AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Che cos'è un gateway di transito?

Un gateway di transito è un hub di transito della rete che puoi utilizzare per collegare i VPC alle reti locali. Man mano che la tua infrastruttura cloud si espande a livello globale, il peering interregionale connette i gateway di transito tra loro 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 VPC
  - Un'appliance di rete Connect SD-WAN/di terze parti
  - Un gateway AWS Direct Connect
  - Una connessione peering con un altro gateway di transito
  - Una connessione VPN a un gateway di transito
- Unità massima di trasmissione (MTU) del gateway di transito: l'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande che può essere trasmesso con 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 una MTU di 8500 byte per il traffico tra VPC, AWS Direct Connect, Transit Gateway Connect e collegamenti peering. Il traffico su connessioni VPN può avere una MTU di 1500 byte.
- 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 route: un VPC, una connessione VPN o un gateway Direct Connect possono propagare le route in modo dinamico verso una tabella di instradamento di un gateway di transito.

Per impostazione predefinita, con un allegato Connect le route vengono propagate a una tabella di routing del gateway di transito. Con un VPC, per inviare traffico verso il gateway di transito è necessario creare route statici. Con una connessione VPN, i route sono propagati dal gateway di transito verso il router locale tramite il Border Gateway Protocol (BGP). Con un gateway Direct Connect, i prefissi consentiti sono generati verso il router on-premise tramite il protocollo 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
- Nozioni di base
- 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.
- Interfaccia a riga di comando di AWS (AWS CLI): fornisce i comandi per una vasta gamma di servizi AWS, tra cui Amazon VPC, ed è supportata da Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- SDK di AWS: forniscono interfacce API specifiche per ogni lingua e si occupano di molti dettagli della connessione, ad esempio il calcolo delle firme e la gestione dei tentativi di richiesta e degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'API di interrogazione è il modo più diretto per accedere ad Amazon VPC, ma richiede che la propria applicazione gestisca dettagli di basso livello, come la generazione di un hash per la firma della richiesta e la gestione degli errori. Per ulteriori informazioni, consulta il documento Riferimento alle API di Amazon EC2.

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.

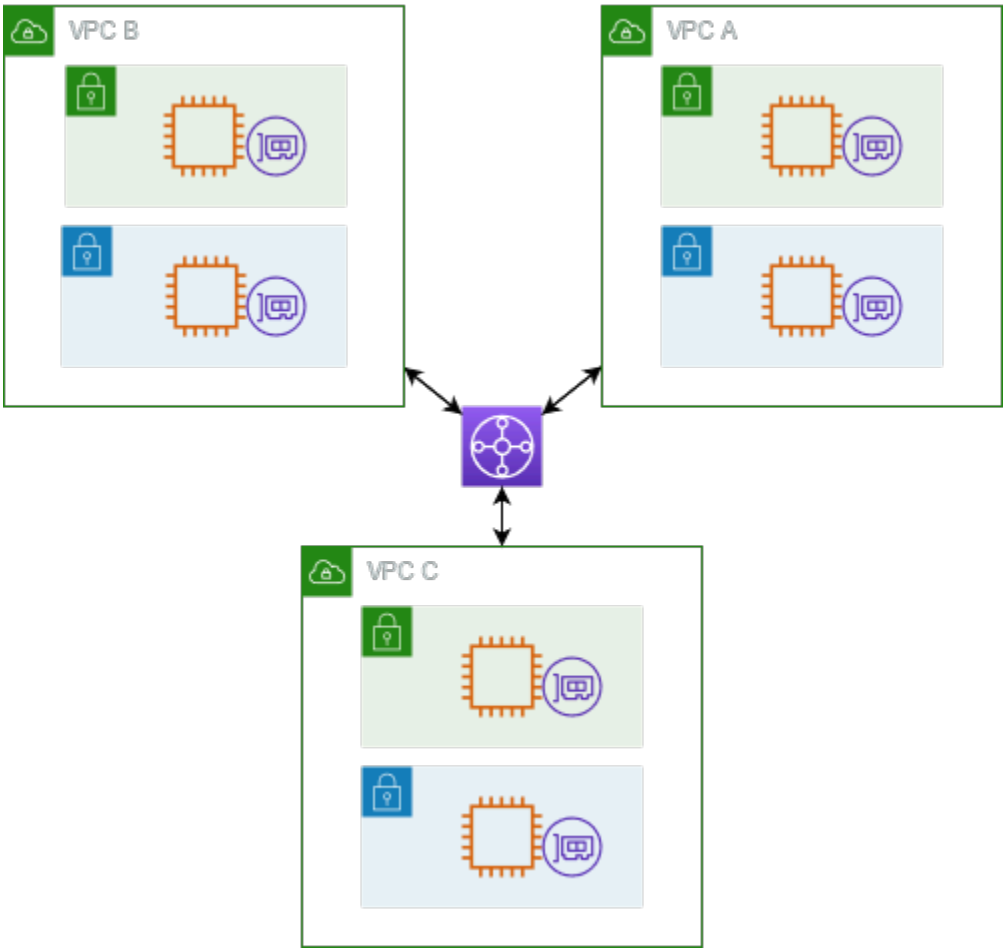
Come funzionano i gateway di transito

Un gateway di transito svolge le funzioni di router virtuale regionale per il traffico che viaggia tra i VPC (Virtual Private Cloud) 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.

Indice

Diagramma architetturale

Il seguente diagramma mostra un gateway di transito con tre collegamenti VPC. La tabella di routing per ciascuno di questi VPC include il routing locale e i routing che inviano il traffico destinato agli altri due VPC 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 blocchi CIDR per ogni VPC si propagano alla tabella di instradamento. Pertanto, ogni collegamento può instradare i pacchetti agli altri due collegamenti.

Destinazione	Target	Tipo di route
VPC A CIDR	*Collegamento per VPC A*	propagata
VPC B CIDR	*Collegamento per VPC B*	propagata
VPC C CIDR	*Collegamento per 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 più VPC. AWS Transit Gateway implementa un'interfaccia di rete elastica all'interno delle sottoreti VPC, 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.
- Una o più connessioni VPN
- AWS Direct Connect Uno o più gateway
- Uno o più allegati Transit Gateway Connect
- Una o più connessioni di peering del gateway di transito
- Un collegamento del gateway di transito alla VPN costituisce sia una sorgente che una destinazione di pacchetti

Instradamento Equal Cost Multipath

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

- VPC: VPC non supporta ECMP poiché i blocchi CIDR non possono sovrapporsi. Ad esempio, non è possibile collegare un VPC con un CIDR 10.1.0.0/16 con un secondo VPC che utilizza lo stesso CIDR a un gateway di transito e quindi configurare l'instradamento per bilanciare il carico del traffico tra di essi.
- VPN: quando l'opzione di supporto VPN ECMP è disabilitata, un gateway di transito utilizza parametri interni per determinare il percorso preferito in caso di prefissi uguali su più percorsi. Per ulteriori informazioni sull'attivazione o la disattivazione di ECMP per un collegamento VPN, consulta the section called “Gateway di transito”.

- AWS Transit Gateway Connect: gli allegati AWS Transit Gateway Connect supportano automaticamente ECMP.
- AWS Direct Connect Gateway: gli allegati del AWS Direct Connect gateway supportano automaticamente l'ECMP su 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 supporta ECMP poiché non supporta l'instradamento dinamico né è possibile configurare lo stesso percorso statico su due destinazioni diverse.

> **Note**
>
> - BGP Multipath AS-Path Relax non è supportato, quindi non è possibile utilizzare ECMP su diversi numeri di sistema autonomi (ASN).
> - ECMP non è supportato tra diversi tipi di collegamenti. Ad esempio, non è possibile abilitare ECMP tra una VPN e un collegamento VPC. 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 su più interfacce virtuali di transito. Pertanto, si consiglia di configurare e utilizzare un solo gateway Direct Connect e di non configurare e utilizzare più gateway per sfruttare ECMP. Per ulteriori informazioni sui gateway Direct Connect e sulle interfacce virtuali pubbliche, vedi Come si configura una connessione Direct Connect attiva/attiva o attiva/passiva da AWS un'interfaccia virtuale pubblica? .

Zone di disponibilità

Quando si collega un VPC a un gateway di transito, è necessario abilitare una o più zone di disponibilità che il gateway di transito utilizza per indirizzare il traffico verso le risorse nelle sottoreti del VPC. 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 instradato a tutte le sottoreti nel VPC, 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 si prevede di configurare un'appliance di rete con stato nel VPC, è possibile abilitare il supporto della modalità appliance per l'allegato VPC in cui si trova l'appliance. Ciò garantisce che il gateway di transito utilizzi la stessa zona di disponibilità per l'allegato VPC per tutta la durata di un flusso di traffico tra origine e destinazione. Consente inoltre al gateway di transito di inviare traffico a qualsiasi zona di disponibilità nel VPC, a condizione che vi sia un'associazione di subnet in tale zona. Per ulteriori informazioni, consulta Esempio: appliance in un VPC di servizi condivisi.

Routing

Il gateway di transito instrada i pacchetti IPv4 e IPv6 tra allegati utilizzando le tabelle di route del gateway di transito. Puoi configurare queste tabelle di routing per propagare gli instradamenti dalle tabelle di routing per i VPC collegati, le connessioni VPN e i gateway 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.

Indice

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 colleghi un VPC a un gateway di transito, devi aggiungere un instradamento alla tabella di routing della sottorete affinché il traffico sia instradato attraverso il gateway di transito. Per maggiori informazioni, consulta Routing per un gateway di transito nella Guida per l'utente di Amazon VPC.

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 allegato VPC, i blocchi CIDR del VPC vengono propagati alla tabella di instradamento del gateway di transito.

Quando il routing dinamico viene utilizzato con un allegato VPN o un allegato gateway Direct Connect, è possibile propagare le route apprese dal router on-premise tramite BGP a qualsiasi tabella di routing del transit gateway.

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

Per un allegato Connect, i routing nella tabella di instradamento associati all'allegato Connect vengono pubblicizzati alle appliance virtuali di terze parti, come le appliance SD-WAN, in esecuzione in un VPC tramite BGP.

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 instradato al gateway di transito peer può quindi essere instradato agli allegati VPC e VPN 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.
- Se le route hanno lo stesso indirizzo IP di destinazione ma target diversi, la priorità della route è la seguente:
  - Route statiche (ad esempio, route statiche Site-to-Site VPN)
  - Route referenziate dell'elenco di prefissi
  - Route propagate VPC
  - Route propagate del gateway Direct Connect
  - Route propagate Transit Gateway Connect
  - Percorsi propagati privati da sito a sito VPN
  - Percorsi VPN pubblici propagati da sito a sito
  - Instradamenti propagati tramite peering di Transit Gateway (Cloud WAN)

Transit Gateway mostra solo una route preferita. Una route di backup verrà visualizzata solo nella tabella di routing Transit Gateway se tale route non è più pubblicizzata. Ad esempio, se pubblicizzi gli

stessi percorsi tramite il gateway Direct Connect e tramite la VPN Site-to-Site. AWS Transit Gateway mostrerà solo le rotte ricevute dalla rotta gateway Direct Connect, che è la rotta preferita. La Site-to-Site VPN, che è il routing di backup, verrà visualizzata solo quando il gateway Direct Connect non viene più pubblicizzato.

Differenze tra le tabelle di routing tra VPC e gateway di transito

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

L'esempio seguente mostra una tabella di routing VPC. Il route VPC locale ha la priorità più alta, seguito dai route 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 del gateway di transito. Se si preferisce l'allegato gateway AWS Direct Connect all'allegato VPN, utilizzare una connessione VPN BGP e propagare le route nella tabella di instradamento 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

Destinazione	Allegato (target)	Tipo di risorsa	Tipo di route	Priorità
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

Nozioni di base sui gateway di transito

Le seguenti attività consentono di acquisire familiarità con i gateway di transito. Si creerà un gateway di transito e quindi si collegherà due VPC utilizzando il gateway di transito.

Processi

- Prerequisiti
- Fase 1: creazione del gateway di transito
- Fase 2: collegare il VPC al gateway di transito
- Fase 3: aggiungere le route tra il gateway di transito e i VPC
- Fase 4: testa il gateway di transito
- Fase 5: eliminare il gateway di transito

Prerequisiti

- Per dimostrare un semplice esempio di utilizzo di un gateway di transito, creare due VPC nella stessa regione. I VPC non possono avere CIDR sovrapposti. Avviare un'istanza Amazon EC2 in ogni VPC. Per ulteriori informazioni, consulta le Nozioni di base su Amazon VPC nella Guida per l'utente di Amazon VPC.
- Non è possibile avere route identiche che puntano a due diversi VPC. Un gateway di transito non propaga i CIDR di un VPC appena collegato se esiste una rotta identica nelle tabelle di route 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 per i gateway di transito.
- Non è possibile eseguire il ping tra gli host se non hai aggiunto una regola ICMP a ciascuno dei gruppi di sicurezza dell'host. Per ulteriori informazioni, consulta Utilizzo dei gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel selettore della regione, selezionare la regione utilizzata per la creazione del VPC.
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. In Amazon side Autonomous System Number (ASN lato Amazon), inserire ASN privato per il gateway di transito. Dovrebbe essere l'ASN del lato AWS di una sessione Border Gateway Protocol (BGP).

   Per ASN a 16 bit l'intervallo va da 64512 a 65534.

   Per ASN a 32 bit l'intervallo va da 4200000000 a 4294967294.

   Se si dispone di una distribuzione tra regioni, si consiglia di utilizzare un ASN univoco per ognuno dei propri gateway di transito.
8. (Facoltativo) È possibile modificare le impostazioni predefinite qualora fosse necessario disabilitare il supporto DNS o se non si desidera utilizzare la tabella di routing predefinita per le associazioni o la tabella di routing predefinita per la propagazione.
9. Selezionare Create Transit Gateway (Crea gateway di transito). Quando il gateway viene creato, lo stato iniziale del gateway di transito è `pending`.

Fase 2: collegare il VPC 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. Creare un collegamento per ogni VPC.

Verificare di aver creato due VPC e di aver avviato un'istanza EC2 in ognuno di essi, come descritto in Prerequisiti.

Creare un collegamento del gateway di transito a un VPC

1. Accedere alla console Amazon VPC 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. In Attachment type (Tipo collegamento), selezionare VPC.
7. Selezionare se abilitare il DNS support (Supporto DNS). in questa esercitazione, non abilitare IPv6 support (Supporto IPv6).
8. Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito.
9. In Subnet IDs (ID sottoreti), selezionare una sottorete per ogni zona di disponibilità che deve essere utilizzata 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 Casi d'uso di esempio.

Fase 3: aggiungere le route tra il gateway di transito e i VPC

Una tabella di routing include percorsi dinamici e statici che determinano il segmento di rete successivo per i VPC associati in 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 maggiori informazioni, consulta Routing per un gateway di transito nella Guida per l'utente di Amazon VPC.

Per aggiungere una nuova route a una tabella di routing di un VPC

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Route Tables (Tabelle di routing).
3. Selezionare la tabella di instradamento personalizzata associata al VPC.
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. Seleziona Salva modifiche.

Fase 4: testa il gateway di transito

È possibile verificare che il gateway di transito sia stato creato correttamente collegandosi a un'istanza Amazon EC2 in ciascun VPC e quindi inviando dati tra di esse, ad esempio tramite un comando ping. Per ulteriori informazioni, consultare Connessione a un'istanza Linux o Connessione a un'istanza Windows.

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. Accedere alla console Amazon VPC 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.

Best practice per la progettazione di gateway di transito

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

- Utilizza una sottorete separata per ogni allegato VPC del gateway di transito. Per ogni sottorete, utilizza 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:
  - Utilizza liste di controllo degli accessi di rete in ingresso e in uscita associate alle sottoreti aperte in Transit Gateway.
  - A seconda del flusso di traffico, puoi applicare liste di controllo degli accessi di rete alle sottoreti del carico di lavoro.
- Crea una lista di controllo degli accessi di rete e associala a tutte le sottoreti associate al gateway di transito. Mantieni aperta la lista di controllo degli accessi di rete in entrata e in uscita.
- Associa la stessa tabella di routing VPC a tutte le sottoreti associate al gateway di transito, a meno che la progettazione di rete non richieda più tabelle di routing VPC (ad esempio, un VPC middle-box che instrada il traffico attraverso più gateway NAT).
- Utilizzare connessioni Site-to-Site VPN Border Gateway Protocol (BGP). 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 AWS Direct Connect gateway e gli allegati VPN Site-to-Site BGP.
- Durante la migrazione dal peering VPC all'utilizzo di un gateway di transito. Una mancata corrispondenza delle dimensioni MTU tra il peering VPC e il gateway di transito potrebbe causare il calo di alcuni pacchetti per il traffico asimmetrico. Aggiorna entrambi i VPC allo stesso tempo per evitare che i pacchetti jumbo cadano a causa della mancata corrispondenza delle 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 distribuzioni con più gateway di transito, ti consigliamo di utilizzare un Autonomous System Number univoco (ASN) per ciascuno dei gateway di transito. È anche possibile usare il peering tra

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

Di seguito, sono riportati i casi di utilizzo comuni per i 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.

Esempi

- Esempio: router centralizzato
- Esempio: VPC isolati
- Esempio: VPC isolati con servizi condivisi
- Esempio: gateway di transito in peering
- Esempio: Routing in uscita centralizzato verso Internet
- Esempio: appliance in un VPC di servizi condivisi

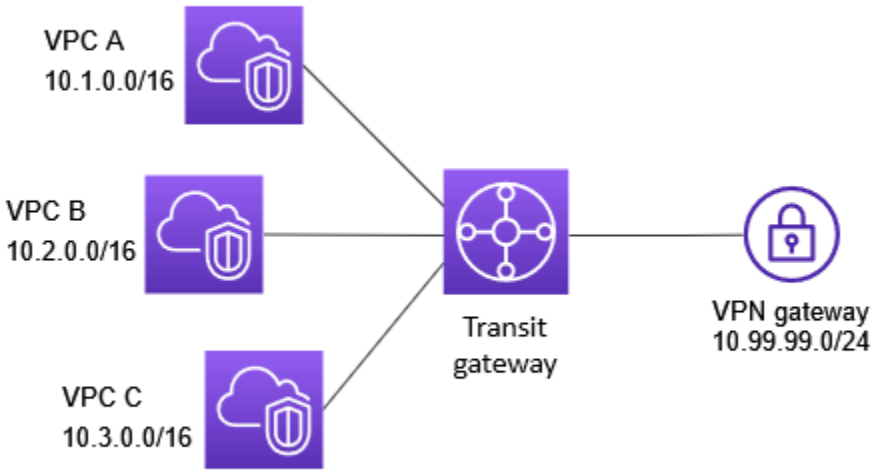
Esempio: router centralizzato

È possibile configurare il gateway di transito come router centralizzato che collega tutti i VPC, AWS Direct Connect e connessioni Site-to-Site VPN. 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

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



Risorse

Crea le seguenti risorse per questo scenario:

- Tre VPC. Per maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati VPC sul gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
- Un allegato VPN Site-to-Site nel gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di routing del gateway di transito. Quando la connessione VPN è attiva, viene stabilita la sessione BGP e la CIDR di VPN Site-to-Site si propaga alla tabella di routing del gateway di transito e tutti i CIDR VPC vengono aggiunti alla tabella BGP del gateway del cliente. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”.

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

Routing

Ogni VPC ha una tabella di routing ed esiste una tabella di routing per gateway di transito.

Tabelle di routing VPC

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è quella predefinita per il routing IPv4 locale nel VPC; questa voce permette alle istanze del VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito. La tabella seguente mostra i route 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	*Collegamento per VPC A*	propagata
10.2.0.0/16	*Collegamento per VPC B*	propagata
10.3.0.0/16	*Collegamento per VPC C*	propagata
10.99.99.0/24	*Collegamento per connessione VPN*	propagata

Tabella BGP gateway del cliente

La tabella BGP gateway del cliente contiene i seguenti CIDR VPC.

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

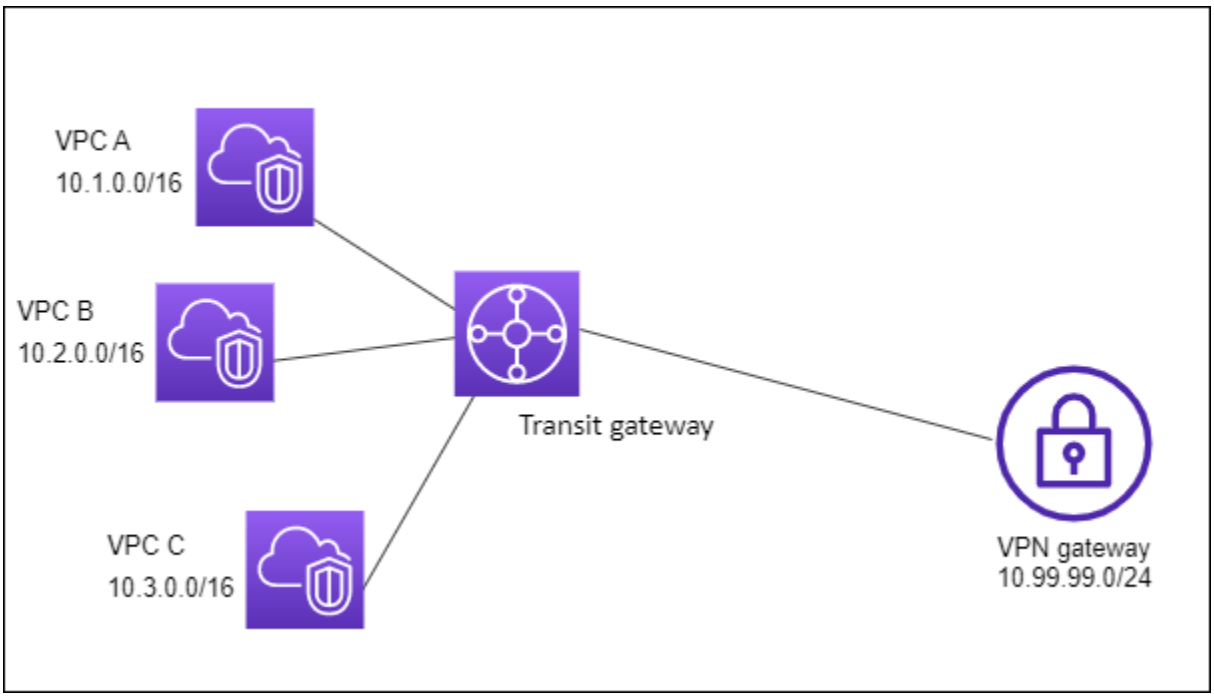
Esempio: VPC isolati

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 da VPC A, VPC B e VPC C instradano al gateway di transito. Pacchetti dalle sottoreti in VPC A, VPC B e VPC C che hanno Internet come primo routing della destinazione tramite il gateway di transito e poi il routing alla connessione VPN Site-to-Site (se la destinazione è all'interno di quella rete). I pacchetti da un VPC che hanno una destinazione di una sottorete in un altro VPC, ad esempio da 10.1.0.0 a 10.2.0.0, vengono instradati tramite il gateway di transito, dove vengono bloccati perché per questi non è specificato un route nella tabella di routing nel gateway di transito.



Risorse

Crea le seguenti risorse per questo scenario:

- Tre VPC. Per maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
- 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 tre VPC. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
- Un allegato Site-to-Site VPN nel gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”. Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN.

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

Routing

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

Tabelle di routing VPC A, VPC B e VPC C

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è quella predefinita per il routing locale IPv4 nel VPC. Questa voce consente alle istanze di questo VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito. La tabella seguente mostra i route VPC A.

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

Tabelle di routing del gateway di transito

In questo scenario viene utilizzata una tabella di instradamento per i VPC e una tabella di instradamento per la connessione VPN.

Gli allegati VPC sono associati alla seguente tabella di instradamento, che ha una route propagata per l'allegato VPN.

Destinazione	Target	Tipo di route
10.99.99.0/24	*Collegamento per connessione VPN*	propagata

L'allegato VPN è associato alla seguente tabella di instradamento, con route propagate per ciascuno degli allegati VPC.

Destinazione	Target	Tipo di route

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

Per ulteriori informazioni sulla propagazione delle route in una tabella di routing del gateway di transito, consulta Propagare una tabella di instradamento di un gateway di transito..

Tabella BGP gateway del cliente

La tabella BGP gateway del cliente contiene i seguenti CIDR VPC.

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

Esempio: VPC isolati con servizi condivisi

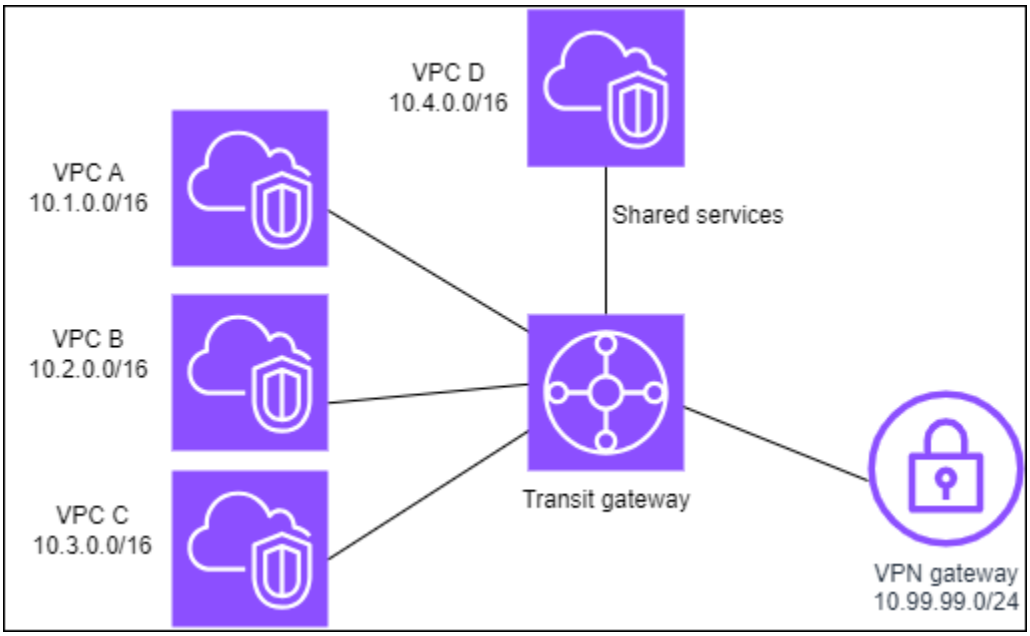
È possibile configurare il gateway di transito come molteplici router isolati che utilizzano un servizio condiviso. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. 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

- Risorse
- Routing

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. I pacchetti dalle sottoreti nel VPC A, VPC B e VPC C che hanno Internet come destinazione, vengono instradati prima tramite il gateway di transito, quindi verso il gateway del cliente per la VPN Site-to-Site. I pacchetti provenienti da sottoreti nel VPC A, VPC B o VPC C che hanno una destinazione di una sottorete in VPC A, VPC B o VPC C si instradano attraverso il gateway di transito, dove sono bloccati perché non vi è alcuna route per loro nella tabella di instradamento del gateway di transito. I pacchetti da VPC A, VPC B e VPC C che hanno VPC D come destinazione vengono instradati tramite il gateway di transito al VPC D.



Risorse

Crea le seguenti risorse per questo scenario:

- Quattro VPC. Per maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
- 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 “Creare un collegamento del gateway di transito a un VPC”.

- Un allegato Site-to-Site VPN nel gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”.

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

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

- Ogni VPC isolato è associato alla tabella di instradamento isolata ed è propagato alla tabella di instradamento condivisa.
- Ogni VPC dei servizi condivisi è associato alla tabella di instradamento isolata ed è propagato a entrambe le tabelle di instradamento.

Routing

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

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

Ogni VPC ha una tabella di instradamento con due voci. La prima voce è quella predefinita per il routing locale nel VPC; questa voce abilita la comunicazione tra le istanze in questo VPC. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	*ID gateway di transito*

Tabelle di routing del gateway di transito

In questo scenario viene utilizzata una tabella di instradamento per i VPC e una tabella di instradamento per la connessione VPN.

I collegamenti VPC A, B e C sono associati alla seguente tabella di instradamento, che ha una route propagata per il collegamento VPN e una route propagata per il collegamento VPC D.

Destinazione	Target	Tipo di route
10.99.99.0/24	*Collegamento per connessione VPN*	propagata
10.4.0.0/16	*Collegamento per VPC D*	propagata

Il collegamento VPN e i collegamenti VPC dei servizi condivisi (VPC D) sono associati alla seguente tabella di instradamento, che contiene voci che puntano a ciascuno dei collegamenti VPC. Ciò consente la comunicazione con i VPC dalla connessione VPN e dal VPC dei servizi condivisi.

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

Per ulteriori informazioni, consulta Propagare una tabella di instradamento di un gateway di transito..

Tabella BGP gateway del cliente

La tabella BGP del gateway del cliente contiene i CIDR per tutti e quattro i VPC.

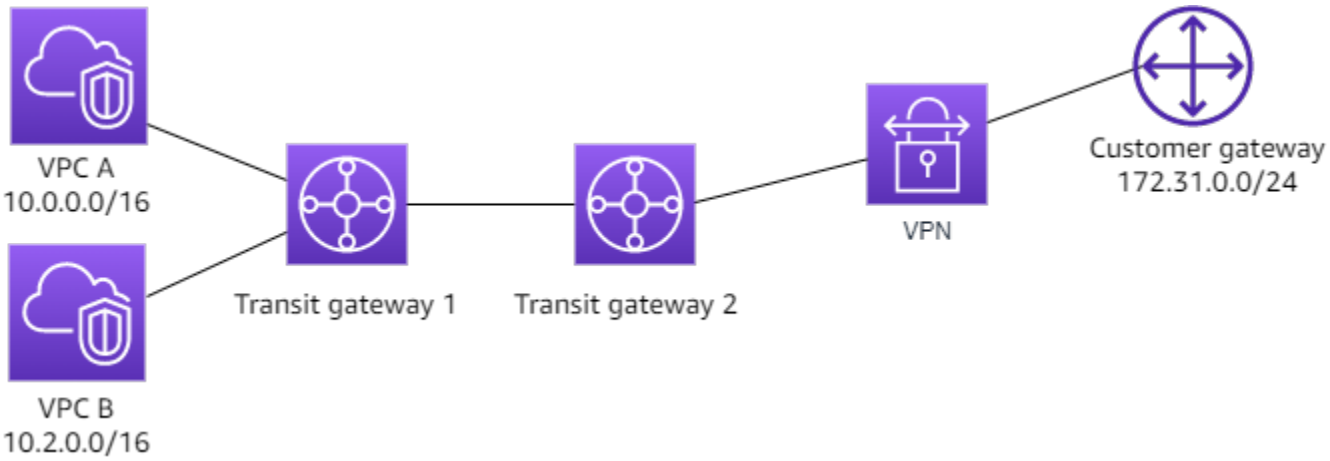
Esempio: gateway di transito in peering

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, tutti gli allegati VPC e VPN sono associati alla tabella di instradamento predefinita del gateway di transito e si propagano alla tabella di instradamento 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 dispone di due allegati VPC e il gateway di transito 2 dispone di un allegato Site-to-Site VPN. Pacchetti dalle sottoreti in VPC A e VPC B che hanno Internet come primo route di destinazione attraverso il gateway di transito 1, poi il gateway di transito 2 e quindi instradano alla connessione VPN.



Risorse

Crea le seguenti risorse per questo scenario:

- Due VPC. Per maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
- 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 allegati VPC sul primo gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
- Un allegato Site-to-Site VPN nel secondo gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una 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 Accessori di peering del gateway di transito.

Quando si creano gli allegati VPC, i CIDR per ogni VPC si propagano alla tabella di routing per il gateway di transito 1. Quando la connessione VPN è attiva, si verificano le seguenti operazioni:

- Viene stabilita la sessione BGP
- Il CIDR Site-to-Site VPN si propaga alla tabella di route per il gateway di transito 2
- I CIDR VPC vengono aggiunti alla tabella BGP del gateway del cliente

Routing

Ogni VPC ha una tabella di route e ogni gateway di transito ha una tabella di route.

Tabelle di routing VPC A e VPC B

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è quella predefinita per il routing locale IPv4 nel VPC. Questa voce predefinita consente alle risorse di questo VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito. La tabella seguente mostra i route 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	*ID allegato per VPC A*	propagata

Destinazione	Target	Tipo di route
10.2.0.0/16	*ID allegato per VPC B*	propagata
0.0.0.0/0	*ID allegato per la connessione di peering*	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	*ID allegato per connessione VPN*	propagata
10.0.0.0/16	*ID allegato per la connessione di peering*	static
10.2.0.0/16	*ID allegato per la connessione di peering*	static

Tabella BGP gateway del cliente

La tabella BGP gateway del cliente contiene i seguenti CIDR VPC.

- 10.0.0.0/16
- 10.2.0.0/16

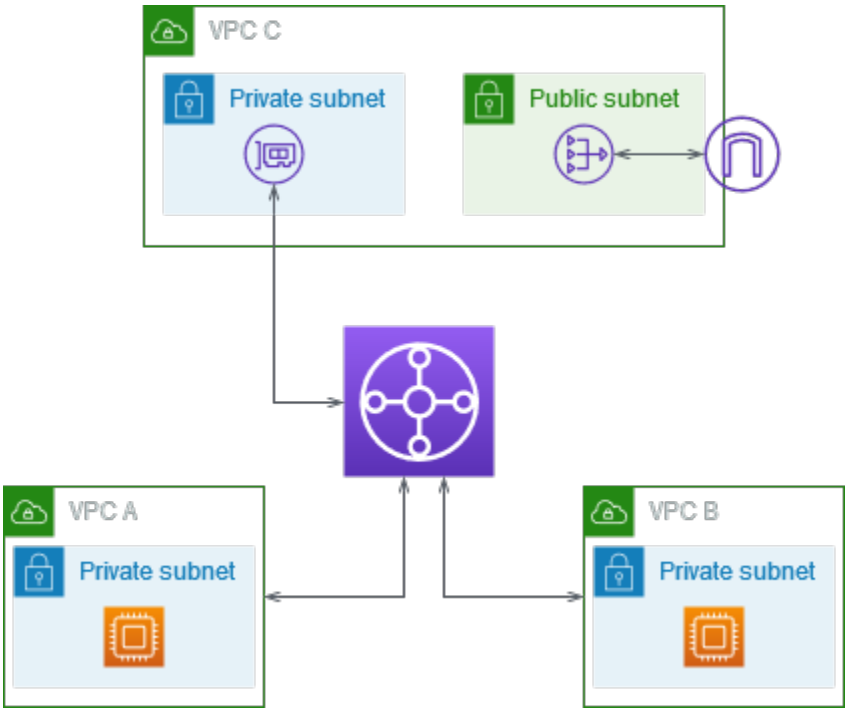
Esempio: Routing in uscita centralizzato verso Internet

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

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Sono presenti applicazioni in VPC A e VPC B che richiedono l'accesso a Internet solo in uscita. Puoi configurare il VPC C con un gateway NAT pubblico e un gateway Internet e una sottorete privata per il collegamento VPC. Connetti tutti i VPC 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 e arrivi a VPC C. Il gateway NAT in VPC C instrada il traffico al gateway Internet.



Risorse

Crea le seguenti risorse per questo scenario:

- Tre VPC con intervalli di indirizzi IP che non si sovrappongono. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- VPC A e VPC B hanno ognuno delle sottoreti private con istanze EC2.

- VPC C ha le seguenti caratteristiche:
  - Un gateway Internet collegato al VPC. Per ulteriori informazioni, consulta Creazione e collegamento di un gateway Internet nella Guida per l'utente di Amazon VPC.
  - Una sottorete pubblica con un gateway NAT. Per ulteriori informazioni, consulta Creazione di gateway NAT nella Guida per l'utente di Amazon VPC.
  - 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 allegati VPC sul gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di routing del gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”. Per il VPC C, è necessario creare il collegamento 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 il collegamento nella sottorete privata, il traffico viene indirizzato al gateway NAT e il gateway NAT invia il traffico al gateway Internet usando l'indirizzo IP elastico (EIP) come indirizzo IP di origine.

Routing

Sono presenti tabelle di routing per ogni VPC e una tabella di routing per il gateway di transito.

Tabelle di routing

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

Tabella di routing per VPC A

Di seguito è riportato un esempio di tabella di instradamento. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito.

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

Tabella di routing per VPC B

Di seguito è riportato un esempio di tabella di instradamento. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito.

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

Tabelle di instradamento per VPC C

Configura la sottorete pubblica con il gateway NAT aggiungendo una route 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 del VPC di comunicare tra loro. La seconda e la terza voce instradano il traffico per VPC A e VPC B al gateway di transito. La voce rimanente instrada tutto il resto del traffico della sottorete IPv4 al gateway Internet.

Destinazione	Target
VPC C CIDR	locale
VPC A CIDR	*transit-gateway-id*

Destinazione	Target
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 del VPC di comunicare tra loro. La seconda voce instrada tutto il resto del traffico della sottorete IPv4 al gateway NAT.

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 blocchi CIDR per ogni VPC si propagano alla tabella di instradamento del gateway di transito. La route statica invia il traffico Internet in uscita a VPC C. Puoi opzionalmente impedire la comunicazione tra VPC aggiungendo una route blackhole per ogni CIDR VPC.

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

CIDR	Collegamento	Tipo di routing
	Collegamento per VPC C	

Esempio: appliance in un VPC di servizi condivisi

È possibile configurare un accessorio (ad esempio un'appliance di sicurezza) in un VPC di servizi condivisi. Tutto il traffico instradato tra gli allegati del gateway di transito viene prima ispezionato dall'appliance nel VPC di servizi condivisi. Quando la modalità accessorio è abilitata, un gateway di transito seleziona un'unica interfaccia di rete nel VPC dell'appliance, utilizzando un algoritmo hash di flusso, 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. In questo modo, il traffico bidirezionale viene instradato simmetricamente: viene instradato attraverso la stessa zona di disponibilità nell'allegato VPC per tutta la durata del flusso. 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 al VPC dell'appliance per garantire l'aderenza del flusso. Il collegamento di più gateway di transito a un singolo VPC dell'appliance non garantisce l'aderenza del flusso in quanto i gateway di transito non condividono le informazioni sullo stato del flusso tra loro.

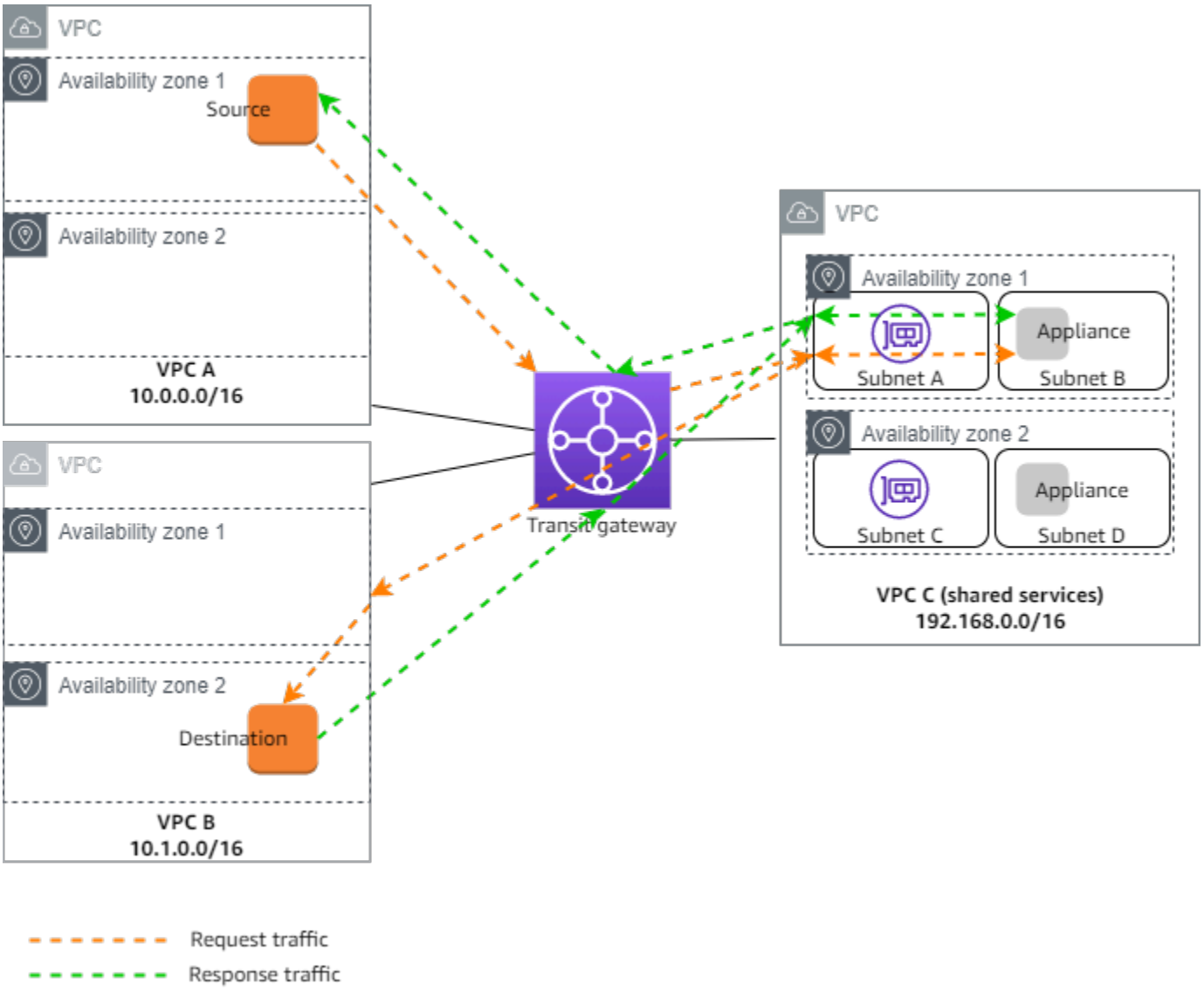
Important

- Il traffico in modalità appliance viene instradato correttamente a condizione che il traffico di fonte e di destinazione arrivi a un VPC centralizzato (VPC di ispezione) dallo stesso allegato del gateway di transito. Il traffico può diminuire se la fonte e la destinazione stanno entrando da due allegati diversi del gateway di transito. La modalità appliance non si applica al traffico in entrata nella rete tramite una VPN.
- L'attivazione della modalità accessorio 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 verso la zona di disponibilità di origine.

Indice

Panoramica

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



In questo scenario, si creano le seguenti risorse:

- Tre VPC. Per informazioni sulla creazione di un VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati VPC - uno per ciascuno dei VPC. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.

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

  Per l'allegato VPC per VPC C, attivare il supporto della modalità accessorio in modo che il traffico di risposta venga instradato alla stessa zona di disponibilità in VPC C del traffico di origine.

  La console Amazon VPC non supporta la modalità accessorio. Puoi anche usare l'API Amazon VPC, un SDK AWS o la AWS CLI per abilitare la modalità accessorio, oppure la AWS CloudFormation. Ad esempio, aggiungilo `--options ApplianceModeSupport=enable` al comando create-transit-gateway-vpc-attachment o modify-transit-gateway-vpc -attachment.

> **Note**
>
> La costanza del flusso in modalità appliance è garantita solo per il traffico di origine e di destinazione proveniente dal VPC di ispezione.

Appliance con stato e modalità appliance

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

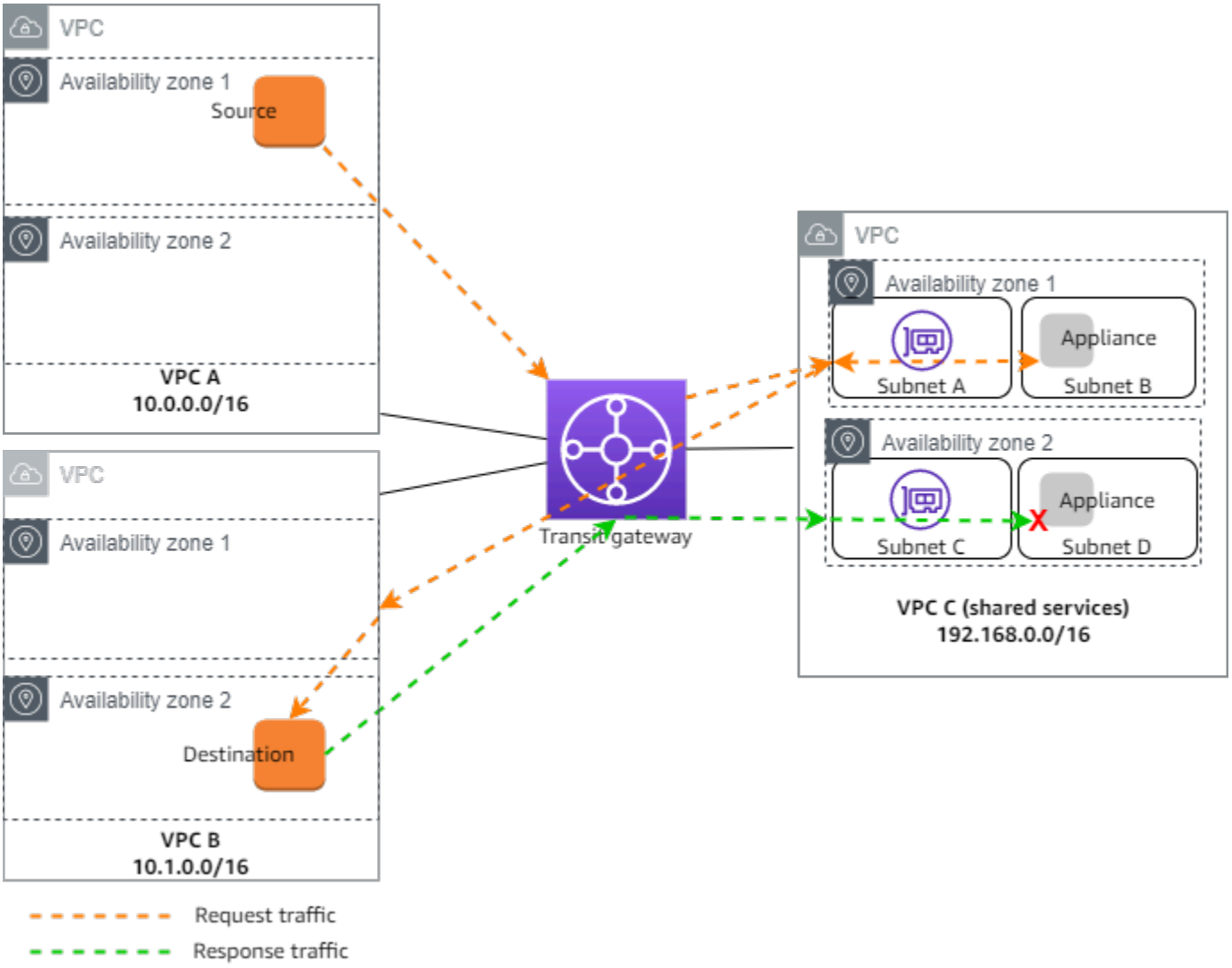
Per ulteriori informazioni, consulta Architettura di ispezione centralizzata nel blog AWS.

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 gli allegati VPC nella zona di disponibilità di origine fino a quando non raggiunge 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 vi sono subnet associate a un allegato VPC in tale zona di disponibilità.

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



Routing

Ogni VPC dispone di una o più tabelle di route e il gateway di transito dispone di due tabelle di route.

Tabelle di routing VPC

VPC A e VPC B

I VPC A e B hanno tabelle di percorso con 2 voci. La prima voce è quella predefinita per il routing locale IPv4 nel VPC. Questa voce predefinita consente alle risorse di questo VPC di comunicare tra loro. La seconda voce instrada tutto il rimanente traffico della sottorete IPv4 al gateway di transito. Di seguito è riportata la tabella dei percorsi per VPC A.

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

VPC C

Il VPC (VPC C) di servizi condivisi dispone di tabelle di route diverse per ogni sottorete. La sottorete A viene utilizzata dal gateway di transito (è possibile specificare questa sottorete quando si crea l'allegato VPC). 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 route per VPC A e VPC B e una tabella di route per i servizi condivisi VPC (VPC C).

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

Destinazione	Target	Tipo di route
0.0.0.0/0	*ID allegato per VPC C*	static

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

Destinazione	Target	Tipo di route
10.0.0.0/16	*ID allegato per VPC A*	propagata
10.1.0.0/16	*ID allegato per VPC B*	propagata

Utilizzo dei gateway di transito

È possibile utilizzare i gateway di transito con la console Amazon VPC o la AWS CLI.

Indice

Gateway di transito

Un Transit Gateway consente di collegare VPC e connessioni VPN e routing di traffico tra loro. Un gateway di transito funziona trasversalmente Account AWS e puoi usarlo AWS RAM per condividere il tuo gateway di transito con altri account. Dopo aver condiviso un gateway di transito con un altro Account AWS, il proprietario dell'account può collegare i propri VPC al gateway di transito. Un utente di uno qualsiasi degli account può eliminare il collegamento in qualsiasi momento.

È possibile abilitare il multicast in un gateway di transito, quindi creare un dominio del gateway di transito multicast che consenta l'invio del traffico multicast dall'fonte multicast ai membri del gruppo multicast tramite allegati VPC associati al dominio.

Ogni collegamento di VPC o VPN è associato a una singola tabella di instradamento. La tabella di routing 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 abilita CIDR e destinazioni sia per IPv4 che per IPv6. Le destinazioni sono VPC e connessioni VPN. Quando colleghi un VPC o crei una connessione VPN verso un gateway di transito, il collegamento viene associato alla tabella di routing predefinita del gateway di transito.

Puoi creare tabelle di routing aggiuntive all'interno del gateway di transito e modificare l'associazione di VPC o VPN in queste tabelle di routing. Tale azione consente la segmentazione della rete. Ad esempio, è possibile associare i VPC di sviluppo a una tabella di routing e i VPC di produzione a una tabella di routing diversa. Questo consente di creare reti isolate all'interno di un gateway di transito con caratteristiche simili a quelle di un VRF (Virtual Routing and Forwarding, Routing e Inoltro Virtuali) nelle reti tradizionali.

I gateway di transito supportano il routing dinamico e statico tra VPC e connessioni VPN collegate. Per ogni collegamento puoi abilitare o disabilitare la propagazione delle route. Gli allegati di peering del gateway di transito supportano solo il routing statico. Tuttavia, non è possibile aggiungere un percorso statico che punti a un peering tra due gateway di transito nella stessa regione.

Facoltativamente, puoi associare uno o più blocchi CIDR IPv4 o IPv6 al gateway di transito. Specifica un indirizzo IP dal blocco CIDR quando stabilisci un peer di Transit Gateway Connect per un collegamento Connect del gateway di transito. Puoi associare qualsiasi intervallo di indirizzi IP pubblici o privati, ad eccezione degli indirizzi nell'intervallo `169.254.0.0/16` e gli intervalli che si sovrappongono agli indirizzi per gli allegati VPC e le reti locali. Per ulteriori informazioni sui blocchi CIDR IPv4 e IPv6, consulta VPC e sottoreti nella Guida per l'utente di Amazon VPC.

Attività

- Creazione di un gateway di transito
- Visualizzazione dei gateway di transito
- Aggiungere o modificare i tag per un gateway di transito
- Modificare un gateway di transito
- Condividere un gateway di transito
- Accettare una condivisione di risorse
- Accettare un allegato condiviso
- Eliminare un gateway di transito

Creazione di un 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. 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. Accedere alla console Amazon VPC 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. In Amazon side Autonomous System Numbr (ASN lato Amazon), non modificare il valore predefinito per utilizzare l'Autonomous System Number (ASN) predefinito, oppure inserire l'ASN privato del gateway di transito. Dovrebbe essere l'ASN per il AWS lato di una sessione BGP (Border Gateway Protocol).

   Per ASN a 16 bit l'intervallo va da 64512 a 65534.

   Per ASN a 32 bit l'intervallo va da 4200000000 a 4294967294.

   Se si dispone di una distribuzione tra regioni, si consiglia di utilizzare un ASN univoco per ognuno dei propri gateway di transito.
7. In DNS support (supporto DNS), selezionare abilita se è necessario che il VPC risolva i nomi di host DNS IPv4 pubblici in indirizzi IPv4 privati quando richiesto da istanze in un altro VPC collegato al gateway di transito.
8. In supporto VPN ECMP, selezionare abilita se è necessario disporre del supporto per l'instradamento Equal Cost Multipath (ECMP) tra i tunnel VPN. Se le connessioni pubblicano gli stessi CIDR, il traffico viene distribuito uniformemente tra di esse.

   Quando selezioni questa opzione, l'ASN GBP annunciato, gli attributi BGP quali il percorso AS e le community per le preferenze devono essere uguali.

   > **Note**
   >
   > Per utilizzare ECMP, è necessario creare una connessione VPN che utilizzi il routing dinamico. Le connessioni VPN che utilizzano il routing statico non supportano ECMP.

9. 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.
10. 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.
11. (Facoltativo) Per utilizzare il gateway di transito come router per il traffico multicast, selezionare Multicast support (Supporto multicast).
12. In Auto accept shared attachments (Accetta automaticamente i collegamenti condivisi), selezionare abilita per accettare automaticamente i collegamenti multi-account.
13. (Facoltativo) In blocchi CIDR del gateway di transito, specifica uno o più blocchi CIDR IPv4 o IPv6 per il gateway di transito.

    Puoi specificare un blocco CIDR di dimensione /24 o superiore (ad esempio /23 o /22) per IPv4 o un blocco CIDR di dimensione /64 o superiore (ad esempio /63 o /62) per IPv6. Puoi quindi associare qualsiasi intervallo di indirizzi IP pubblici o privati, ad eccezione degli indirizzi nell'intervallo 169.254.0.0/16, e gli intervalli che si sovrappongono agli indirizzi degli allegati VPC e delle reti locali.
14. Selezionare Create transit gateway (Crea gateway di transito).

Per creare un gateway di transito utilizzando il AWS CLI

Utilizza il comando create-transit-gateway.

Visualizzazione dei gateway di transito

Per visualizzare i gateway di transito utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito). I dettagli del gateway di transito sono visualizzati sotto l'elenco dei gateway nella pagina.

Per visualizzare i gateway di transito utilizzando il AWS CLI

Utilizza il comando describe-transit-gateways.

Aggiungere o modificare i tag per un gateway di transito

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, consultare Tagging delle risorse Amazon EC2.

Aggiungere tag a un gateway di transito utilizzando la console

1. Accedere alla console Amazon VPC 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 per il quale 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. Selezionare Salva.

Modificare un gateway di transito

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

Modificare un gateway di transito

1. Accedere alla console Amazon VPC 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.

Condividere un gateway di transito

Puoi utilizzarlo AWS RAM per condividere un gateway di transito tra account o tra tutta l'organizzazione in AWS Organizations. Per condividere un gateway di transito di proprietà, attenersi alla procedura descritta di seguito.

Devi abilitare la condivisione delle risorse dall'account di gestione della tua organizzazione. Per informazioni sull'attivazione della condivisione delle risorse, consulta Enable Sharing with AWS Organizations nella AWS RAM User Guide.

Condividere un gateway di transito

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Selezionare Create a resource share (Crea una condivisione di risorse).
3. Sotto Name (Nome), digitare un nome descrittivo della risorsa da condividere.
4. In Select resource type (Seleziona tipo risorsa), selezionare Transit Gateways (Gateway di transito). Selezionare il gateway di transito.
5. (Facoltativo) In Principals (Responsabile), aggiungere i responsabili della condivisione di risorse. Per ogni Account AWS unità organizzativa o organizzazione, specifica il relativo ID e scegli Aggiungi.

   In Consenti account esterni, scegli se consentire la condivisione di questa risorsa con Account AWS utenti esterni all'organizzazione.
6. (Facoltativo) In Tags (Tag) digitare una chiave e un valore per ogni tag. Questi tag sono applicati alla condivisione di risorse ma non al gateway di transito.
7. Selezionare Create resource share (Crea condivisione di risorse).

Accettare una condivisione di risorse

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 Gateway di transito nella console Amazon VPC.

Accettare un allegato condiviso

Se non è stata abilitata la funzionalità Auto accept shared attachments (Accetta automaticamente allegati condivisi) al momento della creazione del gateway di transito, è necessario accettare manualmente gli allegati multiaccount (condivisi).

Per accettare manualmente un allegato condiviso

1. Accedere alla console Amazon VPC 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

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. Accedere alla console Amazon VPC 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.

Collegamenti del gateway di transito a un 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.
- Le risorse in un VPC collegato a un gateway di transito non possono accedere ai gruppi di sicurezza di un altro VPC anch'esso collegato allo stesso gateway di transito.
- Un gateway di transito non supporta la risoluzione DNS per i nomi DNS personalizzati dei VPC collegati impostati utilizzando zone ospitate private in Amazon Route 53. Per configurare la risoluzione dei nomi per le zone private ospitate per tutti i VPC collegati a un gateway di transito, consulta Gestione DNS centralizzata del cloud ibrido con Amazon Route 53 e Transit Gateway AWS.
- Un gateway di transito non supporta il routing tra VPC con CIDR identici. 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.

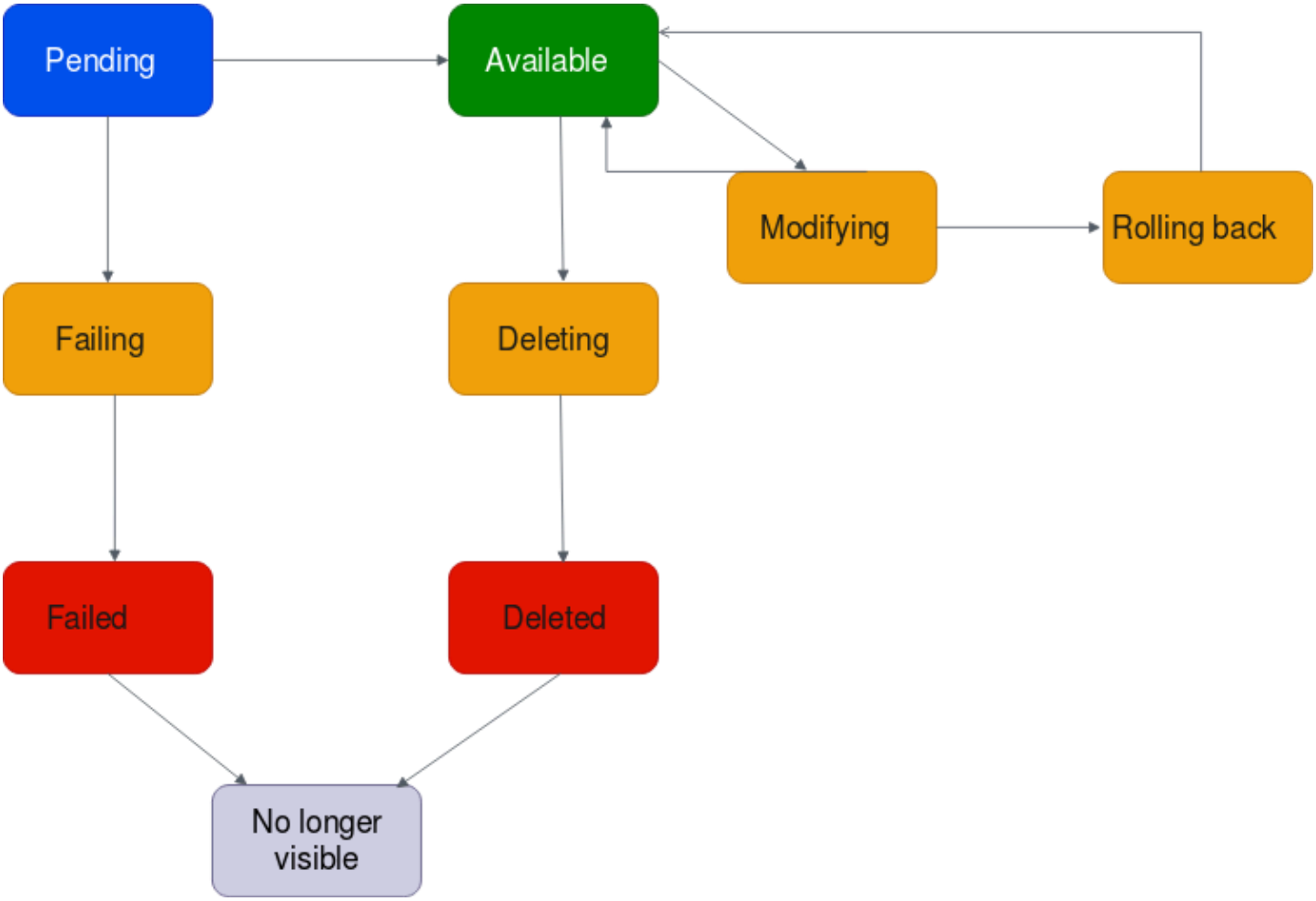
- Non è possibile creare un collegamento del gateway di transito alla VPN utilizzando sottoreti solo IPv6. Le sottoreti di collegamento del gateway di transito alla VPN devono supportare anche gli indirizzi IPv4.
- Un gateway di transito deve avere almeno un allegato VPC prima di poter essere aggiunto a una tabella di routing.

Indice

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.

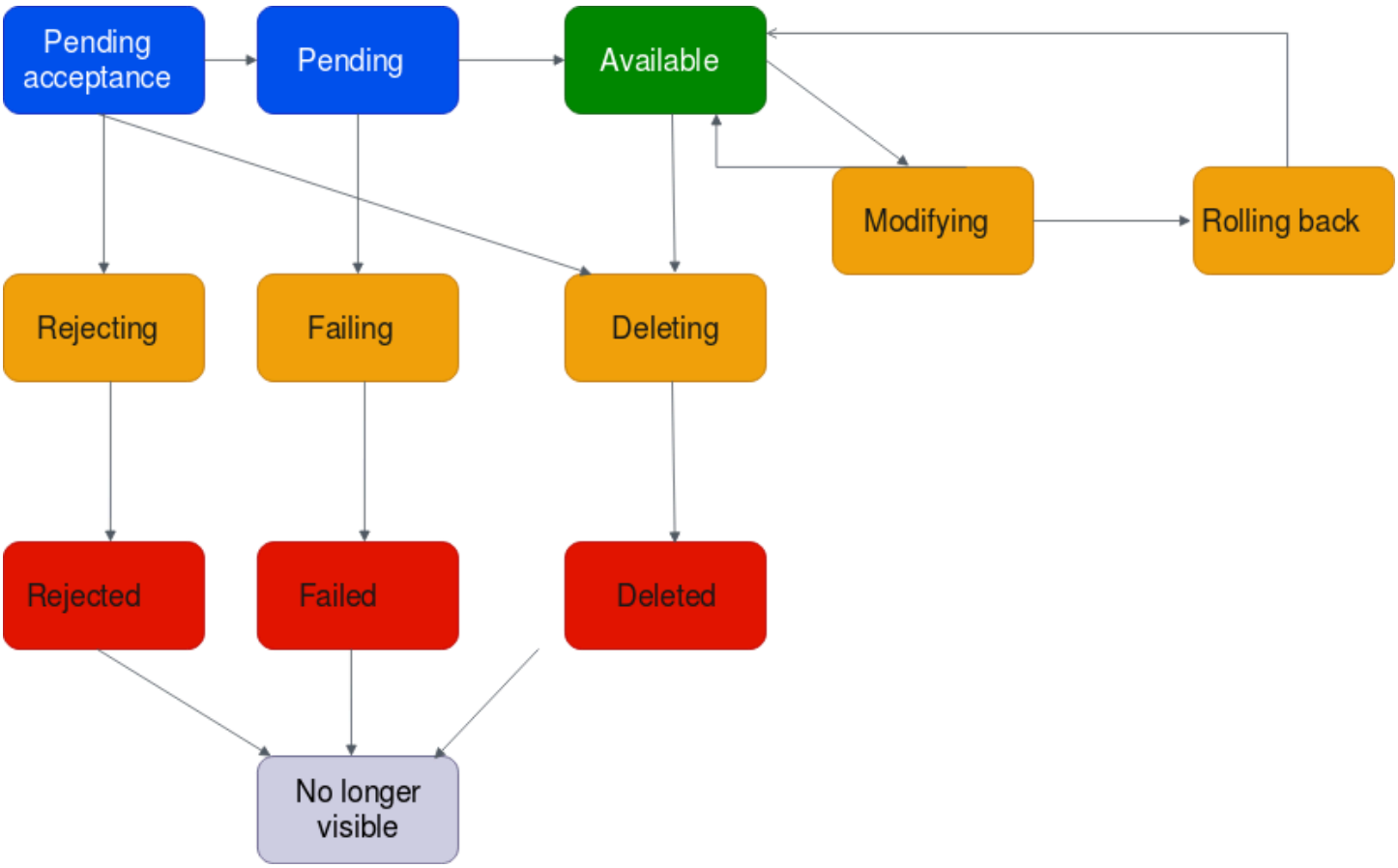
Il diagramma seguente mostra gli stati che un collegamento può avere nella configurazione di un unico account o nella configurazione di più account per cui è attivata l'opzione Accetta automaticamente collegamenti condivisi.



- 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`.

Creare un collegamento del gateway di transito a un VPC

Per creare un collegamento a un VPC utilizzando la console

1. Accedere alla console Amazon VPC 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. In Attachment type (Tipo collegamento), selezionare VPC.
7. Scegli se abilitare il supporto DNS, il supporto IPv6 e il supporto in modalità 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'allegato VPC per tutta la durata di quel flusso.

8. Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito.

   Questo VPC deve possedere almeno una sottorete associata ad esso.

9. In Subnet IDs (ID sottoreti), selezionare una sottorete per ogni zona di disponibilità che deve essere utilizzata 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).

Per creare un allegato VPC utilizzando il AWS CLI

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

Modificare i collegamenti al VPC

Per modificare i collegamenti al VPC utilizzando la console

1. Accedere alla console Amazon VPC 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'allarme, quindi scegliere Actions (Azioni), Modifica collegamento del gateway di transito.
4. Per abilitare il supporto DNS, selezionare DNS support (Supporto DNS).
5. Per aggiungere una sottorete al collegamento, selezionare la casella accanto alla sottorete.

   L'aggiunta o la modifica di una sottorete di allegati VPC potrebbe influire sul traffico dei dati mentre l'allegato è in uno stato di modifica.

6. Scegliere Modifica collegamento del gateway di transito.

Per modificare gli allegati VPC utilizzando il AWS CLI

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

Modificare i tag dei collegamenti al VPC

Per modificare i tag dei collegamenti al VPC utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare il collegamento VPC, quindi scegliere Actions (Azioni), Manage tags (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. Selezionare Salva.

I tag degli allegati VPC possono essere modificati solo utilizzando la console.

Visualizzare i collegamenti al VPC

Per visualizzare i collegamenti al VPC utilizzando la console

1. Accedere alla console Amazon VPC 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, cercaVPC. Questi sono gli allegati del VPC.
4. Selezionare un collegamento per visualizzarne i dettagli.

Per visualizzare gli allegati VPC utilizzando il AWS CLI

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

Eliminare un collegamento a un VPC

Per eliminare un collegamento a un VPC utilizzando la console

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare un collegamento a un VPC.
4. Scegliere Operazioni,Eliminare l'allegato del gateway.
5. Quando richiesto, digitare **`delete`** e scegliere Delete (Elimina).

Per eliminare un allegato VPC utilizzando il AWS CLI

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

Risoluzione dei problemi relativi alla creazione del collegamento VPC

Nel seguente argomento viene descritto come risolvere i problemi che si possono verificare quando si crea un collegamento VPC.

Problema

Il collegamento VPC non è riuscito.

Causa

Di seguito è riportata la possibile causa:

1. L'utente che sta creando il collegamento VPC non dispone delle autorizzazioni corrette per creare un ruolo collegato al servizio.
2. C'è un problema di limitazione a causa delle troppe richieste IAM, ad esempio si utilizza 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 Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM. Dopo che l'utente riceve le autorizzazioni, creare il collegamento VPC.

2. Creare manualmente il collegamento VPC tramite la console o l'API. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un 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 “Visualizzazione dei gateway di transito”.

Collegamenti del gateway di transito a una VPN

Per collegare una connessione VPN a un gateway di transito è necessario specificare il gateway del cliente. Per ulteriori informazioni sui requisiti per il gateway del cliente, consulta Requisiti per il gateway del cliente nella Guida per l'utente AWS Site-to-Site VPN .

Per le VPN statiche, aggiungere le route statiche alla tabella di route del gateway di transito.

Creare un collegamento del gateway di transito a una VPN

Per creare un collegamento a una VPN utilizzando la console

1. Accedere alla console Amazon VPC 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. In Attachment type (Tipo collegamento), selezionare 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 gateway del cliente si trova dietro un dispositivo NAT abilitato per NAT Traversal (NAT-T), utilizzare l'indirizzo IP pubblico del dispositivo NAT e modificare le regole del firewall per sbloccare la porta UDP 4500.
   - Per creare un gateway del cliente, selezionare New (Nuovo), quindi in IP Address (Indirizzo IP), inserire un indirizzo IP pubblico statico e il BGP ASN (ASN BGP).

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

7. In Tunnel Options (Opzioni tunnel), specifica gli intervalli CIDR e le chiavi pre-condivise per il tuo tunnel. Per ulteriori informazioni, consulta Architetture Site-to-Site VPN.
8. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).

Per creare un allegato VPN utilizzando il AWS CLI

Utilizza il comando create-vpn-connection.

Visualizzare i collegamenti alla VPN

Per visualizzare i collegamenti alla VPN utilizzando la console

1. Accedere alla console Amazon VPC 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, cercaVPN. Questi sono gli allegati VPN.
4. Selezionare un collegamento per visualizzarne i dettagli o aggiungere tag.

Per visualizzare gli allegati VPN utilizzando il AWS CLI

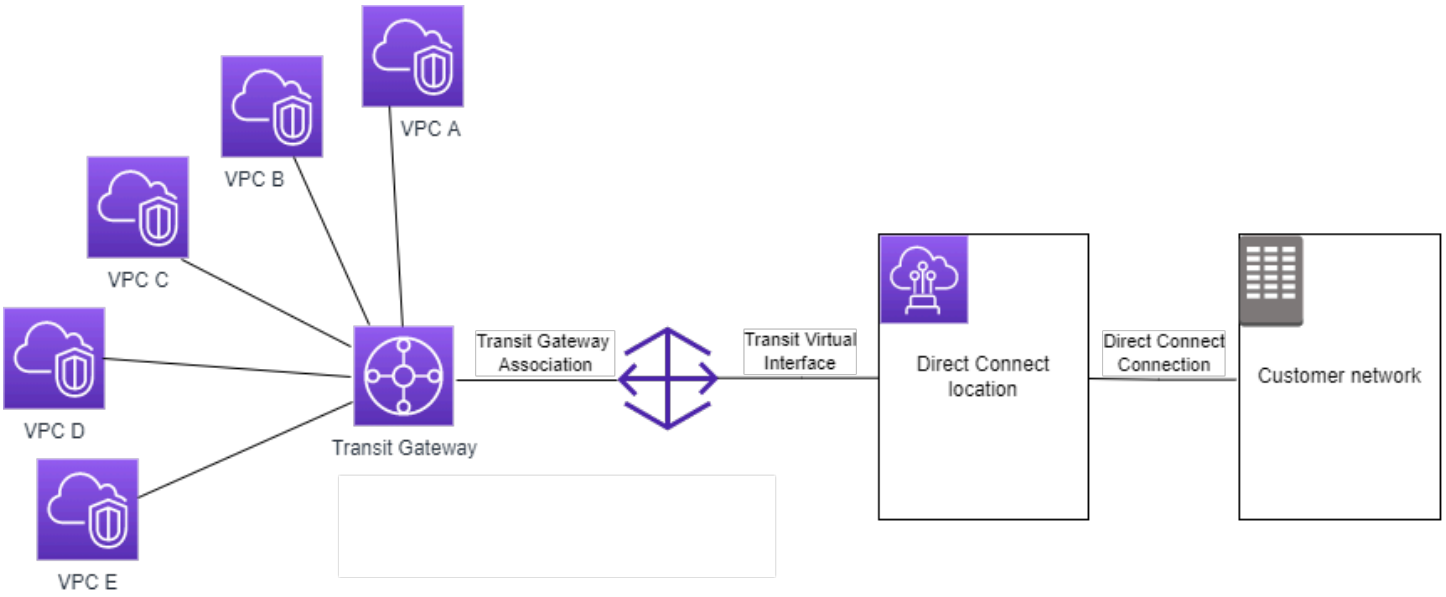
Utilizza il comando describe-transit-gateway-attachments.

Collegamenti di un gateway di transito a un gateway Direct Connect.

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

- Gestire un'unica connessione per più VPC o VPN che si trovano nella stessa regione.
- Pubblicare prefissi da ambienti locali ad AWS e da AWS ad ambienti locali.

Il seguente diagramma illustra il modo in cui il gateway Direct Connect consente di creare un'unica connessione alla connessione Direct Connect che può essere utilizzata da tutti i VPC.



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.

Accessori di peering del gateway di transito

Puoi eseguire il peering di due gateway di transito nella regione e tra regioni e instradare il traffico (sia IPv4 che IPv6) tra loro. 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 in un altro Account AWS.

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.

È consigliabile utilizzare ASN univoci per i gateway di transito peer per sfruttare le future funzionalità di propagazione della route.

Il peering del gateway di transito non supporta la risoluzione dei nomi host DNS IPv4 pubblici o privati in indirizzi IPv4 privati su VPC su entrambi i lati del collegamento peering del gateway di transito alla VPN utilizzando il Amazon Route 53 Resolver in un'altra Regione. 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 sui 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 i collegamenti peering dei gateway di transito, consulta Domande frequenti su AWS Transit Gateway.

Creare un allegato di peering

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, assicurarsi di disporre dell'ID Account AWS 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. Accedere alla console Amazon VPC 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 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.
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 si trova in un Account AWS diverso, scegliere 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 l AWS CLI

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

Accettare o rifiutare una richiesta di allegato peering

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. Accedere alla console Amazon VPC 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. Accedere alla console Amazon VPC 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 la AWS CLI

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

Aggiungere una route alla tabella di route del gateway di transito

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. Accedere alla console Amazon VPC 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 Create static route (Crea route statico), immettere il blocco CIDR per cui creare una route. Ad esempio, specificare il blocco CIDR di un VPC 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 route statica mediante la AWS CLI

Utilizzare 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 routing di un gateway di transito.”.

Visualizzare gli allegati di connessione peering del gateway di transito

È possibile visualizzare gli allegati di peering del gateway di transito e le informazioni su di essi.

Per visualizzare gli allegati di peering utilizzando la console

1. Accedere alla console Amazon VPC 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 Peering. Questi sono gli allegati di peering.
4. Selezionare un collegamento per visualizzarne i dettagli.

Per visualizzare gli allegati di peering del gateway di transito utilizzando l'opzione AWS CLI

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

Eliminare un allegato di peering

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. Accedere alla console Amazon VPC 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 l AWS CLI

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

Considerazioni sulle regioni AWS di attivazione

Puoi eseguire il peering dei gateway di transito attraverso i confini della regione di attivazione. Per informazioni su queste regioni e su come attivarle, consulta Gestione delle regioni AWS nella Riferimenti generali di Amazon Web Services. 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 il collegamento peering:
  - ID Account AWS
  - 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.

Collegamenti di Transit gateway Connect e peer di Transit Gateway Connect

Puoi creare un collegamento Connect del gateway di transito per stabilire una connessione tra un gateway di transito e appliance virtuali di terze parti (ad esempio le appliance SD-WAN) in esecuzione in un VPC. Un collegamento Connect supporta il protocollo del tunnel GRE (Generic Routing Encapsulation) per prestazioni elevate e Border Gateway Protocol (BGP) per il routing

dinamico. Dopo aver creato un collegamento Connect, puoi creare uno o più tunnel GRE (detti anche peer di Transit Gateway Connect) sul collegamento Connect in modo da connettere il gateway di transito e l'appliance di terze parti. In questo modo vengono stabilite due sessioni BGP attraverso il tunnel GRE per scambiare informazioni di routing.

> **Important**
>
> Un peer di Transit Gateway Connect è costituito da due sessioni di peering BGP che terminano sull'infrastruttura gestita da AWS. Le due sessioni di peering BGP forniscono la ridondanza del piano di routing, assicurando che la perdita di una sessione di peering BGP non influisca sulle operazioni di routing. Le informazioni di routing ricevute da entrambe le sessioni BGP vengono accumulate per il peer di Connect specificato. Le due sessioni di peering BGP proteggono anche da qualsiasi operazione sull'infrastruttura AWS come manutenzione ordinaria, applicazione di patch, aggiornamenti hardware e sostituzioni. Se il peer di Connect funziona senza la sessione di peering BGP doppia consigliata e configurata per la ridondanza, potrebbe verificarsi una momentanea perdita di connettività durante le operazioni sull'infrastruttura AWS. Consigliamo vivamente di configurare entrambe le sessioni di peering BGP sul peer di Connect. Se più peer di Connect sono stati configurati per supportare l'elevata disponibilità lato appliance, si consiglia di configurare entrambe le sessioni di peering BGP su ciascuno dei peer di Connect.

Un collegamento Connect utilizza un collegamento VPC o Direct Connect esistente come meccanismo di trasporto sottostante. Questo è detto collegamento di trasporto. Il gateway di transito identifica i pacchetti GRE corrispondenti dell'appliance di terze parti come traffico proveniente dal collegamento Connect. Tutti gli altri pacchetti, inclusi i pacchetti GRE con informazioni di origine o di destinazione errate, verranno trattati come traffico proveniente dal collegamento di trasporto.

> **Note**
>
> Per utilizzare un allegato Direct Connect come meccanismo di trasporto, devi prima integrare Direct Connect con il gateway di transito di AWS. Per le istruzioni per creare questa integrazione, consulta Integra i dispositivi SD-WAN con il gateway di transito AWS e AWS Direct Connect.

Indice

Peer Connect

Un peer Connect (tunnel GRE) è costituito dai componenti riportati di seguito.

Blocchi CIDR interni (indirizzi BGP)

Gli indirizzi IP interni utilizzati per il peering BGP. Per IPv4 devi specificare un blocco /29 CIDR dall'intervallo `169.254.0.0/16`. Facoltativamente puoi specificare un blocco CIDR /125 dall'intervallo `fd00::/8` per IPv6. I seguenti blocchi CIDR 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

Il primo indirizzo dell'intervallo IPv4 deve essere configurato sull'appliance come indirizzo IP BGP. Se utilizzi IPv6, se il blocco CIDR interno è fd00::/125, allora dovrai configurare il primo indirizzo di questo intervallo (fd00::1) sull'interfaccia tunnel dell'appliance.

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

Indirizzo IP peer

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

Indirizzo gateway di transito

L'indirizzo IP peer (indirizzo IP esterno GRE) sul lato gateway di transito del peer Connect. L'indirizzo IP deve essere specificato dal blocco CIDR del gateway di transito e deve essere univoco tra i collegamenti Connect nel gateway di transito. Se non specifichi un indirizzo IP, verrà utilizzato il primo indirizzo disponibile dal blocco CIDR del gateway di transito.

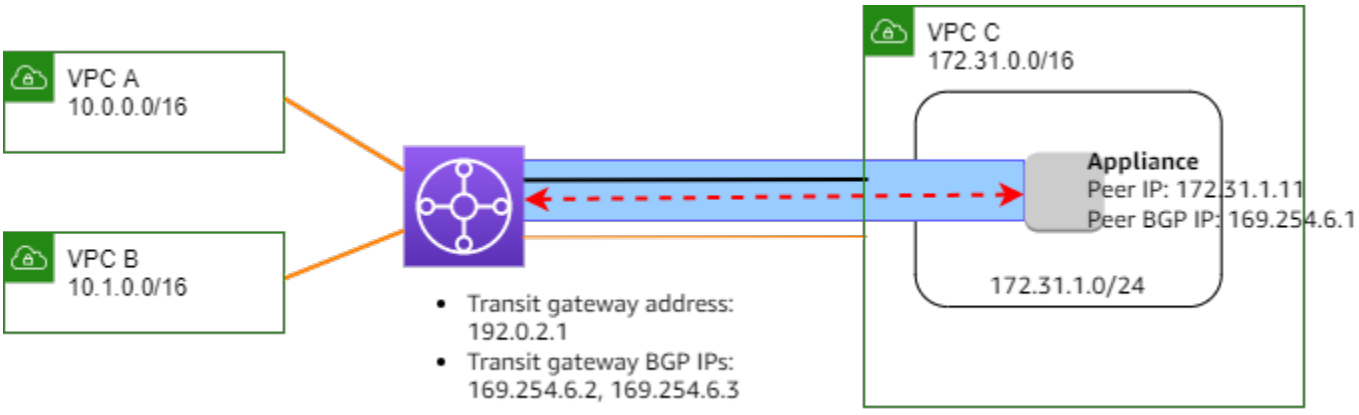
Puoi aggiungere un blocco CIDR del gateway di transito quando crei o modifichi un gateway di transito.

L'indirizzo IP può essere un indirizzo IPv4 o IPv6, ma deve essere la 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 peering BGP supporta solo BGP multiprotocollo (MP-BGP), dove l'indirizzamento Unicast IPv4 è richiesto per stabilire anche una sessione BGP per Unicast IPv6. Puoi usare sia indirizzi IPv4 che IPv6 per indirizzi IP esterni del GRE.

Nell'esempio seguente viene riportato un collegamento Connect tra un gateway di transito e un'appliance in un VPC.



Componente diagramma	Description
	Collegamento VPC
	Collegamento Connect
	Tunnel GRE (peer Connect)
	Sessione di peering BGP

Nell'esempio precedente viene creato un collegamento Connect su un collegamento VPC esistente (il collegamento di trasporto). Viene quindi creato un peer Connect sul collegamento Connect per stabilire una connessione a un'appliance nel VPC. L'indirizzo del gateway di transito è `192.0.2.1`, e l'intervallo di indirizzi BGP è `169.254.6.0/29`. Il primo indirizzo IP dell'intervallo (`169.254.6.1`) viene configurato sull'appliance come indirizzo IP BGP peer.

La tabella di routing della rottorete per il VPC C dispone di una route che instrada il traffico destinato al blocco CIDR del gateway di transito al 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 i collegamenti Connect, consulta le Domande frequenti su Transit Gateway di AWS.
- L'appliance di terze parti deve essere configurata per inviare e ricevere traffico attraverso un tunnel GRE da e verso il gateway di transito tramite il collegamento Connect.
- L'appliance di terze parti deve essere configurata per utilizzare BGP per gli aggiornamenti delle route dinamiche e i controlli di integrità.

- Sono supportati i seguenti tipi di BGP:
  - BGP esterno (eBGP): utilizzato per la connessione a router che si trovano in un sistema autonomo diverso da quello del gateway di transito. Se utilizzi un eBGP, dovrai configurare ebgp-multihop con un valore time-to-live (TTL) pari a 2.
  - BGP interno (iBGP): utilizzato per la connessione a router che si trovano nello stesso sistema autonomo del gateway di transito. Il gateway di transito non installa route da un peer iBGP (appliance di terze parti), a meno che le route non siano originate da un peer eBGP e non devono avere next-hop-self configurato. Le route pubblicizzate dall'appliance di terze parti tramite il peering iBGP devono avere un ASN.
  - MP-BGP (estensioni multiprotocol for BGP): utilizzato per supportare più tipi di protocollo, ad esempio famiglie di indirizzi IPv4 e IPv6.
- Il timeout di keep-alive BGP predefinito è di 10 secondi e il timer di attesa predefinito è di 30 secondi.
- Il peering BGP IPv6 non è supportato; è supportato solo il peering BGP basato su IPv4. I prefissi IPv6 vengono scambiati tramite peering IPv4 BGP utilizzando MP-BGP.
- Il rilevamento bidirezionale di inoltro (BFD) non è supportato.
- Non è supportato il riavvio gestito automaticamente di BGP.
- Se crei un peer del gateway di transito, se non specifichi un numero ASN peer, verrà selezionato il numero ASN del gateway di transito. Ciò significa che l'appliance e il gateway di transito saranno nello stesso sistema autonomo che esegue iBGP.
- Un peer di Connect che utilizza l'attributo BGP AS-PATH è il percorso preferito quando disponi di due peer Connect.

  Per utilizzare il routing ECMP (Equal-Cost Multi-Path) tra più appliance, dovrai configurare l'appliance in modo che pubblicizzi gli stessi prefissi al gateway di transito con lo stesso attributo BGP AS-PATH. Affinché il gateway di transito scelga tutti i percorsi ECMP disponibili, l'AS-PATH e il numero di sistema autonomo (ASN) devono corrispondere. Il gateway di transito può utilizzare ECMP tra peer Connect per lo stesso collegamento Connect o tra collegamenti Connect sullo stesso gateway di transito. Il gateway di transito non può utilizzare ECMP tra entrambi i peering BGP ridondanti che un singolo peer 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 tuo dispositivo di terze parti (sorgente tunnel) sia la Maximum Transmission Unit (MTU)
  - corrisponde all'MTU dell'interfaccia del tunnel GRE, oppure
  - dovrebbe essere maggiore di quella dell'interfaccia del tunnel GRE.

Crea un collegamento Connect.

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

Per creare un collegamento Connect utilizzando la console

1. Accedere alla console Amazon VPC 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 collegamento Connect utilizzando la AWS CLI

Utilizza il comando create-transit-gateway-connect.

Crea un peer Connect (tunnel GRE)

Puoi creare un peer Connect (tunnel GRE) per un collegamento Connect esistente. Prima di iniziare, assicurarsi di aver configurato un blocco CIDR del gateway di transito. Puoi configurare un blocco CIDR del gateway di transito quando crei o modifichi un gateway di transito.

Quando crei il peer Connect, devi specificare l'indirizzo IP esterno GRE sul lato appliance del peer Connect.

Per creare un peer Connect utilizzando la console

1. Accedere alla console Amazon VPC 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) In indirizzo GRE del gateway di transito, specifica l'indirizzo IP esterno GRE per il gateway di transito. Per impostazione predefinita, viene utilizzato il primo indirizzo disponibile dal blocco CIDR del gateway di transito.
6. Per Indirizzo GRE peer, specifica l'indirizzo IP esterno GRE per il lato appliance del peer Connect.
7. In IPv4 blocchi CIDR interni BGP, specifica l'intervallo di indirizzi IPv4 interni utilizzati per il peering BGP. Specifica un blocco CIDR /29 dall'intervallo `169.254.0.0/16`.
8. (Facoltativo) In IPv6 blocchi CIDR interni BGP, specifica l'intervallo di indirizzi IPv6 interni utilizzati per il peering BGP. Specifica un blocco CIDR /125 dall'intervallo `fd00::/8`.
9. (Facoltativo) In ASN peer, specifica il Border Gateway Protocol (BGP) Autonomous System Number (ASN) per l'appliance. Puoi utilizzare un ASN esistente assegnato alla tua rete. Se non ne hai uno, puoi utilizzare un ASN privato compreso nell'intervallo 64512–65534 (ASN a 16 bit) o 4200000000–4294967294 (ASN a 32 bit).

   Il valore predefinito è lo stesso ASN del gateway di transito. Se configuri l'ASN peer in modo che sia diverso dall'ASN del gateway di transito (eBGP), dovrai configurare il parametro ebgp-multihop con un valore TTL (time-to-live) pari a 2.
10. Scegliere Crea peer connect.

Per creare un peer di Connect utilizzando la AWS CLI

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

Visualizza i Collegamenti Connect e peer Connect

Puoi visualizzare i collegamenti Connect e i peer Connect.

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

1. Accedere alla console Amazon VPC 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 i collegamenti Connect e i peer Connect utilizzando la AWS CLI

Utilizza i comandi describe-transit-gateway-connects e describe-transit-gateway-connect-peers.

Modifica il collegamento Connect e i tag del peer Connect

Puoi modificare i tag per il collegamento Connect.

Per modificare i tag del collegamento Connect utilizzando la console

1. Accedere alla console Amazon VPC 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. Accedere alla console Amazon VPC 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.

Elimina un peer Connect

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

Per eliminare un peer Connect utilizzando la console

1. Accedere alla console Amazon VPC 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 di Conncet utilizzando la AWS CLI

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

Elimina un collegamento Connect

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. Accedere alla console Amazon VPC 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 collegamento Connect utilizzando la AWS CLI

Utilizza il comando delete-transit-gateway-connect.

Tabelle di routing del gateway di transito

Utilizzare le tabelle di route del gateway di transito per configurare il routing per gli allegati del gateway di transito.

Creare una tabella di routing di un gateway di transito.

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

1. Accedere alla console Amazon VPC 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 di routing del gateway di transito utilizzando il AWS CLI

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

Visualizzare le tabelle di instradamento del gateway di transito

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

1. Accedere alla console Amazon VPC 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 delle rotte 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.

Associare una tabella di routing di un gateway di transito.

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. Accedere alla console Amazon VPC 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 l'associazione di una tabella di routing di un gateway di transito.

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. Accedere alla console Amazon VPC 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.

Propagare una tabella di instradamento di un gateway di transito.

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. Accedere alla console Amazon VPC 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.

Per disabilitare la propagazione delle route

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

Per disabilitare la propagazione delle route utilizzando la console

1. Accedere alla console Amazon VPC 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.

Creare una route statica

È possibile creare una route statica per un allegato di peering VPC, VPN o gateway di transito oppure creare una route blackhole che elimina il traffico corrispondente al percorso.

Le route statiche in una tabella di routing del transit gateway indirizzate a un allegato VPN non vengono filtrate dalla Site-to-Site VPN. Ciò potrebbe consentire un flusso di traffico in uscita non intenzionale quando si utilizza una VPN basata su BGP.

Per creare una route statica mediante la console

1. Accedere alla console Amazon VPC 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 Create route (Crea routing), immettere il blocco CIDR per cui creare il routing, quindi selezionare Active (Attiva).
6. Selezionare il collegamento per la route.
7. Scegliere Create static route (Crea routing statico).

Per creare una route blackhole mediante la console

1. Accedere alla console Amazon VPC 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 Create route (Crea route), immettere il blocco CIDR per cui creare il routing, quindi selezionare Blackhole.
6. Scegliere Create static route (Crea routing statico).

Per creare una route statica o una route blackhole utilizzando il AWS CLI

Utilizza il comando create-transit-gateway-route.

Eliminare una route statica

Puoi eliminare route statiche da una tabella di instradamento del gateway di transito.

Per eliminare una route statica mediante la console

1. Accedere alla console Amazon VPC 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 rotta statica utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway-route.

Sostituisci un percorso statico

È possibile sostituire 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. Accedere alla console Amazon VPC 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 una rotta statica utilizzando il AWS CLI

Utilizza il comando replace-transit-gateway-route.

Esportare tabelle di route in Amazon S3

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

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

1. Accedere alla console Amazon VPC 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 alle route esportate, apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/ 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 un file JSON contenente informazioni su due route propagate 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 la tabella di routing di un gateway di transito.

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

1. Accedere alla console Amazon VPC 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.

Riferimenti elenco dei prefissi

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 blocco CIDR 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 specifichi frequentemente gli stessi CIDR di destinazione in più tabelle di instradamento del gateway di transito, puoi gestirli in un unico elenco di prefissi invece di fare riferimento ripetutamente agli stessi CIDR in ogni tabella di instradamento. Se hai la necessità di rimuovere un blocco CIDR di destinazione, puoi rimuovere la voce dall'elenco dei prefissi anziché rimuovere l'instradamento da ogni tabella di instradamento 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 maggiori informazioni sugli elenchi di prefissi, consulta Elenchi di prefissi nella Guida dell'utente di Amazon VPC.

Creare un riferimento all'elenco dei prefissi

È possibile creare un riferimento a un elenco di prefissi nella tabella di instradamento del gateway di transito.

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

1. Accedere alla console Amazon VPC 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.

Creazione di un riferimento a un elenco di prefissi tramite la AWS CLI

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

Visualizzare riferimenti all'elenco dei prefissi

È possibile visualizzare i riferimenti all'elenco dei prefissi nella tabella di instradamento del gateway di transito. È inoltre possibile visualizzare ogni voce nell'elenco dei prefissi come percorso individuale nella tabella di instradamento del gateway di transito. Il tipo di route per un route elenco di prefissi è `propagated`.

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

1. Accedere alla console Amazon VPC 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. Vengono elencati i riferimenti all'elenco dei prefissi.

5. Scegliere Percorsi. Ogni voce dell'elenco di prefissi viene elencata come route nella tabella di instradamento.

Visualizzazione di un riferimento a un elenco di prefissi tramite la AWS CLI

Utilizzare il comando get-transit-gateway-prefix-list-references.

Modificare un riferimento a un elenco di prefissi

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 maggiori informazioni, consulta Modifica di un elenco di prefissi nella Guida dell'utente di Amazon VPC.

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

1. Accedere alla console Amazon VPC 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.

Modifica di un riferimento a un elenco di prefissi tramite la AWS CLI

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

Eliminare un riferimento a un elenco di prefissi

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. Accedere alla console Amazon VPC 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.

Eliminazione di un riferimento a un elenco di prefissi tramite la AWS CLI

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

Tabelle di policy del gateway di transito

Il routing dinamico del gateway di transito utilizza tabelle di policy per instradare il traffico di rete per AWS Cloud WAN. 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 di policy del gateway di transito al momento sono supportate in Cloud WAN solo quando si crea una connessione di peering del gateway di transito. 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 Cloud WAN, consulta Peerings (Peering) nella Guida per l'utente di AWS Cloud WAN.

Creazione di una tabella di policy del gateway di transito

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

1. Apri alla console Amazon VPC 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 delle politiche del gateway di transito utilizzando il AWS CLI

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

Eliminazione di una tabella di policy di un gateway di transito

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 alla console Amazon VPC 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 sui gateway di transito

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 dei VPC collegati e funziona da router multicast per istanze che inviano traffico destinato a più istanze di ricezione.

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 al gruppo multicast è definita da singole interfacce di rete elastiche collegate alle istanze EC2.
- IGMP (Internet Group Management Protocol): un protocollo Internet che consente agli host e ai router di gestire dinamicamente l'appartenenza ai gruppi multicast. Un dominio multicast IGMP contiene host che utilizzano il protocollo IGMP per partecipare, lasciare e inviare messaggi. AWS supporta il protocollo IGMPv2 e i domini multicast di appartenenza ai gruppi sia IGMP che statici (basati su API).

- Origine multicast: una interfaccia di rete elastica associata a un'istanza EC2 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 protocollo IGMP per unire, abbandonare e inviare messaggi. Si utilizza per aggiungere una fonte e i membri del gruppo. AWS CLI L'origine aggiunta staticamente invia traffico multicast e i membri ricevono traffico multicast.
- Membro del gruppo multicast – Interfaccia di rete elastica associata a un'istanza EC2 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 di gruppo IGMP, i membri possono sia inviare che ricevere traffico.

Considerazioni

- Per informazioni sulle regioni supportate, consulta le Domande frequenti su AWS Transit Gateway.
- 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 the AWS CLI o IGMP.
- Una sottorete può trovarsi in un solo dominio multicast.
- Se si utilizza un'istanza non Nitro, è necessario disabilitare il controllo Source/Dest (Origine/Dest). Per informazioni sulla disattivazione del controllo, consulta Modifica del controllo di origine o destinazione nella Guida dell'utente di Amazon EC2 per le istanze Linux.
- Un'istanza non Nitro non può essere un mittente multicast.
- Il routing multicast non è supportato sugli allegati Site-to-Site VPN AWS Direct Connect, peering Allegati o Transit Gateway Connect.
- 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 IGMP invia più messaggi JOIN IGMP per unirsi a un gruppo multicast (in genere, 2-3 tentativi). Nel caso improbabile che tutti i messaggi JOIN IGMP vengano persi, l'host non entrerà a far parte del gruppo multicast del gateway di transito. In tale scenario dovrai riattivare il messaggio JOIN IGMP dall'host utilizzando metodi specifici dell'applicazione.
- L'appartenenza al gruppo inizia con la ricezione del messaggio JOIN IGMPv2 dal gateway di transito e termina con la ricezione del messaggio LEAVE IGMPv2. Il gateway di transito tiene traccia degli host che sono entrati a far parte correttamente del gruppo. In qualità di router multicast su cloud, il gateway di transito emette un messaggio di QUERY IGMPv2 a tutti i membri ogni due minuti. Ogni membro invia un messaggio JOIN IGMPv2 in risposta: è il modo in cui i membri rinnovano la loro appartenenza. 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 dal suo elenco. to-be-queried Un messaggio LEAVE IGMPv2 esplicito 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, questo continuerà a inviare dati multicast all'host per sette minuti (420 secondi) dopo l'ultimo messaggio JOIN IGMP inviato correttamente. Il gateway di

transito continua a inviare query di appartenenza all'host per un massimo di 12 ore o fino a quando non riceve un messaggio LEAVE IGMP dall'host.

- Il gateway di transito invia pacchetti di query di appartenenza a tutti i membri IGMP in modo che possa tenere traccia dell'appartenenza al gruppo multicast. L'IP di origine di questi pacchetti di query IGMP 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 host IGMP (istanze) e qualsiasi configurazione ACL nelle sottoreti dell'host devono consentire questi messaggi di protocollo IGMP.
- Quando l'origine e la destinazione multicast si trovano nello stesso VPC, non è possibile utilizzare i riferimenti ai gruppi di sicurezza per impostare il gruppo di sicurezza di destinazione affinché accetti il traffico dal gruppo di sicurezza di origine.
- Per i gruppi e le fonti multicast (trasmissione uno a molti) statici, i Transit Gateway di Amazon VPC rimuovono automaticamente i gruppi e le fonti statici per gli ENI che non esistono più. Questa operazione viene eseguita assumendo periodicamente il ruolo collegato al servizio di Transit Gateway per descrivere gli ENI nell'account.
- Solo il multicast statico supporta IPv6. Il multicast dinamico non lo fa.

Multicast (trasmissione uno a molti) con Windows Server

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. Utilizzando PowerShell, esegui i seguenti comandi:

1. Cambia Windows Server per utilizzare 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 deve essere. `Value 3` Invece di modificare il registro di Windows, è possibile eseguire il comando seguente per impostare la versione IGMP su 2. :
> `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Per impostazione predefinita, Windows Firewall elimina la maggior parte del traffico UDP. 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 porte UDP 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.

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.

Liste di controllo accessi di rete

Le regole ACL 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 Liste di controllo accessi di rete nella Guida per l'utente di Amazon VPC.

Per il traffico multicast IGMP, le regole minime in entrata sono le seguenti. 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

Tipo	Protocollo	Crea	Descrizione
Protocollo UDP personalizzato	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

Di seguito sono riportate le regole minime in uscita per IGMP.

Type (Tipo)	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	IGMP(2)	224.0.0.2/32	Uscita IGMP
Protocollo personalizzato	IGMP(2)	Indirizzo IP del gruppo multicast	Join IGMP
Protocollo UDP 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 Gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

Per il traffico multicast IGMP, è necessario disporre almeno delle 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 UDP personalizzato	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

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

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	2	224.0.0.2/32	Uscita IGMP
Protocollo personalizzato	2	Indirizzo IP del gruppo multicast	Join IGMP
Protocollo UDP personalizzato	UDP	Indirizzo IP del gruppo multicast	Traffico multicast in uscita

Utilizzo di multicast

Puoi configurare il multicast sui gateway di transito utilizzando la console Amazon VPC o la AWS CLI.

Prima di creare un dominio multicast, è necessario sapere se gli host utilizzano il protocollo IGMP (Internet Group Management Protocol) per il traffico multicast.

Indice

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) Supporto per IGMPv2 (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 protocollo IGMP. I membri si uniscono al gruppo multicast in uno dei seguenti modi: • I membri che supportano IGMP utilizzano i messaggi `JOIN` e `LEAVE`. • I membri che non supportano IGMP devono essere aggiunti o rimossi dal gruppo utilizzando la console Amazon VPC o la AWS CLI. Se registri membri del gruppo multicast, è necessario anche annullarne la registrazione. Il gateway di transito ignora un messaggio `LEAVE` IGMP 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 aggiungere sorgenti 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.

Gestione delle configurazioni IGMP

Se disponi di almeno un host che utilizza il protocollo IGMP per il traffico multicast, AWS crea automaticamente il gruppo multicast quando riceve un messaggio `JOIN` IGMP da un'istanza e quindi aggiunge l'istanza come membro di questo gruppo. È inoltre possibile aggiungere staticamente host non IGMP 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 maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per maggiori informazioni sulla creazione di sottoreti, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
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. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
5. Crea un dominio multicast configurato per il supporto IGMP. Per ulteriori informazioni, consulta the section called “Creazione di un dominio multicast IGMP”.

   Utilizzare le seguenti impostazioni:

   - Abilita Supporto per IGMPv2.
   - Disabilita Supporto per origini statiche.
6. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consulta the section called “Associazione di allegati VPC e sottoreti a un dominio multicast”.
7. La versione IGMP predefinita per EC2 è IGMPv3. È necessario modificare la versione per tutti i membri del gruppo IGMP. 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 protocollo IGMP al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrazione di membri con un gruppo multicast”.

Gestione delle configurazioni di origine statica

In questa configurazione, è necessario aggiungere staticamente origini multicast in un gruppo. Gli host non utilizzano il protocollo IGMP per unire o abbandonare 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 maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per maggiori informazioni sulla creazione di sottoreti, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
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. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
5. Crea un dominio multicast configurato senza supporto IGMP e supporto per l'aggiunta statica di origini. Per ulteriori informazioni, consulta the section called “Creazione di un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disabilita supporto per IGMPv2.
   - 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. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione di allegati VPC 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 “Registra le origini con un gruppo multicast”.
8. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrazione di membri con un gruppo multicast”.

Gestione delle configurazioni dei membri del gruppo statico

In questa configurazione, è necessario aggiungere staticamente i membri multicast a un gruppo. Gli host non possono utilizzare il protocollo IGMP per unire 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 maggiori informazioni sulla creazione di VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per maggiori informazioni sulla creazione di sottoreti, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
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. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a un VPC”.
5. Crea un dominio multicast configurato senza supporto IGMP e supporto per l'aggiunta statica di origini. Per ulteriori informazioni, consulta the section called “Creazione di un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disabilita Supporto per IGMPv2.
   - Disabilita Supporto per origini statiche.
6. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione di allegati VPC e sottoreti a un dominio multicast”.
7. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrazione di membri con un gruppo multicast”.

Gestione dei domini multicast

Per iniziare a utilizzare il multicast con un gateway di transito, crea un dominio multicast e associa quindi le sottoreti al dominio.

Indice

- Creazione di un dominio multicast IGMP
- Creazione di un dominio multicast di origine statica
- Associazione di allegati VPC e sottoreti a un dominio multicast
- Visualizzazione delle associazioni dei domini multicast
- Dissociazione di sottoreti da un dominio multicast
- Aggiunta di tag a un dominio multicast
- Eliminazione di un dominio multicast

Creazione di un dominio multicast IGMP

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

Console

Per creare un dominio multicast IGMP utilizzando la console

1. Apri alla console Amazon VPC 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. Seleziona la casella di controllo Supporto IGMPv2.
7. Deseleziona la casella di controllo di Supporto origini statiche.
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.

Command line

Per creare un dominio multicast IGMP utilizzando il 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
```

Creazione di un dominio multicast di origine statica

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

Console

Per creare un dominio multicast statico utilizzando la console

1. Apri alla console Amazon VPC 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. Deselezionare la casella di controllo Supporto IGMPv2.
7. Per Supporto origini 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.

Command line

Per creare un dominio multicast statico utilizzando il 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 allegati VPC e sottoreti a un dominio multicast

Utilizzare la procedura seguente per associare un allegato VPC 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 allegato VPC sul gateway di transito. Per ulteriori informazioni, consulta Collegamenti del gateway di transito a un VPC.

Console

Per associare allegati VPC a un dominio multicast utilizzando la console

1. Apri alla console Amazon VPC 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).

Command line

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

Utilizzare il comando -domainassociate-transit-gateway-multicast.

Visualizzazione delle associazioni dei domini multicast

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

Console

Per visualizzare un dominio multicast utilizzando la console

1. Apri alla console Amazon VPC 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).

Command line

Per visualizzare un dominio multicast utilizzando il AWS CLI

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

Dissociazione di sottoreti da un dominio multicast

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

Console

Per disassociare le sottoreti utilizzando la console

1. Apri alla console Amazon VPC 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.

Command line

Per dissociare le sottoreti utilizzando il AWS CLI

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

Aggiunta di tag a un dominio multicast

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, consultare Tagging delle risorse Amazon EC2.

Console

Per aggiungere tag a un dominio multicast utilizzando la console

1. Apri alla console Amazon VPC 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. Selezionare Salva.

Command line

Per aggiungere tag a un dominio multicast utilizzando il AWS CLI

Utilizzare il comando crea tag.

Eliminazione di un dominio multicast

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

Console

Per eliminare un dominio multicast utilizzando la console

1. Apri alla console Amazon VPC 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.

Command line

Per eliminare un dominio multicast utilizzando il AWS CLI

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

Gestione dei gruppi multicast

Indice

Registra le origini con un gruppo multicast

> **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
- Gli ID delle interfacce di rete delle origini
- L'indirizzo IP del gruppo multicast

Console

Per registrare le origini utilizzando la console

1. Apri alla console Amazon VPC 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 Group IP address (Indirizzo IP del gruppo), immettere il blocco CIDR IPv4 o il blocco CIDR IPv6 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).

Command line

Per registrare le fonti utilizzando il AWS CLI

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

Registrazione di membri con un gruppo multicast

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
- Gli ID delle interfacce di rete dei membri del gruppo
- L'indirizzo IP del gruppo multicast

Console

Per registrare i membri utilizzando la console

1. Apri alla console Amazon VPC 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 Group IP address (Indirizzo IP del gruppo), immettere il blocco CIDR IPv4 o il blocco CIDR IPv6 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).

Command line

Per registrare i membri utilizzando il AWS CLI

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

Annullamento della registrazione delle origini da un gruppo multicast

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

Console

Per rimuovere un'origine utilizzando la console

1. Apri alla console Amazon VPC 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).

Command line

Per rimuovere una fonte utilizzando il AWS CLI

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

Annullamento della registrazione di membri da un gruppo multicast

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

Console

Per annullare la registrazione dei membri utilizzando la console

1. Apri alla console Amazon VPC 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).

Command line

Per annullare la registrazione dei membri utilizzando il AWS CLI

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

Visualizzazione dei gruppi multicast

Puoi visualizzare informazioni sui gruppi multicast per verificare che i membri siano stati rilevati tramite il protocollo IGMPv2. Il tipo di membro (nella console) o `MemberType` (in AWS CLI) visualizza IGMP quando vengono AWS rilevati membri con il protocollo.

Console

Per visualizzare gruppi multicast utilizzando la console

1. Apri alla console Amazon VPC 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).

Command line

Per visualizzare i gruppi multicast utilizzando il AWS CLI

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

Nell'esempio seguente viene riportato che il protocollo IGMP ha rilevato 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"
        }
    ]
}
```

Utilizzo di domini multicast condivisi

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. I consumer 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:

- Account AWS all'interno della propria organizzazione o tra organizzazioni in AWS Organizations
- Un'unità organizzativa all'interno dell'organizzazione in AWS Organizations
- L'intera organizzazione in AWS Organizations
- Account AWS esterni a AWS Organizations.

  Per condividere un dominio multicast (trasmissione uno a molti) con un account AWS esterno all'organizzazione, è necessario creare una condivisione di risorse utilizzandoAWS Resource Access Manager e quindi selezionare Consenti condivisione con chiunque quando si selezionano gli utenti principali con cui condividere il dominio multicast (trasmissione uno a molti). 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

- Servizi correlati
- Condivisione tra le zone di disponibilità
- Condivisione di un dominio multicast
- Annullamento della condivisione di un dominio multicast condiviso
- Identificazione di un dominio multicast condiviso
- Autorizzazioni del dominio multicast condiviso
- Fatturazione e misurazione
- Quote

Prerequisiti per la condivisione di un dominio multicast

- Per condividere un dominio multicast, è necessario averlo nel proprio 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 dei domini multicast si integra con AWS Resource Access Manager (AWS RAM). AWS RAM è un servizio che consente di condividere le risorse AWS con qualsiasi account AWS o tramite AWS Organizations. Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e i consumatori con cui condividerle. I consumatori possono essere account AWS singoli oppure unità organizzative o un'intera organizzazione in AWS Organizations.

Per ulteriori informazioni su AWS RAM, consulta la Guida per l'utente di AWS RAM.

Condivisione tra le zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona di disponibilità `us-east-1a` per l'account AWS potrebbe avere un'ubicazione diversa rispetto a `us-east-1a` per un altro account AWS.

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 univoco ed è lo stesso identificatore di una zona di disponibilità per tutti gli account AWS. Ad esempio, `use1-az1` è un ID della zona di disponibilità per la regione `us-east-1` e ha la stessa posizione in ogni account AWS.

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

1. Aprire la console AWS RAM all'indirizzo https://console.aws.amazon.com/ram.
2. Gli ID AZ per la regione attuale vengono visualizzati nel pannello Il tuo ID AZ sul lato destro dello schermo.

Condivisione di un dominio multicast

Quando un proprietario condivide un dominio multicast con un consumer, il consumer può effettuare le seguenti operazioni:

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

Per condividere un dominio multicast, dovrai aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che ti consente di condividere le risorse tra account AWS. Un condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi un dominio multicast utilizzando la 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 in AWS Organizations e la condivisione all'interno della tua organizzazione è abilitata, ai consumatori nella tua organizzazione viene automaticamente concesso l'accesso all'elenco dei domini multicast. 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 *console Amazon Virtual Private Cloud Console, la console AWS RAM o la AWS CLI.

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

1. Aprire la console Amazon VPC 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 .

Condivisione di un dominio multicast di tua proprietà tramite la AWS CLI

Utilizza il comando create-resource-share.

Annullamento della condivisione di un dominio multicast condiviso

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. Puoi farlo dalla console di AWS RAM o dalla AWS CLI.

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà, devi rimuoverlo dalla condivisione di risorse. È possibile effettuare tale operazione mediante la *Amazon Virtual Private Cloud Console, la console AWS RAM o la AWS CLI.

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

1. Aprire la console Amazon VPC 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 .

Annullamento della condivisione di un dominio multicast condiviso di proprietà tramite la AWS CLI

Usa il comando disassociate-resource-share.

Identificazione di un dominio multicast condiviso

Proprietari e consumer possono identificare i domini multicast condivisi tramite la *console Amazon Virtual Private Cloud Console e AWS CLI.

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

1. Aprire la console Amazon VPC 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 dominio multicast del gateway di transito visualizza l'ID proprietario per identificare l'ID AWS del dominio multicast.

Identificazione di un dominio multicast condiviso tramite la AWS CLI

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

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 consumer nei domini multicast condivisi.

Autorizzazioni per i consumatori

I consumer possono completare le seguenti operazioni sui domini multicast condivisi nello stesso modo con cui lo farebbero nei domini multicast 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 per le quote di dominio multicast del proprietario e del consumer.

Considerazioni sulla condivisione dei gateway di transito

È possibile utilizzare AWS Resource Access Manager (RAM) per condividere un gateway di transito per gli allegati VPC tra più account o all'interno dell'organizzazione in AWS Organizations. La RAM deve essere abilitata 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.

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

- Un allegato AWS Site-to-Site VPN deve essere creato nello stesso account AWS che possiede il gateway di transito.
- Un allegato al gateway Direct Connect utilizza un'associazione gateway di transito e può trovarsi nello stesso account AWS del gateway Direct Connect o in uno diverso.

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per creare o modificare le risorse AWS RAM. Per consentire agli utenti di creare o modificare risorse ed eseguire attività, devi creare delle policy IAM che forniscano l'autorizzazione per l'uso di risorse e operazioni API specifiche. Quindi, collega queste policy agli utenti o ai gruppi IAM che hanno bisogno delle 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.
- Eseguire tutte le API di tabelle di routing di gateway di transito, allegati di gateway di transito e 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.
- Puoi eseguire l'API `DescribeTransitGateways`.
- Eseguire le API che creano e descrivono gli allegati, ad esempio `CreateTransitGatewayVpcAttachment` e `DescribeTransitGatewayVpcAttachments` nei rispettivi VPC.
- 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 e viene 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 viene annullata la condivisione di un gateway di transito con un altro account AWS, o se l'account AWS con cui è condiviso il gateway di transito viene rimosso dall'organizzazione, il gateway di transito stesso non ne risentirà.

Sottoreti condivise

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

Per ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Registrazione del traffico di rete utilizzando i registri di flusso di Transit Gateway

I registri di flusso di Transit Gateway sono una funzionalità che consente di acquisire le informazioni sul traffico IP da e per i 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”. Utilizza i registri di flusso per VPC acquisire le informazioni sul traffico IP verso e dalle interfacce di rete nel VPC. 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, è necessario essere il proprietario del gateway di transito o, in caso contrario, il proprietario del gateway di transito deve concedere 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. Per ulteriori informazioni, consulta Creazione di un log di flusso.

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 log di flusso.

Indice

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 di testo normale, tutti i campi sono di tipo STRING. Se il formato è Parquet, vedere la tabella per i tipi di dati di campo.

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. Questa può essere un TransitGateway o un TransitGatewayAttachment.	6

Campo	Descrizione	Versione
	Tipo di dati Parquet: STRING	
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
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

Campo	Descrizione	Versione
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
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

Campo	Descrizione	Versione
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_64	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 Guida per l'utente di Amazon EC2 per le istanze Linux. 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 indirizzi IP indica 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 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

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.

Crea un log di flusso da pubblicare su Logs CloudWatch

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 campo IngestionTime 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

Ruoli IAM per la pubblicazione dei log di flusso in Logs CloudWatch

Il ruolo IAM 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 ruolo IAM 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 flusso di log e l'ARN di origine è l'ARN del flusso di log. Se non si conosce l'ID del flusso di log, è possibile sostituire quella parte dell'ARN con un carattere jolly (*) e quindi aggiornare la policy dopo aver creato il flusso di log.

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

Creare o aggiornare un ruolo IAM per i flussi di log

Puoi aggiornare un ruolo esistente o utilizzare la seguente procedura per creare un nuovo ruolo per l'utilizzo con log di flusso.

Per creare un ruolo IAM per i log di flusso

1. Aprire la console IAM 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 Use case (Caso d'uso), selezionare EC2. Seleziona Successivo.
4. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next: Tags (Successivo: Tag) e aggiungi facoltativamente i tag. Seleziona Successivo.
5. Nella pagina Name, review, and create (Nomina, verifica e crea) immetti un nome per il ruolo e, facoltativamente, una descrizione. Scegli Crea ruolo.
6. Scegli il nome del ruolo. In Add permissions (Aggiungi autorizzazioni), scegli Create inline policy (Crea policy in linea), quindi seleziona la scheda JSON.
7. Copiare la prima policy da Ruoli IAM 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 Summary (Riepilogo), prendere nota dell'ARN per il ruolo. Questo ARN sarà necessario al momento della creazione del log di flusso.

Autorizzazioni per gli utenti IAM per passare un ruolo

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 log di flusso da pubblicare su Logs CloudWatch

È possibile creare registri di flusso per i gateway di transito. Se si esegue questa procedura come utente IAM, assicurarsi di disporre delle autorizzazioni per utilizzare l'operazione `iam:PassRole`. Per ulteriori informazioni, consulta Autorizzazioni per gli utenti IAM per passare un ruolo.

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

1. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
3. Selezionare le caselle di controllo per uno o più gateway di transito e scegliere Actions (Operazioni), quindi Create flow log (Crea registro di flusso).
4. Per Destinazione, scegli Invia ai CloudWatch registri.
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 ruolo IAM, specifica il nome del ruolo che dispone delle autorizzazioni per pubblicare i log in Logs. 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-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API di interrogazione Amazon EC2)

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
```

Elabora i record del log di flusso in Logs CloudWatch

È possibile utilizzare i record del log di flusso come si farebbe 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 Searching and Filtering Log Data 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 `eni-1a2b3c4d`. Si desidera creare un allarme che avvisa se si sono verificati almeno 10 tentativi di connessione all'istanza sulla porta TCP 22 (SSH) entro un periodo di tempo 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 il filtro parametri per traffico SSH 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 Logs (Registri), Log groups (Gruppi di registri).
3. Seleziona la casella di controllo per il gruppo di log e scegli Operazioni, poi Crea filtri parametri.
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 Notification (Notifica), scegli un argomento SNS esistente oppure scegli Create new topic (Crea nuovo argomento) per crearne uno nuovo. Seleziona 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).

Creazione di un log di flusso che pubblica 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 flussi di log, consulta Creazione di un bucket nella Guida per l'utente di Amazon Simple Storage Service.

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

Log di flusso VPC è una caratteristica che raccoglie record di log di flusso, li consolida in file di log e pubblica questi ultimi nel bucket Amazon S3 a intervalli di cinque 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
```

Ad esempio, di seguito viene mostrata la struttura di cartelle e il nome di un file di log per un flusso di log creato dall' Account AWS 123456789012, per una risorsa nella Regione us-east-1 su June 20, 2018 in 16:20 UTC. Il file contiene i registri dei flussi di log con un'ora di fine tra 16:20:00 e 16:24:59.

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

Policy IAM per le entità IAM che pubblicano i log di flusso in Amazon S3

Il principale IAM che crea il log di flusso deve disporre delle autorizzazioni seguenti, necessarie per pubblicare 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 maggiori informazioni, consulta Utilizzo delle policy 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:*"
                }
            }
        }
    ]
}
```

L'ARN per cui si specifica *my-s3-arn* dipende dal fatto che si utilizzino 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 best practice, ti consigliamo di concedere queste autorizzazioni al responsabile del servizio di consegna dei log anziché ai singoli ARN. Account AWS 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 flusso di log e l'ARN di origine è l'ARN jolly (*) del servizio log.

Policy di chiave richiesta per l'uso con SSE-KMS

Puoi proteggere i dati nel tuo bucket Amazon S3 abilitando la crittografia lato server con Amazon S3 Managed Keys (SSE-S3) o la crittografia lato server con chiavi archiviate in 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 AWS gestita dal cliente. Con una chiave AWS gestita, non è possibile 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 tra account al tuo bucket S3, usa una chiave gestita dal cliente e specifica l'Amazon Resource Name (ARN) della chiave gestita dal cliente quando abiliti la crittografia del bucket. Per ulteriori informazioni, consulta Specifica della crittografia lato server con AWS KMS nella Guida per l'utente di Amazon S3.

Quando utilizzi SSE-KMS con una chiave gestita dal cliente, dovrai aggiungere quanto segue alla policy di chiavi per la tua chiave (non la policy di bucket per il bucket S3), in modo che i flussi di log del VPC possano scrivere nel bucket S3.

```
{
    "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

In aggiunta alle policy dei bucket obbligatorie, Amazon S3 utilizza liste di controllo accessi per gestire l'accesso ai file di log 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 Panoramica della lista di controllo accessi nella Guida per l'utente di Amazon Simple Storage Service.

Creazione di un log di flusso che pubblica in Amazon S3

Dopo aver creato e configurato il bucket Amazon S3, è possibile creare registri di flusso per i gateway di transito.

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

1. Apri alla console Amazon VPC 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 S3 bucket ARN (ARN bucket S3), specificare 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 `my-bucket`, utilizzare il seguente 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-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API di interrogazione Amazon EC2)

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico del gateway di transito per `tgw-00112233344556677` VPC 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/'
```

Elaborazione di record del log di flusso 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.

Pubblicare i log di flusso su Firehose

Argomenti

- Ruoli IAM per la consegna tra account
- Creare un log di flusso da pubblicare su Firehose

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 un ruolo IAM nell'account di origine e un ruolo IAM nell'account di destinazione.

Roles

- Ruolo dell'account di origine
- Ruolo dell'account di destinazione

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 si crea la propria policy, specifica i VPC, le interfacce di rete o le sottoreti che si stanno 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"
    }
  ]
}
```

Dall'account di origine, utilizza la seguente procedura per creare il ruolo.

Creazione del ruolo dell'account di origine

1. Accedi AWS Management Console e apri la console IAM 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. Seleziona 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).

Ruolo dell'account di destinazione

Nell'account di destinazione, crea un ruolo con un nome che inizia con. AWSLogsDeliveryFirehoseCrossAccountRole 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"
    }
  ]
}
```

Dall'account di destinazione, utilizza la seguente procedura per creare il ruolo.

Creazione del ruolo dell'account di destinazione

1. Accedi AWS Management Console e apri la console IAM 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 policy che inizia con AWSLogDeliveryFirehoseCrossAccountRole, quindi scegli 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. Seleziona 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).

Creare un log di flusso da pubblicare su Firehose

Per creare un log di flusso del gateway di transito da pubblicare su Firehose utilizzando la console

1. Apri alla console Amazon VPC 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 Firehose Delivery Stream ARN (ARN flusso di consegna Firehose), scegli l'ARN di un flusso di consegna che hai creato dove deve essere pubblicato 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 (CLI)AWS

- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API di interrogazione Amazon EC2)

Il seguente esempio AWS CLI 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
```

Il seguente esempio AWS CLI 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
```

Utilizzo dei regisri di flusso di Transit Gateway

Puoi lavorare con i Transit Gateway Flow Logs utilizzando le console Amazon EC2, Amazon VPC CloudWatch e Amazon S3.

Attività

- Controllo dell'utilizzo dei log di flusso
- Creazione di un log di flusso
- Visualizzazione dei log di flusso
- Aggiunta o rimozione di tag per i log di flusso
- Visualizzazione dei record dei log di flusso

- Ricerca dei record dei log di flusso
- Eliminazione di un log di flusso
- Panoramica e limitazioni su API e CLI

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 la sezione relativa alla Concessione agli utenti IAM delle autorizzazioni richieste per risorse di Amazon EC2 nella Guida di riferimento alle API di Amazon EC2.

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 Crea un log di flusso da pubblicare su Logs CloudWatch e Creazione di un log di flusso che pubblica in Amazon S3.

Creazione di un log di flusso

Puoi creare log di flusso per i tuoi gateway di transito in grado di pubblicare dati su CloudWatch Logs, Amazon S3 o 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

Visualizzazione dei log di flusso

È possibile visualizzare informazioni sui registri di flusso nelle console Amazon VPC visualizzando la scheda Flow Logs (Registri di flusso) per una risorsa specifica. Quando la risorsa viene selezionata, vengono elencati tutti i registri di flusso per tale 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 alla console Amazon VPC 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.

Aggiunta o rimozione di tag per i log di flusso

Puoi aggiungere o rimuovere tag per un log di flusso nelle console Amazon EC2 e Amazon VPC.

Per aggiungere o rimuovere tag per un log di flusso del gateway di transito

1. Apri alla console Amazon VPC 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. Selezionare Salva.

Visualizzazione dei record dei log di flusso

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.

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

1. Apri la console Amazon S3 su 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 Name (Nome), selezionare la casella di controllo accanto al file di log. Nel pannello di panoramica dell'oggetto, scegliere Download (Scarica).

Ricerca dei record dei log di flusso

È possibile cercare i record del 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 log di flusso

È possibile eliminare un log di flusso del gateway di transito usando la console Amazon VPC.

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 che pubblica in Amazon S3 non rimuove le policy di bucket e le liste di controllo accessi del file di log.

Per eliminare un log di flusso del gateway di transito

1. Apri alla console Amazon VPC 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).

Panoramica e limitazioni su API e CLI

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando o l'API.

Le seguenti limitazioni si applicano quando si utilizza l'API `CreateFlowLogs` o la CLI `create-flow-logs`:

- `--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)
- CreateFlowLogs(API di interrogazione Amazon EC2)

Descrizione dei log di flusso

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs(API di interrogazione Amazon EC2)

Visualizzazione dei record del log di flusso (eventi di log)

- get-log-events (AWS CLI)
- LogEventGet-CWL ()AWS Tools for Windows PowerShell
- GetLogEvents(API) CloudWatch

Eliminazione di un log di flusso

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs(API di interrogazione Amazon EC2)

Monitoraggio dei gateway di transito

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.

Parametri di CloudWatch

Puoi utilizzare Amazon CloudWatch per recuperare le statistiche sui punti dati per i gateway di transito come set ordinato di dati delle serie temporali, noti come parametri. È possibile utilizzare queste metriche per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta Metriche di CloudWatch per i gateway di transito.

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 i log di flusso VPC per acquisire informazioni dettagliate sul traffico in entrata e in uscita dai VPC collegati ai gateway di transito. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

Log di CloudTrail

È possibile utilizzare AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate all'API del gateway di transito e memorizzarle come file di log in Amazon S3. È possibile utilizzare i log di CloudTrail per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proveniva la chiamata, chi l'ha effettuata, quando e così via. Per ulteriori informazioni, consulta Registrazione delle chiamate API al gateway di transito tramite AWS CloudTrail.

CloudWatch Events con Network Manager

Puoi utilizzare AWS Network Manager per inoltrare gli eventi a CloudWatch 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 Events nella guida per l'utente di reti globali per i gateway di transito AWS.

Metriche di CloudWatch per i gateway di transito

Amazon VPC pubblica punti dati su Amazon CloudWatch per i gateway di transito e gli allegati del gateway di transito. CloudWatch ti consente di recuperare le statistiche su quei punti di dati come set ordinato di dati di serie temporali, i cosiddetti parametri. 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 allarme CloudWatch per monitorare un parametro specificato e avviare un'operazione (come l'invio di una notifica a un indirizzo e-mail) se il parametro non rientra in un intervallo che consideri accettabile.

Amazon VPC misura e invia le sue metriche a CloudWatch a intervalli di 60 secondi.

Per ulteriori informazioni, consulta la Guida per l'utente di Amazon CloudWatch.

Indice

Metriche dei gateway di transito

Il namespace `AWS/TransitGateway` include le metriche descritte di seguito.

Parametro	Descrizione
`BytesDropCountBlackhole`	Il numero di byte persi perché intercettati da una route `blackhole` .
`BytesDropCountNoRoute`	Il numero di byte persi perché non corrispondenti a una route esistente.
`BytesIn`	Numero di byte ricevuti dal gateway di transito.
`BytesOut`	Numero di byte inviati dal gateway di transito.
`PacketsIn`	Il numero di pacchetti ricevuti dal gateway di transito.

Parametro	Descrizione
PacketsOut	Il numero di pacchetti inviati dal gateway di transito.
PacketDropCountBlackhole	Il numero di pacchetti persi perché intercettati da una route blackhole .
PacketDropCountNoRoute	Il numero di pacchetti persi perché non presente una route corrispondente.

Metriche a livello di allegato

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”.

Parametro	Descrizione
BytesDropCountBlackhole	Numero di byte eliminati perché corrispondono a una route blackhole nell'allegato del gateway di transito.
BytesDropCountNoRoute	Numero di byte eliminati perché non corrispondono a una route nell'allegato del gateway di transito.
BytesIn	Numero di byte ricevuti dal gateway di transito dall'allegato.
BytesOut	Numero di byte inviati dal gateway di transito all'allegato.
PacketsIn	Numero di pacchetti ricevuti dal gateway di transito dall'allegato.
PacketsOut	Numero di pacchetti inviati dal gateway di transito all'allegato.
PacketDropCountBlackhole	Numero di pacchetti eliminati perché corrispondono a una route blackhole nell'allegato del gateway di transito.

Parametro	Descrizione
`PacketDropCountNoRoute`	Numero di pacchetti eliminati perché non corrispondono a una route nell'allegato del gateway di transito.

Dimensioni delle metriche per i gateway di transito

Per filtrare le metriche per i gateway di transito, utilizzare le dimensioni seguenti.

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.

Registrazione delle chiamate API al gateway di transito tramite AWS CloudTrail

AWS CloudTrail è un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS. CloudTrail acquisisce tutte le chiamate API del gateway di transito come eventi. Le chiamate acquisite includono le chiamate dalla AWS Management Console e le chiamate di codice alle operazioni API del gateway di transito. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per i gateway di transito. Se non configuri un trail, puoi comunque visualizzare gli eventi più recenti nella console CloudTrail nella cronologia degli eventi. Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata all'API del gateway di transito, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni sulle API del gateway di transito, consulta la sezione Operazioni del gateway di transito AWS nella Guida di riferimento delle API di Amazon EC2.

Per ulteriori informazioni su CloudTrail, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni sul gateway di transito in CloudTrail

CloudTrail è abilitato sul tuo account AWS al momento della sua creazione. Quando si verifica un'attività tramite l'API del gateway di transito, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi nella cronologia degli eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi relativi alle API del gateway di transito, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Tutte le chiamate alle azioni del gateway di transito vengono registrate da CloudTrail. Ad esempio, le chiamate alle operazioni `CreateTransitGateway` generano voci nei file di log di CloudTrail.

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 credenziali utente AWS Identity and Access Management o root.
- 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.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail.

Comprensione delle voci dei file di log del gateway di transito

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 che specifichi. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, sulla data e sull'ora dell'operazione, sui parametri richiesti e così via. I file di log CloudTrail non sono una traccia di stack ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

I file di log includono gli eventi per tutte le chiamate API per l'account AWS, non solo per le chiamate API del gateway di transito. Puoi individuare le chiamate all'API del gateway di transito controllando gli elementi `eventSource` 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 sono riportati alcuni record di log CloudTrail per l'API del gateway di transito 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`. Puoi identificare le chiamate API invocate utilizzando l'elemento `eventName`. 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 per i gateway di transito

AWS utilizza le credenziali di sicurezza per identificarti e per concederti l'accesso alle risorse AWS. Puoi utilizzare le caratteristiche di AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le risorse AWS completamente o in modo limitato, senza condividere le credenziali di sicurezza.

Per impostazione predefinita, gli utenti IAM non dispongono dell'autorizzazione per creare, visualizzare o modificare le risorse AWS. 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, tramite essa viene concessa o rifiutata agli utenti l'autorizzazione per l'esecuzione delle attività specificate per le risorse specificate.

Per operare su un gateway di transito è possibile che una delle seguenti policy gestite da AWS soddisfi 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/*"
        }
    ]
}
```

Criteri di esempio per la gestione di AWS Network Manager

Per esempi di policy, consultare Policy di esempio per la gestione di Network Manager nella Guida per l'utente di Reti globali AWS per gateway di transito.

Utilizzo dei ruoli collegati ai servizi per i 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. Per ulteriori informazioni, consulta Utilizzo di 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 usa il ruolo collegato ai servizi denominato AWSServiceRoleForVPCTransitGateway per effettuare le chiamate per conto dell'utente alle seguenti operazioni quando durante l'utilizzo di un gateway di transito:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

Ai fini dell'assunzione del ruolo, il ruolo AWSServiceRoleForVPCTransitGateway considera attendibili i seguenti servizi:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway utilizza la policy gestita AWSVPCTransitGatewayServiceRolePolicy.

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.

Affinché Amazon VPC crei un ruolo collegato ai servizi, è necessario disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Modifica del ruolo collegato ai servizi

È possibile modificare la descrizione del ruolo AWSServiceRoleForVPCTransitGateway utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato ai servizi

Se non è più necessario utilizzare gateway di transito, consigliamo di eliminare il ruolo AWSServiceRoleForVPCTransitGateway.

È possibile eliminare questo ruolo collegato ai servizi solo dopo aver eliminato tutti i collegamenti al VPC del gateway di transito esistenti nell'account AWS dell'utente. 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 Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Dopo aver eliminato il ruolo AWSServiceRoleForVPCTransitGateway, Amazon VPC lo ricrea nuovamente in caso di collegamento di un VPC dell'account dell'utente a un gateway di transito.

Criteri gestiti da AWS per gateway di transito

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. 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 policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

Per operare su un gateway di transito è possibile che una delle seguenti policy gestite da AWS soddisfi le tue esigenze:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Policy gestita AWS: AWSVPCTransitGatewayServiceRolePolicy

Questa politicy è associata al ruolo AWSServiceRoleForVPCTransitGateway. Ciò consente ad Amazon VPC di creare e gestire risorse per collegamento del gateway di transito alla VPN.

Per visualizzare le autorizzazioni per questa policy, consultare AWSVPCTransitGatewayServiceRolePolicy nella Guida di riferimento della policy gestita AWS.

Aggiornamenti del gateway di transito alle policy gestite AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per gateway di transito da quando Amazon VPC ha iniziato a tenere traccia delle modifiche a marzo 2021.

Modifica	Descrizione	Data
Amazon VPC ha iniziato a monitorare le modifiche	Amazon VPC ha iniziato a monitorare le modifiche per le sue policy gestite da AWS.	1° marzo 2021

Funzionamento degli ACL di rete con i gateway di transito

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 istanze EC2 e l'associazione del gateway di transito”
- the section called “Sottoreti diverse per le istanze EC2 e l'associazione del gateway di transito”

Stessa sottorete per le istanze EC2 e l'associazione del gateway di transito

Si consideri una configurazione in cui nella stessa sottorete sono presenti istanze EC2 e un'associazione del gateway di transito. La stessa ACL di rete viene utilizzata sia per il traffico dalle istanze EC2 al gateway di transito che 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 le istanze EC2 e l'associazione del gateway di transito

Si consideri una configurazione in cui sono presenti istanze EC2 in una sottorete e un'associazione del gateway di transito in una sottorete diversa, con ogni sottorete associata a un'ACL di rete diversa.

Le regole delle ACL di rete vengono applicate come segue per la sottorete di istanze 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, utilizza 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 applicare liste di controllo degli accessi di rete alle sottoreti del carico di lavoro.

Per ulteriori informazioni sul funzionamento degli allegati VPC, consulta the section called “Collegamenti alle risorse”.

Quote per i gateway di transito

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

Ci sono molti fattori che possono influenzare la larghezza di banda realizzata attraverso una connessione Site-to-Site VPN, tra cui, a titolo esemplificativo, la dimensione dei pacchetti, il mix di traffico (TCP/UDP), la definizione o la limitazione delle policy sulle reti intermedie, il meteo Internet e i requisiti specifici delle applicazioni. 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'MTU di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito che può essere passato 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 VPC, AWS Direct Connect Transit Gateway Connect e allegati di peering. 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 i VPC allo stesso tempo per evitare che i pacchetti jumbo cadano a causa di una mancata corrispondenza delle dimensioni.
- I pacchetti con una dimensione maggiore di 8500 byte che arrivano al gateway di transito vengono eliminati.
- Il gateway di transito non genera il FRAG_NEDED per il pacchetto ICMPv4 o il PTB (Packet Too Big) per il pacchetto ICMPv6. Pertanto, il percorso MTU Discovery (PMTUD) non è supportato.
- Il gateway di transito applica il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per maggiori informazioni, consulta RFC879.
- Per informazioni dettagliate sulle quote di VPN sito-sito per MTU, consulta Maximum Transmission Unit (MTU) nella Guida per l'utente di AWS Site-to-Site VPN .

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
Origini per gruppo multicast del gateway di transito	1	Sì

Nome	Predefinita	Adattabile
Membri e origini del gruppo multicast statico e IGMPv2 per gateway di transito	10.000	No
Membri del gruppo multicast statico e IGMPv2 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:

- Quote di Site-to-Site VPN nella Guida per l'utente AWS Site-to-Site VPN
- 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
Quote di Transit Gateway AWS	Sono stati aggiunti limiti di larghezza di banda.	14 agosto 2023
Registri di flusso di AWS Transit Gateway	I gateway di transito ora supportano i registri di flusso di Transit Gateway, consentendo 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 un gateway di transito nella stessa regione.	1 dicembre 2021
Transit Gateway Connect	Puoi stabilire una connessio ne tra un gateway di transito	10 dicembre 2020

	e appliance virtuali di terzi in esecuzione in un VPC.	
Modalità Appliance	È possibile attivare la modalità appliance su un allegato VPC per garantire che il traffico bidirezionale scorra 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
Metriche CloudWatch per gli allegati del gateway di transito	È possibile visualizzare le metriche CloudWatch 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 sottoreti dei VPC collegati e funge da router multicast per 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
Supporto AWS Direct Connect	È possibile utilizzare un gateway AWS Direct Connect per collegare la connessio ne AWS Direct Connect tramite un'interfaccia virtuale di transito ai VPC o alle VPN collegate al gateway di transito.	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.