AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Che cos'è Amazon VPC Transit Gateways?

Amazon VPC Transit Gateways è un hub di transito di rete utilizzato per interconnettere cloud privati virtuali (VPCs) e reti locali. Man mano che la tua infrastruttura cloud si espande a livello globale, il peering interregionale collega i gateway di transito utilizzando l'infrastruttura globale. AWS Tutto il traffico di rete tra AWS i data center viene automaticamente crittografato a livello fisico.

Per ulteriori informazioni, consulta AWS Transit Gateway.

Concetti dei gateway di transito

Di seguito sono riportati i concetti chiave per i gateway di transito:

- Collegamenti: puoi decidere di collegare quanto segue:
  - Uno o più VPCs
  - Un dispositivo di rete Connect WAN SD/di terze parti
  - Un gateway AWS Direct Connect
  - Una connessione peering con un altro gateway di transito
  - Una VPN connessione a un gateway di transito
- Unità di trasmissione massima del gateway di transito (MTU): l'unità di trasmissione massima (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito che può essere passato sulla connessione. Maggiore è la dimensione MTU di una connessione, maggiore è la quantità di dati che possono essere trasmessi in un singolo pacchetto. Un gateway MTU di transito supporta 8500 byte per il traffico tra VPCs AWS Direct Connect, Transit Gateway Connect e gli allegati di peering (allegati di peering intra-regionale, interregionale e cloud). WAN Il traffico sulle connessioni può avere una dimensione di 1500 byte. VPN MTU
- Tabella di routing del gateway di transito: un gateway di transito ha una tabella di routing predefinita e facoltativamente può avere tabelle di routing aggiuntive. Una tabella di routing include route dinamiche e statiche che determinano il segmento di rete successivo in base all'indirizzo IP di destinazione del pacchetto. L'obiettivo di queste route potrebbe essere qualsiasi collegamento di un gateway di transito. Per impostazione predefinita, gli allegati del gateway di transito sono associati alla tabella di route del gateway di transito predefinita.
- Associazioni: ogni collegamento è associato a una sola tabella di routing. Le tabelle di routing possono essere associate a nessuno o a molti collegamenti.

- Propagazione delle rotte: un gatewayVPC, VPN connection o Direct Connect può propagare dinamicamente le rotte a una tabella di routing del gateway di transito. Per impostazione predefinita, con un allegato Connect le route vengono propagate a una tabella di routing del gateway di transito. Con aVPC, è necessario creare percorsi statici per inviare il traffico al gateway di transito. Con una VPN connessione, le rotte vengono propagate dal gateway di transito al router locale utilizzando Border Gateway Protocol ()BGP. Con un gateway Direct Connect, i prefissi consentiti vengono originati sul router locale utilizzando. BGP Con un allegato di peering, è necessario creare un route statico nella tabella di routing del gateway di transito per puntare all'allegato di peering.

Come iniziare a usare i gateway di transito

Utilizza le risorse seguenti per creare e utilizzare un gateway di transito.

- Come funzionano i gateway di transito
- Inizia a usare Transit Gateways
- Best Practice di progettazione

Utilizzo dei gateway di transito

Puoi creare, accedere e gestire i gateway di transito utilizzando una qualsiasi delle seguenti interfacce:

- AWS Management Console — Fornisce un'interfaccia web da utilizzare per l'accesso ai gateway di transito.
- AWS Command Line Interface (AWS CLI): fornisce comandi per un'ampia gamma di AWS servizi, tra cui AmazonVPC, ed è supportato su Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS SDKs— Fornisce API operazioni specifiche della lingua e si occupa di molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta AWS SDKs.
- Interrogazione API: fornisce azioni di basso livello API richiamabili utilizzando le richieste. HTTPS L'uso di Query API è il modo più diretto per accedere ad AmazonVPC, ma richiede che l'applicazione gestisca dettagli di basso livello come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta Amazon EC2 API Reference.

Prezzi

Ti verrà addebitata ogni ora per ogni allegato in un gateway di transito e ti verrà addebitata la quantità di traffico elaborata sul gateway di transito. Per ulteriori informazioni, consulta Prezzi di AWS Transit Gateway.

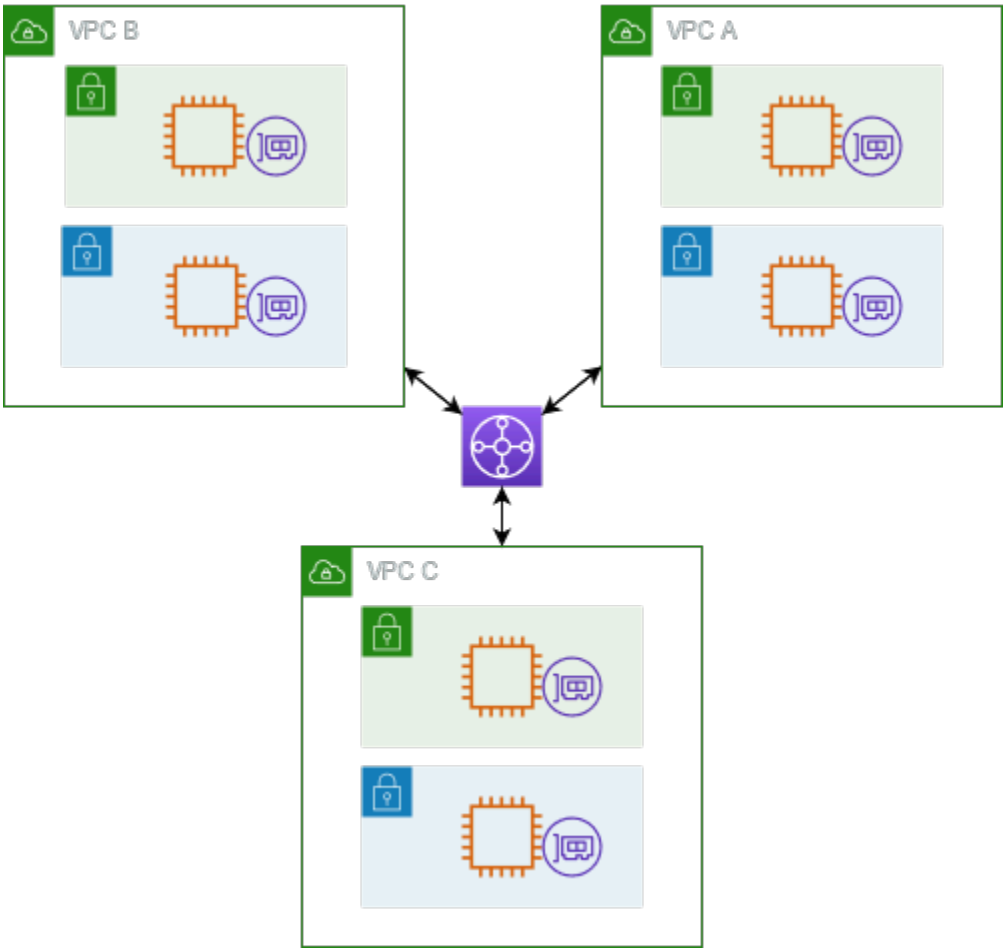
Come funzionano Amazon VPC Transit Gateways

In AWS Transit Gateway, un gateway di transito funge da router virtuale regionale per il flusso di traffico tra i cloud privati virtuali (VPCs) e le reti locali. Un gateway di transito si ridimensiona in modo elastico sulla base del volume di traffico di rete. Il routing attraverso un gateway di transito opera al livello 3, in cui i pacchetti vengono inoltrati a uno specifico collegamento di un sistema adiacente, in base agli indirizzi IP di destinazione.

Argomenti

Esempio di diagramma di architettura

Il diagramma seguente mostra un gateway di transito con tre VPC allegati. La tabella dei percorsi per ognuno di questi VPCs include il percorso locale e i percorsi che inviano il traffico destinato agli altri due VPCs al gateway di transito.



Di seguito è riportato un esempio di una tabella di instradamento del gateway di transito di default per i collegamenti mostrati nel diagramma precedente. I CIDR blocchi per ciascuno VPC si propagano alla tabella delle rotte. Pertanto, ogni collegamento può instradare i pacchetti agli altri due collegamenti.

Destinazione	Target	Tipo di route
VPC A CIDR	*Attachment for VPC A*	propagata
VPC B CIDR	*Attachment for VPC B*	propagata
VPC C CIDR	*Attachment for VPC C*	propagata

Collegamenti alle risorse

Un collegamento a un gateway di transito costituisce sia una sorgente che una destinazione di pacchetti. È possibile allegare le seguenti risorse al gateway di transito:

- Uno o piùVPCs. AWS Transit Gateway implementa un'interfaccia di rete elastica all'interno delle VPC sottoreti, che viene quindi utilizzata dal gateway di transito per instradare il traffico da e verso le sottoreti scelte. È necessario disporre di almeno una sottorete per ciascuna zona di disponibilità, che consente al traffico di raggiungere le risorse in tutte le sottorete di tale zona. Durante la creazione di allegati, le risorse all'interno di una particolare zona di disponibilità possono raggiungere un gateway di transito solo se una sottorete è abilitata all'interno della stessa zona. Se una tabella di routing di sottorete include un routing al gateway di transito, il traffico viene inoltrato al gateway di transito solo quando il gateway di transito dispone di un allegato in una sottorete nella stessa zona di disponibilità.
- VPNUna o più connessioni
- Uno o più AWS Direct Connect gateway
- Uno o più allegati Transit Gateway Connect
- Una o più connessioni di peering del gateway di transito

Instradamento Equal Cost Multipath

AWS Transit Gateway supporta il routing Equal Cost Multipath (ECMP) per la maggior parte degli allegati. Per un VPN allegato, è possibile abilitare o disabilitare il ECMP supporto utilizzando la console durante la creazione o la modifica di un gateway di transito. Per tutti gli altri tipi di allegati, si applicano le seguenti ECMP restrizioni:

- VPC- VPC non supporta ECMP poiché i CIDR blocchi non possono sovrapporsi. Ad esempio, non è possibile collegare un gateway di transito a un gateway di transito VPC con un CIDR 10.1.0.0/16 con un secondo VPC utilizzo dello stesso e quindi impostare il routing CIDR per bilanciare il carico del traffico tra di essi.
- VPN- Quando l'opzione di VPNECMPsupporto è disabilitata, un gateway di transito utilizza metriche interne per determinare il percorso preferito in caso di prefissi uguali su più percorsi. Per ulteriori informazioni sull'attivazione o la disabilitazione di un VPN allegato, ECMP vedere. the section called “Gateway di transito”
- AWS Transit Gateway Connect: supporto ECMP automatico per gli allegati AWS Transit Gateway Connect.

- AWS Direct Connect Gateway: gli allegati AWS Direct Connect gateway supportano ECMP automaticamente più allegati Direct Connect Gateway quando il prefisso di rete, la lunghezza del prefisso e AS_ PATH sono esattamente gli stessi.
- Peering del gateway di transito - Il peering del gateway di transito non è supportato in ECMP quanto non supporta il routing dinamico né è possibile configurare la stessa route statica su due destinazioni diverse.

> **Note**
>
> - BGPMultipath AS-Path Relax non è supportato, quindi non è possibile utilizzarlo ECMP su diversi Autonomous System Numbers (). ASNs
> - ECMPnon è supportato tra diversi tipi di allegati. Ad esempio, non è possibile abilitare ECMP tra a VPN e un VPC allegato. Invece, vengono valutate le route del gateway di transito e il traffico viene indirizzato in base alla route valutata. Per ulteriori informazioni, consulta the section called “Ordine di valutazione route”.
> - Un singolo gateway Direct Connect supporta ECMP più interfacce virtuali di transito. Pertanto, si consiglia di configurare e utilizzare un solo gateway Direct Connect e di ECMP non configurare e utilizzare più gateway da sfruttare. Per ulteriori informazioni sui gateway Direct Connect e sulle interfacce virtuali pubbliche, vedi Come si configura una connessione Active/Active or Active/Passive Direct Connect AWS da un'interfaccia virtuale pubblica? .

Zone di disponibilità

Quando si collega VPC a un gateway di transito, è necessario abilitare una o più zone di disponibilità affinché il gateway di transito utilizzi per indirizzare il traffico verso le risorse nelle VPC sottoreti. Per abilitare ogni zona di disponibilità, è necessario specificare una sola sottorete. Il gateway di transito crea un'interfaccia di rete in tale sottorete usando un indirizzo IP della sottorete stessa. Dopo aver abilitato una zona di disponibilità, il traffico può essere indirizzato a tutte le sottoreti della stessaVPC, non solo alla sottorete o alla zona di disponibilità specificata. Tuttavia, solo le risorse che risiedono nelle zone di disponibilità in cui è presente un collegamento del gateway di transito alla VPN possono raggiungere il gateway di transito.

Se il traffico proviene da una zona di disponibilità in cui l'allegato di destinazione non è presente, AWS Transit Gateway indirizzerà internamente tale traffico verso una zona di disponibilità casuale in

cui è presente l'allegato. Non è previsto alcun costo aggiuntivo per il gateway di transito per questo tipo di traffico tra Zone di disponibilità.

Per assicurare la disponibilità, raccomandiamo di abilitare molteplici zone di disponibilità.

Utilizzo del supporto della modalità accessorio

Se prevedi di configurare un'appliance di rete con stato sul tuo dispositivoVPC, puoi abilitare il supporto in modalità appliance per l'VPCallegato in cui si trova l'appliance. Ciò garantisce che il gateway di transito utilizzi la stessa zona di disponibilità per l'VPCallegato per l'intera durata di un flusso di traffico tra origine e destinazione. Consente inoltre al gateway di transito di inviare traffico a qualsiasi zona di disponibilità dellaVPC, purché esista un'associazione di sottoreti in quella zona. Per ulteriori informazioni, consulta Esempio: dispositivo in un servizio condiviso VPC.

Routing

Il gateway di transito instrada IPv4 e IPv6 i pacchetti tra gli allegati utilizzando le tabelle di routing del gateway di transito. È possibile configurare queste tabelle di routing per propagare le route dalle tabelle di route per i gateway collegatiVPCs, VPN le connessioni e Direct Connect. È inoltre possibile aggiungere route statiche alle tabelle di route del gateway di transito. Quando un pacchetto proviene da un collegamento, viene indirizzato a un altro collegamento utilizzando la route che contiene una regola per l'indirizzo IP di destinazione.

Per gli allegati di peering del gateway di transito, sono supportati solo route statici.

Argomenti di routing

- Tabelle di instradamento
- Associazione di tabelle di routing
- Propagazione delle tabelle di routing
- Route per gli allegati peering
- Ordine di valutazione route

Tabelle di instradamento

Il gateway di transito viene fornito automaticamente con una tabella dei percorsi predefinita. Per impostazione predefinita, questa tabella di routing è la tabella di routing predefinita per i collegamenti nonché la tabella di routing predefinita per la propagazione. In alternativa, disabilitando

la propagazione del routing e l'associazione della tabella di routing, AWS non crea una tabella di routing predefinita per il gateway di transito.

È possibile creare tabelle di route aggiuntive per il gateway di transito. Ciò permette di isolare gruppi di collegamenti. Ogni allegato può essere associato a una tabella di instradamento. Un allegato può propagare i propri instradamenti a una o più tabelle di routing

È possibile creare una route blackhole nella tabella di routing del gateway di transito che intercetti il traffico corrispondente alla route.

Quando si collega un gateway di transito VPC a un gateway di transito, è necessario aggiungere un percorso alla tabella delle rotte della sottorete affinché il traffico possa attraversare il gateway di transito. Per ulteriori informazioni, consulta Routing for a Transit Gateway nella Amazon VPC User Guide.

Associazione di tabelle di routing

È possibile associare un allegato del gateway di transito a una singola tabella di route. Ogni tabella di routing può essere associata da zero a molti collegamenti e può inoltrare i pacchetti agli altri allegati.

Propagazione delle tabelle di routing

Ogni collegamento dispone di route che possono essere installate in una o più tabelle di routing del gateway di transito. Quando un collegamento è propagato a una tabella di routing del gateway di transito, tali route sono aggiunte alla tabella di routing. Non è possibile filtrare i percorsi pubblicizzati.

Per un VPC allegato, i CIDR blocchi di VPC vengono propagati alla tabella di routing del gateway di transito.

Quando il routing dinamico viene utilizzato con un VPN allegato o un allegato gateway Direct Connect, è possibile propagare i percorsi appresi dal router locale BGP a qualsiasi tabella di routing del gateway di transito.

Quando il routing dinamico viene utilizzato con un VPN allegato, le rotte nella tabella di routing associata all'VPNallegato vengono pubblicizzate al gateway del cliente tramite. BGP

Per un allegato Connect, le route nella tabella delle route associata all'allegato Connect vengono pubblicizzate alle appliance virtuali di terze parti, come le WAN appliance SD, che funzionano in modalità VPC throughBGP.

Per un collegamento al gateway Direct Connect, le interazioni con prefissi consentiti controllano da quali percorsi vengono pubblicizzati alla rete del cliente. AWS

Quando una route statica e una route propagata hanno la stessa destinazione, la route statica ha la priorità più alta e la route propagata non viene quindi inclusa nella tabella di instradamento. Se si rimuove la route statica, la route propagata sovrapposta viene inclusa nella tabella di instradamento.

Route per gli allegati peering

È possibile eseguire il peering di due gateway di transito e instradare il traffico tra di loro. A tale scopo, creare un allegato di peering nel gateway di transito e specificare il gateway di transito peer con cui creare la connessione di peering. È quindi necessario creare una route statica nella tabella di route del gateway di transito per instradare il traffico all'allegato peering del gateway di transito. Il traffico indirizzato al gateway di transito peer può quindi essere instradato verso VPN gli allegati VPC e per il gateway di transito peer.

Per ulteriori informazioni, consulta Esempio: gateway di transito in peering.

Ordine di valutazione route

I route dei gateway di transito sono valutati nell'ordine seguente:

- Il percorso più specifico per l'indirizzo di destinazione.
- Per i percorsi con gli stessi CIDR tipi di allegati ma con tipi di allegati diversi, la priorità del percorso è la seguente:
  - Percorsi statici (ad esempio percorsi Site-to-Site VPN statici)
  - Route referenziate dell'elenco di prefissi
  - VPC-rotte propagate
  - Percorsi propagati dal gateway Direct Connect
  - Percorsi propagati da Transit Gateway Connect
  - Site-to-Site VPNsu percorsi privati propagati da Direct Connect
  - Site-to-Site VPN-percorsi propagati
  - Percorsi propagati tramite peering Transit Gateway (Cloud) WAN

Alcuni allegati supportano Route Advertising over. BGP Per i percorsi con lo stesso CIDR tipo di allegato e dello stesso tipo di allegato, la priorità del percorso è controllata da BGP attributi:

- Lunghezza del percorso AS più breve
- MEDValore inferiore
- I BGP percorsi e BGP over i sono preferiti, se l'allegato lo supporta

> **Important**
>
> AWS non può garantire un ordine di priorità delle rotte coerente per le BGP rotte con lo stesso CIDR tipo di allegato e gli stessi BGP attributi elencati sopra.

AWS Transit Gateway mostra solo una rotta preferita. Un percorso di backup verrà visualizzato nella tabella delle rotte Transit Gateway solo se tale percorso non è più pubblicizzato, ad esempio se pubblicizzi gli stessi percorsi tramite il gateway Direct Connect e oltre Site-to-SiteVPN. AWS Transit Gateway mostrerà solo le rotte ricevute dalla rotta gateway Direct Connect, che è la rotta preferita. Il Site-to-SiteVPN, che è il percorso di backup, verrà visualizzato solo quando il gateway Direct Connect non è più pubblicizzato.

VPCe differenze nella tabella delle rotte del gateway di transito

La valutazione della tabella delle rotte varia a seconda che si utilizzi una tabella di VPC rotte o una tabella di rotte del gateway di transito.

L'esempio seguente mostra una tabella di VPC rotte. Il percorso VPC locale ha la priorità più alta, seguito dai percorsi più specifici. Quando un route statico e propagato hanno la stessa destinazione, la route statica ha la priorità più alta.

Destinazione	Target	Priorità
10.0.0.0/16	locale	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (statico) o tgw-12345 (statico)	2
172.31.0.0/16	vgw-12345 (propagato)	3
0.0.0.0/0	igw-12345	4

L'esempio seguente mostra una tabella delle rotte dei gateway di transito. Se preferite l'allegato del AWS Direct Connect gateway all'VPNallegato, utilizzate una BGP VPN connessione e propagate le rotte nella tabella delle rotte del gateway di transito.

Destinazione	Allegato (target)	Tipo di risorsa	Tipo di route	Priorità
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Statico o propagato	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Statico	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect gateway	Propagato	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Connessione	Propagato	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagato	5

Esempi di scenari di gateway di transito

Di seguito sono riportati casi di utilizzo comuni per i gateway di transito. I gateway di transito non sono limitati a questi casi di utilizzo.

Esempio: router centralizzato

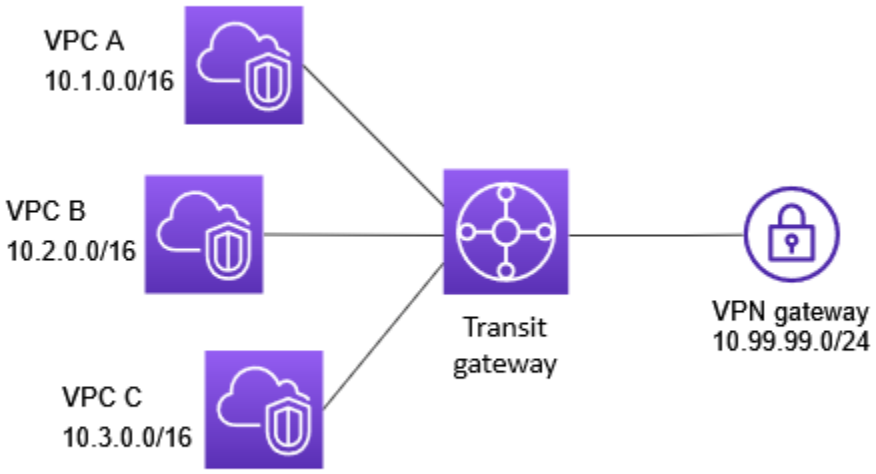
Puoi configurare il tuo gateway di transito come un router centralizzato che collega tutte le tue connessioni e Site-to-Site VPN tutte VPCs le AWS Direct Connect tue connessioni. In questo scenario, tutti i allegati sono associati alla tabella di routing predefinita del gateway di transito e si propagano alla tabella di routing del gateway di transito. Pertanto, tutti i collegamenti possono instradare i pacchetti tra di essi, con il gateway di transito che assume il ruolo di un semplice router IP di livello 3.

Indice

- Panoramica
- Risorse
- Routing

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. In questo scenario, ci sono tre VPC allegati e un Site-to-Site VPN allegato al gateway di transito. I pacchetti provenienti dalle sottoreti in A, VPC B e VPC C destinati a VPC una sottorete in un'altra VPC o alla prima VPN connessione vengono instradati attraverso il gateway di transito.



Risorse

Crea le seguenti risorse per questo scenario:

- TreVPCs. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre VPC allegati sul gateway di transito. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
- Un Site-to-Site VPN allegato sul gateway di transito. I CIDR blocchi per ciascuno di essi VPC si propagano nella tabella delle rotte del gateway di transito. Quando la VPN connessione è attiva, la

BGP sessione viene stabilita e si Site-to-Site VPN CIDR propaga alla tabella di routing del gateway di transito e viene VPC CIDRs aggiunta alla tabella del gateway BGP del cliente. Per ulteriori informazioni, consulta the section called “Crea un gateway di transito collegato a VPN”.

Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Routing

Ciascuno VPC ha una tabella di routing e c'è una tabella di routing per il gateway di transito.

VPCtabelle dei percorsi

Ciascuna VPC ha una tabella dei percorsi con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale inVPC; questa voce consente alle istanze in essa contenute di VPC comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i percorsi VPC A.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	tgw-id

Tabella di routing del gateway di transito

Di seguito è riportato un esempio di una tabella di instradamento predefinita per i collegamenti mostrati nel diagramma precedente, con la propagazione delle route abilitate.

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata
10.3.0.0/16	*Attachment for VPC C*	propagata

Destinazione	Target	Tipo di route
10.99.99.0/24	*Attachment for VPN connection*	propagata

BGPTabella Customer Gateway

La BGP tabella Customer Gateway contiene quanto segue VPCCIDRs.

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

Esempio: isolato VPCs

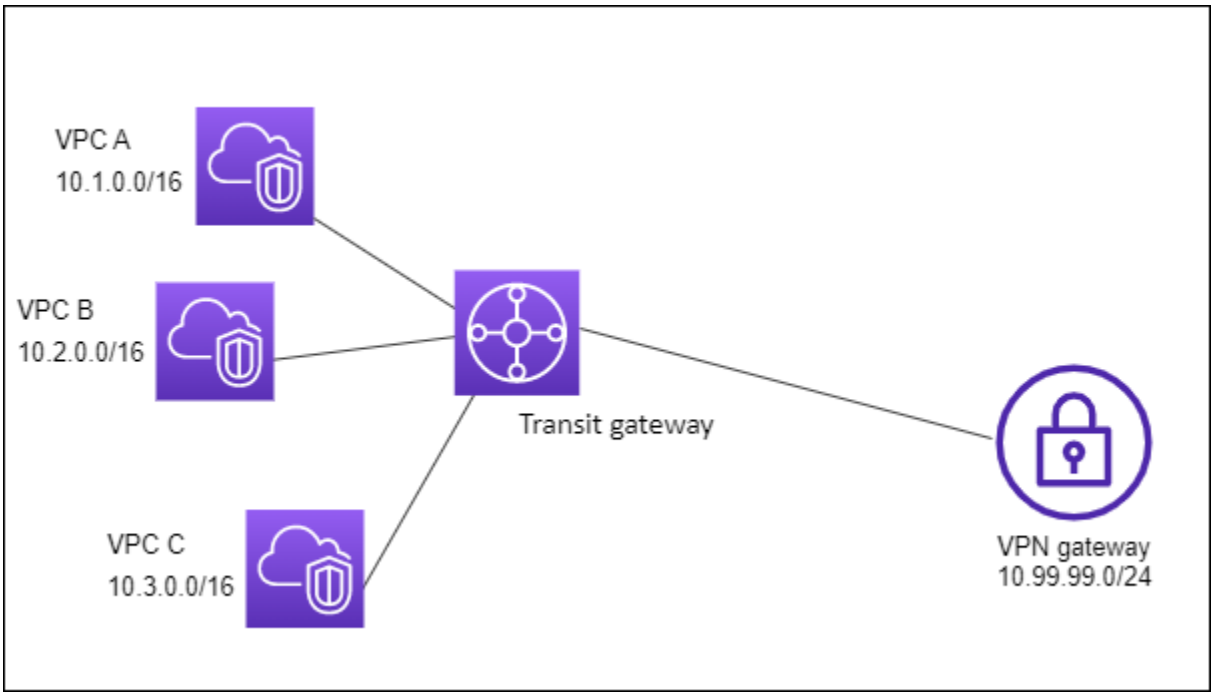
È possibile configurare il gateway di transito come più router isolati. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. In questo scenario, ogni router isolato dispone di una singola tabella di routing. Tutti i collegamenti associati a un router isolato propagano e associano la sua tabella di instradamento. I collegamenti associati a un router isolato possono instradare i pacchetti tra loro, ma non possono instradare o ricevere pacchetti dai collegamenti di un altro router isolato.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. I pacchetti provenienti da VPC A, VPC B e VPC C vengono instradati verso il gateway di transito. I pacchetti provenienti dalle sottoreti di VPC A, VPC B e VPC C che hanno Internet come destinazione vengono prima instradati attraverso il gateway di transito e quindi vengono indirizzati verso la Site-to-Site VPN connessione (se la destinazione si trova all'interno di tale rete). I pacchetti provenienti da uno VPC che ha la destinazione di una sottorete in un'altraVPC, ad esempio da 10.1.0.0 a 10.2.0.0,

vengono instradati attraverso il gateway di transito, dove vengono bloccati perché non esiste un percorso per loro nella tabella delle rotte del gateway di transito.



Risorse

Crea le seguenti risorse per questo scenario:

- TreVPCs. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati sul gateway di transito per i treVPCs. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
- Un Site-to-Site VPN allegato sul gateway di transito. Per ulteriori informazioni, consulta the section called “Crea un gateway di transito collegato a VPN”. Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Quando la VPN connessione è attiva, la BGP sessione viene stabilita e VPN CIDR si propaga alla tabella di routing del gateway di transito e viene VPC CIDRs aggiunta alla BGP tabella del gateway del cliente.

Routing

Ciascuna VPC ha una tabella di routing e il gateway di transito ha due tabelle di routing, una per la connessione VPCs e una per la connessione. VPN

VPCTabelle di routing VPC A, B e C VPC

Ciascuna VPC ha una tabella dei percorsi con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale in. VPC Questa voce consente alle istanze in essa contenute VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i percorsi VPC A.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	tgw-id

Tabelle di routing del gateway di transito

Questo scenario utilizza una tabella di routing per VPCs e una tabella di route per la VPN connessione.

Gli VPC allegati sono associati alla seguente tabella di routing, che contiene una route propagata per l'VPNallegato.

Destinazione	Target	Tipo di route
10.99.99.0/24	*Attachment for VPN connection*	propagata

L'VPNallegato è associato alla seguente tabella di routing, che contiene percorsi propagati per ciascuno degli allegati. VPC

Destinazione	Target	Tipo di route

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata
10.3.0.0/16	*Attachment for VPC C*	propagata

Per ulteriori informazioni sulla propagazione delle route in una tabella di routing del gateway di transito, consulta Abilita la propagazione delle rotte su una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways.

Tabella Customer Gateway BGP

La BGP tabella Customer Gateway contiene quanto segue VPCCIDRs.

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

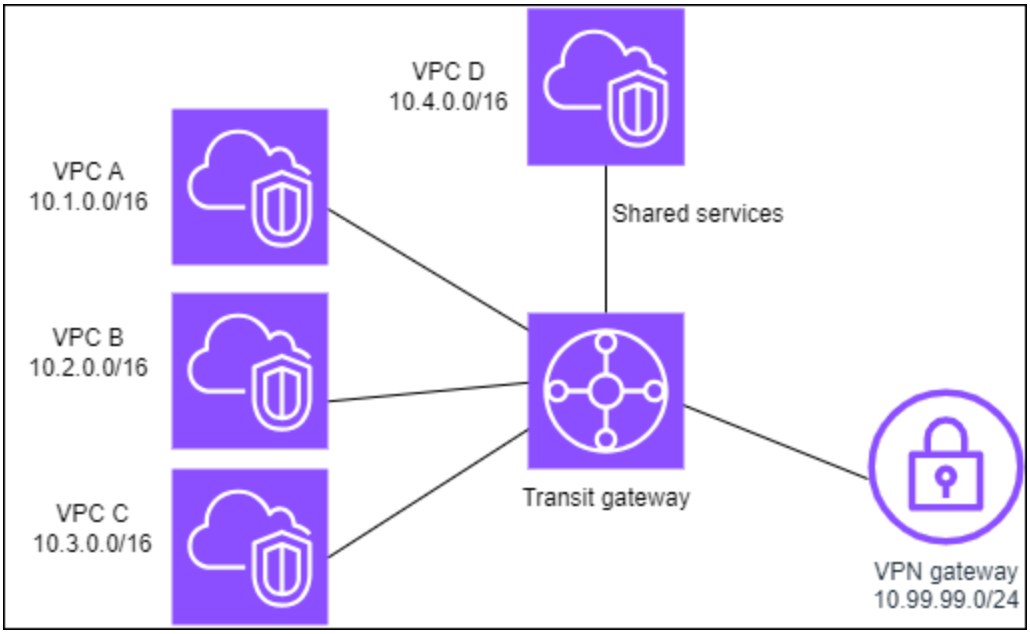
Esempio: isolato VPCs con servizi condivisi

È possibile configurare il gateway di transito come molteplici router isolati che utilizzano un servizio condiviso. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. In questo scenario, ogni router isolato dispone di una singola tabella di routing. Tutti i collegamenti associati a un router isolato propagano e associano la sua tabella di instradamento. I collegamenti associati a un router isolato possono instradare i pacchetti tra loro, ma non possono instradare o ricevere pacchetti dai collegamenti di un altro router isolato. Gli allegati possono instradare pacchetti oppure per ricevere i pacchetti dai servizi condivisi. È possibile utilizzare questo scenario in presenza di gruppi che devono essere isolati, ma che utilizzano un servizio condiviso, ad esempio un sistema di produzione.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. I pacchetti provenienti dalle sottoreti in VPC A, VPC B e VPC C che hanno Internet come destinazione, vengono prima instradati attraverso il gateway di transito e poi vengono indirizzati verso il gateway del cliente per. Site-to-Site VPN I pacchetti provenienti da sottoreti in VPC A, VPC B o VPC C che hanno come destinazione una sottorete in A, VPC B o VPC C attraversano il gateway di transito, dove vengono bloccati perché non esiste VPC un relativo percorso nella tabella delle rotte del gateway di transito. I pacchetti provenienti da VPC A, VPC B e VPC C che hanno VPC D come percorso di destinazione attraverso il gateway di transito e quindi verso D. VPC



Risorse

Crea le seguenti risorse per questo scenario:

- QuattroVPCs. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- Un gateway di transito. Per ulteriori informazioni, consulta Gateway di transito.
- Quattro allegati sul gateway di transito, uno per. VPC Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
- Un Site-to-Site VPN allegato sul gateway di transito. Per ulteriori informazioni, consulta the section called “Crea un gateway di transito collegato a VPN”.

  Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Quando la VPN connessione è attiva, la BGP sessione viene stabilita e VPN CIDR si propaga alla tabella di routing del gateway di transito e viene VPC CIDRs aggiunta alla BGP tabella del gateway del cliente.

- Ogni isolato VPC viene associato alla tabella di routing isolata e propagato alla tabella di routing condivisa.
- Ogni servizio condiviso VPC è associato alla tabella di routing condivisa e propagato a entrambe le tabelle di routing.

Routing

Ciascuna VPC ha una tabella di routing e il gateway di transito ha due tabelle di routing, una per la VPN connessione VPCs e una per i servizi condivisi. VPC

VPCTabelle di VPC routing A, B, VPC C e D VPC

Ciascuna VPC ha una tabella dei percorsi con due voci. La prima voce è la voce predefinita per il routing locale inVPC; questa voce consente alle istanze in essa contenute di VPC comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	*transit gateway ID*

Tabelle di routing del gateway di transito

Questo scenario utilizza una tabella di routing per VPCs e una tabella di route per la VPN connessione.

Gli allegati VPC A, B e C sono associati alla seguente tabella di routing, che contiene una route propagata per l'VPNattacco e una route propagata per l'attacco per D. VPC

Destinazione	Target	Tipo di route
10.99.99.0/24	*Attachment for VPN connection*	propagata

Destinazione	Target	Tipo di route
10.4.0.0/16	*Attachment for VPC D*	propagata

Gli VPN allegati e i servizi condivisi VPC (VPCD) sono associati alla seguente tabella di routing, che contiene voci che puntano a ciascuno degli allegati. VPC Ciò consente la comunicazione VPCs tra la VPN connessione e i servizi condivisi. VPC

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata
10.3.0.0/16	*Attachment for VPC C*	propagata

Per ulteriori informazioni, consulta Abilita la propagazione delle rotte su una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways.

BGPTabella Customer Gateway

La BGP tabella Customer Gateway contiene i CIDRs dati per tutti e quattroVPCs.

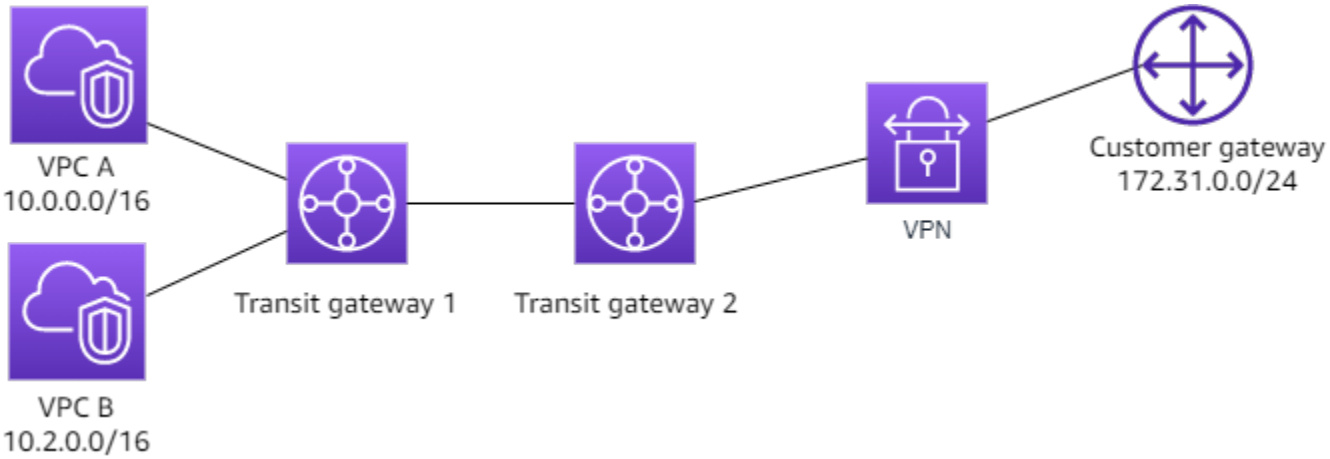
Esempio: gateway di transito in peering

È possibile creare una connessione di peering del gateway di transito tra gateway di transito. È quindi possibile instradare il traffico tra gli allegati per ciascuno dei gateway di transito. In questo scenario, VPN gli VPC allegati sono associati alle tabelle di routing predefinite del gateway di transito e si propagano alle tabelle di routing predefinite del gateway di transito. Ogni tabella di instradamento del gateway di transito ha un route statico che punta all'allegato peering del gateway di transito.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Il gateway di transito 1 ha due VPC allegati e il gateway di transito 2 ha un allegato. Site-to-Site VPN I pacchetti provenienti dalle sottoreti in VPC A e VPC B che hanno Internet come destinazione vengono prima instradati attraverso il gateway di transito 1, quindi il gateway di transito 2 e quindi vengono instradati verso la connessione. VPN



Risorse

Crea le seguenti risorse per questo scenario:

- Due VPCs. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- Due gateway di transito. Possono trovarsi nella stessa regione o in diverse regioni. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Due VPC allegati sul primo gateway di transito. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
- Un Site-to-Site VPN allegato sul secondo gateway di transito. Per ulteriori informazioni, consulta the section called “Crea un gateway di transito collegato a VPN”. Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .
- Un allegato peering del gateway di transito tra i due gateway di transito. Per ulteriori informazioni, consulta Allegati di peering del gateway di transito in Amazon VPC Transit Gateway.

Quando si creano gli VPC allegati, CIDRs for each si VPC propagano alla tabella di routing per il gateway di transito 1. Quando la VPN connessione è attiva, si verificano le seguenti azioni:

- La BGP sessione viene stabilita

- Site-to-SiteVPNCIDRSi propaga alla tabella delle rotte per il gateway di transito 2
- VPCCIDRsVengono aggiunti alla tabella del gateway BGP del cliente

Routing

Ciascuno VPC ha una tabella delle rotte e ogni gateway di transito ha una tabella delle rotte.

VPCTabelle di routing A e VPC B

Ciascuna VPC ha una tabella dei percorsi con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale in. VPC Questa voce predefinita consente alle risorse in essa contenute VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i percorsi VPC A.

Destinazione	Target
10.0.0.0/16	locale
0.0.0.0/0	tgw-1-id

Tabelle di routing del gateway di transito

Di seguito è riportato un esempio della tabella di instradamento predefinita per il gateway di transito 1, con la propagazione del percorso abilitata.

Destinazione	Target	Tipo di route
10.0.0.0/16	*Attachment ID for VPC A*	propagata
10.2.0.0/16	*Attachment ID for VPC B*	propagata
0.0.0.0/0	*Attachment ID for peering connection*	static

Di seguito è riportato un esempio di tabella di instradamento predefinita per il gateway di transito 2, con la propagazione del routing attivata.

Destinazione	Target	Tipo di route
172.31.0.0/24	*Attachment ID for VPN connection*	propagata
10.0.0.0/16	*Attachment ID for peering connection*	static
10.2.0.0/16	*Attachment ID for peering connection*	static

BGPTabella Customer Gateway

La BGP tabella Customer Gateway contiene quanto segue VPCCIDRs.

- 10.0.0.0/16
- 10.2.0.0/16

Esempio: Routing in uscita centralizzato verso Internet

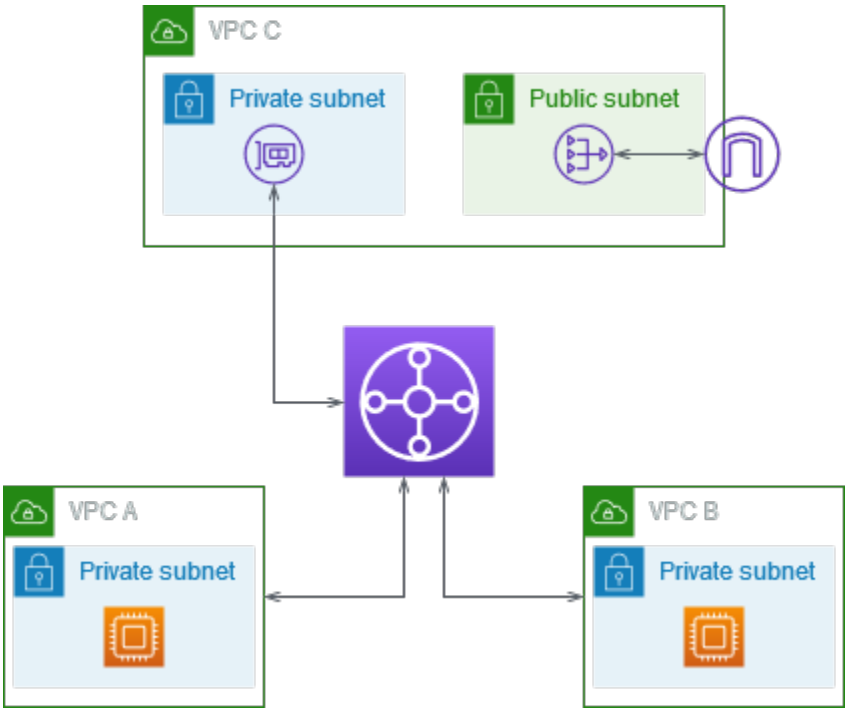
È possibile configurare un gateway di transito per indirizzare il traffico Internet in uscita da un gateway Internet VPC senza un gateway Internet a un gateway VPC che contiene un NAT gateway e un gateway Internet.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Esistono applicazioni in VPC A e VPC B che richiedono solo l'accesso a Internet in uscita. VPCC

viene configurato con un NAT gateway pubblico e un gateway Internet e una sottorete privata per l'VPCallegato. Connect tutto VPCs a un gateway di transito. Configura il routing in modo che il traffico Internet in uscita da VPC A e VPC B attraversi il gateway di transito verso VPC C. Il NAT gateway in VPC C indirizza il traffico verso il gateway Internet.



Risorse

Crea le seguenti risorse per questo scenario:

- Tre VPCs con intervalli di indirizzi IP che non si sovrappongono. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- VPCA e VPC B hanno entrambe sottoreti private con EC2 istanze.
- VPCC ha quanto segue:
  - Un gateway Internet collegato aVPC. Per ulteriori informazioni, consulta Creare e collegare un gateway Internet nella Amazon VPC User Guide.
  - Una sottorete pubblica con un NAT gateway. Per ulteriori informazioni, consulta Create a NAT gateway nella Amazon VPC User Guide.
  - Una sottorete privata per il collegamento del gateway di transito alla VPN. La sottorete privata deve trovarsi nella stessa zona di disponibilità della sottorete pubblica.
- Un gateway di transito Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.

- Tre VPC allegati sul gateway di transito. I CIDR blocchi per ciascuno di essi VPC si propagano nella tabella delle rotte del gateway di transito. Per ulteriori informazioni, consulta the section called "Crea un allegato VPC". Per VPC C, è necessario creare l'allegato utilizzando la sottorete privata. Se crei l'allegato utilizzando la sottorete pubblica, il traffico dell'istanza viene indirizzato al gateway Internet, ma il gateway Internet interrompe il traffico perché le istanze non dispongono di indirizzi IP pubblici. Inserendo l'allegato nella sottorete privata, il traffico viene indirizzato al gateway e il NAT gateway invia il traffico al NAT gateway Internet utilizzando il relativo indirizzo IP elastico come indirizzo IP di origine.

Routing

Sono disponibili tabelle di routing per ciascuno di essi VPC e una tabella di routing per il gateway di transito.

Tabelle di instradamento

- Tabella delle rotte per VPC A
- Tabella delle rotte per B VPC
- Tabelle di routing per C VPC
- Tabella di routing del gateway di transito

Tabella delle rotte per VPC A

Di seguito è riportato un esempio di tabella di instradamento. La prima immissione consente alle istanze in VPC di comunicare tra loro. La seconda entrata indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target
VPC A CIDR	locale
0.0.0.0/0	*transit-gateway-id*

Tabella delle rotte per B VPC

Di seguito è riportato un esempio di tabella di instradamento. La prima immissione consente alle istanze presenti in VPC di comunicare tra loro. La seconda entrata indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target
VPC B CIDR	locale
0.0.0.0/0	*transit-gateway-id*

Tabelle di routing per C VPC

Configura la sottorete con il NAT gateway come sottorete pubblica aggiungendo un percorso al gateway Internet. Lascia l'altra sottorete come sottorete privata.

Di seguito è riportata una tabella di instradamento di esempio per la sottorete pubblica. La prima voce consente alle istanze di VPC comunicare tra loro. La seconda e la terza entrata indirizzano il traffico per VPC A e VPC B verso il gateway di transito. Le entrate rimanenti indirizzano tutto il resto del traffico di IPv4 sottorete verso il gateway Internet.

Destinazione	Target
VPC C CIDR	locale
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

Di seguito è riportata una tabella di instradamento di esempio per la sottorete privata. La prima voce consente alle istanze in VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il NAT gateway.

Destinazione	Target
VPC C CIDR	locale
0.0.0.0/0	*nat-gateway-id*

Tabella di routing del gateway di transito

Di seguito è riportato un esempio della tabella di instradamento del gateway di transito. I CIDR blocchi di ciascuno di essi VPC si propagano alla tabella delle rotte del gateway di transito. La route statica invia il traffico internet in uscita a VPC C. È possibile opzionalmente impedire le VPC intercomunicazioni aggiungendo una route blackhole per ciascuna di esse. VPC CIDR

CIDR	Collegamento	Tipo di routing
VPC A CIDR	*Attachment for VPC A*	propagata
VPC B CIDR	*Attachment for VPC B*	propagata
VPC C CIDR	*Attachment for VPC C*	propagata
0.0.0.0/0	*Attachment for VPC C*	static

Esempio: dispositivo in un servizio condiviso VPC

È possibile configurare un dispositivo (ad esempio un dispositivo di sicurezza) in un servizio condiviso. VPC Tutto il traffico instradato tra gli allegati del gateway di transito viene prima ispezionato dall'appliance nei servizi condivisi. VPC Quando la modalità appliance è abilitata, un gateway di transito seleziona una singola interfaccia di rete nell'applianceVPC, utilizzando un algoritmo di flow hash, a cui inviare il traffico per tutta la durata del flusso. Il gateway di transito utilizza la stessa interfaccia di rete per il traffico di ritorno. Ciò garantisce che il traffico bidirezionale venga instradato in modo simmetrico: viene instradato attraverso la stessa zona di disponibilità nell'allegato per tutta la durata del flusso. VPC Se nell'architettura sono presenti più gateway

di transito, ogni gateway di transito mantiene la propria affinità di sessione e può selezionare un'interfaccia di rete diversa.

È necessario collegare esattamente un gateway di transito all'appliance per garantire la continuità del flusso. VPC Il collegamento di più gateway di transito a un singolo dispositivo VPC non garantisce la persistenza del flusso, in quanto i gateway di transito non condividono tra loro le informazioni sullo stato del flusso.

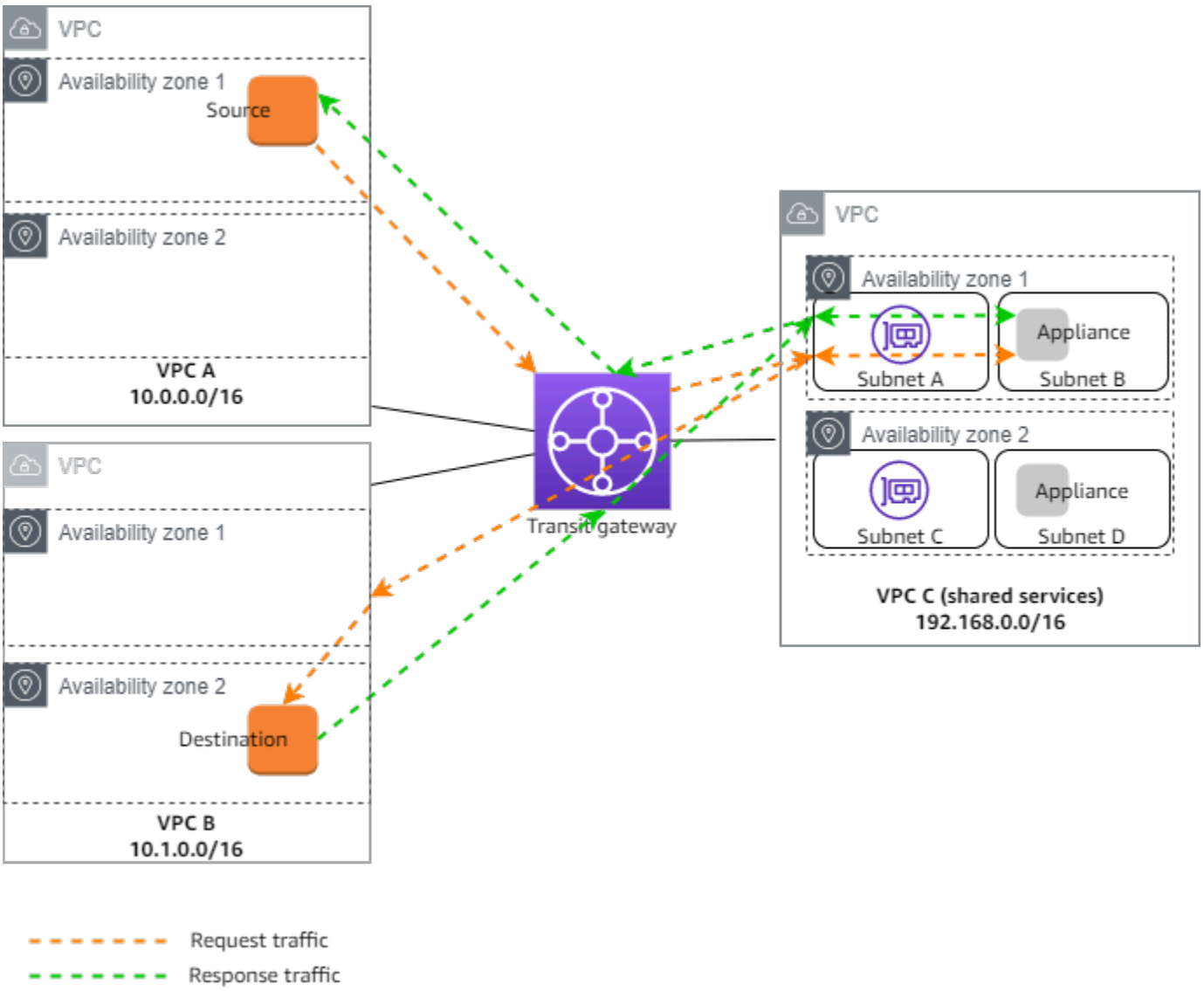
⚠ Important

- Il traffico in modalità appliance viene instradato correttamente a condizione che il traffico di origine e quello di destinazione arrivino a un sistema centralizzato VPC (ispezioneVPC) dallo stesso collegamento del gateway di transito. Il traffico può diminuire se l'origine e la destinazione si trovano su due diversi allegati del gateway di transito. Il traffico può diminuire se il sistema centralizzato VPC riceve il traffico da un gateway diverso, ad esempio un gateway Internet, e quindi lo invia all'allegato del gateway di transito dopo l'ispezione.
- L'attivazione della modalità appliance su un allegato esistente potrebbe influire sul percorso corrente dell'allegato, in quanto l'allegato può attraversare qualsiasi zona di disponibilità. Quando la modalità appliance non è abilitata, il traffico viene mantenuto nella zona di disponibilità di origine.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Il gateway di transito ha tre VPC allegati. VPC C è un servizio condivisoVPC. Il traffico tra VPC A e VPC B viene indirizzato al gateway di transito, quindi indirizzato a un dispositivo di sicurezza in VPC C per l'ispezione prima di essere indirizzato alla destinazione finale. L'appliance è un'appliance stateful, pertanto viene ispezionato sia il traffico di richiesta che di risposta. Per un'elevata disponibilità, è presente un'appliance in ogni zona di disponibilità in C. VPC



In questo scenario, si creano le seguenti risorse:

- TreVPCs. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre VPC allegati, uno per ciascuno deiVPCs. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.

  Per ogni VPC allegato, specificare una sottorete in ogni zona di disponibilità. Per i servizi condivisiVPC, queste sono le sottoreti a cui viene indirizzato il traffico proveniente VPC dal gateway di transito. Nell'esempio precedente, si tratta di sottoreti A e C.

Per l'VPCallegato per VPC C, abilita il supporto della modalità appliance in modo che il traffico di risposta venga indirizzato alla stessa zona di disponibilità in VPC C del traffico di origine.

La VPC console Amazon supporta la modalità appliance. Puoi anche utilizzare Amazon VPCAPI, un AWS SDK, AWS CLI per abilitare la modalità appliance o AWS CloudFormation. Ad esempio, aggiungi `--options ApplianceModeSupport=enable` al comando create-transit-gateway-vpc-attachment o modify-transit-gateway-vpc-attachment.

> **Note**
>
> La persistenza del flusso in modalità appliance è garantita solo per il traffico di origine e di destinazione che ha origine verso l'ispezione. VPC

Appliance con stato e modalità appliance

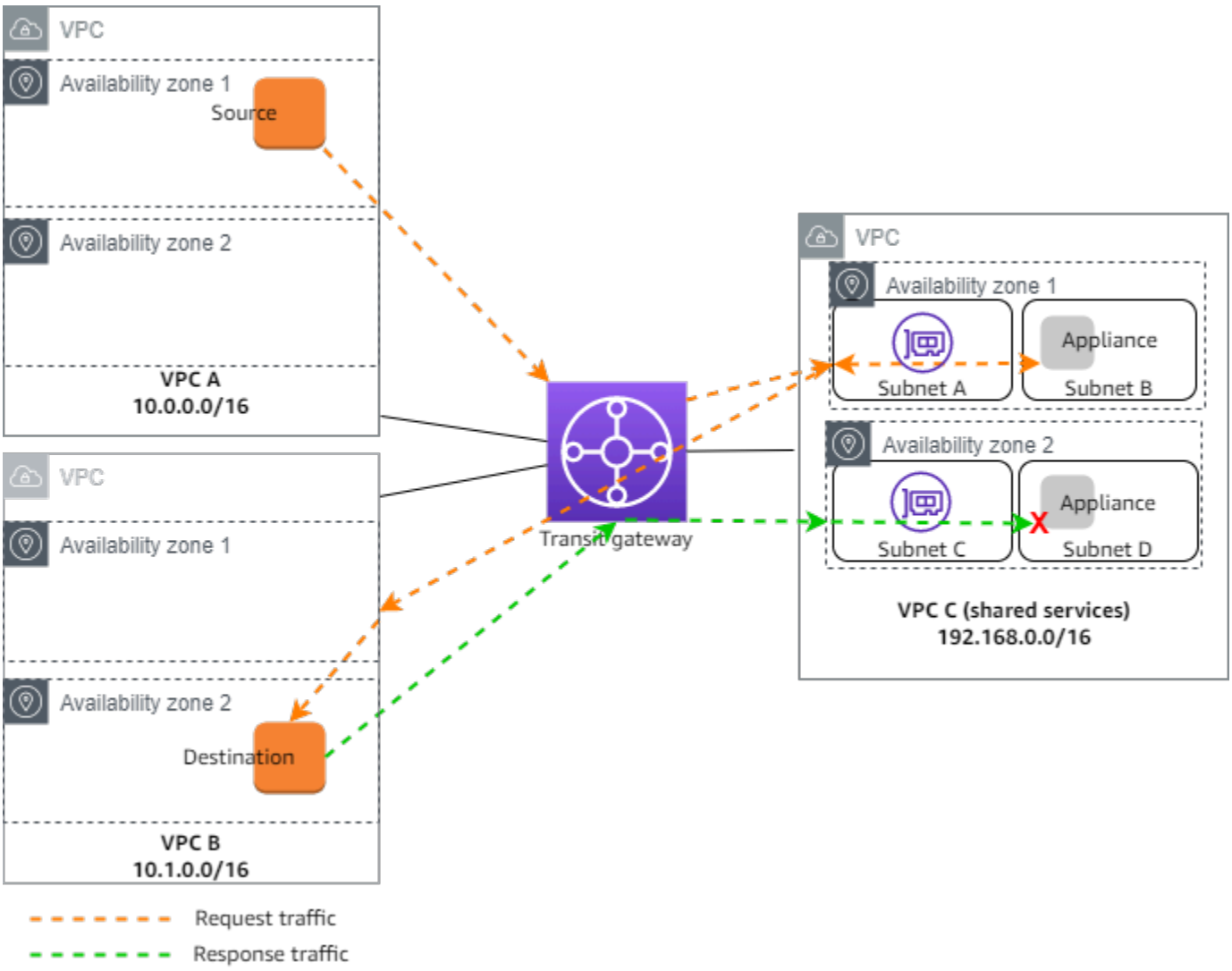
Se gli VPC allegati si estendono su più zone di disponibilità e si richiede che il traffico tra gli host di origine e di destinazione venga instradato attraverso lo stesso dispositivo per l'ispezione dello stato, abilita il supporto in modalità appliance per l'allegato in cui si trova l'appliance. VPC

Per ulteriori informazioni, consultate Centralized Inspection Architecture nel blog. AWS

Comportamento quando la modalità appliance non è abilitata

Quando la modalità appliance non è abilitata, un gateway di transito tenta di mantenere il traffico instradato tra VPC gli allegati nella zona di disponibilità di origine fino a raggiungere la destinazione. Il traffico attraversa le zone di disponibilità tra gli allegati solo se si verifica un errore nella zona di disponibilità o se non ci sono sottoreti associate a un allegato in quella zona di disponibilità. VPC

Il diagramma seguente mostra un flusso di traffico quando il supporto della modalità appliance non è abilitato. Il traffico di risposta proveniente dalla zona di disponibilità 2 in VPC B viene instradato dal gateway di transito verso la stessa zona di disponibilità in VPC C. Il traffico viene quindi interrotto, poiché l'appliance nella zona di disponibilità 2 non è a conoscenza della richiesta originale proveniente dalla fonte in A. VPC



Routing

Ciascuna VPC ha una o più tabelle di routing e il gateway di transito ha due tabelle di routing.

VPCtabelle di routing

VPCA e VPC B

VPCsA e B hanno tabelle di percorso con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale in. VPC Questa voce predefinita consente alle risorse in essa contenute VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. Di seguito è riportata la tabella dei percorsi per A. VPC

Destinazione	Target

Destinazione	Target
10.0.0.0/16	locale
0.0.0.0/0	tgw-id

VPCC

I servizi condivisi VPC (VPCC) hanno tabelle di routing diverse per ogni sottorete. La subnet A viene utilizzata dal gateway di transito (questa sottorete viene specificata quando si crea l'VPCallegato). La tabella di route per la sottorete A indirizza tutto il traffico all'accessorio nella sottorete B.

Destinazione	Target
192.168.0.0/16	locale
0.0.0.0/0	appliance-eni-id

La tabella dei percorsi per la sottorete B (che contiene l'accessorio) indirizza il traffico al gateway di transito.

Destinazione	Target
192.168.0.0/16	locale
0.0.0.0/0	tgw-id

Tabelle di routing del gateway di transito

Questo gateway di transito utilizza una tabella di routing per VPC A e VPC B e una tabella di routing per i servizi condivisi VPC (VPCC).

Gli allegati VPC A e VPC B sono associati alla seguente tabella di routing. La tabella dei percorsi indirizza tutto il traffico verso C. VPC

Destinazione	Target	Tipo di route
0.0.0.0/0	*Attachment ID for VPC C*	static

L'allegato VPC C è associato alla seguente tabella di percorsi. Indirizza il traffico verso VPC A e VPC B.

Destinazione	Target	Tipo di route
10.0.0.0/16	*Attachment ID for VPC A*	propagata
10.1.0.0/16	*Attachment ID for VPC B*	propagata

Inizia a usare Amazon VPC Transit Gateways

Le seguenti attività ti aiutano a familiarizzare con i gateway di transito in Amazon VPC Transit Gateways. Questa attività ti guida nella creazione di un gateway di transito e nel successivo collegamento di due dei tuoi VPCs tramite quel gateway di transito.

Attività

- Prerequisiti
- Fase 1: creazione del gateway di transito
- Passaggio 2: collega il tuo VPCs al gateway di transito
- Fase 3: Aggiungi percorsi tra il gateway di transito e il VPCs
- Fase 4: testa il gateway di transito
- Fase 5: eliminare il gateway di transito

Prerequisiti

- Per illustrare un semplice esempio di utilizzo di un gateway di transito, VPCs creane due nella stessa regione. VPCsNon possono avere sovrapposizioniCIDRs. Avvia un'EC2istanza Amazon in ciascunaVPC. Per ulteriori informazioni, consulta Create a VPC in Amazon VPC User Guide e Launch an istance nella Amazon EC2 User Guide.
- Non puoi avere percorsi identici che puntano a due percorsi diversiVPCs. Un gateway di transito non propaga quello CIDRs di un nuovo collegamento VPC se esiste un percorso identico nelle tabelle di routing del gateway di transito.
- Verificare di disporre delle autorizzazioni necessarie per l'utilizzo di gateway di transito. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in Amazon VPC Transit Gateway .
- Non puoi eseguire il ping tra host se non hai aggiunto una ICMP regola a ciascuno dei gruppi di sicurezza dell'host. Per ulteriori informazioni, consulta Configurare le regole dei gruppi di sicurezza nella Amazon VPC User Guide.

Fase 1: creazione del gateway di transito

Quando crei un gateway di transito, viene creata una tabella di routing predefinita per il gateway di transito e questa viene utilizzata come tabella di routing predefinita per le associazioni nonché come tabella di routing predefinita per la propagazione.

Creazione di un gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel selettore della regione, scegli la regione che hai usato quando hai creato ilVPCs.
3. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
4. Selezionare Create Transit Gateway (Crea gateway di transito).
5. (Facoltativo) Per Name tag (Tag nome), immettere un nome per il gateway di transito. Tale azione crea un tag con chiave "Name" e il nome specificato come valore.
6. (Facoltativo) In Description (Descrizione) inserire una descrizione per il gateway di transito.
7. Nella sezione Configura il gateway di transito, procedi come segue:

   1. Per il numero di sistema autonomo (ASN) lato Amazon, inserisci il numero privato ASN per il tuo gateway di transito. Questo dovrebbe essere il ASN AWS lato di una sessione di Border Gateway Protocol (BGP).

      L'intervallo va da 64512 a 65534 per 16 bit. ASNs

      L'intervallo va da 4200000000 a 4294967294 per 32 bit. ASNs

      Se disponi di una distribuzione multiregionale, ti consigliamo di utilizzarne una univoca ASN per ciascuno dei tuoi gateway di transito.
   2. (Facoltativo) Scegli se abilitare una delle seguenti opzioni:
      - DNSsupporto per il VPCs collegamento a questo gateway di transito.
      - VPNECMPsupporto per VPN le connessioni collegate al gateway di transito.
      - Associazione della tabella di routing predefinita, che associa automaticamente gli allegati del gateway di transito alla tabella di routing predefinita di questo gateway di transito.
      - Propagazione della tabella di routing predefinita, che propaga automaticamente gli allegati della tabella di routing alla tabella di routing predefinita di questo gateway di transito.
      - Supporto multicast, che consente di creare domini multicast in questo gateway di transito.

8. (Facoltativo) Nella sezione delle opzioni di Configure-cross-account condivisione, scegli se accettare automaticamente gli allegati condivisi. Se abilitato, gli allegati vengono accettati automaticamente. Altrimenti, è necessario accettare o rifiutare le richieste di allegati.
9. (Facoltativo) Nella sezione Transit gateway CIDR blocks, aggiungete un CIDR blocco di dimensione pari o superiore a /24 per IPv4 gli indirizzi o un blocco /64 o più grande CIDR per gli indirizzi. IPv6 È possibile associare qualsiasi intervallo di indirizzi IP pubblico o privato, ad eccezione degli indirizzi nell'intervallo 169.254.0.0/16 e degli intervalli che si sovrappongono agli indirizzi degli allegati e delle reti locali. VPC

   > **Note**
   >
   > I CIDR blocchi Transit Gateway vengono utilizzati se si configurano gli allegati Connect (GRE) o PrivateIP. VPNs Transit Gateway assegna IPs gli endpoint del tunnel (GRE/ privateIPVPN) da questo intervallo.

10. (Facoltativo) Aggiungi tag chiave-valore a questo gateway di transito per facilitarne ulteriormente l'identificazione.
    1. Scegli Aggiungi nuova scheda.
    2. Inserisci il nome della chiave e il valore associato.
    3. Scegli Aggiungi nuovo tag per aggiungere altri tag o vai al passaggio successivo.
11. Selezionare Create Transit Gateway (Crea gateway di transito). Quando il gateway viene creato, lo stato iniziale del gateway di transito è `pending`.

Passaggio 2: collega il tuo VPCs al gateway di transito

Prima di procedere con la creazione di un collegamento, attendere fino a quando il gateway di transito creato nella sezione precedente è indicato come disponibile. Crea un allegato per ciascunoVPC.

Conferma di averne creati due VPCs e avviato un'EC2istanza in ciascuno, come descritto inPrerequisiti.

Crea un gateway di transito allegato a un VPC

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).
4. (Facoltativo) In Name tag (Tag nome), inserire il nome del collegamento.
5. In Transit gateway ID (ID gateway di transito), selezionare il gateway di transito da usare per il collegamento.
6. Per Tipo di allegato, scegli VPC.
7. Scegli se abilitare DNSil supporto. Per questo esercizio, non abilitate IPv6il supporto.
8. Per VPCID, scegli VPC da collegare al gateway di transito.
9. Per Subnet IDs, selezionate una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
10. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Ogni collegamento è sempre associato a una sola tabella di instradamento. Le tabelle di routing possono essere associate a nessuno o a molti collegamenti. Per determinare le route da configurare, decidere il caso d'uso per il gateway di transito, quindi configurare le route. Per ulteriori informazioni, consulta the section called “Esempi di scenari di gateway di transito”.

Fase 3: Aggiungi percorsi tra il gateway di transito e il VPCs

Una tabella di routing include route dinamiche e statiche che determinano l'hop successivo da associare in VPCs base all'indirizzo IP di destinazione del pacchetto. Configura un instradamento con una destinazione per gli instradamenti non locali e la destinazione dell'ID allegato del gateway di transito. Per ulteriori informazioni, consulta Routing for a transit gateway nella Amazon VPC User Guide.

Per aggiungere un percorso a una tabella di VPC rotte

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Route Tables (Tabelle di routing).
3. Scegli la tabella dei percorsi associata alla tuaVPC.
4. selezionare la scheda Routes (Route), selezionare Edit routes (Modifica route).
5. Selezionare Add route (Aggiungi route).

6. Nella colonna Destination (Destinazione), immettere l'intervallo di indirizzi IP di destinazione. Per Target, scegliere Gateway di transito e quindi scegliere l'ID del gateway di transito.
7. Scegli Save changes (Salva modifiche).

Fase 4: testa il gateway di transito

Puoi confermare che il gateway di transito è stato creato correttamente connettendoti a un'EC2istanza Amazon in ciascuna VPC istanza e quindi inviando dati tra di esse, ad esempio un comando ping. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.

Fase 5: eliminare il gateway di transito

Quando non è più necessario un gateway di transito, è possibile eliminarlo.

Non è possibile eliminare un gateway di transito con allegati di risorse. Se provi a eliminare un gateway di transito che ha degli allegati, ti verrà richiesto di eliminare prima gli allegati. Non appena il gateway di transito viene eliminato, smetti di incorrere in addebiti per esso.

Per eliminare il gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Seleziona il gateway di transito, quindi scegli Actions (Operazioni), Delete transit gateway (Elimina gateway di transito).
4. Immettere **`delete`** e scegliere Delete (Elimina).

   Lo stato del gateway di transito sulla pagina Transit gateways (Gateway di transito) è Deleting (Eliminazione in corso). Una volta eliminato, il gateway di transito viene rimosso dalla pagina.

Le best practice di progettazione di Amazon VPC Transit Gateways

Di seguito sono riportate le best practice per la progettazione del gateway di transito:

- Utilizza una sottorete separata per ogni VPC allegato del gateway di transito. Per ogni sottorete, ad esempioCIDR, utilizzane una piccola/28, in modo da avere più indirizzi per le EC2 risorse. Quando usi una sottorete separata, puoi configurare quanto segue:
  - Mantieni aperta la rete in entrata e in uscita ACLs associata alle sottoreti del gateway di transito.
  - A seconda del flusso di traffico, puoi applicare la rete alle sottoreti del carico ACLs di lavoro.
- Crea una rete ACL e associala a tutte le sottoreti associate al gateway di transito. Mantieni la rete ACL aperta sia in entrata che in uscita.
- Associate la stessa tabella di VPC routing a tutte le sottoreti associate al gateway di transito, a meno che la progettazione della rete non richieda più tabelle di VPC routing (ad esempio, una casella centrale VPC che indirizza il traffico attraverso più gateway). NAT
- Utilizzate le connessioni Border Gateway Protocol (). BGP Site-to-Site VPN Se il dispositivo gateway del cliente o il firewall per la connessione supporta la funzione percorso multiplo, abilita la caratteristica.
- Abilita la propagazione delle rotte per gli allegati e BGP Site-to-Site VPN gli allegati del AWS Direct Connect gateway.
- Durante la migrazione dal VPC peering all'utilizzo di un gateway di transito. Una mancata corrispondenza MTU delle dimensioni tra il VPC peering e il gateway di transito potrebbe causare la perdita di alcuni pacchetti a causa del traffico asimmetrico. Aggiorna entrambi VPCs contemporaneamente per evitare che i pacchetti jumbo cadano a causa di disallineamenti tra le dimensioni.
- Non sono necessari gateway di transito aggiuntivi per un'elevata disponibilità, perché i gateway di transito sono altamente disponibili in base alla progettazione.
- Limitare il numero di tabelle di route gateway di transito a meno che la progettazione non richieda più tabelle di route gateway di transito.
- Per la ridondanza, utilizza un unico gateway di transito in ogni regione per il ripristino di emergenza.
- Per le implementazioni con più gateway di transito, si consiglia di utilizzare un numero di sistema autonomo (ASN) univoco per ciascuno dei gateway di transito. È anche possibile usare il peering

tra regioni. Per ulteriori informazioni, consulta Creazione di una rete globale utilizzando il peering interregionale. AWS Transit Gateway

Lavora con i gateway di transito utilizzando Amazon VPC Transit Gateways

Puoi lavorare con i gateway di transito utilizzando la VPC console Amazon o il AWS CLI.

Argomenti

Gateway di transito condivisi

È possibile utilizzare AWS Resource Access Manager (RAM) per condividere un gateway di transito per VPC gli allegati tra account o in tutta l'organizzazione in AWS Organizations. RAMdeve essere abilitato e le risorse devono essere condivise con un'organizzazione. Per ulteriori informazioni, consulta Abilitare la condivisione delle risorse con AWS Organizations nella Guida per l'utente di AWS RAM .

Considerazioni

Se desideri condividere un gateway di transito, tieni presente quanto segue.

- È necessario creare un AWS Site-to-Site VPN allegato nello stesso AWS account proprietario del gateway di transito.

- Un collegamento a un gateway Direct Connect utilizza un'associazione di gateway di transito e può trovarsi nello stesso AWS account del gateway Direct Connect o in uno diverso dal gateway Direct Connect.

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per creare o modificare AWS RAM risorse. Per consentire agli utenti di creare o modificare risorse ed eseguire attività, è necessario creare IAM politiche che consentano l'utilizzo di risorse e API azioni specifiche. È quindi possibile allegare tali politiche agli IAM utenti o ai gruppi che richiedono tali autorizzazioni.

Solo il proprietario della risorsa è in grado di eseguire le operazioni descritte di seguito:

- Creare una condivisione di risorse.
- Aggiornare una condivisione di risorse.
- Visualizzare una condivisione di risorse.
- Visualizzare le risorse condivise dall'account in tutte le condivisioni di risorse.
- Visualizzare i principali con cui condividi le risorse in tutte le condivisioni di risorse. Visualizzare i principali con si effettua la condivisione consente di determinare gli utenti che hanno accesso alle risorse condivise.
- Eliminare una condivisione di risorse.
- Esegui tutte le tabelle APIs di routing dei gateway di transito, degli allegati dei gateway di transito e dei gateway di transito.

Puoi eseguire le operazioni illustrate di seguito sulle risorse condivise con te:

- Accettare o respingere un invito alla condivisione di risorse.
- Visualizzare una condivisione di risorse.
- Visualizzare le risorse condivise a cui accedere.
- Visualizzare un elenco di tutti i principali che condividono risorse con l'utente. Puoi vedere le risorse e le condivisioni di risorse con te condivise.
- Può eseguire il `DescribeTransitGateways`API.
- Esegui quelli APIs che creano e descrivono gli allegati, ad esempio `CreateTransitGatewayVpcAttachment` e`DescribeTransitGatewayVpcAttachments`, in loroVPCs.
- Lasciare una condivisione di risorse.

Quando un gateway di transito viene condiviso con te, non potrai creare, modificare o eliminare le tabelle di instradamento del gateway di transito o le propagazioni e le associazioni di queste tabelle.

Quando si crea un gateway di transito, il gateway di transito viene creato nella zona di disponibilità mappata all'account ed è indipendente da altri account. Quando il gateway di transito e le entità dell'allegato si trovano in account diversi, utilizzare gli ID della zona di disponibilità per identificare in modo univoco e coerente la zona di disponibilità. Ad esempio, use1-az1 è un ID AZ per la regione us-east-1 ed è mappato alla stessa posizione in ogni account. AWS

Eliminare la condivisione di un gateway di transito

Quando il proprietario della condivisione annula la condivisione del gateway di transito, si applicano le seguenti regole:

- L'allegato del gateway di transito rimane funzionante.
- L'account condiviso non può descrivere il gateway di transito.
- Il proprietario del gateway di transito e il proprietario della condivisione possono eliminare l'allegato del gateway di transito.

Quando un gateway di transito non viene condiviso con un altro AWS account o se l' AWS account con cui è condiviso il gateway di transito viene rimosso dall'organizzazione, il gateway di transito stesso non ne risentirà.

Sottoreti condivise

Un VPC proprietario può collegare un gateway di transito a una sottorete VPC condivisa. I partecipanti non possono. Il traffico proveniente dalle risorse del partecipante può utilizzare gli allegati a seconda dei percorsi impostati nella VPC sottorete condivisa dal proprietario. VPC

Per ulteriori informazioni, consulta Condividi il tuo account VPC con altri account nella Amazon VPC User Guide.

Gateway di transito in Amazon VPC Transit Gateways

Un gateway di transito consente di collegare VPCs e instradare il traffico tra di esse e le VPN connessioni. Un gateway di transito funziona trasversalmente Account AWS e puoi AWS RAM utilizzarlo per condividere il gateway di transito con altri account. Dopo aver condiviso un gateway

di transito con un altro Account AWS, il proprietario dell'account può collegarlo VPCs al gateway di transito. Un utente di uno qualsiasi degli account può eliminare il collegamento in qualsiasi momento.

È possibile abilitare il multicast su un gateway di transito e quindi creare un dominio multicast del gateway di transito che consenta l'invio del traffico multicast dalla sorgente multicast ai membri del gruppo multicast tramite VPC allegati associati al dominio.

Ogni VPN allegato è associato a VPC una singola tabella di routing. La tabella di instradamento definisce il successivo segmento di rete su cui inoltrare il traffico proveniente dallo specifico collegamento della risorsa. Una tabella di routing all'interno del gateway di transito consente sia l'utilizzo di IPv4 OR che IPv6 CIDRs le destinazioni. Gli obiettivi sono VPCs e VPN le connessioni. Quando si collega VPC o si crea una VPN connessione su un gateway di transito, l'allegato viene associato alla tabella di routing predefinita del gateway di transito.

È possibile creare tabelle di routing aggiuntive all'interno del gateway di transito e modificare l'VPNassociazione VPC o l'associazione a tali tabelle di routing. Tale azione consente la segmentazione della rete. Ad esempio, è possibile VPCs associare lo sviluppo a una tabella di routing e la produzione VPCs a una tabella di routing diversa. Ciò consente di creare reti isolate all'interno di un gateway di transito in modo simile al routing e all'inoltro virtuali (VRFs) nelle reti tradizionali.

I gateway di transito supportano il routing dinamico e statico tra collegamenti collegati e connessioni. VPCs VPN Per ogni collegamento puoi abilitare o disabilitare la propagazione delle route. Gli allegati di peering del gateway di transito supportano solo il routing statico. È possibile indirizzare i percorsi nelle tabelle di routing dei gateway di transito all'allegato di peering per instradare il traffico tra i gateway di transito peer.

Facoltativamente, puoi associare uno IPv4 o più IPv6 CIDR blocchi al tuo gateway di transito. Si specifica un indirizzo IP dal CIDR blocco quando si stabilisce un peer Transit Gateway Connect per un allegato Transit Gateway Connect. È possibile associare qualsiasi intervallo di indirizzi IP pubblico o privato, ad eccezione degli indirizzi compresi nell'`169.254.0.0/16`intervallo, e gli intervalli che si sovrappongono agli indirizzi degli VPC allegati e delle reti locali. Per ulteriori informazioni su IPv4 e IPv6 CIDR blocchi, consulta l'indirizzo IP nella Amazon VPC User Guide.

Attività

- Crea un gateway di transito utilizzando Amazon VPC Transit Gateways
- Visualizza le informazioni sui gateway di transito utilizzando Amazon VPC Transit Gateways
- Aggiungi o modifica tag per un gateway di transito utilizzando Amazon VPC Transit Gateways

- Modifica un gateway di transito utilizzando Amazon VPC Transit Gateways
- Accetta una condivisione di risorse utilizzando Amazon VPC Transit Gateways
- Accetta un allegato condiviso utilizzando Amazon VPC Transit Gateways
- Eliminare un gateway di transito utilizzando Amazon VPC Transit Gateways

Crea un gateway di transito utilizzando Amazon VPC Transit Gateways

Quando crei un gateway di transito, viene creata una tabella di routing predefinita per il gateway di transito e questa viene utilizzata come tabella di routing predefinita per le associazioni nonché come tabella di routing predefinita per la propagazione. Se scegli di non creare la tabella di routing del gateway di transito predefinita, è possibile crearne una in un secondo momento. Per ulteriori informazioni sui routing e sulle tabelle di routing, consulta ???.

Per creare un gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Selezionare Create Transit Gateway (Crea gateway di transito).
4. Per Tag nome, è possibile inserire un nome per il gateway di transito. Un tag nome può semplificare l'identificazione di uno specifico gateway nell'elenco dei gateway. Quando aggiungi un Name tag (Tag nome), viene creato un tag con chiave Name e il valore corrispondente a quello inserito.
5. In Description (Descrizione), immettere una descrizione facoltativa per il gateway di transito.
6. Per il lato Amazon Autonomous System Number (ASN), lascia il valore predefinito per utilizzare quello predefinito ASN o inserisci quello privato ASN per il tuo gateway di transito. Questo dovrebbe essere il ASN AWS lato di una sessione di Border Gateway Protocol (BGP).

   L'intervallo è compreso tra 64512 e 65534 per 16 bit. ASNs

   L'intervallo è compreso tra 4200000000 e 4294967294 per 32 bit. ASNs

   Se disponi di un'implementazione multiregionale, ti consigliamo di utilizzarne una univoca ASN per ciascuno dei tuoi gateway di transito.
7. Per ricevere DNSassistenza, seleziona questa opzione se hai bisogno di VPC convertire i nomi di IPv4 DNS host pubblici in IPv4 indirizzi privati quando le richieste vengono eseguite da istanze di un'altra istanza VPC collegata al gateway di transito.

8. Per il supporto Security Group Referencing, abilita questa funzionalità per fare riferimento a un gruppo di sicurezza VPCs collegato a un gateway di transito. Per ulteriori informazioni sui riferimenti ai gruppi di sicurezza, vedere. the section called “Riferimenti dei gruppi di sicurezza”
9. Per VPNECMPassistenza, selezionate questa opzione se avete bisogno del supporto di routing Equal Cost Multipath (ECMP) tra i tunnel. VPN Se le connessioni pubblicizzano lo stesso messaggioCIDRs, il traffico viene distribuito equamente tra di loro.

   Quando si seleziona questa opzione, gli attributi pubblicizzati BGP ASN e quindi gli BGP attributi come AS-Path devono essere gli stessi.

   > **Note**
   >
   > Per utilizzarloECMP, è necessario creare una VPN connessione che utilizzi il routing dinamico. VPNle connessioni che utilizzano il routing statico non sono supportate. ECMP

10. In Default route table association (Associazione tabella di routing predefinita), selezionare abilita per associare automaticamente gli allegati del gateway di transito alla tabella di routing predefinita per il gateway di transito.
11. In Default route table propagation (Propagazione tabella di routing predefinita), selezionare abilita per propagare automaticamente gli allegati del gateway di transito alla tabella di routing predefinita per il gateway di transito.
12. (Facoltativo) Per utilizzare il gateway di transito come router per il traffico multicast, selezionare Multicast support (Supporto multicast).
13. (Facoltativo) Nella sezione delle opzioni di Configure-cross-account condivisione, scegli se accettare automaticamente gli allegati condivisi. Se abilitato, gli allegati vengono accettati automaticamente. Altrimenti, è necessario accettare o rifiutare le richieste di allegati.

    In Auto accept shared attachments (Accetta automaticamente i collegamenti condivisi), selezionare abilita per accettare automaticamente i collegamenti multi-account.
14. (Facoltativo) Per i CIDRblocchi Transit gateway, specificate uno IPv4 o più IPv6 CIDR blocchi per il gateway di transito.

    È possibile specificare un CIDR blocco di dimensione /24 o superiore (ad esempio, /23 o /22) perIPv4, oppure un CIDR blocco di dimensione /64 o superiore (ad esempio, /63 o /62) per. IPv6 È possibile associare qualsiasi intervallo di indirizzi IP pubblico o privato, ad eccezione degli indirizzi nell'intervallo 169.254.0.0/16 e degli intervalli che si sovrappongono agli indirizzi degli allegati e delle reti locali. VPC

> **Note**
>
> I CIDR blocchi Transit Gateway vengono utilizzati se si configurano gli allegati Connect (GRE) o PrivateIP. VPNs Transit Gateway assegna IPs gli endpoint del tunnel (GRE/privateIPVPN) da questo intervallo.

15. Selezionare Create Transit Gateway (Crea gateway di transito).

Per creare un gateway di transito utilizzando il AWS CLI

Utilizza il comando create-transit-gateway.

Visualizza le informazioni sui gateway di transito utilizzando Amazon VPC Transit Gateways

Visualizza tutti i tuoi gateway di transito.

Per visualizzare un gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Transit Gateways. I dettagli del gateway di transito sono visualizzati sotto l'elenco dei gateway sulla pagina.

Per visualizzare un gateway di transito utilizzando il AWS CLI

Utilizza il comando describe-transit-gateways.

Aggiungi o modifica tag per un gateway di transito utilizzando Amazon VPC Transit Gateways

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. È possibile aggiungere più tag a ogni gateway di transito. Le chiavi di tag devono essere univoche per ogni gateway di transito. Se aggiungi un tag con una chiave già associata al gateway di transito, il valore del tag viene aggiornato. Per ulteriori informazioni, consulta Tagging your Amazon EC2 Resources.

Aggiungere tag a un gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Scegli il gateway di transito per il quale desideri aggiungere o modificare i tag.
4. Selezionare la scheda Tags (Tag) nella parte inferiore della pagina.
5. Scegliere Gestisci tag.
6. Scegliere Aggiungi nuovo tag.
7. Digitare una Key (Chiave) e un Value (Valore) per il tag.
8. Seleziona Salva.

Modifica un gateway di transito utilizzando Amazon VPC Transit Gateways

È possibile modificare le opzioni di configurazione per il gateway di transito. Quando si modifica un gateway di transito, le opzioni modificate vengono applicate solo ai nuovi allegati del gateway di transito. I collegamenti del gateway di transito alla VPN esistenti non vengono modificati e non rilevano alcuna interruzione del servizio.

Non è possibile modificare un gateway di transito condiviso con l'utente.

Non è possibile rimuovere un CIDR blocco per il gateway di transito se uno qualsiasi degli indirizzi IP è attualmente utilizzato per un peer Connect.

Modificare un gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Scegliere il gateway di transito da modificare.
4. Scegliere Azioni, Modifica gateway di transito.
5. Modificare le opzioni in base alle esigenze e scegliere Modifica gateway di transito.

Per modificare il gateway di transito utilizzando il AWS CLI

Utilizza il comando modify-transit-gateway.

Accetta una condivisione di risorse utilizzando Amazon VPC Transit Gateways

Se sei stato aggiunto a una condivisione di risorse, riceverai un invito a partecipare alla condivisione stessa. Prima di poter accedere alle risorse condivise dovrai accettare la condivisione di risorse.

Per accettare una condivisione di risorse

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione, selezionare Shared with me (Condivise con me), Resource shares (Condivisioni di risorse).
3. Selezionare la condivisione di risorse.
4. Selezionare Accept resource share (Accetta condivisione di risorse).
5. Per visualizzare il gateway di transito condiviso, apri la pagina Transit Gateways nella VPC console Amazon.

Accetta un allegato condiviso utilizzando Amazon VPC Transit Gateways

Se non hai abilitato la funzionalità di accettazione automatica degli allegati condivisi quando hai creato il gateway di transito, devi accettare manualmente gli allegati multiaccount (condivisi) utilizzando la VPC console Amazon o il. AWS CLI

Per accettare manualmente un allegato condiviso

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Accept transit gateway attachment (Accetta il collegamento del gateway di transito alla VPN).

Per accettare un allegato condiviso utilizzando il AWS CLI

Utilizzare il comando accept-transit-gateway-vpc-attachment.

Eliminare un gateway di transito utilizzando Amazon VPC Transit Gateways

Non è possibile eliminare un gateway di transito con allegati esistenti. Prima di poter eliminare un gateway di transito è necessario eliminare tutti i collegamenti.

Per eliminare un gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegliere il gateway di transito da eliminare.
3. Scegliere Azioni, Eliminare il gateway di transito. Immettere **`delete`** e quindi scegliere Delete (Elimina) per confermare l'eliminazione.

Per eliminare un gateway di transito utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway.

Allegati Amazon VPC nei gateway di transito Amazon VPC

Un allegato Amazon Virtual Private Cloud (VPC) a un gateway di transito consente di indirizzare il traffico da e verso una o più sottoreti VPC. Quando si collega un VPC a un gateway di transito, è necessario specificare una sottorete di ciascuna zona di disponibilità che deve essere utilizzata dal gateway di transito per instradare il traffico. L'indicazione di una sottorete da una zona di disponibilità permette al traffico di raggiungere le risorse in tutte le sottoreti di tale zona di disponibilità.

Limiti

- Quando si associa un VPC a un gateway di transito, le eventuali risorse nelle zone di disponibilità in cui non vi sia un collegamento con il gateway di transito non possono raggiungere il gateway di transito. Se è presente un percorso al gateway di transito in una tabella di routing di sottorete, il traffico viene inoltrato al gateway di transito solo quando il gateway di transito dispone di un collegamento in una sottorete nella stessa zona di disponibilità.
- Un gateway di transito non supporta la risoluzione DNS per i nomi DNS personalizzati della VPCs configurazione collegata utilizzando zone ospitate private in Amazon Route 53. Per configurare la risoluzione dei nomi per le zone ospitate private per tutte le aree VPCs collegate a un gateway di transito, consulta Gestione DNS centralizzata del cloud ibrido con Amazon Route 53 e AWS Transit Gateway.
- Un gateway di transito non supporta il routing tra due VPCs unità identiche. CIDRs Se si collega un VPC a un gateway di transito e il relativo CIDR è identico al CIDR di un altro VPC già collegato al

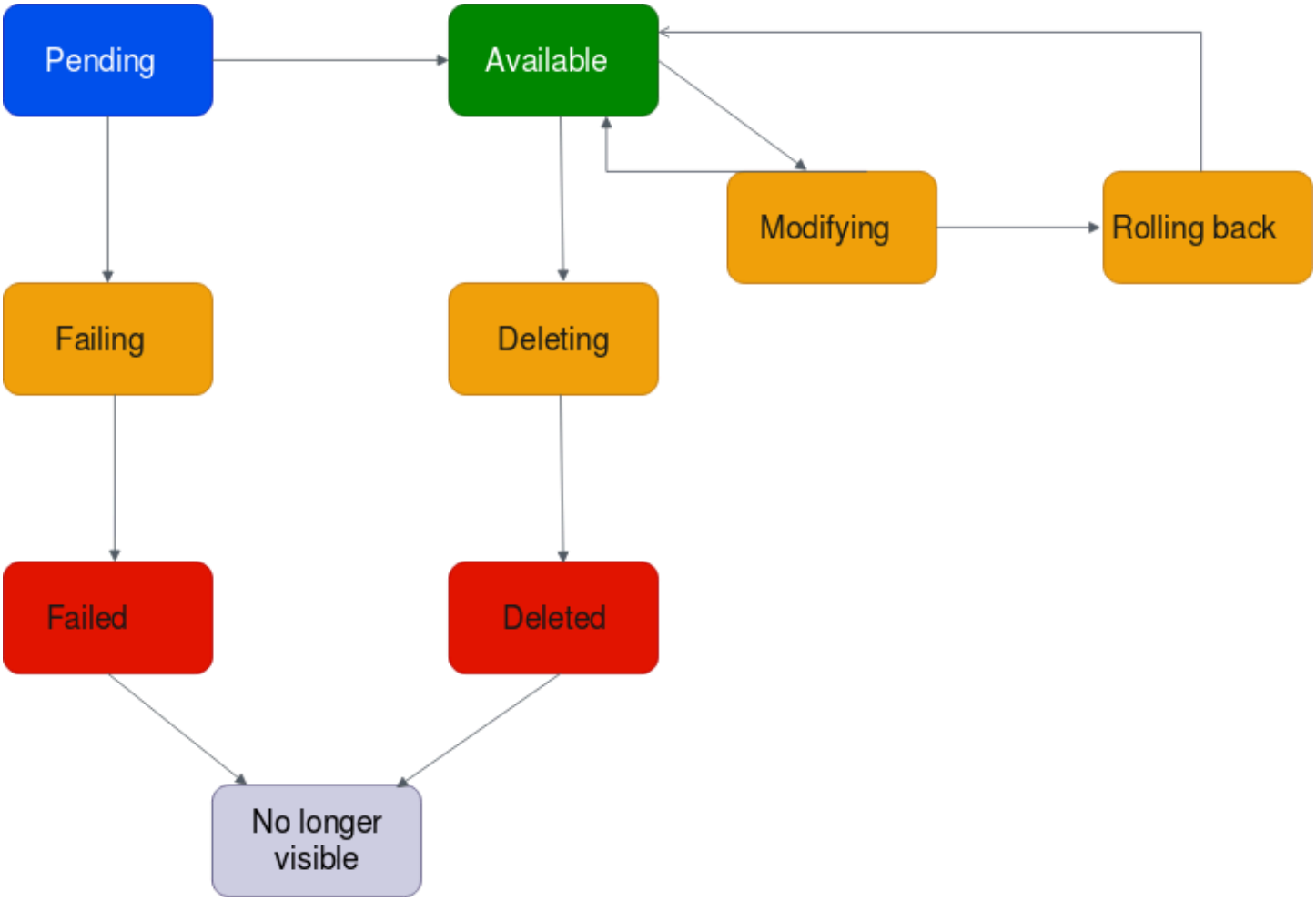
gateway di transito, le routing per il VPC appena collegato non vengono propagate nella tabella di routing del gateway di transito.

- Non è possibile creare un allegato per una sottorete VPC che risiede in una zona locale. Tuttavia, puoi configurare la rete in modo che le sottoreti nella zona locale possano connettersi a un gateway di transito attraverso la zona di disponibilità padre. Per ulteriori informazioni, vedi Connessione delle sottoreti delle zone locali a un gateway di transito.
- Non è possibile creare un allegato al gateway di transito utilizzando le sottoreti IPv6 -only. Le sottoreti allegate del gateway Transit devono supportare anche gli indirizzi. IPv4
- Un gateway di transito deve avere almeno un allegato VPC prima di poter essere aggiunto a una tabella di routing.

Ciclo di vita del collegamento VPC

Un collegamento VPC passa attraverso varie fasi, a partire dal momento in cui viene avviata la richiesta. È possibile che in ogni fase sia necessario eseguire alcune operazioni e che, alla fine del relativo ciclo di vita, il collegamento VPC rimanga visibile nella Amazon Virtual Private Cloud Console e nell'API o nell'output della riga di comando per un determinato periodo di tempo.

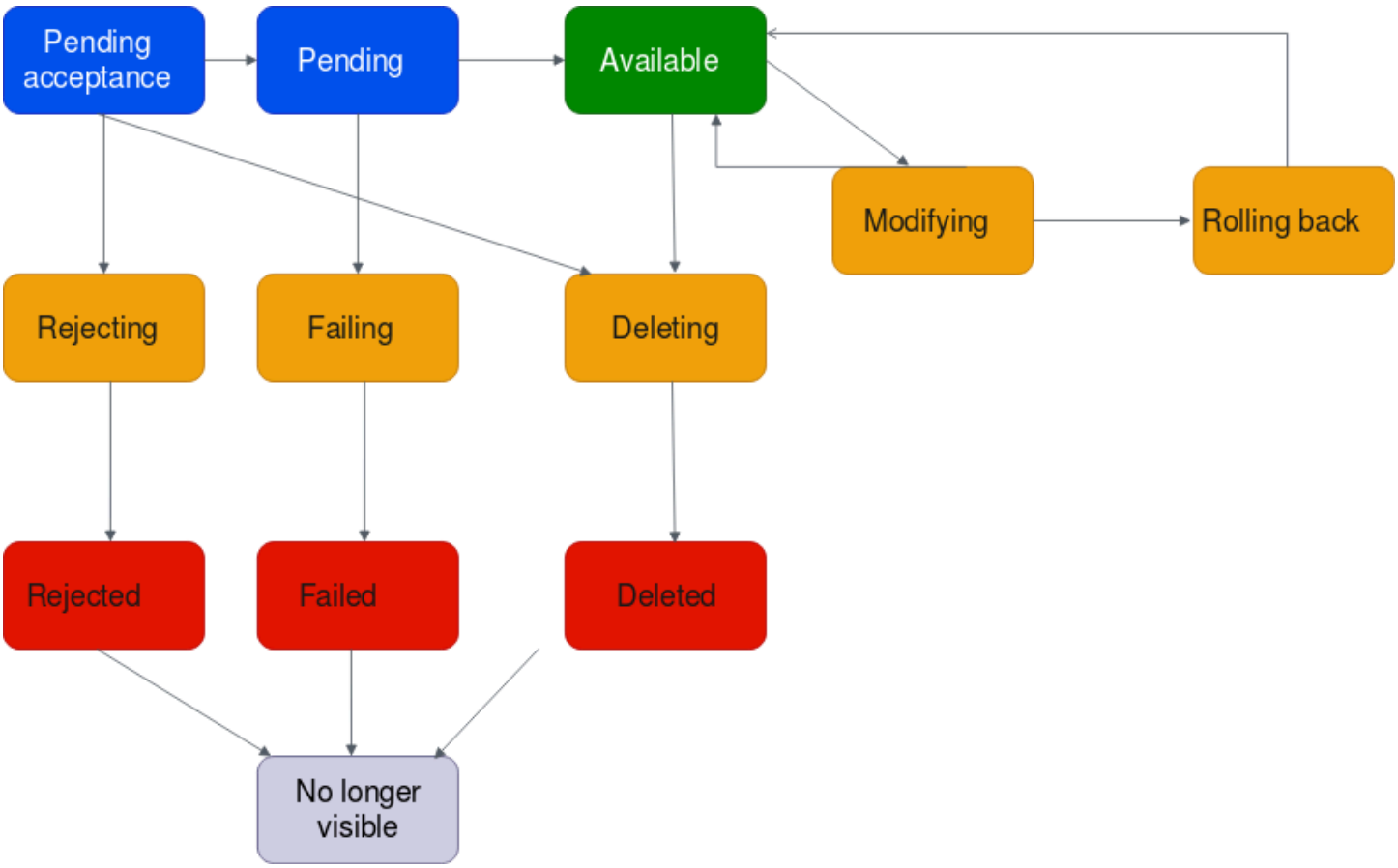
Il diagramma seguente mostra gli stati che un collegamento può avere nella configurazione di un unico account o nella configurazione di più account per cui è attivata l'opzione Accetta automaticamente collegamenti condivisi.



- In sospeso: una richiesta per un collegamento VPC è stata avviata e si trova nel processo di provisioning. In questa fase, il collegamento può non riuscire o passare allo stato `available`.
- Errore: una richiesta per un collegamento VPC ha avuto esito negativo. In questa fase, il collegamento VPC passa allo stato `failed`.
- Non riuscita: la richiesta di collegamento VPC non è riuscita. Mentre si trova in questo stato, non può essere eliminata. Il collegamento VPC non riuscito rimane visibile per 2 ore, dopo di che non è più visibile.
- Disponibile: il collegamento VPC è disponibile e il traffico può fluire tra il VPC e il gateway di transito. In questa fase, il collegamento può passare allo stato `modifying` o allo stato `deleting`.
- Eliminazione: un collegamento VPC che è in fase di eliminazione. In questa fase, il collegamento può passare allo stato `deleted`.
- Eliminato: un collegamento VPC `available` è stato eliminato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.

- Modifica: è stata effettuata una richiesta di modifica delle proprietà del collegamento VPC. In questa fase, il collegamento può passare allo stato `available` o allo stato `rolling back`.
- Rollback: la richiesta di modifica del collegamento VPC non può essere completata e il sistema sta annullando le modifiche apportate. In questa fase, il collegamento può passare allo stato `available`.

Il diagramma seguente mostra gli stati che un collegamento può avere nella configurazione di più account per cui è attivata l'opzione Accetta automaticamente collegamenti condivisi.



- Pending-acceptance: la richiesta di collegamento VPC è in attesa di essere accettata. In questa fase, il collegamento può passare allo stato `pending`, allo stato `rejecting` o allo stato `deleting`.
- Rifiuto: un collegamento VPC che sta per essere rifiutato. In questa fase, il collegamento può passare allo stato `rejected`.
- Rifiutato: un collegamento VPC `pending acceptance` è stato rifiutato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.

- In sospeso: un collegamento VPC è stato accettato e si trova nel processo di provisioning. In questa fase, il collegamento può non riuscire o passare allo stato `available`.
- Errore: una richiesta per un collegamento VPC ha avuto esito negativo. In questa fase, il collegamento VPC passa allo stato `failed`.
- Non riuscita: la richiesta di collegamento VPC non è riuscita. Mentre si trova in questo stato, non può essere eliminata. Il collegamento VPC non riuscito rimane visibile per 2 ore, dopo di che non è più visibile.
- Disponibile: il collegamento VPC è disponibile e il traffico può fluire tra il VPC e il gateway di transito. In questa fase, il collegamento può passare allo stato `modifying` o allo stato `deleting`.
- Eliminazione: un collegamento VPC che è in fase di eliminazione. In questa fase, il collegamento può passare allo stato `deleted`.
- Eliminato: un collegamento VPC `available` o `pending acceptance` è stato eliminato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.
- Modifica: è stata effettuata una richiesta di modifica delle proprietà del collegamento VPC. In questa fase, il collegamento può passare allo stato `available` o allo stato `rolling back`.
- Rollback: la richiesta di modifica del collegamento VPC non può essere completata e il sistema sta annullando le modifiche apportate. In questa fase, il collegamento può passare allo stato `available`.

Modalità Appliance

Se prevedi di configurare un'appliance di rete con stato nel tuo VPC, puoi abilitare il supporto in modalità appliance per l'attacco VPC in cui si trova l'appliance quando crei un allegato. Ciò garantisce che AWS Transit Gateway utilizzi la stessa zona di disponibilità per quell'allegato VPC per tutta la durata del flusso di traffico tra un'origine e una destinazione. Consente inoltre a un gateway di transito di inviare traffico a qualsiasi zona di disponibilità nel VPC purché esista un'associazione di sottoreti in quella zona. Sebbene la modalità appliance sia supportata solo sugli allegati VPC, il flusso di rete può provenire da qualsiasi altro tipo di allegato del gateway di transito, inclusi gli allegati VPC, VPN e Connect. La modalità Appliance funziona anche per i flussi di rete che hanno origini e destinazioni diverse. Regioni AWS I flussi di rete possono potenzialmente essere ribilanciati tra diverse zone di disponibilità se inizialmente non si abilita la modalità appliance ma successivamente si modifica la configurazione degli allegati per abilitarla. È possibile abilitare o disabilitare la modalità appliance utilizzando la console, la riga di comando o l'API.

La modalità Appliance in AWS Transit Gateway ottimizza il routing del traffico considerando le zone di disponibilità di origine e di destinazione quando si determina il percorso attraverso un VPC in modalità appliance. Questo approccio migliora l'efficienza e riduce la latenza. Di seguito sono riportati alcuni scenari di esempio.

Scenario 1: routing del traffico all'interno della zona di disponibilità tramite un VPC dell'appliance

Quando il traffico fluisce da una zona di disponibilità di origine in us-east-1a a una zona di disponibilità di destinazione in us-east-1a, con allegati in modalità appliance sia in us-east-1a che in us-east-1b, Transit Gateway sceglie un'interfaccia di rete da us-east-1a all'interno del VPC dell'appliance. AWS Questa zona di disponibilità viene mantenuta per l'intera durata del flusso di traffico tra origine e destinazione.

Scenario 2: routing del traffico tra zone di disponibilità tramite un VPC dell'appliance

Per il traffico che scorre da una zona di disponibilità di origine in us-east-1a a una zona di disponibilità di destinazione in us-east-1b, con allegati VPC in modalità appliance sia in us-east-1a che in us-east-1b, AWS Transit Gateway utilizza un algoritmo di hash di flusso per selezionare us-east-1a o us-east-1b nel VPC dell'appliance. La zona di disponibilità scelta viene utilizzata in modo coerente per tutta la durata del flusso.

Scenario 3: instradamento del traffico attraverso un VPC dell'appliance senza dati sulla zona di disponibilità

Quando il traffico proviene dalla zona di disponibilità di origine in us-east-1a verso una destinazione senza informazioni sulla zona di disponibilità, ad esempio il traffico legato a Internet, con allegati VPC in modalità appliance sia in us-east-1a che in us-east-1b, Transit Gateway sceglie un'interfaccia di rete da us-east-1a all'interno del VPC dell'appliance. AWS

Scenario 4: instradamento del traffico attraverso una zona di disponibilità distinta dall'origine o dalla destinazione

Quando il traffico fluisce da una zona di disponibilità di origine in us-east-1a a una zona di disponibilità di destinazione us-east-1b con allegati VPC in modalità appliance in zone di disponibilità diverse dall'origine o dalla destinazione (ad esempio, le modalità appliance VPCs sono in us-east-1c e us-east-1d), AWS Transit Gateway utilizza un algoritmo di hash di flusso per selezionare us-east-1c o us-east-1d nel VPC dell'appliance. La zona di disponibilità scelta viene utilizzata in modo coerente per tutta la durata del flusso.

> **Note**
>
> La modalità Appliance è supportata solo per gli allegati VPC.

Riferimenti dei gruppi di sicurezza

È possibile utilizzare questa funzionalità per semplificare la gestione dei gruppi di sicurezza e il controllo del instance-to-instance traffico collegato allo stesso gateway di VPCs transito. È possibile fare riferimenti incrociati ai gruppi di sicurezza solo nelle regole in entrata. Le regole di sicurezza in uscita non supportano i riferimenti ai gruppi di sicurezza. Non sono previsti costi aggiuntivi associati all'attivazione o all'utilizzo dei riferimenti ai gruppi di sicurezza.

Il supporto per i riferimenti ai gruppi di sicurezza può essere configurato sia per i gateway di transito che per gli allegati VPC del gateway di transito e funzionerà solo se è stato abilitato sia per un gateway di transito che per i relativi allegati VPC.

Limitazioni

Le seguenti limitazioni si applicano quando si utilizza il riferimento a gruppi di sicurezza con un allegato VPC.

- Il riferimento ai gruppi di sicurezza non è supportato per gli allegati VPC nella zona di disponibilità use1-az3.
- Il riferimento ai gruppi di sicurezza non è supportato per gli endpoint. PrivateLink Si consiglia di utilizzare regole di sicurezza basate su IP CIDR come alternativa.
- Il riferimento ai gruppi di sicurezza funziona per Elastic File System (EFS) purché sia configurata una regola del gruppo di sicurezza Allow Output per le interfacce EFS nel VPC.
- Per la connettività alla zona locale tramite un gateway di transito, sono supportate solo le seguenti Local Zone: us-east-1-atl-2a, us-east-1-dfw-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a e us-west-2-phx-2a.
- Ti consigliamo di disabilitare questa funzionalità a livello di collegamento VPC VPCs per le sottoreti in Local Zones, AWS Outposts e AWS Wavelength Zones non supportate, poiché potrebbe causare interruzioni del servizio.
- Se disponi di un VPC di ispezione, il riferimento al gruppo di sicurezza tramite il gateway di transito non funziona tramite Gateway Load AWS Balancer o un Network Firewall. AWS

Attività

- Creare un VPC allegato utilizzando Amazon VPC Transit Gateways
- Modifica un VPC allegato utilizzando Amazon VPC Transit Gateways
- Modifica i tag VPC degli allegati utilizzando Amazon VPC Transit Gateways
- Visualizza un VPC allegato utilizzando Amazon VPC Transit Gateways
- Eliminare un VPC allegato utilizzando Amazon VPC Transit Gateways
- Aggiornare le AWS Transit Gateway regole in entrata dei gruppi di sicurezza
- Identifica i AWS Transit Gateway gruppi di sicurezza referenziati
- Rimuovi le regole obsolete AWS Transit Gateway dei gruppi di sicurezza
- Risoluzione dei problemi relativi alla creazione di allegati Amazon VPC Transit Gateways VPC

Creare un VPC allegato utilizzando Amazon VPC Transit Gateways

Per creare un VPC allegato utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).
4. Per Name tag (Tag nome), è possibile inserire un nome per il gateway di transito.
5. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito di cui si è proprietari o un gateway di transito condiviso con l'utente.
6. Per Tipo di allegato, scegli VPC.
7. Scegli se abilitare il DNSsupporto in modalità IPv6Support, Support e Appliance.

   Se viene scelta la modalità appliance, il flusso di traffico tra un'origine e una destinazione utilizza la stessa zona di disponibilità per l'VPCallegato per tutta la durata di tale flusso.
8. Scegli se abilitare il supporto Security Group Referencing. Abilita questa funzionalità per fare riferimento a un gruppo di sicurezza VPCs collegato a un gateway di transito. Per ulteriori informazioni sulla referenziazione dei gruppi di sicurezza, vederethe section called “Riferimenti dei gruppi di sicurezza”.
9. Scegli se abilitare IPv6Support.

10. Per VPCID, scegli VPC da collegare al gateway di transito.

    A questo VPC deve essere associata almeno una sottorete.
11. Per Subnet IDs, selezionare una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
12. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Per creare un VPC allegato utilizzando AWS CLI

Usare il comando create-transit-gateway-vpc-attachment.

Modifica un VPC allegato utilizzando Amazon VPC Transit Gateways

Per modificare gli VPC allegati utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Seleziona l'VPCallegato, quindi scegli Azioni, Modifica allegato del gateway di transito.
4. Abilita o disabilita una delle seguenti opzioni:

   - Supporto DNS
   - Supporto IPv6
   - Supporto in modalità appliance
5. Per aggiungere o rimuovere una sottorete dall'allegato, selezionate o deselezionate la casella di controllo accanto all'ID di sottorete che desiderate aggiungere o rimuovere.

   > **Note**
   >
   > L'aggiunta o la modifica di una sottorete di VPC allegati potrebbe influire sul traffico di dati mentre l'allegato è in fase di modifica.
6. Per poter fare riferimento a un gruppo di sicurezza tramite collegamento a un gateway VPCs di transito, seleziona Security Group Referencing support. Per ulteriori informazioni sulla referenziazione dei gruppi di sicurezza, vedere. the section called “Riferimenti dei gruppi di sicurezza”

> **Note**
>
> Se disabiliti il riferimento ai gruppi di sicurezza per un gateway di transito esistente, verrà disabilitato su tutti gli VPC allegati.

7. Scegliere Modifica collegamento del gateway di transito.

Per modificare gli VPC allegati utilizzando il AWS CLI

Utilizzate il comando modify-transit-gateway-vpc-attachment.

Modifica i tag VPC degli allegati utilizzando Amazon VPC Transit Gateways

Per modificare i tag VPC degli allegati utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Seleziona l'VPCallegato, quindi scegli Azioni, Gestisci tag.
4. [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:
   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.
5. [Rimuovere un tag] Accanto al tag, scegliere Rimuovi.
6. Seleziona Salva.

VPCi tag degli allegati possono essere modificati solo utilizzando la console.

Visualizza un VPC allegato utilizzando Amazon VPC Transit Gateways

Per visualizzare gli VPC allegati utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Nella colonna Tipo di risorsa, cerca VPC. Questi sono gli VPC allegati.

4. Selezionare un collegamento per visualizzarne i dettagli.

Per visualizzare gli VPC allegati utilizzando il AWS CLI

Utilizzare il comando describe-transit-gateway-vpc-attachments.

Eliminare un VPC allegato utilizzando Amazon VPC Transit Gateways

Per eliminare un VPC allegato utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Seleziona l'VPCallegato.
4. Scegliere Operazioni,Eliminare l'allegato del gateway.
5. Quando richiesto, digitare **`delete`** e scegliere Delete (Elimina).

Per eliminare un VPC allegato utilizzando il AWS CLI

Utilizzare il comando delete-transit-gateway-vpc-attachment.

Aggiornare le AWS Transit Gateway regole in entrata dei gruppi di sicurezza

È possibile aggiornare qualsiasi regola del gruppo di sicurezza in entrata associata a un gateway di transito. Puoi aggiornare le regole dei gruppi di sicurezza utilizzando la VPC console Amazon Console o la riga di comando o. API Per ulteriori informazioni sulla referenziazione dei gruppi di sicurezza, consulta. the section called “Riferimenti dei gruppi di sicurezza”

Per aggiornare le regole di gruppo di sicurezza tramite la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Seleziona il gruppo di sicurezza e scegli Azioni, Modifica regole in entrata per modificare le regole in entrata.

4. Per aggiungere una regola, scegli Aggiungi regola e specifica il tipo, il protocollo e l'intervallo di porte. Per Source (regola in entrata), inserisci l'ID del gruppo di sicurezza nel gateway VPC connesso al transito.

> **Note**
>
> I gruppi di sicurezza in un gateway VPC connesso al transito non vengono visualizzati automaticamente.

5. Per modificare una regola esistente, cambia i relativi valori (ad esempio, l'origine o la descrizione).
6. Per eliminare una regola, seleziona il pulsante Elimina accanto alla regola corrispondente.
7. Scegliere Salva regole.

Per aggiornare le regole in entrata tramite la riga di comando

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

Identifica i AWS Transit Gateway gruppi di sicurezza referenziati

Per determinare se il vostro gruppo di sicurezza è referenziato nelle regole di un gruppo di sicurezza in un gateway di transito VPC collegato allo stesso gateway di transito, utilizzate uno dei seguenti comandi.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

Rimuovi le regole obsolete AWS Transit Gateway dei gruppi di sicurezza

Una regola del gruppo di sicurezza obsoleta è una regola che fa riferimento a un gruppo di sicurezza eliminato nello stesso gateway di transito VPC o VPC collegato allo stesso gateway di transito. Quando una regola di gruppo di sicurezza diventa obsoleta, non viene automaticamente rimossa dal gruppo di sicurezza, ma deve essere eliminata manualmente.

Puoi visualizzare ed eliminare le regole obsolete dei gruppi di sicurezza per un VPC utilizzo della VPC console Amazon.

Per visualizzare Ed eliminare regole di gruppo di sicurezza obsolete

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Seleziona Actions (Operazioni), Manage stale rules (Gestisci regole obsolete).
4. Perché VPC, scegli quello VPC con le regole obsolete.
5. Scegli Modifica.
6. Scegliere il pulsante Delete (Elimina) a destra della regola da eliminare. Scegliere Preview changes (Anteprima modifiche), Save rules (Salva regole).

Per descrivere le regole obsolete del gruppo di sicurezza utilizzando la riga di comando

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Dopo aver identificato le regole obsolete del gruppo di sicurezza, potete eliminarle utilizzando i comandi revoke-security-group-ingresso revoke-security-group-egress.

Risoluzione dei problemi relativi alla creazione di allegati Amazon VPC Transit Gateways VPC

Il seguente argomento può aiutarti a risolvere i problemi che potresti riscontrare durante la creazione di un allegato. VPC

Problema

L'VPCallegato non è riuscito.

Causa

Di seguito è riportata la possibile causa:

1. L'utente che sta creando l'VPCallegato non dispone delle autorizzazioni corrette per creare un ruolo collegato al servizio.

2. Esiste un problema di limitazione a causa del numero eccessivo di IAM richieste, ad esempio utilizzate AWS CloudFormation per creare autorizzazioni e ruoli.
3. L'account è dotato del ruolo collegato al servizio e il ruolo collegato al servizio è stato modificato.
4. Il gateway di transito non è nello stato `available`.

Soluzione

A seconda della causa, provare quanto segue:

1. Verificare che l'utente disponga delle autorizzazioni corrette per creare ruoli collegati ai servizi. Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente. IAM Dopo che l'utente ha ottenuto le autorizzazioni, crea l'allegato. VPC
2. Crea l'VPCallegato manualmente. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
3. Verificare che il ruolo collegato al servizio disponga delle autorizzazioni corrette. Per ulteriori informazioni, consulta the section called “Gateway di transito”.
4. Verificare che il gateway di transito sia nello stato `available`. Per ulteriori informazioni, consulta the section called “Visualizza un gateway di transito”.

AWS Site-to-Site VPN allegati in Amazon VPC Transit Gateways

Puoi connettere un Site-to-Site VPN allegato a un gateway di transito in Amazon VPC Transit Gateways, consentendoti di connettere la tua VPCs rete a quella locale. Sono supportati sia i percorsi dinamici che quelli statici, così come IPv4 e. IPv6

Requisiti

- Per collegare una VPN connessione al gateway di transito è necessario specificare il gateway del VPN cliente, che ha requisiti specifici per i dispositivi. Prima di creare un Site-to-Site VPN allegato, esamina i requisiti del gateway del cliente per assicurarti che il gateway sia configurato correttamente. Per ulteriori informazioni su questi requisiti, inclusi esempi di file di configurazione del gateway, consulta Requisiti per il dispositivo gateway Site-to-Site VPN del cliente nella Guida per l'AWS Site-to-Site VPN utente.
- Per quanto riguarda le rotte staticheVPNs, è inoltre necessario aggiungere prima le rotte statiche alla tabella delle rotte del gateway di transito. Le rotte statiche in una tabella di routing del gateway di transito che hanno come destinazione un VPN allegato non vengono filtrate in base a, in Site-to-

Site VPN quanto ciò potrebbe consentire un flusso di traffico in uscita non intenzionale quando si utilizza un formato basato. BGP VPN Per i passaggi per aggiungere una route statica a una tabella di routing del gateway di transito, vedere. Creare una route statica

Puoi creare, visualizzare o eliminare un Site-to-Site VPN allegato del gateway di transito utilizzando la VPC console Amazon o utilizzando il AWS CLI.

Attività

- Crea un gateway di transito collegato a un Amazon VPC Transit Gateways che VPN utilizza
- Visualizza un VPN allegato utilizzando Amazon VPC Transit Gateways
- Eliminare un VPN allegato utilizzando Amazon VPC Transit Gateways

Crea un gateway di transito collegato a un Amazon VPC Transit Gateways che VPN utilizza

Per creare un VPN allegato utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).
4. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito che possiedi.
5. Per Tipo di allegato, scegli VPN.
6. In Customer Gateway (Gateway del cliente), eseguire una delle seguenti operazioni:
   - Per utilizzare un gateway del cliente esistente selezionare Existing (Esistente) e quindi selezionare il gateway da utilizzare.

     Se il tuo customer gateway è protetto da un dispositivo di traduzione degli indirizzi di rete (NAT) abilitato all'NATattraversamento (NAT-T), utilizza l'indirizzo IP pubblico del NAT dispositivo e modifica le regole del firewall per UDP sbloccare la porta 4500.
   - Per creare un gateway per il cliente, scegli Nuovo, quindi in Indirizzo IP, digita un indirizzo IP pubblico statico e. BGPASN

In Routing options (Opzioni di routing), selezionare se utilizzare la modalità Dynamic (Dinamica) o Static (Statica). Per ulteriori informazioni, consulta Opzioni Site-to-Site VPN di routing nella Guida per l'AWS Site-to-Site VPN utente.

7. Per le opzioni del tunnel, inserisci gli CIDR intervalli e le chiavi precondivise per il tunnel. Per ulteriori informazioni, consulta Site-to-Site VPNarchitetture.
8. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).

Per creare un VPN allegato utilizzando AWS CLI

Utilizza il comando create-vpn-connection.

Visualizza un VPN allegato utilizzando Amazon VPC Transit Gateways

Per visualizzare gli VPN allegati utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Nella colonna Tipo di risorsa, cerca VPN. Questi sono gli VPN allegati.
4. Selezionare un collegamento per visualizzarne i dettagli o aggiungere tag.

Per visualizzare gli VPN allegati utilizzando il AWS CLI

Utilizza il comando describe-transit-gateway-attachments.

Eliminare un VPN allegato utilizzando Amazon VPC Transit Gateways

Per eliminare un VPN allegato utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Seleziona l'VPNallegato.
4. Scegli l'ID della risorsa della VPN connessione per accedere alla pagina VPNConnessioni.
5. Selezionare Actions (Operazioni), Delete (Elimina).

6. Quando viene richiesta la conferma, selezionare Delete (Elimina).

Per eliminare un VPN allegato utilizzando il AWS CLI

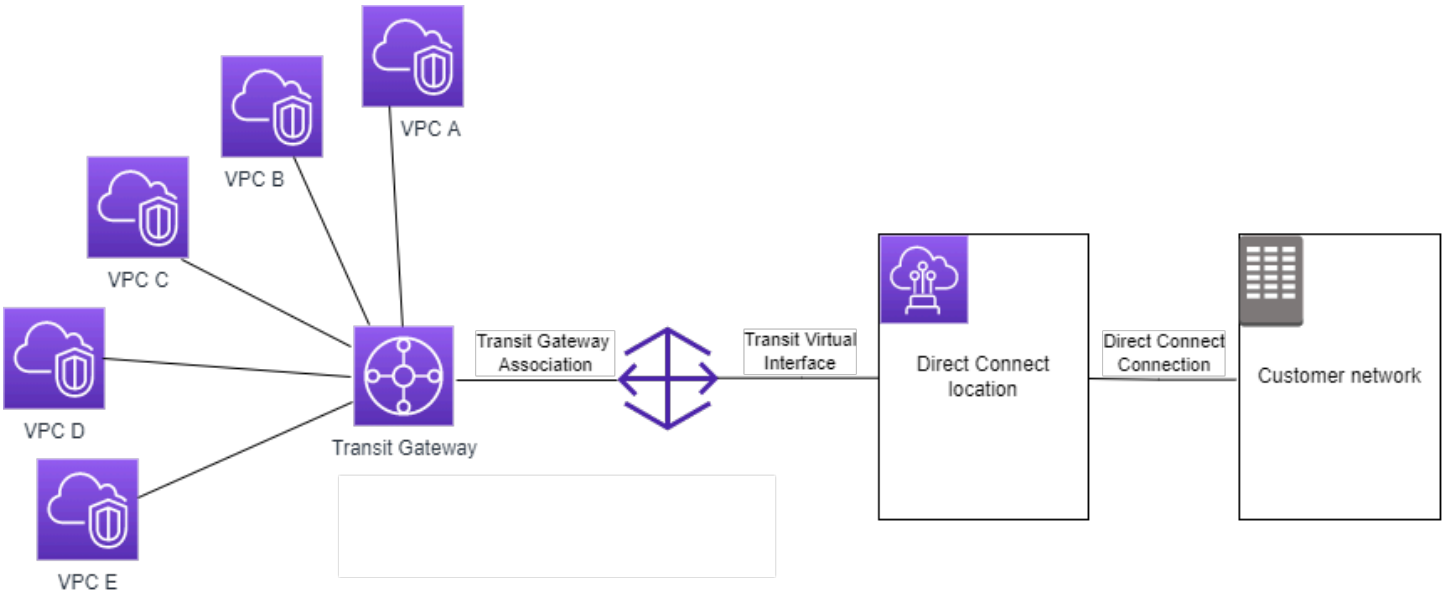
Utilizza il comando delete-vpn-connection.

Collegamenti del gateway di transito a un gateway Direct Connect in Amazon VPC Transit Gateways

Collegare un gateway di transito a un gateway Direct Connect usando un'interfaccia virtuale di transito. Questa configurazione offre i seguenti vantaggi. È possibile:

- Gestisci una singola connessione per più VPCs o VPNs che si trovano nella stessa regione.
- Pubblicizza prefissi da locale a locale AWS e da locale a locale. AWS

Il diagramma seguente illustra come il gateway Direct Connect consente di creare una singola connessione alla connessione Direct Connect VPCs utilizzabile da tutti.



La soluzione prevede i seguenti componenti:

- Un gateway di transito.
- Un gateway Direct Connect.
- Un'associazione tra il gateway Direct Connect e il gateway di transito.

- Un'interfaccia virtuale di transito collegata al gateway Direct Connect.

Per informazioni sulla configurazione dei gateway Direct Connect con gateway di transito, vedere Associazioni gateway di transito nel Manuale per l'utente di AWS Direct Connect .

Allegati di peering del gateway di transito in Amazon VPC Transit Gateway

È possibile effettuare il peering dei gateway di transito interregionali e interregionali e instradare il traffico tra di essi, incluso il traffico e il traffico. IPv4 IPv6 A tale scopo, creare un allegato di peering sul gateway di transito e specificare un gateway di transito. Il gateway di transito peer può trovarsi nel tuo account o provenire da un altro account. Puoi anche richiedere un allegato di peering dal tuo account a un gateway di transito di un altro account.

Dopo aver creato una richiesta di allegato di peering, il proprietario del gateway di transito peer (denominato anche gateway di transito accettatore) deve accettare la richiesta. Per instradare il traffico tra i gateway di transito, è necessario aggiungere un route statico alla tabella di routing del gateway di transito che punti all'allegato di peering del gateway di transito.

Ti consigliamo di utilizzare unique ASNs per ogni gateway di transito peer-to-peer per sfruttare le future funzionalità di propagazione delle rotte.

Il peering del gateway di transito non supporta la risoluzione di nomi host IPv4 DNS pubblici o privati in IPv4 indirizzi privati VPCs su entrambi i lati dell'allegato di peering del gateway di transito utilizzando l'allegato di peering del gateway di transito utilizzando l'allegato in un'altra regione. Amazon Route 53 Resolver Per maggiori informazioni sul resolver Route 53, consulta Cos'è un resolver Route 53? nella Guida per gli sviluppatori di Amazon Route 53.

Il peering del gateway tra le regioni utilizza la stessa infrastruttura di rete del peering VPC. Pertanto il traffico viene crittografato utilizzando la crittografia AES-256 a livello di rete virtuale mentre si sposta tra le regioni. Il traffico viene crittografato anche utilizzando la crittografia AES-256 a livello fisico quando attraversa collegamenti di rete che sono al di fuori del controllo fisico di AWS. Di conseguenza, il traffico viene crittografato due volte su collegamenti di rete al di fuori del controllo fisico di. AWS Nella stessa regione, il traffico viene crittografato a livello fisico solo quando attraversa collegamenti di rete che sono al di fuori del controllo fisico di AWS.

Per informazioni sulle regioni che supportano gli allegati di peering del gateway di transito, consulta AWS Transit Gateways. FAQs

Considerazioni relative alla regione di opt-in AWS

Puoi eseguire il peering dei gateway di transito attraverso i confini della regione di attivazione. Per informazioni su queste regioni e su come aderire, consulta Gestione delle AWS regioni. Se utilizzi il peering del gateway di transito in queste regioni, tieni in considerazione quanto segue:

- Puoi eseguire il peering in una regione di attivazione a condizione che l'account che accetta il collegamento peering abbia optato per tale regione.
- Indipendentemente dallo stato di attivazione della regione, AWS condivide i seguenti dati dell'account con l'account che accetta l'allegato di peering:
  - Account AWS ID
  - ID gateway di transito
  - Codice regione
- Quando elimini il collegamento del gateway di transito, i dati dell'account sopra riportati vengono eliminati.
- Si consiglia di eliminare il collegamento del peering del gateway di transito prima di disattivare la regione. Se non elimini il collegamento del peering, il traffico potrebbe continuare ad essere instradato sul collegamento e potresti continuare a sostenerne i costi. Se non elimini il collegamento, puoi riattivare e quindi eliminarlo.
- In generale, il gateway di transito ha un modello di pagamento a carico del richiedente. Utilizzando un collegamento peering del gateway di transito attraverso un limite di attivazione, potresti sostenere addebiti in una regione che accetta il collegamento, incluse le regioni che non hai scelto. Per ulteriori informazioni, consulta Prezzi di AWS Transit Gateway.

Attività

- Crea un allegato di peering utilizzando Amazon VPC Transit Gateways
- Accetta o rifiuta una richiesta di peering di allegati utilizzando Amazon VPC Transit Gateways
- Aggiungi un percorso a una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways
- Eliminare un allegato di peering utilizzando Amazon VPC Transit Gateways

Crea un allegato di peering utilizzando Amazon VPC Transit Gateways

Prima di iniziare, assicurarsi di disporre dell'ID del gateway di transito che si desidera allegare. Se il gateway di transito si trova in un altro Account AWS, assicurati di avere l' Account AWS ID del proprietario del gateway di transito.

Dopo aver creato l'allegato peering, il proprietario del gateway di transito dell'accettante deve accettare la richiesta di allegato.

Per creare un allegato di peering utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).
4. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito che possiedi. I gateway di transito condivisi con te non sono disponibili per il peering.
5. Per Attachment type (Tipo di allegato), scegliere Peering Connection (Connessione peering).
6. Facoltativamente immettere un tag nome per l'allegato.
7. In Add account (Aggiungi account), eseguire una delle seguenti operazioni:
   - Se il gateway di transito è nel tuo account, scegliere Il mio account.
   - Se il gateway di transito è diverso Account AWS, scegli Altro account. In Account ID (ID account) immettere l'ID dell'account Account AWS .
8. Per Regione, scegliere la regione in cui si trova il gateway di transito.
9. Per Transit gateway (accettatore), immettere l'ID del gateway di transito che si desidera allegare.
10. Selezionare Create transit gateway attachment (Crea collegamento del gateway di transito).

Per creare un allegato di peering utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-peering-attachment.

Accetta o rifiuta una richiesta di peering di allegati utilizzando Amazon VPC Transit Gateways

Per attivare l'allegato peering, il proprietario del gateway di transito accettatore deve accettare la richiesta di allegato peering. Ciò è necessario anche se entrambi i gateway di transito si trovano nello stesso account. L'allegato di peering deve essere nello stato `pendingAcceptance`. Accettare la richiesta di allegato peering dall'area geografica in cui si trova il gateway di transito accettatore.

Puoi rifiutare qualsiasi richiesta di connessione peering VPC che hai ricevuto e il cui stato è `pendingAcceptance`. È necessario rifiutare la richiesta dalla regione geografica in cui si trova il gateway di transito accettatore.

Per accettare una richiesta di allegato peering utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Accept transit gateway attachment (Accetta il collegamento del gateway di transito alla VPN).
5. Aggiungere il route statico alla tabella di route del gateway di transito. Per ulteriori informazioni, consulta the section called “Creare una route statica”.

Per rifiutare una richiesta di allegato peering utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Reject transit gateway attachment (Rifiuta il collegamento del gateway di transito alla VPN).

Per accettare o rifiutare un allegato di peering utilizzando il AWS CLI

Utilizzate i comandi accept-transit-gateway-peering-attachment e reject-transit-gateway-peering-attachment.

Aggiungi un percorso a una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

Per instradare il traffico tra i gateway di transito con peering, è necessario aggiungere una route statica alla tabella di routing del gateway di transito che punti all'allegato di peering del gateway di transito. Il proprietario del gateway di transito dell'accettante deve inoltre aggiungere un route statico alla tabella dei percorsi del gateway di transito.

Per creare una route statica mediante la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Crea percorso statico, inserisci il CIDR blocco per il quale creare il percorso. Ad esempio, specifica il CIDR blocco di un VPC che è collegato al gateway di transito peer.
6. Scegliere l'allegato di peering per il percorso.
7. Scegliere Create static route (Crea route statico).

Per creare una rotta statica utilizzando AWS CLI

Utilizza il comando create-transit-gateway-route.

> **Important**
>
> Dopo aver creato il percorso, associare la tabella di route del gateway di transito all'allegato peering del gateway di transito. Per ulteriori informazioni, consulta the section called “Associare una tabella di instradamento di un gateway di transito.”.

Eliminare un allegato di peering utilizzando Amazon VPC Transit Gateways

È possibile eliminare un allegato peering del gateway di transito. Il proprietario di uno dei gateway di transito può eliminare l'allegato.

Per eliminare un allegato di peering utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito.
4. Scegliere Operazioni, Eliminare collegamento del gateway di transito.
5. Immettere **`delete`** e scegliere Delete (Elimina).

Per eliminare un allegato di peering utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-peering-attachment.

Allegati Transit Gateway Connect e peer Transit Gateway Connect in Amazon VPC Transit Gateways

È possibile creare un allegato Transit Gateway Connect per stabilire una connessione tra un gateway di transito e dispositivi virtuali di terze parti (come i WAN dispositivi SD) in esecuzione in unVPC. Un allegato Connect supporta il protocollo tunnel Generic Routing Encapsulation (GRE) per prestazioni elevate e il Border Gateway Protocol (BGP) per il routing dinamico. Dopo aver creato un allegato Connect, è possibile creare uno o più GRE tunnel (denominati anche peer Transit Gateway Connect) sull'allegato Connect per connettere il gateway di transito e l'appliance di terze parti. Si stabiliscono due BGP sessioni sul GRE tunnel per lo scambio di informazioni di routing.

> **Important**
>
> Un peer Transit Gateway Connect è costituito da due sessioni di BGP peering che terminano su AWS un'infrastruttura gestita. Le due sessioni di BGP peering forniscono la ridondanza del piano di routing, garantendo che la perdita di una sessione di BGP peering non influisca sulle operazioni di routing. Le informazioni di routing ricevute da entrambe le BGP sessioni vengono accumulate per il peer Connect specificato. Le due sessioni di BGP peering proteggono inoltre da qualsiasi operazione AWS dell'infrastruttura, come la manutenzione ordinaria, l'applicazione di patch, gli aggiornamenti hardware e le sostituzioni. Se il peer Connect funziona senza la sessione di dual BGP peering consigliata configurata per la ridondanza, potrebbe verificarsi una perdita momentanea di connettività durante le operazioni dell'infrastruttura. AWS Ti consigliamo vivamente di configurare entrambe le sessioni di

BGP peering sul tuo peer Connect. Se hai configurato più peer Connect per supportare l'alta disponibilità sul lato appliance, ti consigliamo di configurare entrambe le sessioni di BGP peering su ciascuno dei tuoi peer Connect.

Un allegato Connect utilizza un allegato esistente VPC o Direct Connect come meccanismo di trasporto sottostante. Questo è detto collegamento di trasporto. Il gateway di transito identifica i GRE pacchetti corrispondenti provenienti dall'appliance di terze parti come traffico proveniente dall'allegato Connect. Tratta tutti gli altri pacchetti, compresi i GRE pacchetti con informazioni errate sull'origine o sulla destinazione, come traffico proveniente dall'allegato di trasporto.

> **Note**
>
> Per utilizzare un collegamento Direct Connect come meccanismo di trasporto, devi prima integrare Direct Connect con AWS Transit Gateway. Per i passaggi per creare questa integrazione, consulta Integrazione WAN dei dispositivi SD con AWS Transit Gateway e AWS Direct Connect.

Peer Connect

Un peer (GREtunnel) Connect è costituito dai seguenti componenti.

CIDRBlocchi interni (BGPindirizzi)

Gli indirizzi IP interni utilizzati per il BGP peering. È necessario specificare un CIDR blocco /29 dall'`169.254.0.0/16`intervallo per. IPv4 Facoltativamente, è possibile specificare un CIDR blocco /125 dall'`fd00::/8`intervallo per. IPv6 I seguenti CIDR blocchi sono riservati e non possono essere utilizzati:

- 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

È necessario configurare il primo indirizzo dell'IPv4intervallo sull'appliance come indirizzo BGP IP. Quando si utilizzaIPv6, se il CIDR blocco interno è fd00: :/125, è necessario configurare il primo indirizzo di questo intervallo (fd00: :1) sull'interfaccia tunnel dell'appliance.

Gli BGP indirizzi devono essere univoci in tutti i tunnel di un gateway di transito.

Indirizzo IP peer

L'indirizzo IP del peer (indirizzo IP GRE esterno) sul lato appliance del peer Connect. Questo può essere un qualsiasi indirizzo IP. L'indirizzo IP può essere un IPv6 indirizzo IPv4 o, ma deve appartenere alla stessa famiglia di indirizzi IP dell'indirizzo del gateway di transito.

Indirizzo gateway di transito

L'indirizzo IP del peer (indirizzo IP GRE esterno) sul lato gateway di transito del peer Connect. L'indirizzo IP deve essere specificato dal CIDR blocco del gateway di transito e deve essere univoco per tutti gli allegati Connect sul gateway di transito. Se non specifichi un indirizzo IP, utilizziamo il primo indirizzo disponibile del CIDR blocco del gateway di transito.

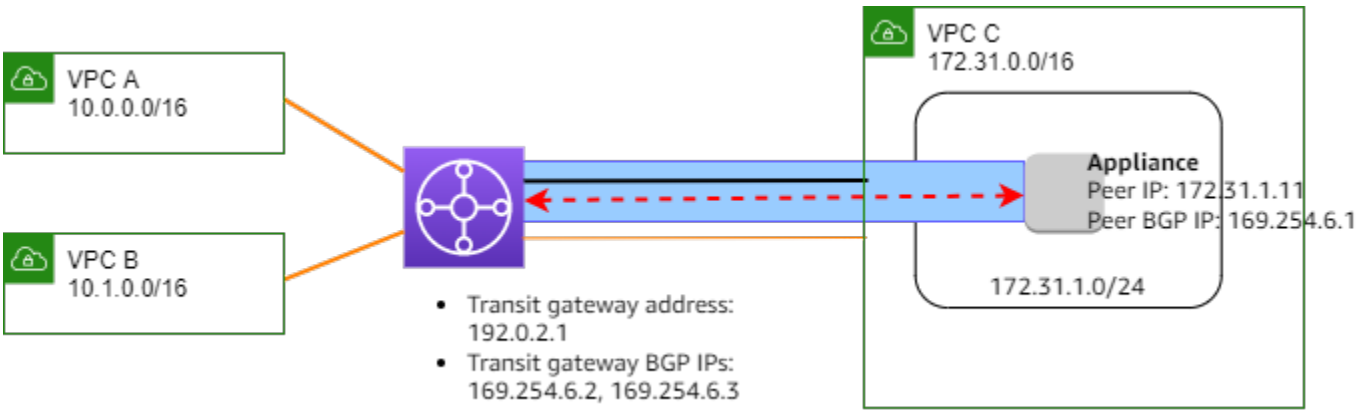
Puoi aggiungere un CIDR blocco gateway di transito quando crei o modifichi un gateway di transito.

L'indirizzo IP può essere un IPv6 indirizzo IPv4 o, ma deve appartenere alla stessa famiglia di indirizzi IP dell'indirizzo IP peer.

L'indirizzo IP peer e l'indirizzo del gateway di transito vengono utilizzati per identificare in modo univoco il tunnel. GRE Puoi riutilizzare entrambi gli indirizzi in più tunnel, ma non entrambi nello stesso tunnel.

Transit Gateway Connect per il BGP peering supporta solo Multiprotocol BGP (MP-BGP), dove è richiesto l'indirizzamento IPv4 Unicast per stabilire anche una BGP sessione per Unicast. IPv6 È possibile utilizzare entrambi IPv6 gli indirizzi IPv4 E per gli indirizzi IP esterni. GRE

L'esempio seguente mostra un allegato Connect tra un gateway di transito e un dispositivo in unVPC.



Componente diagramma	Descrizione
	VPCallegato
	Collegamento Connect
	GREtunnel (Connect peer)
	BGPsessione di peering

Nell'esempio precedente, un allegato Connect viene creato su un VPC allegato esistente (l'allegato di trasporto). Un peer Connect viene creato sull'allegato Connect per stabilire una connessione a un dispositivo in. VPC L'indirizzo del gateway di transito è`192.0.2.1`, e l'intervallo di BGP indirizzi è. `169.254.6.0/29` Il primo indirizzo IP nell'intervallo (`169.254.6.1`) è configurato sull'appliance come BGP indirizzo IP peer.

La tabella di routing di sottorete per VPC C ha una route che indirizza il traffico destinato al CIDR blocco del gateway di transito verso il gateway di transito.

Destinazione	Target
172.31.0.0/16	Locale
192.0.2.0/24	tgw-id

Requisiti e considerazioni

Di seguito sono riportati i requisiti e le considerazioni per un collegamento Connect.

- Per informazioni sulle regioni che supportano gli allegati Connect, consulta AWS Transit Gateway FAQ.
- L'appliance di terze parti deve essere configurata per inviare e ricevere traffico su un GRE tunnel da e verso il gateway di transito utilizzando l'allegato Connect.
- L'appliance di terze parti deve essere configurata per essere utilizzata BGP per gli aggiornamenti dinamici delle rotte e i controlli dello stato.
- Sono supportati i seguenti tipi BGP di:
  - Esterno BGP (eBGP): utilizzato per la connessione a router che si trovano in un sistema autonomo diverso rispetto al gateway di transito. Se usi eBGP, devi configurare ebgp-multihop con un valore time-to-live () TTL di 2.
  - Interno BGP (iBGP): utilizzato per la connessione a router che si trovano nello stesso sistema autonomo del gateway di transito. Il gateway di transito non installerà rotte da un i BGP peer (dispositivo di terze parti), a meno che le rotte non provengano da un e BGP peer e abbiano dovuto essere configurate. next-hop-self I percorsi pubblicizzati da un dispositivo di terze parti tramite i peering devono avere un. BGP ASN
  - MP- BGP (estensioni multiprotocollo perBGP): utilizzato per supportare più tipi di protocolli, ad esempio famiglie di indirizzi. IPv4 IPv6
- Il timeout BGP keep-alive predefinito è di 10 secondi e il timer di attesa predefinito è di 30 secondi.
- IPv6BGPil peering non è supportato; è supportato solo il peering IPv4 basatoBGP. IPv6i prefissi vengono scambiati tramite IPv4 BGP peering utilizzando MP-. BGP
- Il rilevamento dell'inoltro bidirezionale () non è supportato. BFD
- BGPil riavvio gradito non è supportato.
- Quando crei un gateway di transito peer, se non specifichi un numero di peer, scegliamo il ASN numero del gateway di transito. ASN Ciò significa che l'appliance e il gateway di transito si troveranno nello stesso sistema autonomo che esegue i. BGP
- Un peer Connect che utilizza l'PATHattributo BGP AS- è la route preferita quando si hanno due peer Connect.

  Per utilizzare il routing multipath (ECMP) equal-cost tra più dispositivi, è necessario configurare l'appliance in modo che annunci gli stessi prefissi al gateway di transito con lo stesso attributo AS-. BGP PATH Affinché il gateway di transito scelga tutti i ECMP percorsi disponibili, l'AS- PATH e

l'Autonomous System Number () devono corrispondere. ASN Il gateway di transito può essere utilizzato ECMP tra peer Connect per lo stesso allegato Connect o tra allegati Connect sullo stesso gateway di transito. Il gateway di transito non può essere utilizzato ECMP tra entrambi i peer ridondanti che un BGP singolo peer gli stabilisce.

- Per impostazione predefinita, con un allegato Connect le route vengono propagate a una tabella di routing del gateway di transito.
- Le route statiche non sono supportate.
- Assicurati che l'interfaccia esterna del dispositivo di terze parti (sorgente del tunnel) sia la Maximum Transmission Unit () MTU
  - corrisponde a quella MTU dell'interfaccia del GRE tunnel, oppure
  - dovrebbe essere maggiore di quella dell'interfaccia GRE del tunnel.

Attività

- Crea un allegato Connect utilizzando Amazon VPC Transit Gateways
- Crea un peer Connect utilizzando Amazon VPC Transit Gateways
- Visualizza gli allegati Connect e i peer Connect utilizzando Amazon VPC Transit Gateways
- Modifica gli allegati Connect e i peer tag Connect utilizzando Amazon VPC Transit Gateways
- Eliminare un peer Connect utilizzando Amazon VPC Transit Gateways
- Eliminare un allegato Connect utilizzando Amazon VPC Transit Gateways

Crea un allegato Connect utilizzando Amazon VPC Transit Gateways

Per creare un collegamento Connect, devi specificare un collegamento esistente come collegamento di trasporto. È possibile specificare un VPC allegato o un allegato Direct Connect come allegato di trasporto.

Per creare un collegamento Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Selezionare Create transit gateway attachments (crea collegamenti del gateway di transito).
4. (Facoltativo) In Tag nome, specifica un nome di tag per il collegamento.
5. Per ID gateway di transito, scegliere il gateway di transito per il collegamento.

6. In Tipo collegamento, seleziona Connect.
7. Per ID collegamento di trasporto, seleziona l'ID di un collegamento esistente (collegamento di trasporto).
8. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Per creare un allegato Connect utilizzando il AWS CLI

Utilizza il comando create-transit-gateway-connect.

Crea un peer Connect utilizzando Amazon VPC Transit Gateways

È possibile creare un peer Connect (GREtunnel) per un allegato Connect esistente. Prima di iniziare, assicurati di aver configurato un CIDR blocco di gateway di transito. È possibile configurare un CIDR blocco gateway di transito quando si crea o si modifica un gateway di transito.

Quando si crea il peer Connect, è necessario specificare l'indirizzo IP GRE esterno sul lato appliance del peer Connect.

Per creare un peer Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect e scegli Azioni, Crea peer connect.
4. (Facoltativo) In Tag nome, specifica un tag di nome per il peer di Connect.
5. (Facoltativo) Per Transit gateway GRE Address, specifica l'indirizzo IP GRE esterno per il gateway di transito. Per impostazione predefinita, viene utilizzato il primo indirizzo disponibile del CIDR blocco Transit Gateway.
6. Per Indirizzo peer, specificare l'GREindirizzo IP GRE esterno per il lato appliance del peer Connect.
7. Per i CIDRblocchi BGP Inside IPv4, specifica l'intervallo di IPv4 indirizzi interni utilizzati per il peering. BGP Specificate un CIDR blocco /29 dall'`169.254.0.0/16`intervallo.
8. (Facoltativo) Per CIDRi blocchi BGP Inside IPv6, specificate l'intervallo di IPv6 indirizzi interni utilizzati per il BGP peering. Specificate un CIDR blocco /125 dall'`fd00::/8`intervallo.
9. (Facoltativo) Per Peer ASN, specificare il Border Gateway Protocol (BGP) Autonomous System Number (ASN) per l'appliance. È possibile utilizzare un dispositivo esistente ASN assegnato alla

rete. Se non ne hai uno, puoi usarne uno privato ASN nell'intervallo 64512—65534 (16 bitASN) o 4200000000—4294967294 (32 bit). ASN

L'ASNimpostazione predefinita è la stessa del gateway di transito. Se configuri il Peer ASN in modo che sia diverso dal gateway di transito ASN (eBGP), devi configurare ebgp-multihop con un valore time-to-live (TTL) pari a 2.

10. Scegliere Crea peer connect.

Per creare un peer Connect utilizzando AWS CLI

Usate il comando create-transit-gateway-connect-peer.

Visualizza gli allegati Connect e i peer Connect utilizzando Amazon VPC Transit Gateways

Visualizza gli allegati Connect e i colleghi Connect.

Per visualizzare i collegamenti Connect e i peer Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect.
4. Per visualizzare i peer Connect per il collegamento, seleziona la scheda Peer Connect .

Per visualizzare gli allegati Connect e i colleghi Connect utilizzando il AWS CLI

Usa i comandi describe-transit-gateway-connectse describe-transit-gateway-connect-peers.

Modifica gli allegati Connect e i peer tag Connect utilizzando Amazon VPC Transit Gateways

Puoi modificare i tag per il collegamento Connect.

Per modificare i tag del collegamento Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito.

3. Seleziona il collegamento Connect, quindi seleziona Operazioni, Gestisci tag.
4. Per aggiungere un tag, seleziona Aggiungi un nuovo tag e specifica il nome e il valore della chiave.
5. Per rimuovere un tag, scegli Remove (Rimuovi).
6. Seleziona Salva.

Puoi modificare i tag per il peer Connect.

Per modificare i tag del peer Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito.
3. Seleziona il collegamento Connect, quindi seleziona Peer Connect.
4. Seleziona il peer di Connect, quindi scegli Operazioni, Gestisci tag.
5. Per aggiungere un tag, seleziona Aggiungi un nuovo tag e specifica il nome e il valore della chiave.
6. Per rimuovere un tag, scegli Remove (Rimuovi).
7. Seleziona Salva.

Per modificare l'allegato Connect e i tag del peer Connect utilizzando la AWS CLI

Utilizza i comandi create-tags e delete-tags.

Eliminare un peer Connect utilizzando Amazon VPC Transit Gateways

Se non hai più bisogno di un peer Connect, puoi eliminarlo.

Per eliminare un peer Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect.
4. Nella scheda Peer di Connect, seleziona il peer Connect e scegli Azioni, Elimina peer Connect.

Per eliminare un peer Connect utilizzando AWS CLI

Utilizzate il comando delete-transit-gateway-connect-peer.

Eliminare un allegato Connect utilizzando Amazon VPC Transit Gateways

Se non hai più bisogno di un collegamento Connect, puoi eliminarlo. Per prima cosa, devi eliminare tutti i peer Connect per il collegamento.

Per eliminare un collegamento Connect utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect e scegli Operazioni, Eliminare il collegamento del gateway.
4. Inserire **`delete`**, quindi scegliere Delete (Elimina).

Per eliminare un allegato Connect utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway-connect.

Tabelle di routing dei gateway di transito in Amazon VPC Transit Gateways

Utilizzare le tabelle di route del gateway di transito per configurare il routing per gli allegati del gateway di transito. Una tabella di routing è una tabella che contiene le regole che stabiliscono il modo in cui il traffico di rete viene instradato tra il tuo VPCs e. VPNs Ogni route della tabella contiene l'intervallo di indirizzi IP per le destinazioni a cui si desidera inviare il traffico.

Le tabelle di routing del gateway di transito consentono di associare una tabella a un allegato del gateway di transito. VPC,VPN, Gli allegati Direct Connect gateway, Peering e Connect sono tutti supportati. Se associati, i percorsi per questi allegati vengono propagati dall'allegato alla tabella di routing del gateway di transito di destinazione. Un allegato può essere propagato a più tabelle di routing.

Inoltre è possibile creare e gestire percorsi statici con una tabella di routing. Ad esempio, potresti avere una route statica che viene utilizzata come route di backup in caso di interruzione della rete che influisca su qualsiasi route dinamica.

Attività

- Crea una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

- Visualizza le tabelle delle rotte dei gateway di transito utilizzando Amazon VPC Transit Gateways
- Associa una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways
- Eliminare un'associazione per una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways
- Abilita la propagazione delle rotte su una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways
- Disattiva la propagazione delle rotte utilizzando Amazon VPC Transit Gateways
- Crea un percorso statico utilizzando Amazon VPC Transit Gateways
- Eliminare una route statica utilizzando Amazon VPC Transit Gateways
- Sostituisci un percorso statico utilizzando Amazon VPC Transit Gateways
- Esporta le tabelle di routing su Amazon S3 utilizzando Amazon VPC Transit Gateways
- Eliminare una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways
- Crea un riferimento all'elenco di prefissi della tabella di routing utilizzando Amazon VPC Transit Gateways
- Modifica di un riferimento a un elenco di prefissi utilizzando Amazon VPC Transit Gateways
- Eliminare un riferimento a un elenco di prefissi utilizzando Amazon VPC Transit Gateways

Crea una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

Per creare una tabella di route del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare Create Transit Gateway Route Table (Crea una tabella di routing del gateway di transito).
4. (Facoltativo) Per Tag nome, digitare un nome per la tabella di route del gateway di transito. Questa operazione crea un tag con la chiave impostata a "Name" e il valore corrispondente al nome indicato.
5. Per ID gateway di transito, selezionare il gateway di transito per la tabella di routing.
6. Selezionare Create transit gateway route table (Crea una tabella di routing del gateway di transito).

Per creare una tabella delle rotte del gateway di transito utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-route-table.

Visualizza le tabelle delle rotte dei gateway di transito utilizzando Amazon VPC Transit Gateways

Visualizzazione delle tabelle di instradamento del gateway di transito tramite la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. (Facoltativo) Per trovare una tabella di instradamento specifica o un insieme di tabelle, inserisci tutto il nome o una sua parte, una parola chiave o un attributo nel campo di filtro.
4. Seleziona la casella di controllo per una tabella di instradamento o scegli il suo ID per visualizzare informazioni sulle relative associazioni, propagazioni, route e tag.

Per visualizzare le tabelle dei percorsi dei gateway di transito utilizzando il AWS CLI

Utilizzate il comando describe-transit-gateway-route-tables.

Per visualizzare le rotte per una tabella delle rotte di un gateway di transito utilizzando il AWS CLI

Utilizza il comando search-transit-gateway-routes.

Per visualizzare le propagazioni delle rotte per una tabella delle rotte di un gateway di transito utilizzando il AWS CLI

Utilizzate il comando get-transit-gateway-route-table-propagations.

Per visualizzare le associazioni per una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando get-transit-gateway-route-table-associations.

Associa una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

È possibile associare una tabella di route del gateway di transito a un allegato del gateway di transito.

Per associare una tabella di route del gateway di transito tramite la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento.
4. Nella parte inferiore della pagina, selezionare la scheda Associations (Associazioni).
5. Selezionare Create association (Crea associazione).
6. Selezionare il collegamento da associare e quindi selezionare Create association (Crea associazione).

Per associare una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando associate-transit-gateway-route-table.

Eliminare un'associazione per una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

È possibile disassociare una tabella di route del gateway di transito da un allegato del gateway di transito.

Per disassociare una tabella di route del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento.
4. Nella parte inferiore della pagina, selezionare la scheda Associations (Associazioni).
5. Selezionare il collegamento per il quale eliminare l'associazione e quindi selezionare Delete association (Elimina associazione).
6. Quando viene richiesta la conferma, selezionare Delete association (Elimina associazione).

Per dissociare una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando disassociate-transit-gateway-route-table.

Abilita la propagazione delle rotte su una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

Utilizza la propagazione delle route per aggiungere una route da un collegamento a una tabella di routing.

Per propagare un route a una tabella di route degli allegati del gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare la propagazione.
4. Selezionare Actions (Operazioni), Create propagation (Crea propagazione).
5. Selezionare il collegamento nella pagina Create propagation (Crea propagazione).
6. Selezionare Create propagation (Crea propagazione).

Per abilitare la propagazione delle rotte utilizzando il AWS CLI

Utilizzate il comando enable-transit-gateway-route-table-propagation.

Disattiva la propagazione delle rotte utilizzando Amazon VPC Transit Gateways

Rimuovere una route propagata dalla tabella di instradamento di un collegamento.

Per disabilitare la propagazione delle route utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento dalla quale eliminare la propagazione.
4. Nella parte inferiore della pagina, selezionare la scheda Propagations (Propagazioni).
5. Selezionare il collegamento e quindi selezionare Delete propagation (Elimina propagazione).
6. Quando viene richiesta la conferma, selezionare Delete propagation (Elimina propagazione).

Per disabilitare la propagazione delle rotte utilizzando il AWS CLI

Utilizzate il comando disable-transit-gateway-route-table-propagation.

Crea un percorso statico utilizzando Amazon VPC Transit Gateways

Crea un percorso statico per un VPC allegato di peering del gateway di transito oppure puoi creare un percorso a buco nero che riduca il traffico corrispondente al percorso. VPN

Le route statiche in una tabella di routing del gateway di transito destinate a un VPN allegato non vengono filtrate da. Site-to-Site VPN Ciò potrebbe consentire un flusso di traffico in uscita non intenzionale quando si utilizza un basato. BGP VPN

Per creare una route statica mediante la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Crea percorso statico, inserisci il CIDR blocco per il quale creare il percorso, quindi scegli Attivo.
6. Selezionare il collegamento per la route.
7. Scegliere Create static route (Crea routing statico).

Per creare una route blackhole mediante la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Crea percorso statico, inserisci il CIDR blocco per il quale creare il percorso, quindi scegli Blackhole.
6. Scegliere Create static route (Crea route statico).

Per creare una rotta statica o una rotta a buco nero utilizzando il AWS CLI

Utilizza il comando create-transit-gateway-route.

Eliminare una route statica utilizzando Amazon VPC Transit Gateways

Elimina percorsi statici da una tabella di routing del gateway di transito.

Per eliminare una route statica mediante la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento da cui eliminare la route e scegliere Routes (Route).
4. Selezionare la route da eliminare.
5. Scegliere Eliminare routing statico.
6. Nella finestra del box di conferma, selezionare Delete static route (Elimina routing statico).

Per eliminare una route statica utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway-route.

Sostituisci un percorso statico utilizzando Amazon VPC Transit Gateways

Sostituisci una route statica in una tabella di routing del gateway di transito con una route statica diversa.

Sostituire una route statica mediante la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Scegli il percorso che desideri sostituire nella tabella di routing.
4. Nella sezione dei dettagli, scegli la scheda Route.
5. Scegli Azioni, Sostituisci route statica.
6. Per il Tipo, scegli Attivo o Blackhole.
7. Dal menu a discesa Scegli allegato, scegli il gateway di transito che sostituirà quello corrente nella tabella di routing.
8. Scegl Sostituisci route statica.

Per sostituire un percorso statico utilizzando il AWS CLI

Utilizza il comando replace-transit-gateway-route.

Esporta le tabelle di routing su Amazon S3 utilizzando Amazon VPC Transit Gateways

È possibile esportare le route nelle tabelle di routing del gateway di transito in un bucket Amazon S3. I percorsi vengono salvati nel bucket Amazon S3 specificato in un file. JSON

Per esportare le tabelle di route del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento che include le route da esportare.
4. Selezionare Actions (Operazioni), Export routes (Esporta route).
5. Nella pagina Export routes (Esporta routes), in S3 bucket name (Nome bucket S3), indicare il nome del bucket S3.
6. Per filtrare le route esportate, specificare i parametri di filtro nella sezione Filters (Filtri) della pagina.
7. Selezionare Export routes (Esporta route).

Per accedere ai percorsi esportati, apri la console Amazon S3 https://console.aws.amazon.com/s3/all'indirizzo e accedi al bucket specificato. Il nome del file include l' Account AWS ID, la AWS regione, l'ID della tabella di percorso e un timestamp. Selezionare il file e scegliere Download (Scarica). Di seguito è riportato un esempio di JSON file che contiene informazioni su due percorsi propagati per gli allegati. VPC

```
{
  "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"
    }
  ]
}
```

Eliminare una tabella di routing del gateway di transito utilizzando Amazon VPC Transit Gateways

Per eliminare una tabella di route del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento da eliminare.
4. Scegliere Operazioni,Eliminare la tabella di instradamento del gateway di transito.
5. Immettere **`delete`**, quindi scegliere Delete (Elimina) per confermare l'eliminazione

Per eliminare una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-route-table.

Crea un riferimento all'elenco di prefissi della tabella di routing utilizzando Amazon VPC Transit Gateways

È possibile fare riferimento a un elenco di prefissi nella tabella di instradamento del gateway di transito. Un elenco di prefissi è un insieme di una o più voci di CIDR blocco definite e gestite dall'utente. È possibile utilizzare un elenco di prefissi per semplificare la gestione degli indirizzi IP a cui si fa riferimento nelle risorse per instradare il traffico di rete. Ad esempio, se specificate spesso la stessa destinazione CIDRs in più tabelle di routing dei gateway di transito, potete gestirle CIDRs in un unico elenco di prefissi, anziché fare ripetutamente riferimento allo stesso CIDRs in ogni tabella di routing. Se è necessario rimuovere un CIDR blocco di destinazione, è possibile rimuovere la relativa voce dall'elenco dei prefissi anziché rimuovere la route da ogni tabella di route interessata.

Quando si crea un riferimento all'elenco di prefissi nella tabella di instradamento del gateway di transito, ogni voce dell'elenco dei prefissi viene rappresentata come route nella tabella route del gateway di transito.

Per ulteriori informazioni sugli elenchi di prefissi, consulta Elenchi di prefissi nella Amazon VPC User Guide.

Per creare un riferimento all'elenco di prefissi utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.
3. Seleziona la tabella di instradamento del gateway di transito.
4. Scegliere Operazioni, Crea riferimento all'elenco dei prefissi.
5. Per ID elenco prefissi, scegliere l'ID dell'elenco dei prefissi.
6. PerType (Tipo), scegliere se è consentito il traffico verso questo elenco di prefissi (Active (Attivo)) o abbandonato (Blackhole).
7. Per Transit gateway attachment ID (ID allegato gateway di transito), scegliere l'ID dell'allegato a cui indirizzare il traffico routing.
8. Scegliere Crea riferimento elenco di prefissi.

Per creare un riferimento a un elenco di prefissi utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-prefix-list-reference.

Modifica di un riferimento a un elenco di prefissi utilizzando Amazon VPC Transit Gateways

È possibile modificare un riferimento a un elenco di prefissi modificando l'allegato a cui viene instradato il traffico o indicando se eliminare il traffico corrispondente al percorso.

Non è possibile modificare le singole route per un elenco di prefissi nella scheda Route. Per modificare le voci nell'elenco dei prefissi, utilizzare la schermata Elenchi prefissi gestiti. Per ulteriori informazioni, consulta Modificare un elenco di prefissi nella Amazon VPC User Guide.

Per modificare un riferimento a un elenco di prefissi utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.
3. Seleziona la tabella di instradamento del gateway di transito.
4. Nel riquadro inferiore, scegliere Riferimenti elenco prefissi.
5. Scegliete il riferimento all'elenco dei prefissi e scegliete Modifica riferimenti.
6. PerType (Tipo), scegliere se è consentito il traffico verso questo elenco di prefissi (Active (Attivo)) o abbandonato (Blackhole).
7. Per Transit gateway attachment ID (ID allegato gateway di transito), scegliere l'ID dell'allegato a cui indirizzare il traffico routing.
8. Scegliere Modifica riferimento elenco prefissi.

Per modificare un riferimento a un elenco di prefissi utilizzando il AWS CLI

Utilizzate il comando modify-transit-gateway-prefix-list-reference.

Eliminare un riferimento a un elenco di prefissi utilizzando Amazon VPC Transit Gateways

Se non è più necessario un riferimento all'elenco di prefissi, è possibile eliminarlo dalla tabella di instradamento del gateway di transito. L'eliminazione del riferimento non comporta l'eliminazione dell'elenco dei prefissi.

Per eliminare un riferimento a un elenco di prefissi utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.
3. Seleziona la tabella di instradamento del gateway di transito.
4. Scegliere la referenza all'elenco dei prefissi, quindi selezionare Elimina riferimenti.
5. Scegliere Elimina riferimenti.

Per modificare un riferimento a un elenco di prefissi utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-prefix-list-reference.

Tabelle delle policy dei gateway di transito in Amazon VPC Transit Gateways

Il routing dinamico del gateway di transito utilizza tabelle di policy per indirizzare il traffico di rete per il AWS cloudWAN. La tabella contiene le regole di policy per la corrispondenza del traffico di rete in base agli attributi delle policy, quindi mappa il traffico che corrisponde alla regola in una tabella di instradamento di destinazione.

È possibile utilizzare il routing dinamico per i gateway di transito per lo scambio automatico di informazioni di instradamento e raggiungibilità con tipi di gateway di transito in peering. A differenza di un instradamento statico, il traffico può essere instradato lungo un percorso diverso in base alle condizioni della rete, come guasti del percorso o congestione. Il routing dinamico aggiunge anche un ulteriore livello di sicurezza in quanto è più facile reinstradare il traffico in caso di violazione o incursione nella rete.

> **Note**
>
> Le tabelle delle policy di Transit Gateway sono attualmente supportate in Cloud solo WAN quando si crea una connessione peering Transit Gateway. Quando crei una connessione peering, puoi associare quella tabella alla connessione. L'associazione quindi compila automaticamente la tabella con le regole delle policy.
> Per ulteriori informazioni sulle connessioni peering in CloudWAN, consulta la Guida per l'utente di Peerings in the AWS Cloud. WAN

Attività

- Crea una tabella di policy sui gateway di transito utilizzando Amazon VPC Transit Gateways
- Eliminare una tabella di policy del gateway di transito utilizzando Amazon VPC Transit Gateways

Crea una tabella di policy sui gateway di transito utilizzando Amazon VPC Transit Gateways

Per creare una tabella di policy del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit gateway policy table (Tabella di policy del gateway di transito).
3. Selezionare Create transit gateway policy table (Crea tabella di policy del gateway di transito).
4. (Facoltativo) Per Name tag (Tag nome), immettere un nome per la policy del gateway di transito. In questo modo viene creato un tag con valore corrispondente al nome specificato.
5. Per Transit gateway ID (ID gateway di transito), selezionare il gateway di transito per la tabella di policy.
6. Selezionare Create transit gateway policy table (Crea tabella di policy del gateway di transito).

Per creare una tabella di policy sui gateway di transito utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-policy-table.

Eliminare una tabella di policy del gateway di transito utilizzando Amazon VPC Transit Gateways

Eliminazione di una tabella di policy di un gateway di transito. Quando una tabella viene eliminata, tutte le regole di policy all'interno di tale tabella vengono eliminate.

Per eliminare una tabella di policy del gateway di transito utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit gateway policy tables (Tabelle di policy del gateway di transito).
3. Selezionare la tabella di policy del gateway di transito da eliminare.

4. Seleziona Actions (Operazioni), quindi Delete policy table (Elimina tabella della policy).
5. Confermare l'eliminazione della tabella.

Per eliminare una tabella di policy del gateway di transito utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-policy-table.

Multicast in Amazon VPC Transit Gateway

Multicast è un protocollo di comunicazione utilizzato per fornire un singolo flusso di dati a più computer riceventi contemporaneamente. Transit Gateway supporta il routing del traffico multicast tra sottoreti collegate VPCs e funge da router multicast per le istanze che inviano traffico destinato a più istanze di ricezione.

Argomenti

Concetti multicast

Di seguito sono elencati i concetti fondamentali relativi al multicast:

- Dominio multicast: consente la segmentazione di una rete multicast in domini diversi e fa sì che il gateway di transito agisca come router multicast multipli. È possibile definire l'appartenenza al dominio multicast a livello di sottorete.
- Gruppo multicast: identifica un insieme di host che invieranno e riceveranno lo stesso traffico multicast. Un gruppo multicast è identificato da un indirizzo IP del gruppo. L'appartenenza ai gruppi multicast è definita da singole interfacce di rete elastiche collegate alle istanze. EC2
- Internet Group Management Protocol (IGMP): un protocollo Internet che consente a host e router di gestire dinamicamente l'appartenenza a gruppi multicast. Un dominio IGMP multicast contiene host che utilizzano il IGMP protocollo per partecipare, lasciare e inviare messaggi. AWS supporta il IGMPv2 protocollo IGMP e entrambi i domini multicast di appartenenza al gruppo statici (APIbasati).

- Sorgente multicast: un'interfaccia di rete elastica associata a un'EC2istanza supportata configurata staticamente per inviare traffico multicast. Un'origine multicast si applica solo alle configurazioni di origine statica.

  Un dominio multicast di origine statica contiene host che non utilizzano il IGMP protocollo per partecipare, lasciare e inviare messaggi. Si utilizza AWS CLI per aggiungere una fonte e i membri del gruppo. L'origine aggiunta staticamente invia traffico multicast e i membri ricevono traffico multicast.
- Membro del gruppo multicast: un'interfaccia di rete elastica associata a un'EC2istanza supportata che riceve traffico multicast. Un gruppo multicast dispone di più membri del gruppo. In una configurazione di appartenenza a un gruppo di origine statica, i membri del gruppo multicast possono ricevere solo traffico. In una configurazione IGMP di gruppo, i membri possono inviare e ricevere traffico.

Considerazioni

- Per informazioni sulle regioni supportate, consulta AWS Transit Gateway FAQs.
- Per supportare il multicast è necessario creare un nuovo gateway di transito.
- L'appartenenza a gruppi multicast viene gestita utilizzando Amazon Virtual Private Cloud Console o AWS CLI, oIGMP.

- Una sottorete può trovarsi in un solo dominio multicast.
- Se utilizzi un'istanza diversa da Nitro, devi disabilitare la casella di controllo Source/Dest. Per informazioni sulla disabilitazione del controllo, consulta Changing the source or destination checking nella Amazon EC2 User Guide.
- Un'istanza non Nitro non può essere un mittente multicast.
- Il routing multicast non è supportato sugli AWS Direct Connect allegati di peering o sugli allegati Transit Gateway Connect. Site-to-Site VPN
- Un gateway di transito non supporta la frammentazione dei pacchetti multicast. I pacchetti multicast frammentati vengono eliminati. Per ulteriori informazioni, consulta Unità di trasmissione massima (MTU).
- All'avvio, un host ne invia più IGMP IGMP JOIN messaggi per entrare a far parte di un gruppo multicast (in genere da 2 a 3 tentativi). Nell'improbabile eventualità che tutte le IGMP JOIN i messaggi vengono persi, l'host non entrerà a far parte del gruppo multicast di Transit Gateway. In uno scenario del genere sarà necessario riattivare il IGMP JOIN messaggio dall'host utilizzando metodi specifici dell'applicazione.
- L'iscrizione al gruppo inizia con la ricezione di IGMPv2 JOIN messaggio inviato dal gateway di transito e termina con la ricezione del IGMPv2 LEAVE messaggio. Il gateway di transito tiene traccia degli host che sono entrati a far parte correttamente del gruppo. In qualità di router multicast cloud, Transit Gateway emette un IGMPv2 QUERY messaggio a tutti i membri ogni due minuti. Ogni membro invia un IGMPv2 JOIN messaggio in risposta, che è il modo in cui i membri rinnovano la propria iscrizione. Se un membro non risponde a tre query consecutive, il gateway di transito rimuove questa appartenenza da tutti i gruppi di cui si è entrati fa parte. Tuttavia, continua a inviare domande a questo membro per 12 ore prima di rimuoverlo definitivamente dalla sua to-be-queried lista. Un esplicito IGMPv2 LEAVE il messaggio rimuove immediatamente e definitivamente l'host da qualsiasi ulteriore elaborazione multicast.
- Il gateway di transito tiene traccia degli host che sono entrati a far parte correttamente del gruppo. In caso di interruzione del gateway di transito, il gateway di transito continua a inviare dati multicast all'host per sette minuti (420 secondi) dopo l'ultimo successo IGMP JOIN messaggio. Il gateway di transito continua a inviare richieste di iscrizione all'host per un massimo di 12 ore o fino a quando non riceve un IGMP LEAVE messaggio dall'host.
- Il gateway di transito invia pacchetti di query di appartenenza a tutti i IGMP membri in modo da poter tenere traccia dell'appartenenza ai gruppi multicast. L'IP di origine di questi pacchetti di IGMP query è 0.0.0.0/32, l'IP di destinazione è 224.0.0.1/32 e il protocollo è 2. La configurazione del gruppo di sicurezza sugli IGMP host (istanze) e qualsiasi ACLs configurazione sulle sottoreti host devono consentire questi messaggi di protocollo. IGMP

- Quando la sorgente e la destinazione multicast coincidonoVPC, non è possibile utilizzare i riferimenti ai gruppi di sicurezza per impostare il gruppo di sicurezza di destinazione in modo che accetti il traffico proveniente dal gruppo di sicurezza dell'origine.
- Per i gruppi e le sorgenti multicast statici, Amazon VPC Transit Gateways rimuove automaticamente i gruppi statici e le fonti ENIs che non esistono più. Questa operazione viene eseguita assumendo periodicamente il ruolo collegato al servizio Transit Gateway da descrivere ENIs nell'account.
- Supporta solo il multicast statico. IPv6 Il multicast dinamico non lo fa.

Routing multicast

Quando si abilita il multicast in un gateway di transito, esso funge da router multicast. Quando a un dominio multicast viene aggiunta una sottorete, tutto il traffico multicast viene inviato al gateway di transito che è associato a quel dominio multicast.

Rete ACLs

ACLLe regole di rete funzionano a livello di sottorete. Si applicano al traffico multicast, poiché i gateway di transito risiedono all'esterno della sottorete. Per ulteriori informazioni, consulta Network ACLs nella Amazon VPC User Guide.

Per il traffico multicast di Internet Group Management Protocol (IGMP), le seguenti sono le regole minime in entrata. L'host remoto è l'host che invia il traffico multicast.

Tipo	Protocollo	Crea	Descrizione
Protocollo personalizzato	IGMP(2)	0.0.0.0/32	Query IGMP
UDPProtocollo personalizzato	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

Di seguito sono riportate le regole minime in uscita perIGMP.

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	IGMP(2)	224.0.0.2/32	IGMPlasciare
Protocollo personalizzato	IGMP(2)	Indirizzo IP del gruppo multicast	IGMPaderire
UDPProtocollo personalizzato	UDP	Indirizzo IP del gruppo multicast	Traffico multicast in uscita

Gruppi di sicurezza

Le regole dei gruppi di sicurezza operano a livello di istanza. Possono essere applicati sia al traffico multicast in entrata che in uscita. Il comportamento è lo stesso del traffico unicast. Per tutte le istanze dei membri del gruppo, è necessario consentire il traffico in ingresso dall'origine del gruppo. Per ulteriori informazioni, consulta Security groups nella Amazon VPC User Guide.

Per il traffico IGMP multicast, devi avere almeno le seguenti regole in entrata. L'host remoto è l'host che invia il traffico multicast. Non è possibile specificare un gruppo di sicurezza come origine della regola UDP in entrata.

Tipo	Protocollo	Crea	Descrizione
Protocollo personalizzato	2	0.0.0.0/32	Query IGMP
Protocollo personalizzato UDP	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

Per il traffico IGMP multicast, è necessario disporre almeno delle seguenti regole in uscita.

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	2	224.0.0.2/32	IGMPpartire

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	2	Indirizzo IP del gruppo multicast	IGMPaderire
UDPProtocollo personalizzato	UDP	Indirizzo IP del gruppo multicast	Traffico multicast in uscita

Domini multicast in Amazon VPC Transit Gateways

Un dominio multicast consente la segmentazione di una rete multicast in diversi domini. Per iniziare a utilizzare il multicast con un gateway di transito, crea un dominio multicast e associa quindi le sottoreti al dominio.

Attributi di dominio multicast

Nella tabella seguente vengono descritti in dettaglio gli attributi del dominio multicast. Non è possibile abilitare entrambi gli attributi contemporaneamente.

Attributo	Descrizione
`Igmpv2Support` (AWS CLI) IGMPv2supporto (console)	Questo attributo determina il modo in cui i membri del gruppo si uniscono o abbandonano un gruppo multicast. Quando questo attributo è disattivato, è necessario aggiungere manualmente i membri del gruppo al dominio. Abilita questo attributo se almeno un membro utilizza il IGMP protocollo. I membri si uniscono al gruppo multicast in uno dei seguenti modi: • I membri che supportano IGMP utilizzano i `LEAVE` messaggi `JOIN` and. • I membri che non supportano il supporto IGMP devono essere aggiunti o rimossi dal gruppo utilizzando la VPC console Amazon o il AWS CLI.

Attributo	Descrizione
	Se registri membri del gruppo multicast, è necessario anche annullarne la registrazione. Il gateway di transito ignora un IGMP `LEAVE` messaggio inviato da un membro del gruppo aggiunto manualmente.
`StaticSourcesSupport` (AWS CLI) Supporto per origini statiche (console)	Questo attributo determina se esistono origini multicast statiche per il gruppo. Quando questo attributo è abilitato, è necessario aggiunger e fonti per un dominio multicast utilizzando register-transit-gateway-multicast -group-sources. Solo le origini multicast possono inviare traffico multicast. Quando questo attributo è impostato su disabilitato, non esistono origini multicast designate. Tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono traffico multicast.

Crea un dominio IGMP multicast utilizzando Amazon VPC Transit Gateways

Se non lo hai già fatto, esamina gli attributi del dominio multicast disponibili. Per ulteriori informazioni, consulta the section called “Domini multicast”.

Per creare un dominio IGMP multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Scegliere Crea dominio multicast gateway di transito.
4. Per Name tag (Tag nome) immettere un nome per il dominio.
5. Per ID gateway di transito, seleziona il gateway di transito che elabora il traffico multicast.
6. Per ricevere IGMPv2assistenza, seleziona la casella di controllo.
7. Per il supporto delle fonti statiche, deseleziona la casella di controllo.

8. Per accettare automaticamente le associazioni di sottoreti tra account per questo dominio multicast, seleziona Accetta automaticamente associazioni condivise.
9. Scegliere Crea dominio multicast gateway di transito.

Per creare un dominio IGMP multicast utilizzando AWS CLI

Utilizzate il comando create-transit-gateway-multicast-domain.

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

Crea un dominio multicast di origine statica utilizzando Amazon VPC Transit Gateways

Se non lo hai già fatto, esamina gli attributi del dominio multicast disponibili. Per ulteriori informazioni, consulta the section called “Domini multicast”.

Per creare un dominio multicast statico utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Scegliere Crea dominio multicast gateway di transito.
4. (Facoltativo) Per Tag nome, specifica un nome per identificare il dominio.
5. Per ID gateway di transito, seleziona il gateway di transito che elabora il traffico multicast.
6. Per ricevere IGMPv2assistenza, deseleziona la casella di controllo.
7. Per il supporto delle fonti statiche, seleziona la casella di controllo.
8. Per accettare automaticamente le associazioni di sottoreti tra account per questo dominio multicast, seleziona Accetta automaticamente associazioni condivise.
9. Scegliere Crea dominio multicast gateway di transito.

Per creare un dominio multicast statico utilizzando AWS CLI

Utilizzate il comando create-transit-gateway-multicast-domain.

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

Associazione di VPC allegati e sottoreti a un dominio multicast utilizzando Amazon Transit Gateways VPC

Utilizzare la procedura seguente per associare un VPC allegato a un dominio multicast. Quando si crea un'associazione, è possibile selezionare le sottoreti da includere nel dominio multicast.

Prima di iniziare, è necessario creare un VPC allegato sul gateway di transito. Per ulteriori informazioni, consulta Allegati Amazon VPC nei gateway di transito Amazon VPC.

Per associare VPC gli allegati a un dominio multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Crea associazione.
4. Per Scegli l'allegato da associare, selezionare l'allegato del gateway di transito.
5. In Scegli sottoreti da associare, seleziona le sottoreti da includere nel dominio.
6. Selezionare Create association (Crea associazione).

Per associare VPC gli allegati a un dominio multicast utilizzando il AWS CLI

Utilizzate il comando associate-transit-gateway-multicast-domain.

Dissociare una sottorete da un dominio multicast utilizzando Amazon Transit Gateways VPC

Utilizza la procedura riportata di seguito per dissociare le sottoreti da un dominio multicast.

Per disassociare le sottoreti utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Associations (Associazioni).
5. Selezionare la sottorete, quindi scegli Operazioni,Elimina associazione.

Per dissociare le sottoreti utilizzando il AWS CLI

Utilizzate il comando -domaindisassociate-transit-gateway-multicast.

Visualizza le associazioni di domini multicast utilizzando Amazon VPC Transit Gateways

Visualizza i tuoi domini multicast per verificare che siano disponibili e che contengano le sottoreti e gli allegati appropriati.

Per visualizzare un dominio multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Associations (Associazioni).

Per visualizzare un dominio multicast utilizzando il AWS CLI

Utilizzate il comando describe-transit-gateway-multicast-domains.

Aggiungi tag a un dominio multicast utilizzando Amazon VPC Transit Gateways

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. Puoi aggiungere più tag a ciascun dominio multicast. Le chiavi di tag devono essere univoche per ogni dominio multicast. Se aggiungi un tag con una chiave già associata al dominio multicast, il valore del tag viene aggiornato. Per ulteriori informazioni, consulta Tagging your Amazon EC2 Resources.

Per aggiungere tag a un dominio multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).

5. (Facoltativo) Per ogni tag, seleziona Aggiungi nuovo tag e immetti una chiave e un valore per il tag.
6. Seleziona Salva.

Per aggiungere tag a un dominio multicast utilizzando il AWS CLI

Utilizzare il comando crea tag.

Eliminare un dominio multicast utilizzando Amazon VPC Transit Gateways

Utilizza la procedura riportata di seguito per eliminare un dominio multicast.

Per eliminare un dominio multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Elimina dominio multicast.
4. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un dominio multicast utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-multicast-domain.

Domini multicast condivisi in Amazon VPC Transit Gateways

Con la condivisione di domini multicast, i proprietari di domini multicast possono condividere il dominio con altri account AWS all'interno della propria organizzazione in AWS Organizations. In qualità di proprietario del dominio multicast, puoi creare e gestire il dominio multicast a livello centrale. Una volta condivise, tali utenti possono eseguire le seguenti operazioni su un dominio multicast condiviso:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo nel dominio multicast
- Associare una sottorete al dominio multicast e dissociare le sottoreti dal dominio multicast

Un proprietario di dominio multicast può condividere un dominio multicast con:

- AWS account all'interno della propria organizzazione o tra organizzazioni in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations
- AWS conti esterni a AWS Organizations.

  Per condividere un dominio multicast con un AWS account esterno all'organizzazione, è necessario creare una condivisione di risorse utilizzando AWS Resource Access Manager e quindi scegliere Consenti la condivisione con chiunque quando selezioni i Principali con cui condividere il dominio multicast. Per ulteriori informazioni sulla creazione di una condivisione di risorse, consulta Creazione di una condivisione di risorse AWS RAM nella Guida per l'utente di AWS RAM .

Indice

Prerequisiti per la condivisione di un dominio multicast

- Per condividere un dominio multicast, devi possederlo nel tuo account. AWS Non puoi condividere un dominio multicast che è stato condiviso.
- Per condividere un dominio multicast con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con. AWS Organizations Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Servizi correlati

La condivisione di domini multicast si integra con AWS Resource Access Manager ().AWS RAM AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite. AWS Organizations Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione di risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione. AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Autorizzazioni del dominio multicast condiviso

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione del dominio multicast e dei membri e degli allegati che registrano o associano al dominio. I proprietari possono modificare o revocare l'accesso condiviso in qualsiasi momento. Possono utilizzare AWS Organizations per visualizzare, modificare ed eliminare le risorse create dai consumatori su domini multicast condivisi.

Autorizzazioni per gli utenti

Gli utenti del dominio multicast condiviso possono eseguire le seguenti operazioni sui domini multicast condivisi nello stesso modo in cui lo farebbero sui domini multicast da loro creati:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo nel dominio multicast
- Associare una sottorete al dominio multicast e dissociare le sottoreti dal dominio multicast

I consumer sono responsabili della gestione delle risorse create nel dominio multicast condiviso.

I clienti non possono visualizzare o modificare le risorse di proprietà di altri consumer o del proprietario del dominio multicast e non possono modificare i domini multicast con loro condivisi.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di domini multicast per il proprietario o per i consumer.

Quote

Un dominio multicast condiviso viene conteggiato ai fini delle quote di dominio multicast del proprietario e dell'utente condiviso.

Condividi le risorse tra le zone di disponibilità in Amazon VPC Transit Gateways

Per garantire che le risorse siano distribuite tra le zone di disponibilità di una regione, Amazon VPC Transit Gateways mappa in modo indipendente le zone di disponibilità ai nomi di ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione del dominio multicast relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità (ID AZ). L'ID AZ è un identificatore univoco e coerente per una zona di disponibilità per tutti gli AWS account. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione ed è la stessa posizione in ogni AWS account.

Per visualizzare la AZ IDs per le zone di disponibilità nel tuo account

1. Apri la AWS RAM console in https://console.aws.amazon.com/ram.
2. Le AZ IDs per la regione corrente vengono visualizzate nel pannello Your AZ ID sul lato destro dello schermo.

Condividi un dominio multicast utilizzando Amazon VPC Transit Gateways

Quando un proprietario condivide un dominio multicast con te, puoi fare quanto segue:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo
- Associare e dissociare sottoreti

> **Note**
>
> Per condividere un dominio multicast, dovrai aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra AWS account. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi un dominio multicast utilizzando il Amazon Virtual Private Cloud Console, lo aggiungi a una condivisione di risorse esistente.

Per aggiungere il dominio multicast a una nuova condivisione di risorse, dovrai innanzitutto creare la condivisione di risorse tramite la console AWS RAM.
Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al dominio multicast condiviso. In caso contrario, i consumer ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso al dominio multicast condiviso.

Puoi condividere un dominio multicast di tua proprietà utilizzando la Amazon Virtual Private Cloud console, la AWS RAM console o il. AWS CLI

Per condividere un dominio multicast di tua proprietà utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast, quindi scegli Operazioni, Condividi dominio multicast.
4. Seleziona la condivisione di risorse e scegli Condividi dominio multicast.

Per condividere un dominio multicast di tua proprietà utilizzando la console AWS RAM

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere un dominio multicast di tua proprietà utilizzando AWS CLI

Utilizza il comando create-resource-share.

Annulla la condivisione di un dominio multicast condiviso utilizzando Amazon VPC Transit Gateways

Quando un dominio multicast condiviso non viene più condiviso, per le risorse del dominio multicast del consumer si verifica quanto segue:

- Le sottoreti del consumer vengono dissociate dal dominio multicast. Le sottoreti rimangono nell'account del consumer.
- Le origini dei gruppi di consumer e i membri del gruppo vengono dissociati dal dominio multicast e quindi eliminati dall'account del consumer.

Per annullare la condivisione di un dominio multicast, devi rimuoverlo dalla condivisione di risorse. È possibile eseguire questa operazione dalla AWS RAM console o dal AWS CLI.

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà, devi rimuoverlo dalla condivisione di risorse. È possibile eseguire questa operazione utilizzando la Amazon Virtual Private Cloud, AWS RAM console o la AWS CLI.

Per annullare la condivisione di un dominio multicast condiviso di proprietà utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast, quindi scegli Operazioni, Interrompi condivisione.

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà utilizzando AWS CLI

Utilizza il comando disassociate-resource-share.

Identifica un dominio multicast condiviso utilizzando Amazon VPC Transit Gateways

I proprietari e i consumatori possono identificare i domini multicast condivisi utilizzando e Amazon Virtual Private Cloud AWS CLI

Per identificare un dominio multicast condiviso utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast.
4. Nella pagina Dettagli del dominio multicast di transito, visualizza l'ID del proprietario per identificare l'ID dell' AWS account del dominio multicast.

Per identificare un dominio multicast condiviso utilizzando AWS CLI

Utilizzate il comando describe-transit-gateway-multicast-domains. Il comando restituisce i domini multicast di tua proprietà e i domini multicast che sono condivisi con te. `OwnerId`mostra l'ID dell' AWS account del proprietario del dominio multicast.

Registra le fonti con un gruppo multicast utilizzando Amazon VPC Transit Gateways

> **Note**
>
> Questa procedura è necessaria solo se l'attributo Supporto origini statiche è stato impostato su enable.

Utilizzare la procedura seguente per registrare le origini con un gruppo multicast. L'origine è l'interfaccia di rete che invia il traffico multicast.

Prima di aggiungere un'origine, sono necessarie le seguenti informazioni:

- L'ID del dominio multicast
- Le IDs interfacce di rete dei sorgenti
- L'indirizzo IP del gruppo multicast

Per registrare le origini utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Aggiungi origini gruppo.
4. Per l'indirizzo IP del gruppo, inserisci il IPv4 CIDR blocco o il IPv6 CIDR blocco da assegnare al dominio multicast.
5. In Choose network interfaces (Scegli interfacce di rete), selezionare le interfacce di rete dei mittenti multicast.
6. Scegliere Add sources (Aggiungi origini).

Per registrare le fonti utilizzando il AWS CLI

Utilizzate il comando register-transit-gateway-multicast-group-sources.

Registrare membri in un gruppo multicast utilizzando Amazon VPC Transit Gateways

Utilizzare la procedura seguente per registrare i membri del gruppo con un gruppo multicast.

Prima di aggiungere membri, sono necessarie le seguenti informazioni:

- L'ID del dominio multicast
- Le IDs interfacce di rete dei membri del gruppo
- L'indirizzo IP del gruppo multicast

Per registrare i membri utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Aggiungi membri del gruppo.
4. Per l'indirizzo IP del gruppo, inserisci il IPv4 CIDR blocco o il IPv6 CIDR blocco da assegnare al dominio multicast.
5. In Choose network interfaces (Scegli interfacce di rete), selezionare le interfacce di rete dei ricevitori multicast.
6. Scegliere Add members (Aggiungi membri).

Per registrare i membri utilizzando il AWS CLI

Utilizzare il comando register-transit-gateway-multicast-group-members.

Annulla la registrazione delle sorgenti da un gruppo multicast utilizzando Amazon Transit Gateways VPC

Non è necessario seguire questa procedura a meno che non sia stata aggiunta manualmente un'origine al gruppo multicast.

Per rimuovere un'origine utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).
5. Selezionare le origini, quindi scegliere Remove source (Rimuovi origine).

Per rimuovere una fonte utilizzando il AWS CLI

Utilizzate il comando deregister-transit-gateway-multicast-group-sources.

Annullare la registrazione dei membri di un gruppo multicast utilizzando Amazon Transit Gateways VPC

Non è necessario seguire questa procedura a meno che non sia stato aggiunto manualmente un membro al gruppo multicast.

Per annullare la registrazione dei membri utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).
5. Selezionare i membri, quindi scegliere Remove member (Rimuovi membro).

Per annullare la registrazione dei membri utilizzando il AWS CLI

Utilizzare il comando deregister-transit-gateway-multicast-group-members.

Visualizza gruppi multicast utilizzando Amazon VPC Transit Gateways

È possibile visualizzare le informazioni sui gruppi multicast per verificare che i membri siano stati scoperti utilizzando il IGMPv2 protocollo. Il tipo di membro (nella console) o `MemberType` (in AWS CLI) viene visualizzato IGMP quando vengono AWS rilevati i membri con il protocollo.

Per visualizzare gruppi multicast utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).

Per visualizzare i gruppi multicast utilizzando il AWS CLI

Utilizzate il comando search-transit-gateway-multicast-groups.

L'esempio seguente mostra che il IGMP protocollo ha rilevato i membri del gruppo multicast.

```
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"
        }
    ]
}
```

Configurazione del multicast per Windows Server in Amazon VPC Transit Gateways

Sarà necessario eseguire passaggi aggiuntivi per configurare il multicast (trasmissione uno a molti) per funzionare con i gateway di transito su Windows Server 2019 o 2022. Per configurarlo dovrai usare PowerShell ed eseguire i seguenti comandi:

Per configurare il multicast per Windows Server utilizzando PowerShell

1. Modificare Windows Server per utilizzarlo IGMPv2 anziché IGMPv3 per lo stack TCP /IP:

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

> **Note**
>
> `New-ItemProperty`è un indice di proprietà che specifica la versione. IGMP Poiché IGMP v2 è la versione supportata per il multicast, la proprietà `Value` deve essere. `3` Invece di modificare il registro di Windows, è possibile eseguire il comando seguente per impostare la IGMP versione su 2. :
> `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Windows Firewall interrompe la maggior parte UDP del traffico per impostazione predefinita. Per prima cosa devi verificare quale profilo di connessione viene utilizzato per il multicast (trasmissione uno a molti):

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

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

3. Aggiorna il profilo di connessione dal passaggio precedente per consentire l'accesso alle UDP porte richieste:

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

4. Riavvia l'istanza EC2.
5. Esegui il test della tua applicazione multicast (trasmissione uno a molti) per assicurarti che il traffico scorra come previsto.

Esempio: gestione IGMP delle configurazioni utilizzando Amazon VPC Transit Gateways

Questo esempio mostra almeno un host che utilizza il IGMP protocollo per il traffico multicast. AWS crea automaticamente il gruppo multicast quando riceve un IGMP `JOIN` messaggio da un'istanza, quindi aggiunge l'istanza come membro di questo gruppo. È inoltre possibile aggiungere staticamente persone non IGMP ospitanti come membri a un gruppo utilizzando. AWS CLI Tutte le istanze presenti

nelle sottoreti associate al dominio multicast possono inviare traffico e i membri del gruppo ricevono il traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
2. Creare una sottorete in VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Crea un VPC allegato. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
5. Crea un dominio multicast configurato per il IGMP supporto. Per ulteriori informazioni, consulta the section called “Crea un dominio multicast IGMP”.

   Utilizzare le seguenti impostazioni:

   - Abilita il IGMPv2supporto.
   - Disabilita Supporto per origini statiche.
6. Crea un'associazione tra le sottoreti nell'VPCallegato del gateway di transito e il dominio multicast. Per ulteriori informazioni, consulta the section called “Associazione VPC di allegati e sottoreti a un dominio multicast”.
7. La IGMP versione predefinita per è. EC2 IGMPv3 È necessario modificare la versione per tutti i membri IGMP del gruppo. È anche possibile emettere il seguente comando:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Aggiungi i membri che non utilizzano il IGMP protocollo al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Esempio: gestione di configurazioni di sorgenti statiche utilizzando Amazon VPC Transit Gateways

Questo esempio aggiunge staticamente sorgenti multicast a un gruppo. Gli host non utilizzano il IGMP protocollo per unirsi o abbandonare i gruppi multicast. Dovrai aggiungere staticamente i membri del gruppo che ricevono il traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
2. Creare una sottorete in VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Crea un VPC allegato. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
5. Crea un dominio multicast configurato per l'assenza di IGMP supporto e il supporto per l'aggiunta statica di fonti. Per ulteriori informazioni, consulta the section called “Crea un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disabilita IGMPv2 il supporto.
   - Per aggiungere manualmente le origini, imposta Supporto origini statiche.

     Le origini sono le uniche risorse che possono inviare traffico multicast quando l'attributo è impostato su abilitato. In caso contrario, tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono il traffico multicast.
6. Crea un'associazione tra le sottoreti nell'VPCallegato del gateway di transito e il dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione VPC di allegati e sottoreti a un dominio multicast”.
7. Se imposti l'attributo Supporto origini statiche, aggiungi l'origine al gruppo multicast. Per ulteriori informazioni, consultare the section called “Registrare le origini con un gruppo multicast”.

8. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Esempio: gestione delle configurazioni statiche dei membri del gruppo in Amazon VPC Transit Gateways

Questo esempio mostra l'aggiunta statica di membri multicast a un gruppo. Gli host non possono utilizzare il IGMP protocollo per unirsi o abbandonare gruppi multicast. Tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Create a VPC in the Amazon VPC User Guide.
2. Creare una sottorete in VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Crea un VPC allegato. Per ulteriori informazioni, consulta the section called “Crea un allegato VPC”.
5. Crea un dominio multicast configurato per l'assenza di IGMP supporto e il supporto per l'aggiunta statica di fonti. Per ulteriori informazioni, consulta the section called “Crea un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disattiva IGMPv2 il supporto.
   - Disabilita Supporto per origini statiche.
6. Crea un'associazione tra le sottoreti nell'VPCallegato del gateway di transito e il dominio multicast. Per ulteriori informazioni, consulta the section called “Associazione VPC di allegati e sottoreti a un dominio multicast”.
7. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Registri di flusso dei gateway di transito Amazon VPC

Transit Gateway Flow Logs è una funzionalità di Amazon VPC Transit Gateways che consente di acquisire informazioni sul traffico IP in entrata e in uscita dai gateway di transito. I dati dei log di flusso possono essere pubblicati su Amazon CloudWatch Logs, Amazon S3 o Firehose. Dopo aver creato un log di flusso, puoi recuperare e visualizzarne i dati nella destinazione scelta. I dati di log del flusso vengono raccolti al di fuori del percorso del traffico di rete e pertanto non influiscono sulla velocità effettiva o sulla latenza della rete. È possibile creare o eliminare i log di flusso senza alcun rischio di impatto sulle prestazioni della rete. I registri di flusso del gateway di transito acquisiscono informazioni relative solo ai gateway di transito, descritti in the section called “Log di flusso del gateway di transito”. Se desideri acquisire informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete del tuo computer VPCs, utilizza VPC Flow Logs. Per ulteriori informazioni consulta Logging IP traffic using VPC Flow Logs (Registrazione del traffico IP utilizzando i registri di flusso VPC) nella Guida per l'utente di Amazon VPC.

> **Note**
>
> Per creare un log di flusso del gateway di transito, devi essere il proprietario del gateway di transito. Se non sei il proprietario, il proprietario del gateway di transito deve darti l'autorizzazione.

I dati del log di flusso per un gateway di transito monitorato vengono registrati come record del log di flusso, ossia eventi di log costituiti da campi che descrivono il flusso di traffico. Per ulteriori informazioni, consulta Log di flusso del gateway di transito.

Per creare un log di flusso, occorre specificare:

- La risorsa per cui creare il log di flusso
- Le destinazioni in cui pubblicare i dati del log di flusso

Dopo aver creato un flusso di log, potrebbero essere necessari diversi minuti prima di iniziare a raccogliere dati e pubblicarli nelle destinazioni scelte. I registri di flusso non acquisiscono flussi di log in tempo reale per i gateway di transito.

È possibile applicare tag ai log di flusso. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag consentono di organizzare i log di flusso, ad esempio per scopo o proprietario.

Se un log di flusso non è più necessario, puoi eliminarlo. L'eliminazione di un log di flusso disattiva il servizio di log di flusso per la risorsa e nessun nuovo record del log di flusso viene creato o pubblicato su CloudWatch Logs o Amazon S3. L'eliminazione del log di flusso non elimina alcun record o flusso di log di flusso esistente (per CloudWatch Logs) o oggetti di file di log (per Amazon S3) per un gateway di transito. Per eliminare un flusso di log esistente, usa la console Logs. CloudWatch Per eliminare oggetti file di log esistenti, utilizza la console Amazon S3. Dopo aver eliminato un log di flusso, potrebbero essere necessari diversi minuti per interrompere la raccolta dati. Per ulteriori informazioni, consulta Eliminazione di un record di Amazon VPC Transit Gateways Flow Logs.

Puoi creare log di flusso per i tuoi gateway di transito in grado di pubblicare dati su CloudWatch Logs, Amazon S3 o Amazon Data Firehose. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Crea un log di flusso da pubblicare su Logs CloudWatch
- Creazione di un log di flusso che pubblica in Amazon S3
- Creare un log di flusso da pubblicare su Firehose

Limitazioni

Le seguenti limitazioni si applicano ai Transit Gateway Flow Logs:

- Il traffico multicast non è supportato.
- Gli allegati Connect non sono supportati. Tutti i log di flusso di Connect vengono visualizzati sotto l'allegato di trasporto e devono pertanto essere abilitati sul gateway di transito o sull'allegato di trasporto Connect.

Log di flusso del gateway di transito

Un record del log di flusso rappresenta un flusso di rete nel gateway di transito. Ogni record è una stringa con campi separati da spazi. Un record include valori per i vari componenti del flusso di traffico tra cui, ad esempio, origine, destinazione e protocollo.

Quando crei un log di flusso, puoi utilizzare il formato predefinito oppure specificare un formato personalizzato.

Indice

Formato predefinito

Con il formato predefinito, i record del log di flusso includono tutti i campi dalla versione 2 alla versione 6, nell'ordine mostrato nella tabella dei campi disponibili. Non è possibile personalizzare o modificare il formato predefinito. Per acquisire i campi aggiuntivi o un diverso sottoinsieme di campi, specifica un formato personalizzato.

Formato personalizzato

Con un formato personalizzato, è possibile specificare quali campi sono inclusi nei record del log di flusso e il relativo ordine. Ciò permette di creare registri di flusso specifici per le proprie esigenze e omettere i campi non pertinenti. L'uso di un formato personalizzato può anche ridurre la necessità di processi separati per estrarre informazioni specifiche dai log di flusso pubblicati. Puoi specificare un numero qualsiasi di campi del log di flusso disponibili, ma devi specificarne almeno uno.

Campi disponibili

Nella tabella seguente sono descritti tutti i campi disponibili per un record del log di flusso di un gateway di transito. La colonna Version (Versione) indica la versione in cui è stato introdotto il campo.

Quando si pubblicano i dati del flusso di log su Amazon S3, il tipo di dati per i campi dipende dal formato del flusso di log. Se il formato è testo semplice, tutti i campi sono di tipo STRING. Se il formato è Parquet, consulta la tabella per i tipi di dati dei campi.

Se un campo non è applicabile o non può essere calcolato per un record specifico, il record visualizza un simbolo "-" per tale voce. I campi dei metadati che non provengono direttamente dall'intestazione del pacchetto sono approssimazioni ottimali e i loro valori potrebbero essere mancanti o imprecisi.

Campo	Descrizione	Versione
version	Indica la versione in cui è stato introdotto il campo. Il formato predefinito include tutti i campi della versione 2 nello stesso ordine in cui sono riportati nella tabella. Tipo di dati Parquet: INT_32	2
resource-type	Il tipo di risorsa su cui viene creata la sottoscrizione. Per i Transit Gateway Flow Logs, questo sarà TransitGateway. Tipo di dati Parquet: STRING	6
account-id	L' Account AWS ID del proprietario del gateway di transito di origine. Tipo di dati Parquet: STRING	2
tgw-id	L'ID del gateway di transito per il quale viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-attachment-id	L'ID del collegamento del gateway di transito alla VPN per il quale viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-src-vpc-account-id	L' Account AWS ID per il traffico VPC di origine. Tipo di dati Parquet: STRING	6
tgw-dst-vpc-account-id	L' Account AWS ID per il traffico VPC di destinazione. Tipo di dati Parquet: STRING	6
tgw-src-vpc-id	L'ID del VPC di origine per il gateway di transito Tipo di dati Parquet: STRING	6
tgw-dst-vpc-id	L'ID del VPC di destinazione per il gateway di transito. Tipo di dati Parquet: STRING	6

Campo	Descrizione	Versione
tgw-src-subnet-id	L'ID della sottorete per il traffico di origine del gateway di transito. Tipo di dati Parquet: STRING	6
tgw-dst-subnet-id	L'ID della sottorete per il traffico di destinazione del gateway di transito. Tipo di dati Parquet: STRING	6
tgw-src-eni	L'ID dell'ENI del collegamento del gateway di transito alla VPN di origine per il flusso. Tipo di dati Parquet: STRING	6
tgw-dst-eni	L'ID dell'ENI del collegamento del gateway di transito alla VPN di destinazione per il flusso. Tipo di dati Parquet: STRING	6
tgw-src-az-id	L'ID della zona di disponibilità che contiene il gateway di transito di origine per cui viene registrato il traffico. Se il traffico proviene da una posizione secondaria, il record visualizza un simbolo '-' per questo campo. Tipo di dati Parquet: STRING	6
tgw-dst-az-id	L'ID della zona di disponibilità che contiene il gateway di transito di destinazione per cui viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-pair-attachment-id	A seconda della direzione del flusso, questo è l'ID allegato in uscita o in ingresso del flusso. Tipo di dati Parquet: STRING	6
srcaddr	L'indirizzo di origine per traffico in entrata. Tipo di dati Parquet: STRING	2

Campo	Descrizione	Versione
dstaddr	L'indirizzo di destinazione per il traffico in uscita. Tipo di dati Parquet: STRING	2
srcport	La porta di origine del traffico. Tipo di dati parquet: INT_32	2
dstport	La porta di destinazione del traffico. Tipo di dati Parquet: INT_32	2
protocol	Il numero di protocollo IANA del traffico. Per ulteriori informazioni, consulta la sezione relativa ai numeri di protocollo Internet assegnati. Tipo di dati Parquet: INT_32	2
packets	Il numero di pacchetti trasferiti durante il flusso. Tipo di dati parquet: INT_64	2
bytes	Il numero di byte trasferiti durante il flusso. Tipo di dati Parquet: INT_64	2
start	L'ora, in secondi Unix, di ricezione del primo pacchetto del flusso all'interno dell'intervallo di aggregazione. Potrebbe durare fino a 60 secondi oltre l'avvenuta trasmissione o ricezione del pacchetto da parte del gateway di transito. Tipo di dati Parquet: INT_64	2
end	L'ora, in secondi Unix, in cui l'ultimo pacchetto del flusso è stato ricevuto entro l'intervallo di aggregazione. Potrebbe durare fino a 60 secondi oltre l'avvenuta trasmissione o ricezione del pacchetto da parte del gateway di transito. Tipo di dati Parquet: INT_64	2

Campo	Descrizione	Versione
log-status	Lo stato del log di flusso: • OK: i dati vengono registrati normalmente nelle destinazioni scelte. • NODATA: non vi è alcun traffico di rete da o per l'interfaccia di rete durante l'intervallo di aggregazione. • SKIPDATA: alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione. Ciò può essere causato da un vincolo di capacità interna o da un errore interno. Tipo di dati Parquet: STRING	2
type	Il tipo di traffico. I valori possibili sono IPv4 | IPv6 | EFA. Per ulteriori informazioni, consulta Elastic Fabric Adapter nella Amazon EC2 User Guide. Tipo di dati parquet: STRING	3
packets-lost-no-route	I pacchetti sono andati persi perché non è stata specificata alcuna route. Tipo di dati Parquet: INT_64	6
packets-lost-blackhole	I pacchetti sono andati persi a causa di un buco nero. Tipo di dati Parquet: INT_64	6
packets-lost-mtu-exceeded	I pacchetti sono andati persi a causa delle dimensioni che superano la MTU. Tipo di dati Parquet: INT_64	6
packets-lost-ttl-expired	I pacchetti persi a causa della scadenza di time-to-live. Tipo di dati Parquet: INT_64	6

Campo	Descrizione	Versione
tcp-flags	Il valore bitmask per i seguenti flag TCP: • FIN - 1 • SYN - 2 • RST - 4 • PSH - 8 • ACK - 16 • SYN-ACK - 18 • URG - 32 **Important** Quando una voce del log di flusso è composta solo da pacchetti ACK, il valore del flag è 0, non 16. Per informazioni generali sui flag TCP (come il significato di flag come FIN, SYN e ACK), consulta Struttura del segmento TCP su Wikipedia. I flag TCP sono introdotti da un operatore OR durante l'intervallo di aggregazione. Per le connessioni brevi, i flag possono essere impostati sulla stessa riga nel record del log di flusso, ad esempio 19 per SYN-ACK e FIN e 3 per SYN e FIN. Tipo di dati parquet: INT_32	3
region	La Regione che contiene il gateway di transito in cui viene registrato il traffico. Tipo di dati parquet: STRING	4

Campo	Descrizione	Versione
flow-direction	La direzione del flusso rispetto all'interfaccia in cui viene catturato il traffico. I valori possibili sono: ingress | egress. Tipo di dati parquet: STRING	5
pkt-src-aws-service	Il nome del sottoinsieme di intervalli di indirizzi IP per il campo srcaddr se l'indirizzo IP di origine è per un AWS servizio. I valori possibili sono: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Tipo di dati parquet: STRING	5
pkt-dst-aws-service	Il nome del sottoinsieme di intervalli di indirizzi IP per il campo dstaddr campo, se l'indirizzo IP di destinazione è per un AWS servizio. Per un elenco di possibili valori, consulta il campo pkt-src-aws-service . Tipo di dati parquet: STRING	5

Controllo dell'utilizzo dei log di flusso

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per utilizzare log di flusso. Puoi creare una policy dell'utente che concede agli utenti le autorizzazioni per creare, descrivere ed eliminare log di flusso. Per ulteriori informazioni, consulta Concessione delle autorizzazioni richieste agli utenti IAM per le EC2 risorse Amazon nell'Amazon EC2 API Reference.

Di seguito è riportata una policy di esempio che concede agli utenti autorizzazioni complete per creare, descrivere ed eliminare log di flusso.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

È necessaria una configurazione aggiuntiva dei ruoli e delle autorizzazioni IAM, a seconda che tu stia pubblicando su CloudWatch Logs o Amazon S3. Per ulteriori informazioni, consulta Transit Gateway Flow registra i record in Amazon CloudWatch Logs e Transit Gateway Flow Registra i record in Amazon S3 .

Prezzi dei log di flusso di Transit Gateway

Gli addebiti per l'importazione dei dati e l'archiviazione per i log distribuiti vengono applicati quando si pubblicano i log di flusso del gateway di transito. Per ulteriori informazioni sui prezzi per la pubblicazione dei log venduti, apri Amazon CloudWatch Pricing, quindi, in Livello a pagamento, seleziona Log e trova Vended Logs.

Creare o aggiornare un IAM ruolo per i log di flusso di Amazon VPC Transit Gateways

È possibile aggiornare un ruolo esistente o utilizzare la procedura seguente per creare un nuovo ruolo da utilizzare con i log di flusso utilizzando la AWS Identity and Access Management console.

Per creare un IAM ruolo per i log di flusso

1. Apri la IAM console all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione seleziona Ruoli, quindi Crea ruolo.
3. In Seleziona tipo di entità attendibile, scegli Servizio AWS . Per Caso d'uso, scegli EC2. Scegli Next (Successivo).

4. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next: Tags (Successivo: Tag) e aggiungi facoltativamente i tag. Scegli Next (Successivo).
5. Nella pagina Name, review, and create (Nomina, verifica e crea) immetti un nome per il ruolo e, facoltativamente, una descrizione. Scegliere Crea ruolo.
6. Scegli il nome del ruolo. Per Aggiungi autorizzazioni, scegli Crea politica in linea, quindi scegli la JSONscheda.
7. Copiare la prima policy da IAMruoli per la pubblicazione dei log di flusso in Logs CloudWatch e incollarla nella finestra. Scegliere Review policy (Esamina policy).
8. Immettere un nome per la policy e scegliere Create policy (Crea policy).
9. Selezionare il nome del ruolo. In Trust Relationships (Relazioni di trust), scegliere Edit Trust Relationship (Modifica relazione di trust). Nel documento di policy esistente, cambiare il servizio da `ec2.amazonaws.com` a `vpc-flow-logs.amazonaws.com`. Selezionare Update Trust Policy (Aggiorna policy di trust).
10. Nella pagina di riepilogo, prendi nota del ruolo che ti ARN interessa. Ne hai bisogno ARN quando crei il log di flusso.

Transit Gateway Flow registra i record in Amazon CloudWatch Logs

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Amazon CloudWatch.

Quando vengono pubblicati su CloudWatch Logs, i dati del log di flusso vengono pubblicati in un gruppo di log e ogni gateway di transito ha un flusso di log unico nel gruppo di log. I flussi di log contengono record del log di flusso. Puoi creare più log di flusso che pubblicano dati nello stesso gruppo di log. Se lo stesso gateway di transito è presente in uno o più registri di flusso nello stesso gruppo di flussi di log, esso dispone di un flusso di log combinato. Se è stato specificato che un log di flusso deve acquisire traffico rifiutato e l'altro log di flusso deve acquisire traffico accettato, il flusso di log combinato acquisisce tutto il traffico.

I costi di inserimento e archiviazione dei dati per i log venduti si applicano quando si pubblicano i log di flusso su Logs. CloudWatch Per ulteriori informazioni, consulta la pagina CloudWatch dei prezzi di Amazon.

In CloudWatch Logs, il campo timestamp corrisponde all'ora di inizio registrata nel record del log di flusso. Il ingestionTimecampo fornisce la data e l'ora in cui il record del log di flusso è stato ricevuto

da Logs. CloudWatch Questo timestamp è successivo all'ora di fine acquisita nel record del log di flusso.

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Logs nella Amazon CloudWatch CloudWatch Logs User Guide.

Indice

IAMruoli per la pubblicazione dei log di flusso in Logs CloudWatch

Il IAM ruolo associato al log di flusso deve disporre di autorizzazioni sufficienti per pubblicare i log di flusso nel gruppo di log specificato in Logs. CloudWatch Il IAM ruolo deve appartenere al tuo. Account AWS

La policy IAM collegata al ruolo IAM deve includere almeno le autorizzazioni seguenti.

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

Accertarti inoltre che il ruolo disponga di una relazione di trust che consenta al servizio log di flusso di assumere il ruolo.

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

Si consiglia di utilizzare il le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy di attendibilità precedente. L'account di origine è il proprietario del log di flusso e l'origine ARN è il log di flussoARN. Se non conosci l'ID del log di flusso, puoi sostituire quella parte ARN con un carattere jolly (*) e quindi aggiornare la policy dopo aver creato il log di flusso.

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

Autorizzazioni per l'invio di un ruolo da parte degli utenti IAM

Gli utenti devono anche disporre delle autorizzazioni per utilizzare l'operazione`iam:PassRole` per il ruolo IAM associato al log di flusso.

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

```
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Crea un record Transit Gateways Flow Logs da pubblicare su Amazon CloudWatch Logs

È possibile creare registri di flusso per i gateway di transito. Se esegui questa procedura come utente IAM, assicurati di disporre delle autorizzazioni per utilizzare l'operazione `iam:PassRole`. Per ulteriori informazioni, consulta Autorizzazioni per l'invio di un ruolo da parte degli utenti IAM.

Puoi creare un log di CloudWatch flusso Amazon utilizzando la VPC console Amazon o il AWS CLI.

Per creare un log di flusso del gateway di transito utilizzando la console

1. Accedi a AWS Management Console e apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
3. Scegli le caselle di controllo per uno o più gateway di transito e scegli Azioni, Crea log di flusso.
4. Per Destinazione, scegli Invia ai registri. CloudWatch
5. Per Gruppo di log di destinazione, scegli il nome di un gruppo di log di destinazione corrente.

   > **Note**
   >
   > Se il gruppo di log di destinazione non esiste ancora, l'inserimento di un nuovo nome in questo campo creerà un nuovo gruppo di log di destinazione.

6. Per il IAMruolo, specifica il nome del ruolo che dispone delle autorizzazioni per pubblicare i log nei registri. CloudWatch
7. Per Formato record di log, seleziona il formato per il record del log di flusso.

   - Per utilizzare il formato del record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per utilizzare un formato personalizzato, scegli Formato personalizzato, quindi seleziona i campi da Formato di log .

8. (Facoltativo) Seleziona Aggiungi tag per applicare i tag al log di flusso.
9. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso utilizzando la riga di comando

Utilizzare uno dei seguenti comandi.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce le informazioni sul gateway di transito. I log di flusso vengono consegnati a un gruppo di log in CloudWatch Logs chiamato`my-flow-logs`, nell'account 123456789101, utilizzando il ruolo. IAM `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
```

Visualizza i record dei log di Transit Gateway Flow in Amazon CloudWatch

Puoi visualizzare i record dei log di flusso utilizzando la console CloudWatch Logs o la console Amazon S3, a seconda del tipo di destinazione scelto. Dopo che il flusso di log è stato creato, potrebbero essere necessari alcuni minuti prima che sia visibile nella console.

Per visualizzare i record dei log di flusso pubblicati su Logs CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, scegliere Logs (Log) e selezionare il gruppo di log contenente il log di flusso. Viene mostrato un elenco di flussi di log per ogni gateway di transito.
3. Selezionare il flusso di log contenente l'ID del gateway di transito per il quale si desidera visualizzare i record del registro di flusso. Per ulteriori informazioni, consulta Log di flusso del gateway di transito.

Elaborazione dei record di Transit Gateway Flow Logs in Amazon CloudWatch Logs

È possibile utilizzare i record del log di flusso come con qualsiasi altro evento di registro raccolto da CloudWatch Logs. Per ulteriori informazioni sul monitoraggio dei dati di log e sui filtri delle metriche, consulta Creazione di metriche dagli eventi di registro utilizzando i filtri nella Amazon CloudWatch User Guide.

Esempio: crea un filtro CloudWatch metrico e un allarme per un log di flusso

In questo esempio, si dispone di un log di flusso per `tgw-123abc456bca`. Vuoi creare un allarme che ti avvisi se ci sono stati 10 o più tentativi rifiutati di connessione alla tua istanza tramite la TCP porta 22 (SSH) entro un periodo di 1 ora. Innanzitutto, crea un filtro parametri che corrisponde al modello di traffico per il quale creare l'allarme. Quindi, puoi creare un allarme per il filtro parametri.

Per creare un filtro metrico per il SSH traffico rifiutato e creare un allarme per il filtro

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione a sinistra, scegli Log, Gruppi di log.
3. Seleziona la casella di controllo per il gruppo di log, quindi scegli Azioni, Crea filtro metrico.
4. Per Filter Pattern (Modello di filtro), immettere quanto segue.

```
[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. Per Select Log Data to Test (Seleziona i dati di registro per il test), seleziona il flusso di log per il gateway di transito. (Facoltativo) Per visualizzare le righe di dati di log che corrispondono al modello di filtro, scegli Test Pattern (Modello di test). Al termine, scegli Next (Successivo).
6. Inserisci un nome per il filtro, uno spazio dei nomi dei parametri e il nome del parametro. Imposta il valore del parametro su **1**. Al termine, scegli Next (Successivo) e in seguito Create metric filter (Crea filtri parametri).
7. Nel pannello di navigazione, seleziona Alarms (Allarmi), All alarms (Tutti gli allarmi).

8. Scegli Crea allarme.
9. Scegli lo spazio dei nomi per il filtro parametri che hai creato.

   Per visualizzare il nuovo parametro nella console potrebbero essere necessari alcuni minuti.
10. Seleziona il nome del parametro creato e scegli Next (Successivo).
11. Configura l'allarme come segue, quindi scegli Next (Successivo):

    - Per Statistic (Statistica), scegliere Sum (Somma). Ciò ti garantisce di acquisire il numero totale di punti di dati per il periodo di tempo specificato.
    - Per Period (Periodo), scegli 1 Hour (1 ora).
    - Per Whenever (Ogni volta che) , scegli Greater/Equal (Maggiore di/Uguale a) e inserisci **10** come soglia.
    - In Additional configuration (Configurazione aggiuntiva), per Datapoints to alarm (Punti dati per allarme) lascia il valore predefinito **1**.
12. Per Notifica, seleziona un SNS argomento esistente o scegli Crea nuovo argomento per crearne uno nuovo. Scegli Next (Successivo).
13. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
14. Al termine della configurazione dell'allarme, scegli Create alarm (Crea allarme).

Transit Gateway Flow Registra i record in Amazon S3

I log di flusso possono pubblicare dati di log di flusso in Amazon S3.

Durante la pubblicazione in Amazon S3, i dati del log di flusso vengono pubblicati in un bucket Amazon S3 esistente specificato. I record del log di flusso per tutti i gateway di transito monitorati vengono pubblicati in una serie di oggetti file di log che sono archiviati nel bucket.

I costi di inserimento e archiviazione dei dati vengono applicati ai log venduti quando si pubblicano Amazon CloudWatch i log di flusso su Amazon S3. Per ulteriori informazioni sui CloudWatch prezzi dei log venduti, apri Amazon CloudWatch Pricing, scegli Logs, quindi trova Vending Logs.

Per creare un bucket Amazon S3 da utilizzare con i log di flusso, consulta Create a bucket nella Amazon S3 User Guide.

Per ulteriori informazioni sulla registrazione di più account, consulta Registrazione centrale nella libreria di soluzioni di AWS .

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Amazon S3 nella Amazon Logs User Guide CloudWatch .

Indice

File di log di flusso

VPCFlow Logs è una funzionalità che raccoglie i record dei log di flusso, li consolida in file di log e quindi li pubblica nel bucket Amazon S3 a intervalli di 5 minuti. Ogni file di log contiene record di log di flusso per il traffico IP registrato nei cinque minuti precedenti.

Le dimensioni file massime per un file di log sono di 75 MB. Se il file di log raggiunge le dimensioni massime previste entro il periodo di 5 minuti, il log di flusso smette di aggiungervi record. Pubblica il file di log nel bucket Amazon S3 e crea un nuovo file di log.

In Amazon S3, il campo Last modified (Ultima modifica) per il file di log di flusso indica la data e l'ora in cui il file è stato caricato nel bucket Amazon S3. Questa è successiva al timestamp nel nome del file e differisce per il tempo impiegato per caricare il file nel bucket Amazon S3.

Formato dei file di log

Per i file di log, puoi specificare uno dei seguenti formati. Ciascun file viene compresso in un singolo file Gzip.

- Text: Testo normale. Questo è il formato predefinito.
- Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con

compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.

Opzioni di file di log

È inoltre possibile specificare le seguenti opzioni.

- Hive-compatible S3 prefixes (Prefissi S3 compatibili con Hive): Abilita i prefissi compatibili con Hive invece di importare partizioni negli strumenti compatibili. Prima di eseguire query, utilizza il comando MSCK REPAIR TABLE.
- Hourly partitions (Partizioni orarie): se disponi di un grande volume di registri e di solito indirizzi le query a un'ora specifica, partizionando i log su base oraria puoi ottenere risultati più rapidi e risparmiare sui costi delle query.

Struttura del bucket S3 dei file di log

I file di log vengono salvati nel bucket Amazon S3; utilizzando una struttura di cartelle determinata dall'ID del flusso di log, dalla Regione e dalla loro data di creazione.

Per impostazione predefinita, i file vengono recapitati alla seguente posizione.

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

Se abiliti i prefissi S3 compatibili con Hive, i file vengono recapitati nella seguente posizione.

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

Se abiliti le partizioni orarie, i file vengono recapitati nella seguente posizione.

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

Se abiliti le partizioni compatibili con Hive e partizioni il flusso di log per ora, i file vengono recapitati nella posizione seguente.

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

Nome del file di log

Il nome di un file di log si basa sull'ID del flusso di log, sulla Regione e sulla data e ora di creazione. I nomi file utilizzano il formato seguente.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Di seguito è riportato un esempio di file di registro per un log di flusso creato da Account AWS 123456789012, per una risorsa in us-east-1 Regione, su June 20, 2018 at 16:20 UTC. Il file contiene i record del registro di flusso con un orario di fine compreso tra 16:20:00 e 16:24:59.

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

IAMpolitica per IAM i responsabili che pubblicano i log di flusso su Amazon S3

Il IAM principale che crea il log di flusso deve disporre delle seguenti autorizzazioni, necessarie per pubblicare i log di flusso nel bucket Amazon S3 di destinazione.

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

Autorizzazioni dei bucket Amazon S3 per log di flusso

Per impostazione predefinita, i bucket Amazon S3 e gli oggetti che contengono sono privati. Solo il proprietario del bucket può accedere al bucket e agli oggetti in esso archiviati. Il proprietario del bucket, tuttavia, può concedere l'accesso ad altre risorse e ad altri utenti scrivendo una policy di accesso.

Se l'utente che crea il flusso di log è il proprietario del bucket e ha le autorizzazioni `PutBucketPolicy` e `GetBucketPolicy` per il bucket, verrà automaticamente allegata la seguente policy al bucket. Questa policy sovrascrive qualsiasi policy esistente collegata al bucket.

In caso contrario, il proprietario del bucket deve aggiungere tale policy al bucket, specificando l'ID dell' Account AWS del creatore del flusso di log o la creazione del flusso di log fallirà. Per ulteriori informazioni, consulta le politiche di Bucket nella Guida per l'utente di 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:*"
                }
            }
        }
```

```
    ]
}
```

ARNCiò che specifichi *my-s3-arn* dipende dall'utilizzo o meno di prefissi S3 compatibili con Hive.

- Prefissi di default

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

- Prefissi S3 compatibili con Hive

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

Come procedura ottimale, si consiglia di concedere queste autorizzazioni al responsabile del servizio di consegna dei log anziché al singolo individuo. Account AWS ARNs Una best practice è anche usare le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". L'account di origine è il proprietario del log di flusso e l'origine ARN è la jolly (*) ARN del servizio di log.

Politica chiave richiesta per l'uso con - SSE KMS

Puoi proteggere i dati nel tuo bucket Amazon S3 abilitando la crittografia lato server con chiavi gestite da Amazon S3 (-S3) o la crittografia lato server con chiavi (SSE-). KMS SSE KMS Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server nella Guida per l'utente di Amazon S3.

Con SSE -KMS, puoi utilizzare una chiave gestita o una chiave gestita dal cliente. AWS Con una chiave AWS gestita, non puoi utilizzare la consegna tra account. I log di flusso vengono recapitati dall'account di recapito del log, pertanto è necessario concedere l'accesso per la consegna tra account. Per concedere l'accesso a più account al tuo bucket S3, utilizza una chiave gestita dal cliente e specifica l'Amazon Resource Name (ARN) della chiave gestita dal cliente quando abiliti la crittografia dei bucket. Per ulteriori informazioni, consulta Specifica della crittografia lato server con AWS KMS nella Guida per l'utente di Amazon S3.

Quando utilizzi SSE una chiave gestita dal cliente, devi aggiungere quanto segue alla policy chiave della tua chiave (non alla policy del bucket per il tuo bucket S3), in modo che VPC Flow Logs possa scrivere sul tuo bucket S3. KMS

```
{
```

```
    "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": "*"
}
```

Autorizzazioni del file di log Amazon S3

Oltre alle policy dei bucket richieste, Amazon S3 utilizza le liste di controllo degli accessi ACLs () per gestire l'accesso ai file di registro creati da un log di flusso. Per impostazione predefinita, il proprietario del bucket dispone di autorizzazioni `FULL_CONTROL` su ogni file di log. Il proprietario della distribuzione dei log, se diverso dal proprietario del bucket, non dispone di autorizzazioni. L'account di distribuzione dei log dispone delle autorizzazioni `READ` e `WRITE`. Per ulteriori informazioni, consulta la panoramica di Access control list (ACL) nella Guida per l'utente di Amazon Simple Storage Service.

Creare il ruolo dell'account di origine Transit Gateway Flow Logs per Amazon S3

Dall'account di origine, crea il ruolo di origine nella AWS Identity and Access Management console.

Creazione del ruolo dell'account di origine

1. Accedi AWS Management Console e apri la IAM console all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:

1. Scegli JSON.
2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
4. Immetti un nome per la policy e una descrizione facoltativa, quindi scegli Create policy (Crea policy).

5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Crea un record Transit Gateway Flow Logs da pubblicare su Amazon S3

Dopo aver creato e configurato il bucket Amazon S3, è possibile creare registri di flusso per i gateway di transito. Puoi creare un log di flusso di Amazon S3 utilizzando la VPC console Amazon o il. AWS CLI

Creare un log di flusso del gateway di transito che pubblichi in Amazon S3 utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare le caselle di controllo per uno o più gateway di transito o collegamenti del gateway di transito alla VPN.

4. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
5. Configura le impostazioni del flusso di log. Per ulteriori informazioni, consulta Come configurare le impostazioni del flusso di log.

Configurazione delle impostazioni del flusso di log utilizzando la console

1. Per Destination (Destinazione), scegli Send to an S3 bucket (Invia a un bucket S3).
2. Per il bucket S3 ARN, specifica l'Amazon Resource Name (ARN) di un bucket Amazon S3 esistente. Puoi anche includere una sottocartella. Ad esempio, per specificare una sottocartella denominata `my-logs` in un bucket denominato, usa quanto segue: `my-bucket` ARN

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

   Il bucket non può utilizzare `AWSLogs` come nome di sottocartella, in quanto si tratta di un termine riservato.

   Se si è il proprietario del bucket, noi creiamo automaticamente una policy delle risorse e la colleghiamo al bucket. Per ulteriori informazioni, consulta Autorizzazioni dei bucket Amazon S3 per log di flusso.
3. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.

   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.
4. Per Log file format (Formato dei file di log), specifica il formato per il file di log.

   - Text: Testo normale. Questo è il formato predefinito.
   - Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.
5. (Facoltativo) Per utilizzare prefissi S3 compatibili con Hive, scegli Hive-compatible S3 prefix (Prefisso S3 compatibile con Hive),Enable (Abilita).

6. (Facoltativo) Per partizionare i flussi di log per ora, scegli Every 1 hour (60 mins) Ogni ora (60 minuti).
7. (Facoltativo) Per aggiungere un tag al flusso di log, scegli Add new tag (Aggiungi nuovo tag) e specifica la chiave e il valore del tag.
8. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso che pubblica in Amazon S3 utilizzando uno strumento a riga di comando

Utilizzare uno dei seguenti comandi.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico del gateway di transito VPC `tgw-00112233344556677` e consegna i log di flusso a un bucket Amazon S3 chiamato. `flow-log-bucket` Il parametro `--log-format` specifica un formato personalizzato per i record di log di flusso.

```
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/'
```

Visualizza i record dei log di flusso del Transit Gateway in Amazon S3

Per visualizzare i record del log di flusso pubblicati in Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Per Bucket name (Nome bucket), selezionare il bucket in cui vengono pubblicati i log di flusso.
3. Per Nome, seleziona la casella di controllo accanto al file di registro. Nel pannello di panoramica dell'oggetto, scegliere Download (Scarica).

Record di log di flusso elaborati in Amazon S3

I file di log sono compressi. Se si aprono i file di log utilizzando la console Amazon S3, vengono decompressi e i record del log di flusso visualizzati. Se i file vengono scaricati, devono essere decompressi per visualizzare i record del log di flusso.

Transit Gateway Flow registra i record in Amazon Data Firehose

Argomenti

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Firehose. Puoi scegliere di pubblicare i log di flusso sullo stesso account del monitor delle risorse o su un altro account.

Prerequisiti

Durante la pubblicazione su Firehose, i dati del log di flusso vengono pubblicati in un flusso di distribuzione Firehose, in formato testo semplice. È innanzitutto necessario aver creato un flusso di distribuzione Firehose. Per i passaggi per creare un flusso di distribuzione, consulta Creating an Amazon Data Firehose Delivery Stream nella Amazon Data Firehose Developer Guide.

Prezzi

Si applicano le spese standard di acquisizione e consegna. Per ulteriori informazioni, apri Amazon CloudWatch Pricing, seleziona Logs e trova Vending Logs.

Ruoli IAM per la consegna tra account

Quando si pubblica su Kinesis Data Firehose, è possibile scegliere un flusso di consegna che si trova nello stesso account della risorsa da monitorare (l'account di origine) o in un altro account (l'account di destinazione). Per consentire la consegna dei log di flusso su più account a Firehose, è necessario creare IAM un ruolo nell'account di origine e IAM un ruolo nell'account di destinazione.

Roles

Ruolo dell'account di origine

Nell'account di origine, crea un ruolo che conceda le seguenti autorizzazioni. In questo esempio, il nome del ruolo è `mySourceRole` ma è possibile scegliere un nome diverso. L'ultima istruzione

consente al ruolo nell'account di destinazione di assumere questo ruolo. Le istruzioni sulle condizioni assicurano che questo ruolo venga passato solo al servizio di consegna dei log e solo durante il monitoraggio della risorsa specificata. Quando crei la tua policy, specifica le VPCs interfacce di rete o le sottoreti che stai monitorando con la chiave di condizione. `iam:AssociatedResourceARN`

```
{
  "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"
    }
  ]
}
```

Verifica che questo ruolo abbia la seguente policy di attendibilità che consente al servizio di consegna dei log di assumere il ruolo.

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

Ruolo dell'account di destinazione

Nell'account di destinazione, crea un ruolo con un nome che inizia con AWSLogDeliveryFirehoseCrossAccountRole. Questo ruolo deve concedere le autorizzazioni riportate di seguito.

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

Assicurarsi che questo ruolo abbia la seguente policy di attendibilità, che consenta al ruolo creato nell'account di origine di assumere questo ruolo.

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

```
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creare il ruolo dell'account di origine Transit Gateway Flow Logs per Amazon Data Firehose

Dall'account di origine, crea il ruolo di origine nella AWS Identity and Access Management console.

Creazione del ruolo dell'account di origine

1. Accedi AWS Management Console e apri la IAM console all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
    1. Scegli JSON.
    2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
    3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
    4. Immetti un nome per la policy e una descrizione facoltativa, quindi scegli Create policy (Crea policy).
5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

    ```
    "Principal": {
    ```

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Creare il ruolo dell'account di destinazione Transit Gateway Flow Logs per Amazon Data Firehose

Dall'account di destinazione, crea il ruolo di destinazione nella AWS Identity and Access Management console.

Creazione del ruolo dell'account di destinazione

1. Accedi AWS Management Console e apri la IAM console all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
   1. Scegli JSON.
   2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
   3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
   4. Inserisci un nome per la tua politica che inizia con AWSLogDeliveryFirehoseCrossAccountRole, quindi scegli Crea politica.
5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

```
"Principal": {
```

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Crea un record Transit Gateway Flow Logs da pubblicare su Amazon Data Firehose

Crea un Transit Gateway Flow Log da pubblicare su Amazon Data Firehose. Prima di creare il log di flusso, assicurati di aver impostato i ruoli dell'IAMaccount di origine e di destinazione per la distribuzione tra account e di aver creato il flusso di distribuzione Firehose. Per ulteriori informazioni, consulta Registri di flusso di Amazon Data Firehose. È possibile creare un log di flusso Firehose utilizzando la VPC console Amazon o il. AWS CLI

Per creare un log di flusso del gateway di transito da pubblicare su Firehose utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare le caselle di controllo per uno o più gateway di transito o collegamenti del gateway di transito alla VPN.
4. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
5. Per Destination (Destinazione), scegli Send to a Firehose Delivery System (Invia a un sistema di consegna Firehose).
6. Per il Firehose Delivery Stream ARN, scegli uno ARN dei flussi di consegna che hai creato in cui pubblicare il log di flusso.
7. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.

   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.

8. (Facoltativo) Per aggiungere un tag al flusso di log, scegli Add new tag (Aggiungi nuovo tag) e specifica la chiave e il valore del tag.
9. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso da pubblicare su Firehose utilizzando lo strumento da riga di comando

Utilizzare uno dei seguenti comandi:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

L' AWS CLIesempio seguente crea un log di flusso che acquisisce le informazioni sul gateway di transito e invia il log di flusso al flusso di distribuzione Firehose specificato.

```
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
```

L' AWS CLIesempio seguente crea un log di flusso che acquisisce le informazioni sul gateway di transito e invia il log di flusso a un flusso di consegna Firehose diverso dall'account di origine.

```
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
```

Crea e gestisci i log di flusso di Amazon VPC Transit Gateways utilizzando APIs o CLI

Puoi eseguire le attività descritte in questa pagina utilizzando la riga di comando.

Le seguenti limitazioni si applicano all'utilizzo del create-flow-logscomando:

- `--resource-ids` ha un vincolo massimo di 25 tipi di risorse `TransitGateway` o `TransitGatewayAttachment`.
- `--traffic-type` non è un campo obbligatorio per impostazione predefinita. Se lo si fornisce per i tipi di risorse del gateway di transito, viene restituito un errore. Questo limite si applica solo ai tipi di risorsa del gateway di transito.
- `--max-aggregation-interval` ha un valore predefinito di `60`, ed è l'unico valore accettato per i tipi di risorse del gateway di transito. Se si tenta di passare qualsiasi altro valore, viene restituito un errore. Questo limite si applica solo ai tipi di risorsa del gateway di transito.
- `--resource-type` supporta due nuovi tipi di risorsa, il `TransitGateway` e il `TransitGatewayAttachment`.
- Se non si impostano i campi che si desiderano includere, `--log-format` include tutti i campi di log per i tipi di risorsa del gateway di transito. Questo vale solo per i tipi di risorse del gateway di transito.

Creazione di un log di flusso

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Descrizione dei log di flusso

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Visualizzazione dei record del log di flusso (eventi di log)

- get-log-events (AWS CLI)
- Get- CWLLogEvent (AWS Tools for Windows PowerShell)

Eliminazione di un log di flusso

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Visualizza i record dei log di flusso di Amazon VPC Transit Gateways

Visualizza le informazioni sui log di flusso del tuo gateway di transito tramite AmazonVPC. Quando scegli una risorsa, vengono elencati tutti i log di flusso relativi a quella risorsa. Le informazioni visualizzate includono l'ID del log di flusso, la configurazione del log di flusso e le informazioni relative allo stato del log di flusso.

Per visualizzare informazioni sui registri di flusso per i gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare un gateway di transito o un collegamento del gateway di transito alla VPN e scegliere Flow Logs (Registri di flusso). Le informazioni relative ai log di flusso vengono visualizzate nella scheda. La colonna Destination type (Tipo di destinazione) indica la destinazione in cui i log di flusso vengono pubblicati.

Gestione dei tag dei log di flusso di Amazon VPC Transit Gateways

Puoi aggiungere o rimuovere tag per un log di flusso nelle VPC console Amazon EC2 e Amazon.

Per aggiungere o rimuovere tag per un log di flusso del gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare un gateway di transito o un collegamento del gateway di transito alla VPN
4. Scegliere Manage tags (Gestisci tag) per il log di flusso richiesto.
5. Per aggiungere un nuovo tag, scegliere Create Tag (Crea tag). Per rimuovere un tag, scegliere il pulsante Elimina (x).
6. Seleziona Salva.

Cerca nei record dei log di flusso di Amazon VPC Transit Gateways

Puoi cercare i record dei log di flusso pubblicati su CloudWatch Logs utilizzando la console CloudWatch Logs. È possibile utilizzare filtri metrici per filtrare i record del log di flusso. I record del log di flusso sono delimitati da spazio.

Per cercare i record del log di flusso utilizzando la CloudWatch console Logs

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione scegli Log, quindi Gruppi di log.
3. Selezionare il gruppo di flussi di log contenente il registro di flusso. Viene mostrato un elenco di flussi di log per ogni gateway di transito.
4. Selezionare il singolo flusso di log se si conosce il gateway di transito che si sta cercando. In alternativa, scegliere Cerca gruppo di log per cercare l'intero gruppo di log. Ciò potrebbe richiedere del tempo se nel gruppo di flussi di log sono presenti molti gateway di transito, o in base all'intervallo di tempo selezionato.
5. Per gli Eventi Filtro, immettere la stringa seguente. Ciò presuppone che il record del log di flusso utilizzi il formato predefinito.

```
[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. Modificare il filtro in base alle esigenze specificando i valori per i campi. Negli esempi seguenti il filtro viene applicato in base a specifici indirizzi IP di origine.

```
[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]
```

L'esempio seguente filtra in base all'ID del gateway di transito tgw-123abc456bca, alla porta di destinazione e al numero di byte.

```
[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]
```

Eliminazione di un record di Amazon VPC Transit Gateways Flow Logs

Puoi eliminare un log di flusso del gateway di transito utilizzando la VPC console Amazon.

Queste procedure disabilitano il servizio del log di flusso per una risorsa. L'eliminazione di un log di flusso non elimina i flussi di log esistenti da CloudWatch Logs o i file di log da Amazon S3. I dati del log di flusso esistenti devono essere eliminati utilizzando la rispettiva console del servizio. Inoltre, l'eliminazione di un log di flusso pubblicato su Amazon S3 non rimuove le policy dei bucket e gli elenchi di controllo degli accessi ai file di registro (). ACLs

Per eliminare un log di flusso del gateway di transito

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
3. Scegliere un Transit gateway ID (ID gateway di transito).

4. Nella sezione Flow logs (Registri di flusso), scegliere i registri di flusso che si desiderano eliminare.
5. Scegliere Actions (Operazioni), quindi scegliere Delete flow logs (Elimina registri di flusso).
6. Confermare che si desidera eliminare il flusso scegliendo Delete (Elimina).

Monitora i gateway di transito utilizzando Amazon VPC Transit Gateways

È possibile utilizzare le seguenti funzionalità per monitorare i gateway di transito, analizzare i modelli di traffico e risolvere i problemi relativi ai gateway di transito.

CloudWatch metriche

Puoi utilizzare Amazon CloudWatch per recuperare le statistiche sui punti dati per i tuoi gateway di transito sotto forma di set ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta CloudWatch metriche in Amazon VPC Transit Gateways.

Registri di flusso di Transit Gateway

È possibile utilizzare i registri di flusso di Transit Gateway per acquisire informazioni dettagliate sul traffico di rete sui gateway di transito. Per ulteriori informazioni, consulta Registri di flusso di Transit Gateway.

Log di flusso VPC

Puoi utilizzare VPC Flow Logs per acquisire informazioni dettagliate sul traffico in entrata e in uscita dai gateway di transito collegati ai tuoi VPCs gateway di transito. Per ulteriori informazioni, consulta VPCFlow Logs nella Amazon VPC User Guide.

CloudTrail registri

Puoi utilizzarle AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate al gateway di transito API e archiviarle come file di registro in Amazon S3. È possibile utilizzare questi CloudTrail registri per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata, quando è stata effettuata la chiamata e così via. Per ulteriori informazioni, consulta CloudTrail registri.

CloudWatch Eventi che utilizzano Network Manager

È possibile utilizzarli AWS Network Manager per inoltrare CloudWatch gli eventi e quindi indirizzarli a funzioni o flussi di destinazione. Network Manager genera eventi per le modifiche alla topologia, gli aggiornamenti del routing e gli aggiornamenti di stato, che possono essere utilizzati per avvisare l'utente dei cambiamenti nei gateway di transito. Per ulteriori informazioni, consulta Monitoraggio della rete globale con CloudWatch eventi nella Guida per l'utente di AWS Global Networks for Transit Gateways.

CloudWatch metriche in Amazon VPC Transit Gateways

Amazon VPC pubblica punti dati su Amazon CloudWatch per i tuoi gateway di transito e gli allegati dei gateway di transito. CloudWatchti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a una metrica come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. A ogni dato sono associati una marcatura temporale e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica non rientra nell'intervallo che consideri accettabile.

Amazon VPC misura e invia i propri parametri CloudWatch a intervalli di 60 secondi.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Metriche dei gateway di transito

Il namespace `AWS/TransitGateway` include le metriche descritte di seguito.

Tutte le metriche vengono sempre riportate. I loro valori dipendono dal traffico attraverso il gateway di transito. Vedi Dimensioni metriche del gateway di transito per le dimensioni supportate.

Parametro	Descrizione
`BytesDropCountBlackhole`	Il numero di byte persi perché intercettati da una route `blackhole` . Statistiche: l'unica statistica significativa è `Sum`.
`BytesDropCountNoRoute`	Il numero di byte persi perché non corrispondenti a una route esistente.

Parametro	Descrizione
	Statistiche: l'unica statistica significativa è `Sum`.
`BytesIn`	Numero di byte ricevuti dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesOut`	Numero di byte inviati dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsIn`	Il numero di pacchetti ricevuti dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsOut`	Il numero di pacchetti inviati dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountBlackhole`	Il numero di pacchetti persi perché intercettati da una route `blackhole` . Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountNoRoute`	Il numero di pacchetti persi perché non presente una route corrispondente. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropTTLExpired`	Il numero di pacchetti persi perché è TTL scaduto. Statistiche: l'unica statistica significativa è `Sum`.

Metriche a livello di allegato e zona di disponibilità

Le metriche seguenti sono disponibili per gli allegati del gateway di transito. Tutti i parametri degli allegati vengono pubblicati nell'account del proprietario del gateway di transito. Anche i singoli parametri degli allegati vengono pubblicati nell'account del proprietario dell'allegato. Il proprietario dell'allegato può visualizzare solo i parametri del proprio allegato. Per ulteriori informazioni sui tipi di allegati supportati, vedi the section called “Collegamenti alle risorse”.

Le metriche delle zone di disponibilità sono disponibili per aver abilitato le zone di disponibilità () sugli allegati del gateway di transito. AZs Solo gli VPC allegati supportano le metriche Per-AZ. Tutte le metriche di livello AZ vengono pubblicate sull'account del proprietario del gateway di transito. Le metriche AZ individuali per un allegato vengono pubblicate anche nell'account del proprietario dell'allegato. Il proprietario dell'allegato può visualizzare solo le metriche per-AZ per il proprio allegato.

Tutte le metriche vengono sempre riportate. I loro valori dipendono dal traffico in entrata e/o in uscita dall'allegato del gateway di transito. Vedi Dimensioni metriche del gateway di transito per le dimensioni supportate.

Parametro	Descrizione
`BytesDropCountBlackhole`	Numero di byte eliminati perché corrispondono a una route `blackhole` nell'allegato del gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesDropCountNoRoute`	Numero di byte eliminati perché non corrispondono a una route nell'allegato del gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesIn`	Numero di byte ricevuti dal gateway di transito dall'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`BytesOut`	Numero di byte inviati dal gateway di transito all'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsIn`	Numero di pacchetti ricevuti dal gateway di transito dall'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsOut`	Numero di pacchetti inviati dal gateway di transito all'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountBlackhole`	Numero di pacchetti eliminati perché corrispondono a una route `blackhole` nell'allegato del gateway di transito.

Parametro	Descrizione
	Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountNoRoute`	Il numero di pacchetti persi perché non presente una route corrispondente. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropTTLExpired`	Il numero di pacchetti persi perché è TTL scaduto. Statistiche: l'unica statistica significativa è `Sum`.

Dimensioni metriche del gateway di transito

Filtra i dati metrici del gateway di transito utilizzando le seguenti dimensioni:

Dimensione	Descrizione
`TransitGateway`	Filtra i dati delle metriche in base al gateway di transito.
`TransitGatewayAttachment`	Filtra i dati delle metriche in base all'allegato del gateway di transito.
`TransitGateway` , `AvailabilityZone`	Filtra i dati metrici sia per gateway di transito che per zona di disponibilità.
`TransitGatewayAttachment` , `AvailabilityZone`	Filtra i dati metrici sia in base all'allegato del gateway di transito che alla zona di disponibilità.

Registra le API chiamate Amazon VPC Transit Gateways utilizzando AWS CloudTrail

Amazon VPC Transit Gateways è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le API chiamate per Transit Gateway come eventi. Le chiamate acquisite includono chiamate dalla console Transit Gateway e chiamate in codice alle API operazioni Transit Gateway. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Transit Gateway, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente di IAM Identity Center.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un percorso a regione singola o multiregione utilizzando. AWS CLI La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio account Regioni AWS . Se crei un percorso a regione singola, puoi visualizzare solo gli eventi registrati nel percorso. Regione

AWS Per ulteriori informazioni sui percorsi, consulta Creazione di un percorso per te Account AWS e Creazione di un percorso per un'organizzazione nella Guida per l'AWS CloudTrail utente.

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query SQL basate sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in JSON formato basato su righe in formato Apache. ORC ORCè un formato di archiviazione colonnare ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

Eventi di gestione Transit Gateway

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse del sistema Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon VPC Transit Gateways registra tutte le operazioni del piano di controllo Transit Gateway come eventi di gestione. Per un elenco delle operazioni del piano di controllo di Amazon VPC Transit Gateways a cui Transit Gateway accede CloudTrail, consulta Amazon VPC Transit API Gateways Reference.

Esempi di eventi Transit Gateway

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'APIoperazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via.

CloudTrail i file di registro non sono una traccia stack ordinata delle API chiamate pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle API chiamate pubbliche, quindi non vengono visualizzati in un ordine specifico.

I file di registro includono gli eventi per tutte le API chiamate per l' AWS account, non solo per le API chiamate di transito tramite gateway. È possibile localizzare le chiamate al gateway di transito API controllando gli `eventSource` elementi con il valore`ec2.amazonaws.com`. Per visualizzare il record di un'operazione specifica, ad esempio `CreateTransitGateway`, verifica la presenza di elementi `eventName` con il nome dell'operazione.

Di seguito è riportato un esempio di record di CloudTrail registro per il gateway di transito API per un utente che ha creato un gateway di transito utilizzando la console. Puoi identificare l'interfaccia a riga di comando utilizzando l'elemento `userAgent`. È possibile identificare la API chiamata richiesta utilizzando gli `eventName` elementi. Le informazioni relative all'utente (`Alice`) sono disponibili nell'elemento `userIdentity`.

Example Esempio: 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"
}
```

Gestione delle identità e degli accessi in Amazon VPC Transit Gateway

AWS utilizza credenziali di sicurezza per identificarti e concederti l'accesso alle tue AWS risorse. Puoi utilizzare le funzionalità di AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le tue AWS risorse completamente o in modo limitato, senza condividere le tue credenziali di sicurezza.

Per impostazione predefinita, gli utenti IAM non sono autorizzati a creare, visualizzare o modificare AWS le risorse. Per consentire a un utente di accedere a risorse come un gateway di transito e di eseguire attività, è necessario creare una policy IAM che conceda all'utente l'autorizzazione per utilizzare le risorse specifiche e le operazioni API di cui ha bisogno, quindi collegare la policy al gruppo a cui appartiene tale utente. Quando si collega una policy a un utente o a un gruppo di utenti, viene concessa o rifiutata agli utenti l'autorizzazione per l'esecuzione delle attività specificate sulle risorse specificate.

Per lavorare con un gateway di transito, una delle seguenti politiche AWS gestite potrebbe soddisfare le tue esigenze:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Policy di esempio per la gestione dei gateway di transito

Di seguito sono riportate le policy IAM di esempio per l'utilizzo dei gateway di transito.

Creazione di un gateway di transito con i tag necessari

L'esempio seguente consente agli utenti di creare gateway di transito. La chiave di condizione `aws:RequestTag` richiede agli utenti di contrassegnare il gateway di transito con il tag `stack=prod`. La chiave di condizione `aws:TagKeys` utilizza il modificatore `ForAllValues` per indicare che soltanto la chiave `stack` è consentita nella richiesta (non è possibile specificare altri tag). Se gli utenti non passano questo tag specifico quando creano il gateway di transito o se non specificano affatto i tag, la richiesta non riesce.

La seconda istruzione utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `CreateTransitGateway`.

```
{
    "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"
                }
            }
        }
    ]
}
```

Utilizzo delle tabelle di routing del gateway di transito

L'esempio seguente consente agli utenti di creare ed eliminare tabelle di routing del gateway di transito solo per un gateway di transito specifico (`tgw-11223344556677889`). Gli utenti possono inoltre creare e sostituire route in qualsiasi tabella di routing del gateway di transito, ma solo per gli allegati con il 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/*"
        }
    ]
}
```

Usa ruoli collegati ai servizi per i gateway di transito in Amazon VPC Transit Gateway

Amazon VPC utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Per ulteriori informazioni, consulta Ruoli collegati ai servizi nella Guida per l'utente di IAM.

Ruolo collegato ai servizi per il gateway di transito

Amazon VPC utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto quando lavori con un gateway di transito.

Autorizzazioni concesse dal ruolo collegato ai servizi

Amazon VPC utilizza il ruolo collegato al servizio denominato AWSServiceRoleForVPCTransitGateway per eseguire le seguenti azioni per tuo conto quando lavori con un gateway di transito:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

Il ruolo AWSServiceRoleForVPCTransitGateway prevede che i seguenti servizi assumano il ruolo:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway utilizza la policy AWSVPCTransitGatewayServiceRolePolicy gestita.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi

Non è necessario creare manualmente il ruolo AWSServiceRoleForVPCTransitGateway. Amazon VPC crea questo ruolo quando colleghi un VPC nel tuo account a un gateway di transito.

Modifica del ruolo collegato ai servizi

Puoi modificare la descrizione di AWSServiceRoleForVPCTransitGateway utilizzando IAM. Per ulteriori informazioni, consulta Modificare una descrizione di ruolo collegato al servizio nella Guida per l'utente IAM.

Eliminazione del ruolo collegato ai servizi

Se non hai più bisogno di utilizzare i gateway di transito, ti consigliamo di eliminare Gateway. AWSService RoleFor VPCTransit

Puoi eliminare questo ruolo collegato al servizio solo dopo aver eliminato tutti gli allegati VPC del gateway di transito nel tuo account. AWS Questa procedura impedisce di rimuovere involontariamente l'autorizzazione ad accedere ai collegamenti al VPC.

Per eliminare i ruoli collegati ai servizi, puoi utilizzare la console IAM, l'interfaccia a riga di comando IAM CLI o l'API IAM. Per ulteriori informazioni, consulta Eliminare un ruolo collegato al servizio nella Guida per l'utente IAM.

Dopo aver eliminato AWSServiceRoleForVPCTransitGateway, Amazon VPC crea nuovamente il ruolo se colleghi un VPC nel tuo account a un gateway di transito.

AWS politiche gestite per i gateway di transito in Amazon VPC Transit Gateways

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

Per lavorare con un gateway di transito, una delle seguenti politiche AWS gestite potrebbe soddisfare le tue esigenze:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS politica gestita: AWSVPCTransit GatewayServiceRolePolicy

Questa politica è allegata al ruolo AWSServiceRoleForVPCTransitGateway. Ciò consente ad Amazon VPC di creare e gestire risorse per collegamento del gateway di transito alla VPN.

Per vedere le autorizzazioni per questa policy, consulta AWSVPCTransitGatewayServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

Transit Gateway si aggiorna alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per i gateway di transito da quando Amazon VPC ha iniziato a tracciare queste modifiche nel marzo 2021.

Modifica	Descrizione	Data
Amazon VPC ha iniziato a monitorare le modifiche	Amazon VPC ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	1 marzo 2021

Rete ACLs per gateway di transito in Amazon VPC Transit Gateways

Una lista di controllo accessi di rete (NACL) è un livello facoltativo di protezione.

Le regole delle liste di controllo accessi di rete (NACL) vengono applicate in modo diverso, a seconda dello scenario:

- the section called “Stessa sottorete per le EC2 istanze e l'associazione dei gateway di transito”
- the section called “Sottoreti diverse per EC2 le istanze e l'associazione dei gateway di transito”

Stessa sottorete per le EC2 istanze e l'associazione dei gateway di transito

Prendi in considerazione una configurazione in cui siano presenti EC2 istanze e un'associazione di gateway di transito nella stessa sottorete. Lo stesso ACL di rete viene utilizzato sia per il traffico dalle EC2 istanze al gateway di transito sia per il traffico dal gateway di transito alle istanze.

Le regole delle liste di controllo accessi di rete (NACL) per il traffico dalle istanze al gateway di transito vengono applicate nel modo seguente:

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per la valutazione.
- Le regole in ingresso utilizzano l'indirizzo IP di origine per la valutazione.

Le regole delle liste di controllo accessi di rete (NACL) per il traffico dal gateway di transito alle istanze vengono applicate nel modo seguente:

- Le regole in uscita non vengono valutate.
- Le regole in entrata non vengono valutate.

Sottoreti diverse per EC2 le istanze e l'associazione dei gateway di transito

Prendi in considerazione una configurazione in cui sono presenti EC2 istanze in una sottorete e un'associazione di gateway di transito in una sottorete diversa e ogni sottorete è associata a un ACL di rete diverso.

Le regole ACL di rete vengono applicate come segue per la sottorete dell'istanza: EC2

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per valutare il traffico dalle istanze al gateway di transito.
- Le regole in entrata utilizzano l'indirizzo IP di origine per valutare il traffico dal gateway di transito alle istanze.

Le regole dell'NACL per la sottorete del gateway di transito vengono applicate come segue:

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per valutare il traffico dal gateway di transito alle istanze.
- Le regole in uscita non vengono utilizzate per valutare il traffico dalle istanze al gateway di transito.
- Le regole in entrata utilizzano l'indirizzo IP di origine per valutare il traffico dalle istanze al gateway di transito.
- Le regole in entrata non vengono utilizzate per valutare il traffico dal gateway di transito alle istanze.

Best practice

Utilizza una sottorete separata per ogni allegato VPC del gateway di transito. Per ogni sottorete, utilizzate un piccolo CIDR, ad esempio /28, in modo da avere più indirizzi per le risorse. EC2 Quando usi una sottorete separata, puoi configurare quanto segue:

- Tieni aperta la lista di controllo accessi di rete in ingresso e in uscita associata alla sottorete del gateway di transito.
- A seconda del flusso di traffico, puoi applicarlo NACLs alle sottoreti del carico di lavoro.

Per ulteriori informazioni sul funzionamento degli allegati VPC, consulta the section called “Collegamenti alle risorse”.

Quote dei gateway di transito Amazon VPC

Hai Account AWS le seguenti quote (precedentemente denominate limiti) relative ai gateway di transito. Salvo diversa indicazione, ogni quota si applica a una regione specifica.

La console Service Quotas fornisce informazioni sulle quote per il tuo account. È possibile utilizzare la console Service Quotas per visualizzare le quote di default e richiedere aumenti delle quote per le quote regolabili. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente delle Service Quotas.

Se una quota regolabile non è ancora disponibile nelle Service Quotas, è possibile aprire un ticket di supporto.

Generali

Nome	Predefinita	Adattabile
Gateway di transito per account	5	Sì
Blocchi CIDR per gateway di transito	5	No

I blocchi CIDR sono utilizzati nella funzione the section called “Collegamenti Connect e peer Connect”.

Routing

Nome	Predefinita	Adattabile
Tabelle di routing del gateway di transito per gateway di transito	20	Sì
Percorsi combinati totali (dinamici e statici) su tutte le tabelle delle rotte per un singolo gateway di transito	10.000	Sì

Nome	Predefinita	Adattabile
Instradamenti dinamici annunciati da un'appliance router virtuale a un peer Connect	1.000	Sì
Instradamenti annunciati da un peer Connect su un gateway di transito a un'appliance router virtuale	5.000	No
Route statiche per un prefisso di un singolo allegato	1	No

Gli instradamenti annunciati provengono dalla tabella di instradamento associata al collegamento Connect.

Collegamenti del gateway di transito

Un gateway di transito non può avere più di un allegato VPC allo stesso VPC.

Nome	Predefinita	Adattabile
Collegamenti per gateway di transito	5.000	No
Gateway di transito per VPC	5	No
Collegamenti peering per gateway di transito	50	Sì
Collegamenti peering in sospeso per gateway di transito	10	Sì
Allegati di peering tra due gateway di transito o tra un gateway di transito e un core network edge (CNE) di Cloud WAN	1	No
Peer di Connect (tunnel GRE) per collegamento Connect	4	No

Larghezza di banda

Esistono molti fattori che possono influire sulla larghezza di banda ottenuta tramite una connessione Site-to-Site VPN, tra cui, a titolo esemplificativo ma non esaustivo: dimensione dei pacchetti, mix di traffico (TCP/UDP), definizione o limitazione delle politiche sulle reti intermedie, condizioni meteorologiche relative a Internet e requisiti applicativi specifici. Per i collegamenti VPC, gateway AWS Direct Connect , o collegamenti del gateway di transito alla VPN peer-to-peer, cercheremo di fornire una larghezza di banda aggiuntiva oltre al valore predefinito.

Nome	Predefinita	Adattabile
Larghezza di banda per collegamento VPC per zona di disponibilità	Fino a 100 Gb/s	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Pacchetti al secondo per gateway di transito, collegamento VPC per zona di disponibilità	Fino a 7.500.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Larghezza di banda per la connessione AWS Direct Connect gateway o gateway di transito peer-to-peer per zona di disponibilità disponibi le nella regione	Fino a 100 Gb/s	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Pacchetti al secondo per allegato del gateway di transito (AWS Direct Connect e allegati peering) per zona di disponibilità disponibile nella regione	Fino a 7.500.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager

Nome	Predefinita	Adattabile
		(TAM) per ulteriore assistenza.
Larghezza di banda massima per tunnel VPN	Fino a 1,25 Gb/s	No
Numero massimo di pacchetti al secondo per tunnel VPN	Fino a 140.000	No
Larghezza di banda massima per peer Connect (tunnel GRE) per collegamento Connect	Fino a 5 Gb/s	No
Numero massimo di pacchetti al secondo per peer Connect	Fino a 300.000	No

È possibile utilizzare routing a percorsi multipli a costo uguale ECMP per ottenere una larghezza di banda VPN maggiore tramite l'aggregazione di molteplici tunnel VPN. Per utilizzare ECMP, la connessione VPN deve essere configurata per il routing dinamico. ECMP non è supportato nelle connessioni VPN che utilizzano routing statico.

È possibile creare fino a 4 peer Connect per allegato Connect (fino a 20 Gbps di larghezza di banda totale per allegato Connect), purché l'allegato di trasporto sottostante (VPC o AWS Direct Connect) supporti la larghezza di banda richiesta. Puoi utilizzare l'instradamento ECMP per ottenere una lunghezza di banda maggiore con il dimensionamento orizzontale tra più peer di Connect dello stesso collegamento Connect o tra più collegamenti Connect sullo stesso gateway di transito. Il gateway di transito non può utilizzare ECMP tra peering BGP dello stesso peer Connect.

AWS Direct Connect gateway

Nome	Predefinita	Adattabile
AWS Direct Connect gateway per gateway di transito	20	No
Gateway di transito per gateway AWS Direct Connect	6	No

Unità di trasmissione massima (MTU)

- L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito trasferibile attraverso la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. Un gateway di transito supporta un MTU di 8500 byte per il traffico tra VPCs, Transit AWS Direct Connect Gateway Connect e gli allegati di peering (allegati peering intra-regionali, interregionali e Cloud WAN). Il traffico su connessioni VPN può avere una MTU di 1500 byte.
- Quando si esegue la migrazione dal peering VPC per utilizzare un gateway di transito, una mancata corrispondenza di dimensioni MTU tra il peering VPC e il gateway di transito potrebbe causare il calo di alcuni pacchetti di traffico asimmetrico. Aggiorna entrambi contemporaneamente per evitare che i pacchetti VPCs jumbo cadano a causa di una mancata corrispondenza delle dimensioni.
- Il gateway di transito applica il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per ulteriori informazioni, consulta RFC879.
- Per informazioni dettagliate sulle quote Site-to-Site VPN per MTU, consulta Maximum Transmission Unit (MTU) nella Guida per l'utente.AWS Site-to-Site VPN
- I gateway di transito supportano Path MTU Discovery (PMTUD) per l'ingresso del traffico sugli allegati VPC e Connect. Il gateway di transito genera i pacchetti for e for packets. `FRAG_NEEDED` ICMPv4 `Packet Too Big (PTB)` ICMPv6 I gateway di transito non supportano PMTUD sugli allegati VPN Site-to-site, Direct Connect e Peering. Per ulteriori informazioni su Path MTU Discovery, consulta Path MTU Discovery nella Amazon VPC User Guide

Multicast

Nome	Predefinita	Adattabile
Domini multicast per gateway di transito	20	Sì
Interfacce di rete multicast per gateway di transito	10.000	Sì
Associazioni di dominio multicast per VPC	20	Sì

Nome	Predefinita	Adattabile
Origini per gruppo multicast del gateway di transito	1	Sì
Membri e fonti di gruppi statici e IGMPv2 multicast per gateway di transito	10.000	No
Membri del gruppo statico e IGMPv2 multicast per gruppo multicast del gateway di transito	100	No
Throughput multicast massimo per flusso	1 Gb/s	No
Throughput multicast aggregato massimo per zona di disponibilità	20 Gb/s	No

AWS Gestore di rete

Nome	Predefinita	Adattabile
Reti globali per Account AWS	5	Sì
Dispositivi per rete globale	200	Sì
Collegamenti per rete globale	200	Sì
Siti per rete globale	200	Sì
Connessioni per rete globale	500	No

Risorse aggiuntive delle quote

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Site-to-Site Quote VPN nella Guida per l'AWS Site-to-Site VPN utente
- Quote Amazon VPC nella Guida per l'utente di Amazon VPC
- Quote di AWS Direct Connect nella Guida per l'utente AWS Direct Connect

Cronologia dei documenti per i gateway di transito

Nella tabella seguente vengono descritte le release per i gateway di transito.

Modifica	Descrizione	Data
Supporto per la referenzi azione dei gruppi di sicurezza	Ora puoi fare riferimento a un gruppo di sicurezza tramite collegamento VPCs a un gateway di transito.	25 settembre 2024
AWS Quote Transit Gateway	Sono stati aggiunti limiti di larghezza di banda.	14 agosto 2023
AWS Registri di flusso Transit Gateway	I gateway di transito ora supportano i registri di flusso di Transit Gateway, consenten do di monitorare e registrare il traffico di rete tra i gateway di transito.	14 luglio 2022
Tabelle di policy del gateway di transito	Utilizzare le tabelle di policy per impostare il routing dinamico per i gateway di transito per lo scambio automatico di informazioni di instradamento e raggiungibilità con tipi di gateway di transito in peering.	13 luglio 2022
Guida per l'utente di Network Manager	Network Manager è stato creato come guida autonoma e non è più incluso come parte della Guida per l'utente di AWS Transit Gateway.	2 dicembre 2021
Peering di allegati	È possibile creare una connessione di peering con	1 dicembre 2021

	un gateway di transito nella stessa regione.	
Transit Gateway Connect	È possibile stabilire una connessione tra un gateway di transito e dispositivi virtuali di terze parti in esecuzione in unVPC.	10 dicembre 2020
Modalità Appliance	È possibile abilitare la modalità appliance su un VPC allegato per garantire che il traffico bidirezionale fluisca attraverso la stessa zona di disponibilità per l'allegato.	29 ottobre 2020
Riferimenti elenco dei prefissi	È possibile fare riferimento a un elenco di prefissi nella tabella di instradamento del gateway di transito.	24 agosto 2020
Modifica gateway di transito	È possibile modificare le opzioni di configurazione per il gateway di transito.	24 agosto 2020
CloudWatch metriche per gli allegati del gateway di transito	È possibile visualizzare le CloudWatch metriche per i singoli allegati del gateway di transito.	6 luglio 2020
Network Manager Route Analyzer	È possibile analizzare le route nelle tabelle di routing del gateway di transito nella rete globale.	4 maggio 2020

Peering di allegati	È possibile creare una connessione di peering con un gateway di transito in un'altra regione.	3 dicembre 2019
Supporto multicast	Transit Gateway supporta il routing del traffico multicast tra le sottoreti di dispositivi collegati VPCs e funge da router multicast per le istanze che inviano traffico destinato a più istanze di ricezione.	3 dicembre 2019
AWS Network Manager	È possibile visualizzare e monitorare le reti globali costruite attorno ai gateway di transito.	3 dicembre 2019
AWS Direct Connect supporto	È possibile utilizzare un AWS Direct Connect gateway per connettere la AWS Direct Connect connessione tramite un'interfaccia virtuale di transito al gateway di transito VPCs o VPNs collegata allo stesso.	27 marzo 2019
Versione iniziale	Questa versione introduce i gateway di transito.	26 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.