung der Route-Propagierung und Zuordnung der Routing-Tabelle erstellt AWS keine Standard-Routing-Tabelle für das Transit Gateway.

Sie können zusätzliche Routing-Tabellen für Ihr Transit Gateway erstellen. Auf diese Weise können Sie Teilmengen von Anhängen isolieren. Jeder Anhang kann einer Routing-Tabelle zugeordnet sein. Ein Anhang kann ihre Routen an eine oder mehrere Routing-Tabelle propagieren.

Sie können eine Blackhole-Route in Ihrer Transit-Gateway-Routing-Tabelle erstellen, die den Datenverkehr unterbricht, der der Route entspricht.

Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie der Subnetz-Routing-Tabelle eine Route hinzufügen, damit der Datenverkehr über das Transit Gateway weitergeleitet wird. Weitere Informationen finden Sie unter Routing für ein Transit Gateway im Amazon-VPC-Benutzerhandbuch.

Routing-Tabellenzuordnung

Ein Transit-Gateway-Anhang kann einer einzigen Routing-Tabelle zugeordnet werden. Jede Routing-Tabelle kann keiner, aber auch mehreren Anhängen zugeordnet werden und Pakete an Anhänge oder andere Routing-Tabellen weiterleiten.

Routing-Propagierung

Jeder Anhang bietet Routen, die in einer oder mehreren Transit-Gateway-Routing-Tabellen installiert werden können. Wenn ein Anhang auf eine Transit-Gateway-Routing-Tabelle übertragen wird, werden diese Routen in der Routing-Tabelle installiert. Sie können nicht nach angekündigten Routen filtern.

Bei einem VPC-Anhang werden die CIDR-Blöcke der VPC an die Routing-Tabelle des Transit Gateways weitergegeben.

Wenn dynamisches Routing mit einem VPN-Anhang oder einer Direct-Connect-Gateway-Anhang verwendet wird, können Sie die vom On-Premises-Router über BGP erlernten Routen zu einer Transit-Gateway-Routing-Tabelle übertragen.

Wenn dynamisches Routing mit einem VPN-Anhang verwendet wird, werden die Routen in der Routing-Tabelle, die dem VPN-Anhang zugeordnet ist, über BGP dem Kunden-Gateway angekündigt.

Für einen Connect-Anhang werden Routen in der mit dem Connect-Anhang verbundenen Routing-Tabelle an virtuelle Appliances von Drittanbietern wie SD-WAN-Appliances angekündigt, die in einer VPC über BGP ausgeführt werden.

Bei einem Direct Connect-Gateway-Anhang steuern zulässige Präfixe, von welchen Routen aus das Kundennetzwerk angekündigt wird. AWS

Wenn eine statische Route und eine propagierte Route das gleiche Ziel haben, hat die statische Route die höhere Priorität, sodass die propagierte Route nicht in der Routing-Tabelle enthalten ist. Wenn Sie die statische Route entfernen, wird die überlappende propagierte Route in die Routing-Tabelle aufgenommen.

Routen für Peering-Anhänge

Sie können für zwei Transit Gateways Peering durchführen und den Verkehr zwischen ihnen weiterleiten. Dazu erstellen Sie einen Peering-Anhang auf Ihrem Transit Gateway und geben das Peer-Transit-Gateway an, mit dem die Peering-Verbindung erstellt werden soll. Anschließend erstellen Sie eine statische Route in der Transit-Gateway-Routing-Tabelle, um Datenverkehr an den Transit-Gateway-Peering-Anhang weiterzuleiten. Datenverkehr, der an das Peer-Transit-Gateway weitergeleitet wird, kann dann an die VPC- und VPN-Anhänge für das Peer-Transit-Gateway weitergeleitet werden.

Weitere Informationen finden Sie unter Beispiel: Per Peering verbundene Transit Gateways.

Reihenfolge der Routenauswertung

Transit-Gateway-Routen werden in der folgenden Reihenfolge ausgewertet:

- die spezifischste Route für die Zieladresse.
- Für Routen mit derselben Ziel-IP-Adresse, aber unterschiedlichen Zielen ist die Routenpriorität wie folgt:
  - Statische Routen (z. B. statische Site-to-Site-VPN-Routen)
  - Präfixlisten referenzierter Routen
  - Von VPC propagierte Routen
  - Von Direct-Connect-Gateway propagierte Routen
  - Von Transit-Gateway-Connect propagierte Routen
  - Private weitergegebene Site-to-Site-VPN-Routen
  - Von Standort zu Standort übertragene öffentliche VPN-Routen
  - Durch Transit-Gateway-Peering propagierte Routen (Cloud WAN)

Transit Gateway zeigt nur eine bevorzugte Route an. Eine Sicherungsroute wird nur in der Transit Gateway-Routentabelle angezeigt, wenn diese Route nicht mehr angekündigt wird. Zum Beispiel, wenn Sie dieselben Routen über das Direct Connect-Gateway und über Site-to-Site VPN bewerben. AWS Transit Gateway zeigt nur die Routen an, die von der Direct Connect-Gateway-Route empfangen wurden, was die bevorzugte Route ist. Das Site-to-Site VPN, bei dem es sich um die Backup-Route handelt, wird nur angezeigt, wenn das Direct Connect-Gateway nicht mehr angekündigt wird.

Unterschiede in der Routentabelle von VPC und Transit Gateway

Die Auswertung von Routentabellen unterscheidet sich je nachdem, ob Sie eine VPC-Routentabelle oder eine Transit-Gateway-Routentabelle verwenden.

Das folgende Beispiel zeigt eine VPC-Routentabelle. Die lokale VPC-Route hat höchste Priorität, gefolgt von den Routen, die am spezifischsten sind. Wenn eine statische und eine propagierte Route dasselbe Ziel haben, hat die statische Route eine höhere Priorität.

Zielbereich	Ziel	Priorität
10.0.0.0/16	Lokal	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (statisch) oder tgw-12345 (statisch)	2
172.31.0.0/16	vgw-12345 (propagiert)	3
0.0.0.0/0	igw-12345	4

Das folgende Beispiel zeigt eine Transit-Gateway-Routentabelle. Wenn Sie den AWS Direct Connect -Gateway-Anhang vor dem VPN-Anhang verwenden möchten, verwenden Sie eine BGP-VPN-Verbindung und propagieren Sie die Routen in der Transit-Gateway-Routing-Tabelle.

Zielbereich	Anhang (Ziel)	Ressourcentyp	Routing-Typ	Priorität
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Statisch oder propagiert	1

Zielbereich	Anhang (Ziel)	Ressourcentyp	Routing-Typ	Priorität
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Statisch	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect Gateway	Propagiert	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Verbinden	Propagiert	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagiert	5

Erste Schritte mit Transit Gateways

Die folgenden Aufgaben helfen Ihnen, sich mit Transit Gateways vertraut zu machen. Sie erstellen ein Transit Gateway und verbinden dann zwei Ihrer VPCs über das Transit Gateway.

Aufgaben

- Voraussetzungen
- Schritt 1: Erstellen des Transit Gateway
- Schritt 2: Anhängen Ihrer VPCs an Ihre Transit Gateways
- Schritt 3: Hinzufügen von Routen zwischen dem Transit Gateway und Ihren VPCs
- Schritt 4: Testen des Transit Gateways
- Schritt 5: Löschen des Transit Gateway

Voraussetzungen

- Zur Veranschaulichung eines einfachen Beispiels für die Verwendung eines Transit Gateways müssen zwei VPCs in der gleichen Region erstellt werden. Die VPCs dürfen keine überlappenden CIDRs haben. Starten Sie eine Amazon-EC2-Instance in jeder VPC. Weitere Informationen finden Sie unter Erste Schritte mit Amazon VPC im Amazon-VPC-Benutzerhandbuch.
- Identische Routen, die auf zwei unterschiedliche VPCs verweisen, sind nicht zulässig. Ein Transit Gateway propagiert die CIDRs einer neu angefügten VPC nicht, wenn in den Routing-Tabellen des Transit Gateways eine identische Route vorhanden ist.
- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen zum Arbeiten mit Transit Gateways verfügen. Weitere Informationen finden Sie unter Identity and Access Management für Ihre Transit Gateways.
- Sie können nicht zwischen Hosts pingen, wenn Sie keiner der Host-Sicherheitsgruppen eine ICMP-Regel hinzugefügt haben. Weitere Informationen finden Sie unter Arbeiten mit Sicherheitsgruppen im Amazon-VPC-Benutzerhandbuch.

Schritt 1: Erstellen des Transit Gateway

Wenn Sie ein Transit Gateway erstellen, erstellen wir eine Standard-Transit-Gateway-Routing-Tabelle und verwenden sie als Standard-Zuordnungs-Routing-Tabelle und als standardmäßige Route-Propagierung-Tabelle.

So erstellen Sie ein Transit Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie in der Regionsauswahl die Region aus, die Sie beim Erstellen der VPCs verwendet haben.
3. Klicken Sie im Navigationsbereich auf Transit Gateways.
4. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.
5. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für das Transit Gateway ein. Dadurch wird ein Tag mit "Name" als Schlüssel und dem Namen, den Sie angegeben haben, als Wert erstellt.
6. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für das Transit Gateway ein.
7. Geben Sie bei Amazon side Autonomous System Number (ASN) (Amazon-seitige ASN) die private autonome Systemnummer (ASN) für Ihr Transit Gateway ein. Dabei sollte es sich um die ASN für die AWS-Seite einer BGP-Sitzung (Border Gateway Protocol) handeln.

   Für 16-Bit-ASNs liegt der Bereich zwischen 64 512 und 65 534.

   Für 32-Bit-ASNs liegt der Bereich zwischen 4 200 000 000 und 4 294 967 294.

   Für eine Multiregion-Bereitstellung empfehlen wir die Verwendung einer eindeutigen ASN für jedes Ihrer Transit Gateways.
8. (Optional) Sie können die Standardeinstellungen ändern, wenn Sie die DNS-Unterstützung deaktivieren müssen oder Sie die standardmäßige Zuordnungs-Routing-Tabelle oder standardmäßige Route-Propagierung-Tabelle nicht verwenden möchten.
9. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus. Wenn das Gateway erstellt wird, ist der Ausgangszustand des Transit-Gateways `pending`.

Schritt 2: Anhängen Ihrer VPCs an Ihre Transit Gateways

Warten Sie, bis das im vorherigen Abschnitt erstellte Transit Gateway als verfügbar angezeigt wird, bevor Sie mit dem Erstellen eines Anhangs beginnen. Erstellen Sie einen Anhang für jede VPC.

Vergewissern Sie sich, dass Sie zwei VPCs erstellt und eine EC2-Instance in jeder gestartet haben, wie in Voraussetzungen beschrieben.

Erstellen eines Transit-Gateway-Anhangs an eine VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. (Optional) Geben Sie unter Name tag (Namens-Tag) einen Namen für den Anhang ein.
5. Wählen Sie für Transit Gateway-ID das Transit Gateway aus, das für den Anhang verwendet werden soll.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
7. Wählen Sie aus, ob Sie DNS support (DNS-Unterstützung) aktivieren möchten. Für diese Übung wird IPv6 support (IPv6-Unterstützung) nicht aktiviert.
8. Wählen Sie für VPC ID die VPC aus, die dem Transit Gateway angehängt werden soll.
9. Wählen Sie für Subnet IDs (Subnetz-IDs) ein Subnetz für jede Availability Zone aus, die das Transit Gateway für die Weiterleitung des Datenverkehrs verwenden wird. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
10. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

Jeder Anhang ist immer genau einer Routing-Tabelle zugeordnet. Routing-Tabellen können keinem, aber auch mehreren Anhängen zugeordnet sein. Um die zu konfigurierenden Routen zu bestimmen, entscheiden Sie sich für den Anwendungsfall Ihres Transit Gateways und konfigurieren Sie dann die Routen. Weitere Informationen finden Sie unter Beispielanwendungsfälle.

Schritt 3: Hinzufügen von Routen zwischen dem Transit Gateway und Ihren VPCs

Eine Routing-Tabelle umfasst dynamische und statische Routen, die den nächsten Hop für zugeordnete VPCs basierend auf der Ziel-IP-Adresse des Pakets bestimmen. Konfigurieren Sie eine Route, die ein Ziel für nicht-lokale Routen und das Ziel der Transit-Gateway-Anhangs-ID hat. Weitere Informationen finden Sie unter Routing für ein Transit Gateway im Amazon-VPC-Benutzerhandbuch.

Hinzufügen einer Route zu einer VPC-Routing-Tabelle

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle aus, die Ihrer VPC zugeordnet ist.
4. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
5. Wählen Sie Add Route (Route hinzufügen) aus.
6. Geben Sie in der Spalte Destination (Ziel) den Ziel-IP-Adressbereich ein. Als Target (Ziel) wählen Sie Transit Gateway dann die ID des Transit-Gateways aus.
7. Wählen Sie Save Changes.

Schritt 4: Testen des Transit Gateways

Um zu überprüfen, ob das Transit Gateway erfolgreich erstellt wurde, können Sie eine Verbindung mit einer Amazon-EC2-Instance in jeder VPC herstellen und Daten zwischen ihnen senden, beispielsweise einen Ping-Befehl. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance oder unter Herstellen einer Verbindung mit Ihrer Windows-Instance.

Schritt 5: Löschen des Transit Gateway

Wenn Sie ein Transit Gateway nicht mehr benötigen, können Sie es löschen.

Transit Gateways mit angefügten Ressourcen können nicht gelöscht werden. Wenn Sie versuchen, ein Transit-Gateway mit Anhängen zu löschen, werden Sie aufgefordert, zuerst diese Anhänge zu löschen, bevor Sie das Transit-Gateway löschen können. Sobald das Transit Gateway gelöscht wurde, fallen keine Gebühren dafür mehr an.

So löschen Sie Ihr Transit Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das Transit-Gateway und dann Actions (Aktionen), Delete transit gateway (Transit-Gateway löschen) aus.
4. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

   Der State (Status) des Transit-Gateway auf der Seite Transit gateways (Transit-Gateways) lautet Deleting (Wird gelöscht). Nach dem Löschen wird das Transit-Gateway von der Seite entfernt.

Bewährte Methoden für das Transit-Gateway-Design

Im Folgenden finden Sie die bewährten Methoden für Ihr Transit-Gateway-Design:

- Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz. Verwenden Sie für jedes Subnetz einen kleinen CIDR, z. B. `/28`, damit Sie mehr Adressen für EC2-Ressourcen haben. Wenn Sie ein separates Subnetz verwenden, können Sie Folgendes konfigurieren:
  - Halten Sie die eingehende und ausgehende Netzwerk-ACLs offen, die den Transit-Gateway-Subnetzen zugeordnet sind.
  - Abhängig von Ihrem Datenfluss können Sie Netzwerk-ACLs auf Ihre Workload-Subnetze anwenden.
- Erstellen Sie eine Netzwerk-ACL und weisen Sie diese allen Subnetzen zu, die mit dem Transit Gateway verbunden sind. Halten Sie die Netzwerk-ACL sowohl in der Richtung für eingehenden als auch in der Richtung für ausgehender Datenverkehr geöffnet.
- Ordnen Sie dieselbe VPC-Routentabelle allen Subnetzen zu, die dem Transit Gateway zugeordnet sind, es sei denn, Ihr Netzwerkdesign erfordert mehrere VPC-Routing-Tabellen (z. B. eine Middlebox-VPC, die den Verkehr über mehrere NAT-Gateways weiterleitet).
- Verwenden Sie Site-to-Site-VPN-Verbindungen von Border Gateway Protocol (BGP). Wenn Ihr Kunden-Gateway-Gerät oder Ihre Firewall Mehrwegverbindungen für die Verbindung unterstützt, aktivieren Sie das Feature.
- Aktivieren Sie die Route-Propagierung für AWS Direct Connect Gateway-Anhänge und BGP Site-to-Site-VPN-Anhänge.
- Bei der Migration von VPC-Peering zur Verwendung eines Transit-Gateways. Eine Nichtübereinstimmung der MTU-Größe zwischen VPC-Peering und dem Transit Gateway kann dazu führen, dass einige Pakete für asymmetrischen Datenverkehr gelöscht werden. Aktualisieren Sie beide VPCs gleichzeitig, um zu vermeiden, dass Jumbo-Pakete aufgrund von Größenunterschieden gelöscht werden.
- Für die Hochverfügbarkeit benötigen Sie keine zusätzlichen Transit Gateways, da Transit Gateways speziell auf Hochverfügbarkeit ausgelegt sind.
- Begrenzen Sie die Anzahl der Transit-Gateway-Routing-Tabellen, es sei denn, Ihr Design erfordert mehrere Transit-Gateway-Routing-Tabellen.
- Verwenden Sie für die Redundanz ein einziges Transit Gateway in jeder Region für die Notfallwiederherstellung.

- Bei Bereitstellungen mit mehreren Transit Gateways empfehlen wir, dass Sie für jedes Ihrer Transit Gateways eine eindeutige autonome Systemnummer (ASN) verwenden. Sie können auch interregionales Peering verwenden. Weitere Informationen finden Sie unter Aufbau eines globalen Netzwerks mithilfe AWS Transit Gateway von regionsübergreifendem Peering.

Die folgenden Szenarien sind für Transit-Gateways

Die folgenden Szenarien sind gängige Anwendungsfälle für Transit-Gateways. Ihre Transit Gateways sind nicht auf diese Anwendungsfälle beschränkt.

Beispiele

- Beispiel: Zentralisierter Router
- Beispiel: Isolierte VPCs
- Beispiel: Isolierte VPCs mit freigegeben Services
- Beispiel: Per Peering verbundene Transit Gateways
- Beispiel: Zentralisiertes Outbound-Routing ins Internet
- Beispiel: Appliance in einer VPC mit freigegeben Services

Beispiel: Zentralisierter Router

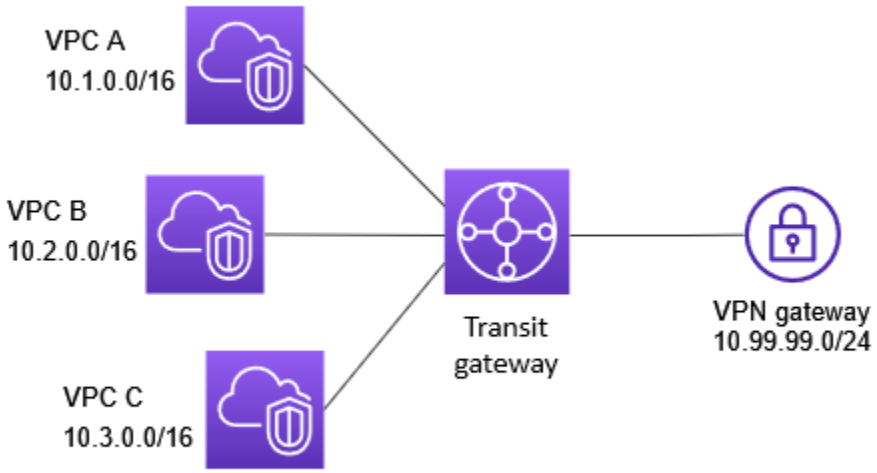
Sie können Ihr Transit Gateway als zentralisierten Router konfigurieren, der alle Ihre VPCs, AWS Direct Connect, und Site-to-Site-VPN-Verbindungen miteinander verbindet. In diesem Szenario sind alle Anhänge der standardmäßigen Transit-Gateway-Routing-Tabelle zugeordnet und propagieren an die standardmäßige Transit-Gateway-Routing-Tabelle. Daher können alle Anhänge Pakete untereinander weiterleiten, wobei das Transit Gateway dient als einfacher Layer-3-IP-Router dient.

Inhalt

- Übersicht
- Ressourcen
- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. In diesem Szenario gibt es drei VPC-Anhänge und einen Site-to-Site-VPN-Anhang an das Transit Gateway. Pakete aus den Subnetzen in VPC A, VPC B und VPC C, die für ein Subnetz in einer anderen VPC oder für die VPN-Verbindung bestimmt sind, werden zuerst an das Transit Gateway gesendet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
- Drei VPC-Anhänge im Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
- Ein Site-to-Site-VPN-Anhang auf dem Transit Gateway. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Wenn die VPN-Verbindung besteht, wird die BGP-Sitzung hergestellt und das Site-to-Site-VPN-CIDR wird auf die Transit-Gateway-Routing-Tabelle übertragen. Die VPC-CIDRs werden dann der Kunden-Gateway-BGP-Tabelle hinzugefügt. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”.

  Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN-Benutzerhandbuch.

Routing

Jede VPC hat eine Routing-Tabelle und es ist eine Routing-Tabelle für das Transit Gateway vorhanden.

VPC-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für lokales IPv4-Routing in der VPC; dieser Eintrag befähigt die Instances in dieser VPC miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Ziel
10.1.0.0/16	Lokal
0.0.0.0/0	tgw-id

Routing-Tabelle für Transit Gateway

Folgendes ist ein Beispiel für eine Standard-Routing-Tabelle für die Anhänge aus der vorherigen Grafik. Die Routing-Verbreitung ist aktiviert.

Zielbereich	Ziel	Routing-Typ
10.1.0.0/16	*Anfügung für VPC A*	propagiert
10.2.0.0/16	*Anfügung für VPC B*	propagiert
10.3.0.0/16	*Anfügung für VPC C*	propagiert
10.99.99.0/24	*Anfügung für VPN-Verbindung*	verbreitet

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

Beispiel: Isolierte VPCs

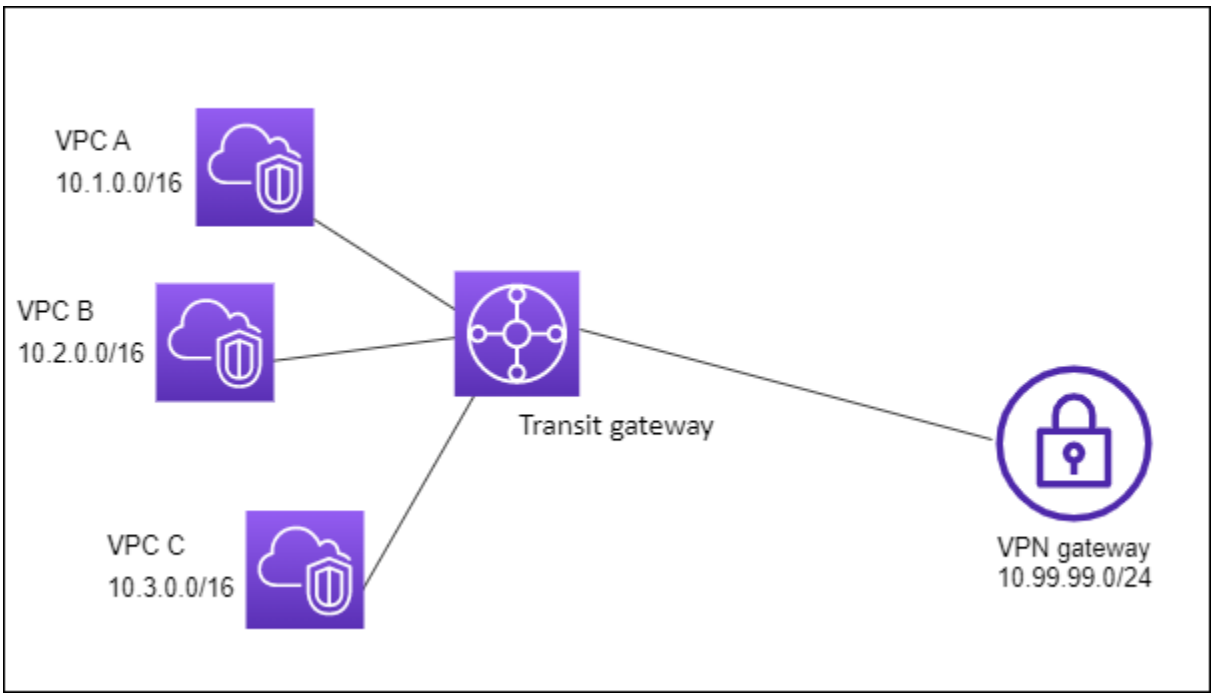
Sie können Ihr Transit-Gateway als mehrere isolierte Router konfigurieren. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern. In diesem Szenario verfügt jeder isolierte Router über eine einzige Routing-Tabelle. Alle Anfügungen, die diesem isolierten Router zugeordnet sind, verbreiten mit seiner Routing-Tabelle und werden ihr zugeordnet. Die Anfügungen, die einem isolierten Router zugeordnet sind, können Pakete untereinander weiterleiten. Sie können aber keine Pakete an Anfügungen eines anderen isolierten Routers leiten oder Pakete von ihnen empfangen.

Inhalt

- Übersicht
- Ressourcen
- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Pakete von VPC A, VPC B und VPC C werden an das Transit-Gateway weitergeleitet. Pakete von den Subnetzen in VPC A, VPC B und VPC C, die das Internet als Ziel haben, werden zuerst an das Transit-Gateway und dann an die Site-to-Site VPN-Verbindung weitergeleitet (wenn sich das Ziel innerhalb dieses Netzwerks befindet). Pakete von einer VPC, die als Ziel ein Subnetz in einer anderen VPC haben, z. B. von 10.1.0.0 nach 10.2.0.0, werden über das Transit-Gateway weitergeleitet, wo sie blockiert werden, da für sie keine Route in der Transit-Gateway-Routing-Tabelle vorhanden ist.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
- Drei Anfügungen im Transit-Gateway für die drei VPCs. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
- Ein Site-to-Site-VPN-Anhang auf dem Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”. Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN-Benutzerhandbuch.

Wenn die VPN-Verbindung besteht, wird die BGP-Sitzung hergestellt und das VPN-CIDR wird auf die Transit-Gateway-Routing-Tabelle übertragen. Die VPC-CIDRs werden dann der BGP-Kunden-Gateway-Tabelle hinzugefügt.

Routing

Jede VPC verfügt über eine Routing-Tabelle, und das Transit-Gateway über zwei Routing.Tabellen – eine für die VPCs und eine für die VPN-Verbindung.

Routing-Tabellen VPC A, VPC B und VPC C

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Dieser Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Ziel
10.1.0.0/16	Lokal
0.0.0.0/0	tgw-id

Transit-Gateway-Routing-Tabellen

In diesem Szenario werden eine Routing-Tabelle für die VPCs und eine Routing-Tabelle für die VPN-Verbindung verwendet.

Die VPC-Anhänge sind der folgenden Routing-Tabelle zugeordnet, die eine weitergegebene Route für den VPN-Anhang enthält.R

Zielbereich	Ziel	Routing-Typ
10.99.99.0/24	*Anfügung für VPN-Verbindung*	propagiert

Der VPN-Anhang ist der folgenden Routing-Tabelle zugeordnet, in der die Routen für die einzelnen VPC-Anhänge verteilt wurden.

Zielbereich	Ziel	Routing-Typ

Zielbereich	Ziel	Routing-Typ
10.1.0.0/16	*Anfügung für VPC A*	propagiert
10.2.0.0/16	*Anfügung für VPC B*	propagiert
10.3.0.0/16	*Anfügung für VPC C*	propagiert

Weitere Informationen zum Übertragen von Routen in einer Transit-Gateway-Routing-Tabelle finden Sie unter Verbreiten einer Route an eine Transit-Gateway-Routing-Tabelle.

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

Beispiel: Isolierte VPCs mit freigegeben Services

Sie können Ihr Transit-Gateway als mehrere isolierte Router konfigurieren, die einen freigegebenen Service verwenden. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern. In diesem Szenario verfügt jeder isolierte Router über eine einzige Routing-Tabelle. Alle Anfügungen, die diesem isolierten Router zugeordnet sind, verbreiten mit seiner Routing-Tabelle und werden ihr zugeordnet. Die Anfügungen, die einem isolierten Router zugeordnet sind, können Pakete untereinander weiterleiten. Sie können aber keine Pakete an Anfügungen eines anderen isolierten Routers leiten oder Pakete von ihnen empfangen. Anfügungen können Pakete an freigegebene Services weiterleiten oder sie davon empfangen. Sie können dieses Szenario verwenden, wenn Sie Gruppen haben, die isoliert sein müssen, aber einen freigegebenen Service verwenden, z. B. ein Produktionssystem.

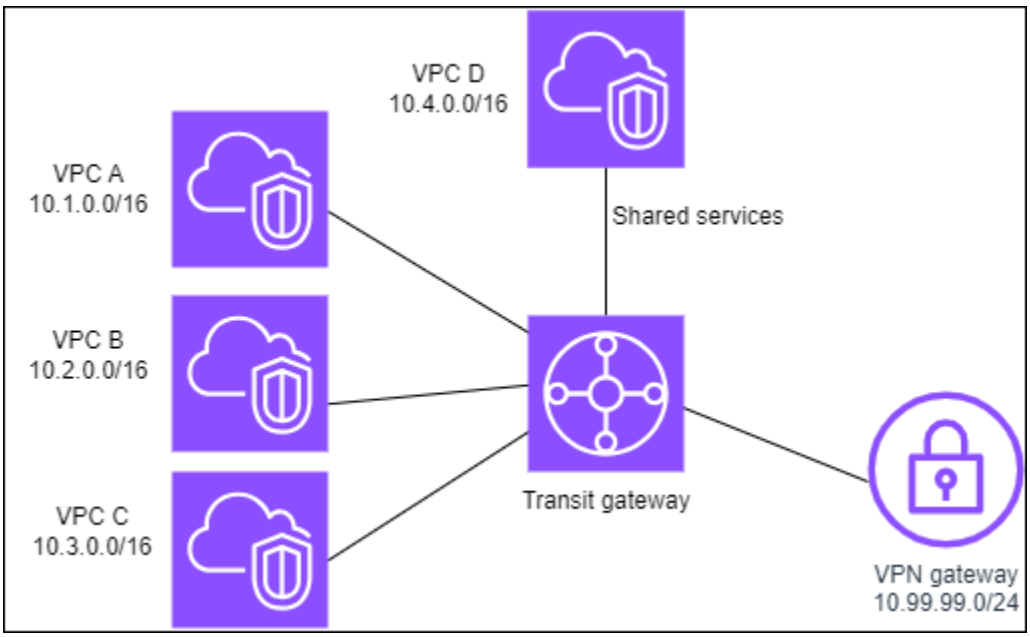
Inhalt

- Übersicht
- Ressourcen

- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Pakete von den Subnetzen in VPC A, VPC B und VPC C, die das Internet als Ziel haben, werden zuerst über das Transit-Gateway und dann an das Kunden-Gateway für Site-to-Site VPN weitergeleitet. Pakete aus Subnetzen in VPC A, VPC B oder VPC C, die als Ziel ein Subnetz in VPC A, VPC B oder VPC C haben, werden über das Transit-Gateway weitergeleitet, in dem sie blockiert werden, da für sie in der Transit-Gateway-Routing-Tabelle keine Route vorhanden ist. Pakete aus VPC A, VPC B und VPC C, die VPC D als Zielroute haben, werden über das Transit-Gateway und dann an VPC D weitergeleitet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Vier VPCs. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.
- Ein Transit-Gateway. Weitere Informationen finden Sie unter Erstellen eines Transit-Gateways.
- Vier Anhänge im Transit Gateway, eine pro VPC. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
- Ein Site-to-Site-VPN-Anhang auf dem Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”.

Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN-Benutzerhandbuch.

Wenn die VPN-Verbindung besteht, wird die BGP-Sitzung hergestellt und das VPN-CIDR wird auf die Transit-Gateway-Routing-Tabelle übertragen. Die VPC-CIDRs werden dann der BGP-Kunden-Gateway-Tabelle hinzugefügt.

- Jede isolierte VPC wird der isolierten Routing-Tabelle zugeordnet und an die freigegebene Routing-Tabelle weitergegeben.
- Jede freigegebene Services-VPC wird der freigegebenen Routing-Tabelle zugeordnet und an beide Routing-Tabellen weitergegeben.

Routing

Jede VPC besitzt eine Routing-Tabelle, und das Transit-Gateway verfügt über zwei Routing-Tabellen – eine für die VPCs und eine für die VPN-Verbindung und VPC freigegebener Services.

VPC A-, VPC B-, VPC C- und VPC-D-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit zwei Einträgen. Der erste Eintrag ist der Standardeintrag für lokales Routing in der VPC; dieser Eintrag befähigt die Instances in der VPC miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Ziel
10.1.0.0/16	Lokal
0.0.0.0/0	*Transit-Gateway-ID*

Transit-Gateway-Routing-Tabellen

In diesem Szenario werden eine Routing-Tabelle für die VPCs und eine Routing-Tabelle für die VPN-Verbindung verwendet.

Die VPC A-, B- und C-Anhänge sind der folgenden Routing-Tabelle zugeordnet, die eine propagierte Route für den VPN-Anhang und eine propagierte Route für den Anhang für VPC D enthält.

Zielbereich	Ziel	Routing-Typ
10.99.99.0/24	*Anfügung für VPN-Verbindung*	propagiert
10.4.0.0/16	*Anfügung für VPC D*	verbreitet

Der VPN-Anhang und Anhänge der VPC mit freigegebenen Services (VPC D) sind der folgenden Routing-Tabelle zugeordnet, die Einträge enthält, die auf die einzelnen VPC-Anhänge verweisen. Dies ermöglicht die Kommunikation mit den VPCs von der VPN-Verbindung und der VPC mit freigegebenen Services.

Zielbereich	Ziel	Routing-Typ
10.1.0.0/16	*Anfügung für VPC A*	propagiert
10.2.0.0/16	*Anfügung für VPC B*	propagiert
10.3.0.0/16	*Anfügung für VPC C*	verbreitet

Weitere Informationen finden Sie unter Verbreiten einer Route an eine Transit-Gateway-Routing-Tabelle.

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält CIDRs für alle vier VPCs.

Beispiel: Per Peering verbundene Transit Gateways

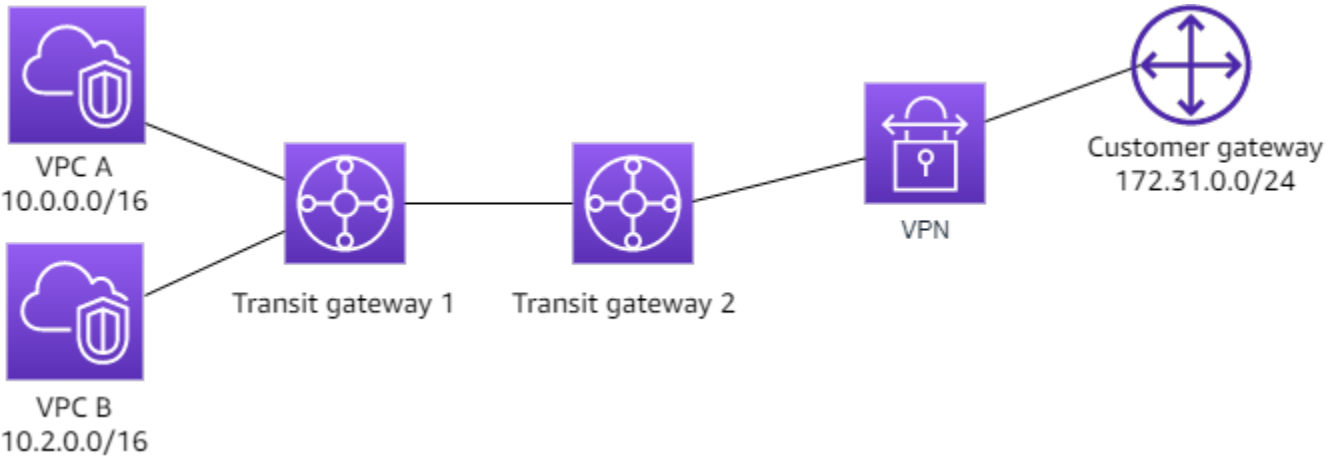
Sie können eine Transit Gateway-Peering-Verbindung zwischen Transit Gateways erstellen. Anschließend können Sie den Datenverkehr zwischen den Anlagen für jedes Transit Gateway weiterleiten. In diesem Szenario sind alle VPC- und VPN-Anhänge den standardmäßigen Transit-Gateway-Routing-Tabellen zugeordnet und an die standardmäßige Transit-Gateway-Routing-Tabelle geleitet. Jede Transit-Gateway-Routing-Tabelle verfügt über eine statische Route, die auf den Peering-Anhang des Transit Gateways verweist.

Inhalt

- Übersicht
- Ressourcen
- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Das Transit Gateway 1 verfügt über zwei VPC-Anhänge und das Transit Gateway 2 über einen Site-to-Site-VPN-Anhang. Pakete aus den Subnetzen in VPC A und VPC B, die das Internet als Ziel haben, werden zuerst durch das Transit Gateway 1, dann durch das Transit Gateway 2 und schließlich an die VPN-Verbindung weitergeleitet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Zwei VPCs. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.
- Zwei Transit Gateways. Sie können sich in derselben Region oder in verschiedenen Regionen befinden. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
- Zwei VPC-Anhänge auf dem ersten Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
- Ein Site-to-Site-VPN-Anhang auf dem zweiten Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”. Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN-Benutzerhandbuch.

- Ein Transit-Gateway-Peering-Anhang zwischen den beiden Transit Gateways. Weitere Informationen finden Sie unter Transit-Gateway-Peering-Anlagen.

Wenn Sie den VPC-Anhang erstellen, werden die CIDRs für jede VPC auf die Routing-Tabelle für Transit Gateway 1 übertragen. Wenn die VPN-Verbindung besteht, werden die folgenden Aktionen ausgeführt:

- Die BGP-Sitzung wird eingerichtet
- Das Site-to-Site-VPN-CIDR wird automatisch auf die Routing-Tabelle für das Transit Gateway 2 geleitet.
- Die VPC-CIDRs werden der Kunden-Gateway-BGP-Tabelle hinzugefügt.

Routing

Jede VPC verfügt über eine Routing-Tabelle und jedes Transit Gateway hat ebenfalls eine Routing-Tabelle.

VPC-A- und VPC-B-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Mit diesem Standardeintrag können die Ressourcen in dieser VPC miteinander kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Ziel
10.0.0.0/16	Lokal
0.0.0.0/0	tgw-1-id

Transit-Gateway-Routing-Tabellen

Im Folgenden finden Sie ein Beispiel für die Standard-Routing-Tabelle für Transit Gateway 1 mit aktivierter Routen-Propagierung.

Zielbereich	Ziel	Routing-Typ
10.0.0.0/16	*Anhang-ID für VPC A*	verbreitet
10.2.0.0/16	*Anhang-ID für VPC B*	verbreitet
0.0.0.0/0	*Anhang-ID für Peering-Verbindung*	statisch

Im Folgenden finden Sie ein Beispiel für die Standard-Routing-Tabelle für Transit Gateway 2 mit aktivierter Routen-Propagierung.

Zielbereich	Ziel	Routing-Typ
172.31.0.0/24	*Anhang-ID für VPN-Verbindung*	propagiert
10.0.0.0/16	*Anhang-ID für Peering-Verbindung*	statisch
10.2.0.0/16	*Anhang-ID für Peering-Verbindung*	statisch

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

- 10.0.0.0/16
- 10.2.0.0/16

Beispiel: Zentralisiertes Outbound-Routing ins Internet

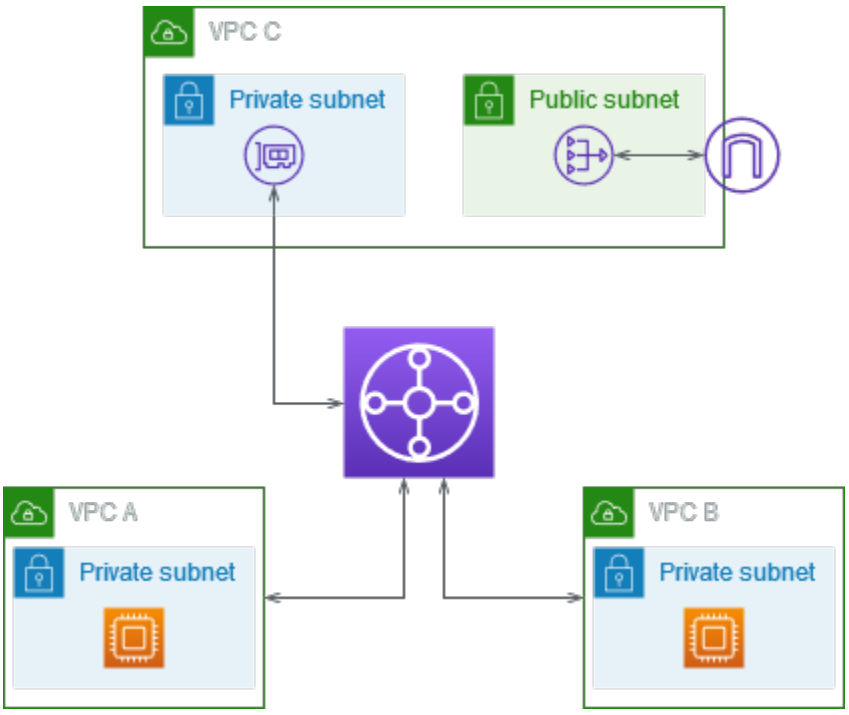
Sie können ein Transit-Gateway konfigurieren, um den ausgehenden Internetverkehr von einer VPC ohne Internet-Gateway an eine VPC zu leiten, die ein NAT-Gateway und ein Internet-Gateway enthält.

Inhalt

- Übersicht
- Ressourcen
- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Sie haben Anwendungen in VPC A und VPC B, die nur ausgehenden Internetzugang benötigen. Sie konfigurieren VPC C mit einem öffentlichen NAT-Gateway und einem Internet-Gateway sowie einem privaten Subnetz für den VPC-Anhang. Verbinden Sie alle VPCs mit einem Transit-Gateway. Konfigurieren Sie das Routing so, dass ausgehender Internetdatenverkehr von VPC A und VPC B das Transit Gateway zu VPC C durchquert. Das NAT-Gateway in VPC C leitet den Datenverkehr an das Internet-Gateway weiter.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs mit IP-Adressbereichen, die sich nicht überschneiden. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.

- VPC A und VPC B verfügen jeweils über private Subnetze mit EC2-Instances.
- VPC C verfügt über Folgendes:
  - Ein Internet-Gateway, das an die VPC angefügt ist. Weitere Informationen finden Sie unter Erstellen und Anfügen eines Internet-Gateways im Amazon-VPC-Benutzerhandbuch.
  - Ein öffentliches Subnetz mit einem NAT-Gateway. Weitere Informationen finden Sie unter Erstellen und Anfügen eines NAT-Gateways im Amazon-VPC-Benutzerhandbuch.
  - Ein privates Subnetz für den Transit-Gateway-Anhang. Das private Subnetz sollte sich in derselben Availability Zone wie das öffentliche Subnetz befinden.
- Ein Transit-Gateway Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
- Drei VPC-Anhänge im Transit Gateway. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”. Für VPC C müssen Sie den Anhang mithilfe des privaten Subnetzes erstellen. Wenn Sie den Anhang mithilfe des öffentlichen Subnetzes erstellen, wird der Instance-Datenverkehr an das Internet-Gateway weitergeleitet, aber das Internet-Gateway lehnt den Datenverkehr ab, da die Instances keine öffentlichen IP-Adressen haben. Durch das Platzieren des Anhangs im privaten Subnetz wird der Datenverkehr an das NAT-Gateway weitergeleitet, und das NAT-Gateway sendet über die Elastic IP-Adresse als Quell-IP-Adresse den Datenverkehr an das öffentliche Internet-Gateway.

Routing

Es gibt Routing-Tabellen für jede VPC und eine Routing-Tabelle für das Transit Gateway.

Routing-Tabellen

- Routing-Tabelle für VPC A
- Routing-Tabelle für VPC B
- Routing-Tabellen für VPC C
- Routing-Tabelle für Transit Gateway

Routing-Tabelle für VPC A

Es folgt ein Beispiel für eine Routing-Tabelle. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Ziel
VPC A CIDR	Lokal
0.0.0.0/0	*Transit-Gateway-ID*

Routing-Tabelle für VPC B

Es folgt ein Beispiel für eine Routing-Tabelle. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Ziel
VPC B CIDR	Lokal
0.0.0.0/0	*Transit-Gateway-ID*

Routing-Tabellen für VPC C

Konfigurieren Sie das Subnetz mit dem NAT-Gateway als öffentliches Subnetz, indem Sie dem Internet-Gateway eine Route hinzufügen. Das andere Subnetz bleibt ein privates Subnetz.

Im Folgenden finden Sie ein Beispiel einer Routing-Tabelle für das öffentliche Subnetz. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Die zweiten und dritten Einträge leiten Datenverkehr für VPC A und VPC B zum Transit Gateway. Der verbleibende Eintrag leitet den übrigen IPv4-Datenverkehr des Subnetzes an das Internet-Gateway.

Zielbereich	Ziel
VPC C CIDR	Lokal
VPC A CIDR	*Transit-Gateway-ID*

Zielbereich	Ziel
VPC B CIDR	*Transit-Gateway-ID*
0.0.0.0/0	*internet-gateway-id*

Das Folgende ist ein Beispiel einer Routing-Tabelle für das private Subnetz. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das NAT-Gateway weiter.

Zielbereich	Ziel
VPC C CIDR	Lokal
0.0.0.0/0	*nat-gateway-id*

Routing-Tabelle für Transit Gateway

Es folgt ein Beispiel für die Routing-Tabelle des Transit-Gateways. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Sie können die Kommunikation zwischen VPC C optional verhindern, indem Sie ein Blackhole-Routing für jede VPC CIDR hinzufügen.

CIDR	Attachment	Routing-Typ
VPC A CIDR	*Anfügung für VPC A*	propagiert
VPC B CIDR	*Anfügung für VPC B*	propagiert
VPC C CIDR	*Anfügung für VPC C*	propagiert
0.0.0.0/0	*Anfügung für VPC C*	statisch

Beispiel: Appliance in einer VPC mit freigegeben Services

Sie können in einer VPC freigegebener Services eine Appliance (z. B. eine Sicherheits-Appliance) konfigurieren. Der gesamte Datenverkehr, der zwischen Transit-Gateway-Anhängen weitergeleitet wird, wird zuerst von der Appliance in der VPC freigegebener Services überprüft. Wenn der Appliance-Modus aktiviert ist, wählt ein Transit Gateway eine einzelne Netzwerkschnittstelle in der Appliance-VPC unter Verwendung eines Flow-Hash-Algorithmus aus, an die er während der gesamten Lebensdauer des Datenflusses Datenverkehr sendet. Das Transit Gateway verwendet dieselbe Netzwerkschnittstelle für den Rückverkehr. Dadurch wird sichergestellt, dass der bidirektionale Datenverkehr symmetrisch weitergeleitet wird – er wird während der gesamten Lebensdauer des Datenflusses durch dieselbe Availability Zone in den VPC-Anhang weitergeleitet. Wenn Sie mehrere Transit Gateways in Ihrer Architektur haben, behält jedes Transit Gateway seine eigene Sitzungsaffinität bei und jedes Transit Gateway kann eine andere Netzwerkschnittstelle auswählen.

Sie müssen genau ein Transit Gateway mit der Appliance-VPC verbinden, um die Flow-Stickiness zu gewährleisten. Durch das Verbinden mehrerer Transit Gateways mit einer einzelnen Appliance-VPC wird die Flow-Stickiness nicht gewährleistet, da die Transit Gateways keine Flussstatusinformationen miteinander teilen.

Important

- Der Datenverkehr im Appliance-Modus wird korrekt weitergeleitet, solange der Quell- und Zieldatenverkehr von demselben Transit-Gateway-Anhang auf eine zentrale VPC (Inspection VPC) gelangt. Der Datenverkehr kann gelöscht werden, wenn Quelle und Ziel von zwei verschiedenen Transit-Gateway-Anhängen eingehen. Der Appliance-Modus gilt nicht für Datenverkehr, der über ein VPN in das Netzwerk gelangt.
- Das Aktivieren des Appliance-Modus für einen vorhandenen Anhang kann sich auf die aktuelle Route dieses Anhangs auswirken, da der Anhang durch jede Availability Zone fließen kann. Wenn der Appliance-Modus nicht aktiviert ist, wird der Datenverkehr in der ursprünglichen Availability Zone beibehalten.

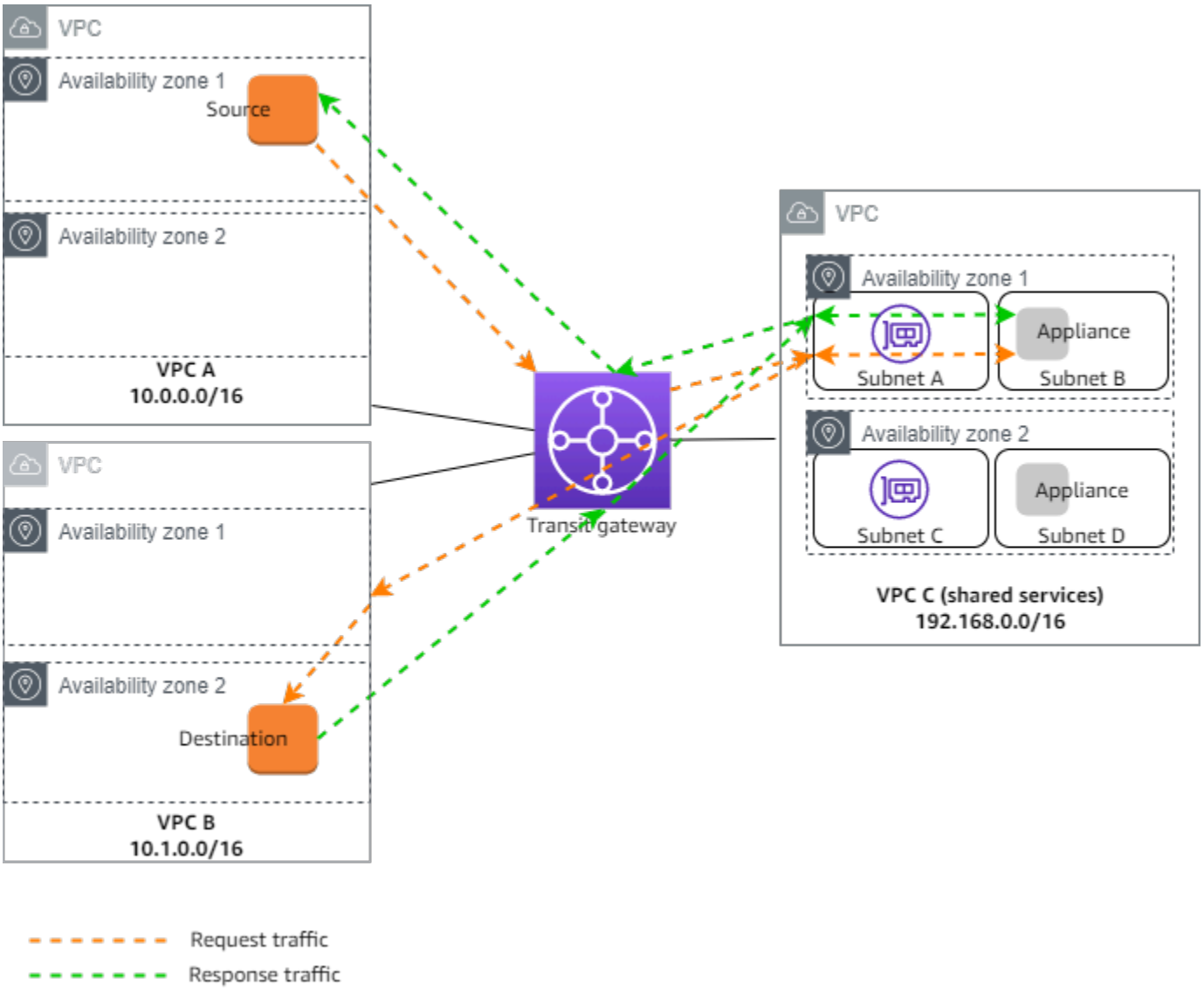
Inhalt

- Übersicht
- Statusbehaftete Appliances und Appliance-Modus

- Routing

Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Das Transit Gateway hat drei VPC-Anhänge. VPC C ist eine freigegebene Services-VPC. Der Datenverkehr zwischen VPC A und VPC B wird an das Transit Gateway und dann zur Überprüfung an eine Sicherheits-Appliance in VPC C weitergeleitet, bevor er zum endgültigen Ziel weitergeleitet wird. Da die Appliance ist eine zustandsbehaftete Appliance ist, wird sowohl der Anforderungs- als auch der Antwortdatenverkehr überprüft. Für hohe Verfügbarkeit gibt es in jeder Availability Zone in VPC C eine Appliance.



Sie erstellen die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Informationen über das Erstellen einer VPC finden Sie unter Erstellen einer VPC im Amazon-Virtual-Private-Cloud-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
- Drei VPC-Anhänge – einer für jede der VPCs. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.

  Geben Sie für jeden VPC-Anhang ein Subnetz in jeder Availability Zone an. Für die VPC freigegebener Services sind dies die Subnetze, in denen der Datenverkehr vom Transit Gateway an die VPC geleitet wird. Im vorangehenden Beispiel sind dies Subnetze A und C.

  Aktivieren Sie für den VPC-Anhang für VPC C die Unterstützung des Appliance-Modus, damit der Antwortdatenverkehr an dieselbe Availability Zone in VPC C wie der Quelldatenverkehr weitergeleitet wird.

  Die Amazon-VPC-Konsole unterstützt den Appliance-Modus. Sie können auch die Amazon-VPC-API, ein AWS-SDK, die AWS CLI, um den Appliance-Modus zu aktivieren, oder AWS CloudFormation verwenden. Fügen Sie beispielsweise `--options ApplianceModeSupport=enable` zum Befehl create-transit-gateway-vpc-attachment oder modify-transit-gateway-vpc-attachment hinzu.

> **Note**
>
> Flow-Stickiness im Appliance-Modus ist nur für Quell- und Zieldatenverkehr gewährleistet, der von der Inspection-VPC ausgeht.

Statusbehaftete Appliances und Appliance-Modus

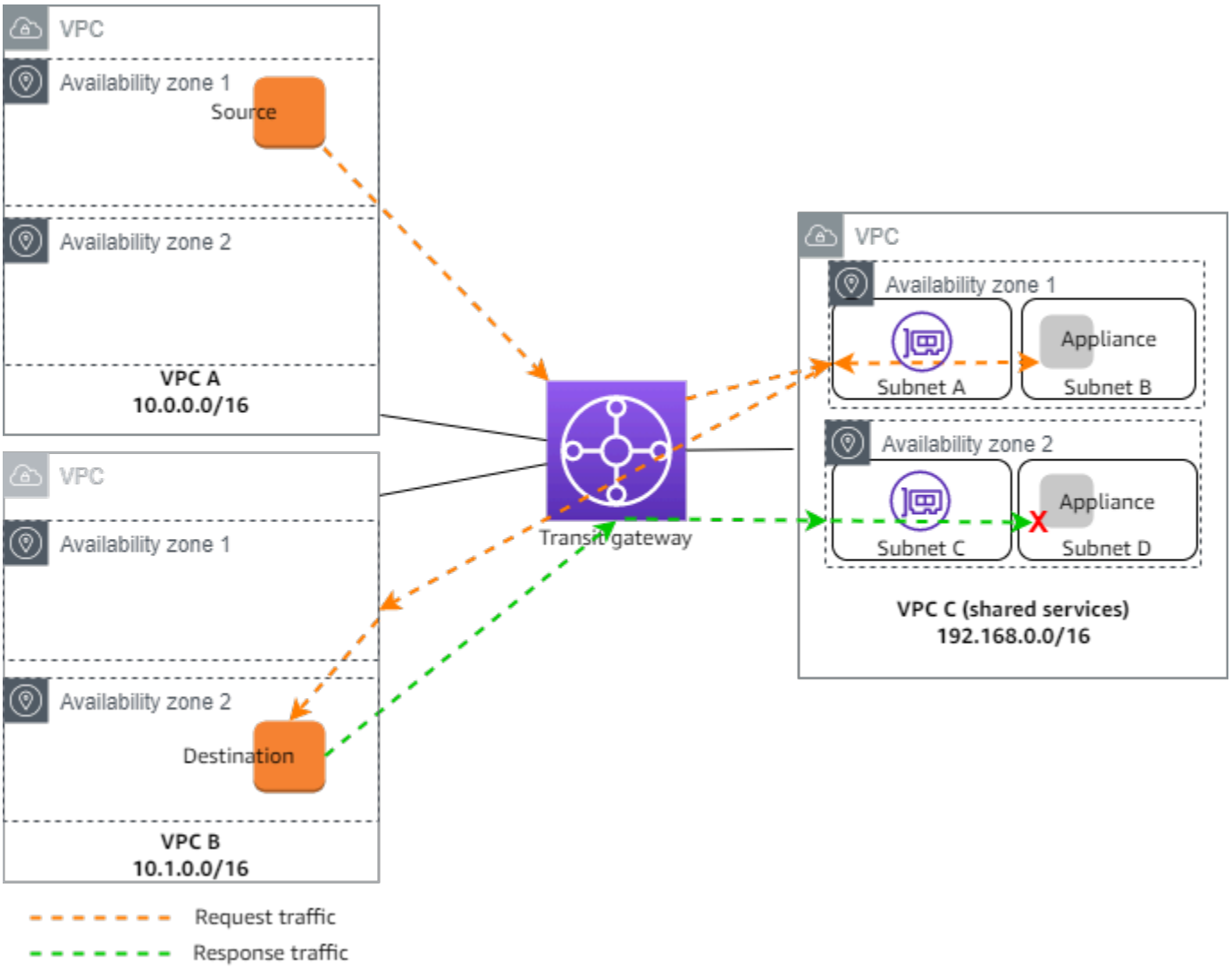
Wenn sich Ihre VPC-Anhänge über mehrere Availability Zones erstrecken und Sie verlangen, dass der Datenverkehr zwischen Quell- und Zielhosts zur zustandsbehafteten Prüfung über dieselbe Appliance geleitet wird, aktivieren Sie die Unterstützung des Appliance-Modus für den VPC-Anhang, in der sich die Appliance befindet.

Weitere Informationen finden Sie unter Zentralisierte Inspektionsarchitektur im AWS-Blog.

Verhalten bei nicht aktiviertem Appliance-Modus

Wenn der Appliance-Modus nicht aktiviert ist, versucht ein Transit Gateway, den Datenverkehr zwischen VPC-Anhängen in der ursprünglichen Availability Zone weitergeleitet zu halten, bis er sein Ziel erreicht. Der Datenverkehr durchquert Availability Zones zwischen Anhängen nur dann, wenn ein Availability Zone-Ausfall vorliegt oder wenn keine Subnetze mit einem VPC-Anhang in dieser Availability Zone verknüpft sind.

Das folgende Diagramm zeigt einen Datenverkehrsfluss, wenn die Unterstützung des Appliance-Modus nicht aktiviert ist. Der Antwortdatenverkehr, der von Availability Zone 2 in VPC B stammt, wird vom Transit Gateway zur gleichen Availability Zone in VPC C weitergeleitet. Der Datenverkehr wird daher unterbrochen, da der Appliance in Availability Zone 2 die ursprüngliche Anforderung von der Quelle in VPC A nicht bekannt ist.



Routing

Jede VPC verfügt über eine oder mehrere Routing-Tabellen und das Transit Gateway verfügt über zwei Routing-Tabellen.

VPC-Routing-Tabellen

VPC A und VPC B

VPCs A und B haben Routing-Tabellen mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Mit diesem Standardeintrag können die Ressourcen in dieser VPC miteinander kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Das Folgende ist die Routing-Tabelle für VPC A.

Zielbereich	Ziel
10.0.0.0/16	Lokal
0.0.0.0/0	tgw-id

VPC C

Die VPC freigegebener Services (VPC C) verfügt für jedes Subnetz über unterschiedliche Routing-Tabellen. Subnetz A wird vom Transit Gateway verwendet (Sie geben dieses Subnetz an, wenn Sie den VPC-Anhang erstellen). Die Routing-Tabelle für Subnetz A leitet den gesamten Datenverkehr an die Appliance im Subnetz B.

Zielbereich	Ziel
192.168.0.0/16	Lokal
0.0.0.0/0	appliance-eni-id

Die Routing-Tabelle für Subnetz B (die die Appliance enthält) leitet den Datenverkehr zurück zum Transit Gateway.

Zielbereich	Ziel
192.168.0.0/16	Lokal
0.0.0.0/0	tgw-id

Transit-Gateway-Routing-Tabellen

Dieses Transit Gateway verwendet eine Routing-Tabelle für VPC A und VPC B und eine Routing-Tabelle für die VPC freigegebener Services (VPC C).

Die VPC A- und VPC B-Anhänge sind der folgenden Routing-Tabelle zugeordnet. Die Routing-Tabelle leitet den gesamten Datenverkehr zu VPC C.

Zielbereich	Ziel	Routing-Typ
0.0.0.0/0	*Attachment-ID für VPC C*	statisch

Der VPC C-Anhang ist mit der folgenden Routing-Tabelle verknüpft. Sie leitet den Datenverkehr zu VPC A und VPC B.

Zielbereich	Ziel	Routing-Typ
10.0.0.0/16	*Anhang-ID für VPC A*	propagiert
10.1.0.0/16	*Anhang-ID für VPC B*	propagiert

Arbeiten mit Transit Gateways

Sie können Transit Gateways über die Amazon-VPC-Konsole oder die AWS CLI verwenden.

Inhalt

- Transit Gateways
- Transit-Gateway-Anhänge an eine VPC
- Transit-Gateway-VPN-Anhänge
- Transit-Gateway-Anhänge an ein Direct-Connect-Gateway
- Transit-Gateway-Peering-Anlagen
- Transit-Gateway-Connect-Anhänge und Transit-Gateway-Connect-Peers
- Transit-Gateway-Routing-Tabellen
- Transit-Gateway-Richtlinientabellen
- Multicast auf Transit Gateways

Transit Gateways

Ein Transit Gateway ermöglicht es Ihnen, VPCs und VPN-Verbindungen anzufügen und Datenverkehr zwischen ihnen weiterzuleiten. Ein Transit-Gateway funktioniert überall AWS-Konten, und Sie können es verwenden, AWS RAM um Ihr Transit-Gateway mit anderen Konten zu teilen. Nachdem Sie ein Transit-Gateway mit einem anderen geteilt haben AWS-Konto, kann der Kontoinhaber seine VPCs an Ihr Transit-Gateway anhängen. Benutzer in einem der Konten können die Anhang jederzeit löschen.

Sie können Multicast auf einem Transit Gateway aktivieren und dann eine Transit Gateway-Multicast-Domain erstellen, mit der Multicast-Datenverkehr von der Multicast-Quelle über VPC-Anhängen, die Sie der Domain zuordnen, an Multicast-Gruppenmitglieder gesendet werden kann.

Jede VPC- oder VPN-Anhang ist einer einzigen Routing-Tabelle zugeordnet. Diese Routing-Tabelle bestimmt den nächsten Hop für Datenverkehr, der von diesem Ressourcen-Anhang kommt. Eine Routing-Tabelle innerhalb des Transit Gateways unterstützt IPv4- oder IPv6-CIDRs und Ziele. Diese Ziele sind VPCs und VPN-Verbindungen. Wenn Sie eine VPC anhängen oder eine VPN-Verbindung auf einem Transit Gateway erstellen, wird der Anhang der Standard-Routing-Tabelle des Transit-Gateways zugeordnet.

Sie können zusätzliche Routing-Tabellen innerhalb des Transit Gateways erstellen und die VPC- oder VPN-Zuordnung auf diese Routing-Tabellen umstellen. Das ermöglicht Ihnen die Segmentierung Ihres Netzwerks. Sie können beispielsweise Entwicklungs-VPCs einer Routing-Tabelle zuordnen und Produktions-VPCs einer anderen. Auf diese Weise erstellen Sie innerhalb eines Transit Gateways isolierte Netzwerke, ähnlich dem Virtual Routing and Forwarding (VRFs) in herkömmlichen Netzwerken.

Transit Gateways unterstützen dynamisches und statisches Routing zwischen angefügten VPCs und VPN-Verbindungen. Sie können die Route-Propagierung für jeden Anhang aktivieren oder deaktivieren. Transit-Gateway-Peering-Anhänge unterstützen nur statisches Routing. Sie können jedoch keine statische Route hinzufügen, die auf ein Peering zwischen zwei Transit-Gateways in derselben Region verweist.

Sie können optional einen oder mehrere IPv4- oder IPv6-CIDR-Blöcke mit Ihrem Transit Gateway verknüpfen. Sie geben eine IP-Adresse aus dem CIDR-Block an, wenn Sie einen Transit-Gateway-Connect-Peer für einen Transit-Gateway-Connect-Anhang einrichten. Sie können jeden öffentlichen oder privaten IP-Adressbereich zuordnen, mit Ausnahme von Adressen im `169.254.0.0/16` Bereich und Bereichen, die sich mit den Adressen für Ihre VPC-Anhänge und On-Premises-Netzwerke überschneiden. Weitere Informationen zu IPv4- und IPv6-CIDR-Blöcken finden Sie unter VPC und Subnetze im Amazon VPC-Benutzerhandbuch.

Aufgaben

- Erstellen eines Transit Gateways
- Anzeigen Ihrer Transit Gateways
- Hinzufügen oder Bearbeiten von Tags für ein Transit Gateway
- Ändern eines Transit Gateways
- Freigabe eines Transit Gateways
- Akzeptieren einer Ressourcenfreigabe
- Akzeptieren eines freigegebenen Anhangs
- Löschen eines Transit Gateways

Erstellen eines Transit Gateways

Wenn Sie ein Transit Gateway erstellen, erstellen wir eine Standard-Transit Gateway-Routing-Tabelle und verwenden sie als Standard-Zuordnungs-Routing-Tabelle und als standardmäßige Route-Propagierung-Tabelle. Wenn Sie die Standard-Transit-Gateway-Routing-Tabelle nicht erstellen

möchten, können Sie später eine erstellen. Weitere Informationen über Routen und Routing-Tabellen finden Sie unter ???.

So erstellen Sie ein Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.
4. Geben Sie für Name tag (Namens-Tag) optional einen Namen für das Transit Gateway ein. Ein Namens-Tag kann die Identifizierung eines bestimmten Gateways in der Liste von Gateways erleichtern. Wenn Sie ein Name tag (Namens-Tag) hinzufügen, wird ein Tag mit dem Schlüssel Name und einem Wert erstellt, der dem von Ihnen eingegebenen Wert entspricht.
5. Geben Sie im Feld Description (Beschreibung) optional eine Beschreibung für das Transit Gateway ein.
6. Belassen Sie für Amazon side Autonomous System Number (ASN) (Amazon-seitige ASN) entweder den Standardwert, um die standardmäßige ASN zu verwenden, oder geben Sie die private ASN für Ihr Transit Gateway ein. Dies sollte die ASN für die AWS Seite einer Border Gateway Protocol (BGP) -Sitzung sein.

   Für 16-Bit-ASNs liegt der Bereich zwischen 64 512 und 65 534.

   Für 32-Bit-ASNs liegt der Bereich zwischen 4 200 000 000 und 4 294 967 294.

   Für eine Multiregion-Bereitstellung empfehlen wir die Verwendung einer eindeutigen ASN für jedes Ihrer Transit Gateways.
7. Bei DNS support (DNS-Unterstützung) wählen Sie diese Option aus, wenn die VPC bei Abfragen von Instances in einer anderen VPC, die dem Transit Gateway angefügt ist, öffentliche IPv4-DNS-Hostnamen in private IPv4-Adressen auflösen soll.
8. Wählen Sie diese Option bei VPN ECMP support (VPN-ECMP-Unterstützung), wenn ECMP-Routing (Equal Cost Multipath-Routing) zwischen VPN-Tunnel unterstützt werden soll. Wenn Verbindungen die gleichen CIDRs angeben, wird der Datenverkehr gleichmäßig zwischen ihnen aufgeteilt.

   Wenn Sie diese Option auswählen, müssen die angekündigte BGP ASN, die BGP-Attribute wie der AS-Pfad und die Communitys für Präferenzen dieselben sein.

> **Note**
>
> Zur Verwendung von ECMP müssen Sie eine VPN-Verbindung herstellen, die dynamisches Routing nutzt. VPN-Verbindungen, die statisches Routing nutzen, unterstützen ECMP nicht.

9. Wählen Sie diese Option für Default route table association (Standard-Routing-Tabellenzuordnung), damit Transit-Gateway-Anhänge automatisch der Standard-Routing-Tabelle für das Transit Gateway zugeordnet werden.
10. Wählen Sie diese Option für Default route table propagation (standardmäßige Route-Propagierung-Tabellenverbreitung), damit Transit-Gateway-Anhänge automatisch auf die Standard-Routing-Tabelle für das Transit Gateway übertragen werden.
11. (Optional) Um das Transit Gateway als Router für Multicast-Datenverkehr zu verwenden, wählen Sie Multicast support (Multicast-Unterstützung) aus.
12. Wählen Sie diese Option für Auto accept shared attachments (Gemeinsame Anhänge automatisch akzeptieren), um kontoübergreifende Anhänge automatisch zu akzeptieren.
13. (Optional) Geben Sie für CIDR-Blöcke mit Transit Gateway einen oder mehrere IPv4- oder IPv6-CIDR-Blöcke für Ihr Transit Gateway an.

    Sie können einen CIDR-Block der Größe /24 oder größer (z. B. /23 oder /22) für IPv4 oder einen CIDR-Block der Größe /64 oder größer (z. B. /63 oder /62) für IPv6 angeben. Sie können jeden öffentlichen oder privaten IP-Adressbereich zuordnen, mit Ausnahme von Adressen im Bereich von 169.254.0.0/16 und Bereichen, die sich mit den Adressen für Ihre VPC-Anhänge und On-Premises-Netzwerke überschneiden.
14. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.

Um ein Transit-Gateway mit dem zu erstellen AWS CLI

Verwenden Sie den create-transit-gateway-Befehl.

Anzeigen Ihrer Transit Gateways

So zeigen Sie Ihre Transit Gateways mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateways. Die Details für das Transit Gateway werden unter der Liste der Gateways auf der Seite angezeigt.

Um Ihre Transit-Gateways anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den describe-transit-gateways-Befehl.

Hinzufügen oder Bearbeiten von Tags für ein Transit Gateway

Fügen Sie Ihren Ressourcen-Tags hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können jedem Transit Gateway mehrere Tags hinzufügen. Tag-Schlüssel müssen für jedes Transit Gateway eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der dem Transit Gateway bereits zugeordnet ist, ändert sich der Wert dieses Tags. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen.

Hinzufügen von Tags zu einem Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das Transit Gateway aus, für das Sie Tags hinzufügen oder bearbeiten möchten.
4. Wählen Sie die Registerkarte Tags im unteren Bereich der Seite aus.
5. Wählen Sie Tags verwalten aus.
6. Wählen Sie Neues Tag hinzufügen aus.
7. Geben Sie einen Key (Schlüssel) und einen Value (Wert) für das Tag ein.
8. Wählen Sie Save (Speichern) aus.

Ändern eines Transit Gateways

Sie können die Konfigurationsoptionen für das Transit Gateway ändern. Wenn Sie einen Transit Gateway ändern, werden die geänderten Optionen nur auf neue Transit-Gateway-Anhänge angewendet. Die vorhandenen Transit-Gateway-Anhänge werden nicht geändert und es kommt zu keiner Betriebsunterbrechung.

Sie können kein Transit Gateway ändern, der für Sie freigegeben wurde.

Sie können einen CIDR-Block für das Transit-Gateway nicht entfernen, wenn eine der IP-Adressen derzeit für einen Connect-Peerverwendet wird.

So ändern Sie einen Transit Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das zu ändernde Transit Gateway aus.
4. Wählen Sie Aktionen, Ändern des Transit Gateways aus.
5. Ändern Sie die Optionen wie benötigt. Wählen Sie anschließend Modify transit gateway (Transit Gateway ändern) aus.

Um Ihr Transit-Gateway zu ändern, verwenden Sie AWS CLI

Verwenden Sie den modify-transit-gateway-Befehl.

Freigabe eines Transit Gateways

Sie können AWS RAM es verwenden, um ein Transit-Gateway kontenübergreifend oder unternehmensweit gemeinsam zu nutzen in AWS Organizations. Führen Sie die folgenden Schritte aus, um ein Transit Gateway freizugeben, das Ihnen gehört.

Sie müssen die Ressourcenfreigabe über das Hauptkonto Ihrer Organisation ermöglichen. Informationen zur Aktivierung der gemeinsamen Nutzung von Ressourcen finden Sie unter Aktivieren der gemeinsamen Nutzung mit AWS Organizations im AWS RAM Benutzerhandbuch.

So geben Sie ein Transit Gateway frei

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie Create a resource share (Ressourcenfreigabe erstellen) aus.
3. Geben Sie unter Name einen beschreibenden Namen für die Ressourcenfreigabe ein.
4. Wählen Sie bei Select resource type (Ressourcentyp auswählen) die Option Transit Gateways aus. Wählen Sie das Transit Gateway aus.
5. (Optional) Bei Principals (Prinzipale) können Sie der Ressource Prinzipale hinzufügen. Geben Sie für jede AWS-Konto Organisationseinheit oder Organisation ihre ID an und klicken Sie auf Hinzufügen.

   Wählen Sie unter Externe Konten zulassen aus, ob die gemeinsame Nutzung dieser Ressource mit AWS-Konten Personen außerhalb Ihrer Organisation zulässig sein soll.

6. (Optional) Geben Sie unter Tags ein Schlüssel-Wert-Paar für jedes Tag ein. Diese Tags werden auf die Ressourcenfreigabe, aber nicht auf das Transit Gateway angewendet.
7. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

Akzeptieren einer Ressourcenfreigabe

Wenn Sie zu einer Ressourcenfreigabe hinzugefügt wurden, erhalten Sie eine Einladung, um der Ressourcenfreigabe beizutreten. Sie müssen die Ressourcenfreigabe akzeptieren, bevor Sie auf die freigegebenen Ressourcen zugreifen können.

Akzeptieren einer Ressourcenfreigabe

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im Navigationsbereich Shared with me (Für mich freigegeben) und Resources shares (Ressourcenfreigaben) aus.
3. Wählen Sie die Ressourcenfreigabe aus.
4. Wählen Sie Accept resource share (Ressourcenfreigabe akzeptieren) aus.
5. Öffnen Sie die Seite Transit Gateways in der Amazon-VPC-Konsole, um das freigegebene Transit Gateway anzuzeigen.

Akzeptieren eines freigegebenen Anhangs

Wenn Sie die Funktionalität Auto accept shared attachments (Freigegebene Anhänge automatisch akzeptieren) bei der Erstellung Ihres Transit Gateways nicht aktiviert haben, müssen Sie kontenübergreifende (freigegebene) Anhänge manuell akzeptieren.

So akzeptieren Sie einen freigegebene Anhang manuell:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Transit-Gateway-Anhang aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Akzeptieren des Transit-Gateway-Anhangs aus.

Um einen geteilten Anhang zu akzeptieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl accept-transit-gateway-vpc-attachment.

Löschen eines Transit Gateways

Ein Transit Gateway mit vorhandenen Anhängen kann nicht gelöscht werden. Um ein Transit Gateway löschen zu können, müssen Sie zunächst alle Anhänge löschen.

So löschen Sie ein Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie das zu löschende Transit Gateway aus.
3. Wählen Sie Aktionen, Löschen des Transit Gateways aus. Geben Sie **`delete`** ein und wählen Sie dann Löschen, um das Löschen zu bestätigen.

Um ein Transit-Gateway mit dem zu löschen AWS CLI

Verwenden Sie den delete-transit-gateway-Befehl.

Transit-Gateway-Anhänge an eine VPC

Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie ein Subnetz aus jeder Availability Zone angeben, die das Transit Gateway für die Weiterleitung des Datenverkehrs verwenden soll. Die Angabe eines Subnetzes aus einer Availability Zone ermöglicht es, Datenverkehr an Ressourcen in jedem Subnetz in dieser Availability Zone zu leiten.

Einschränkungen

- Wenn Sie eine VPC an ein Transit Gateway anhängen, können keine Ressourcen in Availability Zones ohne Transit-Gateway-Anhang das Transit Gateway nicht erreichen. Wenn in einer Subnetz-Routing-Tabelle eine Route zum Transit Gateway vorhanden ist, wird Datenverkehr nur dann zum Transit Gateway weitergeleitet, wenn das Transit Gateway eine Anhang in einem Subnetz in dieser Availability Zone besitzt.
- Die Ressourcen in einer VPC, die einem Transit Gateway angefügt ist, können nicht auf die Sicherheitsgruppen einer anderen VPC zugreifen, die ebenfalls diesem Transit Gateway angehängt ist.
- Ein Transit Gateway unterstützt keine DNS-Auflösung für benutzerdefinierte DNS-Namen von angefügten VPCs, die mit privaten gehosteten Zonen in Amazon Route 53 eingerichtet wurden. Informationen zur Konfiguration der Namensauflösung für privat gehostete Zonen für alle VPCs, die an ein Transit-Gateway angeschlossen sind, finden Sie unter Zentralisierte DNS-Verwaltung der Hybrid Cloud mit Amazon Route 53 und AWS Transit Gateway.

- Ein Transit Gateway unterstützt kein Routing zwischen VPCs mit identischen CIDRs. Wenn Sie eine VPC an ein Transit Gateway anschließen und ihr CIDR mit dem CIDR einer anderen VPC identisch ist, die bereits an das Transit Gateway angeschlossen ist, werden die Routen für die neu angeschlossene VPC nicht an die Transit-Gateway-Routing-Tabelle weitergegeben.
- Sie können keinen Anhang für ein VPC-Subnetz erstellen, das sich in einer Local Zone befindet. Jedoch können Sie Ihr Netzwerk so konfigurieren, dass Subnetze in der Local Zone eine Verbindung mit einem Transit-Gateway über die übergeordnete Availability Zone herstellen. Weitere Informationen finden Sie unter Verbinden von Subnetzen der Local Zone mit einem Transit Gateway.
- Sie können keinen Transit-Gateway-Anhang mit reinen IPv6-Subnetzen erstellen. Subnetze für Transit-Gateway-Anhänge müssen auch IPv4-Adressen unterstützen.
- Ein Transit-Gateway muss mindestens einen VPC-Anhang haben, bevor dieses Transit-Gateway zu einer Routing-Tabelle hinzugefügt werden kann.

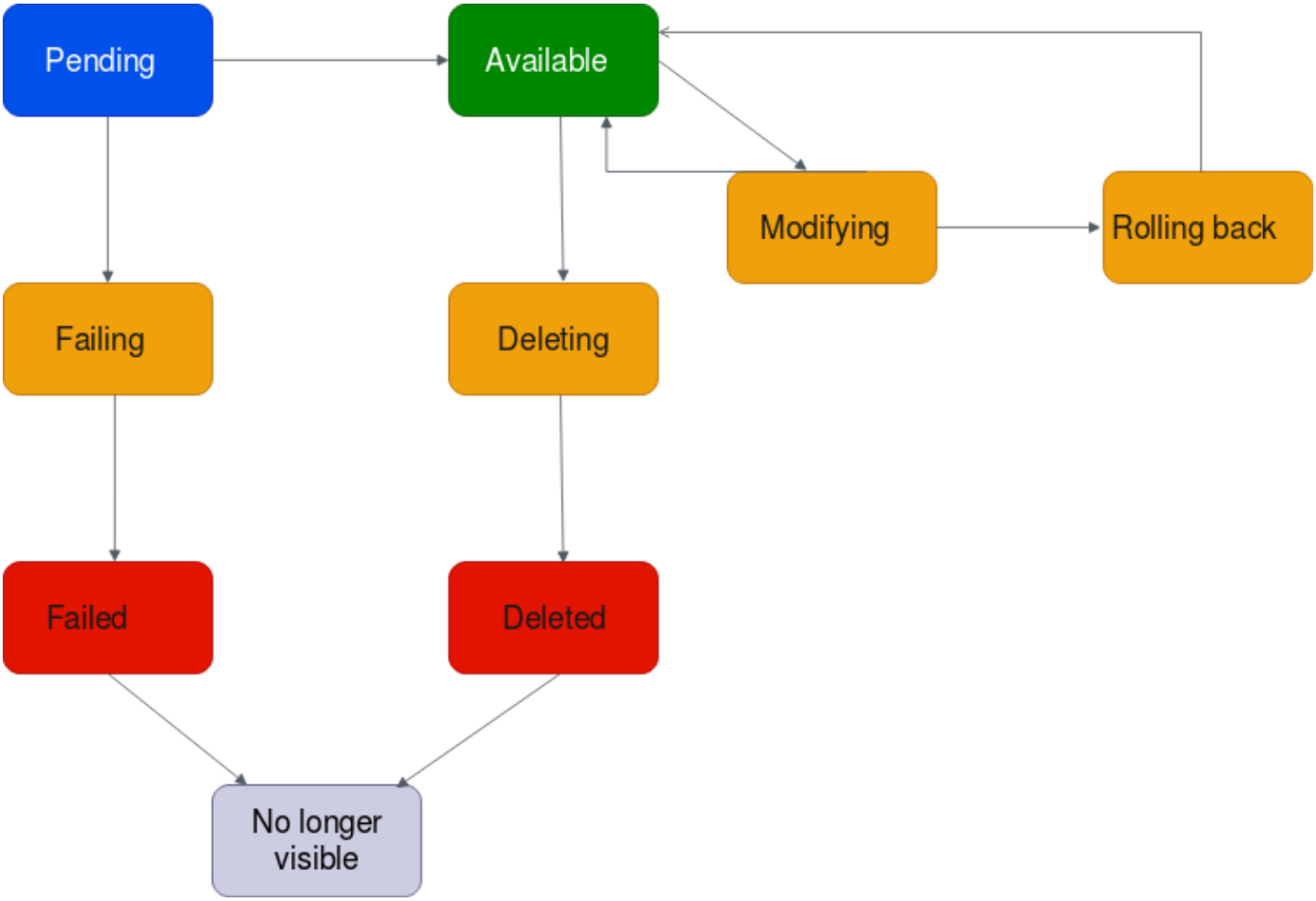
Inhalt

- Lebenszyklus von VPC-Anhängen
- Erstellen eines Transit-Gateway-Anhangs an eine VPC
- Ändern des VPC-Anhangs
- Ändern der VPC-Anhang-Tags
- Anzeigen Ihrer VPC-Anhänge
- Löschen eines VPC-Anhangs
- Problembehandlung bei der Erstellung von VPC-Anhängen

Lebenszyklus von VPC-Anhängen

Eine VPC-Anhang durchläuft verschiedene Phasen, die mit der Einleitung der Anforderung beginnen. In jeder Phase kann es Aktionen geben, die Sie einleiten können. Am Ende Ihres Lebenszyklus bleibt der VPC-Anhang in der Amazon Virtual Private Cloud Console und in der API- oder Befehlszeilenausgabe eine Zeit lang sichtbar.

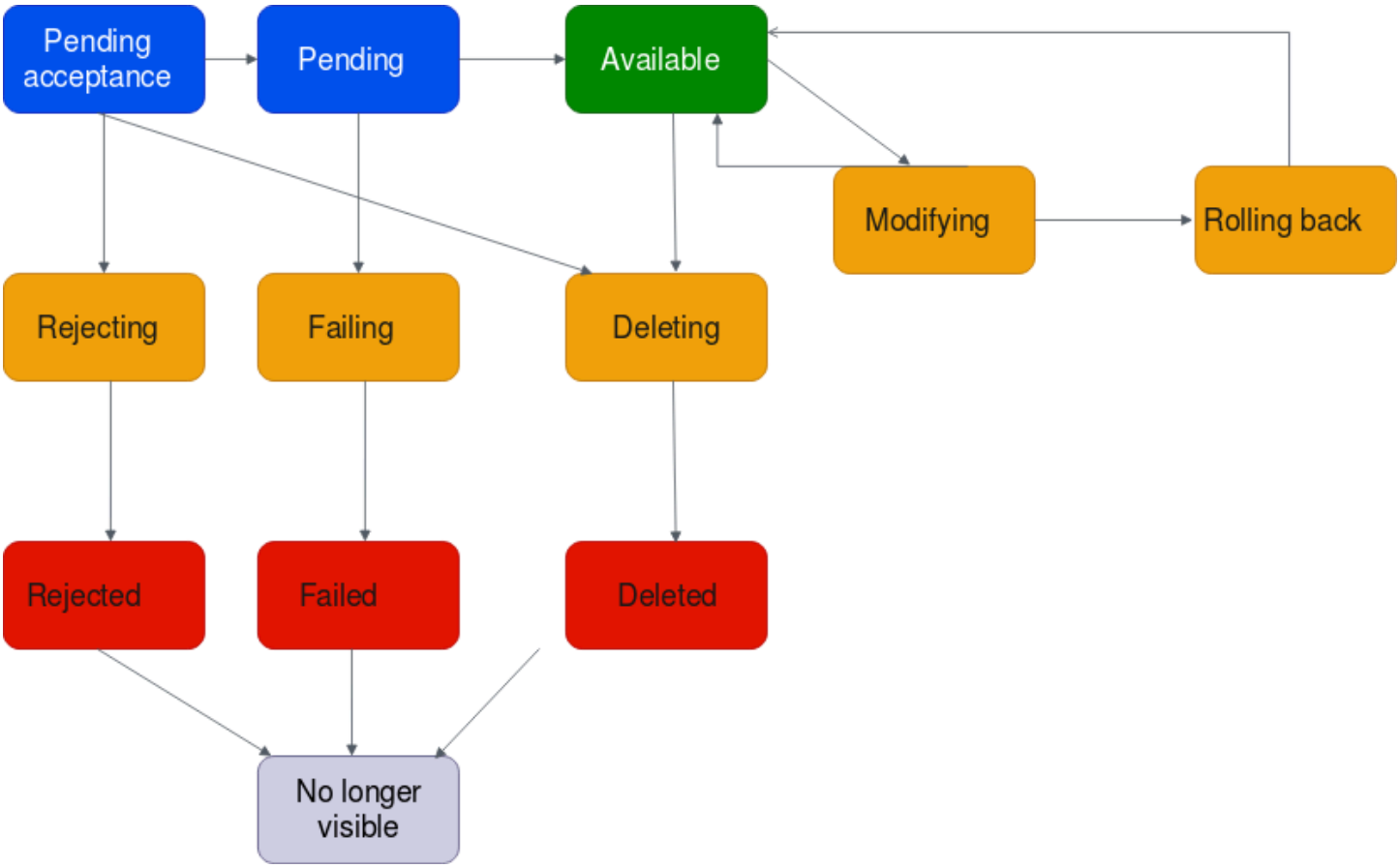
Das folgende Diagramm zeigt die Phasen, die eine Anhang in einer einzelnen Kontokonfiguration oder eine kontoübergreifende Konfiguration durchlaufen kann, bei der Auto accept shared attachments (Gemeinsame Anhänge automatisch akzeptieren) werden aktiviert ist.



- Ausstehend: Eine Anfrage für einen VPC-Anfügung wurde initiiert und befindet sich im Bereitstellungsprozess. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.
- Fehlgeschlagen: Eine Anfrage für einen VPC-Anfügung schlägt fehl. In dieser Phase kann die VPC-Anfügung nach `failed` verschoben werden.
- Fehlgeschlagen: Die Anforderung für die VPC-Anfügungen ist fehlgeschlagen. In dieser Phase kann er nicht gelöscht werden. Der fehlgeschlagene VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Verfügbar: Die VPC-Anfügung ist verfügbar und der Datenverkehr kann zwischen der VPC und dem Transit-Gateway fließen. In dieser Phase kann eine Anfügung fehlschlagen oder nach `modifying` bzw. `deleting` verschoben werden.
- Löschen: Eine VPC-Anfügung , die gerade gelöscht wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `deleted` verschoben werden.

- Gelöscht: Eine `available`-VPC-Anfügung wurde gelöscht. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Ändern: Es wurde eine Anfrage zum Ändern der Eigenschaften der VPC-Anfügung gestellt. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` bzw. `rolling back` verschoben werden.
- Wiederherstellen: Die VPC-Anfügungsanforderung kann nicht abgeschlossen werden, und das System macht alle vorgenommenen Änderungen rückgängig. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.

Das folgende Diagramm zeigt die Phasen, die eine Anfügung in einer kontoübergreifenden Konfiguration durchlaufen kann, bei der Auto accept shared attachments (Gemeinsame Anfügungen automatisch akzeptieren) deaktiviert ist.



- Ausstehende Annahme: Die VPC-Anfügungsanfrage wartet auf Annahme. In dieser Phase kann die Anfügung nach `pending`, `rejecting` oder `deleting` verschoben werden.

- Ablehnen: Eine VPC-Anfügung, die gerade abgelehnt wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `rejected` verschoben werden.
- Abgelehnt: Eine `pending acceptance`-VPC-Anfügung wurde abgelehnt. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Ausstehend: Die VPC-Anfügung wurde angenommen und befindet sich im Bereitstellungsprozess. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.
- Fehlgeschlagen: Eine Anfrage für einen VPC-Anfügung schlägt fehl. In dieser Phase kann die VPC-Anfügung nach `failed` verschoben werden.
- Fehlgeschlagen: Die Anforderung für die VPC-Anfügungen ist fehlgeschlagen. In dieser Phase kann er nicht gelöscht werden. Der fehlgeschlagene VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Verfügbar: Die VPC-Anfügung ist verfügbar und der Datenverkehr kann zwischen der VPC und dem Transit-Gateway fließen. In dieser Phase kann eine Anfügung fehlschlagen oder nach `modifying` bzw. `deleting` verschoben werden.
- Löschen: Eine VPC-Anfügung , die gerade gelöscht wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `deleted` verschoben werden.
- Gelöscht: Ein `available`- oder `pending acceptance`-VPC-Anhang wurde gelöscht. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden sichtbar und ist dann nicht mehr sichtbar.
- Ändern: Es wurde eine Anfrage zum Ändern der Eigenschaften der VPC-Anfügung gestellt. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` bzw. `rolling back` verschoben werden.
- Wiederherstellen: Die VPC-Anfügungsanforderung kann nicht abgeschlossen werden, und das System macht alle vorgenommenen Änderungen rückgängig. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.

Erstellen eines Transit-Gateway-Anhangs an eine VPC

Erstellen eines VPC-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

4. Geben Sie für Name tag (Namens-Tag) optional einen Namen für den Transit-Gateway-Anhang ein.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Sie besitzen, oder ein Transit Gateway, das für Sie freigegeben wurde.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
7. Wählen Sie aus, ob DNS-Unterstützung, IPv6-Unterstützung und Appliance-Modus-Unterstützung aktiviert werden sollen.

   Wenn der Appliance-Modus ausgewählt ist, verwendet der Verkehrsfluss zwischen einer Quelle und einem Ziel für die gesamte Lebensdauer dieses Flusses dieselbe Availability Zone für den VPC-Anhang.
8. Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll.

   Dieser VPC muss mindestens ein Subnetz zugeordnet sein.
9. Wählen Sie für Subnet IDs (Subnetz-IDs) ein Subnetz für jede Availability Zone aus, die das Transit Gateway für die Weiterleitung des Datenverkehrs verwenden wird. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
10. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

So erstellen Sie einen VPC-Anhang mit dem AWS CLI

Verwenden Sie den Befehl create-transit-gateway-vpc-attachment.

Ändern des VPC-Anhangs

So zeigen Sie VPC-Anhänge mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang und dann Aktionen, Ändern des Transit-Gateway-Anhangs aus.
4. Wählen Sie zum Aktivieren der DNS-Unterstützung DNS support (DNS-Unterstützung) aus.
5. Um dem Anhang ein Subnetz hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dem Subnetz.

Das Hinzufügen oder Ändern eines VPC-Anhangs-Subnetzes kann sich auf den Datenverkehr auswirken, während sich der Anhang in einem Änderungszustand befindet.

6. Wählen Sie Ändern des Transit-Gateway-Anhangs aus.

So ändern Sie Ihre VPC-Anlagen mit dem AWS CLI

Verwenden Sie den Befehl modify-transit-gateway-vpc-attachment.

Ändern der VPC-Anhang-Tags

So zeigen Sie VPC-Anhang-Tags mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang und dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
4. [Tag (Markierung) hinzufügen] Wählen Sie Add new tag (Neuen 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.
5. [Tag entfernen] Wählen Sie neben dem Tag die Option Remove (Entfernen) aus.
6. Wählen Sie Speichern.

VPC-Anhangs-Tags können nur mit der Konsole geändert werden.

Anzeigen Ihrer VPC-Anhänge

Anzeigen Ihrer VPC-Anhänge mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Resource type (Ressourcentyp) nach VPC. Dies sind die VPC-Anhänge.
4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen.

So zeigen Sie Ihre VPC-Anlagen mit dem AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-vpc-attachments.

Löschen eines VPC-Anhangs

Löschen eines VPC-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang aus.
4. Wählen Sie Aktionen, Löschen des Transit-Gateway-Anhangs aus.
5. Geben Sie bei der Aufforderung **`delete`** ein und wählen Sie Delete (Löschen) aus.

Um einen VPC-Anhang mit dem AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-vpc-attachment.

Problembehandlung bei der Erstellung von VPC-Anhängen

Das folgende Thema kann Ihnen bei der Behebung von Problemen helfen, die beim Erstellen eines VPC-Anhangs auftreten könnten.

Problem

Der VPC-Anhang ist fehlgeschlagen.

Ursache

Dies kann folgende Ursachen haben:

1. Der Benutzer, der den VPC-Anhang erstellt, hat keine korrekten Berechtigungen zum Erstellen einer serviceverknüpften Rolle.
2. Es gibt ein Problem mit der Drosselung aufgrund zu vieler IAM-Anforderungen. Sie verwenden zum Beispiel AWS CloudFormation , um Berechtigungen und Rollen zu erstellen.
3. Das Konto hat die serviceverknüpfte Rolle, und die serviceverknüpfte Rolle wurde geändert.
4. Das Transit-Gateway befindet sich nicht in der Phase `available`.

Lösung

Versuchen Sie je nach Ursache Folgendes:

1. Stellen Sie sicher, dass der Benutzer über die richtigen Berechtigungen zum Erstellen von serviceverknüpften Rollen verfügt. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch. Nachdem der Benutzer die Berechtigungen hat, erstellen Sie den VPC-Anhang.
2. Erstellen Sie den VPC-Anhang manuell über die Konsole oder API. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
3. Stellen Sie sicher, dass die serviceverknüpfte Rolle die richtigen Berechtigungen hat. Weitere Informationen finden Sie unter the section called “Transit Gateway”.
4. Prüfen Sie, ob das Transit-Gateway sich in der Phase `available` befindet. Weitere Informationen finden Sie unter the section called “Anzeigen Ihrer Transit Gateways”.

Transit-Gateway-VPN-Anhänge

Um Ihrem Transit Gateway eine VPN-Verbindung anzuhängen, müssen Sie das Kunden-Gateway angeben. Weitere Informationen zu den Anforderungen an ein Kunden-Gateway-Gerät finden Sie unter Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN -Benutzerhandbuch.

Für statische VPNs fügen Sie die statischen Routen der Transit-Gateway-Routing-Tabelle hinzu.

Erstellen eines Transit-Gateway-Anhangs an ein VPN

Erstellen eines VPN-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Ihnen gehört.
5. Wählen Sie bei Attachment type (Anfügungstyp) die Option VPN aus.
6. Wählen Sie bei Customer Gateway (Kunden-Gateway) eine der folgenden Vorgehensweise:
   - Zum Verwenden eines vorhandenen Kunden-Gateways wählen Sie Existing (Vorhanden) und dann das zu verwendende Gateway aus.

Wenn sich Ihr Kunden-Gateway hinter einem NAT-Gerät (Network Address Translation) befindet, das für die NAT-Übersetzung (NAT-T) aktiviert ist, verwenden Sie die öffentliche IP-Adresse Ihres NAT-Geräts und ändern Sie Ihre Firewall-Regeln derart, das die Blockierung des UDP-Ports 4500 aufgehoben wird.

- Zum Erstellen eines Kunden-Gateways wählen Sie New (Neu) aus. Bei IP Address (IP-Adresse) geben Sie dann eine statische öffentliche IP-Adresse und eine BGP ASN (BGP-ASN) ein.

  Bei Routing options (Routing-Optionen) wählen Sie aus, ob Dynamic (Dynamisch) oder Static (Statisch) verwendet werden soll. Weitere Informationen finden Sie unter Site-to-Site-VPN-Routing-Optionen im AWS Site-to-Site VPN -Benutzerhandbuch.

7. Geben Sie für Tunnel Options (Tunneloptionen) die CIDR-Bereiche und Pre-Shared-Schlüssel für Ihren Tunnel ein. Weitere Informationen finden Sie unter Site-to-Site VPN-Architekturen.
8. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

Um einen VPN-Anhang mit dem zu erstellen AWS CLI

Verwenden Sie den create-vpn-connection-Befehl.

Anzeigen Ihrer VPN-Anhänge

Anzeigen Ihrer VPN-Anhänge mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Resource type (Ressourcentyp) nach VPN. Dies sind die VPN-Anhänge.
4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen oder ihm Tags hinzuzufügen.

Um Ihre VPN-Anhänge anzusehen, verwenden Sie AWS CLI

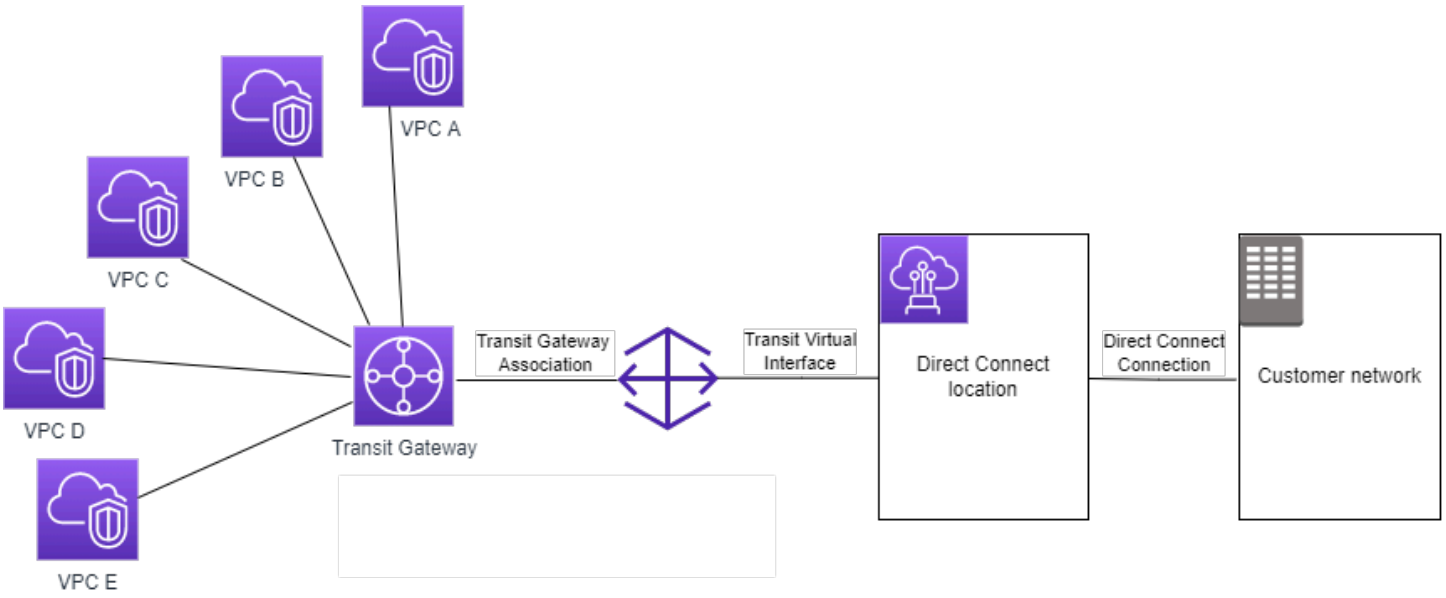
Verwenden Sie den describe-transit-gateway-attachments-Befehl.

Transit-Gateway-Anhänge an ein Direct-Connect-Gateway

Sie können einem Direct-Connect-Gateway mithilfe einer virtuellen Transit-Schnittstelle ein Transit-Gateway anhängen. Diese Konfiguration bietet die folgenden Vorteile. Sie haben folgende Möglichkeiten:

- Verwaltung einer einzigen Verbindung für mehrere VPCs oder VPNs, die sich in der gleichen Region befinden
- Ankündigung von Präfixen, von der On-Premises-Umgebung an AWS sowie ausgehend von AWS an die On-Premises-Umgebung

In der folgenden Grafik ist dargestellt, wie das Direct-Connect-Gateway es Ihnen ermöglicht, eine einzige Verbindung zu Ihrer Direct-Connect-Verbindung zu erstellen, die dann von allen Ihren VPCs genutzt werden kann.



Die Lösung umfasst die folgenden Komponenten:

- Ein Transit Gateway.
- Ein Direct-Connect-Gateway
- Eine Zuordnung zwischen dem Direct-Connect-Gateway und dem Transit Gateway.
- Eine dem Direct-Connect-Gateway angefügte virtuelle Transit-Schnittstelle

Informationen zur Konfiguration von Direct-Connect-Gateways mit Transit Gateways finden Sie unter Transit-Gateway-Zuordnungen im AWS Direct Connect-Direct-Connect-Benutzerhandbuch.

Transit-Gateway-Peering-Anlagen

Sie können sowohl Transit-Gateways innerhalb einer Region als auch Transit-Gateways zwischen den Regionen einbinden und den Datenverkehr zwischen ihnen weiterleiten, einschließlich IPv4- und IPv6-Datenverkehr. Erstellen Sie dazu einen Peering-Anhang auf Ihrem Transit Gateway und geben Sie einen Transit Gateway an. Das Peer-Transit-Gateway kann sich in Ihrem Konto oder in einem anderen AWS-Konto befinden.

Nachdem Sie eine Peering-Anhangs-Anforderung erstellt haben, muss der Besitzer des Peer-Transit-Gateways (auch als Accepter Transit Gatewaybezeichnet) die Anforderung akzeptieren. Um Datenverkehr zwischen durch Peering verbundenen Transit Gateways weiterzuleiten, müssen Sie der Transit-Gateway-Routing-Tabelle eine statische Route hinzufügen, die auf den Peering-Anhang des Transit Gateways verweist.

Es wird empfohlen, eindeutige ASNs für jeden Transit Gateway mit Peering zu verwenden, um zukünftige Routen-Propagierungsfunktionen zu nutzen.

Transit-Gateway-Peering unterstützt nicht die Auflösung öffentlicher oder privater IPv4-DNS-Hostnamen in private IPv4-Adressen. Dies erfolgt über VPCs auf beiden Seiten des Transit-Gateway-Peering-Anhangs mithilfe von Amazon Route 53 Resolver in einer anderen Region. Weitere Informationen zum Route 53 Resolver finden Sie unter Was ist Route 53 Resolver? im Entwicklerhandbuch zu Amazon Route 53.

Interregionales Gateway-Peering verwendet dieselbe Netzwerkinfrastruktur wie VPC-Peering. Daher wird der Datenverkehr mit AES-256-Verschlüsselung auf der virtuellen Netzwerkschicht verschlüsselt, während er zwischen Regionen verläuft. Der Datenverkehr wird auch mit AES-256-Verschlüsselung auf der physischen Ebene verschlüsselt, wenn er Netzwerkverbindungen durchquert, die außerhalb der physischen Kontrolle von AWS liegen. Infolgedessen wird der Datenverkehr auf Netzwerkverbindungen, die außerhalb der physischen Kontrolle von AWS liegen, doppelt verschlüsselt. Innerhalb derselben Region wird der Datenverkehr nur dann auf der physischen Ebene verschlüsselt, wenn er Netzwerkverbindungen durchquert, die außerhalb der physischen Kontrolle von AWS liegen.

Informationen dazu, welche Regionen Transit-Gateway-Peering-Anhänge unterstützen, finden Sie unter AWS-Transit-Gateways – Häufig gestellte Fragen.

Erstellen eines Peering-Anhangs

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die ID des Transit Gateways verfügen, das Sie anhängen möchten. Wenn sich das Transit Gateway in einem anderen AWS-Konto befindet, stellen Sie sicher, dass Sie über die AWS-Konto-ID des Besitzers des Transit Gateways verfügen.

Nachdem Sie den Peering-Anhang erstellt haben, muss der Besitzer des annehmenden Transit-Gateways die Anhangs-Anforderung akzeptieren.

So erstellen Sie einen Peering-Anhang mit der Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Sie besitzen, oder ein Transit Gateway, das für Sie freigegeben wurde.
5. Wählen Sie für Attachment type (Anhangstyp) die Option Peering Connection (Peering-Verbindung).
6. Geben Sie optional ein Namen-Tag für den Anhang ein.
7. Führen Sie unter Account (Konto) eine der folgenden Aktionen aus:
   - Wenn sich das Transit Gateway in Ihrem Konto befindet, wählen Sie My account (Mein Konto) aus.
   - Wenn sich das Transit Gateway in einem anderen AWS-Konto befindet, wählen Sie Anderes Konto aus. Geben Sie für Konto-ID die AWS-Konto-ID ein.
8. Wählen Sie unter Region die Region aus, in der sich das Transit Gateway befindet.
9. Geben Sie für Transit Gateway (Accepter) die ID des Transit Gateways ein, das Sie anhängen möchten.
10. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

So erstellen Sie einen Peering-Anhang mit der AWS CLI

Verwenden Sie den Befehl create-transit-gateway-peering-attachment.

Annehmen oder Ablehnen einer Peering-Anhangs-Anforderung

Um den Peering-Anhang zu aktivieren, muss der Eigentümer des Transit Gateways die Peering-Anhangs-Anforderung akzeptieren. Dies ist auch dann erforderlich, wenn sich beide Transit Gateways im selben Konto befinden. Der Peering-Anhang muss sich im Zustand `pendingAcceptance` befinden. Akzeptieren Sie die Peering-Anhangs-Anforderung aus der Region, in der sich das Transit Gateway des Empfängers befindet.

Sie können jede Anforderung für eine Peering-Verbindung ablehnen, die Sie erhalten haben, wenn diese sich im Status `pendingAcceptance` befindet. Sie müssen die Anforderung von der Region ablehnen, in der sich das Transit Gateway des Empfängers befindet.

So akzeptieren Sie eine Peering-Anhangs-Anforderung über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Akzeptieren des Transit-Gateway-Anhangs aus.
5. Fügen Sie die statische Route zur Transit-Gateway-Routing-Tabelle hinzu. Weitere Informationen finden Sie unter the section called “Erstellen einer statischen Route”.

So lehnen Sie eine Peering-Anhangs-Anforderung über die Konsole ab:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Ablehnen des Transit-Gateway-Anhangs aus.

So nehmen Sie mit der AWS CLI einen Peering-Anhang an oder lehnen sie ab.

Verwenden Sie die Befehle accept-transit-gateway-peering-attachment und reject-transit-gateway-peering-attachment.

Hinzufügen einer Route zur Routing-Tabelle des Transit Gateways

Um Datenverkehr zwischen durch Peering verbundenen Transit Gateways weiterzuleiten, müssen Sie der Routing-Tabelle des Transit Gateways eine statische Route hinzufügen, die auf die Peering-

Anlage des Transit Gateways verweist. Der Besitzer des annehmenden Transit Gateways muss auch eine statische Route zur Routing-Tabelle ihres Transit Gateways hinzufügen.

So erstellen Sie eine Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create static route (Statische Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Geben Sie beispielsweise den CIDR-Block einer VPC an, die mit dem Peer-Transport-Gateway verbunden ist.
6. Wählen Sie den Peering-Anhang für die Route aus.
7. Wählen Sie Create static route (Statische Route erstellen) aus.

So erstellen Sie eine statische Route mit der AWS CLI

Verwenden Sie den Befehl create-transit-gateway-route.

> **Important**
>
> Nachdem Sie die Route erstellt haben, ordnen Sie die Transit-Gateway-Routing-Tabelle dem Transit-Gateway-Peering-Anhang zu. Weitere Informationen finden Sie unter the section called “Zuordnen einer Transit-Gateway-Routing-Tabelle”.

Anzeigen Ihrer Transit-Gateway-Peering-Verbindungs-Anhängen

Sie können Ihre Transit-Gateway-Peering-Anhänge und Informationen dazu anzeigen.

Anzeigen Ihrer Peering-Anhänge mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Resource type (Ressourcentyp) nach Peering. Dies sind die Peering-Anhänge.

4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen.

So zeigen Sie Ihre Transit-Gateway-Peering-Anhänge mithilfe des AWS CLI an

Verwenden Sie den Befehl describe-transit-gateway-peering-attachments.

Löschen eines Peering-Anhangs

Sie können einen Transit-Gateway-Peering-Anhang löschen. Der Besitzer eines der Transit-Gateways kann den Anhang löschen.

So löschen Sie einen Peering-Anhang über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus.
4. Wählen Sie Aktionen, Löschen des Transit-Gateway-Anhangs aus.
5. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

So löschen Sie einen Peering-Anhang mit der AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-peering-attachment.

Überlegungen zu Opt-inAWS-Regionen

Sie können Peering-Verbindungen zwischen Transit Gateways über Opt-In-Regionengrenzen hinweg herstellen. Informationen über diese Regionen und wie Sie sich anmelden, finden Sie unter Verwalten von AWS-Regionen in der Allgemeine Amazon Web Services-Referenz. Berücksichtigen Sie Folgendes, wenn Sie Transit-Gateway-Peering in diesen Regionen verwenden:

- Sie können ein Peering in einer Opt-in-Region durchführen, solange sich das Konto, das der Peering-Anhang akzeptiert, für diese Region angemeldet ist.
- Unabhängig vom Opt-In-Status der Region teilt AWS die folgenden Kontodaten mit dem Konto, das den Peering-Anhang akzeptiert:
  - AWS-Konto ID
  - Transit-Gateway-ID
  - Regionscode

- Wenn Sie den Transit-Gateway-Anhang löschen, werden die oben genannten Kontodaten gelöscht.
- Wir empfehlen, dass Sie den Peering-Anhang des Transit Gateways löschen, bevor Sie sich von der Region abmelden. Wenn Sie den Peering-Anhang nicht löschen, wird der Datenverkehr möglicherweise weiterhin über den Anhang geleitet und es entstehen weiterhin Gebühren. Wenn Sie den Anhang nicht löschen, können Sie sich wieder anmelden und den Anhang dann löschen.
- Im Allgemeinen verfügt das Transit Gateway über ein Modell, in dem der Sender zahlt. Durch die Verwendung eines Transit-Gateway-Peering-Anhangs über eine Opt-in-Grenze hinweg können Gebühren in einer Region anfallen, die den Anhang akzeptiert, einschließlich der Regionen, für die Sie sich nicht angemeldet haben. Weitere Informationen finden Sie unter AWS-Transit-Gateway-Preise.

Transit-Gateway-Connect-Anhänge und Transit-Gateway-Connect-Peers

Sie können einen Transit-Gateway-Connect-Anhang erstellen, um eine Verbindung zwischen einem Transit Gateway und virtuellen Appliances von Drittanbietern (wie SD-WAN-Appliances) herzustellen, die in einer VPC ausgeführt werden. Ein Connect-Anhang unterstützt das Generic Routing Encapsulation (GRE) Tunnelprotokoll für hohe Leistung und das Border Gateway Protocol (BGP) für dynamisches Routing. Nachdem Sie einen Connect-Anhang erstellt haben, können Sie einen oder mehrere GRE-Tunnel (auch Transit-Gateway-Connect-Peersgenannt) in dem Connect-Anhang erstellen, um das Transit Gateway und die Drittanbieter-Appliance zu verbinden. Sie bauen zwei BGP-Sitzungen über den GRE-Tunnel auf, um Routing-Informationen auszutauschen.

> **Important**
>
> Ein Transit-Gateway-Connect-Peer besteht aus zwei BGP-Peering Sitzungen, die auf AWS-verwalteter Infrastruktur enden. Die beiden BGP-Peering-Sitzungen bieten Redundanz der Routingebene und stellen sicher, dass der Verlust einer BGP-Peering-Sitzung Ihren Routing-Vorgang nicht beeinträchtigt. Die von beiden BGP-Sitzungen empfangenen Routing-Informationen werden für den angegebenen Connect-Peer gesammelt. Die beiden BGP-Peering-Sitzungen schützen auch vor AWS-Infrastrukturvorgängen wie routinemäßige Wartung, Patches, Hardware-Upgrades und Austausch. Wenn Ihr Connect-Peer ohne die empfohlene duale BGP-Peering-Sitzung arbeitet, die für Redundanz konfiguriert ist, kann es währenddessen zu einem vorübergehenden Verbindungsverlust während AWS-Infrastrukturbetrieben kommen. Wir empfehlen dringend, dass Sie beide BGP-Peering-Sitzungen auf Ihrem Connect-Peer konfigurieren. Wenn Sie mehrere Connect-Peers

konfiguriert haben, um Hochverfügbarkeit auf Geräteseite zu unterstützen, empfehlen wir Ihnen, beide BGP-Peering-Sitzungen auf jedem Ihrer Connect-Peers zu konfigurieren.

Ein Connect-Anhang verwendet eine vorhandene VPC- oder einen -Direct-Connect-Anhang als zugrundeliegenden Transportmechanismus. Dies wird als Transport-Anhang bezeichnet. Das Transit Gateway identifiziert übereinstimmende GRE-Pakete der Drittanbieter-Appliance als Datenverkehr aus dem Connect-Anhang. Es behandelt alle anderen Pakete, einschließlich GRE-Pakete mit falschen Quell- oder Zielinformationen, als Datenverkehr aus dem Transport-Anhang.

Note

Um einen Direct-Connect-Anhang als Transportmechanismus zu verwenden, müssen Sie zunächst Direct Connect in AWS Transit Gateway integrieren. Die Schritte zum Erstellen dieser Integration finden Sie unter Integrieren von SD-WAN-Geräten in AWS Transit Gateway und AWS Direct Connect.

Inhalt

- Connect-Peers
- Anforderungen und Überlegungen
- Erstellen Sie einen Connect-Anhang
- Erstellen Sie einen Connect-Peer (GRE-Tunnel)
- So können Sie sich Ihre Connect-Anfügungen und Connect-Peers anzeigen lassen
- Ändern Ihrer Connect-Anfügung und Connect Peer-Tags
- Löschen eines Connect-Peers
- Löschen Sie einen Connect-Anhang

Connect-Peers

Ein Connect-Peer (GRE-Tunnel) besteht aus folgenden Komponenten.

Innere CIDR-Blöcke (BGP-Adressen)

Die inneren IP-Adressen, die für BGP-Peering verwendet werden. Sie müssen einen /29 CIDR-Block aus dem `169.254.0.0/16` Bereich für IPv4 angeben. Sie können optional einen /125

CIDR-Block aus dem `fd00::/8` Bereich für IPv6 angeben. Die folgenden CIDR-Blöcke sind reserviert und können nicht verwendet werden:

- 169.254.0.0/29
- 169,254.1.0/29
- 169,254.2.0/29
- 169,254,3,0/29
- 169,254,4,0/29
- 169,254,5,0/29
- 169.254.169.248/29

Sie müssen die erste Adresse aus dem IPv4-Bereich der Appliance als BGP-IP-Adresse konfigurieren. Wenn Sie IPv6 verwenden und Ihr innerer CIDR-Block fd00:: /125 ist, müssen Sie die erste Adresse in diesem Bereich (fd00:: 1) auf der Tunnel-Schnittstelle der Appliance konfigurieren.

Die BGP-Adressen müssen in allen Tunneln eines Transit Gateways eindeutig sein.

Peer-IP-Adressen

Die Peer-IP-Adresse (äußere GRE-IP-Adresse) auf der Appliance-Seite des Connect-Peers. Dies kann eine beliebige IP-Adresse sein. Die IP-Adresse kann eine IPv4- oder IPv6-Adresse sein, muss jedoch von derselben IP-Adressfamilie wie die Transit-Gateway-Adresse sein.

Transit-Gateway-Adresse

Die Peer-IP-Adresse (äußere GRE-IP-Adresse) auf der Transit-Gateway-Seite des Connect-Peers. Die IP-Adresse muss aus dem CIDR-Block des Transit Gateways angegeben werden und für Connect-Anhänge auf dem Transit Gateway eindeutig sein. Wenn Sie keine IP-Adresse angeben, wird die erste verfügbare Adresse aus dem CIDR-Block des Transit Gateways verwendet.

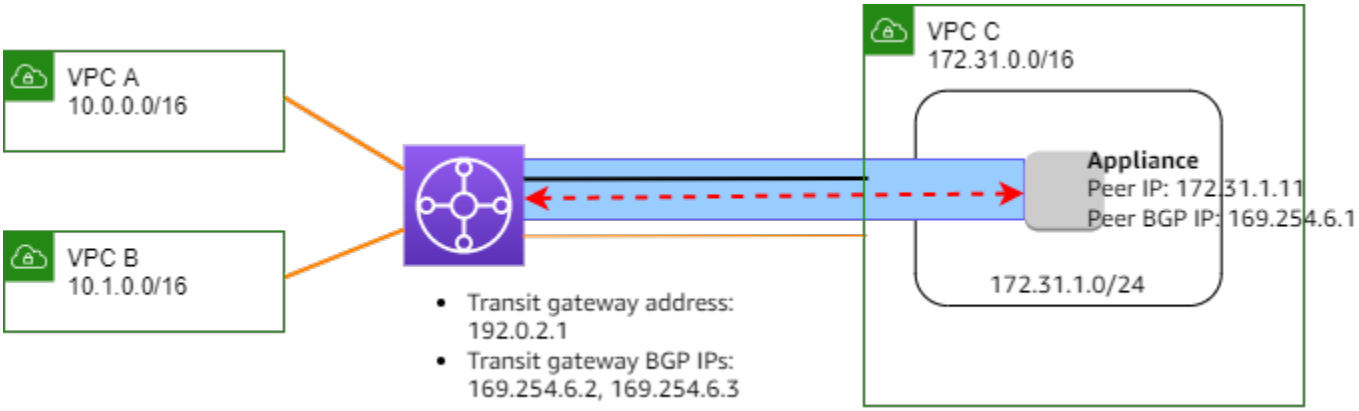
Sie können einen CIDR-Block für das Transit Gateway hinzufügen, wenn Sie ein Transit Gateway erstellen oder ändern .

Die IP-Adresse kann eine IPv4- oder IPv6-Adresse sein, muss jedoch von derselben IP-Adressfamilie sein wie die Peer-IP-Adresse.

Die Peer-IP-Adresse und die Transit-Gateway-Adresse werden verwendet, um den GRE-Tunnel eindeutig zu identifizieren. Sie können beide Adressen für mehrere Tunnel wiederverwenden, aber nicht beide im selben Tunnel.

Transit-Gateway-Connect für das BGP-Peering unterstützt nur Multiprotokoll-BGP (MP-BGP), wobei die IPv4-Unicast-Adressierung erforderlich ist, um auch eine BGP-Sitzung für IPv6-Unicast einzurichten. Sie können IPv4- und IPv6-Adressen für die äußeren IP-Adressen der GRE verwenden.

Das folgende Beispiel zeigt einen Connect-Anhang zwischen einem Transit Gateway und einer Appliance in einer VPC.



Diagrammkomponente	Beschreibung
	VPC-Anhang
	Connect-Anhang
	GRE-Tunnel (Connect-Peer)
	BGP-Peering-Sitzung

Im vorherigen Beispiel wird ein Transit-Gateway-Connect-Anhang auf einem vorhandenen VPC-Anhang (dem Transport-Anhang) erstellt. In der Connect-Anfügung wird ein Connect-Peer erstellt, um eine Verbindung zu einer Appliance in der VPC herzustellen. Die Adresse des Transit Gateways ist `192.0.2.1`, und der Bereich der BGP-Adressen ist `169.254.6.0/29`. Die erste IP-Adresse in dem Bereich (`169.254.6.1`) wird auf der Appliance als Peer-BGP-IP-Adresse konfiguriert.

Die Subnetz-Routing-Tabelle für VPC C umfasst eine Route, die den für den CIDR-Block des Transit Gateways bestimmten Datenverkehr zum Transit Gateway anzeigt.

Zielbereich	Ziel
172.31.0.0/16	Local
192.0.2.0/24	tgw-id

Anforderungen und Überlegungen

Nachfolgend werden Anforderungen und Überlegungen für einen Connect-Anhang aufgeführt:

- Informationen dazu, welche Regionen Connect-Anhänge unterstützen, finden Sie unter AWS – Häufig gestellte Fragen.
- Die Drittanbieter-Appliance muss so konfiguriert sein, dass sie mit dem Connect-Anhang Datenverkehr über einen GRE-Tunnel zum und vom Transit Gateway sendet und empfängt.
- Die Drittanbieter-Appliance muss so konfiguriert sein, dass sie BGP für dynamische Routen-Aktualisierungen und Zustandsprüfungen verwendet.
- Folgende Arten von BGP werden unterstützt:
  - Exterior BGP (eBGP): Wird für die Verbindung mit Routern verwendet, die sich in einem anderen autonomen System befinden als das Transit Gateway. Wenn Sie eBGP verwenden, müssen Sie ebgp-multihop mit einem Time-to-Live-Wert (TTL) von 2 konfigurieren.
  - Interior BGP (iBGP): Wird für die Verbindung mit Routern verwendet, die sich im selben autonomen System wie das Transit Gateway befinden. Das Transit-Gateway installiert keine Routen von einem iBGP-Peer (Drittanbieter-Appliance), es sei denn, die Routen stammen von einem eBGP-Peer und sollten mit next-hop-self konfiguriert sein. Die Routen, die von einer Drittanbieter-Appliance über das iBGP-Peering angekündigt werden, müssen über eine ASN verfügen.
  - MP-BGP (Multiprotocol BGP): Wird zur Unterstützung mehrerer Protokolltypen wie IPv4- und IPv6-Adressfamilien verwendet.
- Das standardmäßige BGP-Keep-Alive-Timeout beträgt 10 Sekunden und der standardmäßige Hold-Timer beträgt 30 Sekunden.
- IPv6-BGP-Peering wird nicht unterstützt; nur IPv4-basiertes BGP-Peering wird unterstützt. IPv6-Präfixe werden über IPv4-BGP-Peering mit MP-BGP ausgetauscht.

- Bidirectional Forwarding Detection (BFD) wird nicht unterstützt.
- Der kontrollierte Neustart von BGP wird nicht unterstützt.
- Wenn Sie einen Transit-Gateway-Peer erstellen und keine Peer-ASN-Nummer angeben, wählen wir die ASN-Nummer des Transit Gateways aus. Das bedeutet, dass sich Ihre Appliance und Ihr Transit Gateway im selben autonomen System wie IBGP befinden.
- Wenn Sie über zwei Connect-Peers verfügen, ist der Connect-Peer, der das Attribut BGP AS-PATH verwendet, die bevorzugte Route.

  Um kostengünstiges Multi-Path-Routing (ECMP) zwischen mehreren Appliances zu verwenden, müssen Sie die Appliance so konfigurieren, dass dieselben Präfixe für das Transit Gateway mit demselben BGP-AS-PATH-Attribut angekündigt werden. Damit das Transit Gateway alle verfügbaren ECMP-Pfade auswählen kann, müssen der AS-PFAD und die Autonomous System Number (ASN) übereinstimmen. Das Transit-Gateway kann ECMP zwischen Connect-Peers für dieselbe Connect-Anfügung oder zwischen Connect-Anfügungen auf demselben Transit-Gateway verwenden. Für das Transit Gateway ist kein ECMP zwischen den beiden redundanten BGP-Peerings möglich.
- Bei einem Connect-Anhang werden die Routen standardmäßig an eine Transit-Gateway-Routing-Tabelle weitergegeben.
- Statische Routen werden nicht unterstützt.
- Stellen Sie sicher, dass die externe Schnittstelle (Tunnel-Quelle) Ihres Drittanbietergeräts Maximum Transmission Unit (MTU) entweder
  - der MTU der GRE-Tunnel-Schnittstelle entspricht oder
  - größer sein muss als die der GRE-Tunnel-Schnittstelle.

Erstellen Sie einen Connect-Anhang

Um einen Connect-Anhang zu erstellen, müssen Sie einen vorhandenen Anhang als Transport-Anhang angeben. Sie können eine VPC-Anfügung oder eine Direct Connect-Anfügung als Transportanfügung angeben.

So erstellen Sie einen Peering-Anhang über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

4. (Optional) Geben Sie unter Name tag (Namens-Tag) einen Namens-Tag für den Anhang an.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option Connect aus.
7. Wählen Sie für die Transport Attachment ID (ID des Transport-Anhangs) die ID eines vorhandenen Anhangs (der Transport-Anhang).
8. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

So erstellen Sie einen Peering-Anhang über die AWS CLI

Verwenden Sie den Befehl create-transit-gateway-connect.

Erstellen Sie einen Connect-Peer (GRE-Tunnel)

Sie können einen Connect-Peer (GRE-Tunnel) für eine bestehende Connect-Anfügung erstellen. Stellen Sie zuvor sicher, dass Sie einen CIDR-Block für das Transit Gateway konfiguriert haben. Sie können einen CIDR-Block für Transit Gateways konfigurieren, wenn Sie ein Transit Gateway erstellen oder ändern .

Wenn Sie den Connect-Peer erstellen, müssen Sie die äußere GRE-IP-Adresse auf der Appliance-Seite des Connect-Peers angeben.

So erstellen Sie einen Connect-Peer über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus und wählen Sie Actions (Aktionen), Create Connect Peer (Connect-Peer erstellen).
4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namenstag für den Connect-Peer an.
5. (Optional) Geben Sie für Transit Gateway GRE Address (Transit-Gateway-GRE-Adresse) die äußere GRE-IP-Adresse für das Transit Gateway an. Standardmäßig wird die erste verfügbare Adresse aus dem CIDR-Block des Transit Gateways verwendet.
6. Geben Sie für Peer GRE Address (Peer-GRE-Adresse)die äußere GRE-IP-Adresse für die Appliance-Seite des Connect-Peers an.
7. Geben Sie für BGP Inside CIDR blocks IPv4den Bereich der inneren IPv4-Adressen an, die für BGP-Peering verwendet werden. Ein CIDR-Block der Größe /29 aus dem Bereich `169.254.0.0/16`.

8. (Optional) Geben Sie für BGP Inside CIDR-Blöcke IPv6 den Bereich der internen IPv6-Adressen an, die für BGP-Peering verwendet werden. Ein CIDR-Block der Größe /125 aus dem Bereich `fd00::/8`.
9. (Optional) Geben Sie für Peer-ASNdie Border Gateway Protocol (BGP) Autonomous System Number (ASN) für die Appliance an. Sie können eine bereits zu Ihrem Netzwerk zugewiesene ASN verwenden. Wenn Sie über keine ASN verfügen, können Sie eine private ASN im Bereich zwischen 64512 und 65534 (16-Bit-ASN) oder 4200000000 und 4294967294 (32-Bit-ASN) verwenden.

   Der Standardwert ist die gleiche ASN wie das Transit Gateway. Wenn Sie die Peer-ASN so konfigurieren, dass sie sich von der ASN des Transit Gateways (eBGP) unterscheidet, müssen Sie ebgp-Multihop mit einem Time-to-Live-Wert (TTL) von 2 konfigurieren.
10. Wählen Sie Connect Peer erstellen aus.

So erstellen Sie ein Connect-Peer mit der AWS CLI

Verwenden Sie den Befehl create-transit-gateway-connect-peer .

So können Sie sich Ihre Connect-Anfügungen und Connect-Peers anzeigen lassen

Sie können sich Ihre Connect-Anfügungen und Connect-Peers anzeigen lassen.

So können Sie sich Ihre Connect-Anfügungen und Connect-Peers über die Konsole anzeigen lassen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus.
4. Um die Connect-Peers für die Anfügung einzusehen, wählen Sie die Registerkarte Connect-Peers.

So können Sie sich Ihre Connect-Anfügungen und Connect-Peers über die AWS CLI anzeigen lassen

Verwenden Sie die Befehle describe-transit-gateway-connects und describe-transit-gateway-connect-peers.

Ändern Ihrer Connect-Anfügung und Connect Peer-Tags

Sie können die Tags für Ihren Connect-Anhang ändern.

So können Sie sich Connect-Anhangs-Tags über die Konsole anzeigen lassen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang und dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
4. Um einen Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüsselnamen und den Schlüsselwert an.
5. Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
6. Wählen Sie Speichern.

Sie können die Tags für Ihren Connect-Peer ändern.

So ändern Sie Ihre Connect Peer-Tags über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang und dann Connect peers (Connect-Peers) aus.
4. Wählen Sie den Connect-Peer aus und wählen Sie dann Actions (Aktionen), Manage tags (Tags verwalten).
5. Um einen Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüsselnamen und den Schlüsselwert an.
6. Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
7. Wählen Sie Speichern.

So ändern Sie Ihre Connect-Anfügung und Connect Peer-Tags über die AWS CLI

Verwenden Sie die Befehle create-tags und delete-tags.

Löschen eines Connect-Peers

Wenn Sie einen Connect-Peer nicht mehr benötigen, können Sie diesen löschen.

So löschen Sie einen Connect-Peer über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus.
4. Wählen Sie auf der Registerkarte Connect Peers den Connect-Peer aus und wählen Sie Actions (Aktionen), Delete Connect Peer (Connect-Peer löschen).

So löschen Sie ein Connect-Peer mithilfe der AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-connect-peer.

Löschen Sie einen Connect-Anhang

Wenn Sie einen Connect-Anhang nicht mehr benötigen, können Sie ihn löschen. Sie müssen zunächst alle Connect-Peers für die Anfügung löschen.

So löschen Sie einen Peering-Anhang über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus und wählen Sie Aktionen, Löschen von Transit-Gateway-Anhang.
4. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

So löschen Sie einen Peering-Anhang über die AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-connect.

Transit-Gateway-Routing-Tabellen

Verwenden Sie Transit-Gateway-Routing-Tabellen, um die Weiterleitung für Ihre Transit-Gateway-Anhänge zu konfigurieren.

Erstellen einer Transit-Gateway-Routing-Tabelle

So erstellen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie Create Transit Gateway Route Table (Transit-Gateway-Routing-Tabelle erstellen) aus.
4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für die Routing-Tabelle des Transit-Gateways ein. Dadurch wird ein Tag erstellt, das "Name" als Tag-Schlüssel und den von Ihnen angegebenen Namen als Tag-Wert hat.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für die Routing-Tabelle aus.
6. Wählen Sie Create Transit Gateway Route Table (Transit-Gateway-Routing-Tabelle erstellen) aus.

Um eine Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den Befehl create-transit-gateway-route-table.

Anzeigen von Transit-Gateway-Routing-Tabellen

So zeigen Sie Ihre Transit-Gateway-Routing-Tabellen mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. (Optional) Zum Finden einer bestimmte Routing-Tabelle oder einer Reihe von Tabellen geben Sie den Namen, das Schlüsselwort oder das Attribut ganz oder teilweise in das Filterfeld ein.
4. Aktivieren Sie das Kontrollkästchen für eine Routing-Tabelle oder wählen Sie ihre ID aus, um Informationen über ihre Zuordnungen, Propagationen, Routen und Tags anzuzeigen.

Um Ihre Transit-Gateway-Routentabellen mit dem AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-route-tables.

Um die Routen für eine Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den search-transit-gateway-routes-Befehl.

Um die Route-Propagationen für eine Transit-Gateway-Routentabelle anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl get-transit-gateway-route-table-propagations.

Um die Verknüpfungen für eine Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den Befehl get-transit-gateway-route-table-associations.

Zuordnen einer Transit-Gateway-Routing-Tabelle

Sie können eine Transit-Gateway-Routing-Tabelle einem Transit-Gateway-Anhang zuordnen.

So ordnen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole zu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus.
4. Wählen Sie unten auf der Seite die Registerkarte Associations (Zuordnungen) aus.
5. Wählen Sie Create association (Zuordnung erstellen) aus.
6. Wählen Sie die für die Zuordnung zu verwendende Anfügung und dann Create association (Zuordnung erstellen) aus.

Um eine Transit-Gateway-Routentabelle mit dem zu verknüpfen AWS CLI

Verwenden Sie den Befehl associate-transit-gateway-route-table.

Löschen einer Zuordnung für eine Transit-Gateway-Routing-Tabelle

Sie können die Zuordnung einer Transit-Gateway-Routing-Tabelle zu einem Transit-Gateway-Anhang aufheben.

So heben Sie die Zuordnung einer Transit-Gateway-Routing-Tabelle mit der Konsole auf

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus.
4. Wählen Sie unten auf der Seite die Registerkarte Associations (Zuordnungen) aus.
5. Wählen Sie die für das Aufheben der Zuordnung zu verwendende Anfügung und dann Delete association (Zuordnung löschen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete association (Zuordnung löschen) aus.

Um die Zuordnung einer Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den Befehl disassociate-transit-gateway-route-table.

Verbreiten einer Route an eine Transit-Gateway-Routing-Tabelle

Verwenden Sie die Route-Propagierung, um eine Route aus einer Anhang zu einer Routing-Tabelle hinzuzufügen.

So verbreiten Sie eine Route an eine Routing-Tabelle für Transit-Gateway-Anhänge

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Propagierung erstellt werden soll.
4. Wählen Sie Actions (Aktionen) und Create propagation (Verbreitung erstellen) aus.
5. Wählen Sie auf der Seite Create propagation (Verbreitung erstellen) die Anfügung aus.
6. Wählen Sie Create propagation (Verbreitung erstellen) aus.

Um die Route-Propagierung mit dem zu aktivieren AWS CLI

Verwenden Sie den Befehl enable-transit-gateway-route-table-propagation.

Deaktivieren der Route-Propagierung

Sie können eine verbreitete Route aus einer Routing-Tabellen-Anhang entfernen.

Deaktivieren der Route-Propagierung mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, aus der die Propagierung gelöscht werden soll.
4. Wählen Sie unten auf der Seite die Registerkarte Propagations (Verbreitungen) aus.
5. Wählen Sie die Anfügung und dann Delete propagation (Verbreitung erstellen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete propagation (Verbreitung löschen) aus.

Um die Route-Propagierung zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl disable-transit-gateway-route-table-propagation.

Erstellen einer statischen Route

Sie können eine statische Route für eine VPC-, VPN- oder Transit-Gateway-Peering-Anlage erstellen, oder Sie können eine Blackhole-Route erstellen, die den Datenverkehr unterlässt, der der Route entspricht.

Statische Routen in einer Routing-Tabelle des Transit-Gateways, die ein VPN-Anhang abzielen, werden nicht vom Site-to-Site VPN gefiltert. Dies kann einen unbeabsichtigten ausgehenden Datenverkehr erlauben, wenn ein BGP-basiertes VPN verwendet wird.

So erstellen Sie eine Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create route (Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Wählen Sie dann Active aus.
6. Wählen Sie die Anhang für die Route aus.

7. Wählen Sie Create static route (Statische Route erstellen) aus.

So erstellen Sie eine Blackhole-Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create static route (Statische Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Wählen Sie dann Blackhole aus.
6. Wählen Sie Create static route (Statische Route erstellen) aus.

Um eine statische Route oder Blackhole-Route mit dem AWS CLI

Verwenden Sie den create-transit-gateway-route-Befehl.

Löschen einer statischen Route

Sie können statische Routen aus einer Transit-Gateway-Routing-Tabelle löschen.

So löschen Sie eine statische Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle, aus der eine Route gelöscht werden soll, und dann Routes (Routen) aus.
4. Wählen Sie die zu löschende Route aus.
5. Wählen Sie Statischen Route löschen aus.
6. Wählen Sie im Bestätigungsfeld Delete static route (Statische Route löschen) aus.

Um eine statische Route zu löschen, verwenden Sie AWS CLI

Verwenden Sie den delete-transit-gateway-route-Befehl.

Eine statische Route ersetzen

Sie können eine statische Route in einer Transit-Gateway-Routing-Tabelle durch eine andere statische Route ersetzen.

So ersetzen Sie eine statische Route mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie in der Routing-Tabelle die Route aus, die Sie ersetzen möchten.
4. Wählen Sie im Abschnitt Details die Registerkarte Routen aus.
5. Wählen Sie Aktionen, Statische Route ersetzen aus.
6. Wählen Sie als Typ entweder Aktiv oder Blackhole aus.
7. Wählen Sie in der Dropdown-Liste Anhang auswählen das Transit-Gateway aus, das das aktuelle Gateway in der Routing-Tabelle ersetzen soll.
8. Wählen Sie Statische Route ersetzen aus.

Um eine statische Route mit dem zu ersetzen AWS CLI

Verwenden Sie den replace-transit-gateway-route-Befehl.

Exportieren von Routing-Tabellen zu Amazon S3

Sie können die Routen in den Transit-Gateway-Routing-Tabellen in einen Amazon-S3-Bucket exportieren. Die Routen werden im angegebenen Amazon-S3-Bucket in einer JSON-Datei gespeichert.

So exportieren Sie Transit-Gateway-Routing-Tabellen mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, die die zu exportierenden Routen enthält.
4. Wählen Sie Actions (Aktionen) und Export routes (Routen exportieren) aus.

5. Geben Sie auf der Seite Export routes (Routen exportieren) bei S3 bucket name (S3-Bucket-Name) den Namen des S3-Buckets ein.
6. Zum Filtern der Routen, die exportiert werden, geben Sie Filterparameter im Abschnitt Filters (Filter) der Seite ein.
7. Wählen Sie Export routes (Routen exportieren) aus.

Um auf die exportierten Routen zuzugreifen, öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/ und navigieren Sie zu dem von Ihnen angegebenen Bucket. Der Dateiname umfasst die AWS-Konto ID, die AWS Region, die Routentabellen-ID und einen Zeitstempel. Wählen Sie die Datei aus und klicken Sie auf Download (Herunterladen). Im Folgenden finden Sie ein Beispiel für eine JSON-Datei, die Informationen zu zwei verbreiteten Routen für VPC-Anhänge enthält.


```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
```

```
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Löschen einer Transit-Gateway-Routing-Tabelle

So löschen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, die gelöscht werden soll.
4. Wählen Sie Aktionen, Löschen der Transit-Gateway-Routing-Tabelle aus.
5. Geben Sie **`delete`** ein und wählen Sie dann Löschen, um das Löschen zu bestätigen.

Um eine Transit-Gateway-Routentabelle mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-route-table.

Präfixlisten-Verweise

Sie können in der Transit-Gateway-Routing-Tabelle auf eine Präfixliste verweisen. Eine Präfixliste ist ein Satz von einem oder mehreren CIDR-Blockeinträgen, die Sie definieren und verwalten. Zur Vereinfachung der Verwaltung der IP-Adressen, auf die Sie in Ihren Ressourcen zur Weiterleitung von Netzwerkdatenverkehr verweisen, können Sie eine Präfixliste verwenden. Wenn Sie beispielsweise häufig die gleichen Ziel-CIDRs in mehreren Transit-Gateway-Routing-Tabellen angeben, können Sie diese CIDRs in einer einzelnen Präfixliste verwalten, anstatt wiederholt auf dieselben CIDRs in jeder Routingtabelle zu verweisen. Wenn Sie einen CIDR-Zielblock entfernen müssen, können Sie seinen Eintrag aus der Präfixliste entfernen, anstatt die Route aus jeder betroffenen Routingtabelle zu entfernen.

Wenn Sie in Ihrer Transit-Gateway-Routing-Tabelle einen Präfixlisten-Verweis erstellen, wird jeder Präfixlisten-Eintrag in der Transit-Gateway-Routing-Tabelle als Route dargestellt.

Weitere Informationen zu Präfixlisten finden Sie unter Präfixlisten im Amazon VPC-Benutzerhandbuch.

Erstellen eines Präfixlisten-Verweises

Sie können in der Transit-Gateway-Routing-Tabelle einen Verweis auf eine Präfixliste erstellen.

So erstellen Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit Gateways aus.
4. Wählen Sie Actions (Aktionen), Create prefix list reference (Präfixlistenreferenz erstellen) aus.
5. Wählen Sie in Prefix list ID (Präfixlisten-ID) die ID der Präfixliste aus.
6. Wählen Sie für Typ aus, ob Datenverkehr zu dieser Präfixliste zulässig sein soll (Aktiv) oder aufgegeben (Blackhole).
7. Wählen Sie in Transit gateway attachment ID (Transit-Gateway-Anhangs-ID) die ID des Anhangs aus, an den der Datenverkehr weitergeleitet werden soll.
8. Wählen Sie Create prefix list reference (Präfixlistenreferenz erstellen).

So erstellen Sie eine Präfixlisten-Verweis über die AWS CLI

Verwenden Sie den Befehl create-transit-gateway-prefix-list-reference.

Anzeigen von Präfixlisten-Verweisen

Sie können die Präfixlisten-Verweise in der Transit-Gateway-Routing-Tabelle anzeigen. Sie können in der Präfixliste in der Transit-Gateway-Routing-Tabelle jeden Eintrag auch als einzelne Route anzeigen. Der Routentyp für eine Präfixlistenroute ist `propagated`.

So zeigen Sie einen Präfixlisten-Verweis über die Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit-Gateways aus.
4. Wählen Sie im unteren Bereich Prefix list references (Präfixlistenreferenzen)aus. Die Präfixlisten-Verweise werden aufgelistet.
5. Wählen Sie Routes (Routen) aus. Jeder Präfixlisten-Eintrag wird in der Routing-Tabelle als Route aufgelistet.

So zeigen Sie einen Präfixlisten-Verweis über die AWS CLI an

Verwenden Sie den Befehl get-transit-gateway-prefix-list-references.

Ändern eines Präfixlisten-Verweises

Sie können einen Präfixlisten-Verweis ändern, indem Sie den Anhang ändern, an den der Datenverkehr weitergeleitet wird. Sie können auch angeben, ob der Datenverkehr gelöscht werden soll, der mit der Route übereinstimmt.

Sie können auf der Registerkarte Routes (Routen) die einzelnen Routen für eine Präfixliste nicht ändern. Um die Einträge in der Präfixliste zu ändern, müssen Sie das Fenster Managed Prefix Lists (Verwaltete Präfixlisten) verwenden. Weitere Informationen finden Sie unter Ändern einer Präfixliste im Amazon VPC-Benutzerhandbuch.

So ändern Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit-Gateways aus.
4. Wählen Sie im unteren Bereich Prefix list references (Präfixlistenreferenzen)aus.
5. Wählen Sie die Präfixlistenreferenz und anschließend Modify references (Referenzen ändern) aus.
6. Wählen Sie für Typ aus, ob Datenverkehr zu dieser Präfixliste zulässig sein soll (Aktiv) oder aufgegeben (Blackhole).
7. Wählen Sie in Transit gateway attachment ID (Transit-Gateway-Anhangs-ID) die ID des Anhangs aus, an den der Datenverkehr weitergeleitet werden soll.

8. Wählen Sie Modify prefix list reference (Präfixlistenreferenz ändern) aus.

So ändern Sie einen Präfixlisten-Verweis über die AWS CLI

Verwenden Sie den Befehl modify-transit-gateway-prefix-list-reference.

Löschen eines Präfixlisten-Verweises

Wenn Sie einen Präfixlisten-Verweis nicht mehr benötigen, können Sie diese aus der Transit-Gateway-Routing-Tabelle löschen. Durch das Löschen des Verweises wird die Präfixliste nicht gelöscht.

So löschen Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit Gateways aus.
4. Wählen Sie die Präfixlistenreferenz und anschließend Delete references (Referenzen löschen) aus.
5. Wählen Sie Delete references (Referenzen löschen) aus.

So löschen Sie einen Präfixlisten-Verweis über die AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-prefix-list-reference.

Transit-Gateway-Richtlinientabellen

Dynamisches Transit-Gateway-Routing verwendet Richtlinientabellen, um den Netzwerkverkehr für AWS -Cloud-WAN zu leiten. Die Tabelle enthält Richtlinienregeln für den Abgleich des Netzwerkverkehrs nach Richtlinienattributen und ordnet dann den Datenverkehr, der mit der Regel übereinstimmt, einer Ziel-Routing-Tabelle zu.

Sie können dynamisches Routing für Transit-Gateways verwenden, um Routing- und Erreichbarkeitsinformationen automatisch mit Peered-Transit-Gateway-Typen auszutauschen. Im Gegensatz zu einer statischen Route kann der Datenverkehr basierend auf Netzwerkbedingungen wie Pfadausfällen oder Überlastung auf einem anderen Pfad weitergeleitet werden. Dynamisches

Routing bietet außerdem eine zusätzliche Sicherheitsebene, da es einfacher ist, den Datenverkehr im Falle einer Netzwerkverletzung oder eines Netzwerkeinbruchs umzuleiten.

> **Note**
>
> Transit-Gateway-Richtlinientabellen werden derzeit nur in Cloud WAN unterstützt, wenn eine Transit-Gateway-Peering-Verbindung erstellt wird. Beim Erstellen einer Peering-Verbindung können Sie diese Tabelle der Verbindung zuordnen. Die Zuordnung füllt die Tabelle dann automatisch mit den Richtlinienregeln.
> Weitere Informationen zu Peering-Verbindungen in Cloud WAN finden Sie unter Peerings im Benutzerhandbuch von AWS Cloud WAN.

Erstellen einer Transit-Gateway-Richtlinientabelle

So erstellen Sie eine Transit-Gateway-Richtlinientabelle mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle).
3. Wählen Sie Create Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle erstellen) aus.
4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für die Transit-Gateway-Richtlinientabelle ein. Dadurch wird ein Tag erstellt und der Wert ist der von Ihnen angegebene Name.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für die Richtlinientabelle aus.
6. Wählen Sie Create Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle erstellen) aus.

Um eine Transit-Gateway-Richtlinientabelle mit dem AWS CLI

Verwenden Sie den Befehl create-transit-gateway-policy-table.

Löschen einer Transit-Gateway-Richtlinientabelle

Löschen Sie eine Transit-Gateway-Richtlinientabelle. Wenn eine Tabelle gelöscht wird, werden alle Richtlinienregeln in dieser Tabelle gelöscht.

So löschen Sie eine Transit-Gateway-Richtlinientabelle mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Policy Tables (Transit-Gateway-Richtlinientabellen).
3. Wählen Sie die zu löschende Transit-Gateway-Richtlinientabelle aus.
4. Wählen Sie Actions (Aktionen) und anschließend Delete policy table (Richtlinientabelle löschen) aus.
5. Bestätigen Sie, dass Sie die Tabelle löschen möchten.

Um eine Transit-Gateway-Richtlinientabelle mit dem AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-policy-table.

Multicast auf Transit Gateways

Multicast ist ein Kommunikationsprotokoll, das für die gleichzeitige Bereitstellung eines einzelnen Datenstroms an mehrere empfangende Computer verwendet wird. Transit Gateway unterstützt das Routing von Multicast-Datenverkehr zwischen Subnetzen angefügter VPCs und dient als Multicast-Router für Instances, die Datenverkehr an mehrere empfangende Instances senden.

Multicast-Konzepte

Die wichtigsten Konzepte für Multicast sind folgende:

- Multicast-Domain – Ermöglicht die Segmentierung eines Multicast-Netzwerks in verschiedene Domains und sorgt dafür, dass das Transit Gateway als mehrere Multicast-Router fungiert. Sie definieren die Mitgliedschaft von Multicast-Domains auf Subnetzebene.
- Multicast-Gruppe – Identifiziert eine Gruppe von Hosts, die denselben Multicast-Verkehr senden und empfangen. Eine Multicast-Gruppe wird durch eine Gruppen-IP-Adresse identifiziert. Die Mitgliedschaft in Multicast-Gruppen wird durch einzelne Elastic Network-Schnittstellen definiert, die an EC2-Instances angeschlossen sind.
- Internet Group Management Protocol (IGMP) – Internetprotokoll, das es Hosts und Routern ermöglicht, die Multicast-Gruppenmitgliedschaft dynamisch zu verwalten. Eine IGMP-Multicast-Domäne enthält Hosts, die das IGMP-Protokoll verwenden, um Nachrichten hinzuzufügen, zu verlassen und zu senden. AWS unterstützt das IGMPv2-Protokoll sowie sowohl IGMP- als auch statische (API-basierte) Multicast-Domänen für Gruppenmitgliedschaften.

- Multicast-Quelle – Elastic-Network-Schnittstelle, die einer unterstützten EC2-Instance zugeordnet ist, die statisch für das Senden von Multicast-Datenverkehr konfiguriert ist. Eine Multicast-Quelle gilt nur für statische Quellenkonfigurationen.

  Eine Multicast-Domain mit statischer Quelle enthält Hosts, die das IGMP-Protokoll nicht zum Beitreten, Verlassen und Senden von Nachrichten verwenden. Sie verwenden die AWS CLI , um eine Quelle und Gruppenmitglieder hinzuzufügen. Die statisch hinzugefügte Quelle sendet Multicast-Datenverkehr und die Mitglieder erhalten Multicast-Datenverkehr.
- Multicast-Gruppenmitglied – Eine Elastic Network-Schnittstelle, die einer unterstützten EC2-Instance zugeordnet ist, die Multicast-Datenverkehr empfängt. Eine Multicast-Gruppe hat mehrere Gruppenmitglieder. In einer Gruppenmitgliedschaft mit statischer Quelle können Multicast-Gruppenmitglieder nur Datenverkehr empfangen. In einer IGMP-Gruppenkonfiguration können Mitglieder sowohl Datenverkehr senden als auch empfangen.

Überlegungen

- Informationen zu unterstützten Regionen finden Sie unter Häufig gestellte Fragen zu AWS -Transit-Gateway.
- Sie müssen ein neues Transit Gateway erstellen, damit Multicast unterstützt wird.
- Die Multicast-Gruppenmitgliedschaft wird mithilfe der Amazon Virtual Private Cloud Console oder der AWS CLIoder IGMP verwaltet.
- Ein Subnetz kann sich nur in einer Multicast-Domain befinden.
- Wenn Sie eine Nicht-Nitro-Instance verwenden, müssen Sie die Source/Dest (Quelle/Ziel)-Prüfung deaktivieren. Informationen zum Deaktivieren der Prüfung finden Sie unter Ändern der Quell- oder Zielüberprüfung im Amazon EC2-Benutzerhandbuch für Linux-Instances.
- Eine Nicht-Nitro-Instance kann kein Multicast-Sender sein.
- Multicast-Routing wird für AWS Direct Connect, Site-to-Site VPN, Peering-Anhänge oder Transit-Gateway-Connect-Anhänge nicht unterstützt.
- Ein Transit Gateway unterstützt keine Fragmentierung von Multicast-Paketen. Fragmentierte Multicast-Pakete werden verworfen. Weitere Informationen finden Sie unter Maximum Transmission Unit (MTU).
- Beim Startup sendet ein IGMP-Host mehrere JOIN-IGMP-Nachrichten, um einer Multicast-Gruppe beizutreten (normalerweise 2 bis 3 Wiederholungsversuche). In dem unwahrscheinlichen Fall, dass alle JOIN IGMP-Nachrichten verloren gehen, wird der Host nicht Teil der Transit-Gateway-

Multicast-Gruppe. In einem solchen Szenario müssen Sie die JOIN IGMP-Nachricht vom Host mit anwendungsspezifischen Methoden erneut auslösen.

- Eine Gruppenmitgliedschaft beginnt mit dem Erhalt der iGMPv2 JOIN-Nachricht durch das Transit Gateway und endet mit dem Erhalt der IgMPv2 LEAVE-Nachricht. Das Transit Gateway verfolgt Hosts, die der Gruppe erfolgreich beigetreten sind. Als Cloud-Multicast-Router sendet Transit Gateway eine IgMPv2 QUERY-Nachricht alle zwei Minuten an alle Mitglieder. Jedes Mitglied sendet ein IgMPv2 JOIN-Nachricht als Antwort, so erneuern die Mitglieder ihre Mitgliedschaft. Wenn ein Mitglied nicht auf drei aufeinanderfolgende Anfragen antwortet, entfernt das Transit Gateway diese Mitgliedschaft aus allen verbundenen Gruppen. Es sendet jedoch weiterhin 12 Stunden lang Abfragen an dieses Mitglied, bevor es das Mitglied dauerhaft aus seiner to-be-queried Liste entfernt. Eine explizite IgMPv2 LEAVE-Nachricht entfernt den Host sofort und dauerhaft aus jeder weiteren Multicastverarbeitung.
- Das Transit Gateway verfolgt Hosts, die der Gruppe erfolgreich beigetreten sind. Im Falle eines Ausfalls des Transit Gateways sendet das Transit Gateway nach der letzten erfolgreichen IGMP JOIN-Nachricht weiterhin Multicastdaten für 7 Minuten (420 Sekunden) an den Host. Das Transit-Gateway sendet weiterhin Mitgliedschaftsabfragen für bis zu 12 Stunden an den Host oder bis er eine LEAVE IGMP-Nachricht vom Host erhält.
- Das Transit Gateway sendet Mitgliedschaftsabfrage-Pakete an alle IGMP-Mitglieder, um die Multicast-Gruppenmitgliedschaft zu verfolgen. Die Quell-IP dieser IGMP-Abfragepakete ist 0.0.0.0/32, die Ziel-IP ist 224.0.0.1/32 und das Protokoll ist 2. Ihre Sicherheitsgruppen-Konfiguration auf den IGMP-Hosts (Instances) und jede ACLs-Konfiguration in den Host-Subnetzen müssen diese IGMP-Protokollnachrichten zulassen.
- Wenn sich die Multicast-Quelle und das Ziel in derselben VPC befinden, können Sie keine Sicherheitsgruppen-Referenzierung verwenden, um die Zielsicherheitsgruppe so festzulegen, dass sie Datenverkehr von der Sicherheitsgruppe der Quelle akzeptiert.
- Bei statischen Multicast-Gruppen und -Quellen entfernen Amazon-VPC-Transit-Gateways automatisch statische Gruppen und Quellen für ENIs, die nicht mehr vorhanden sind. Dies erfolgt durch die regelmäßige Übernahme der serviceverknüpften Rolle des Transit-Gateways zur Beschreibung von ENIs im Konto.
- Nur statischer Multicast unterstützt IPv6. Dynamischer Multicast nicht.

Multicast mit Windows Server

Sie müssen zusätzliche Schritte ausführen, wenn Sie Multicast für die Verwendung mit Transit-Gateways unter Windows Server 2019 oder 2022 einrichten. PowerShellFühren Sie mit die folgenden Befehle aus:

1. Ändern Sie Windows Server so, dass IGMPv2 anstelle von IGMPv3 für den TCP/IP-Stack verwendet wird:

   ```
   PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
   \Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
   ```

   > **Note**
   >
   > `New-ItemProperty` ist ein Eigenschaftsindex, der die IGMP-Version angibt. Da IGMP v2 die unterstützte Version für Multicast ist, `Value` muss die Eigenschaft sein3. Anstatt die Windows-Registrierung zu bearbeiten, können Sie den folgenden Befehl ausführen, um die IGMP-Version auf 2 festzulegen:
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Die Windows-Firewall verwirft standardmäßig den größten Teil des UDP-Datenverkehrs. Sie müssen zunächst überprüfen, welches Verbindungsprofil für Multicast verwendet wird:

   ```
   PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

   NetworkCategory
   ---------------
            Public
   ```

3. Aktualisieren Sie das Verbindungsprofil aus dem vorherigen Schritt, um den Zugriff auf die erforderlichen UDP-Ports zu ermöglichen:

   ```
   PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
   ```

4. Starten Sie die EC2-Instance neu.
5. Testen Sie Ihre Multicast-Anwendung, um sicherzustellen, dass der Datenverkehr wie erwartet fließt.

Multicast-Routing

Wenn Sie Multicast auf einem Transit Gateway aktivieren, fungiert es als Multicast-Router. Der gesamte Multicast-Datenverkehr wird an den der betreffenden Multicast-Domain zugeordneten Transit Gateway gesendet, wenn Sie dieser Multicast-Domain ein Subnetz hinzufügen.

Netzwerk-ACLs

Die Regeln für Netzwerk-ACL arbeiten auf Subnetz-Ebene. Sie gelten für Multicast-Datenverkehr, da sich Transit Gateways außerhalb des Subnetzes befinden. Weitere Informationen finden Sie unter Netzwerk-ACLs im Amazon-VPC-Benutzerhandbuch.

Für den Multicast-Datenverkehr des Internet Group Management Protocol (IGMP) gelten die folgenden Mindestregeln für eingehenden Verkehr. Der Remote-Host ist der Host, der den Multicast-Datenverkehr sendet.

Typ	Protokoll	Quelle	Beschreibung
Benutzerdefiniertes Protokoll	IGMP(2)	0.0.0.0/32	IGMP-Abfrage
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse des Remote-Hosts	Eingehender Multicast-Datenverkehr

Im Folgenden sind die Mindestregeln für ausgehenden Datenverkehr für IGMP aufgeführt.

Typ	Protokoll	Zielbereich	Beschreibung
Benutzerdefiniertes Protokoll	IGMP(2)	224.0.0.2/32	IGMP verlassen
Benutzerdefiniertes Protokoll	IGMP(2)	IP-Adresse der Multicast-Gruppe	IGMP beitreten
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse der Multicast-Gruppe	Ausgehenden Multicast-Datenverkehr

Sicherheitsgruppen

Sicherheitsgruppenregeln werden auf Instance-Ebene ausgeführt. Sie können sowohl auf eingehenden als auch auf ausgehenden Multicast-Datenverkehr angewendet werden. Das Verhalten ist dasselbe wie beim Unicast-Datenverkehr. Sie müssen für alle Gruppenmitglied-Instances von der Gruppenquelle eingehenden Datenverkehr zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen im Amazon-VPC-Benutzerhandbuch.

Sie müssen mindestens die folgenden eingehenden Regeln für IGMP-Multicast-Datenverkehr haben. Der Remote-Host ist der Host, der den Multicast-Datenverkehr sendet. Sie können keine Sicherheitsgruppe als Quelle der UDP-Eingangsregel angeben.

Typ	Protokoll	Quelle	Beschreibung
Benutzerdefiniertes Protokoll	2	0.0.0.0/32	IGMP-Abfrage
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse des Remote-Hosts	Eingehender Multicast-Datenverkehr

Sie müssen mindestens die folgenden Regeln für ausgehenden IGMP-Multicast-Datenverkehr haben.

Typ	Protokoll	Zielbereich	Beschreibung
Benutzerdefiniertes Protokoll	2	224.0.0.2/32	IGMP verlassen
Benutzerdefiniertes Protokoll	2	IP-Adresse der Multicast-Gruppe	IGMP beitreten
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse der Multicast-Gruppe	Ausgehenden Multicast-Datenverkehr

Arbeiten mit Multicast

Sie können Multicast mit der Amazon-VPC-Konsole oder der AWS CLI auf Transit Gateways konfigurieren.

Bevor Sie eine Multicast-Domäne erstellen, müssen Sie wissen, ob Ihre Hosts das IGMP-Protokoll (Internet Group Management Protocol) für Multicast-Datenverkehr verwenden.

Inhalt

- Multicast-Domänenattribute
- Verwalten von IGMP-Konfigurationen
- Verwalten der Konfigurationen statischer Quellen
- Verwalten von Konfigurationen statischer Gruppenmitglieder
- Verwalten von Multicast-Domänen
- Verwalten von Multicastgruppen
- Arbeiten mit gemeinsam genutzten Multicast-Domänen

Multicast-Domänenattribute

Die folgende Tabelle enthält Details zu den Multicast-Domänenattributen. Sie können nicht beide Attribute gleichzeitig aktivieren.

Attribut	Beschreibung
`Igmpv2Support` (AWS CLI) Unterstützung für IGMPpv2 (Konsole)	Dieses Attribut legt fest, wie Gruppenmitglieder einer Multicast-Gruppe beitreten oder diese verlassen. Wenn dieses Attribut deaktiviert ist, müssen Sie die Gruppenmitglieder manuell zur Domäne hinzufügen. Aktivieren Sie dieses Attribut, wenn mindestens ein Mitglied das IGMP-Protokoll verwendet. Mitglieder treten der Multicast-Gruppe auf eine der folgenden Arten bei: • Mitglieder, die IGMP unterstützen, verwenden die `JOIN` und `LEAVE` Nachrichten. • Mitglieder, die IGMP nicht unterstützen, müssen mithilfe der Amazon-VPC-Konsole oder der AWS CLI zur Gruppe hinzugefügt oder daraus entfernt werden.

Attribut	Beschreibung
	Wenn Sie Mitglieder von Multicast-Gruppen registrieren, müssen Sie sie auch abmelden. Das Transit Gateway ignoriert `LEAVE`-IGMP-Nachrichten, die von einem manuell hinzugefügten Gruppenmitglied gesendet werden.
`StaticSourcesSupport` (AWS CLI) Unterstützung für statische Quellen (Konsole)	Dieses Attribut legt fest, ob es statische Multicast-Quellen für die Gruppe gibt. Wenn dieses Attribut aktiviert ist, müssen Sie Quellen für eine Multicast-Domäne mithilfe register-transit-gateway-multicastvon -group-sources hinzufügen. Nur Multicast-Quellen können Multicast-Datenverkehr senden. Wenn dieses Attribut auf Disable (Deaktivieren) gesetzt ist, gibt es keine designierten Multicast-Quellen. Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, können Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Verwalten von IGMP-Konfigurationen

Wenn Sie mindestens einen Host haben, der das IGMP-Protokoll für Multicast-Datenverkehr verwendet, erstellt A AWS automatisch die Multicast-Gruppe, wenn es eine `JOIN` IGMP-Nachricht von einer Instance empfängt, und fügt die Instance dann als Gruppenmitglied hinzu. Sie können auch statisch Nicht-IGMP-Hosts als Mitglieder zu einer Gruppe hinzufügen, indem Sie verwenden AWS CLI. Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, können Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch.
2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen zum Erstellen von Subnetzen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon VPC-Benutzerhandbuch.

3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
5. Erstellen Sie eine Multicast-Domäne, die für IGMP-Unterstützung konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen einer IGMP-Multicast-Domäne”.

   Verwenden Sie die folgenden Einstellungen:

   - Aktivieren von Unterstützung für IGMPv2.
   - Deaktivieren von Unterstützung für statische Quellen.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Die standardmäßige IGMP-Version für EC2 ist IGMPv3. Sie müssen die Version für alle Mitglieder der IGMP-Gruppe ändern. Sie können folgenden Befehl ausführen:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Fügen Sie die Mitglieder, die das IGMP-Protokoll nicht verwenden, der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Verwalten der Konfigurationen statischer Quellen

In dieser Konfiguration müssen Sie Multicast-Quellen statisch zu einer Gruppe hinzufügen. Hosts verwenden das IGMP-Protokoll nicht, um Multicast-Gruppen beizutreten oder diese zu verlassen. Sie müssen die Gruppenmitglieder, die den Multicast-Datenverkehr erhalten, statisch hinzufügen.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch.
2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen zum Erstellen von Subnetzen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon VPC-Benutzerhandbuch.

3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
5. Erstellen Sie eine Multicast-Domäne, die so konfiguriert ist, dass sie keine IGMP-Unterstützung oder Unterstützung für das statische Hinzufügen von Quellen bietet. Weitere Informationen finden Sie unter the section called “Erstellen einer Multicast-Domäne mit statischer Quelle”.

   Verwenden Sie die folgenden Einstellungen:

   - Deaktivieren von Unterstützung für IGMPv2.
   - Um Quellen manuell hinzuzufügen, setzen Sie Static sources support (Unterstützung statischer Quellen) auf Enable (Aktivieren).

     Quellen sind die einzigen Ressourcen, die Multicast-Datenverkehr senden können, wenn das Attribut aktiviert ist. Andernfalls können alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Wenn Sie Static sources support (Unterstützung statischer Quellen) auf Enable (Aktivieren)festlegen, fügen Sie die Quelle der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Quellen bei einer Multicast-Gruppe”.
8. Fügen Sie die Mitglieder der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Verwalten von Konfigurationen statischer Gruppenmitglieder

In dieser Konfiguration müssen Sie Multicast-Mitglieder statisch zu einer Gruppe hinzufügen. Hosts können das IGMP-Protokoll nicht verwenden, um Multicast-Gruppen beizutreten oder diese zu verlassen. Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, können Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen zum Erstellen von VPCs finden Sie unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch.
2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen zum Erstellen von Subnetzen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon VPC-Benutzerhandbuch.
3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an eine VPC”.
5. Erstellen Sie eine Multicast-Domäne, die so konfiguriert ist, dass sie keine IGMP-Unterstützung oder Unterstützung für das statische Hinzufügen von Quellen bietet. Weitere Informationen finden Sie unter the section called “Erstellen einer Multicast-Domäne mit statischer Quelle”.

   Verwenden Sie die folgenden Einstellungen:

   - Deaktivieren von Unterstützung für IGMPv2.
   - Deaktivieren von Unterstützung für statische Quellen.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Fügen Sie die Mitglieder der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Verwalten von Multicast-Domänen

Um Multicast mit einem Transit Gateway zu verwenden, erstellen Sie eine Multicast-Domäne und ordnen Sie dann Subnetze der Domäne zu.

Inhalt

- Erstellen einer IGMP-Multicast-Domäne
- Erstellen einer Multicast-Domäne mit statischer Quelle
- Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne
- Anzeigen Ihrer Multicast-Domänenzuordnungen
- Trennen von Subnetzen von einer Multicast-Domäne

- Hinzufügen von Tags zu einer Multicast-Domäne
- Löschen einer Multicast-Domäne

Erstellen einer IGMP-Multicast-Domäne

Wenn Sie dies noch nicht getan haben, überprüfen Sie die verfügbaren Multicast-Domänen-Attribute. Weitere Informationen finden Sie unter the section called “Arbeiten mit Multicast”.

Console

So erstellen Sie eine Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.
4. Geben Sie unter Name tag (Namens-Tag) einen Namen für die Domäne ein.
5. Wählen Sie für Transit Gateway ID (Transit-Gateway-ID) das Transit Gateway aus, das den Multicast-Datenverkehr verarbeitet.
6. Aktivieren Sie das Kontrollkästchen für die IGMPv2-Unterstützung.
7. Deaktivieren Sie für die Unterstützung statischer Quellendas Kontrollkästchen.
8. Um automatisch kontoübergreifende Subnetzzuordnungen für diese Multicast-Domäne zu akzeptieren, wählen Sie Auto accept shared associations (Freigegebene Zuordnungen automatisch akzeptieren).
9. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.

Command line

So erstellen Sie eine IGMP-Multicast-Domäne mit der AWS CLI

Verwenden Sie den Befehl create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Erstellen einer Multicast-Domäne mit statischer Quelle

Wenn Sie dies noch nicht getan haben, überprüfen Sie die verfügbaren Multicast-Domänen-Attribute. Weitere Informationen finden Sie unter the section called “Arbeiten mit Multicast”.

Console

So erstellen Sie eine statische Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.
4. Geben Sie für Name Tag (Namens-Tag) einen Namen ein, um die Domäne zu identifizieren.
5. Wählen Sie für Transit Gateway ID (Transit-Gateway-ID) das Transit Gateway aus, das den Multicast-Datenverkehr verarbeitet.
6. Deaktivieren Sie das Kontrollkästchen, um IGMPv2-Unterstützung zu erhalten.
7. Aktivieren Sie für die Unterstützung statischer Quellen das Kontrollkästchen.
8. Um automatisch kontoübergreifende Subnetzzuordnungen für diese Multicast-Domäne zu akzeptieren, wählen Sie Auto accept shared associations (Freigegebene Zuordnungen automatisch akzeptieren).
9. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.

Command line

So erstellen Sie eine statische Multicast-Domäne mit der AWS CLI

Verwenden Sie den Befehl create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne

Gehen Sie wie folgt vor, um einen VPC-Anhang einer Multicast-Domäne zuzuordnen. Wenn Sie eine Zuordnung erstellen, können Sie dann die Subnetze auswählen, die in die Multicast-Domäne aufgenommen werden sollen.

Bevor Sie beginnen, müssen Sie auf Ihrem Transit-Gateway einen VPC-Anhang erstellen. Weitere Informationen finden Sie unter Transit-Gateway-Anhänge an eine VPC.

Console

So verknüpfen Sie VPC-Anhänge mit einer Multicast-Domäne über die Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Create association (Zuordnung erstellen).
4. Wählen Sie für Anhang zum Zuordnen wählen den Transit-Gateway-Anhang aus.
5. Wählen Sie unter Choose subnets to associate (Subnetze für Zuordnung auswählen) die Subnetze aus, die in die Multicast-Domäne aufgenommen werden sollen.
6. Wählen Sie Create association (Zuordnung erstellen) aus.

Command line

So verknüpfen Sie VPC-Anfügungen mit einer Multicast-Domäne mithilfe der AWS CLI

Verwenden Sie den Befehl associate-transit-gateway-multicast-domain.

Anzeigen Ihrer Multicast-Domänenzuordnungen

Sie können sich Ihre Multicast-Domänen anzeigen lassen, um sicherzustellen, dass sie verfügbar sind und die entsprechenden Subnetze und Anhänge enthalten.

Console

So lassen Sie sich eine Multicast-Domäne mithilfe der Konsole anzeigen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Associations (Zuordnungen).

Command line

So zeigen Sie eine Multicast-Domäne mit der an AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-multicast-domains.

Trennen von Subnetzen von einer Multicast-Domäne

Gehen Sie wie folgt vor, um Subnetze von einer Multicast-Domäne zu trennen.

Console

So trennen Sie die Zuordnung von Subnetzen über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Associations (Zuordnungen).
5. Wählen Sie das Subnetz aus und dann Aktionen, Verknüpfung löschen.

Command line

So trennen Sie Subnetze mithilfe der AWS CLI

Verwenden Sie den Befehl disassociate-transit-gateway-multicast-domain.

Hinzufügen von Tags zu einer Multicast-Domäne

Fügen Sie Ihren Ressourcen Tags hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können jeder Multicast-Domäne mehrere Tags hinzufügen. Tag-Schlüssel müssen für jede Multicast-Domäne eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der der Multicast-Domäne bereits zugeordnet ist, ändert sich der Wert dieses Tags. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen.

Console

So können Sie Tags zu einer Multicast-Domäne mithilfe der Konsole anfügen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
5. Wählen Sie für jede Markierung Neue Markierung hinzufügen und geben Sie den Schlüssel und Wert der Markierung ein.
6. Wählen Sie Speichern.

Command line

So fügen Sie Tags zu einer Multicast-Domäne mithilfe der hinzu AWS CLI

Verwenden Sie den Befehl create-tags.

Löschen einer Multicast-Domäne

Gehen Sie folgendermaßen vor, um eine Multicast-Domäne zu löschen.

Console

So löschen Sie eine Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Delete multicast domain (Multicast-Domäne löschen).
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

Command line

So löschen Sie eine Multicast-Domäne mithilfe der AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-multicast-domain.

Verwalten von Multicastgruppen

Inhalt

- Registrieren von Quellen bei einer Multicast-Gruppe
- Registrieren von Mitgliedern bei einer Multicast-Gruppe
- Registrierung von Quellen aus einer Multicast-Gruppe entfernen
- Registrierung von Mitgliedern aus einer Multicast-Gruppe entfernen
- Anzeigen Ihrer Multicast-Gruppen

Registrieren von Quellen bei einer Multicast-Gruppe

> **Note**
>
> Dieses Verfahren ist nur erforderlich, wenn Sie das AttributUnterstützung statischer Quellen auf Enable (Aktivieren)gesetzt haben.

Gehen Sie wie folgt vor, um Quellen bei einer Multicast-Gruppe zu registrieren. Die Quelle ist die Netzwerkschnittstelle, die Multicast-Datenverkehr sendet.

Sie benötigen die folgenden Informationen, bevor Sie eine Quelle hinzufügen:

- Die ID der Multicast-Domäne
- Die IDs der Netzwerkschnittstellen der Quellen
- Die IP-Adresse der Multicast-Gruppe

Console

So registrieren Sie Quellen über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Add group sources (Gruppenquellen hinzufügen).
4. Geben Sie für die Group IP Address (Gruppen-IP-Adresse) entweder den IPv4-CIDR-Block oder den IPv6-CIDR-Block ein, der der Multicast-Domäne zugewiesen werden soll.

5. Wählen Sie unter Choose network interfaces (Netzwerkschnittstellen auswählen) die Netzwerkschnittstellen der Multicast-Sender aus.
6. Wählen Sie Add sources (Quellen hinzufügen).

Command line

So registrieren Sie Quellen mithilfe der AWS CLI

Verwenden Sie den Befehl register-transit-gateway-multicast-group-sources.

Registrieren von Mitgliedern bei einer Multicast-Gruppe

Gehen Sie wie folgt vor, um Gruppenmitglieder bei einer Multicast-Gruppe zu registrieren.

Sie benötigen die folgenden Informationen, bevor Sie Mitglieder hinzufügen:

- Die ID der Multicast-Domäne
- Die IDs der Netzwerkschnittstellen der Gruppenmitglieder
- Die IP-Adresse der Multicast-Gruppe

Console

So registrieren Sie Mitglieder über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne und anschließend Actions (Aktionen), Add group members (Gruppenmitglieder hinzufügen).
4. Geben Sie für die Group IP Address (Gruppen-IP-Adresse) entweder den IPv4-CIDR-Block oder den IPv6-CIDR-Block ein, der der Multicast-Domäne zugewiesen werden soll.
5. Wählen Sie unter Choose network interfaces (Netzwerkschnittstellen auswählen) die Netzwerkschnittstellen der Multicast-Empfänger aus.
6. Wählen Sie Add members (Mitglieder hinzufügen).

Command line

So registrieren Sie Mitglieder mithilfe der AWS CLI

Verwenden Sie den Befehl register-transit-gateway-multicast-group-members.

Registrierung von Quellen aus einer Multicast-Gruppe entfernen

Sie müssen diesen Vorgang nur ausführen, wenn Sie der Multicast-Gruppe manuell eine Quelle hinzugefügt haben.

Console

So entfernen Sie eine Quelle über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wählen Sie die Quellen aus und anschließend Remove source (Quelle entfernen).

Command line

So entfernen Sie eine Quelle mithilfe der AWS CLI

Verwenden Sie den Befehl deregister-transit-gateway-multicast-group-sources.

Registrierung von Mitgliedern aus einer Multicast-Gruppe entfernen

Sie müssen diesen Vorgang nur ausführen, wenn Sie der Multicast-Gruppe manuell ein Mitglied hinzugefügt haben.

Console

So entfernen Sie die Registrierung von Mitgliedern über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wählen Sie die Mitglieder aus und klicken Sie dann auf Remove member (Mitglied entfernen).

Command line

So heben Sie die Registrierung von Mitgliedern mithilfe der auf AWS CLI

Verwenden Sie den Befehl deregister-transit-gateway-multicast-group-members.

Anzeigen Ihrer Multicast-Gruppen

Sie können sich Informationen über Ihre Multicast-Gruppen anzeigen lassen, um zu überprüfen, ob Mitglieder mithilfe des IGMPv2-Protokolls entdeckt wurden. Der Mitgliedstyp (in der Konsole) oder `MemberType` (in der AWS CLI) zeigt IGMP an, wenn Mitglieder mit dem Protokoll AWS entdeckt hat.

Console

So zeigen Sie Multicast-Gruppen mithilfe der Konsole an:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).

Command line

So zeigen Sie Multicast-Gruppen mit der an AWS CLI

Verwenden Sie den Befehl search-transit-gateway-multicast-groups.

Das folgende Beispiel zeigt, dass das IGMP-Protokoll Multicast-Gruppenmitglieder entdeckt hat.

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-
domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
```

```
        }
    ]
}
```

Arbeiten mit gemeinsam genutzten Multicast-Domänen

Mit der gemeinsamen Nutzung von Multicast-Domänen können Besitzer von Multicast-Domänen die Domäne mit anderen AWS-Konten innerhalb ihrer Organisation oder über Organisationen hinweg in AWS Organizations teilen. Als Besitzer der Multicast-Domäne können Sie die Multicast-Domäne zentral erstellen und verwalten. Konsumenten können die folgenden Vorgänge für eine gemeinsam genutzte Multicast-Domäne ausführen:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen in der Multicast-Domäne
- Verknüpfen eines Subnetzes mit der Multicast-Domäne und Trennen von Subnetzen von der Multicast-Domäne

Ein Multicast-Domäneninhaber kann eine Multicast-Domäne teilen mit:

- AWS-Konten innerhalb ihrer Organisation oder über Organisationen hinweg in AWS Organizations
- Eine Organisationseinheit innerhalb seiner Organisation in AWS Organizations
- Seine gesamte Organisation in AWS Organizations
- AWS Konten außerhalb von AWS Organizations.

  Um eine Multicast-Domain mit einem AWS-Konto außerhalb Ihrer Organisation zu teilen, müssen Sie mit AWS Resource Access Manager eine Ressourcenfreigabe erstellen und dann bei der Auswahl der Prinzipal, mit denen Sie die Multicast-Domain teilen möchten, die Option Allow sharing with anyone (Freigabe für alle zulassen) wählen. Informationen zum Erstellen einer Ressourcenfreigabe finden Sie unter Erstellen einer Ressourcenfreigabe in AWS RAM im AWS RAM-Benutzerhandbuch.

Inhalt

- Voraussetzungen für die gemeinsame Nutzung einer Multicast-Domäne
- Zugehörige Services
- Freigeben in mehreren Availability Zones
- Teilen einer Multicast-Domäne

- Aufheben der Freigabe einer gemeinsam genutzten Multicast-Domäne
- Identifizieren einer gemeinsam genutzten Multicast-Domäne
- Berechtigungen für freigegebene Multicast-Domänen
- Fakturierung und Messung
- Kontingente

Voraussetzungen für die gemeinsame Nutzung einer Multicast-Domäne

- Um eine Multicast-Domäne freizugeben, müssen Sie diese in Ihrem AWS-Konto besitzen. Sie können keine Multicast-Domäne freigeben, die mit Ihnen geteilt wurde.
- Um eine Multicast-Domäne für Ihre Organisation oder eine Organisationseinheit in AWS Organizations freigeben zu können, müssen Sie die Freigabe mit AWS Organizations aktivieren. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM-Benutzerhandbuch.

Zugehörige Services

Die Multicast-Domänen-Freigabe wird in AWS Resource Access Manager (AWS RAM) integriert. AWS RAM ist ein Service, mit dem Sie Ihre AWS-Ressourcen für jedes beliebige AWS-Konto oder über AWS Organizations zur gemeinsamen Nutzung freigeben können. Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Konsumenten können einzelne AWS-Konten oder Organisationseinheiten oder gesamte Organisationen in AWS Organizations sein.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM-Benutzerhandbuch.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS-Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS-Konto.

Um den Ort Ihrer Multicast-Domäne relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability Zone-ID (AZ-ID). Die AZ-ID ist eine eindeutige, konsistente Kennung für eine Availability

Zone innerhalb aller AWS-Konten. Beispielsweise ist `use1-az1` eine AZ-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS-Konto.

So zeigen Sie die AZ-IDs für die Availability Zones in Ihrem Konto an

1. Öffnen Sie die AWS RAM-Konsole unter https://console.aws.amazon.com/ram.
2. Die AZ-IDs für die aktuelle Region werden im Feld Your AZ ID (Ihre AZ-ID) rechts im Bildschirm angezeigt.

Teilen einer Multicast-Domäne

Wenn ein Besitzer eine Multicast-Domäne mit einem Verbraucher teilt, hat der Verbraucher folgende Optionen:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen
- Verknüpfen und Trennen von Subnetzen

Um eine Multicast-Domäne zu teilen, müssen Sie sie zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM-Ressource, mit der Sie Ihre Ressourcen in mehreren AWS-Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie eine Multicast-Domäne über die Amazon Virtual Private Cloud Console freigeben, fügen Sie sie einer vorhandenen Ressourcenfreigabe hinzu. Um die Multicast-Domäne zu einer neuen Ressourcenfreigabe hinzuzufügen, müssen Sie zunächst die Ressourcenfreigabe mithilfe der AWS RAM-Konsoleerstellen.

Wenn Sie Teil einer Organisation in AWS Organizations sind und die Freigabe innerhalb Ihrer Organisation aktiviert ist, wird Konsumenten in Ihrer Organisation automatisch Zugriff auf die freigegebene Multicast-Domäne gewährt. Andernfalls erhalten Verbraucher eine Einladung zur Teilnahme an der Ressourcenfreigabe, und nach Annahme der Einladung wird ihnen Zugriff auf die freigegebene Multicast-Domäne gewährt.

Sie können eine Multicast-Domäne, die Sie besitzen, über die Amazon Virtual Private Cloud Console-Konsole, die AWS RAM-Konsole oder die AWS CLI freigeben.

So teilen Sie eine Multicast-Domäne, die Sie besitzen, mit der *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne aus und anschließend Actions (Aktionen), Share multicast domain (Multicast-Domäne freigeben).
4. Wählen Sie Ihre Ressourcenfreigabe und anschließend Share multicast domain (Multicast-Domäne freigeben) aus.

So teilen Sie eine Multicast-Domäne, die Sie besitzen, mit der AWS RAM-Konsole

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

So teilen Sie mit der AWS CLI eine Multicast-Domäne, die Sie besitzen

Verwenden Sie den Befehl create-resource-share.

Aufheben der Freigabe einer gemeinsam genutzten Multicast-Domäne

Wenn die Freigabe einer gemeinsam genutzten Multicast-Domäne aufgehoben wird, passiert Folgendes mit den Ressourcen der Verbraucher-Multicast-Domäne:

- Verbraucher-Subnetze werden von der Multicast-Domäne getrennt. Die Subnetze verbleiben im Verbraucherkonto.
- Quellen der Verbrauchergruppe und Gruppenmitglieder werden von der Multicast-Domäne getrennt und dann vom Verbraucherkonto gelöscht.

Um die Freigabe einer Multicast-Domäne aufzuheben, müssen Sie sie aus der Ressourcenfreigabe entfernen. Hierfür können Sie die AWS RAM-Konsole oder die AWS CLI verwenden.

Um die Freigabe einer freigegebenen Multicast-Domäne, deren Eigentümer Sie sind, aufzuheben, müssen Sie sie aus der Ressourcenfreigabe entfernen. Hierfür können Sie die *Amazon Virtual Private Cloud Console, die AWS RAM-Konsole oder die AWS CLI verwenden.

So heben Sie die Freigabe einer gemeinsam genutzten Multicast-Domäne, deren Besitzer Sie sind, mit der au *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne und dann Actions (Aktionen), Stop sharing (Freigabe aufheben) aus.

So heben Sie die Freigabe einer gemeinsam genutzten Multicast-Domäne, deren Besitzer Sie sind, mit der AWS RAM-Konsole auf

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

So heben Sie die Freigabe einer gemeinsam genutzten Multicast-Domäne, deren Besitzer Sie sind, mit der AWS CLI auf

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren einer gemeinsam genutzten Multicast-Domäne

Besitzer und Verbraucher können freigegebene Multicast-Domänen mit der *Amazon Virtual Private Cloud Console oder der AWS CLI identifizieren.

So identifizieren Sie eine gemeinsam genutzte Multicast-Domäne mit der *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne aus.
4. Lassen Sie sich auf der Seite Details zu Transit-Multicast-Domänen die Besitzer-ID anzeigen, um die AWS-Konto-ID der Multicast-Domäne zu identifizieren.

So identifizieren Sie eine gemeinsam genutzte Multicast-Domäne mit der AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-multicast-domains. Der Befehl gibt die Multicast-Domänen zurück, die Sie besitzen, und die Multicast-Domänen, die mit Ihnen geteilt werden.`OwnerId` zeigt die AWS-Konto-ID des Multicast-Domänenbesitzers an.

Berechtigungen für freigegebene Multicast-Domänen

Berechtigungen für Besitzer

Die Besitzer sind für die Verwaltung der Multicast-Domain und der Mitglieder und Anhänge verantwortlich, die sie registrieren oder mit der Domain verknüpfen. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Sie können AWS Organizations verwenden, um Ressourcen anzuzeigen, zu ändern und zu löschen, die Konsumenten in gemeinsam genutzten Multicast-Domänen erstellen.

Berechtigungen für Konsumenten

Konsumenten können die folgenden Vorgänge für gemeinsam genutzte Multicast-Domänen auf die gleiche Weise ausführen wie bei Multicast-Domänen, die sie erstellt haben:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen in der Multicast-Domäne
- Verknüpfen eines Subnetzes mit der Multicast-Domäne und Trennen von Subnetzen von der Multicast-Domäne

Konsumenten sind verantwortlich für die Verwaltung der Ressourcen, die sie auf der gemeinsam genutzten Multicast-Domäne erstellen.

Kunden können keine Ressourcen anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer der Multicast-Domäne gehören, und sie können keine Multicast-Domänen ändern, die mit ihnen geteilt werden.

Fakturierung und Messung

Weder für den Besitzer noch für den Konsumenten fallen keine zusätzlichen Gebühren für die gemeinsame Nutzung von Multicast-Domänen an.

Kontingente

Eine gemeinsam genutzte Multicast-Domäne wird auf die Multicast-Domänenkontingente des Besitzers und des Konsumenten angerechnet.

Überlegungen zur Transit-Gateway-Freigabe

Sie können den AWS Resource Access Manager (RAM) verwenden, um ein Transit Gateway für VPC-Anhänge über verschiedene Konten hinweg oder für Ihre Organisation in AWS Organizations freizugeben. RAM muss aktiviert sein und Ressourcen müssen mit einer Organisation gemeinsam genutzt werden. Weitere Informationen finden Sie unter Ressourcenfreigabe für AWS Organizations aktivieren im AWS RAM-Benutzerhandbuch.

Berücksichtigen Sie Folgendes, wenn Sie ein Transit Gateway freigeben möchten.

- Ein AWS Site-to-Site VPN-Site-to-Site-VPN-Anhang muss in demselben AWS-Konto erstellt werden, in dessen Besitz sich das Transit Gateway befindet.
- Ein Anhang an ein Direct-Connect-Gateway verwendet eine Transit-Gateway-Zuordnung und kann sich in demselben AWS-Konto wie das Direct-Connect-Gateway befinden oder in einem anderen als das Direct-Connect-Gateway.

Benutzer sind standardmäßig nicht berechtigt, AWS RAM-Ressourcen zu erstellen oder zu ändern. Um Benutzern zu erlauben, Ressourcen zu erstellen oder zu ändern und Aufgaben durchzuführen, müssen Sie IAM-Richtlinien erstellen, die Berechtigungen gewähren, bestimmte Ressourcen und API-Aktionen zu nutzen. Ordnen Sie dann diese Richtlinien den IAM-Benutzern oder -Gruppen zu, die diese Berechtigungen benötigen.

Nur der Ressourcen-Besitzer kann die folgenden Vorgänge ausführen:

- Erstellen einer Ressourcen-Freigabe
- Aktualisieren einer Ressourcen-Freigabe
- Anzeigen einer Ressourcen-Freigabe
- Anzeigen der von Ihrem Konto freigegebenen Ressourcen innerhalb aller Ressourcen-Freigaben
- Anzeigen der Pinzipale, für die Sie Ihre Ressourcen freigeben, innerhalb aller Ressourcen-Freigaben. Durch Anzeigen der Prinzipale, für die Sie Ressourcen freigeben, können Sie bestimmen, wer Zugriff auf Ihre freigegebenen Ressourcen hat.
- Löschen einer Ressourcen-Freigabe
- Führen Sie alle APIs für Transit Gateways, Transit-Gateway-Anhänge und Transit-Gateway-Routing-Tabellen aus.

Sie können die folgenden Operationen für Ressourcen ausführen, die für Sie freigegeben sind:

- Annehmen oder Ablehnen einer Einladung zur Ressourcen-Freigabe
- Anzeigen einer Ressourcen-Freigabe
- Anzeigen der freigegebenen Ressourcen, auf die Sie Zugriff haben
- Anzeigen einer Liste aller der Prinzipale, die Ressourcen für Sie freigeben. Sie können sehen, welche Ressourcen und Ressourcen-Freigaben sie für Sie freigegeben haben.
- Ausführen der `DescribeTransitGateways`-API
- Ausführen der APIs, die in ihren VPCs Anhänge erstellen und beschreiben, beispielsweise `CreateTransitGatewayVpcAttachment` und `DescribeTransitGatewayVpcAttachments`.
- Verlassen einer Ressourcen-Freigabe

Wenn ein Transit Gateway für Sie freigegeben wurde, können Sie seine Transit-Gateway-Routing-Tabellen oder dessen Transit-Gateway-Routing-Tabellenpropagationen und -zuordnungen erstellen, ändern oder löschen.

Wenn Sie ein Transit Gateway erstellen, wird das Transit Gateway in der Availability Zone erstellt, die Ihrem Konto zugeordnet und unabhängig von anderen Konten ist. Wenn sich das Transit Gateway und die Anhangs-Entitäten in verschiedenen Konten befinden, können Sie die Availability Zone mithilfe der Availability Zone-ID eindeutig und konsistent identifizieren. Beispielsweise ist „use1-az1“ eine AZ-ID für die Region us-east-1 und hat in jedem AWS-Konto den gleichen Standort.

Aufheben der Freigabe eines Transit Gateways

Wenn der Besitzer der Freigabe die Freigabe des Transit Gateways aufhebt, gelten die folgenden Regeln:

- Der Transit-Gateway-Anhang funktioniert weiterhin.
- Das freigegebene Konto kann das Transit Gateway nicht beschreiben.
- Der Besitzer des Transit Gateways und der Freigabe-Besitzer sind zum Löschen des Transit-Gateway-Anhangs berechtigt.

Wenn die Freigabe eines Transit-Gateways für ein anderes AWS-Konto aufgehoben wird oder wenn das AWS-Konto, für das das Transit-Gateway freigegeben ist, aus der Organisation entfernt wird, wird das Transit-Gateway selbst nicht beeinträchtigt.

Gemeinsame Subnetze

Ein VPC-Besitzer kann ein Transit-Gateway an das gemeinsam genutzte VPC-Subnetz anfügen. Die Teilnehmer können es nicht. Der Datenverkehr von den Ressourcen des Teilnehmers kann die Anhänge verwenden, abhängig von den Routen, die der VPC-Besitzer im gemeinsam genutzten VPC-Subnetz eingerichtet hat.

Weitere Informationen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

Protokollieren des Netzwerkverkehrs mithilfe von Flow-Protokollen für Transit-Gateway

Flow-Protokolle für Transit-Gateway sind eine Funktion, mit der Sie Informationen über den IP-Datenverkehr zu und von Ihren Transit-Gateways erfassen können. Flow-Protokolldaten können in Amazon CloudWatch Logs, Amazon S3 oder Firehose veröffentlicht werden. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten abrufen und an dem gewählten Ziel anzeigen. Flow-Potokolldaten werden außerhalb des Pfades des Netzwerkdatenverkehrs erfasst und wirken sich daher nicht auf den Netzwerkdurchsatz oder die Latenz aus. Sie können Flow-Protokolle erstellen oder löschen, ohne dass die Netzwerkleistung beeinträchtigt wird. Flow-Protokolle für Transit-Gateway erfassen Informationen, die sich ausschließlich auf Transit-Gateways beziehen, die in the section called “Flow-Protokolldatensätze für Transit-Gateway” beschrieben sind. Wenn Sie Informationen zum ein- und ausgehenden IP-Datenverkehr über Netzwerkschnittstellen in Ihren VPCs erfassen möchten, nutzen Sie VPC-Flow-Protokolle. Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC-Flow-Protokollen im Amazon-VPC-Benutzerhandbuch.

> **Note**
>
> Um ein Flow-Protokoll für Transit-Gateway zu erstellen, müssen Sie Besitzer des Transit-Gateway-Kontos sein. Andernfalls muss Ihnen der Besitzer des Transit-Gateways die entsprechende Berechtigung erteilen.

Flow-Protokolldaten für ein überwachtes Transit-Gateway werden als Flow-Protokolldatensätze aufgezeichnet. Hierbei handelt es sich um Protokollereignisse bestehend aus Feldern, die den Datenverkehrfluss beschreiben. Weitere Informationen finden Sie unter Flow-Protokolldatensätze für Transit-Gateway.

Für die Erstellung eines Flow-Protokolls geben Sie Folgendes an:

- Die Ressource, für die das Flow-Protokoll erstellt werden soll
- Die Ziele, an die die Flow-Protokolldaten veröffentlicht werden sollen.

Nach dem Erstellen eines Flow-Protokolls kann es einige Minuten dauern, bis Daten erfasst und an den gewünschten Zielen veröffentlicht werden. Flow-Protokolle erfassen keine

Echtzeitprotokollstreams für Ihre Transit-Gateways. Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls.

Sie können auf Ihre Flow-Protokolle Tags anwenden. Jeder Tag besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Tags können Ihnen dabei helfen, Ihre Flow-Protokolle zu organisieren, z. B. nach Zweck oder Besitzer.

Wenn Sie ein Flow-Protokoll nicht mehr benötigen, können Sie es löschen. Durch das Löschen eines Flow-Protokolls wird der Flow-Log-Service für die Ressource deaktiviert, und es werden keine neuen Flow-Protokolldatensätze erstellt oder in CloudWatch Logs oder Amazon S3 veröffentlicht. Durch das Löschen des Flow-Protokolls werden keine vorhandenen Flow-Protokolldatensätze oder Protokollstreams (für CloudWatch Logs) oder Protokolldateiobjekte (für Amazon S3) für ein Transit-Gateway gelöscht. Um einen vorhandenen Protokollstream zu löschen, verwenden Sie die CloudWatch Logs-Konsole. Vorhandene Protokolldateiobjekte können auf der Amazon S3-Konsole gelöscht werden. Nach dem Löschen eines Flow-Protokolls kann es einige Minuten dauern, bis keine Daten mehr erfasst werden. Weitere Informationen finden Sie unter Löschen eines Flow-Protokolls.

Inhalt

- Flow-Protokolldatensätze für Transit-Gateway
- Flow-Protokolle für Transit-Gateway – Preise
- Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch
- Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht
- Veröffentlichen Sie Flow-Logs in Firehose
- Arbeiten mit Flow-Protokollen für Transit-Gateway

Flow-Protokolldatensätze für Transit-Gateway

Ein Flow-Protokolldatensatz repräsentiert einen Netzwerk-Flow in Ihrem Transit-Gateway. Jeder Datensatz ist ein String mit durch Leerzeichen getrennten Feldern. Der Datensatz enthält Werte für die verschiedenen Komponenten des Datenverkehrsflusses, zum Beispiel Quelle, Ziel und Protokoll.

Wenn Sie ein Flow-Protokoll erstellen, können Sie das Standardformat für den Flow-Protokolldatensatz verwenden oder ein benutzerdefiniertes Format angeben.

Inhalt

- Standardformat
- Benutzerdefiniertes Format

- Verfügbare Felder

Standardformat

Mit dem Standardformat enthalten die Flow-Protokolldatensätze alle Felder der Versionen 2 bis 6 in der Reihenfolge, die in der Tabelle Verfügbare Felder angezeigt wird. Das Standardformat kann nicht angepasst oder geändert werden. Um zusätzliche Felder oder eine unterschiedliche Teilmenge an Feldern zu erfassen, müssen Sie stattdessen ein benutzerdefiniertes Format angeben.

Benutzerdefiniertes Format

Mit einem benutzerdefinierten Format geben Sie an, welche Felder in den Flow-Protokolldatensätzen in welcher Reihenfolge enthalten sind. Auf diese Weise können Sie spezifische Flow-Protokolle für Ihre Anforderungen erstellen und Felder auslassen, die nicht relevant sind. Ein benutzerdefiniertes Format kann dazu beitragen, dass weniger separate Prozesse erforderlich sind, um spezifische Informationen aus veröffentlichten Flow-Protokollen zu extrahieren. Sie können eine beliebige Anzahl an verfügbaren Flow-Protokollfeldern angeben, Sie müssen jedoch mindestens eins angeben.

Verfügbare Felder

Die folgende Tabelle beschreibt alle verfügbaren Felder für einen Flow-Protokolldatensatz für Transit-Gateway. In der Spalte Version wird die Version angegeben, in der das Feld eingeführt wurde.

Beim Veröffentlichen von Flow-Protokoll-Daten in Amazon S3 hängt der Datentyp für die Felder vom Flow-Protokoll-Format ab. Wenn das Format reiner Text ist, sind alle Felder vom Typ STRING. Wenn das Format Parquet ist, lesen Sie die Tabelle für die Felddatentypen.

Wenn ein Feld für einen bestimmten Datensatz nicht anwendbar ist oder nicht verarbeitet werden konnte, wird für diesen Eintrag „-“ angezeigt. Metadatenfelder, die nicht direkt aus dem Paket-Header stammen, sind Best-Effort-Annäherungen, und ihre Werte können fehlen oder ungenau sein.

Feld	Beschreibung	Version
version	Gibt die Version an, in der das Feld eingeführt wurde. Das Standardformat enthält alle Felder der Version 2 in der Reihenfolge, in der sie in der Tabelle angezeigt werden. Parquet-Datentyp: INT_32	2

Feld	Beschreibung	Version
resource-type	Der Ressourcentyp, für den das Abonnement erstellt wird. Mögliche Werte sind TransitGateway oder TransitGatewayAttachment. Parquet-Datentyp: STRING	6
account-id	Die AWS-Konto ID des Besitzers des Quell-Transit-Gateways. Parquet-Datentyp: STRING	2
tgw-id	ID des Transit-Gateways, für das der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-attachment-id	ID des Transit-Gateway-Anhangs, für den der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-src-vpc-account-id	Die AWS-Konto ID für den Quell-VPC-Verkehr. Parquet-Datentyp: STRING	6
tgw-dst-vpc-account-id	Die AWS-Konto ID für den Ziel-VPC-Verkehr. Parquet-Datentyp: STRING	6
tgw-src-vpc-id	Die ID der Quell-VPC für das Transit-Gateway Parquet-Datentyp: STRING	6
tgw-dst-vpc-id	Die ID der Ziel-VPC für das Transit-Gateway. Parquet-Datentyp: STRING	6
tgw-src-subnet-id	Die ID des Subnetzes für den Transit-Gateway-Quelldatenverkehr. Parquet-Datentyp: STRING	6

Feld	Beschreibung	Version
tgw-dst-subnet-id	Die ID des Subnetzes für den Transit-Gateway-Zieldatenverkehr. Parquet-Datentyp: STRING	6
tgw-src-eni	Die ID der Anhang-ENI des Quell-Transit-Gateways für den Flow. Parquet-Datentyp: STRING	6
tgw-dst-eni	Die ID der Anhang-ENI des Ziel-Transit-Gateways für den Flow. Parquet-Datentyp: STRING	6
tgw-src-az-id	Die ID der Availability Zone, die den Quell-Transit-Gateway enthält, für die der Datenverkehr aufgezeichnet wird. Wenn der Datenverkehr von einem untergeordneten Standort stammt, zeigt der Datensatz das Symbol „-“ für dieses Feld an. Parquet-Datentyp: STRING	6
tgw-dst-az-id	Die ID der Availability Zone, die das Ziel-Transit-Gateway enthält, für das der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-pair-attachment-id	Abhängig von der Flow-Richtung ist dies entweder die Egress- oder die Ingress-Anhangs-ID des Flows. Parquet-Datentyp: STRING	6
srcaddr	Die Quelladresse für eingehenden Datenverkehr. Parquet-Datentyp: STRING	2
dstaddr	Die Zieladresse für ausgehenden Datenverkehr. Parquet-Datentyp: STRING	2
srcport	Der Quellport des Datenverkehrs Parquet-Datentyp: INT_32	2

Feld	Beschreibung	Version
dstport	Der Zielport des Datenverkehrs Parquet-Datentyp: INT_32	2
protocol	Die IANA-Protokollnummer des Datenverkehrs. Weitere Informationen finden Sie unter Zugewiesene IP-Nummern. Parquet-Datentyp: INT_64	2
packets	Die Anzahl der Pakete, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
bytes	Die Anzahl der Bytes, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
start	Die Zeit, in Unix-Sekunden, in der das erste Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf dem Transit-Gateway übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2
end	Die Zeit, in Unix-Sekunden, in der das letzte Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf dem Transit-Gateway übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2

Feld	Beschreibung	Version
log-status	Der Status des Flow-Protokolls: • OK – Daten werden normal auf den ausgewählten Zielen protokolliert. • NODATA – Während des Aggregationsintervalls gab es keinen Netzwerkverkehr zu oder von der Netzwerkschnittstelle. • SKIPDATA – Einige Flow-Protokolldatensätze wurden während des Aggregationsintervalls übersprungen. Dies kann an internen Kapazitätsbeschränkungen oder einem internen Fehler liegen. Parquet-Datentyp: STRING	2
type	Der Typ des Datenverkehrs. Mögliche Werte sind IPv4 | IPv6 | EFA. Weitere Informationen finden Sie unter Elastic Fabric Adapter im Amazon-EC2-Benutzerhandbuch für Linux-Instances. Parquet-Datentyp: STRING	3
packets-lost-no-route	Die Pakete gingen verloren, weil keine Route angegeben wurde. Parquet-Datentyp: INT_64	6
packets-lost-blackhole	Die Pakete gingen aufgrund eines schwarzen Lochs verloren. Parquet-Datentyp: INT_64	6
packets-lost-mtu-exceeded	Die Pakete gingen aufgrund der Größe verloren, welche die MTU überschreitet. Parquet-Datentyp: INT_64	6
packets-lost-ttl-expired	Die Pakete gingen aufgrund des Ablaufs von time-to-live verloren. Parquet-Datentyp: INT_64	6

Feld	Beschreibung	Version
tcp-flags	Der Bitmasken-Wert für die folgenden TCP-Flags: • FIN — 1 • SYN — 2 • RST — 4 • PSH – 8 • ACK – 16 • SYN-ACK — 18 • URG – 32 **Important** Wenn ein Flow-Protokolleintrag nur aus ACK-Paketen besteht, ist der Flag-Wert 0, nicht 16. Allgemeine Informationen zu TCP-Flags (z. B. die Bedeutung von Flags wie FIN, SYN und ACK) finden Sie unter TCP-Segmentstruktur auf Wikipedia. TCP-Flags können während des Aggregationsintervalls ODER-verknüpft werden. Für kurze Verbindungen können die Flags in derselben Zeile im Flow-Protokolldatensatz festgelegt werden, wie beispielsweise 19 für SYN-ACK und FIN und 3 für SYN und FIN. Parquet-Datentyp: INT_32	3
region	Die Region, die das Transit-Gateway enthält, in der der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	4

Feld	Beschreibung	Version
flow-direction	Die Richtung des Flusses in Bezug auf die Schnittstelle, an der der Verkehr erfasst wird. Die möglichen Werte sind: ingress | egress. Parquet-Datentyp: SCHNUR	5
pkt-src-aws-service	Der Name der Teilmenge von IP-Adressbereichen für den Fall, srcaddr ob die Quell-IP-Adresse für einen AWS Dienst bestimmt ist. Die möglichen Werte sind: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRON T | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTA NCE_CONNECT | GLOBALACCELERATOR | KINESIS_V IDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_R ESOLVER | S3 | WORKSPACES_GATEWAYS. Parquet-Datentyp: SCHNUR	5
pkt-dst-aws-service	Der Name der Teilmenge der IP-Adressbereiche für das dstaddr Feld, wenn die Ziel-IP-Adresse für einen AWS Dienst bestimmt ist. Eine Liste möglicher Werte finden Sie im Feld pkt-src-aws-service. Parquet-Datentyp: SCHNUR	5

Flow-Protokolle für Transit-Gateway – Preise

Es fallen Datenerfassungs- und Speichergebühren für Verkaufsprotokolle an, wenn Sie Transit-Gateway-Flow-Protokolle veröffentlichen. Weitere Informationen zu den Preisen bei der Veröffentlichung von Verkaufslogs erhalten Sie, indem Sie Amazon CloudWatch Pricing öffnen und dann unter Tarif „Bezahlt“ die Option Logs auswählen und nach Verkaufte Logs suchen.

Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch

Flow Logs können Flow-Protokolldaten direkt auf Amazon veröffentlichen CloudWatch.

Bei der Veröffentlichung in CloudWatch Logs werden die Flow-Protokolldaten in einer Protokollgruppe veröffentlicht, und jedes Transit-Gateway hat einen eigenen Protokollstream in der Protokollgruppe. Protokollstreams enthalten Flow-Protokolldatensätze. Sie können mehrere Flow-Protokolle erstellen, die Daten in derselben Protokollgruppe veröffentlichen. Wenn dasselbe Transit-Gateway in einem oder mehreren Flow-Protokollen innerhalb derselben Protokollgruppe besteht, hat es einen kombinierten Protokollstream. Wenn Sie ein Flow-Protokoll zum Erfassen von abgelehntem Datenverkehr und ein weiteres Flow-Protokoll zum Erfassen von zulässigem Datenverkehr erstellt haben, erfasst der kombinierte Protokollstream sämtlichen Datenverkehr.

Wenn Sie Flow-Protokolle in Logs veröffentlichen, fallen Gebühren für Datenaufnahme und Archivierung für verkaufte Protokolle an. CloudWatch Weitere Informationen finden Sie unter CloudWatch Amazon-Preise.

In CloudWatch Logs entspricht das Zeitstempelfeld der Startzeit, die im Flow-Protokolldatensatz erfasst wurde. Das Feld ingestionTime gibt das Datum und die Uhrzeit an, an dem der Flow-Protokolldatensatz von Logs empfangen wurde. CloudWatch Der Zeitstempel ist später als die Endzeit, die im Flow-Protokolldatensatz erfasst wird.

Weitere Informationen zu CloudWatch Logs finden Sie unter Logs sent to CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Inhalt

- IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs
- Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle
- Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch
- Prozessflussprotokolldatensätze in Logs CloudWatch

IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs

Die IAM-Rolle, die Ihrem Flow-Protokoll zugeordnet ist, muss über ausreichende Berechtigungen verfügen, um Flow-Logs in der angegebenen Protokollgruppe in CloudWatch Logs zu veröffentlichen. Die IAM-Rolle muss Ihrer gehören. AWS-Konto

Die IAM-Richtlinie, die mit Ihrer IAM-Rolle verknüpft ist, muss mindestens folgende Berechtigungen enthalten:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Stellen Sie auch sicher, dass Ihre Rolle über eine Vertrauensstellung verfügt, die es dem Flow-Protokoll-Service ermöglicht, die Rolle anzunehmen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zu verwenden, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Beispielsweise können Sie der vorherigen Vertrauensrichtlinie den folgenden Bedingungsblock hinzufügen. Das Quellkonto ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Flow Protokoll-ARN. Wenn Sie die Flow-Protokoll-ID nicht kennen, können Sie diesen Teil des ARN durch einen Platzhalter (*) ersetzen und dann die Richtlinie aktualisieren, nachdem Sie das Flow-Protokoll erstellt haben.

```
"Condition": {
```

```
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Erstellen oder Aktualisieren einer IAM-Rolle für Flow-Protokolle

Sie können eine vorhandene Rolle aktualisieren oder mit dem folgenden Verfahren eine neue Rolle für Flow-Protokolle erstellen.

So erstellen Sie eine IAM-Rolle für Flow-Protokolle

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und Create Role (Rolle erstellen) aus.
3. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität wählen) die Option AWS Service aus. Wählen Sie für Use case (Anwendungsfall) die Option EC2 aus. Wählen Sie Weiter aus.
4. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next: Tags (Weiter: Tags) sowie zusätzliche Tags aus. Wählen Sie Weiter aus.
5. Geben Sie auf der Seite Name, Überprüfung sowie Erstellung einen Namen für die Rolle sowie optional eine Beschreibung ein. Wählen Sie Rolle erstellen aus.
6. Wählen Sie den Namen der Rolle aus. Wählen Sie auf der Registerkarte Add permissions (Berechtigungen hinzufügen) die Option Create Inline Policy (Inline-Richtlinie erstellen) und anschließend die Registerkarte JSON aus.
7. Kopieren Sie die erste Richtlinie aus IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs, und fügen Sie sie in das Fenster ein. Wählen Sie Richtlinie prüfen.
8. Geben Sie einen Namen für Ihre Richtlinie ein und wählen Sie Create policy (Richtlinie erstellen).
9. Wählen Sie den Namen der Rolle aus. Wählen Sie auf der Registerkarte Trust Relationships (Vertrauensstellungen) Edit Trust Relationship (Vertrauensstellungen bearbeiten) aus. Ändern Sie im vorhandenen Richtliniendokument den Service von `ec2.amazonaws.com` zu `vpc-flow-logs.amazonaws.com`. Wählen Sie Update Trust Policy.
10. Notieren Sie sich auf der Seite Summary (Zusammenfassung) den ARN der Rolle. Sie benötigen diesen ARN beim Erstellen des Flow-Protokolls.

Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle

Benutzer müssen auch über die Berechtigungen verfügen, die Aktion `iam:PassRole` für die IAM-Rolle zu verwenden, die dem Flow-Protokoll zugeordnet ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch

Sie können Flow-Protokolle für Transit-Gateways erstellen. Wenn Sie diese Schritte als IAM-Benutzer ausführen, stellen Sie sicher, dass Sie über Berechtigungen zum Verwenden der `iam:PassRole`-Aktion verfügen. Weitere Informationen finden Sie unter Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle.

So erstellen Sie ein Flow-Protokoll für Transit-Gateway mit der Konsole

1. Melden Sie sich bei der Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways aus und wählen Sie Actions (Aktionen) und dann Create flow log (Flow-Protokoll erstellen) aus.
4. Wählen Sie als Ziel die Option An CloudWatchLogs senden aus.
5. Für Ziel-Protokollgruppe, wählen Sie den Namen einer aktuellen Ziel-Protokollgruppe aus.

> **Note**
>
> Wenn die Ziel-Protokollgruppe noch nicht existiert, wird durch Eingabe eines neuen Namens in dieses Feld eine neue Ziel-Protokollgruppe erstellt.

6. Geben Sie für die IAM-Rolle den Namen der Rolle an, die berechtigt ist, Logs in Logs zu CloudWatch veröffentlichen.
7. Für Log record format (Datensatzformat protokollieren) wählen Sie das Format für den Flow-Protokolldatensatz aus.
   - Wenn Sie das Standardformat verwenden möchten, wählen Sie AWS default format (-Standardformat) aus.
   - Um ein benutzerdefiniertes Format zu verwenden, wählen Sie Custom format (Benutzerdefiniertes Format) und dann Felder aus Log format (Format protokollieren) aus.
8. (Optional) Wählen Sie Add new tag (Neuen Tag hinzufügen) aus, um Tags auf das Flow-Protokoll anzuwenden.
9. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll mit der Befehlszeile

Verwenden Sie einen der folgenden Befehle.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(Amazon EC2 EC2-Abfrage-API)

Im folgenden AWS CLI Beispiel wird ein Flow-Protokoll erstellt, das Transit-Gateway-Informationen erfasst. Die Flow-Protokolle werden mithilfe der IAM-Rolle an eine Protokollgruppe in CloudWatch Logs mit dem Namen `my-flow-logs` 123456789101 übermittelt. `publishFlowLogs`

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Prozessflussprotokolldatensätze in Logs CloudWatch

Sie können mit Flow-Protokolldatensätzen genauso arbeiten wie mit allen anderen Protokollereignissen, die von CloudWatch Logs erfasst werden. Weitere Informationen zur Überwachung von Protokolldaten und Metrikfiltern finden Sie unter Suchen und Filtern von Protokolldaten im CloudWatch Amazon-Benutzerhandbuch.

Beispiel: Erstellen Sie einen CloudWatch metrischen Filter und einen Alarm für ein Flow-Protokoll

In diesem Beispiel haben Sie ein Flow-Protokoll für `eni-1a2b3c4d`. Sie möchten einen Alarm erstellen, um benachrichtigt zu werden, wenn ein Verbindungsversuch zu Ihrer Instance über den TCP-Port 22 (SSH) innerhalb einer Stunde mindestens 10 Mal fehlschlägt. Zuerst müssen Sie einen Metrikfilter erstellen, der mit dem Datenverkehrsmuster übereinstimmt, für das Sie den Alarm erstellen möchten. Danach können Sie einen Alarm für den Metrikfilter erstellen.

So erstellen Sie einen Metrikfilter für abgelehnten SSH-Datenverkehr und einen Alarm für den Filter

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle), Log groups (Protokollgruppen) aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe und wählen Sie dann Actions (Aktionen), Create metric filter (Metrikfilter erstellen).
4. Geben Sie für Filter Pattern (Filtermuster) folgende Informationen ein.

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. Wählen Sie für Select Log Data to Test (Die zu testenden Protokolldaten auswählen) den Protokollstream Ihres Transit-Gateways aus. (Optional) Um die Zeilen der Protokolldaten anzuzeigen, die mit dem Filtermuster übereinstimmen, wählen Sie Test Pattern (Testmuster). Wählen Sie danach Next (Weiter) aus.
6. Geben Sie einen Filternamen, einen Metrik-Namespace und einen Metriknamen ein. Legen Sie den Metrikwert auf **1** fest. Wenn Sie fertig sind, wählen Sie Next (Weiter) und dann Create metric filter (Metrikfilter erstellen) aus.
7. Wählen Sie im Navigationsbereich Alarms (Alarme) und All alarms (Alle Alarme) aus.
8. Wählen Sie Create alarm (Alarm erstellen) aus.
9. Wählen Sie den Namespace für den Metrikfilter aus, den Sie erstellt haben.

   Es kann einige Minuten dauern, bis neu erstellte Metriken in der Konsole angezeigt werden.

10. Wählen Sie den Metriknamen aus, den Sie erstellt haben, und klicken Sie dann auf Select metric (Metrik auswählen).
11. Konfigurieren Sie den Alarm wie folgt, und wählen Sie dann Weiter:
    - Wählen Sie für Statistic (Statistik) Sum (Summe) aus. Dadurch wird sichergestellt, dass Sie die Gesamtzahl der Datenpunkte für den angegebenen Zeitraum erfassen.
    - Wählen Sie als Period (Zeitraum) 1 Hour (1 Stunde) aus.
    - Wählen Sie für Whenever (Jederzeit) Greater/Equal (Größer/Gleich) aus und geben Sie **10** für den Schwellenwert ein.
    - Belassen Sie für Additional configuration (Zusätzliche Konfiguration), Datapoints to alarm (Zu alarmierende Datenpunkte) den Standardwert **1**.
12. Wählen Sie für Notification (Benachrichtigung) ein vorhandenes SNS-Thema aus oder wählen Sie Create new topic (Neues Thema erstellen), um ein neues zu erstellen. Wählen Sie Weiter aus.
13. Geben Sie einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
14. Wenn Sie mit der Konfiguration des Alarms fertig sind, wählen Sie Create alarm (Alarm erstellen).

Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht

Flow-Protokolle können Flow-Protokolldaten direkt in Amazon S3 veröffentlichen.

Beim Veröffentlichen in Amazon S3 werden Flow-Protokolldaten in einem vorhandenen Amazon S3-Bucket veröffentlicht, den Sie zuvor angegeben haben. Flow-Protokolldatensätze für alle überwachten Transit-Gateways werden in eine Reihe von Protokolldateiobjekten veröffentlicht, die im Bucket abgelegt sind.

Gebühren für Datenaufnahme und Archivierung werden von Amazon CloudWatch for vended logs erhoben, wenn Sie Flow-Logs auf Amazon S3 veröffentlichen. Weitere Informationen zu den CloudWatch Preisen für verkaufte Logs erhalten Sie, indem Sie Amazon CloudWatch Pricing öffnen, Logs auswählen und dann Vended Logs suchen.

Informationen zum Erstellen eines Amazon-S3-Buckets für die Verwendung mit Flow-Protokollen finden Sie unter Erstellen eines Buckets im Benutzerhandbuch zu Amazon Simple Storage Service.

Weitere Informationen zur Protokollierung mehrerer Konten finden Sie unter Zentrale Protokollierung in der AWS Solutions Library.

Weitere Informationen zu CloudWatch Logs finden Sie unter An Amazon S3 gesendete Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Inhalt

- Flow-Protokolldateien
- IAM-Richtlinie für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen
- Amazon S3-Bucket-Berechtigungen für Flow-Protokolle
- Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS
- Amazon S3-Protokolldateiberechtigungen
- Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht
- Verarbeiten von Flow-Protokolldatensätzen in Amazon S3

Flow-Protokolldateien

VPC-Flow-Protokolle sind eine Funktion, die Flow-Protokoll-Datensätze sammelt, sie in Protokolldateien konsolidiert und die Protokolldateien dann in 5-Minuten-Intervallen im Amazon-S3-Bucket veröffentlicht. Jede Protokolldatei enthält Flow-Protokolldatensätze für den in den letzten fünf Minuten aufgezeichneten IP-Verkehr.

Die maximale Dateigröße für eine Protokolldatei beträgt 75 MB. Wenn die Protokolldatei die Dateigrößenbeschränkung innerhalb des 5-Minuten-Zeitraums erreicht, fügt das Flow-Protokoll keine weiteren Flow-Protokolldatensätze hinzu. Anschließend wird das Flow-Protokoll im Amazon S3-Bucket veröffentlicht und eine neue Protokolldatei erstellt.

In Amazon S3 gibt das Feld Last modified (Zuletzt geändert) für die Flow-Protokolldatei Datum und Uhrzeit an, zu dem/der die Datei in den Amazon S3-Bucket hochgeladen wurde. Dieser Zeitpunkt ist später als der Zeitstempel im Dateinamen und die Differenz ist die Zeitspanne, die zum Upload der Datei in den Amazon S3-Bucket benötigt wird.

Protokolldateiformat

Sie können eines der folgenden Formate für die Protokolldateien festlegen. Jede Datei wird in eine einzelne Gzip-Datei komprimiert.

- Text – Klartext. Dies ist das Standardformat.
- Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im Klartext. Daten im

Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.

Protokolldateioptionen

Optional können Sie folgende Optionen angeben.

- HIVE-kompatible S3-Präfixe – Aktivieren Sie HIVE-kompatible Präfixe, anstatt Partitionen in Ihre HIVE-kompatiblen Tools zu importieren. Bevor Sie Abfragen ausführen, verwenden Sie den MSCK REPAIR TABLE-Befehl.
- Stündliche Partitionen – Wenn Sie über eine große Anzahl von Protokollen verfügen und Abfragen normalerweise auf eine bestimmte Stunde richten, können Sie schnellere Ergebnisse erzielen und Abfragekosten sparen, indem Sie Protokolle stündlich partitionieren.

S3-Bucket-Struktur der Protokolldatei

Protokolldateien werden im angegebenen Amazon-S3-Bucket mit einer Ordnerstruktur gespeichert, die auf der ID, der Region, dem Erstellungsdatum und den Zieloptionen des Flow-Protokolls basiert.

Standardmäßig werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Wenn Sie HIVE-kompatible S3-Präfixe aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-
region=region/year=year/month=month/day=day/
```

Wenn Sie stündliche Partitionen aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Wenn Sie HIVE-kompatible Partitionen aktivieren und das Flow-Protokoll pro Stunde partitionieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/hour=hour/
```

Protokolldateinamen

Der Dateiname einer Protokolldatei basiert auf der Flow-Protokoll-ID, der Region sowie dem Erstellungsdatum und der Uhrzeit. Dateinamen verwenden das folgende Format:

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Im Folgenden sehen Sie ein Beispiel für eine Protokolldatei für ein Flow-Protokoll, das von AWS-Konto 123456789012 für eine Ressource in der us-east-1-Region am June 20, 2018 um 16:20 UTC erstellt wurde. Die Datei enthält die Flow-Protokolldatensätze mit einer Endzeit zwischen 16:20:00 und 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

IAM-Richtlinie für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen

Der IAM-Prinzipal, der das Flow-Protokoll erstellt, muss über die folgenden Berechtigungen verfügen, die für die Veröffentlichung von Flow-Protokollen im Amazon-S3-Ziel-Bucket erforderlich sind.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

Amazon S3-Bucket-Berechtigungen für Flow-Protokolle

Standardmäßig sind Amazon S3-Buckets und die darin enthaltenen Objekte privat. Nur der Bucket-Besitzer kann auf den Bucket und die darin gespeicherten Objekte zugreifen. Der Bucket-Besitzer kann jedoch anderen Ressourcen und Benutzern Zugriffsberechtigungen erteilen, indem er eine Zugriffsrichtlinie schreibt.

Wenn der Benutzer, der das Flow-Protokoll erstellt, Eigentümer des Buckets ist und `PutBucketPolicy`- und `GetBucketPolicy`-Berechtigungen für den Bucket besitzt, fügen wir automatisch die folgende Richtlinie an den Bucket an. Diese Richtlinie überschreibt alle vorhandenen Richtlinien, die bereits an den Bucket angefügt sind.

Ansonsten muss der Bucket-Eigentümer diese Richtlinie zum Bucket hinzufügen und dabei die AWS-Konto -ID des Flow-Protokoll-Erstellers oder die Erstellung des Flow-Logs schlägt fehl. Weitere Informationen finden Sie unter Verwenden von Bucket-Richtlinien im Benutzerhandbuch für Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl", "s3:ListBucket"],
            "Resource": "arn:aws:s3:::bucket_name",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

Der ARN, den Sie für *meine-s3-arn* angeben hängt davon ab, ob Sie HIVE-kompatible S3-Präfixe verwenden.

- Standardpräfixe

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- HIVE-kompatible S3-Präfixe

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Als bewährte Methode empfehlen wir, diese Berechtigungen nicht einzelnen AWS-Konto ARNs, sondern dem Principal des Protokollzustelldienstes zu gewähren. Es ist auch eine bewährte Methode, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zum Schutz vor dem Problem des verwirrten Stellvertreters zu verwenden. Das Quellkonto ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Platzhalter-AARN (*) des Protokolldienstes.

Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS

Sie können die Daten in Ihrem Amazon-S3-Bucket schützen, indem Sie entweder Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder Serverseitige Verschlüsselung mit KMS-Schlüsseln (SSE-KMS) aktivieren. Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon S3-Entwicklerhandbuch.

Mit SSE-KMS können Sie entweder einen AWS verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden. Mit einem AWS verwalteten Schlüssel können Sie die kontoübergreifende Zustellung nicht verwenden. Flow-Protokolle werden vom

Protokollbereitstellungskonto bereitgestellt, daher müssen Sie Zugriff für die kontoübergreifende Bereitstellung gewähren. Um kontoübergreifenden Zugriff auf Ihren S3 Bucket zu gewähren, verwenden Sie einen kundenverwalteten Schlüssel und geben den Amazon-Ressourcennamen (ARN) des vom Kunden verwalteten Schlüssel an, wenn Sie die Bucket-Verschlüsselung aktivieren. Weitere Informationen finden Sie unter Festlegen einer serverseitigen Verschlüsselung mit AWS KMS im Amazon S3-Benutzerhandbuch.

Wenn Sie SSE-KMS mit einem von Kunden verwalteten Schlüssel verwenden, müssen Sie der Schlüsselrichtlinie für Ihren Schlüssel (nicht der Bucket-Richtlinie für Ihren S3 Bucket) Folgendes hinzufügen, damit VPC-Flow-Protokolle in Ihren S3 Bucket schreiben können.

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Amazon S3-Protokolldateiberechtigungen

Zusätzlich zu den erforderlichen Bucket-Richtlinien verwendet Amazon S3 Zugriffskontrolllisten (ACLs), um den Zugriff auf die durch ein Flow-Protokoll erzeugten Protokolldateien zu verwalten. Standardmäßig hat der Bucket-Eigentümer `FULL_CONTROL`-Berechtigungen für jede Protokolldatei. Der Protokollbereitstellungseigentümer hat keine Berechtigungen, wenn er nicht gleichzeitig der Bucket-Eigentümer ist. Das Konto für die Protokollbereitstellung hat `READ`- und `WRITE`-Berechtigungen. Weitere Informationen finden Sie unter Zugriffskontrollliste (ACL) – Übersicht im Benutzerhandbuch zu Amazon Simple Storage Service.

Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht

Nachdem Sie Ihren Amazon S3-Bucket erstellt und konfiguriert haben, können Sie Flow-Protokolle für Transit-Gateways erstellen.

So erstellen Sie ein Flow-Protokoll für Transit-Gateway, das mithilfe der Konsole in Amazon S3 veröffentlicht

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Aktivieren Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways oder Transit-Gateway-Anhänge.
4. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
5. Konfigurieren Sie die Flow-Protokoll-Einstellungen. Weitere Informationen finden Sie unter So konfigurieren Sie Flow-Protokoll-Einstellungen.

So konfigurieren Sie Flow-Protokolleinstellungen mithilfe der Konsole

1. Wählen Sie für Destination (Ziel) die Option Send to an Amazon S3 bucket (An einen S3 Bucket senden).
2. Geben Sie für S3 bucket ARN (S3-Bucket-ARN) den Amazon-Ressourcennamen (ARN) eines vorhandenen Amazon S3-Buckets an. Sie können optional einen Unterordner einfügen. Um beispielsweise den Unterordner `my-logs` im Bucket `my-bucket` anzugeben, verwenden Sie den folgenden ARN:

   ```
   arn:aws::s3:::my-bucket/my-logs/
   ```

   Der Bucket kann als Unterordnername nicht `AWSLogs` verwenden, da dieser Begriff reserviert ist.

   Wenn Sie der Eigentümer des Buckets sind, erstellen wir automatisch eine Ressourcenrichtlinie und fügen sie dem Bucket hinzu. Weitere Informationen finden Sie unter Amazon S3-Bucket-Berechtigungen für Flow-Protokolle.
3. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.

- Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).
- Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.

4. Geben Sie für Log file format (Protokolldateiformat) das Format für die Protokolldatei an.

   - Text – Klartext. Dies ist das Standardformat.
   - Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im Klartext. Daten im Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.

5. (Optional) Um Hive-kompatible S3-Präfixe zu verwenden, wählen Sie Hive-compatible S3 prefix (Hive-kompatibles S3-Präfix), Enable (Aktivieren).
6. (Optional) Um Ihre Flow-Protokolle pro Stunde zu partitionieren, wählen Sie Every 1 hour (60 mins) (Jede 1 Stunde (60 Minuten)).
7. (Optional) Um dem Flow-Protokoll ein Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie den Tag-Schlüssel und -Wert an.
8. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll, das mithilfe eines Befehlszeilen-Tools in Amazon S3 veröffentlicht

Verwenden Sie einen der folgenden Befehle.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(Amazon EC2 EC2-Abfrage-API)

Das folgende AWS CLI Beispiel erstellt ein Flow-Protokoll, das den gesamten Transit-Gateway-Verkehr für VPC erfasst `tgw-00112233344556677` und die Flow-Logs an einen Amazon S3 S3-Bucket namens `flow-log-bucket` übermittelt. Der Parameter `--log-format` legt ein benutzerdefiniertes Format für die Flow-Protokolldatensätze fest.

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Verarbeiten von Flow-Protokolldatensätzen in Amazon S3

Die Protokolldateien werden komprimiert. Wenn Sie die Protokolldateien unter Verwendung der Amazon S3-Konsole öffnen, werden sie dekomprimiert und die Flow-Protokolldatensätze werden angezeigt. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Flow-Protokolldatensätze anzuzeigen.

Veröffentlichen Sie Flow-Logs in Firehose

Themen

- IAM-Rollen für die kontoübergreifende Bereitstellung
- Erstellen Sie ein Flow-Protokoll, das in Firehose veröffentlicht wird

Flow-Logs können Flow-Log-Daten direkt in Firehose veröffentlichen. Sie können wählen, ob Sie Flow-Protokolle für dasselbe Konto wie den Ressourcenmonitor oder für ein anderes Konto veröffentlichen möchten.

Voraussetzungen

Bei der Veröffentlichung in Firehose werden die Flow-Protokolldaten in einem Firehose-Lieferstream im Klartextformat veröffentlicht. Sie müssen zuerst einen Firehose-Lieferstream erstellt haben. Die Schritte zum Erstellen eines Delivery Streams finden Sie unter Creating an Amazon Data Firehose Delivery Stream im Amazon Data Firehose Developer Guide.

Preise

Es fallen die üblichen Kosten für Einnahme und Lieferung an. Weitere Informationen finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vending Logs.

IAM-Rollen für die kontoübergreifende Bereitstellung

Wenn Sie in Kinesis Data Firehose veröffentlichen, können Sie einen Bereitstellungsstream auswählen, der sich in demselben Konto wie die zu überwachende Ressource (das Quellkonto) oder

in einem anderen Konto (dem Zielkonto) befindet. Um die kontoübergreifende Übermittlung von Flow-Protokollen an Firehose zu ermöglichen, müssen Sie eine IAM-Rolle im Quellkonto und eine IAM-Rolle im Zielkonto erstellen.

Rollen

- Rolle des Quellkontos
- Rolle des Zielkontos

Rolle des Quellkontos

Erstellen Sie im Quellkonto eine Rolle, die die folgenden Berechtigungen gewährt. In diesem Beispiel lautet der Name der Rolle `mySourceRole`, allerdings können Sie einen anderen Namen für diese Rolle wählen. Die letzte Anweisung ermöglicht es der Rolle im Zielkonto, diese Rolle zu übernehmen. Die Bedingungsanweisungen stellen sicher, dass diese Rolle nur an den Protokollbereitstellungsservice und nur beim Überwachen der angegebenen Ressource übergeben wird. Geben Sie beim Erstellen Ihrer Richtlinie die VPCs, Netzwerkschnittstellen oder Subnetze, die Sie überwachen, mit dem Bedingungsschlüssel `iam:AssociatedResourceARN` an.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
              ]
          }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:ListLogDeliveries",
            "logs:GetLogDelivery"
        ],
        "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Stellen Sie sicher, dass Ihre Rolle die folgende Vertrauensrichtlinie hat, die es dem Protokollservice erlaubt, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Führen Sie aus dem Quellkonto die folgenden Schritte zum Erstellen der Rolle aus.

So erstellen Sie die Rolle des Quellkontos

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:

1. Wählen Sie JSON.
2. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
3. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Prüfen) aus.
4. Geben Sie einen Namen und eine optionale Beschreibung für Ihre Richtlinie ein und wählen Sie dann Create Policy (Richtlinie erstellen) aus.

5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Rolle erstellen aus.
7. Für Trusted entity type (Vertrauenstyp der Entität) wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Rolle des Zielkontos

Erstellen Sie im Zielkonto eine Rolle mit einem Namen, der mit beginnt. AWSLogsDeliveryFirehoseCrossAccountRole Die Rolle muss die folgenden Berechtigungen enthalten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Stellen Sie sicher, dass diese Rolle über die folgende Vertrauensrichtlinie verfügt, mit der die Rolle, die Sie im Quellkonto erstellt haben, diese Rolle übernehmen kann.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Führen Sie vom Quellkonto die folgenden Schritte zum Erstellen der Rolle aus.

So erstellen Sie die Rolle des Zielkontos

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:
    1. Wählen Sie JSON.
    2. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
    3. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Prüfen) aus.
    4. Geben Sie einen Namen für Ihre Richtlinie ein, der mit beginnt AWSLogDeliveryFirehoseCrossAccountRole, und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.

6. Wählen Sie Rolle erstellen aus.
7. Für Trusted entity type (Vertrauenstyp der Entität) wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Erstellen Sie ein Flow-Protokoll, das in Firehose veröffentlicht wird

So erstellen Sie ein Transit-Gateway-Flow-Protokoll, das mithilfe der Konsole in Firehose veröffentlicht wird

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Aktivieren Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways oder Transit-Gateway-Anhänge.
4. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
5. Wählen Sie als Destination (Ziel) die Option Send to a Firehose Delivery System (An ein Firehose Delivery System senden) aus.
6. Wählen Sie für den Firehose Delivery Stream ARN (Firehose-Bereitstellungs-Stream-ARN den ARN eines von Ihnen erstellten Bereitstellungs-Streams aus, in dem das Flow-Protokoll veröffentlicht werden soll.
7. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.

   - Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).

- Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.

8. (Optional) Um dem Flow-Protokoll ein Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie den Tag-Schlüssel und -Wert an.
9. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

Um ein Flow-Protokoll zu erstellen, das mit dem Befehlszeilentool in Firehose veröffentlicht wird

Verwenden Sie einen der folgenden Befehle:

- create-flow-logs (CLI)AWS
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(Amazon EC2 EC2-Abfrage-API)

Das folgende AWS CLI-Beispiel erstellt ein Flow-Protokoll, das Transit-Gateway-Informationen erfasst und das Flow-Protokoll an den angegebenen Firehose-Lieferstream übermittelt.

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

Das folgende AWS CLI-Beispiel erstellt ein Flow-Protokoll, das Transit-Gateway-Informationen erfasst und das Flow-Protokoll an einen anderen Firehose-Lieferstream als das Quellkonto übermittelt.

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
  --resource-ids gw-1a2b3c4d \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Arbeiten mit Flow-Protokollen für Transit-Gateway

Sie können mit Transit Gateway Flow Logs über die Amazon EC2-, Amazon VPC- und Amazon S3 S3-Konsolen arbeiten. CloudWatch

Aufgaben

- Kontrollieren der Nutzung von Flow-Protokollen
- Erstellen eines Flow-Protokolls
- Anzeigen von Flow-Protokollen
- Hinzufügen oder Entfernen von Tags für Flow-Protokolle
- Anzeigen von Flow-Protokolldatensätzen
- Suche nach Flow-Protokoll-Datensätzen
- Löschen eines Flow-Protokolls
- API- und CLI-Übersicht und -Einschränkungen

Kontrollieren der Nutzung von Flow-Protokollen

Standardmäßig haben -Benutzer keine Berechtigungen zum Arbeiten mit Flow-Protokollen. Sie können eine Benutzerrichtlinie erstellen, über die Benutzer die Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Flow-Protokollen erhalten. Weitere Informationen finden Sie unter IAM-Benutzern die für Amazon EC2-Ressourcen benötigten Berechtigungen erteilen in der Amazon EC2-API-Referenz.

Nachfolgend finden Sie eine Beispielrichtlinie, die Benutzern uneingeschränkte Berechtigungen erteilt, um Flow-Protokolle zu erstellen, zu beschreiben und zu löschen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Je nachdem, ob Sie in CloudWatch Logs oder Amazon S3 veröffentlichen, sind zusätzliche IAM-Rollen- und Berechtigungskonfigurationen erforderlich. Weitere Informationen erhalten Sie unter Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch und Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht.

Erstellen eines Flow-Protokolls

Sie können Flow-Protokolle für Ihre Transit-Gateways erstellen, die Daten in CloudWatch Logs, Amazon S3 oder Firehose veröffentlichen können.

Weitere Informationen finden Sie hier:

- Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch
- Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht
- Erstellen Sie ein Flow-Protokoll, das in Firehose veröffentlicht wird

Anzeigen von Flow-Protokollen

Sie können Informationen zu den Flow-Protokollen in der Amazon VPC-Konsole auf der Registerkarte Flow Logs (Flow-Protokolle) einer bestimmten Ressource anzeigen. Wenn Sie eine Ressource auswählen, werden alle Flow-Protokolle für diese Ressource aufgelistet. Es werden folgende Informationen angezeigt: die ID des Flow-Protokolls, die Flow-Protokollkonfiguration sowie Informationen zum Status des Flow-Protokolls.

So zeigen Sie Informationen zu Flow-Protokollen für Transit-Gateways an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Wählen Sie ein Transit-Gateway oder Transit-Gateway-Anhang aus und wählen Sie Flow Logs (Flow-Protokolle) aus. Die Informationen zu den Flow-Protokollen werden auf der Registerkarte angezeigt. Die Spalte Destination type (Zieltyp) zeigt das Ziel an, in dem die Flow-Protokolle veröffentlicht werden.

Hinzufügen oder Entfernen von Tags für Flow-Protokolle

Sie können Tags für ein Flow-Protokoll in den Konsolen von Amazon EC2 und Amazon VPC hinzufügen oder entfernen.

So fügen Sie Tags für ein Flow-Protokoll für Transit-Gateway hinzu oder entfernen sie

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Wählen Sie ein Transit-Gateway oder einen Transit-Gateway-Anhang
4. Wählen Sie Manage tags (Tags verwalten) für das jeweilige Flow-Protokoll.
5. Um ein neues Tag hinzuzufügen, wählen Sie Create Tag. Zum Entfernen eines Tags wählen Sie die „Löschen“-Schaltfläche (x) aus.
6. Wählen Sie Speichern.

Anzeigen von Flow-Protokolldatensätzen

Sie können Ihre Flow-Protokolldatensätze je nach ausgewähltem Zieltyp mit der CloudWatch Logs-Konsole oder der Amazon S3 S3-Konsole anzeigen. Es kann nach dem Erstellen eines Flow-Protokolls einige Minuten dauern, bis das Protokoll in der Konsole angezeigt wird.

Um die in Logs veröffentlichten Flow-Log-Datensätze einzusehen CloudWatch

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und danach die Protokollgruppe mit Ihrem Flow-Protokoll. Es wird eine Liste der Protokollstreams für die einzelnen Transit-Gateways angezeigt.
3. Wählen Sie den Protokollstream aus, der die ID des Transit-Gateways enthält, für das Sie die Flow-Protokolldatensätze anzeigen möchten. Weitere Informationen finden Sie unter Flow-Protokolldatensätze für Transit-Gateway.

So zeigen Sie in Amazon S3 veröffentlichte Flow-Protokolldatensätze an

1. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.

2. Wählen Sie für Bucket name (Bucket-Name) den Bucket aus, in den die Flow-Protokolle veröffentlicht werden.
3. Markieren Sie für Name das Kontrollkästchen neben der Protokolldatei. Wählen Sie im Objektübersichtsfeld Download.

Suche nach Flow-Protokoll-Datensätzen

Sie können Ihre in CloudWatch Logs veröffentlichten Flow-Protokolldatensätze mithilfe der CloudWatch Logs-Konsole durchsuchen. Sie können Metrikfilter verwenden, um Flow-Protokolldatensätze zu filtern. Flow-Protokolldatensätze sind durch Leerzeichen getrennt.

So suchen Sie mit der CloudWatch Logs-Konsole nach Flow-Log-Datensätzen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und dann Log groups (Protokollgruppen) aus.
3. Wählen Sie die Protokollgruppe mit Ihrem Flow-Protokoll. Es wird eine Liste der Protokollstreams für die einzelnen Transit-Gateways angezeigt.
4. Wählen Sie den einzelnen Protokollstream aus, wenn Sie den Transit-Gateway kennen, nach dem Sie suchen. Alternativ können Sie Search Log Group (Log-Gruppe durchsuchen) wählen, um die gesamte Protokollgruppe zu durchsuchen. Dies kann einige Zeit in Anspruch nehmen, wenn sich viele Transit-Gateways in Ihrer Protokollgruppe befinden oder je nach ausgewähltem Zeitbereich.
5. Geben Sie für Filter events (Filterereignisse) die folgende Zeichenfolge ein. Hierbei wird davon ausgegangen, dass der Flow-Protokolldatensatz das Standardformat verwendet.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. Ändern Sie den Filter nach Bedarf, indem Sie Werte für die Felder angeben. In den folgenden Beispielen wird nach bestimmten Quell-IP-Adressen gefiltert.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Das folgende Beispiel filtert nach Transit-Gateway-ID tgw-123abc456bca, Zielport und Anzahl der Bytes.

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Löschen eines Flow-Protokolls

Sie können ein Flow-Protokoll für Transit-Gateway über die Amazon VPC-Konsole löschen.

Mithilfe dieser Verfahren wird der Flow-Protokoll-Service für eine Ressource deaktiviert. Durch das Löschen eines Flow-Protokolls werden die vorhandenen Protokollstreams aus CloudWatch Protokollen oder Protokolldateien aus Amazon S3 nicht gelöscht. Vorhandene Flow-Protokolldaten müssen über die Konsole des jeweiligen Service gelöscht werden. Außerdem entfernt das Löschen eines Flow-Protokolls, das in Amazon S3 veröffentlicht wird, nicht die Bucket-Richtlinien und die Protokolldatei-Zugriffskontrolllisten (ACLs).

So löschen Sie ein Flow-Protokoll für Transit-Gateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie eine Transit-Gateway-ID aus.
4. Wählen Sie im Abschnitt „Flow-Protokolle“ die Flow-Protokolle aus, die Sie löschen möchten.
5. Wählen Sie Actions (Aktionen) und dann Delete flow logs group (Flow-Protokolle löschen) aus.
6. Bestätigen Sie, dass Sie den Flow löschen möchten, indem Sie Delete (Löschen) auswählen.

API- und CLI-Übersicht und -Einschränkungen

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder API ausführen.

Die folgenden Einschränkungen gelten beim Verwenden des `CreateFlowLogs`-API oder des `create-flow-logs`-CLI:

- `--resource-ids` hat eine maximale Beschränkung von 25 `TransitGateway` oder `TransitGatewayAttachment` Ressourcentypen.
- `--traffic-type` ist standardmäßig kein erforderliches Feld. Ein Fehler wird zurückgegeben, wenn Sie dies für Transit-Gateway-Ressourcentypen angeben. Dieses Limit gilt nur für Transit-Gateway-Ressourcentypen.
- `--max-aggregation-interval` besitzt den `60`-Standardwert und ist der einzige akzeptierte Wert für Transit-Gateway-Ressourcentypen. Wenn Sie versuchen, einen anderen Wert zu übergeben, wird ein Fehler zurückgegeben. Dieses Limit gilt nur für Transit-Gateway-Ressourcentypen.
- `--resource-type` unterstützt zwei neue Ressourcentypen: `TransitGateway` und `TransitGatewayAttachment`.
- `--log-format` schließt alle Protokollfelder für Transit-Gateway-Ressourcentypen ein, wenn Sie nicht festlegen, welche Felder Sie einbeziehen möchten. Dies gilt nur für Transit-Gateway-Ressourcentypen.

Erstellen eines Flow-Protokolls

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

- CreateFlowLogs(Amazon EC2 EC2-Abfrage-API)

Beschreibung Ihrer Flow-Protokolle

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs(Amazon EC2 EC2-Abfrage-API)

Anzeigen Ihrer Flow-Protokolldatensätze (Protokollereignisse)

- get-log-events (AWS CLI)
- GET-cwl (LogEvent)AWS Tools for Windows PowerShell
- GetLogEvents(API) CloudWatch

Löschen eines Flow-Protokolls

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs(Amazon EC2 EC2-Abfrage-API)

Überwachen Ihrer Transit Gateways

Sie können die folgenden Features verwenden, um Ihre Transit Gateways zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihren Transit Gateways beheben.

CloudWatch-Metriken

Sie können mit Amazon-CloudWatch-Statistiken zu Datenpunkten für Ihre Transit Gateways als eine geordnete Reihe von Zeitreihendaten, auch als Metriken bezeichnet, abrufen. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch-Metriken für Ihre Transit Gateways.

Flow-Protokolle für Transit-Gateway

Sie können mit Flow-Protokollen für Transit-Gateway detaillierte Informationen über den Netzwerkverkehr auf Ihren Transit-Gateways erfassen. Weitere Informationen finden Sie unter Flow-Protokolle für Transit-Gateway.

VPC-Flow-Protokolle

Mit VPC-Flow-Protokollen können Sie detaillierte Informationen über den Datenverkehr zu und von den VPCs erfassen, die Ihren Transit Gateways angehängt sind. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon-VPC-Benutzerhandbuch.

CloudTrail-Protokolle

Sie können AWS CloudTrail verwenden, um detaillierte Informationen zu den Aufrufen der Transit-Gateway-API zu erfassen, und sie als Protokolldateien in Amazon S3 speichern. Sie können diese CloudTrail-Protokolle verwenden, um die durchgeführten Aufrufe, die Quell-IP-Adresse, von welcher der Aufruf stammte, den Aufrufer, den Zeitpunkt des Aufrufs usw. zu ermitteln. Weitere Informationen finden Sie unter Protokollieren von API-Aufrufen für Ihr Transit Gateway mit AWS CloudTrail.

CloudWatch Events mit Network Manager

Sie können mit AWS Network Manager Events an CloudWatch und diese dann an Zielfeatures oder Streams weiterleiten. Network Manager generiert Events für Topologieänderungen, Routing-Updates und Statusaktualisierungen, die alle verwendet werden können, um Sie auf Änderungen an Ihren Transit-Gateways aufmerksam zu machen. Weitere Informationen finden Sie unter Überwachung Ihres globalen Netzwerks mit CloudWatch Events im Benutzerhandbuch für AWS globale Netzwerke für Transit Gateways.

CloudWatch-Metriken für Ihre Transit Gateways

Amazon VPC veröffentlicht Datenpunkte für Ihre Transit Gateways und Transit-Gateway-Anhänge in Amazon CloudWatch. CloudWatch ermöglicht Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten, als Metriken bezeichnet, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können z. B. einen CloudWatch-Alarm erstellen, um eine bestimmte Metrik zu überwachen, und eine Aktion einleiten (z. B. Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb eines für Sie akzeptablen Bereichs liegt.

Amazon VPC misst und sendet Metriken in 60-Sekunden-Intervallen an CloudWatch.

Weitere Informationen finden Sie im Amazon-CloudWatch-Benutzerhandbuch.

Inhalt

- Transit-Gateway-Metriken
- Metrik-Dimensionen für Transit Gateways

Transit-Gateway-Metriken

Der `AWS/TransitGateway`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`BytesDropCountBlackhole`	Die Anzahl der verworfenen Bytes, weil sie einer `blackhole` -Route entsprachen
`BytesDropCountNoRoute`	Die Anzahl der verworfenen Bytes, weil sie keiner Route entsprachen.
`BytesIn`	Die Anzahl der vom Transit Gateway empfangenen Bytes.
`BytesOut`	Die Anzahl der vom Transit Gateway gesendeten Bytes.
`PacketsIn`	Die Anzahl der vom Transit Gateway empfangenen Pakete.

Metrik	Beschreibung
`PacketsOut`	Die Anzahl der vom Transit Gateway gesendeten Pakete.
`PacketDropCountBlackhole`	Die Anzahl der verworfenen Pakete, weil sie einer `blackhole` -Route entsprachen
`PacketDropCountNoRoute`	Die Anzahl der verworfenen Pakete, weil sie keiner Route entsprachen

Metriken auf Anhangsebene

Die folgenden Metriken sind für Transit-Gateway-Anhänge verfügbar. Alle Anhangs-Metriken werden im Konto des Transit-Gateway-Besitzers veröffentlicht. Alle Anhangs-Metriken werden im Konto des Anhang-Besitzers veröffentlicht. Der Anhang-Besitzer kann nur die Metriken für seinen eigenen Anhang anzeigen. Weitere Informationen zu den unterstützten Anlagentypen finden Sie unter the section called “Ressourcen-Anhänge”.

Metrik	Beschreibung
`BytesDropCountBlackhole`	Die Anzahl der Bytes, die gelöscht wurden, weil sie einer `blackhole` -Route auf dem Transit-Gateway-Anhang entsprachen.
`BytesDropCountNoRoute`	Die Anzahl der Bytes, die gelöscht wurden, weil sie nicht mit einer Route auf dem Transit-Gateway-Anhang übereinstimmten.
`BytesIn`	Die Anzahl der von dem Transit-Gateway-Anhang empfangenen Bytes.
`BytesOut`	Die Anzahl der vom Transit Gateway an den Anhang gesendeten Bytes.
`PacketsIn`	Die Anzahl der Pakete, die das Transit Gateway von dem Anhang empfangen hat.
`PacketsOut`	Die Anzahl der vom Transit Gateway an den Anhang gesendeten Pakete.

Metrik	Beschreibung
`PacketDropCountBlackhole`	Die Anzahl der Pakete, die gelöscht wurden, weil sie einer `blackhole` -Route auf dem Transit-Gateway-Anhang entsprachen.
`PacketDropCountNoRoute`	Die Anzahl der Pakete, die gelöscht wurden, weil sie nicht mit einer Route auf dem Transit-Gateway-Anhang übereinstimmten.

Metrik-Dimensionen für Transit Gateways

Verwenden Sie die folgenden Dimensionen, um die Metriken für Ihre Transit Gateways zu filtern.

Dimension	Beschreibung
`TransitGateway`	Filtert die Metrikdaten nach Transit Gateway.
`TransitGatewayAttachment`	Filtert die Metrikdaten nach Transit-Gateway-Anhang.

Protokollieren von API-Aufrufen für Ihr Transit Gateway mit AWS CloudTrail

AWS CloudTrail ist ein Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Services protokolliert. CloudTrail erfasst alle API-Aufrufe des Transit Gateways als Ereignisse. Die erfassten Aufrufe enthalten Aufrufe von der AWS Management Console und Code-Aufrufe der Transit-Gateway-API-Operationen. Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignissen für Transit Gateways. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail erfassten Informationen können Sie die an die Transit-Gateway-API gesendete Anforderung, die IP-Adresse, von der die Anforderung stammt, den Initiator der Anforderung, den Zeitpunkt der Anforderung und zusätzliche Details bestimmen.

Weitere Informationen zu Transit-Gateway-APIs finden Sie im Abschnitt AWS-Transit-Gateway-Aktionen in der Amazon-EC2-API-Referenz.

Weitere Informationen über CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Transit-Gateway-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn eine Aktivität über die Transit-Gateway-API stattfindet, wird diese Aktivität in einem CloudTrail-Ereignis zusammen mit anderen AWS-Service-Ereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Erstellen Sie einen Trail für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für die Transit-Gateway-API. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Aufrufe von Transit-Gateway-Aktionen werden von CloudTrail protokolliert. Aufrufe der Aktion `CreateTransitGateway` generieren beispielsweise 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 Anforderung mit Root- oder AWS Identity and Access Management-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

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

Informationen zu Transit-Gateway-Protokolldatei-Einträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Die Protokolldateien enthalten Ereignisse für alle API-Aufrufe für Ihr AWS-Konto, nicht nur Transit-Gateway-API-Aufrufe. Sie können Aufrufe der Transit-Gateway-API finden, indem Sie nach `eventSource`-Elementen mit dem Wert `ec2.amazonaws.com` suchen. Um einen Datensatz für eine bestimmte Aktion anzuzeigen, z. B. `CreateTransitGateway`, suchen Sie nach `eventName`-Elementen mit dem Aktionsnamen.

Im Folgenden finden Sie Beispiele für CloudTrail-Protokoll-Datensätze für die Transit-Gateway-API für einen Benutzer, der ein Transit Gateway mit der Konsole erstellt hat. Sie können die Konsole mithilfe des `userAgent`-Elements identifizieren. Sie können den angeforderten API-Aufruf mithilfe der `eventName`-Elemente identifizieren. Informationen zum Benutzer (`Alice`) finden Sie im `userIdentity`-Element.

Example Beispiel: CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
```

```
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
```

```
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Identity and Access Management für Ihre Transit Gateways

AWS verwendet Sicherheitsanmeldeinformationen, um Sie zu identifizieren und Ihnen Zugriff auf Ihre AWS-Ressourcen zu gewähren. Sie können Funktionen von AWS Identity and Access Management (IAM) verwenden, um anderen Benutzern, Services und Anwendungen die uneingeschränkte oder eingeschränkte Nutzung Ihrer AWS-Ressourcen zu erlauben, ohne Ihre Sicherheitsanmeldeinformationen zu teilen.

IAM-Benutzer sind standardmäßig nicht berechtigt, AWS-Ressourcen zu erstellen, anzuzeigen oder zu ändern. Um einem Benutzer zu erlauben, auf Ressourcen wie ein Transit Gateway zuzugreifen und Aufgaben auszuführen, müssen Sie eine IAM-Richtlinie erstellen, die dem Benutzer die Berechtigung zum Verwenden der spezifischen benötigten Ressourcen und API-Funktionen gewährt. Fügen Sie dann die Richtlinie an die Gruppe an, welcher der Benutzer angehört. Wenn Sie einem Benutzer oder einer Benutzergruppe eine Richtlinie zuordnen, wird den Benutzern die Ausführung der angegebenen Aufgaben für die angegebenen Ressourcen gestattet oder verweigert.

Für ein Transit Gateway kann beispielsweise eine der folgenden von AWS verwalteten Richtlinien Ihre Anforderungen erfüllen:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Beispielrichtlinien für die Verwaltung von Transit Gateways

Im Folgenden finden Sie IAM-Beispielrichtlinien für das Arbeiten mit Transit Gateways.

Erstellen eines Transit Gateways mit den erforderlichen Tags

Im folgenden Beispiel können Benutzer Transit Gateways erstellen. Der `aws:RequestTag`-Bedingungsschlüssel erfordert, dass Benutzer das Transit Gateway mit dem `stack=prod`-Tag kennzeichnen. Der `aws:TagKeys`-Bedingungsschlüssel verwendet den Modifikator `ForAllValues`, um anzuzeigen, dass nur der Schlüssel `stack` in der Anforderung zulässig ist (es können keine anderen Tags angegeben werden). Wenn Benutzer dieses spezifische Tag beim Erstellen des Transit Gateways nicht übergeben, oder wenn sie überhaupt keine Tags angeben, schlägt die Anforderung fehl.

Die zweite Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Benutzer Tags nur im Kontext von `CreateTransitGateway` erstellen können.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Arbeiten mit Transit-Gateway-Routing-Tabellen

Im folgenden Beispiel können Benutzer nur für ein bestimmtes Transit Gateway Routing-Tabellen erstellen und löschen (`tgw-11223344556677889`). Benutzer können Routen auch in einer beliebigen Routing-Tabelle des Transit Gateways erstellen und ersetzen, jedoch nur für Anhänge mit dem Tag `network=new-york-office`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

Beispielrichtlinien für die Verwaltung von AWS-Network Manager

Beispielrichtlinien finden Sie unter Beispielrichtlinien zur Verwaltung von Network Manager im AWS-Benutzerhandbuch für Global Networks for Transit Gateways.

Verwendung von serviceverknüpften Rollen für Ihre Transit Gateways

Amazon VPC nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS-Services in Ihrem Namen benötigt werden. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch.

Serviceverknüpfte Rolle für Transit Gateways

Amazon VPC verwendet serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS-Services in Ihrem Namen benötigt werden, wenn Sie mit einem Transit Gateway arbeiten.

Von der serviceverknüpften Rolle erteilte Berechtigungen

Amazon VPC verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForVPCTransitGateway zum Aufrufen der folgenden Aktionen in Ihrem Namen, wenn Sie mit einem Transit Gateway arbeiten:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

Die Rolle AWSServiceRoleForVPCTransitGateway vertraut den folgenden Services, die diese Rolle übernehmen:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway verwendet die verwaltete Richtlinie AWSVPCTransitGatewayServiceRolePolicy.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpften Rolle

Sie brauchen die Rolle AWSServiceRoleForVPCTransitGateway nicht manuell zu erstellen. Amazon VPC erstellt diese Rolle für Sie, wenn Sie eine VPC in Ihrem Konto an ein Transit Gateway anhängen.

Damit Amazon VPC eine serviceverknüpfte Rolle in Ihrem Namen erstellen kann, müssen Sie über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Bearbeiten der serviceverknüpften Rolle

Sie können die Beschreibung von AWSServiceRoleForVPCTransitGateway mithilfe von IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle

Wenn Sie keine Transit Gateways mehr benötigen, empfehlen wir, die Rolle AWSServiceRoleForVPCTransitGateway zu löschen.

Sie können diese serviceverknüpfte Rolle erst löschen, wenn alle Transit-Gateway-VPC-Anhänge aus Ihrem AWS-Konto gelöscht wurden. Auf diese Weise wird sichergestellt, dass Sie nicht versehentlich die Berechtigung für den Zugriff auf Ihre VPC-Anhänge entfernen.

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um serviceverknüpfte Rollen zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Nach dem Löschen von AWSServiceRoleForVPCTransitGateway erstellt Amazon VPC die Rolle erneut, wenn Sie einem Transit Gateway eine VPC aus Ihrem Konto anhängen.

AWS-verwaltete Richtlinien für Transit Gateways

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind.

Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

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

Für ein Transit Gateway kann beispielsweise eine der folgenden von AWS verwalteten Richtlinien Ihre Anforderungen erfüllen:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS-verwaltete Richtlinie: AWSVPCTransitGatewayServiceRolePolicy

Diese Richtlinie ist der Rolle AWSServiceRoleForVPCTransitGateway zugeordnet. Auf diese Weise kann Amazon VPC Ressourcen für Ihre Transit-Gateway-Anhänge erstellen und verwalten.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AWSVPCTransitGatewayServiceRolePolicy in der AWS-verwalteten Richtlinienreferenz.

Transit-Gateway-Aktualisierungen zur AWS-verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für Transit Gateways, seit Amazon VPC mit der Verfolgung dieser Änderungen im März 2021 begonnen hat.

Änderung	Beschreibung	Datum
Amazon VPC hat mit der Verfolgung von Änderungen begonnen	Amazon VPC begann mit der Nachverfolgung von	1. März 2021

Änderung	Beschreibung	Datum
	Änderungen an seinen von AWS verwalteten Richtlinien.	

Funktionsweise von Netzwerk-ACLs mit Transit Gateways

Eine Netzwerk-ACL (Network Access Control List; NACL) ist eine optionale Sicherheitsebene.

NACL-Regeln werden je nach Szenario unterschiedlich angewendet:

- the section called “Gleiches Subnetz für EC2-Instances und Transit-Gateway-Zuordnung”
- the section called “Verschiedene Subnetze für EC2-Instances und Transit-Gateway-Zuordnung”

Gleiches Subnetz für EC2-Instances und Transit-Gateway-Zuordnung

Betrachten Sie eine Konfiguration, bei der Sie über EC2-Instances und eine Transit-Gateway-Zuordnung im selben Subnetz verfügen. Die gleiche Netzwerk-ACL wird sowohl für den Datenverkehr von den EC2-Instances zum Transit-Gateway als auch für den Datenverkehr vom Transit-Gateway zu den Instances verwendet.

NACL-Regeln werden auf folgende Weise für den Datenverkehr von Instances zum Transit Gateway angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse für die Auswertung.
- Eingehende Regeln verwenden die Quell-IP-Adresse für die Auswertung.

NACL-Regeln werden auf folgende Weise für den Datenverkehr vom Transit Gateway zu den Instances angewendet:

- Ausgehende Regeln werden nicht ausgewertet.
- Eingehende Regeln werden nicht ausgewertet.

Verschiedene Subnetze für EC2-Instances und Transit-Gateway-Zuordnung

Betrachten Sie eine Konfiguration, bei der Sie EC2-Instances in einem Subnetz und eine Transit-Gateway-Zuordnung in einem anderen Subnetz haben und jedes Subnetz einer anderen Netzwerk-ACL zugeordnet ist.

Netzwerk-ACL-Regeln werden für das EC2-Instance-Subnetz wie folgt angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse, um den Datenverkehr von den Instances auf das Transit-Gateway auszuwerten.
- Eingehende Regeln verwenden die Quell-IP-Adresse, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.

NACL-Regeln werden für das Transit-Gateway-Subnetz wie folgt angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.
- Ausgehende Regeln werden nicht verwendet, um den Datenverkehr von den Instances zum Transit-Gateway auszuwerten.
- Eingehende Regeln verwenden die Quell-IP-Adresse, um den Datenverkehr von den Instances auf das Transit-Gateway auszuwerten.
- Eingehende Regeln werden nicht verwendet, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.

Bewährte Methoden

Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz. Verwenden Sie für jedes Subnetz einen kleinen CIDR, z. B. /28, damit Sie mehr Adressen für EC2-Ressourcen haben. Wenn Sie ein separates Subnetz verwenden, können Sie Folgendes konfigurieren:

- Halten Sie die eingehende und ausgehende NACL offen, die den Transit-Gateway-Subnetzen zugeordnet ist.
- Abhängig von Ihrem Datenverkehrsfluss können Sie NACLs auf Ihre Workload-Subnetze anwenden.

Weitere Informationen zu der Funktionsweise von VPC-Anhängen finden Sie unter the section called “Ressourcen-Anhänge”.

Kontingente für Ihre Transit Gateways

Ihr AWS-Konto hat die folgenden Kontingente (früher als Limits bezeichnet) in Bezug auf Transit-Gateways. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Die Service-Quotas-Konsole enthält Informationen zu Kontingenten für Ihr Konto. Sie können die Service Quotas-Konsole verwenden, um Standard-Kontingente anzuzeigen und Kontingent-Erhöhungen für einstellbare Kontingente anzufordern. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service Quotas-Benutzerhandbuch.

Wenn in Service Quotas noch kein anpassbares Kontingent verfügbar ist, können Sie einen Supportfall öffnen.

Allgemeines

Name	Standard	Anpassbar
Transit Gateways pro Konto	5	Ja
CIDR-Blöcke pro Transit Gateway	5	Nein

Die CIDR-Blöcke werden im the section called “Connect-Anfügungen und Connect-Peers”-Feature verwendet.

Routing

Name	Standard	Anpassbar
Transit-Gateway-Routing-Tabellen pro Transit Gateway	20	Ja
Gesamtzahl kombinierter Routen (dynamisch und statisch) über alle Routentabellen für ein einzelnes Transit-Gateway	10.000	Ja

Name	Standard	Anpassbar
Von einer virtuellen Router-Appliance an einen Connect-Peer angekündigte dynamische Routen	1.000	Ja
Von einem Connect-Peer auf einem Transit Gateway an eine virtuelle Router-Appliance angekündigte Routen	5,000	Nein
Statische Routen für ein Präfix eines einzelnen Anhangs	1	Nein

Die angekündigten Routen stammen aus der Routing-Tabelle für den Connect-Anhang.

Transit-Gateway-Anhänge

Ein Transit Gateway darf nicht mehr als einen VPC-Anhang zur selben VPC haben.

Name	Standard	Anpassbar
Anhänge pro Transit Gateway	5,000	Nein
Transit Gateways pro VPC	5	Nein
Peering-Anhänge pro Transit Gateway	50	Ja
Ausstehende Peering-Anhänge pro Transit Gateway	10	Ja
Peering-Verbindungen zwischen zwei Transit-Gateways oder zwischen einem Transit-Gateway und einem Cloud WAN-Core-Netzwerk-Edge (CNE)	1	Nein
Connect-Peers (GRE-Tunnel) pro Connect-Anfügung	4	Nein

Bandbreite

Es gibt viele Faktoren, die die realisierte Bandbreite durch eine Site-to-Site-VPN-Verbindung beeinflussen können, einschließlich, aber nicht beschränkt auf: Paketgröße, Traffic-Mix (TCP/UDP), Gestaltungs- oder Drosselungsrichtlinien in Zwischennetzwerken, Internetwetter und spezifische Anwendungsanforderungen. Für VPC-Anhänge, AWS Direct Connect Gateways oder Peering-Transit-Gateway-Anhänge werden wir versuchen, zusätzliche Bandbreite bereitzustellen, die über den Standardwert hinausgeht.

Name	Standard	Anpassbar
Bandbreite pro VPC-Anhang pro Availability Zone	Bis zu 100 GBit/s	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Pakete pro Sekunde pro Transit-Gateway-VPC-Anhang pro Availability Zone	Bis zu 7 500 000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Bandbreite für die AWS Direct Connect Gateway- oder Peer-Transit-Gateway-Verbindung pro verfügbarer Availability Zone in der Region	Bis zu 100 GBit/s	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Pakete pro Sekunde pro Transit-Gateway-Verbindung (AWS Direct Connect und Peering-Anhängen) pro verfügbarer Availability Zone in der Region	Bis zu 7 500 000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder

Name	Standard	Anpassbar
		Technical Account Manager (TAM).
Maximale Bandbreite pro VPN-Tunnel	Bis zu 1,25 GBit/s	Nein
Maximale Anzahl an Paketen pro Sekunde pro VPN-Tunnel	Bis zu 140.000	Nein
Maximale Bandbreite pro Transit-Gateway-Connect-Peer (GRE-Tunnel) pro Connect-Anhang	Bis zu 5 GBit	Nein
Maximale Anzahl der Pakete pro Sekunde pro Connect-Peer	Bis zu 300.000	Nein

Sie können Equal-Cost Multipath Routing (ECMP) verwenden, um eine höhere VPN-Bandbreite zu erzielen, indem Sie mehrere VPN-Tunnel aggregieren. Zur Verwendung von ECMP muss die VPN-Verbindung für dynamisches Routing konfiguriert sein. ECMP wird nicht für VPN-Verbindungen unterstützt, die statisches Routing nutzen.

Sie können bis zu 4 Connect-Peers pro Connect-Anhang erstellen (bis zu 20 Gbit/s Gesamtbandbreite pro Connect-Anhang), sofern der zugrunde liegende Transportanhang (VPC oder AWS Direct Connect) die erforderliche Bandbreite unterstützt. Sie können Equal-Cost-Multi-Path-Routing (ECMP) verwenden, um eine höhere Bandbreite zu erhalten, indem Sie die horizontale Skalierung über mehrere Connect-Peers derselben Connect-Verbindung oder über mehrere Connect-Verbindungen am selben Transit Gateway nutzen. Für den Transit-Gateway ist kein ECMP zwischen den BGP-Peerings desselben Connect-Peers möglich.

AWS Direct Connect Gateways

Name	Standard	Anpassbar
AWS Direct Connect Gateways pro Transit-Gateway	20	Nein
Transit-Gateways pro Gateway AWS Direct Connect	6	Nein

Maximum Transmission Unit (MTU)

- Die MTU einer Netzwerkverbindung ist die Größe des größten zulässigen Pakets, das über die Verbindung übertragen werden kann, in Byte. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein Transit-Gateway unterstützt eine MTU von 8500 Byte für den Verkehr zwischen VPCs AWS Direct Connect, Transit Gateway Connect und Peering-Anhängen. Datenverkehr über VPN-Verbindungen kann eine MTU von 1 500 Byte haben.
- Eine Nichtübereinstimmung der MTU-Größe zwischen VPC-Peering und dem Transit Gateway kann dazu führen, dass einige Pakete für asymmetrischen Datenverkehr gelöscht werden. Aktualisieren Sie beide VPCs gleichzeitig, um zu vermeiden, dass Jumbo-Pakete aufgrund von Größenunterschieden gelöscht werden.
- Pakete mit einer Größe von mehr als 8 500 Bytes, die am Transit Gateway ankommen, werden verworfen.
- Das Transit Gateway generiert nicht das FRAG_NEEDED für ICMPv4-Pakete bzw. das Packet Too Big (PTB) für ICMPv6-Pakete. Daher wird die Path MTU Discovery (PMTUD) nicht unterstützt.
- Das Transit Gateway erzwingt das Klemmen der maximalen Segmentgröße (MSS) für alle Pakete. Weitere Informationen finden Sie unter RFC879
- Einzelheiten zu Site-to-Site-VPN-Kontingenten für MTU finden Sie unter Maximale Übertragungseinheit (MTU) im AWS Site-to-Site VPN -Benutzerhandbuch.

Multicast

Name	Standard	Anpassbar
Multicast-Domains pro Transit Gateway	20	Ja
Multicast-Netzwerkschnittstellen pro Transit Gateway	10.000	Ja
Multicast-Domainzuordnungen pro VPC	20	Ja
Quellen pro Transit-Gateway-Multicast-Gruppe	1	Ja

Name	Standard	Anpassbar
Statische Multicast-Gruppen- und IGMPv2-Multicast-Gruppenmitglieder und -quellen pro Transit Gateway	10.000	Nein
Statische Multicast-Gruppen- und IGMPv2-Multicast-Gruppenmitglieder pro Transit-Gateway-Multicast-Gruppe	100	Nein
Maximaler Multicast-Durchsatz pro Flow	1 Gbit/s	Nein
Maximaler aggregierter Multicast-Durchsatz pro Availability Zone	20 Gbit/s	Nein

AWS Netzwerk-Manager

Name	Standard	Anpassbar
Globale Netzwerke pro AWS-Konto	5	Ja
Geräte pro globales Netzwerk	200	Ja
Links pro globales Netzwerk	200	Ja
Standorte pro globales Netzwerk	200	Ja
Verbindungen pro globales Netzwerk	500	Nein

Zusätzliche Kontingentressourcen

Weitere Informationen finden Sie unter:

- Site-to-Site VPN-Kontingente im AWS Site-to-Site VPN Benutzerhandbuch
- Amazon-VPC-Kontingente im Amazon-VPC-Benutzerhandbuch
- AWS Direct Connect -KontingenteimAWS Direct Connect Benutzerhandbuch

Dokumentverlauf für Transit Gateways

In der folgenden Tabelle werden die Veröffentlichungen für Transit Gateways beschrieben.

Änderung	Beschreibung	Datum
Kontingente für AWS Transit Gateway	Bandbreitenbeschränkungen wurden hinzugefügt.	14. August 2023
Flow-Protokolle für AWS-Transit-Gateway	Transit Gateways unterstützen jetzt Flow-Protokolle für Transit-Gateway, wodurch Sie den Netzwerkverkehr zwischen Transit-Gateways überwachen und protokollieren können.	14. Juli 2022
Transit-Gateway-Richtlinientabellen	Verwenden Sie Richtlinientabellen, um für ein automatisches Austauschen von Routing- und Erreichbarkeitsinformationen mit Peered-Transit-Gateway-Typen ein dynamisches Routing für Transit-Gateways einzurichten.	13. Juli 2022
Benutzerhandbuch zu Network Manager	Network Manager wurde als eigenständiger Leitfaden erstellt und ist nicht mehr Teil des Benutzerhandbuchs zu AWS Transit Gateway.	2. Dezember 2021
Peering-Anlagen	Sie können eine Peering-Verbindung mit einem Transit Gateway in der gleichen Region erstellen.	1. Dezember 2021

Transit Gateway Connect	Sie können eine Verbindung zwischen einem Transit Gateway und virtuellen Appliances von Drittanbietern herstellen, die in einer VPC ausgeführt werden.	10. Dezember 2020
Appliance-Modus	Sie können den Appliance-Modus für einen VPC-Anhang aktivieren, um sicherzustellen, dass der bidirektionale Datenverkehr durch dieselbe Availability Zone für den Anhang fließt.	29. Oktober 2020
Präfixlistenreferenzen	Sie können in der Transit-Gateway-Routing-Tabelle auf eine Präfixliste verweisen.	24. August 2020
Ändern des Transit-Gateways	Sie können die Konfigurations-Optionen für den Transit Gateway ändern.	24. August 2020
CloudWatch-Metriken für Transit-Gateway-Anfügungen	Sie können CloudWatch-Metriken für einzelne Transit-Gateway-Anhänge anzeigen.	6. Juli 2020
Network Manager Route Analyzer	Sie können die Routen in den Transit-Gateway-Routing-Tabellen in Ihrem globalen Netzwerk analysieren.	4. Mai 2020
Peering-Anlagen	Sie können eine Peering-Verbindung mit einem Transit Gateway in einer anderen Region erstellen.	3. Dezember 2019

Multicast-Unterstützung	Transit Gateway unterstützt das Routing von Multicast-Datenverkehr zwischen Subnetzen angefügter VPCs und dient als Multicast-Router für Instances, die Datenverkehr an mehrere empfangende Instances senden.	3. Dezember 2019
AWS-Network Manager	Sie können globale Netzwerke visualisieren und überwachen, die auf Transit Gateways basieren.	3. Dezember 2019
AWS Direct Connect--Support	Sie können ein AWS Direct Connect-Gateway verwenden, um Ihre AWS Direct Connect-Verbindung über eine virtuelle Transit-Schnittstelle mit den VPCs oder VPNs zu verbinden, die an das Transit Gateway angefügt sind.	27. März 2019
Erstversion	In dieser Version werden Transit Gateways eingeführt.	26. November 2018

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.