aws

Guida per gli sviluppatori

AWS Global Accelerator

AWS Global Accelerator: Guida per gli sviluppatori

Table of Contents

Cos'è AWS Global Accelerator?

AWS Global Accelerator è un servizio in cui si creaAcceleratoriPer migliorare le prestazioni delle applicazioni per utenti locali e globali. A seconda del tipo di acceleratore scelto, puoi ottenere ulteriori vantaggi.

- Utilizzando un acceleratore standard, è possibile migliorare la disponibilità delle applicazioni Internet utilizzate da un pubblico globale. Con un acceleratore standard, Global Accelerator dirige il traffico sulla rete globale AWS verso gli endpoint nella regione più vicina al client.
- Utilizzando un acceleratore di routing personalizzato, è possibile mappare uno o più utenti a una destinazione specifica tra molte destinazioni.

Global Accelerator è un servizio globale che supporta gli endpoint in più regioni AWS, elencati nellaTabella delle regioni AWS: .

Per impostazione predefinita, Global Accelerator fornisce due indirizzi IP statici associati all'acceleratore. Con un acceleratore standard, invece di utilizzare gli indirizzi IP forniti da Global Accelerator, è possibile configurare questi punti di ingresso come indirizzi IPv4 dai propri intervalli di indirizzi IP forniti a Global Accelerator. Gli indirizzi IP statici sono anycast dalla rete perimetrale AWS.

> **Important**
>
> Gli indirizzi IP statici rimangono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se disabiliti l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quandodeleteun acceleratore, si perdono gli indirizzi IP statici ad esso assegnati, in modo da non poter più instradare il traffico utilizzando tali indirizzi. È possibile utilizzare criteri IAM come autorizzazioni basate su tag con Global Accelerator per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

Per gli acceleratori standard, Global Accelerator utilizza la rete globale AWS per indirizzare il traffico all'endpoint regionale ottimale in base all'integrità, alla posizione del client e ai criteri configurati, aumentando così la disponibilità delle applicazioni. Gli endpoint per gli acceleratori standard possono essere Network Load Balancers, Application Load Balancers, istanze Amazon EC2 o indirizzi IP elastici che si trovano in una o più regioni AWS. Il servizio reagisce istantaneamente ai cambiamenti

di integrità o configurazione per garantire che il traffico Internet proveniente dai client sia sempre diretto a endpoint sani.

Gli acceleratori di routing personalizzati supportano solo tipi di endpoint di sottorete Virtual Private Cloud (VPC) e instradano il traffico a indirizzi IP privati nella sottorete.

Per un elenco delle regioni AWS in cui Global Accelerator e altri servizi sono attualmente supportati, consultaTabella delle regioni AWS: .

Argomenti

Componenti AWS Global Accelerator

AWS Global Accelerator include i componenti seguenti:

Indirizzi IP statici

Global Accelerator fornisce un set di due indirizzi IP statici che sono anycast dalla rete perimetrale AWS. Se porti il tuo intervallo di indirizzi IP a AWS (BYOIP) per l'utilizzo con Global Accelerator, puoi invece assegnare indirizzi IP dal tuo pool per l'utilizzo con l'acceleratore. Per ulteriori informazioni, consulta Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator.

Gli indirizzi IP fungono da punti di ingresso fissi singoli per i client. Se per le tue applicazioni sono già impostati i bilanciamenti del carico Elastic Load Balancing, le istanze Amazon EC2 o le risorse degli indirizzi IP elastici, puoi aggiungerli facilmente a un acceleratore standard in Global Accelerator. Ciò consente a Global Accelerator di utilizzare indirizzi IP statici per accedere alle risorse.

Gli indirizzi IP statici rimangono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se disabiliti l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quandodeleteun acceleratore, si perdono gli indirizzi IP statici ad esso assegnati, in modo da non poter più instradare il traffico utilizzando tali indirizzi. È possibile utilizzare criteri IAM come autorizzazioni basate su tag con Global Accelerator per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

Acceleratore

Un acceleratore indirizza il traffico verso gli endpoint attraverso la rete globale AWS per migliorare le prestazioni delle applicazioni Internet. Ogni acceleratore include uno o più ascoltatori.

Esistono due tipi di acceleratori:

- Astandardindirizza il traffico verso l'endpoint AWS ottimale in base a diversi fattori, tra cui la posizione dell'utente, l'integrità dell'endpoint e i pesi dell'endpoint configurati. Questo migliora la disponibilità e le prestazioni delle applicazioni. Gli endpoint possono essere i servizi di bilanciamento del carico di rete, i bilanciamenti del carico delle applicazioni, le istanze di Amazon EC2 o gli indirizzi IP elastici.
- AInstradamento personalizzatoconsente di instradare deterministicamente più utenti a una destinazione EC2 specifica dietro l'acceleratore, come richiesto per alcuni casi d'uso. A tale scopo, indirizzare gli utenti a un indirizzo IP e una porta univoci sull'acceleratore, che Global Accelerator ha mappato alla destinazione.

Per ulteriori informazioni, consulta Tipi di acceleratori.

Nome DNS

Global Accelerator assegna a ogni acceleratore un nome DNS (Domain Name System), simile `aa1234567890abcdef.awsglobalaccelerator.com`, che punta agli indirizzi IP statici che Global Accelerator assegna all'utente o che l'utente sceglie dal proprio intervallo di indirizzi IP. A seconda del caso d'uso, è possibile utilizzare gli indirizzi IP statici dell'acceleratore o il nome DNS per instradare il traffico all'acceleratore oppure impostare record DNS per instradare il traffico utilizzando il proprio nome di dominio personalizzato.

Zona di rete

Una zona di rete gestisce gli indirizzi IP statici dell'acceleratore da una subnet IP univoca. Analogamente a una zona di disponibilità AWS, una zona di rete è un'unità isolata con un proprio set di infrastrutture fisiche. Quando si configura un acceleratore, per impostazione predefinita, Global Accelerator alloca due indirizzi IPv4. Se un indirizzo IP da una zona di rete diventa non disponibile a causa del blocco degli indirizzi IP da parte di determinate reti client o di interruzioni

di rete, le applicazioni client possono riprovare sull'indirizzo IP statico integro dall'altra zona di rete isolata.

Listener

Un listener elabora le connessioni in ingresso dai client a Global Accelerator, in base alla porta (o all'intervallo di porte) e al protocollo (o protocolli) configurati. Un listener può essere configurato per TCP, UDP o entrambi i protocolli TCP e UDP. A ogni listener sono associati uno o più gruppi di endpoint e il traffico viene inoltrato agli endpoint di uno dei gruppi. È possibile associare gruppi di endpoint ai listener specificando le aree in cui si desidera distribuire il traffico. Con un acceleratore standard, il traffico viene distribuito agli endpoint ottimali all'interno dei gruppi endpoint associati a un listener.

Gruppo di endpoint

Ogni gruppo di endpoint è associato a una regione AWS specifica. I gruppi di endpoint includono uno o più endpoint nella regione. Con un acceleratore standard, è possibile aumentare o ridurre la percentuale di traffico che altrimenti verrebbe indirizzato a un gruppo di endpoint regolando un'impostazione denominataComposizione del traffico: . La composizione del traffico consente di eseguire facilmente test delle prestazioni o test di distribuzione blu/verde, ad esempio per le nuove versioni in diverse aree AWS.

Endpoint

Un endpoint è la risorsa a cui Global Accelerator indirizza il traffico.

Gli endpoint per gli acceleratori standard possono essere Network Load Balancers, Application Load Balancers, istanze EC2 o indirizzi IP elastici. Un endpoint di Application Load Balancer può essere interno o connesso a Internet. Il traffico per gli acceleratori standard viene instradato agli endpoint in base allo stato dell'endpoint insieme alle opzioni di configurazione scelte, ad esempio i pesi degli endpoint. Per ogni endpoint, è possibile configurare i pesi, ovvero i numeri che è possibile utilizzare per specificare la proporzione di traffico da instradare a ciascuno di essi. Questo può essere utile, ad esempio, per eseguire test delle prestazioni all'interno di una regione.

Gli endpoint per gli acceleratori di routing personalizzati sono subnet di cloud privato virtuale (VPC) con una o più istanze Amazon EC2 che rappresentano le destinazioni per il traffico.

Come funziona AWS Global Accelerator

Gli indirizzi IP statici forniti da AWS Global Accelerator fungono da punti di ingresso fissi singoli per i tuoi clienti. Quando configuri l'acceleratore con Global Accelerator, associ gli indirizzi IP statici agli

endpoint regionali in una o più regioni AWS. Per gli acceleratori standard, gli endpoint sono Network Load Balancers, Application Load Balancers, Amazon EC2 istanze o indirizzi IP elastici. Per gli acceleratori di routing personalizzati, gli endpoint sono subnet VPC (Virtual Private Cloud) con una o più istanze EC2. Gli indirizzi IP statici accettano il traffico in ingresso nella rete globale AWS dalla posizione perimetrale più vicina agli utenti.

> **Note**
>
> Se porti il tuo intervallo di indirizzi IP a AWS (BYOIP) per l'utilizzo con Global Accelerator, puoi invece assegnare indirizzi IP statici dal tuo pool per l'utilizzo con l'acceleratore. Per ulteriori informazioni, consulta Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator.

Dalla posizione perimetrale, il traffico per l'applicazione viene instradato in base al tipo di acceleratore configurato.

- Per gli acceleratori standard, il traffico viene instradato all'endpoint AWS ottimale in base a diversi fattori, tra cui la posizione dell'utente, l'integrità dell'endpoint e i pesi dell'endpoint configurati.
- Per gli acceleratori di routing personalizzati, ogni client viene instradato a una specifica istanza e porta di Amazon EC2 in una subnet VPC, in base all'indirizzo IP statico esterno e alla porta del listener forniti.

Il traffico viaggia attraverso la rete globale AWS ridondante, ben monitorata e priva di congestione fino all'endpoint. Massimizzando il tempo in cui il traffico si trova sulla rete AWS, Global Accelerator assicura che il traffico venga sempre instradato sul percorso di rete ottimale.

Con alcuni tipi di endpoint (In alcune regioni AWS), è possibile conservare e accedere all'indirizzo IP del client. Due tipi di endpoint possono conservare l'indirizzo IP di origine del client nei pacchetti in ingresso: Application Load Balancers e istanze Amazon EC2. Global Accelerator non supporta la conservazione degli indirizzi IP del client per gli endpoint di Network Load Balancer e degli indirizzi IP elastici. Gli endpoint sugli acceleratori di routing personalizzati mantengono sempre l'indirizzo IP del client.

Global Accelerator interrompe le connessioni TCP dai client in posizioni edge AWS e, quasi contemporaneamente, stabilisce una nuova connessione TCP con gli endpoint. Ciò consente ai client di tempi di risposta più rapidi (latenza inferiore) e maggiore velocità effettiva.

Negli acceleratori standard, Global Accelerator monitora continuamente lo stato di tutti gli endpoint e inizia immediatamente a indirizzare il traffico verso un altro endpoint disponibile quando determina che un endpoint attivo non è integro. Ciò consente di creare un'architettura ad alta disponibilità per le applicazioni su AWS. I controlli di Health non vengono utilizzati con gli acceleratori di routing personalizzati e non vi è alcun failover, poiché si specifica la destinazione a cui instradare il traffico.

Quando si aggiunge un acceleratore, i gruppi di sicurezza e le regole AWS WAF già configurate continuano a funzionare come prima di aggiungere l'acceleratore.

Se si desidera un controllo a grana fine sul traffico globale, è possibile configurare i pesi per gli endpoint in un acceleratore standard. È inoltre possibile aumentare (composizione verso l'alto) o diminuire (composizione verso il basso) la percentuale di traffico verso un particolare gruppo di endpoint, ad esempio per test delle prestazioni o aggiornamenti dello stack.

Quando usi Global Accelerator, tieni presente quanto segue:

- AWS Direct Connect non annuncia i prefissi degli indirizzi IP per AWS Global Accelerator su un'interfaccia virtuale pubblica. Si consiglia di non pubblicizzare gli indirizzi IP utilizzati per comunicare con Global Accelerator tramite l'interfaccia virtuale pubblica AWS Direct Connect. Se si pubblicizzano gli indirizzi IP utilizzati per comunicare con Global Accelerator tramite l'interfaccia virtuale pubblica AWS Direct Connect, si tradurrà in un flusso di traffico asimmetrico: il traffico verso Global Accelerator passa a Global Accelerator tramite Internet, ma il traffico viene restituito al locale arriva sulla tua interfaccia virtuale pubblica AWS Direct Connect.
- Global Accelerator non supporta l'aggiunta come endpoint di una risorsa appartenente a un altro account AWS.

Argomenti

Timeout di inattività in AWS Global Accelerator

AWS Global Accelerator imposta un periodo di timeout inattività che si applica alle sue connessioni. Se allo scadere di questo periodo di timeout di inattività non vengono inviati o ricevuti dati, Global

Accelerator chiude la connessione. Per garantire che la connessione rimanga attiva, il client o l'endpoint deve inviare almeno 1 byte di dati prima che scada il periodo di timeout di inattività.

Il timeout di inattività Global Accelerator per una connessione di rete dipende dal tipo di connessione:

- Il timeout è 340 secondi per le connessioni TCP.
- Il timeout è 30 secondi per le connessioni UDP.

Global Accelerator continua a dirigere il traffico verso un endpoint fino a quando non viene raggiunto il timeout di inattività, anche se l'endpoint è contrassegnato come non integro. Global Accelerator seleziona un nuovo endpoint, se necessario, solo all'avvio di una nuova connessione o dopo un timeout di inattività.

Indirizzi IP statici in AWS Global Accelerator

È possibile utilizzare gli indirizzi IP statici assegnati da Global Accelerator all'acceleratore, o specificati dal proprio pool di indirizzi IP, per gli acceleratori standard, per instradare il traffico Internet alla rete globale AWS vicino a dove si trovano gli utenti, indipendentemente dalla loro posizione. Per gli acceleratori standard, gli indirizzi vengono associati a Network Load Balancers, Application Load Balancers, istanze Amazon EC2 o indirizzi IP elastici eseguiti in una singola area AWS o in più regioni. Per gli acceleratori di routing personalizzati, è possibile indirizzare il traffico verso destinazioni EC2 nelle subnet VPC in una o più aree geografiche. Il routing del traffico attraverso la rete globale AWS migliora la disponibilità e le prestazioni perché il traffico non deve portare più hop su Internet pubblico. L'utilizzo di indirizzi IP statici consente inoltre di distribuire il traffico delle applicazioni in ingresso tra più risorse endpoint in più aree AWS.

Inoltre, l'utilizzo di indirizzi IP statici semplifica l'aggiunta dell'applicazione a più aree geografiche o la migrazione di applicazioni tra aree geografiche. L'utilizzo di indirizzi IP fissi significa che gli utenti dispongono di un modo coerente per connettersi all'applicazione durante le modifiche.

Se lo desideri, puoi associare il tuo nome di dominio personalizzato agli indirizzi IP statici del tuo acceleratore. Per ulteriori informazioni, consulta Instradare il traffico di dominio personalizzato all'acceleratore.

Global Accelerator ti fornisce gli indirizzi IP statici dal pool di indirizzi IP Amazon, a meno che tu non porti il tuo intervallo di indirizzi IP in AWS e quindi specifichi gli indirizzi IP statici di quel pool. (Per ulteriori informazioni, consulta Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator.) Per creare un acceleratore sulla console, il primo passo consiste nel richiedere a Global Accelerator di

eseguire il provisioning degli indirizzi IP statici immettendo un nome per l'acceleratore o scegliendo i propri indirizzi IP statici. Per visualizzare i passaggi per la creazione di un acceleratore, vedereAWS Global Accelerator: .

Gli indirizzi IP statici rimangono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se disabiliti l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quandodeleteun acceleratore, si perdono gli indirizzi IP statici ad esso assegnati, in modo da non poter più instradare il traffico utilizzando tali indirizzi. È possibile utilizzare criteri IAM come autorizzazioni basate su tag con Global Accelerator per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

Gestione del flusso di traffico con quadranti del traffico e pesi degli endpoint

Esistono due modi per personalizzare il modo in cui AWS Global Accelerator invia il traffico ai tuoi endpoint con un acceleratore standard:

- Modificare la composizione del traffico per limitare il traffico per uno o più gruppi di endpoint
- Specificare i pesi per modificare la proporzione di traffico rispetto agli endpoint di un gruppo

Come funzionano i quadranti del traffico

Per ogni gruppo di endpoint in un acceleratore standard, è possibile impostare una composizione del traffico per controllare la percentuale di traffico inviata al gruppo di endpoint. La percentuale viene applicata solo al traffico già indirizzato al gruppo di endpoint, non a tutto il traffico del listener.

La composizione del traffico limita la parte di traffico accettata da un gruppo di endpoint, espressa come percentuale del traffico diretto a tale gruppo di endpoint. Ad esempio, se si imposta la composizione del traffico per un gruppo di endpoint in`us-east-1a` 50 (ovvero 50%) e l'acceleratore indirizza 100 richieste utente a tale gruppo di endpoint, solo 50 richieste vengono accettate dal gruppo. L'acceleratore indirizza le restanti 50 richieste ai gruppi di endpoint in altre regioni.

Per ulteriori informazioni, consulta Regolazione del flusso di traffico con le manopole.

Come funzionano i pesi

Per ogni endpoint di un acceleratore standard, è possibile specificare pesi, ovvero numeri che modificano la proporzione di traffico indirizzato dall'acceleratore a ciascun endpoint. Questo può essere utile, ad esempio, per eseguire test delle prestazioni all'interno di una regione.

Un peso è un valore che determina la proporzione di traffico che l'acceleratore indirizza verso un endpoint. Per impostazione predefinita, il peso di un punto finale è 128, ovvero la metà del valore massimo di un peso, 255.

L'acceleratore calcola la somma dei pesi per gli endpoint in un gruppo endpoint, quindi indirizza il traffico verso gli endpoint in base al rapporto tra il peso di ciascun endpoint e il totale. Per un esempio di come funzionano i pesi, consulta Pesi dell'endpoint: .

I quadranti e i pesi del traffico influenzano il modo in cui l'acceleratore standard serve il traffico in diversi modi:

- Configurare i quadranti del traffico perGruppi di endpoint: . La composizione del traffico consente di interrompere una percentuale del traffico, o di tutto il traffico, verso il gruppo, chiamando verso il basso il traffico che l'acceleratore ha già indirizzato in base ad altri fattori, ad esempio la prossimità.
- I pesi vengono invece utilizzati per impostare i valori perSingole endpointall'interno di un gruppo di endpoint. I pesi consentono di dividere il traffico all'interno del gruppo di endpoint. Ad esempio, è possibile utilizzare i pesi per eseguire test delle prestazioni per endpoint specifici in una regione.

> **Note**
>
> Per ulteriori informazioni su come influiscono sul failover i quadranti e i pesi del traffico, consultaFailover per endpoint non integri: .

Controlli di Health per AWS Global Accelerator

Per gli acceleratori standard, AWS Global Accelerator controlla automaticamente lo stato degli endpoint associati agli indirizzi IP statici e quindi indirizza il traffico degli utenti solo agli endpoint integri.

Global Accelerator include controlli di integrità predefiniti eseguiti automaticamente, ma è possibile configurare la tempistica per i controlli e altre opzioni. Se sono state configurate impostazioni di controllo dello stato personalizzate, Global Accelerator utilizza tali impostazioni in modi specifici, a seconda della configurazione. È possibile configurare tali impostazioni nell'istanza di Global Accelerator per Amazon EC2 o negli endpoint degli indirizzi IP elastici oppure configurando le impostazioni nella console Elastic Load Balancing ad Balancer per Network Load Balancers o Application Load Balancer. Per ulteriori informazioni, consulta Opzioni controllo dello stato.

Quando si aggiunge un endpoint a un acceleratore standard, questo deve superare un controllo di integrità per essere considerato integro prima che il traffico venga indirizzato ad esso. Se Global Accelerator non dispone di endpoint integri a cui instradare il traffico in un acceleratore standard, invia le richieste a tutti gli endpoint.

Tipi di acceleratori

Esistono due tipi di acceleratori che è possibile utilizzare con AWS Global Accelerator:Acceleratori standardeacceleratori di routing personalizzati: . Entrambi i tipi di acceleratori instradano il traffico sulla rete globale AWS per migliorare le prestazioni e la stabilità, ma sono progettati per le diverse esigenze applicative.

Acceleratore standard

Utilizzando un acceleratore standard, è possibile migliorare la disponibilità e le prestazioni delle applicazioni in esecuzione su istanze di bilanciamento del carico delle applicazioni, bilanciamento del carico di rete o Amazon EC2. Con un acceleratore standard, Global Accelerator instrada il traffico client tra gli endpoint regionali in base alla geo-prossimità e all'integrità degli endpoint. Consente inoltre ai clienti di spostare il traffico client tra gli endpoint in base a controlli quali quadranti del traffico e pesi degli endpoint. Questo funziona per un'ampia varietà di casi d'uso, tra cui distribuzione blu/verde, test A/B e distribuzione in più aree. Per visualizzare altri casi d'uso, vedere Case d'uso AWS Global Accelerator: .

Per ulteriori informazioni, vedi Lavorare con gli acceleratori standard in AWS Global Accelerator.

Acceleratore di routing personalizzato

Gli acceleratori di routing personalizzati funzionano bene per scenari in cui si desidera utilizzare la logica dell'applicazione personalizzata per indirizzare uno o più utenti verso una destinazione e una porta specifiche tra molti, pur ottenendo i vantaggi in termini di prestazioni di Global Accelerator. Un esempio è rappresentato dalle applicazioni VoIP che assegnano più chiamanti a un server multimediale specifico per avviare sessioni vocali, video e di messaggistica. Un altro esempio sono le applicazioni di gioco online in tempo reale in cui si desidera assegnare più giocatori a una singola sessione su un server di gioco in base a fattori quali la posizione geografica, l'abilità del giocatore e la modalità di gioco.

Per ulteriori informazioni, vedi Utilizzare acceleratori di routing personalizzati in AWS Global Accelerator.

In base alle esigenze specifiche, è possibile creare uno di questi tipi di acceleratori per accelerare il traffico dei clienti.

Intervalli di ubicazione e indirizzi IP dei server edge di Global Accelerator

Per un elenco di edge server di Global Accelerator, consulta laDove viene distribuito oggi AWS Global Accelerator?nella sezioneDomande frequenti su AWS Global Accelerator(Certificato creato).

AWS pubblica gli intervalli di indirizzi IP attuali in formato JSON. Per visualizzare gli intervalli correnti, scaricaip-ranges.json: . Per ulteriori informazioni, consulta Intervalli di indirizzi IP di AWS nella Amazon Web Services General Reference.

Per trovare intervalli di indirizzi IP associati a server edge edge AWS Global Accelerator, cerca`ip-ranges.json`Per la seguente stringa:

```
"service": "GLOBALACCELERATOR"
```

Voci dell'acceleratore globale che includono`"region": "GLOBAL"`fanno riferimento agli indirizzi IP statici allocati agli acceleratori. Se si desidera filtrare il traffico attraverso l'acceleratore proveniente dai punti di presenza (POP) in un'area, filtrare le voci che includono un'area geografica specifica, ad esempio`us-*`o`eu-*`: . Quindi, ad esempio, se si filtra per`us-*`, vedrai solo il traffico proveniente dai POP negli Stati Uniti (Stati Uniti).

Case d'uso AWS Global Accelerator

L'uso di AWS Global Accelerator consente di raggiungere diversi obiettivi. Questa sezione elenca alcuni di essi, per darvi un'idea su come utilizzare Global Accelerator per soddisfare le vostre esigenze.

Scalabilità per un maggiore utilizzo delle applicazioni

Quando l'utilizzo delle applicazioni aumenta, aumenta anche il numero di indirizzi IP ed endpoint che è necessario gestire. Global Accelerator consente di scalare la rete verso l'alto o verso il basso. Consente di associare risorse internazionali, ad esempio i bilanciamenti del carico e le istanze di Amazon EC2, a due indirizzi IP statici. Questi indirizzi vengono inclusi negli elenchi consentiti solo una volta nelle applicazioni client, nei firewall e nei record DNS. Con Global Accelerator, è possibile aggiungere o rimuovere endpoint nelle regioni AWS, eseguire la distribuzione blu/verde ed eseguire test A/B senza dover aggiornare gli indirizzi IP nelle

applicazioni client. Ciò è particolarmente utile per i casi d'uso IoT, retail, media, automotive e sanitario in cui non è possibile aggiornare facilmente le applicazioni client di frequente.

Accelerazione per applicazioni sensibili alla latenza

Molte applicazioni, in particolare in aree come i giochi, i media, le app mobili e i dati finanziari, richiedono una latenza molto bassa per un'esperienza utente eccezionale. Per migliorare l'esperienza utente, Global Accelerator indirizza il traffico degli utenti all'endpoint dell'applicazione più vicino al client, riducendo la latenza Internet e il jitter. Global Accelerator indirizza il traffico alla posizione perimetrale più vicina utilizzando Anycast, quindi lo instrada all'endpoint regionale più vicino sulla rete globale AWS. Global Accelerator reagisce rapidamente ai cambiamenti nelle prestazioni di rete per migliorare le prestazioni delle applicazioni degli utenti.

Ripristino di emergenza e resilienza in più regioni

Per essere disponibile, devi essere in grado di fare affidamento sulla rete. Potresti eseguire l'applicazione in più aree AWS per supportare il ripristino di emergenza, una maggiore disponibilità, una latenza inferiore o la conformità. Se Global Accelerator rileva che l'endpoint dell'applicazione non funziona nella regione AWS primaria, attiva immediatamente il re-routing del traffico verso l'endpoint dell'applicazione nella regione AWS più vicina e disponibile.

Protezione delle applicazioni

L'esposizione delle origini AWS, ad esempio Application Load Balancers o istanze Amazon EC2, al traffico Internet pubblico crea un'opportunità per attacchi dannosi. Global Accelerator riduce il rischio di attacco mascherando la tua origine dietro due punti di ingresso statici. Questi punti di ingresso sono protetti per impostazione predefinita dagli attacchi DDoS (Distributed Denial of Service) con AWS Shield. Global Accelerator crea una connessione di peering con Amazon Virtual Private Cloud utilizzando indirizzi IP privati, mantenendo le connessioni ai tuoi Application Load Balancer interni o alle istanze EC2 private fuori da Internet pubblico.

Migliorare le prestazioni per VoIP o applicazioni di gioco online

Utilizzando un acceleratore di routing personalizzato, è possibile sfruttare i vantaggi in termini di prestazioni di Global Accelerator per le applicazioni VoIP o di gioco. Ad esempio, è possibile utilizzare Global Accelerator per applicazioni di gioco online che assegnano più giocatori a una singola sessione di gioco. Usa Global Accelerator per ridurre la latenza e il jitter a livello globale per le applicazioni che richiedono una logica personalizzata per mappare gli utenti a endpoint specifici, come giochi multiplayer o chiamate VoIP. È possibile utilizzare un singolo acceleratore per connettere i client a migliaia di istanze Amazon EC2 in esecuzione in una o più regioni AWS, mantenendo il pieno controllo su quale client è indirizzato a quale istanza e porta EC2.

Strumento AWS Global Accelerator

Puoi utilizzare lo strumento AWS Global Accelerator Speed Comparation Tool per visualizzare le velocità di download di Global Accelerator rispetto ai download diretti su Internet, nelle regioni AWS. Questo strumento consente di utilizzare il browser per vedere la differenza di prestazioni quando si trasferiscono dati utilizzando Global Accelerator. È possibile scegliere una dimensione del file da scaricare e lo strumento scarica i file tramite HTTPS/TCP da Application Load Balancers in diverse aree geografiche al browser. Per ogni regione, viene visualizzato un confronto diretto delle velocità di download.

Per accedere allo strumento di confronto velocità, copiare il seguente URL nel browser:

```
https://speedtest.globalaccelerator.aws
```

> **Important**
>
> I risultati possono differire quando si esegue il test più volte. I tempi di download possono variare in base a fattori esterni a Global Accelerator, quali la qualità, la capacità e la distanza della connessione nella rete dell'ultimo miglio in uso.

Come iniziare a utilizzare AWS Global Accelerator

Puoi iniziare a configurare AWS Global Accelerator utilizzando l'API o la console AWS Global Accelerator. Poiché Global Accelerator è un servizio globale, non è legato a una regione AWS specifica. Si noti che Global Accelerator è un servizio globale che supporta gli endpoint in più aree AWS, ma è necessario specificare l'area Stati Uniti occidentali (Oregon) per creare o aggiornare gli acceleratori.

Per iniziare a utilizzare Global Accelerator, attenersi alla seguente procedura generale:

1. Scegliere il tipo di acceleratore che si desidera creare: Un acceleratore standard o un acceleratore di routing personalizzato.
2. Configurare la configurazione iniziale per Global Accelerator: Specifica un nome per l'acceleratore. Configurare quindi uno o più listener per elaborare le connessioni in ingresso dai client, in base al protocollo e alla porta (o all'intervallo di porte) specificati.

3. Configurare i gruppi di endpoint regionali per l'acceleratore: È possibile selezionare uno o più gruppi di endpoint regionali da aggiungere al listener. Il listener instrada le richieste agli endpoint aggiunti a un gruppo di endpoint.

   Per un acceleratore standard, Global Accelerator monitora lo stato degli endpoint all'interno del gruppo utilizzando le impostazioni di controllo dello stato definite per ciascuno degli endpoint. Per ogni gruppo di endpoint in un acceleratore standard, è possibile configurare unComposizione del traffico percentuale per controllare la percentuale di traffico che un gruppo di endpoint accetterà. La percentuale viene applicata solo al traffico già indirizzato al gruppo di endpoint, non a tutto il traffico del listener. Per impostazione predefinita, la composizione del traffico è impostata su 100% per tutti i gruppi di endpoint regionali.

   Per gli acceleratori di routing personalizzati, il traffico viene instradato in modo deterministico a una destinazione specifica in una subnet VPC, in base alla porta del listener su cui viene ricevuto il traffico.
4. Aggiungere endpoint ai gruppi di endpoint: Gli endpoint aggiunti dipendono dal tipo di acceleratore.
   - Per un acceleratore standard, è possibile aggiungere a ciascun gruppo di endpoint una o più risorse regionali, ad esempio i bilanciamenti del carico o gli endpoint delle istanze EC2. Successivamente, è possibile decidere la quantità di traffico da instradare a ciascun endpoint impostando i pesi degli endpoint.
   - Per un acceleratore di routing personalizzato, aggiungi una o più subnet di cloud privato virtuale (VPC) con un massimo di migliaia di destinazioni di istanza Amazon EC2.

Per istruzioni dettagliate su come creare un acceleratore standard o un acceleratore di routing personalizzato utilizzando la console AWS Global Accelerator, vedereAWS Global Accelerator: . Per utilizzare le operazioni API, consultaAzioni comuni che è possibile utilizzare con AWS Global Acceleratore laRiferimento all'API AWS Global Accelerator: .

Tagging in AWS Global Accelerator

I tag sono parole o frasi (metadati) che utilizzi per identificare e organizzare le risorse AWS. Puoi aggiungere più tag a ogni risorsa e ogni tag include una chiave e un valore che definisci. Ad esempio, la chiave potrebbe essere`environment`e il valore potrebbe essere`production`: . Puoi cercare e filtrare le risorse in base ai tag che aggiungi. In AWS Global Accelerator, è possibile taggare gli acceleratori.

Di seguito sono riportati due esempi di come può essere utile lavorare con i tag in Global Accelerator:

- Utilizza i tag per monitorare le informazioni di fatturazione in diverse categorie. A tale scopo, applica i tag agli acceleratori o ad altre risorse AWS (ad esempio, Network Load Balancers, Application Load Balancers o Amazon EC2) e attiva i tag. AWS genera quindi un report di allocazione dei costi come un valore separato da virgole (file CSV) con l'utilizzo e i costi aggregati in base ai tuoi tag attivi. Puoi applicare i tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari) per organizzare i costi tra più servizi. Per ulteriori informazioni, consulta Utilizzo dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing and Cost Management.
- Utilizzare i tag per applicare le autorizzazioni basate su tag per gli acceleratori. A tale scopo, creare criteri IAM che specificano tag e valori di tag per consentire o non consentire azioni. Per ulteriori informazioni, consulta Policy basate su tag.

Per le convenzioni di utilizzo e i collegamenti ad altre risorse sull'assegnazione dei tag, vedereTagging delle risorse AWSnellaRiferimenti generali AWS: . Per suggerimenti sull'utilizzo dei tag, vedereTagging Best practice: Strategia di tagging delle risorsenellaWhitepaper di AWSBlog.

Per conoscere il numero massimo di tag che puoi aggiungere a una risorsa in Global Accelerator, consultaQuote per AWS Global Accelerator: .

È possibile aggiungere e aggiornare i tag utilizzando la console AWS, l'interfaccia a riga di comando di AWS o l'API di Global Accelerator. Questo capitolo include i passaggi per l'utilizzo di tag nella console. Per ulteriori informazioni sull'utilizzo dei tag tramite l'interfaccia della riga di comando AWS e l'API Global Accelerator, inclusi gli esempi di CLI, vedere le operazioni seguenti nellaRiferimento all'API AWS Global Accelerator:

- CreateAccelerator
- TagResource
- UntagResource
- ListTagsForResource

Supporto tagging in Global Accelerator

AWS Global Accelerator supporta il tagging per gli acceleratori.

Global Accelerator supporta la funzionalità di controllo degli accessi basata su tag di AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Policy basate su tag.

Aggiunta, modifica ed eliminazione di tag in Global Accelerator

La procedura seguente descrive come aggiungere, modificare ed eliminare tag per gli acceleratori nella console di Global Accelerator.

> **Note**
>
> È possibile aggiungere o rimuovere tag utilizzando le operazioni della console, l'interfaccia a riga di comando di AWS o l'API di Global Accelerator. Per ulteriori informazioni, inclusi esempi di CLI, consultaTagResourcenellaRiferimento all'API AWS Global Accelerator: .

Per aggiungere tag, modificare o eliminare tag in Global Accelerator

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Scegliere l'acceleratore di cui si desidera aggiungere o aggiornare i tag.
3. NellaTagsPuoi eseguire le seguenti operazioni:

   Aggiungere un tag

   ScegliereAggiungi tagInserisci una chiave e, facoltativamente, un valore per il tag.

   Modificare un tag

   Aggiornare il testo di una chiave, un valore o entrambi. È inoltre possibile cancellare il valore di un tag, ma la chiave è obbligatoria.

   Eliminare un tag

   ScegliereRemoveA destra del campo valori.
4. Seleziona Save changes (Salva modifiche).

Prezzi per AWS Global Accelerator

I prezzi di AWS Global Accelerator sono calcolati in base all'uso effettivo. Per ogni acceleratore nel tuo account verrà addebitata una tariffa oraria e i costi di trasferimento dati. Per ulteriori informazioni, consultaPrezzi AWS Global Accelerator: .

AWS Global Accelerator

Queste esercitazioni forniscono i passaggi per iniziare a utilizzare AWS Global Accelerator utilizzando la console. Puoi anche usare le operazioni API AWS Global Accelerator per creare e personalizzare i tuoi acceleratori. Ad ogni passaggio di questa esercitazione, c'è un collegamento all'operazione API corrispondente per completare l'attività a livello di programmazione. Quando si imposta un acceleratore di routing personalizzato, è necessario utilizzare l'API per alcuni passaggi di configurazione. Per ulteriori informazioni su come utilizzare le operazioni dell'API AWS Global Accelerator, consulta laInformazioni su AWS Global Accelerator: .

> **Tip**
>
> Per scoprire come utilizzare Global Accelerator per migliorare le prestazioni e la disponibilità delle applicazioni Web, consulta il seguente workshop autogestico: AWS Global Accelerator: .

Global Accelerator è un servizio globale che supporta gli endpoint in più regioni AWS, elencati nella sezioneTabella delle regioni AWS: .

Questo capitolo include due esercitazioni: una per la creazione di un acceleratore standard e una per la creazione di un acceleratore di routing personalizzato. Per ulteriori informazioni sui due tipi di acceleratori, consultaLavorare con gli acceleratori standard in AWS Global AcceleratoreUtilizzare acceleratori di routing personalizzati in AWS Global Accelerator: .

Argomenti

- NOzioni di base su un acceleratore di serie
- Introduzione a un acceleratore di routing personalizzato

NOzioni di base su un acceleratore di serie

Questa sezione fornisce i passaggi per la creazione di un acceleratore standard per indirizzare il traffico a un endpoint ottimale.

Attività

- Prima di iniziare

- Fase 1: Creazione di un accelerator
- Fase 2: Aggiunta di un listener
- Fase 3: Aggiungere gruppi di endpoint.
- Fase 4: Aggiungi endpoint
- Fase 5: Verifica il tuo accelerator
- Passaggio 6 (facoltativo): Eliminazione dell'accelerator

Prima di iniziare

Prima di creare un acceleratore, creare almeno una risorsa che è possibile aggiungere come endpoint a cui indirizzare il traffico. Ad esempio, creare uno dei seguenti comandi:

- Avvia almeno un'istanza Amazon EC2 da aggiungere come endpoint. Per ulteriori informazioni, consultaCrea le risorse EC2 e avvia l'istanza EC2nellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux: .
- Facoltativamente, creare uno o più servizi di bilanciamento del carico di rete o di bilanciamento del carico applicazioni che includano istanze EC2. Per ulteriori informazioni, consultaCreare un sistema di bilanciamento del carico dell'applicazione Network Load BalancernellaGuida per l'utente dei sistemi Network Load Balancer: .

Quando si crea una risorsa da aggiungere a Global Accelerator, tenere presente quanto segue:

- Quando si aggiunge un Application Load Balancer interno o un endpoint di istanza EC2 in Global Accelerator, si abilita il flusso del traffico Internet direttamente da e verso l'endpoint nei cloud privati virtuali (VPC) tramite il targeting in una subnet privata. Il VPC contenente il sistema di bilanciamento del carico o l'istanza EC2 deve disporre digateway Internetcollegato ad esso, per indicare che il VPC accetta traffico Internet. Per ulteriori informazioni, consulta Connessioni VPC sicure in AWS Global Accelerator.
- Global Accelerator richiede le regole del router e del firewall per consentire al traffico in ingresso dagli indirizzi IP associati ai controlli integrità Route 53 di completare i controlli di integrità per l'istanza EC2 o gli endpoint degli indirizzi IP elastici. Puoi trovare informazioni sugli intervalli di indirizzi IP associati ai controlli sanitari di Amazon Route 53 inControlli dello stato per i gruppi targetnellaAmazon Route 53: .

Fase 1: Creazione di un accelerator

Per creare il tuo acceleratore, inserisci un nome.

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateAcceleratornellaInformazioni su AWS Global Accelerator: .

Per creare un accelerator

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. ScegliereCrea accelerator: .
3. Fornire un nome per l'acceleratore.
4. Eventualmente, aggiungere uno o più tag per facilitare l'identificazione delle risorse di Global Accelerator.
5. Seleziona Successivo.

Fase 2: Aggiunta di un listener

Create un listener per elaborare le connessioni in ingresso dagli utenti a Global Accelerator.

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateListenernellaAWS Global Accelerator: .

Per creare un listener

1. SulAggiungi listenerimmettere le porte o gli intervalli di porte che si desidera associare al listener. Le porte 1-65535 sono supportate dai listener.
2. Scegliere il protocollo o i protocolli per le porte immesse.
3. Facoltativamente, scegliere di abilitare l'affinità client. L'affinità client per un listener significa che Global Accelerator garantisce che le connessioni da un indirizzo IP di origine specifico (client)

vengano sempre instradate allo stesso endpoint. Per abilitare questo comportamento, nell'elenco a discesa selezionareIP di origine: .

Il valore predefinito èNessuna, il che significa che l'affinità client non è abilitata e Global Accelerator distribuisce il traffico equamente tra gli endpoint nei gruppi di endpoint per il listener.

Per ulteriori informazioni, consulta Affinità del client.

4. Facoltativamente, scegliereAggiungi listenerper aggiungere un listener aggiuntivo.
5. Dopo aver aggiunto i listener, selezionareSuccessivo: .

Fase 3: Aggiungere gruppi di endpoint.

Aggiungere uno o più gruppi di endpoint, ognuno dei quali è associato a una regione AWS specifica.

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateEndPointGroupnellaAWS Global Accelerator: .

Per aggiungere un gruppo di endpoint.

1. SulAggiungere gruppi di endpoint., nella sezione relativa a un listener, scegliere unRegiondall'elenco a discesa.
2. Facoltativamente, perComposizione del traffico, immettere un numero compreso tra 0 e 100 per impostare una percentuale di traffico per questo gruppo di endpoint. La percentuale viene applicata solo al traffico già indirizzato a questo gruppo di endpoint, non a tutto il traffico del listener. Per impostazione predefinita, la composizione del traffico per un gruppo di endpoint è impostata su 100 (ovvero 100%).
3. Facoltativamente, per i valori di controllo dello stato personalizzati, sceglieriConfigurazione dei controlli dello stato: . Quando si configurano le impostazioni di controllo dello stato, Global Accelerator utilizza le impostazioni per i controlli di integrità per gli endpoint dell'istanza EC2 e degli indirizzi IP elastici. Per gli endpoint Network Load Balancer e Application Load Balancer, Global Accelerator utilizza le impostazioni di controllo dello stato già configurate per i bilanciatori stessi. Per ulteriori informazioni, consulta Opzioni controllo dello stato.
4. Facoltativamente, sceglieriAggiungi gruppo di endpointPer aggiungere ulteriori gruppi di endpoint per questo listener o altri listener.

5. Seleziona Successivo.

Fase 4: Aggiungi endpoint

Aggiungere uno o più endpoint associati a gruppi di endpoint specifici. Questo passaggio non è obbligatorio, ma nessun traffico viene indirizzato agli endpoint in una regione a meno che gli endpoint non siano inclusi in un gruppo di endpoint.

> **Note**
>
> Se si sta creando l'acceleratore a livello di programmazione, si aggiungono endpoint come parte dell'aggiunta di gruppi di endpoint. Per ulteriori informazioni, consultaCreateEndPointGroupnellaAWS Global Accelerator: .

Per aggiungere gli endpoint

1. SulCreazione di endpoint, nella sezione relativa a un endpoint, scegliere unEndpoint: .
2. Facoltativamente, perPeso, immettere un numero compreso tra 0 e 255 per impostare un peso per il routing del traffico a questo endpoint. Quando si aggiungono pesi agli endpoint, è possibile configurare Global Accelerator per instradare il traffico in base alle proporzioni specificate. Per impostazione predefinita, tutti gli endpoint hanno un peso di 128. Per ulteriori informazioni, consulta Pesi dell'endpoint.
3. Eventualmente, per un endpoint Application Load Balancer, inPreserve indirizzo IP del clientSELECTPreserve indirizzo: . Per ulteriori informazioni, consulta Conservare gli indirizzi IP client in AWS Global Accelerator.
4. Facoltativamente, scegliereAggiunta di un endpointper aggiungere altri endpoint.
5. Seleziona Successivo.

Dopo aver sceltoSuccessivo, nel dashboard Acceleratore globale verrà visualizzato un messaggio che indica che l'acceleratore è in corso. Al termine del processo, lo stato dell'acceleratore nel cruscotto èActive (Attivo): .

Fase 5: Verifica il tuo accelerator

Effettua la procedura per testare l'acceleratore per assicurarti che il traffico venga indirizzato verso gli endpoint. Ad esempio, esegui un comando curl come il seguente, sostituendo uno degli indirizzi

IP statici dell'acceleratore, per mostrare le regioni AWS in cui vengono elaborate le richieste. Ciò è particolarmente utile se si impostano pesi diversi per gli endpoint o si regola la composizione del traffico nei gruppi di endpoint.

Eseguire un comando curl come il seguente, sostituendo uno degli indirizzi IP statici dell'acceleratore, per chiamare l'indirizzo IP 100 volte e quindi generare un conteggio di dove ogni richiesta è stata elaborata.

```
for ((i=0;i<100;i++)); do  curl http://198.51.100.0/ >> output.txt; done; cat
 output.txt | sort | uniq -c ; rm output.txt;
```

Se è stata regolata la composizione del traffico su qualsiasi gruppo di endpoint, questo comando consente di confermare che l'acceleratore sta indirizzando le percentuali corrette di traffico a gruppi diversi. Per ulteriori informazioni, consulta gli esempi dettagliati nel seguente post sul blog,Gestione del traffico con AWS Global Accelerator: .

Passaggio 6 (facoltativo): Eliminazione dell'accelerator

Se è stato creato un acceleratore come test o se non si utilizza più un acceleratore, è possibile eliminarlo. Sulla console, disabilitare l'acceleratore e quindi eliminarlo. Non è necessario rimuovere i listener e i gruppi di endpoint dall'acceleratore.

Per eliminare un acceleratore utilizzando un'operazione API anziché la console, è necessario rimuovere tutti i listener e i gruppi di endpoint associati all'acceleratore e disabilitarlo. Per ulteriori informazioni, consulta la .DeleteAcceleratoroperazione nellaAWS Global Accelerator: .

Quando si rimuovono endpoint o gruppi di endpoint o si elimina un acceleratore, tenere presente quanto segue:

- Quando si crea un acceleratore, Global Accelerator fornisce un set di due indirizzi IP statici. Gli indirizzi IP vengono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se si disattiva l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quandodeleteun acceleratore, si perdono gli indirizzi IP statici assegnati all'acceleratore, quindi non è più possibile instradare il traffico utilizzando tali indirizzi. Come procedura consigliata, assicurarsi di disporre delle autorizzazioni per evitare di eliminare involontariamente gli acceleratori. È possibile utilizzare i criteri IAM con Global Accelerator, ad esempio le autorizzazioni basate su tag, per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

- Se si termina un'istanza EC2 prima di rimuoverla da un gruppo di endpoint in Global Accelerator e quindi si crea un'altra istanza con lo stesso indirizzo IP privato e si passa i controlli di integrità, Global Accelerator instraderà il traffico al nuovo endpoint. Se non si desidera che ciò accada, rimuovere l'istanza EC2 dal gruppo endpoint prima di terminare l'istanza.

Per eliminare un accelerator

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Scegliere l'acceleratore da eliminare.
3. Seleziona Edit (Modifica).
4. ScegliereDisabilita acceleratore quindi sceglieSave (Salva): .
5. Scegliere l'acceleratore da eliminare.
6. SceglieEliminazione dell'accelerator: .
7. Nella finestra di dialogo di conferma, seleziona Delete (Elimina).

Introduzione a un acceleratore di routing personalizzato

In questa sezione vengono illustrati i passaggi per creare un acceleratore di routing personalizzato che instrada il traffico in modo deterministico alle destinazioni dell'istanza di Amazon EC2 negli endpoint della sottorete di cloud privato virtuale (VPC).

Attività

- Prima di iniziare
- Fase 1: Creazione di un accelerator di routing personalizzato
- Fase 2: Aggiunta di un listener
- Fase 3: Aggiungere gruppi di endpoint.
- Fase 4: Aggiungi endpoint
- Passaggio 5 (facoltativo): Eliminazione dell'accelerator

Prima di iniziare

Prima di creare un acceleratore di routing personalizzato, creare una risorsa che è possibile aggiungere come endpoint a cui indirizzare il traffico. Un endpoint dell'acceleratore di routing

personalizzato deve essere una sottorete di cloud privato virtuale (VPC), che può includere più istanze Amazon EC2. Per le istruzioni su come creare le risorse, consulta:

- Creazione di una sottorete VPC. Per ulteriori informazioni, consultaCrea e configura il VPCnellaAWS Directory Service: .
- Eventualmente, avviare una o più istanze Amazon EC2 nel VPC. Per ulteriori informazioni, consultaCrea le risorse EC2 e avvia l'istanza EC2nellaGuida per l'utente di Amazon EC2 User Guide per le istanze Linux: .

Quando si crea una risorsa da aggiungere a Global Accelerator, tenere presente quanto segue:

- Quando si aggiunge un endpoint di istanza EC2 in Global Accelerator, si abilita il flusso del traffico Internet direttamente da e verso l'endpoint nei VPC indirizzandolo in una subnet privata. Il VPC contenente l'istanza EC2 deve avere ungateway Internetcollegato ad esso, per indicare che il VPC accetta traffico Internet. Per ulteriori informazioni, consulta Connessioni VPC sicure in AWS Global Accelerator.

Fase 1: Creazione di un accelerator di routing personalizzato

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateCustomRoutingAcceleratornellaAWS Global Accelerator: .

Per creare un accelerator

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Fornire un nome per l'acceleratore.
3. PerTipo di acceleratoreSELECTInstradamento personalizzato: .
4. Eventualmente, aggiungere uno o più tag per facilitare l'identificazione delle risorse dell'acceleratore.
5. ScegliereSuccessivoper aggiungere listener, gruppi di endpoint e endpoint di subnet VPC.

Fase 2: Aggiunta di un listener

Create un listener per elaborare le connessioni in ingresso dagli utenti a Global Accelerator.

L'intervallo specificato quando si crea un listener definisce il numero di combinazioni di porte e indirizzi IP di destinazione che è possibile utilizzare con l'acceleratore di routing personalizzato. Per garantire la massima flessibilità, si consiglia di specificare un intervallo di porte ampio. Ogni intervallo di porte del listener specificato deve includere un minimo di 16 porte.

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateCustomRoutingListenernellaAWS Global Accelerator: .

Per creare un listener

1. SulAggiungi listenerimmettere le porte o gli intervalli di porte che si desidera associare al listener. Le porte 1-65535 sono supportate dai listener.
2. Scegliere il protocollo o i protocolli per le porte immesse.
3. Facoltativamente, scegliereAggiungi listenerper aggiungere un listener aggiuntivo.
4. Dopo aver aggiunto i listener, selezionareSuccessivo: .

Fase 3: Aggiungere gruppi di endpoint.

Aggiungere uno o più gruppi di endpoint, ognuno dei quali è associato a una regione AWS specifica. Per ogni gruppo di endpoint, specificare uno o più insiemi di intervalli di porte e protocolli. Global Accelerator li utilizza per indirizzare il traffico verso le istanze Amazon EC2 nelle subnet nella regione.

Per ogni intervallo di porte fornito, è inoltre necessario specificare il protocollo da utilizzare: UDP, TCP o UDP e TCP.

> **Note**
>
> Per completare questa attività utilizzando un'operazione API anziché la console, consultaCreateCustomRoutingEndPointGroupnellaAWS Global Accelerator: .

Per aggiungere un gruppo di endpoint.

1. SulAggiungere gruppi di endpoint., nella sezione relativa a un listener, scegliere unRegion: .
2. PerSet di porte e protocolli, immettere intervalli di porte e protocolli per le istanze Amazon EC2.

   - Inserimento di unDal portoe unAlla portaPer specificare un intervallo di porte.
   - Per ogni intervallo di porte, specificare il protocollo o i protocolli per tale intervallo.

   L'intervallo di porte non deve essere un sottoinsieme dell'intervallo di porte del listener, ma devono essere presenti sufficienti porte totali nell'intervallo delle porte del listener per supportare il numero totale di porte specificato.
3. Seleziona Salva.
4. FacoltativamenteSceglie reAggiungi gruppo di endpointPer aggiungere ulteriori gruppi di endpoint per questo listener o altri listener.
5. Seleziona Successivo.

Fase 4: Aggiungere endpoint di subnet VPC

Aggiungere uno o più endpoint della sottorete di cloud privato virtuale (VPC) per questo gruppo di endpoint regionale. Gli endpoint per gli acceleratori di routing personalizzati definiscono le subnet VPC in grado di ricevere traffico tramite un acceleratore di routing personalizzato. Ogni subnet può contenere una o più destinazioni di istanza Amazon EC2.

Quando si aggiunge un endpoint di subnet VPC, Global Accelerator genera nuovi mapping di porte che è possibile utilizzare per instradare il traffico agli indirizzi IP dell'istanza EC2 di destinazione nella subnet. Quindi è possibile utilizzare l'API Global Accelerator per ottenere un elenco statico di tutti i mapping delle porte per la subnet e utilizzare il mapping per indirizzare deterministicamente il traffico a istanze EC2 specifiche.

> **Note**
>
> I passaggi qui illustrano come aggiungere endpoint nella console. Se si sta creando l'acceleratore a livello di programmazione, è possibile aggiungere endpoint con gruppi di endpoint. Per ulteriori informazioni, consultaCreateCustomRoutingEndPointGroupnellaAWS Global Accelerator: .

Per aggiungere gli endpoint

1. SulAggiungi endpoint, nella sezione relativa al gruppo di endpoint a cui si desidera aggiungere l'endpoint, scegliere un ID sottorete perEndpoint: .
2. Facoltativamente, effettuare una delle seguenti operazioni per abilitare il traffico verso le destinazioni delle istanze EC2 nella subnet:

   - Per consentire al traffico di essere indirizzato a tutti gli endpoint e le porte EC2 nella subnet, selezionareConsenti tutto il traffico
   - Per consentire il traffico verso endpoint e porte EC2 specifici nella subnet, selezionareConsenti traffico verso indirizzi socket di destinazione specifici: . Specificare quindi gli indirizzi IP e le porte o gli intervalli di porte da consentire. Infine, scegliConsenti queste destinazioni: .

   Per impostazione predefinita, non è consentito alcun traffico per gli endpoint di subnet. Se non si seleziona un'opzione per consentire il traffico, il traffico viene negato a tutte le destinazioni nella subnet.

   > **Note**
   >
   > Se si desidera abilitare il traffico verso istanze e porte EC2 specifiche nella subnet, è possibile farlo a livello di programmazione. Per ulteriori informazioni, consultaAllowCustomRoutingTnellaAWS Global Accelerator: .

3. Seleziona Successivo.

Dopo aver sceltoSuccessivo, nel dashboard Acceleratore globale, verrà visualizzato un messaggio che indica che l'acceleratore è in corso. Al termine del processo, lo stato dell'acceleratore nel cruscotto èActive (Attivo): .

Passaggio 5 (facoltativo): Eliminazione dell'accelerator

Se è stato creato un acceleratore come test o se non si utilizza più un acceleratore, è possibile eliminarlo. Sulla console, disabilitare l'acceleratore e quindi eliminarlo. Non è necessario rimuovere i listener e i gruppi di endpoint dall'acceleratore.

Per eliminare un acceleratore utilizzando un'operazione API anziché la console, è necessario rimuovere tutti i listener e i gruppi di endpoint associati all'acceleratore e disabilitarlo. Per

ulteriori informazioni, consulta la .DeleteCustomRoutingAcceleratoroperazione nellaAWS Global Accelerator: .

Quando si elimina un acceleratore, tenere presente quanto segue:

- Quando si crea un acceleratore, Global Accelerator fornisce un set di due indirizzi IP statici. Gli indirizzi IP vengono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se si disattiva l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quandodeleteun acceleratore, si perdono gli indirizzi IP statici assegnati all'acceleratore, quindi non è più possibile instradare il traffico utilizzando tali indirizzi. Come procedura consigliata, assicurarsi di disporre delle autorizzazioni per evitare di eliminare involontariamente gli acceleratori. È possibile utilizzare criteri IAM come autorizzazioni basate su tag con Global Accelerator per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

Per eliminare un accelerator

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Scegliere l'acceleratore da eliminare.
3. Seleziona Edit (Modifica).
4. ScegliereDisabilita acceleratore quindi sceglieresave (Salva): .
5. Scegliere l'acceleratore da eliminare.
6. ScegliereEliminazione dell'accelerator: .
7. Nella finestra di dialogo di conferma, seleziona Delete (Elimina).

Azioni comuni che è possibile utilizzare con AWS Global Accelerator

In questa sezione sono elencate le azioni comuni di AWS Global Accelerator che è possibile utilizzare con le risorse di Global Accelerator, con collegamenti alla documentazione pertinente.

Azioni da utilizzare con risorse standard

Nella tabella seguente sono elencate le azioni più comuni dell'acceleratore globale che è possibile utilizzare con gli acceleratori standard di Global Accelerator, con collegamenti alla documentazione pertinente.

Operazione	Utilizzo della console Global Accelerator	Utilizzo dell'API di Global Accelerator
Creare un acceleratore standard	Consulta NOzioni di base su un acceleratore di serie	Consulta `CreateAccelerator`
Creazione di un listener per un acceleratore standard	Consulta Listener per acceleratori standard in AWS Global Accelerator	Consulta `CreateListener`
Creare un gruppo endpoint per un acceleratore standard	Consulta Gruppi di endpoint per acceleratori standard in AWS Global Accelerator	Consulta `CreateEndpointGroup`
Aggiornare un acceleratore standard	Consulta Acceleratori di AWS Global Accelerator	Consulta `UpdateAccelerator`
Elenca i tuoi acceleratori	Consulta Visualizzazione degli acceleratori	Consulta `ListAccelerator`
Ottieni tutte le informazioni sull'acceleratore	Consulta Visualizzazione degli acceleratori	Consulta `DescribeAccelerator`
Eliminazione di un accelerat ore	Consulta Creazione o aggiornamento di un accelerat ore standard	Consulta `DeleteAccelerator`

Azioni da utilizzare con risorse di routing personalizzate

Nella tabella seguente sono elencate le azioni di acceleratore globale comuni che è possibile utilizzare con gli acceleratori di routing personalizzati, con collegamenti alla documentazione pertinente.

Operazione	Utilizzo della console Global Accelerator	Utilizzo dell'API di Global Accelerator
Creazione di un acceleratore di routing personalizzato	Consulta Introduzione a un acceleratore di routing personalizzato	Consulta CreateCustomRoutingAccelerator
Creazione di un listener per un acceleratore di routing personalizzato	Consulta Listener per acceleratori di routing personalizzati in AWS Global Accelerator	Consulta CreateCustomRoutingListener
Creazione di un gruppo di endpoint per un acceleratore di routing personalizzato	Consulta Gruppi di endpoint per acceleratori di routing personalizzati in AWS Global Accelerator	Consulta CreateCustomRoutingEndpointGroup
Aggiornare un acceleratore di routing personalizzato	Consulta Acceleratori personalizzati in AWS Global Accelerator	Consulta UpdateCustomRoutingAccelerator
Elenca gli acceleratori di routing personalizzati	Consulta Visualizzazione degli acceleratori di routing personalizzati	Consulta ListCustomRoutingAccelerator
Ottieni tutte le informazioni sull'acceleratore di routing personalizzato	Consulta Visualizzazione degli acceleratori di routing personalizzati	Consulta DescribeCustomRoutingAccelerator
Eliminare un acceleratore di routing personalizzato	Consulta Creazione o aggiornamento di un acceleratore di routing personalizzato	Consulta DeleteCustomRoutingAccelerator

Operazione	Utilizzo della console Global Accelerator	Utilizzo dell'API di Global Accelerator
Ottieni la mappatura delle porte statiche per un acceleratore di routing personalizzato	N/D	Consulta `ListCustomRoutingPortMappings`
Consentire tutto il traffico di destinazione per una subnet in un acceleratore di routing personalizzato	Consulta Aggiunta, modifica o rimozione di un endpoint di subnet VPC	Consulta `AllowCustomRoutingTraffic`
Nega tutto il traffico di destinazione per una subnet in un acceleratore di routing personalizzato	Consulta Aggiunta, modifica o rimozione di un endpoint di subnet VPC	Consulta `DenyCustomRoutingTraffic`
Consentire il traffico verso destinazioni specifiche in un acceleratore di routing personalizzato	Consulta Aggiunta, modifica o rimozione di un endpoint di subnet VPC	Consulta `AllowCustomRoutingTraffic`
Negare il traffico a destinazioni specifiche in un acceleratore di routing personalizzato	Consulta Aggiunta, modifica o rimozione di un endpoint di subnet VPC	Consulta `DenyCustomRoutingTraffic`

Lavorare con gli acceleratori standard in AWS Global Accelerator

Questo capitolo include procedure e consigli per la creazione di acceleratori standard in AWS Global Accelerator. Con un acceleratore standard, Global Accelerator sceglie l'endpoint sano più vicino per il traffico.

Se invece si desidera utilizzare la logica dell'applicazione personalizzata per indirizzare uno o più utenti a un endpoint specifico tra molti endpoint, creare un acceleratore di routing personalizzato. Per ulteriori informazioni, consulta Utilizzare acceleratori di routing personalizzati in AWS Global Accelerator.

Per configurare un acceleratore standard, eseguire quanto indicato di seguito:

1. Create un acceleratore e scegliete l'opzione standard dell'acceleratore.
2. Aggiungere un listener con un set specifico di porte o intervallo di porte e scegliere il protocollo da accettare: TCP, UDP o entrambi.
3. Aggiungere uno o più gruppi di endpoint, uno per ogni regione AWS in cui si dispone di risorse endpoint.
4. Aggiungere uno o più endpoint ai gruppi di endpoint. Questo non è obbligatorio, ma il traffico non verrà instradato se non si dispone di endpoint. Gli endpoint possono essere i servizi di bilanciamento del carico di rete, i bilanciamenti del carico delle applicazioni, le istanze di Amazon EC2 o gli indirizzi IP elastici.

Le sezioni seguenti illustrano l'utilizzo di acceleratori standard, listener, gruppi di endpoint e endpoint.

Argomenti

Acceleratori di AWS Global Accelerator

AStandard AcceleratorIn AWS Global Accelerator dirige il traffico verso endpoint ottimali sulla rete globale AWS per migliorare la disponibilità e le prestazioni delle applicazioni Internet che hanno un pubblico globale. Ogni acceleratore include uno o più ascoltatori. Un listener elabora le connessioni in ingresso dai client a Global Accelerator, in base al protocollo (o protocolli) e alla porta (o all'intervallo di porte) configurati.

Quando create un acceleratore, per impostazione predefinita, Global Accelerator fornisce un set di due indirizzi IP statici. Se apporti il tuo intervallo di indirizzi IP ad AWS (BYOIP), puoi invece assegnare indirizzi IP dal tuo pool per l'utilizzo con l'acceleratore. Per ulteriori informazioni, consulta Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator.

> **Important**
>
> Gli indirizzi IP vengono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se si disattiva l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quando sideleteun acceleratore, si perdono gli indirizzi IP statici di Global Accelerator assegnati all'acceleratore, in modo che non sia più possibile instradare il traffico utilizzando tali indirizzi. Come procedura consigliata, assicurarsi di disporre delle autorizzazioni per evitare di eliminare involontariamente gli acceleratori. È possibile utilizzare i criteri IAM con Global Accelerator, ad esempio le autorizzazioni basate su tag, per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

Questa sezione spiega come creare, modificare o eliminare un acceleratore standard nella console Global Accelerator. Per utilizzare le operazioni API con Global Accelerator, consulta laRiferimento all'API AWS Global Accelerator: .

Argomenti

Creazione o aggiornamento di un acceleratore standard

Questa sezione illustra come creare o aggiornare gli acceleratori standard sulla console. Per lavorare con Global Accelerator a livello di programmazione, vedere laRiferimento all'API AWS Global Accelerator: .

Per creare un acceleratore standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. ScegliereCrea acceleratore: .
3. Fornire un nome per l'acceleratore.
4. PerTipo di acceleratoreSELECTstandard: .
5. Facoltativamente, se hai portato i tuoi intervalli di indirizzi IP su AWS (BYOIP), puoi specificare un indirizzo IP statico per il tuo acceleratore, uno per ciascun pool di indirizzi. Effettuare questa scelta per ciascuno dei due indirizzi IP statici dell'acceleratore.
   - Per ogni indirizzo IP statico, scegliere il pool di indirizzi IP da utilizzare.

     > **Note**
     >
     > È necessario scegliere un pool di indirizzi IP diverso per ogni indirizzo IP statico. Questa restrizione è dovuta al fatto che Global Accelerator assegna ogni intervallo di indirizzi a una zona di rete diversa, per una disponibilità elevata.

   - Se è stato scelto il proprio pool di indirizzi IP, scegliere anche un determinato indirizzo IP dal pool. Se scegli il pool di indirizzi IP Amazon predefinito, Global Accelerator assegna un indirizzo IP specifico al tuo acceleratore.
6. Facoltativamente, aggiungi uno o più tag per aiutarti a identificare le risorse acceleratore.
7. ScegliereSuccessivoper aggiungere listener, gruppi di endpoint ed endpoint.

Per modificare un acceleratore standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco degli acceleratori, sceglierne uno, quindi sceglieModificare: .

3. SulModifica acceleratoreApporta le modifiche che preferisci. Ad esempio, è possibile disabilitare l'acceleratore in modo che non accetti più il traffico o in modo da poterlo eliminare. Oppure, se l'acceleratore è disabilitato, è possibile abilitarlo.
4. Seleziona Save changes (Salva modifiche).

Eliminazione di un acceleratore

Se è stato creato un acceleratore come test o se non si utilizza più un acceleratore, è possibile eliminarlo. Sulla console, disabilitare l'acceleratore e quindi eliminarlo. Non è necessario rimuovere i listener e i gruppi di endpoint dall'acceleratore.

Per eliminare un acceleratore utilizzando un'operazione API anziché la console, è necessario innanzitutto rimuovere tutti i listener e i gruppi di endpoint associati all'acceleratore e quindi disabilitarlo. Per ulteriori informazioni, consulta la .DeleteAcceleratoroperazione nellaRiferimento all'API AWS Global Accelerator: .

Per disabilitare un acceleratore

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco, scegli un acceleratore da disabilitare.
3. Seleziona Edit (Modifica).
4. ScegliereDisattiva acceleratore, quindi sceglieresave (Salva): .

Per eliminare un acceleratore

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco, scegli un acceleratore da eliminare.
3. Scegli Elimina.

> **Note**
>
> Se l'acceleratore non è stato disattivato,EliminaNon è disponibile.

4. Nella finestra di dialogo di conferma, seleziona Delete (Elimina).

> **Important**
>
> Quando si elimina un acceleratore, si perdono gli indirizzi IP statici assegnati all'acceleratore, in modo che non sia più possibile instradare il traffico utilizzando tali indirizzi.

Visualizzazione degli acceleratori

Puoi visualizzare informazioni sugli acceleratori sulla console. Per visualizzare le descrizioni degli acceleratori a livello di programmazione, vedereListAcceleratorseDescribeAcceleratornellaRiferimento all'API AWS Global Accelerator: .

Per visualizzare le informazioni sull'acceleratore

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Per visualizzare i dettagli su un acceleratore, nell'elenco scegliere un acceleratore e quindi scegliereVisualizzazione: .

Aggiungere un acceleratore quando si crea un bilanciamento del carico

Quando si crea un Application Load Balancer nella Console di gestione AWS, è possibile facoltativamenteAggiunta di un acceleratore contemporaneamente: . Elastic Load Balancing e Global Accelerator collaborano per aggiungere in modo trasparente l'acceleratore. L'acceleratore viene creato nell'account, con il bilanciamento del carico come endpoint. L'utilizzo di un acceleratore fornisce indirizzi IP statici e migliora la disponibilità e le prestazioni delle applicazioni.

> **Important**
>
> Per creare un acceleratore, è necessario disporre delle autorizzazioni corrette. Per ulteriori informazioni, consulta Autorizzazioni necessarie per l'accesso alla console, la gestione dell'autenticazione e il controllo dell'accesso.

Configura e visualizza il tuo acceleratore

È necessario aggiornare la configurazione DNS per indirizzare il traffico verso gli indirizzi IP statici o il nome DNS per l'acceleratore. Il traffico non passerà attraverso l'acceleratore al bilanciamento del carico fino al completamento delle modifiche alla configurazione.

Dopo aver creato il bilanciamento del carico scegliendo il componente aggiuntivo Global Accelerator sulla console Amazon EC2, vai alla paginaServizi integratiPer visualizzare gli indirizzi IP statici e il nome Domain Name System (DNS) per l'acceleratore. Utilizzare queste informazioni per avviare il routing del traffico utente al bilanciamento del carico tramite la rete globale AWS. Per ulteriori informazioni sul nome DNS assegnato all'acceleratore, consultareIndirizzi DNS e domini personalizzati in AWS Global Accelerator: .

È possibile visualizzare e configurare il proprio acceleratoreNavigazione a Global AcceleratorNella Console di gestione AWS Management Console. Ad esempio, è possibile visualizzare gli acceleratori associati al proprio account o aggiungere altri bilanciatori del carico all'acceleratore. Per ulteriori informazioni, consulta Visualizzazione degli acceleratori e Creazione o aggiornamento di un acceleratore standard.

Prezzi

I prezzi di AWS Global Accelerator sono calcolati in base all'uso effettivo. Per ogni acceleratore nel tuo account verrà addebitata una tariffa oraria e i costi di trasferimento dati. Per ulteriori informazioni, consultaAWS Global Accelerator: .

Smetti di usare l'acceleratore

Se si desidera interrompere il routing del traffico tramite Global Accelerator al bilanciamento del carico, effettuare le seguenti operazioni:

1. Aggiornare la configurazione DNS per indirizzare il traffico direttamente al bilanciamento del carico.
2. Eliminare il bilanciamento del carico dall'acceleratore. Per ulteriori informazioni, consultaPer rimuovere un endpointinAggiunta, modifica o rimozione di un endpoint standard: .
3. Elimina l'accelerator. Per ulteriori informazioni, consulta Eliminazione di un acceleratore.

Utilizzo di indirizzi IP statici globali anziché indirizzi IP statici regionali

Se desideri utilizzare un indirizzo IP statico davanti a una risorsa AWS, ad esempio un'istanza Amazon EC2, hai diverse opzioni. Ad esempio, puoi allocare un indirizzo IP elastico, ovvero un indirizzo IPv4 statico che puoi associare a un'istanza Amazon EC2 o un'interfaccia di rete in una singola area AWS.

Se si dispone di un pubblico globale, è possibile creare un acceleratore con Global Accelerator per ottenere due indirizzi IP statici globali annunciati da sedi perimetrali AWS in tutto il mondo. Se hai già configurato risorse AWS per le tue applicazioni, in una o più aree geografiche, tra cui istanze Amazon EC2, Network Load Balancers e Application Load Balancers, puoi aggiungerle facilmente a Global Accelerator per inoltrarle con indirizzi IP statici globali.

Se si sceglie di utilizzare indirizzi IP statici globali forniti da Global Accelerator, è inoltre possibile migliorare la disponibilità e le prestazioni delle applicazioni. Con Global Accelerator, gli indirizzi IP statici accettano il traffico in ingresso nella rete globale AWS dalla posizione perimetrale più vicina agli utenti. Massimizzare il tempo in cui il traffico è sulla rete AWS può fornire un'esperienza cliente più rapida e migliore. Per ulteriori informazioni, consulta Come funziona AWS Global Accelerator .

È possibile aggiungere un acceleratore dalla console di gestione AWS o utilizzando operazioni API con l'interfaccia CLI o SDK AWS. Per ulteriori informazioni, consulta Creazione o aggiornamento di un acceleratore standard.

Quando si aggiunge un acceleratore, prendere nota di quanto segue:

- Gli indirizzi IP statici globali forniti da Global Accelerator rimangono assegnati all'utente per tutto il tempo in cui l'acceleratore esiste, anche se si disabilita l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, se si elimina un acceleratore, si perdono gli indirizzi IP statici assegnati ad esso. Per ulteriori informazioni, consulta Eliminazione di un acceleratore.
- I prezzi di Global Accelerator sono calcolati in base all'uso effettivo. Per ogni acceleratore nel tuo account verrà addebitata una tariffa oraria e i costi di trasferimento dati. Per ulteriori informazioni, consultaAWS Global Accelerator: .

Listener per acceleratori standard in AWS Global Accelerator

Con AWS Global Accelerator, è possibile aggiungere listener che elaborano le connessioni in ingresso dai client in base alle porte e ai protocolli specificati. I listener supportano TCP, UDP o entrambi i protocolli TCP e UDP.

È possibile definire un listener standard al momento della creazione di un accelerator standard, ed è possibile aggiungere altri listener in qualsiasi momento. È possibile associare ogni listener a uno o più gruppi di endpoint e associare ciascun gruppo di endpoint a un'area AWS.

Argomenti

Aggiunta, modifica o rimozione di un listener standard

Questa sezione illustra come utilizzare listener sulla console AWS Global Accelerator.
Per completare queste attività utilizzando un'operazione API anziché la console, consulta`CreateListener`,`UpdateListener`, e`DeleteListener`nellaInformazioni di riferimento sull'API Global Accelerator: .

Aggiunta di un listener

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un accelerator.
3. Scegli Add listener (Aggiungi listener).
4. SulAggiunta di un listenerimmettere le porte o gli intervalli di porte che si desidera associare al listener. I listener supportano le porte 1-65535.
5. Scegliere il protocollo per le porte immesse.
6. Facoltativamente, scegliere di abilitare l'affinità client. L'affinità client per un listener significa che Global Accelerator garantisce che le connessioni da un indirizzo IP di origine specifico (client) vengano sempre instradate allo stesso endpoint. Per abilitare questo comportamento, nell'elenco a discesa, scegliereIP di origine: .

   Il valore predefinito èNessuna, il che significa che l'affinità client non è abilitata e Global Accelerator distribuisce il traffico equamente tra gli endpoint nei gruppi di endpoint per il listener.

   Per ulteriori informazioni, consulta Affinità del client.
7. Scegli Add listener (Aggiungi listener).

Per modificare un listener standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un accelerator.
3. Scegli un listener, quindi eModifica listener: .
4. SulModifica listenermodificare le porte, gli intervalli di porte o i protocolli che si desidera associare al listener.
5. Facoltativamente, scegliere di abilitare l'affinità client. L'affinità client per un listener significa che Global Accelerator garantisce che le connessioni da un indirizzo IP di origine specifico (client) vengano sempre instradate allo stesso endpoint. Per abilitare questo comportamento, nell'elenco a discesa, scegliereIP di origine: .

   Il valore predefinito èNessuna, il che significa che l'affinità client non è abilitata e Global Accelerator distribuisce il traffico equamente tra gli endpoint nei gruppi di endpoint per il listener.

   Per ulteriori informazioni, consulta Affinità del client.
6. Seleziona Salva.

Per rimuovere un listener

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un accelerator.
3. Scegli un listener, quindi eRemove: .
4. Nella finestra di dialogo di conferma, selezionareRemove: .

Affinità del client

Se si dispone di applicazioni con stato che si utilizzano con un acceleratore standard, è possibile scegliere che Global Accelerator indirizzi tutte le richieste di un utente a un indirizzo IP di origine specifico (client) alla stessa risorsa endpoint, per mantenere l'affinità client.

Per impostazione predefinita, l'affinità client per un listener standard è impostata suNessunae Global Accelerator distribuisce il traffico equamente tra gli endpoint nei gruppi di endpoint per il listener.

Global Accelerator utilizza un algoritmo di hash a flusso coerente per scegliere l'endpoint ottimale per la connessione di un utente. Se si configura l'affinità client per la risorsa Global AcceleratorNessuna, Global Accelerator utilizza le proprietà a 5 tuple, ovvero l'IP di origine, la porta di origine, la porta di destinazione, la porta di destinazione e il protocollo, per selezionare il valore hash. Successivamente, sceglie l'endpoint che fornisce le migliori prestazioni. Se un determinato client utilizza porte diverse per connettersi a Global Accelerator e questa impostazione è stata specificata, Global Accelerator non può garantire che le connessioni dal client siano sempre instradate allo stesso endpoint.

Se si desidera mantenere l'affinità client instradando un utente specifico, identificato dal proprio indirizzo IP di origine, allo stesso endpoint ogni volta che si connette, impostare l'affinità client suIP di origine: . Quando si specifica questa opzione, Global Accelerator utilizza le proprietà a due tuple, ovvero l'IP di origine e l'IP di destinazione, per selezionare il valore hash e instradare l'utente allo stesso endpoint ogni volta che si connettono. Global Accelerator rispetta l'affinità client dopo il gruppo di endpoint selezionato.

Gruppi di endpoint per acceleratori standard in AWS Global Accelerator

Un gruppo di endpoint instrada le richieste a uno o più endpoint registrati in AWS Global Accelerator. Quando si aggiunge un listener in un acceleratore standard, si specificano i gruppi di endpoint a cui Global Accelerator dirigere il traffico. Un gruppo di endpoint e tutti gli endpoint in esso contenuti devono trovarsi in un'unica area AWS. È possibile aggiungere diversi gruppi di endpoint per scopi diversi, ad esempio per test di distribuzione blu/verde.

Global Accelerator indirizza il traffico ai gruppi di endpoint negli acceleratori standard in base alla posizione del client e all'integrità del gruppo di endpoint. Se lo desideri, puoi anche impostare la percentuale di traffico da inviare a un gruppo di endpoint. Per eseguire questa operazione, utilizzare la composizione del traffico per aumentare (composizione verso l'alto) o diminuire (composizione verso il basso) il traffico verso il gruppo. La percentuale viene applicata solo al traffico che Global Accelerator sta già indirizzando al gruppo di endpoint, non a tutto il traffico proveniente da un listener.

È possibile definire le impostazioni di controllo dello stato per Global Accelerator per ogni gruppo di endpoint. Aggiornando le impostazioni di controllo dello stato, puoi modificare i requisiti per il polling e la verifica dello stato degli endpoint dell'istanza di Amazon EC2 e dell'indirizzo IP elastico. Per gli endpoint di Network Load Balancer e di Application Load Balancer, configurare le impostazioni di controllo dello stato nella console Elastic Load Balancing ancer.

Global Accelerator monitora continuamente l'integrità di tutti gli endpoint inclusi in un gruppo di endpoint standard e instrada le richieste solo agli endpoint attivi integri. Se non ci sono endpoint integri a cui instradare il traffico, Global Accelerator instraderà le richieste a tutti gli endpoint.

Questa sezione spiega come utilizzare i gruppi di endpoint per gli acceleratori standard sulla console AWS Global Accelerator. Se desideri utilizzare le operazioni API con AWS Global Accelerator, consulta la documentazioneRiferimento all'API AWS Global Accelerator: .

Argomenti

Aggiunta, modifica o rimozione di un gruppo di endpoint standard

È possibile utilizzare gruppi di endpoint nella console AWS Global Accelerator o utilizzando un'operazione API. È possibile aggiungere o rimuovere endpoint da un gruppo di endpoint in qualsiasi momento.

Questa sezione illustra come utilizzare gruppi di endpoint standard sulla console AWS Global Accelerator. Se desideri usare le operazioni API con Global Accelerator, consulta la documentazioneRiferimento all'API AWS Global Accelerator: .

Per aggiungere un gruppo di endpoint standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, perID del listener, scegliere l'ID del listener a cui aggiungere un gruppo di endpoint.
4. ScegliereAggiungi un gruppo di endpoint: .
5. Nella sezione relativa a un listener, specificare una regione per il gruppo di endpoint selezionandone una dall'elenco a discesa.
6. Facoltativamente, perComposizione del traffico, immettere un numero compreso tra 0 e 100 per impostare una percentuale di traffico per questo gruppo di endpoint. La percentuale viene

applicata solo al traffico già indirizzato a questo gruppo di endpoint, non a tutto il traffico del listener. Per impostazione predefinita, la composizione del traffico è impostata su 100.

7. Facoltativamente, per sovrascrivere la porta del listener utilizzata per instradare il traffico agli endpoint e reindirizzare il traffico verso porte specifiche degli endpoint, scegliereConfigurare le sostituzioni delle porte: . Per ulteriori informazioni, consulta Sostituzioni delle porte.
8. Facoltativamente, per specificare valori di controllo dello stato personalizzati da applicare agli endpoint dell'istanza EC2 e degli indirizzi IP elastici, sceglieConfigurazione dei controlli dello stato: . Per ulteriori informazioni, consulta Opzioni controllo dello stato.
9. Facoltativamente, sceglieAggiungi un gruppo di endpointPer aggiungere gruppi di endpoint aggiuntivi per questo listener o per altri listener.
10. SceglieAggiungi un gruppo di endpoint: .

Per modificare un gruppo di endpoint.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, perID del listener, scegliere l'ID del listener a cui è associato il gruppo di endpoint.
4. SceglieModifica il gruppo di endpoint: .
5. SulModifica il gruppo di endpoint, modificare la regione, regolare la percentuale di composizione del traffico o sceglieConfigurazione dei controlli dello statoPer modificare le impostazioni di controllo dello stato.
6. Seleziona Salva.

Per rimuovere un gruppo di endpoint standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, scegliere un listener e selezionareRemove: .
4. NellaGruppi di endpoint, scegliere un gruppo di endpoint e selezionareRemove: .
5. Nella finestra di dialogo di conferma, selezionareRemove: .

Regolazione del flusso di traffico con le manopole

Per ogni gruppo di endpoint standard, è possibile impostare una composizione del traffico per controllare la percentuale di traffico indirizzato al gruppo. La percentuale viene applicata solo al traffico già indirizzato al gruppo di endpoint, non a tutto il traffico del listener.

Per impostazione predefinita, la composizione del traffico è impostata su 100 (ovvero 100%) per tutti i gruppi di endpoint regionali in un acceleratore. La composizione del traffico consente di eseguire facilmente test delle prestazioni o test di distribuzione blu/verde per le nuove versioni in diverse regioni AWS, ad esempio.

Di seguito sono riportati alcuni esempi che illustrano come utilizzare i quadranti del traffico per modificare il flusso di traffico in gruppi di endpoint.

Aggiorna la tua applicazione per regione

Se si desidera aggiornare un'applicazione in una regione o eseguire la manutenzione, impostare innanzitutto la ghiera del traffico su 0 per interrompere il traffico per la regione. Quando si completa il lavoro e si è pronti a riportare in servizio la regione, regolare la composizione del traffico su 100 per comporre il backup del traffico.

Combinare il traffico tra due regioni

In questo esempio viene illustrato il funzionamento del flusso di traffico quando si modificano contemporaneamente i quadranti del traffico per due gruppi di endpoint regionali. Supponiamo che tu abbia due gruppi di endpoint per il tuo acceleratore, uno per il`us-west-2`Regione e una per il`us-east-1`Area e hai impostato i quadranti del traffico al 50% per ogni gruppo di endpoint.

Ora, diciamo che avete 100 richieste per il vostro acceleratore, con 50 dalla costa orientale degli Stati Uniti e 50 dalla costa occidentale. L'acceleratore dirige il traffico come segue:

- Le prime 25 richieste su ogni costa (50 richieste in totale) vengono servite dal gruppo di endpoint vicino. Cioè, 25 richieste vengono indirizzate al gruppo di endpoint in`us-west-2`e 25 sono indirizzati al gruppo di endpoint in`us-east-1`: .
- Le prossime 50 richieste sono indirizzate alle Regioni opposte. Cioè, le prossime 25 richieste dalla East Coast sono servite da`us-west-2`, e le prossime 25 richieste dalla West Coast sono servite da`us-east-1`: .

Il risultato in questo scenario è che entrambi i gruppi di endpoint servono la stessa quantità di traffico. Tuttavia, ognuna riceve un mix di traffico da entrambe le Regioni.

Sostituzioni delle porte

Per impostazione predefinita, un acceleratore indirizza il traffico utente agli endpoint nelle regioni AWS utilizzando il protocollo e gli intervalli di porte specificati quando si crea un listener. Ad esempio, se si definisce un listener che accetta il traffico TCP sulle porte 80 e 443, l'acceleratore instraderà il traffico a tali porte su un endpoint.

Tuttavia, quando si aggiunge o si aggiorna un gruppo di endpoint, è possibile sostituire la porta del listener utilizzata per il routing del traffico agli endpoint. Ad esempio, è possibile creare una sostituzione di porta in cui il listener riceve il traffico utente sulle porte 80 e 443, ma l'acceleratore instrada tale traffico alle porte 1080 e 1443, rispettivamente, sugli endpoint.

Le sostituzioni delle porte consentono di evitare problemi con l'ascolto su porte con restrizioni. È più sicuro eseguire applicazioni che non richiedono privilegi di superutente (root) sugli endpoint. Tuttavia, in Linux e in altri sistemi Unix, è necessario disporre dei privilegi di superutente per l'ascolto su porte con restrizioni (porte TCP o UDP inferiori a 1024). Mappando una porta con restrizioni su un listener a una porta non limitata su un endpoint, le sostituzioni delle porte consentono di evitare questo problema. È possibile accettare il traffico su porte con restrizioni durante l'esecuzione di applicazioni senza accesso root sugli endpoint dietro Global Accelerator. Ad esempio, è possibile sovrascrivere una porta del listener 443 a una porta dell'endpoint 8443.

Per ogni override della porta, è necessario specificare una porta del listener che accetta il traffico dagli utenti e la porta dell'endpoint a cui Global Accelerator instraderà tale traffico. Per ulteriori informazioni, consulta Aggiunta, modifica o rimozione di un gruppo di endpoint standard.

Quando crei un'override di porta, tieni presente quanto segue:

- Le porte endpoint non possono sovrapporsi agli intervalli di porte del listener. Le porte endpoint specificate in un'override delle porte non possono essere incluse in nessuno degli intervalli di porte del listener configurati per l'acceleratore. Ad esempio, si supponga di disporre di due listener per un acceleratore e di aver definito gli intervalli di porte per tali listener rispettivamente 100-199 e 200-299. Quando si creano override delle porte, non è possibile definirne una dalla porta del listener 100 alla porta dell'endpoint 210, ad esempio, perché la porta endpoint (210) è inclusa in un intervallo di porte del listener definito (200-299).
- Nessuna porta endpoint duplicata. Se l'override di una porta in un acceleratore specifica una porta endpoint, non è possibile specificare la stessa porta endpoint con l'override della porta da una porta del listener diversa. Ad esempio, non è possibile specificare una sostituzione della porta dalla porta del listener 80 alla porta dell'endpoint 90 insieme a un'override dalla porta del listener 81 alla porta dell'endpoint 90.

- Il controllo di Health continua a utilizzare la porta originale. Se si specifica un'override di porta per una porta configurata come porta di controllo dello stato, il controllo di integrità utilizza ancora la porta originale e non la porta di sostituzione. Si supponga, ad esempio, di specificare i controlli di integrità sulla porta del listener 80 e di specificare anche un'override della porta del listener 80 alla porta dell'endpoint 480. I controlli di Health continuano a utilizzare la porta dell'endpoint 80. Tuttavia, il traffico utente che arriva attraverso la porta 80 va alla porta 480 sull'endpoint.

  Questo comportamento mantiene la coerenza tra Network Load Balancer, Application Load Balancer, EC2 istanza e gli endpoint degli indirizzi IP elastici. Poiché Network Load Balancers e Application Load Balancers non mappano le porte di controllo dello stato a porte endpoint diverse quando si specifica un'override di porta in Global Accelerator, non sarebbe coerente per Global Accelerator mappare le porte di controllo dello stato a porte endpoint diverse per l'istanza EC2 ed Elastic IP endpoint di indirizzo.
- Le impostazioni dei gruppi di protezione devono consentire l'accesso alle porte. Assicurarsi che i gruppi di sicurezza consentano al traffico di arrivare alle porte degli endpoint designate nelle sostituzioni delle porte. Ad esempio, se si esegue l'override della porta del listener 443 alla porta dell'endpoint 1433, assicurarsi che eventuali restrizioni di porta impostate nel gruppo di sicurezza per tale endpoint Application Load Balancer o Amazon EC2 consentano il traffico in entrata sulla porta 1433.

Opzioni controllo dello stato

AWS Global Accelerator invia regolarmente delle richieste agli endpoint standard per testare il loro stato. Questi controlli di integrità vengono eseguiti automaticamente. Le indicazioni per determinare l'integrità di ciascun endpoint e la tempistica per i controlli di integrità dipendono dal tipo di risorsa endpoint.

> **Important**
>
> Global Accelerator richiede le regole del router e del firewall per consentire al traffico in ingresso dagli indirizzi IP associati ai controlli integrità Route 53 di completare i controlli di integrità per l'istanza EC2 o gli endpoint degli indirizzi IP elastici. Puoi trovare informazioni sugli intervalli di indirizzi IP associati ai controlli sanitari di Amazon Route 53 in Controlli dello stato per i gruppi target nella Guida per sviluppatori di Amazon Route: .

È possibile configurare le seguenti opzioni di controllo dello stato per un gruppo di endpoint. Se si specificano le opzioni di controllo dello stato, Global Accelerator utilizza le impostazioni per i controlli di integrità dell'istanza EC2 o degli indirizzi IP elastici, ma non per i servizi di bilanciamento del carico di rete o dei servizi di bilanciamento del carico delle applicazioni.

- Per gli endpoint Application Load Balancer o Network Load Balancer, è possibile configurare i controlli di integrità per le risorse utilizzando le opzioni di configurazione Elastic Load Balancing ancer. Per ulteriori informazioni, consultaControlli dello stato per i gruppi target: . Le opzioni di controllo Health selezionate in Global Accelerator non influiscono sui Balancers di carico delle applicazioni o sui servizi di bilanciamento del carico di rete aggiunti come endpoint.

  > **Note**
  >
  > Quando si dispone di un Application Load Balancer o Network Load Balancer che include più gruppi target, Global Accelerator considera l'endpoint di bilanciamento del carico integro solo seOgnidietro il bilanciamento del carico ha almeno un obiettivo integro. Se un singolo gruppo target per il bilanciamento del carico ha solo destinazioni non integri, Global Accelerator considera l'endpoint non integro.

- Per gli endpoint dell'istanza EC2 o degli indirizzi IP elastici aggiunti a un listener configurato con TCP, è possibile specificare la porta da utilizzare per i controlli di integrità. Per impostazione predefinita, se non si specifica una porta per i controlli di integrità, Global Accelerator utilizza la porta del listener specificata per l'acceleratore.
- Per gli endpoint dell'istanza EC2 o degli indirizzi IP elastici con listener UDP, Global Accelerator utilizza la porta del listener e il protocollo TCP per i controlli di integrità, pertanto è necessario disporre di un server TCP sull'endpoint.

  > **Note**
  >
  > Verificare che la porta configurata per il server TCP su ciascun endpoint sia la stessa della porta specificata per il controllo di integrità in Global Accelerator. Se i numeri di porta non sono uguali o se non è stato configurato un server TCP per l'endpoint, Global Accelerator contrassegna l'endpoint come non integro, indipendentemente dall'integrità dell'endpoint.

Porta controllo Health stato

Porta da utilizzare quando Global Accelerator esegue controlli dello stato sugli endpoint che fanno parte di questo gruppo di endpoint.

> **Note**
>
> Non è possibile impostare l'override di una porta per le porte di controllo dello stato.

Protocollo controllo dello stato

Protocollo da utilizzare quando Global Accelerator esegue controlli dello stato sugli endpoint che fanno parte di questo gruppo di endpoint.

Intervallo Health stato

L'intervallo, in secondi, tra ciascun controllo dello stato per un endpoint.

Conteggio della soglia

Il numero di controlli dello stato consecutivi necessari prima di considerare integro un target non integro o non integro.

Ogni listener indirizza le richieste solo agli endpoint integri. Dopo aver aggiunto un endpoint, deve essere sottoposto a un controllo dello stato per essere considerato integro. Dopo il completamento di ciascun controllo dello stato, il listener chiude la connessione stabilita per il controllo dello stato.

Endpoint per acceleratori standard in AWS Global Accelerator

Gli endpoint per gli acceleratori standard in AWS Global Accelerator possono essere Network Load Balancers, Application Load Balancers, istanze Amazon EC2 o indirizzi IP elastici. Con gli acceleratori standard, un indirizzo IP statico funge da singolo punto di contatto per i client e Global Accelerator distribuisce il traffico in entrata tra endpoint integri. Global Accelerator indirizza il traffico agli endpoint utilizzando la porta (o l'intervallo di porte) specificata per il listener a cui appartiene il gruppo di endpoint per l'endpoint.

Ogni gruppo di endpoint può avere più endpoint. È possibile aggiungere ogni endpoint a più gruppi endpoint, ma i gruppi endpoint devono essere associati a listener diversi. Una risorsa deve essere valida e attiva quando viene aggiunta come endpoint.

Global Accelerator monitora continuamente lo stato di tutti gli endpoint inclusi in un gruppo di endpoint standard. Instradare il traffico solo agli endpoint attivi che sono integri. Se Global Accelerator non dispone di endpoint integri a cui instradare il traffico, indirizza il traffico a tutti gli endpoint.

Tenere presente quanto segue per tipi specifici di endpoint standard Global Accelerator:

Endpoint del sistema di bilanciamento del carico

- Un endpoint di Application Load Balancer può essere connesso a Internet o interno. Un endpoint di Network Load Balancer deve essere connesso a Internet.

Endpoint dell'istanza Amazon EC2

- Un endpoint di istanza EC2 (per acceleratori di routing standard e personalizzati) non può essere uno dei seguenti tipi: C1, CC1, CC1, CC1, CC1, CC1, CC1, CC1, CC1, G1, G1, G1, M3 e 1.
- Le istanze EC2 sono supportate come endpoint solo in alcune regioni AWS. Per un elenco delle regioni supportate, consulta Regioni AWS supportate per la conservazione degli indirizzi IP client.
- Si consiglia di rimuovere un'istanza EC2 dai gruppi di endpoint Global Accelerator prima di terminare l'istanza. Se si termina un'istanza EC2 prima di rimuoverla da un gruppo di endpoint in Global Accelerator e quindi si crea un'altra istanza nello stesso VPC con lo stesso indirizzo IP privato e si passa i controlli di integrità, Global Accelerator instraderà il traffico al nuovo endpoint.

Argomenti

Aggiunta, modifica o rimozione di un endpoint standard

È possibile aggiungere endpoint ai gruppi di endpoint in modo che il traffico possa essere indirizzato alle risorse. È possibile modificare un endpoint standard per modificare il peso del punto finale. In alternativa, è possibile rimuovere un endpoint dall'acceleratore rimuovendolo da un gruppo di

endpoint. La rimozione di un endpoint non influisce sull'endpoint stesso, ma Global Accelerator non può più indirizzare il traffico verso tale risorsa.

Gli endpoint in Global Accelerator possono essere Network Load Balancers, Application Load Balancers, istanze Amazon EC2 o indirizzi IP elastici. È necessario prima creare una di queste risorse e quindi aggiungerla come endpoint in Global Accelerator. Una risorsa deve essere valida e attiva quando viene aggiunta come endpoint.

È possibile aggiungere o rimuovere endpoint o endpoint dai gruppi di endpoint in base all'utilizzo. Ad esempio, se la domanda dell'applicazione aumenta, è possibile creare più risorse e quindi aggiungere più endpoint a uno o più gruppi di endpoint per gestire l'aumento del traffico. Global Accelerator inizia a instradare le richieste a un endpoint non appena lo aggiungi e supera i controlli dello stato iniziali. È possibile gestire il traffico verso gli endpoint regolando i pesi su un endpoint, in modo da inviare proporzionalmente più o meno traffico all'endpoint.

Se si aggiunge un endpoint con conservazione dell'indirizzo IP del client, esaminare innanzitutto le informazioni inRegioni AWS supportate per la conservazione degli indirizzi IP clienteConservare gli indirizzi IP client in AWS Global Accelerator: .

È possibile rimuovere gli endpoint dai gruppi di endpoint, ad esempio, se è necessario eseguire la manutenzione degli endpoint. La rimozione di un endpoint rimuove il endpoint dal gruppo di endpoint, ma non influisce in altro modo sull'endpoint. Global Accelerator interrompe l'indirizzamento del traffico verso un endpoint non appena lo si rimuove da un gruppo di endpoint. L'endpoint entra in uno stato in cui attende che tutte le richieste correnti vengano completate in modo che non vi sia alcuna interruzione per il traffico client in corso. Puoi aggiungere di nuovo l'endpoint al gruppo di endpoint quando è possibile riprendere la ricezione delle richieste.

Questa sezione descrive come utilizzare gli endpoint nella console AWS Global Accelerator.
Se desideri utilizzare le operazioni API con AWS Global Accelerator, consulta la documentazioneRiferimento all'API AWS Global Accelerator: .

Per aggiungere un endpoint standard

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, seleziona l'ID del gruppo di endpoint al quale desideri aggiungere un endpoint.

5. NellaEndpoint, scegliereAggiungi endpoint: .
6. SulAggiungi endpoint, scegliere una risorsa dall'elenco a discesa.

   Se non hai risorse AWS, non ci sono elementi nell'elenco. Per continuare, crea risorse AWS come bilanciamento del carico, istanze Amazon EC2 o indirizzi IP elastici. Quindi torna ai passaggi qui e scegli una risorsa dall'elenco.
7. Facoltativamente, perPeso, immettere un numero compreso tra 0 e 255 per impostare un peso per il routing del traffico a questo endpoint. Quando si aggiungono pesi agli endpoint, è possibile configurare Global Accelerator per instradare il traffico in base alle proporzioni specificate. Per impostazione predefinita, tutti gli endpoint hanno un peso di 128. Per ulteriori informazioni, consulta Pesi dell'endpoint.
8. Facoltativamente, abilitare la conservazione degli indirizzi IP del client per un endpoint di Application Load Balancer con connessione Internet. UNDERPreserve l'indirizzo IP del client, selezionaMantieni indirizzo: .

   Questa opzione è sempre selezionata per gli endpoint interni di Application Load Balancer e EC2 e mai selezionata per gli endpoint degli indirizzi IP elastici e di Network Load Balancer. Per ulteriori informazioni, consulta Conservare gli indirizzi IP client in AWS Global Accelerator.

   > **Note**
   >
   > Prima di aggiungere e iniziare a instradare il traffico agli endpoint che conservano l'indirizzo IP del client, assicurarsi che tutte le configurazioni di protezione richieste, ad esempio i gruppi di sicurezza, vengano aggiornate per includere l'indirizzo IP del client utente negli elenchi consentiti.
9. Seleziona Add endpoint (Aggiungi endpoint).

Per modificare un endpoint standard

È possibile modificare una configurazione endpoint per modificare il peso. Per ulteriori informazioni, consulta Pesi dell'endpoint.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.

4. NellaGruppi di endpointSezione, perID gruppo di endpoint, seleziona l'ID del gruppo di endpoint.
5. ScegliereModificare l'endpoint: .
6. SulModificare l'endpoint, apportare aggiornamenti e quindi sceglieSave (Salva): .

Per rimuovere un endpoint

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, seleziona l'ID del gruppo di endpoint.
5. SceglieRemove endpoint: .
6. Nella finestra di dialogo di conferma, sceglieRemove: .

Pesi dell'endpoint

Un peso è un valore che determina la proporzione di traffico che Global Accelerator indirizza a un endpoint in un acceleratore standard. Gli endpoint possono essere i servizi di bilanciamento del carico di rete, i bilanciamenti del carico delle applicazioni, le istanze di Amazon EC2 o gli indirizzi IP elastici. Global Accelerator calcola la somma dei pesi per gli endpoint in un gruppo di endpoint, quindi indirizza il traffico verso gli endpoint in base al rapporto tra il peso di ciascun endpoint e il totale.

Il routing ponderato consente di scegliere la quantità di traffico instradato a una risorsa in un gruppo di endpoint. Questo può essere utile in diversi modi, tra cui il bilanciamento del carico e il test di nuove versioni di un'applicazione.

Come funzionano i pesi degli endpoint

Per utilizzare i pesi, assegni a ogni endpoint in un gruppo di endpoint un peso relativo che corrisponde alla quantità di traffico che desideri inviargli. Per impostazione predefinita, il peso di un punto finale è 128, ovvero la metà del valore massimo di un peso, 255. Global Accelerator invia il traffico a un endpoint in base al peso che assegni come proporzione del peso totale per tutti gli endpoint nel gruppo:

$$\frac{\text{Weight for a specified endpoint}}{\text{Sum of the weights for all endpoints}}$$

Ad esempio, se desideri inviare una piccola porzione di traffico a un endpoint e il resto a un altro endpoint, devi specificare un peso di 1 e 255. L'endpoint con un peso di 1 ottiene 1/256 del traffico (1/1+255) e l'altro endpoint ottiene 255/256 (255/1+255). Puoi modificare gradualmente il carico modificando i pesi. Se desideri che Global Accelerator interrompa l'invio del traffico a un endpoint, devi modificare il peso della risorsa su 0.

Failover per endpoint non integri

Se in un gruppo di endpoint non sono presenti endpoint integri con un peso maggiore di zero, Global Accelerator tenta di eseguire il failover su un endpoint integro con un peso maggiore di zero in un altro gruppo di endpoint. Per questo failover, Global Accelerator ignora l'impostazione di composizione del traffico. Pertanto, se, ad esempio, un gruppo di endpoint ha una composizione del traffico impostata su zero, Global Accelerator include comunque tale gruppo di endpoint nel tentativo di failover.

Se Global Accelerator non trova un endpoint integro con un peso maggiore di zero dopo aver provato tre gruppi di endpoint aggiuntivi (ovvero tre regioni AWS), indirizza il traffico a un endpoint casuale nel gruppo di endpoint più vicino al client. Cioè, èApertura non riuscita: .

Tieni presente quanto segue:

- Il gruppo di endpoint scelto per il failover potrebbe essere uno con una composizione del traffico impostata su zero.
- Il gruppo endpoint più vicino potrebbe non essere il gruppo endpoint originale. Questo perché Global Accelerator considera le impostazioni di composizione del traffico dell'account quando sceglie il gruppo di endpoint originale.

Ad esempio, supponiamo che la tua configurazione abbia due endpoint, uno integro e uno non integro e che tu abbia impostato il peso per ognuno di essi in modo che sia maggiore di zero. In questo caso, Global Accelerator indirizza il traffico all'endpoint integro. Tuttavia, ora si supponga di impostare il peso dell'unico endpoint integro su zero. Global Accelerator tenta quindi tre gruppi di endpoint aggiuntivi per trovare un endpoint sano con un peso maggiore di zero. Se non ne trova uno, Global Accelerator instraderà il traffico a un endpoint casuale nel gruppo di endpoint più vicino al client.

Aggiunta di endpoint con conservazione dell'indirizzo IP del client

Una funzionalità che è possibile utilizzare con alcuni tipi di endpoint, in alcune regioni, èConservazione dell'indirizzo IP del client: . Con questa funzionalità, si conserva l'indirizzo IP di

origine del client originale per i pacchetti che arrivano all'endpoint. È possibile utilizzare questa funzione con Application Load Balancer e gli endpoint di istanza Amazon EC2. Gli endpoint sugli acceleratori di routing personalizzati mantengono sempre l'indirizzo IP del client. Per ulteriori informazioni, consulta Conservare gli indirizzi IP client in AWS Global Accelerator.

Se si intende utilizzare la funzione di conservazione degli indirizzi IP del client, quando si aggiungono endpoint a Global Accelerator tenere presente quanto segue:

Interfacce di rete elastiche

Per supportare la conservazione degli indirizzi IP del client, Global Accelerator crea interfacce di rete elastiche nel tuo account AWS, una per ogni subnet in cui è presente un endpoint. Per ulteriori informazioni sul funzionamento di Global Accelerator con interfacce di rete elastiche, consultaProcedure consigliate per la conservazione degli indirizzi IP client: .

Endpoint nelle sottoreti private

È possibile indirizzare un Application Load Balancer o un'istanza EC2 in una subnet privata utilizzando AWS Global Accelerator, ma è necessario disporre di ungateway Internetcollegato al VPC che contiene gli endpoint. Per ulteriori informazioni, consulta Connessioni VPC sicure in AWS Global Accelerator.

Aggiungi l'indirizzo IP del client all'elenco Consenti

Prima di aggiungere e iniziare a instradare il traffico agli endpoint che conservano l'indirizzo IP del client, assicurarsi che tutte le configurazioni di protezione richieste, ad esempio i gruppi di sicurezza, vengano aggiornate in modo da includere l'indirizzo IP del client utente nell'elenco consentiti. Gli elenchi di controllo accessi di rete (ACL) si applicano solo al traffico in uscita (in uscita). Se è necessario filtrare il traffico in ingresso (in entrata), è necessario utilizzare i gruppi di protezione.

Configurare gli elenchi di controllo accessi di rete

Gli ACL di rete associati alle subnet VPC si applicano al traffico in uscita (in uscita) quando la conservazione degli indirizzi IP del client è abilitata sull'acceleratore. Tuttavia, per consentire l'uscita del traffico tramite Global Accelerator, è necessario configurare l'ACL sia come regola in entrata che in uscita.

Ad esempio, per consentire ai client TCP e UDP che utilizzano una porta di origine effimera di connettersi all'endpoint tramite Global Accelerator, associare la subnet dell'endpoint a un ACL di rete che consente il traffico in uscita destinato a una porta TCP o UDP effimera (intervallo di porte

1024-65535, destinazione 0.0.0.0/0). Inoltre, crea una regola in entrata corrispondente (intervallo di porte 1024-65535, origine 0.0.0.0/0).

> **Note**
>
> Il gruppo di sicurezza e le regole AWS WAF sono un set aggiuntivo di funzionalità che è possibile applicare per proteggere le risorse. Ad esempio, le regole del gruppo di sicurezza in entrata associate alle istanze Amazon EC2 e ai bilanciamenti del carico delle applicazioni consentono di controllare le porte di destinazione a cui i client possono connettersi tramite Global Accelerator, ad esempio la porta 80 per HTTP o la porta 443 per HTTPS. Tieni presente che i gruppi di sicurezza delle istanze Amazon EC2 si applicano a qualsiasi traffico che arriva alle tue istanze, incluso il traffico proveniente da Global Accelerator e qualsiasi indirizzo IP pubblico o elastico assegnato alla tua istanza. Come procedura consigliata, utilizzare le subnet private se si desidera garantire che il traffico venga recapitato solo da Global Accelerator. Assicurarsi inoltre che le regole del gruppo di sicurezza in ingresso siano configurate in modo appropriato per consentire o negare correttamente il traffico per le applicazioni.

Transizione degli endpoint per l'utilizzo della conservazione dell'indirizzo IP del client

Seguire le istruzioni riportate in questa sezione per la transizione di uno o più endpoint nell'acceleratore verso endpoint che conservano l'indirizzo IP del client dell'utente. Facoltativamente, è possibile scegliere di passare un endpoint Application Load Balancer o un endpoint di indirizzo IP elastico a un endpoint corrispondente, un Application Load Balancer o un'istanza EC2, con conservazione dell'indirizzo IP del client. Per ulteriori informazioni, consulta Conservare gli indirizzi IP client in AWS Global Accelerator.

È consigliabile eseguire la transazione all'utilizzo della conservazione degli indirizzi IP del client lentamente. Innanzitutto, aggiungere nuovi endpoint di istanza di Balancer di Application o EC2 abilitati per mantenere l'indirizzo IP del client. Quindi spostare lentamente il traffico dagli endpoint esistenti ai nuovi endpoint configurando i pesi sugli endpoint.

> **Important**
>
> Prima di instradare il traffico agli endpoint che conservano l'indirizzo IP del client, assicurarsi che tutte le configurazioni in cui sono stati inclusi gli indirizzi IP del client Global Accelerator

negli elenchi consentiti vengano aggiornate in modo da includere invece l'indirizzo IP del client utente.

La conservazione degli indirizzi IP del client è disponibile solo in aree AWS specifiche. Per ulteriori informazioni, consulta Regioni AWS supportate per la conservazione degli indirizzi IP client.

Questa sezione descrive come utilizzare i gruppi di endpoint nella console AWS Global Accelerator. Se desideri usare le operazioni API con Global Accelerator, consulta la documentazioneRiferimento all'API AWS Global Accelerator: .

Dopo aver spostato una piccola quantità di traffico nel nuovo endpoint con la conservazione dell'indirizzo IP del client, verificare che la configurazione funzioni come previsto. Quindi aumentare gradualmente la proporzione di traffico rispetto al nuovo endpoint regolando i pesi sugli endpoint corrispondenti.

Per passare agli endpoint che conservano gli indirizzi IP dei client, eseguire la procedura seguente per aggiungere un nuovo endpoint e, per gli endpoint Application Load Balancer con connessione Internet, abilitare la conservazione degli indirizzi IP del client. (L'opzione di conservazione dell'indirizzo IP del client è sempre selezionata per i Balancers applicazioni interne e le istanze EC2.)

Per aggiungere un endpoint con conservazione dell'indirizzo IP del client

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratori, scegliere un accelerator.
3. NellaListener, scegliere un listener.
4. NellaGruppo di endpoint, scegliere un gruppo di endpoint.
5. NellaEndpoint, scegliereAggiungi endpoint: .
6. SulAggiungi endpoint, nellaEndpoint, scegliere un endpoint Application Load Balancer o un endpoint di istanza EC2.
7. NellaPeso, scegliere un numero basso rispetto ai pesi impostati per gli endpoint esistenti. Ad esempio, se il peso di un corrispondente Application Load Balancer è 255, è possibile immettere un peso pari a 5 per il nuovo bilanciamento del carico applicazione, per iniziare. Per ulteriori informazioni, consulta Pesi dell'endpoint.

8. Per un nuovo endpoint Application Load Balancer esterno, inPreserve l'indirizzo IP del client, selezionaMantieni indirizzo: . Questa opzione è sempre selezionata per Application Load Balancers e istanze EC2 interne.
9. Seleziona Save changes (Salva modifiche).

Seguire quindi i passaggi riportati di seguito per modificare gli endpoint esistenti corrispondenti (che si stanno sostituendo con i nuovi endpoint con la conservazione dell'indirizzo IP del client) per ridurre il peso degli endpoint esistenti in modo da ridurre il traffico.

Per ridurre il traffico per gli endpoint esistenti

1. SulGruppo di endpoint, scegliere un endpoint esistente che non dispone della conservazione dell'indirizzo IP del client.
2. Seleziona Edit (Modifica).
3. SulModificare l'endpoint, nellaPeso, immettere un numero inferiore al numero corrente. Ad esempio, se il peso per un endpoint esistente è 255, è possibile immettere un peso di 220 per il nuovo endpoint (con conservazione dell'indirizzo IP del client).
4. Seleziona Save changes (Salva modifiche).

Dopo aver eseguito il test con una piccola parte del traffico originale impostando il peso del nuovo endpoint su un numero basso, è possibile passare lentamente tutto il traffico continuando a regolare i pesi per gli endpoint originali e nuovi.

Ad esempio, si supponga di iniziare con un servizio di Application Load Balancer esistente con un peso impostato su 200 e di aggiungere un nuovo endpoint Application Load Balancer con la conservazione dell'indirizzo IP del client abilitata con un peso impostato su 5. Spostare gradualmente il traffico dal Application Load Balancer originale al nuovo Application Load Balancer aumentando il peso del nuovo Application Load Balancer e diminuendo il peso per il bilanciamento del carico dell'applicazione originale. Ad esempio:

- Peso originale 190/nuovo peso 10
- Peso originale 180/nuovo peso 20
- Peso originale 170/nuovo peso 30, e così via.

Dopo aver ridotto il peso a 0 per l'endpoint originale, tutto il traffico (in questo scenario di esempio) passa al nuovo endpoint Application Load Balancer, che include la conservazione dell'indirizzo IP del client.

Se si dispone di endpoint aggiuntivi (Application Load Balancers o istanze EC2) che si desidera passare per utilizzare la conservazione degli indirizzi IP del client, ripetere i passaggi descritti in questa sezione per la transizione.

Se è necessario ripristinare la configurazione per un endpoint in modo che il traffico verso l'endpoint non conservi l'indirizzo IP del client, è possibile farlo in qualsiasi momento: aumentare il peso per l'endpoint che eseguenothanno la conservazione dell'indirizzo IP del client sul valore originale e ridurre il peso per l'endpointconconservazione dell'indirizzo IP del client a 0.

Utilizzare acceleratori di routing personalizzati in AWS Global Accelerator

Questo capitolo include procedure e consigli per la creazione di acceleratori di routing personalizzati in AWS Global Accelerator. Un acceleratore di routing personalizzato ti consente di utilizzare la logica dell'applicazione per mappare direttamente uno o più utenti a un'istanza di Amazon EC2 specifica tra molte destinazioni, ottenendo al contempo i miglioramenti delle prestazioni dell'instradamento del traffico tramite Global Accelerator. Ciò è utile quando si dispone di un'applicazione che richiede a un gruppo di utenti di interagire tra loro nella stessa sessione in esecuzione su un'istanza e una porta EC2 specifiche, ad esempio applicazioni di gioco o sessioni Voice over IP (VoIP).

Gli endpoint per gli acceleratori di routing personalizzati devono essere subnet di cloud privato virtuale (VPC) e un acceleratore di routing personalizzato può instradare il traffico solo alle istanze Amazon EC2 in tali subnet. Quando crei un acceleratore di routing personalizzato, puoi includere migliaia di istanze Amazon EC2 in esecuzione in una o più subnet VPC. Per ulteriori informazioni, vedi Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator.

Se invece si desidera che Global Accelerator scelga automaticamente l'endpoint integro più vicino ai client, creare un acceleratore standard. Per ulteriori informazioni, consulta Lavorare con gli acceleratori standard in AWS Global Accelerator.

Per impostare l'acceleratore di routing personalizzato, procedi come segue:

1. Esaminare le linee guida e i requisiti per la creazione di un acceleratore di routing personalizzato. Per informazioni, consulta Linee guida e restrizioni per gli acceleratori di routing personalizzati.
2. Creazione di una sottoreti VPC. È possibile aggiungere istanze EC2 alla subnet in qualsiasi momento dopo aver aggiunto la subnet a Global Accelerator.
3. Create un acceleratore e selezionate l'opzione per un acceleratore di routing personalizzato.
4. Aggiungere un listener e specificare un intervallo di porte su cui è possibile ascoltare Global Accelerator. Assicurati di includere una vasta gamma con porte sufficienti affinché Global Accelerator possa mappare tutte le destinazioni che ti aspetti di avere. Queste porte sono distinte dalle porte di destinazione, specificate nel passaggio successivo. Per ulteriori informazioni sui requisiti relativi alle porte del listener, consultaLinee guida e restrizioni per gli acceleratori di routing personalizzati: .
5. Aggiungere uno o più gruppi di endpoint per le regioni AWS in cui si dispone di subnet VPC. Per ogni gruppo di endpoint, è necessario specificare le seguenti opzioni:

- Intervallo di porte endpoint, che rappresenta le porte sulle istanze EC2 di destinazione che saranno in grado di ricevere traffico.
- Il protocollo per ogni intervallo di porte di destinazione: UDP, TCP o UDP e TCP.

6. Per la subnet endpoint, selezionare un ID subnet. È possibile aggiungere più subnet in ogni gruppo di endpoint e le subnet possono avere dimensioni diverse (fino a /17).

Le sezioni seguenti illustrano l'utilizzo di acceleratori di routing personalizzati, listener, gruppi di endpoint ed endpoint.

Argomenti

Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator

Utilizzando un acceleratore di routing personalizzato in AWS Global Accelerator, è possibile utilizzare la logica dell'applicazione per mappare direttamente uno o più utenti a una destinazione specifica tra molte destinazioni, ottenendo comunque i vantaggi in termini di prestazioni di Global Accelerator. Un acceleratore di routing personalizzato associa gli intervalli delle porte del listener alle destinazioni delle istanze EC2 nelle subnet del cloud privato virtuale (VPC). Ciò consente a Global Accelerator di instradare in modo deterministico il traffico a un indirizzo IP privato Amazon EC2 specifico e destinazione della porta nella subnet.

Ad esempio, puoi utilizzare un acceleratore di routing personalizzato con un'applicazione di gioco online in tempo reale in cui assegnare più giocatori a una singola sessione su un server di gioco Amazon EC2 in base a fattori che scegli, come posizione geografica, abilità del giocatore e modalità di gioco. Oppure potresti avere un'applicazione VoIP o social media che assegna più utenti a un server multimediale specifico per sessioni vocali, video e messaggistica.

L'applicazione può chiamare un'API Global Accelerator e ricevere una mappatura statica completa delle porte Global Accelerator e dei relativi indirizzi IP e porte di destinazione associati. È possibile salvare tale mapping statico e quindi il servizio di matchmaking utilizzarlo per instradare gli utenti a istanze EC2 di destinazione specifiche. Non devi effettuare modifiche al tuo software client per iniziare a utilizzare Global Accelerator con la tua applicazione.

Per configurare un acceleratore di routing personalizzato, selezionare un endpoint di subnet VPC. Quindi si definisce un intervallo di porte di destinazione a cui verranno mappate le connessioni in ingresso, in modo che il software possa ascoltare sullo stesso set di porte in tutte le istanze. Global Accelerator crea una mappatura statica che consente al servizio di matchmaking di tradurre un indirizzo IP di destinazione e un numero di porta per una sessione in un indirizzo IP esterno e una porta forniti agli utenti.

Lo stack di rete dell'applicazione potrebbe funzionare su un singolo protocollo di trasporto oppure è possibile utilizzare UDP per la consegna rapida e TCP per una consegna affidabile. È possibile impostare UDP, TCP o UDP e TCP per ogni intervallo di porte di destinazione, in modo da offrire la massima flessibilità senza dover duplicare la configurazione per ogni protocollo.

> **Note**
>
> Per impostazione predefinita, tutte le destinazioni di subnet VPC in un acceleratore di routing personalizzato non sono autorizzate a ricevere traffico. Questo deve essere sicuro per impostazione predefinita e anche per fornire un controllo granulare su quali destinazioni di istanza EC2 private nella subnet sono autorizzate a ricevere traffico. È possibile consentire o negare il traffico alla subnet o a combinazioni di indirizzi IP e porte specifiche (socket di destinazione). Per ulteriori informazioni, consulta Aggiunta, modifica o rimozione di un endpoint di subnet VPC. È inoltre possibile specificare le destinazioni utilizzando l'API Global Accelerator. Per ulteriori informazioni, consultaAllowCustomRoutingTeDenyCustomRoutingTraffic: .

Esempio di funzionamento del routing personalizzato in Global Accelerator

Ad esempio, supponiamo che tu voglia supportare 10.000 sessioni in cui gruppi di utenti interagiscono, ad esempio sessioni di gioco o chiamate VoIP, su 1.000 istanze Amazon EC2 dietro Global Accelerator. In questo esempio, verrà specificato un intervallo di porte del listener 10001-20040 e un intervallo di porte di destinazione 81-90. Diciamo che abbiamo le quattro subnet VPC in us-est-1: subnet-1, subnet-2, subnet-3 e subnet-4.

Nella configurazione di esempio, ogni subnet VPC ha una dimensione di blocco di /24 in modo che possa supportare 251 istanze Amazon EC2. (Cinque indirizzi sono riservati e non disponibili da ogni subnet e questi indirizzi non vengono mappati.) Ogni server in esecuzione su ogni istanza EC2 serve le seguenti 10 porte, specificate per le porte di destinazione nel nostro gruppo di endpoint: 81-90. Ciò significa che abbiamo 2510 porte (10 x 251) associate a ogni subnet. Ogni porta può essere associata a una sessione.

Poiché sono state specificate 10 porte di destinazione su ogni istanza EC2 nella nostra subnet, Global Accelerator le associa internamente a 10 porte listener che è possibile utilizzare per accedere alle istanze EC2. Per illustrarlo semplicemente, diciamo che esiste un blocco di porte del listener che inizia con il primo indirizzo IP della subnet endpoint per il primo set di 10, quindi passa all'indirizzo IP successivo per il set successivo di 10 porte del listener.

> **Note**
>
> La mappatura in realtà non è prevedibile in questo modo, ma stiamo usando una mappatura sequenziale qui per aiutare a mostrare come funziona la mappatura delle porte. Per determinare il mapping effettivo per gli intervalli di porte del listener, utilizzare le seguenti operazioni API: ListCustomRoutingPortMappingseListCustomRoutingPortMappingsByDestination: .

Nel nostro esempio, la prima porta listener è 10001. Tale porta è associata al primo indirizzo IP della subnet, 192.0.2.4, e alla prima porta EC2 81. La porta del listener successivo, 10002, è associata al primo indirizzo IP della subnet, 192.0.2.4, e alla seconda porta EC2 82. Nella tabella seguente viene illustrato il modo in cui questo mapping di esempio continua attraverso l'ultimo indirizzo IP della prima subnet VPC e quindi il primo indirizzo IP della seconda subnet VPC.

Porta del listener Global Accelerator	Sottoreti VPC	Porta istanza EC2
10001	192.0.2.4	81
10002	192.0.2.4	82
10003	192.0.2.4	83
10004	192.0.2.4	84
10005	192.0.2.4	85

Porta del listener Global Accelerator	Sottoreti VPC	Porta istanza EC2
10006	192.0.2.4	86
10007	192.0.2.4	87
10008	192.0.2.4	88
10009	192.0.2.4	89
10010	192.0.2.4	90
10011	192.0.2.5	81
10012	192.0.2.5	82
10013	192.0.2.5	83
10014	192.0.2.5	84
10015	192.0.2.5	85
10016	192.0.2.5	86
10017	192.0.2.5	87
10018	192.0.2.5	88
10019	192.0.2.5	89
10020	192.0.2.5	90
...	...	...
12501	192.0.2.244	81
12502	192.0.2.244	82
12503	192.0.2.244	83
12504	192.0.2.244	84

Porta del listener Global Accelerator	Sottoreti VPC	Porta istanza EC2
12505	192.0.2.244	85
12506	192.0.2.244	86
12507	192.0.2.244	87
12508	192.0.2.244	88
12509	192.0.2.244	89
12510	192.0.2.244	90
12511	192.0.3.4	81
12512	192.0.3.4	82
12513	192.0.3.4	83
12514	192.0.3.4	84
12515	192.0.3.4	85
12516	192.0.3.4	86
12517	192.0.3.4	87
12518	192.0.3.4	88
12519	192.0.3.4	89
12520	192.0.3.4	90

Linee guida e restrizioni per gli acceleratori di routing personalizzati

Quando crei e lavori con acceleratori di routing personalizzati in AWS Global Accelerator, tieni presente le linee guida e le restrizioni seguenti.

Destinazioni delle istanze Amazon EC2

Gli endpoint della sottorete di cloud pubblico virtuale (VPC) in un acceleratore di routing personalizzato possono includere solo istanze EC2. Non sono supportate altre risorse, ad esempio i bilanciamenti del carico, per l'acceleratore di routing personalizzato.

I tipi di istanze EC2 supportate da Global Accelerator sono elencati in Endpoint per acceleratori standard in AWS Global Accelerator: .

Mappature porte

Quando si aggiunge una subnet VPC, Global Accelerator crea un mapping di porte statico degli intervalli di porte del listener agli intervalli di porte supportati dalla subnet. Il mapping delle porte per una subnet specifica non cambia mai.

È possibile visualizzare l'elenco di mappature porte per un acceleratore di routing personalizzato a livello di programmazione. Per ulteriori informazioni, consulta `ListCustomRoutingPortMappings`.

Dimensione della sottorete VPC

Le subnet VPC aggiunte a un acceleratore di routing personalizzato devono essere un minimo di /28 e un massimo di /17.

Gli intervalli di porte del listener

È necessario specificare un numero sufficiente di porte del listener, specificando intervalli di porte del listener, per soddisfare il numero di destinazioni incluse nelle subnet che si prevede di aggiungere all'acceleratore di routing personalizzato. L'intervallo specificato quando si crea un listener determina il numero di combinazioni di porte e indirizzi IP di destinazione che è possibile utilizzare con l'acceleratore di routing personalizzato. Per la massima flessibilità e per ridurre la possibilità di ottenere un errore che non si dispone di porte del listener sufficienti, si consiglia di specificare un intervallo di porte ampio.

Global Accelerator alloca intervalli di porte in blocchi quando si aggiunge una subnet a un acceleratore di routing personalizzato. Si consiglia di allocare gli intervalli delle porte del listener in modo lineare e di rendere gli intervalli sufficientemente grandi da supportare il numero di porte di destinazione che si intende disporre. Cioè, il numero di porte da allocare dovrebbe essere almeno la dimensione della subnet per il numero di porte e protocolli di destinazione (configurazioni di destinazione) che si avrà nella subnet.

> **Note**
>
> L'algoritmo utilizzato da Global Accelerator per allocare i mapping delle porte potrebbe richiedere l'aggiunta di altre porte del listener, oltre a questo totale.

Dopo aver creato un listener, è possibile modificarlo per aggiungere ulteriori intervalli di porte e protocolli associati, ma non è possibile ridurre gli intervalli di porte esistenti. Ad esempio, se si dispone di un intervallo di porte del listener compreso tra 5.000 e 10.000, non è possibile modificare l'intervallo di porte in modo da 5900—10.000 e non è possibile modificare l'intervallo di porte in modo da 5.000—9.900.

Ogni intervallo di porte del listener deve includere un minimo di 16 porte. I listener supportano le porte 1-65535.

Intervalli porte di destinazione

Esistono due posizioni in cui è possibile specificare intervalli di porte per un acceleratore di routing personalizzato: gli intervalli di porte specificati quando si aggiunge un listener e gli intervalli e i protocolli delle porte di destinazione specificati per un gruppo di endpoint.

- Gli intervalli di porte del listener: Le porte del listener sugli indirizzi IP statici di Global Accelerator a cui i client si connettono. Global Accelerator associa ogni porta a un indirizzo IP di destinazione univoco e una porta su una subnet VPC dietro l'acceleratore.
- Gli intervalli di porte di destinazione: I set di intervalli di porte di destinazione specificati per un gruppo di endpoint (denominati anche configurazioni di destinazione) sono le porte dell'istanza EC2 che ricevono il traffico. Per ricevere traffico sulle porte di destinazione, i gruppi di protezione associati alle istanze EC2 devono consentire il traffico su di esse.

Controlli Health e failover

Global Accelerator non esegue controlli di integrità per gli acceleratori di routing personalizzati e non esegue il failover sugli endpoint integri. Il traffico per gli acceleratori di routing personalizzati viene instradato in modo deterministico, indipendentemente dall'integrità di una risorsa di destinazione.

Tutto il traffico viene negato per impostazione predefinita

Per impostazione predefinita, il traffico diretto tramite un acceleratore di routing personalizzato viene negato a tutte le destinazioni nella subnet. Per consentire alle istanze di destinazione di

ricevere traffico, è necessario consentire in modo specifico tutto il traffico verso la subnet o, in alternativa, consentire il traffico verso indirizzi IP di istanza specifici e porte nella subnet.

L'aggiornamento di una subnet o di una destinazione specifica per consentire o negare il traffico richiede tempo per propagarsi su Internet. Per determinare se una modifica è stata propagata, è possibile chiamare il metodo`DescribeCustomRoutingAccelerator`Azione API per controllare lo stato dell'acceleratore. Per ulteriori informazioni, consultaDescribeCustomRoutingAccelerator: .

AWS CloudFormation non è supportato

AWS CloudFormation non è supportato per gli acceleratori di routing personalizzati.

Acceleratori personalizzati in AWS Global Accelerator

AAcceleratore di routing personalizzatoin AWS Global Accelerator consente di utilizzare la logica dell'applicazione personalizzata per indirizzare uno o più utenti a una destinazione specifica tra molte destinazioni, utilizzando al contempo la rete globale AWS per migliorare la disponibilità e le prestazioni dell'applicazione.

Un acceleratore di routing personalizzato indirizza il traffico solo alle porte su istanze Amazon EC2 in esecuzione in subnet di cloud privato virtuale (VPC). Con un acceleratore di routing personalizzato, Global Accelerator non instradare il traffico in base alla geoprossimità o allo stato dell'endpoint. Per ulteriori informazioni, vedi Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator.

Quando create un acceleratore, per impostazione predefinita, Global Accelerator fornisce un set di due indirizzi IP statici. Se apporti il tuo intervallo di indirizzi IP su AWS (BYOIP), puoi invece assegnare indirizzi IP statici dal tuo pool per l'utilizzo con l'acceleratore. Per ulteriori informazioni, consulta Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator.

> **Important**
>
> Gli indirizzi IP vengono assegnati all'acceleratore per tutto il tempo in cui esiste, anche se si disattiva l'acceleratore e non accetta più o indirizza il traffico. Tuttavia, quando sideleteun acceleratore, si perdono gli indirizzi IP statici di Global Accelerator assegnati all'acceleratore, in modo che non sia più possibile instradare il traffico utilizzando tali indirizzi. Come procedura consigliata, assicurarsi di disporre delle autorizzazioni per evitare di eliminare involontariamente gli acceleratori. È possibile utilizzare criteri IAM come autorizzazioni basate

su tag con Global Accelerator per limitare gli utenti che dispongono delle autorizzazioni per eliminare un acceleratore. Per ulteriori informazioni, consulta Policy basate su tag.

In questa sezione viene illustrato come creare, modificare o eliminare un acceleratore di routing personalizzato nella console Global Accelerator. Per informazioni sull'utilizzo delle operazioni API con Global Accelerator, vedere laRiferimento per l'API AWS Global Accelerator: .

Argomenti

Creazione o aggiornamento di un acceleratore di routing personalizzato

Per creare un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. ScegliereCreate accelerator: .
3. Fornisci un nome per l'acceleratore.
4. PerTipo di acceleratore, selezionareRouting personalizzato: .
5. Facoltativamente, se hai portato il tuo intervallo di indirizzi IP su AWS (BYOIP), puoi specificare gli indirizzi IP statici per il tuo acceleratore da quel pool di indirizzi. Effettuare questa scelta per ciascuno dei due indirizzi IP statici dell'acceleratore.
   - Per ogni indirizzo IP statico, scegliere il pool di indirizzi IP da utilizzare.
   - Se è stato scelto il proprio pool di indirizzi IP, scegliere anche un determinato indirizzo IP dal pool. Se hai scelto il pool di indirizzi IP Amazon predefinito, Global Accelerator assegna un indirizzo IP specifico al tuo acceleratore.
6. Eventualmente, è possibile aggiungere uno o più tag per facilitare l'identificazione delle risorse acceleratore.
7. ScegliereSuccessivoper passare alle pagine successive della procedura guidata per aggiungere listener, gruppi di endpoint e endpoint di subnet VPC.

Per modificare un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco degli acceleratori di routing personalizzati, sceglierne uno, quindi scegliereModificare: .
3. SulModifica acceleratoreApporta le modifiche desiderate. Ad esempio, è possibile disabilitare l'acceleratore in modo da poterlo eliminare.
4. Seleziona Salva.

Visualizzazione degli acceleratori di routing personalizzati

È possibile visualizzare informazioni sugli acceleratori di routing personalizzati nella console. Per visualizzare le descrizioni degli acceleratori di routing personalizzati a livello di programmazione, vedereListCustomRoutingAcceleratoreDescribeCustomRoutingAcceleratorNella Riferimento per l'API di AWS Global Accelerator.

Per visualizzare le informazioni sugli acceleratori di routing personalizzati

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Per visualizzare i dettagli di un acceleratore, scegliere un acceleratore, quindi scegliereVisualizzazione: .

Eliminazione di un acceleratore di routing personalizzato

Se è stato creato un acceleratore di routing personalizzato come test o se non si utilizza più un acceleratore, è possibile eliminarlo. Sulla console, disabilitare l'acceleratore e quindi eliminarlo. Non è necessario rimuovere i listener e i gruppi di endpoint dall'acceleratore.

Per eliminare un acceleratore di routing personalizzato utilizzando un'operazione API anziché la console, è necessario innanzitutto rimuovere tutti i listener e i gruppi di endpoint associati all'acceleratore e quindi disabilitarlo. Per ulteriori informazioni, consulta la .DeleteAcceleratoroperazione nellaRiferimento per l'API AWS Global Accelerator: .

Per disattivare un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco, scegliere un acceleratore che si desidera disabilitare.
3. Seleziona Edit (Modifica).
4. ScegliereDisabilita acceleratore, quindi scegliereSave (Salva): .

Per eliminare un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. Nell'elenco, scegliere un acceleratore che si desidera eliminare.
3. Scegli Elimina.

> **Note**
>
> Se non è stato disabilitato l'acceleratore,EliminaNon è disponibile. Per disabilitare l'acceleratore, consultare la procedura precedente.

4. Nella finestra di dialogo di conferma, seleziona Delete (Elimina).

> **Important**
>
> Quando si elimina un acceleratore, si perdono gli indirizzi IP statici assegnati all'acceleratore, in modo che non sia più possibile instradare il traffico utilizzando tali indirizzi.

Listener per acceleratori di routing personalizzati in AWS Global Accelerator

Per un acceleratore di routing personalizzato in AWS Global Accelerator, è possibile configurare un listener che specifica un intervallo di porte del listener con protocolli associati che Global Accelerator esegue il mapping a istanze Amazon EC2 di destinazione specifiche negli endpoint della subnet VPC. Quando si aggiunge un endpoint di subnet VPC, Global Accelerator crea un mapping di porte

statico tra gli intervalli di porte definiti per il listener e gli indirizzi IP di destinazione e le porte nella subnet. Quindi è possibile utilizzare la mappatura delle porte per specificare gli indirizzi IP statici dell'acceleratore insieme a una porta listener e un protocollo per indirizzare il traffico utente verso indirizzi IP e porte dell'istanza Amazon EC2 di destinazione specifica nella subnet VPC.

La definizione del listener avviene al momento della creazione di un acceleratore di routing personalizzato; si possono aggiungere altri listener in qualsiasi momento. Ogni listener può avere uno o più gruppi di endpoint, uno per ogni regione AWS in cui sono presenti endpoint di subnet VPC. Un listener in un acceleratore di routing personalizzato supporta sia i protocolli TCP che UDP. Specificare il protocollo o i protocolli per ogni intervallo di porte di destinazione definito: UDP, TCP o UDP e TCP.

Per ulteriori informazioni, consulta Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator.

Aggiunta, modifica o rimozione di un listener di routing personalizzato

Questa sezione descrive come utilizzare listener di routing personalizzati sulla console di AWS Global Accelerator. Per informazioni sull'utilizzo delle operazioni API con AWS Global Accelerator, vedere laRiferimento all'API AWS Global Accelerator: .

Per aggiungere un listener per un acceleratore di routing personalizzato

L'intervallo specificato quando si crea un listener definisce il numero di combinazioni di porte e indirizzi IP di destinazione che è possibile utilizzare con l'acceleratore di routing personalizzato. Per la massima flessibilità, si consiglia di specificare un intervallo di porte di grandi dimensioni. Ogni intervallo di porte del listener specificato deve includere un minimo di 16 porte.

> **Note**
>
> Dopo aver creato un listener, è possibile modificarlo per aggiungere ulteriori intervalli di porte e protocolli associati, ma non è possibile ridurre gli intervalli di porte esistenti.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un acceleratore di routing personalizzato.
3. Scegli Add listener (Aggiungi listener).

4. SulAggiungi listener, immettere l'intervallo di porte del listener che si desidera associare all'acceleratore.

   Listener supportano le porte 1-65535. Per la massima flessibilità con un acceleratore di routing personalizzato, si consiglia di specificare un ampio intervallo di porte.

5. Scegli Add listener (Aggiungi listener).

Per modificare un listener per un acceleratore di routing personalizzato

Quando si modifica un listener per un acceleratore di routing personalizzato, tenere presente che è possibile aggiungere intervalli di porte aggiuntivi e protocolli associati, aumentare gli intervalli di porte esistenti o modificare i protocolli, ma non è possibile ridurre gli intervalli di porte esistenti.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un accelerator.
3. Scegli un listener, quindiModifica del listener: .
4. SulModifica del listener, apportare le modifiche desiderate agli intervalli di porte o ai protocolli esistenti oppure aggiungere nuovi intervalli di porte.

   Tenere presente che non è possibile ridurre l'intervallo di un intervallo di porte esistente.

5. Seleziona Salva.

Per rimuovere un listener

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegli un accelerator.
3. Scegli un listener, quindiRemove: .
4. Nella finestra di dialogo di conferma, scegliereRemove: .

Gruppi di endpoint per acceleratori di routing personalizzati in AWS Global Accelerator

Con un acceleratore di routing personalizzato in AWS Global Accelerator, un gruppo di endpoint definisce le porte e i protocolli su cui le istanze Amazon EC2 di destinazione nelle subnet cloud privato virtuale (VPC) accettano traffico.

È possibile creare un gruppo di endpoint per l'acceleratore di routing personalizzato per ogni area AWS in cui si trovano le subnet VPC e le istanze EC2. Ogni gruppo di endpoint in un acceleratore di routing personalizzato può avere più endpoint di subnet VPC. Analogamente, è possibile aggiungere ogni VPC a più gruppi di endpoint, ma i gruppi di endpoint devono essere associati a listener diversi.

Per ogni gruppo di endpoint, è necessario specificare un set di uno o più intervalli di porte che includono le porte a cui si desidera indirizzare il traffico sulle istanze EC2 nella regione. Per ogni intervallo di porte del gruppo di endpoint, specificare il protocollo da utilizzare: UDP, TCP o UDP e TCP. Ciò garantisce la massima flessibilità, senza dover duplicare set di intervalli di porte per ogni protocollo. Ad esempio, potresti avere un server di gioco con traffico di gioco in esecuzione su UDP sulle porte 8080-8090 mentre un server ascolta messaggi di chat su TCP sulla porta 80.

Per ulteriori informazioni, vedi Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator.

Aggiunta, modifica o rimozione di un gruppo di endpoint per un acceleratore di routing personalizzato

Si lavora con un gruppo di endpoint per l'acceleratore di routing personalizzato sulla console AWS Global Accelerator o utilizzando un'operazione API. È possibile aggiungere o rimuovere endpoint di subnet VPC da un gruppo di endpoint in qualsiasi momento.

Questa sezione spiega come utilizzare i gruppi di endpoint per l'acceleratore di routing personalizzato sulla console AWS Global Accelerator. Per informazioni sull'utilizzo delle operazioni API con Global Accelerator, vedere laInformazioni su AWS Global Accelerator API: .

Per aggiungere un gruppo di endpoint per un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegliere un acceleratore di routing personalizzato.

3. NellaListenerSezione, perID del listenerScegliere l'ID del listener a cui aggiungere un gruppo di endpoint.
4. ScegliereAggiungi un gruppo di endpoint: .
5. Nella sezione relativa a un listener specificare una regione per il gruppo di endpoint.
6. PerSet di porte e protocolli, immettere intervalli di porte e protocolli per le istanze Amazon EC2.

   - Inserimento di unDal portoe unAlla portaPer specificare un intervallo di porte.
   - Per ogni intervallo di porte, specificare il protocollo o i protocolli per tale intervallo.

   L'intervallo di porte non deve essere necessariamente un sottoinsieme dell'intervallo di porte del listener, ma nell'intervallo delle porte del listener devono essere presenti abbastanza porte totali per supportare il numero totale di porte specificato per i gruppi di endpoint nell'acceleratore di routing personalizzato.
7. Seleziona Salva.
8. FacoltativamenteSceglie reAggiungi un gruppo di endpointPer aggiungere gruppi di endpoint aggiuntivi per questo listener. È inoltre possibile scegliere un altro listener e aggiungere gruppi di endpoint.
9. SceglieReAggiungi un gruppo di endpoint: .

Per modificare un gruppo di endpoint per un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegliere un acceleratore di routing personalizzato.
3. NellaListenerSezione, perID del listenerScegliere l'ID del listener a cui è associato il gruppo di endpoint.
4. SceglieReModifica il gruppo di endpoint: .
5. SulModifica il gruppo di endpoint, modificare la regione, l'intervallo di porte o il protocollo per un intervallo di porte.
6. Seleziona Salva.

Per rimuovere un acceleratore di routing personalizzato

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriScegliere un acceleratore.
3. NellaListenerSelezionare un listener e selezionareRemove: .
4. NellaGruppi di endpointSelezionare un gruppo di endpoint e selezionareRemove: .
5. Nella finestra di dialogo di conferma, selezionareRemove: .

Endpoint di subnet VPC per acceleratori di routing personalizzati in AWS Global Accelerator

Gli endpoint per gli acceleratori di routing personalizzati sono subnet di cloud privato virtuale (VPC) in grado di ricevere traffico tramite un acceleratore. Ogni subnet può contenere una o più destinazioni istanza Amazon EC2. Quando si aggiunge un endpoint di subnet, Global Accelerator genera un nuovo mapping delle porte. È quindi possibile utilizzare l'API Global Accelerator per ottenere un elenco statico di tutti i mapping delle porte per la subnet, che è possibile utilizzare per instradare il traffico agli indirizzi IP dell'istanza EC2 di destinazione nella subnet. Per ulteriori informazioni, consultaListCustomRoutingPortMappings: .

È possibile indirizzare il traffico solo alle istanze EC2 nelle subnet, non ad altre risorse come i bilanciatori di carico (a differenza degli acceleratori standard). I tipi di istanza EC2 supportati sono elencati inEndpoint per acceleratori standard in AWS Global Accelerator: .

Per ulteriori informazioni, vedi Funzionamento degli acceleratori di routing personalizzati in AWS Global Accelerator.

Quando si aggiungono subnet VPC per l'acceleratore di routing personalizzato, tenere presente quanto segue:

- Per impostazione predefinita, il traffico diretto tramite un acceleratore di routing personalizzato non può arrivare a nessuna destinazione nella subnet. Per consentire alle istanze di destinazione di ricevere il traffico, è necessario scegliere di consentire tutto il traffico verso la subnet o, in alternativa, abilitare il traffico verso indirizzi IP e porte specifiche dell'istanza (socket di destinazione) nella subnet.

> **Important**
>
> L'aggiornamento di una subnet o di una destinazione specifica per consentire o negare il traffico richiede tempo per propagarsi su Internet. Per determinare se una modifica è stata propagata, è possibile chiamare il metodo`DescribeCustomRoutingAccelerator`Azione API per controllare lo stato dell'acceleratore. Per ulteriori informazioni, consultaDescribeCustomRoutingAccelerator: .

- Poiché le subnet VPC conservano l'indirizzo IP del client, è consigliabile esaminare le informazioni relative alla protezione e alla configurazione quando si aggiungono subnet come endpoint per gli acceleratori di routing personalizzati. Per ulteriori informazioni, consulta Aggiunta di endpoint con conservazione dell'indirizzo IP del client.

Aggiunta, modifica o rimozione di un endpoint di subnet VPC

È possibile aggiungere endpoint di subnet cloud privato virtuale (VPC) ai gruppi di endpoint negli acceleratori di routing personalizzati in modo da poter indirizzare il traffico degli utenti alle istanze Amazon EC2 di destinazione nella subnet.

Quando si aggiungono e rimuovono istanze EC2 dalla subnet o si attiva o disabilita il traffico verso destinazioni EC2, è possibile modificare se tali destinazioni possono ricevere traffico. Tuttavia, il mapping delle porte Global Accelerator non cambia.

Per consentire il traffico verso alcune destinazioni nella subnet, ma non tutte, immettere gli indirizzi IP per ogni istanza EC2 che si desidera consentire, insieme alle porte dell'istanza che si desidera ricevere il traffico. Gli indirizzi IP specificati devono essere per le istanze EC2 nella subnet. È possibile specificare una porta o un intervallo di porte dalle porte mappate per la subnet.

È possibile rimuovere la subnet VPC dall'acceleratore rimuovendola da un gruppo di endpoint. La rimozione di una subnet non influisce sulla subnet stessa, ma Global Accelerator non può più indirizzare il traffico verso la subnet o verso le istanze Amazon EC2 in essa contenute. Inoltre, Global Accelerator recupererà il mapping delle porte per la subnet VPC per utilizzarle potenzialmente per le nuove subnet aggiunte.

I passaggi descritti in questa sezione spiegano come aggiungere, modificare o rimuovere gli endpoint di subnet VPC nella console AWS Global Accelerator. Per informazioni sull'utilizzo delle operazioni API con AWS Global Accelerator, vedere laInformazioni di riferimento sull'API Global Accelerator: .

Per aggiungere un endpoint di subnet VPC

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriSelezionare, selezionare un acceleratore di routing personalizzato.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, scegliere l'ID del gruppo di endpoint (regione AWS) a cui si desidera aggiungere l'endpoint subnet VPC.
5. NellaEndpoint, scegliereAggiungi endpoint: .
6. SulAggiungi endpointPagina, perEndpoint, scegliere una subnet VPC.

   Se non disponi di un VPC, non ci sono elementi nell'elenco. Per continuare, aggiungere almeno un VPC, quindi tornare ai passaggi qui e scegliere un VPC dall'elenco.
7. Per l'endpoint di subnet VPC aggiunto, è possibile scegliere di consentire o negare il traffico a tutte le destinazioni nella subnet oppure consentire il traffico solo a istanze e porte EC2 specifiche. L'impostazione predefinita è negare il traffico a tutte le destinazioni nella subnet.
8. Seleziona Add endpoint (Aggiungi endpoint).

Per consentire o negare il traffico verso destinazioni specifiche

È possibile modificare il mapping delle porte della subnet VPC per un endpoint per consentire o negare il traffico a istanze e porte EC2 specifiche (socket di destinazione) in una subnet.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriSelezionare, selezionare un acceleratore di routing personalizzato.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, scegliere l'ID del gruppo di endpoint (regione AWS) dell'endpoint della subnet VPC che si desidera modificare.
5. Selezionare una sottorete dell'endpoint, quindi selezionareView details (Visualizza i dettagli): .
6. SulEndpoint, sottoMappature porte, scegli un indirizzo IP, quindi selezionaModificare: .
7. Immetti le porte per le quali desideri abilitare il traffico, quindi selezionaConsenti-queste destinazioni: .

Per consentire o negare TUTTO il traffico a una subnet

È possibile aggiornare un endpoint per consentire o negare il traffico a tutte le destinazioni nella subnet VPC.

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriSelezionare, selezionare un acceleratore di routing personalizzato.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, scegliere l'ID del gruppo di endpoint (regione AWS) dell'endpoint della subnet VPC che si desidera aggiornare.
5. ScegliereConsenti/Nega di tutto: .
6. Scegliere un'opzione per consentire tutto il traffico o negare tutto il traffico, quindi scegliereSave (Salva): .

Per rimuovere un endpoint

1. Aprire la console Global Accelerator all'indirizzohttps://console.aws.amazon.com/globalaccelerator/home: .
2. SulAcceleratoriSelezionare, selezionare un acceleratore di routing personalizzato.
3. NellaListenerSezione, perID del listener, scegliere l'ID di un listener.
4. NellaGruppi di endpointSezione, perID gruppo di endpoint, scegliere l'ID del gruppo di endpoint (regione AWS) dell'endpoint della subnet VPC che si desidera rimuovere.
5. ScegliereRemove dell'endpoint: .
6. Nella finestra di dialogo di conferma, selezionareRemove: .

Indirizzi DNS e domini personalizzati in AWS Global Accelerator

Questo capitolo spiega come AWS Global Accelerator esegue il routing DNS e include informazioni sull'utilizzo di un dominio personalizzato con Global Accelerator.

Argomenti

Support per l'indirizzamento DNS in Global Accelerator

Quando si crea un routing personalizzato o un acceleratore standard, Global Accelerator fornisce due indirizzi IP statici. Assegna inoltre un Domain Name System (DNS) predefinito all'acceleratore, simile `aa1234567890abcdef.awsglobalaccelerator.com`, che punta agli indirizzi IP statici. Gli indirizzi IP statici sono pubblicizzati a livello globale utilizzando anycast dalla rete perimetrale AWS ai tuoi endpoint. È possibile utilizzare gli indirizzi IP statici dell'acceleratore o il nome DNS per instradare il traffico all'acceleratore. I server DNS e i resolver DNS utilizzano un round robin per risolvere il nome DNS per un acceleratore, pertanto il nome viene risolto negli indirizzi IP statici per l'acceleratore, restituiti da Amazon Route 53 in ordine casuale. I client utilizzano in genere il primo indirizzo IP restituito.

> **Note**
>
> Global Accelerator crea due record PTR (Pointer) che mappano gli indirizzi IP statici di un acceleratore al nome DNS corrispondente generato da Global Accelerator, per supportare la ricerca DNS inversa. È noto anche come zona ospitata inversa. Tenere presente che il nome DNS generato da Global Accelerator non è configurabile e non è possibile creare record PTR che puntano al nome di dominio personalizzato. Inoltre, Global Accelerator non crea record PTR per gli indirizzi IP statici da un intervallo di indirizzi IP fornito in AWS (BYOIP).

Instradare il traffico di dominio personalizzato all'acceleratore

Nella maggior parte degli scenari, è possibile configurare DNS per l'utilizzo del nome di dominio personalizzato (ad esempio`www.example.com`) con l'acceleratore, invece di utilizzare gli indirizzi IP statici assegnati o il nome DNS predefinito. Innanzitutto, utilizzando Amazon Route 53 o un altro provider DNS, crea un nome di dominio e quindi aggiungi o aggiorna i record DNS con i tuoi indirizzi IP Global Accelerator. In alternativa, è possibile associare il nome di dominio personalizzato al nome DNS dell'acceleratore. Completare la configurazione DNS e attendere che le modifiche si propagano su Internet. Quando un client invia una richiesta utilizzando il tuo nome di dominio personalizzato, il server DNS lo risolve negli indirizzi IP, in ordine casuale, o nel nome DNS per l'acceleratore.

Per utilizzare il nome di dominio personalizzato con Global Accelerator quando si utilizza Route 53 come servizio DNS, si crea un record alias che punta il nome di dominio personalizzato al nome DNS assegnato all'acceleratore. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, ma è possibile creare un record alias sia per il dominio root, ad esempio`example.com`e per i sottodomini, come`www.example.com`: . Per ulteriori informazioni, consultaScelta tra record alias e non aliasNella Guida per gli sviluppatori di Amazon Route 53.

Per impostare la Route 53 con un record alias per un acceleratore, seguire le istruzioni incluse nel seguente argomento: Destinazione aliasNella Guida per gli sviluppatori di Amazon Route 53. Per visualizzare le informazioni relative a Global Accelerator, scorrere verso il basso sulla schedaDestinazione alias(Certificato creato).

Utilizzare i propri indirizzi IP (BYOIP) in AWS Global Accelerator

AWS Global Accelerator utilizza indirizzi IP statici come punti di ingresso per i tuoi acceleratori. Questi indirizzi IP sono anycast da posizioni edge AWS. Per impostazione predefinita, Global Accelerator fornisce indirizzi IP statici dalPool di indirizzi IP Amazon: . Invece di utilizzare gli indirizzi IP forniti da Global Accelerator, è possibile configurare questi punti di ingresso come indirizzi IPv4 da intervalli di indirizzi personalizzati. Questo argomento spiega come utilizzare i propri intervalli di indirizzi IP personalizzati con Global Accelerator.

È possibile impiegare una parte o tutti i propri indirizzi IPv4 pubblici dalla rete locale per il proprio account AWS per l'utilizzo con Global Accelerator. Continuerai a essere il titolare degli intervalli di indirizzi, ma AWS li pubblicizza su Internet.

Non puoi utilizzare gli indirizzi IP che porti ad AWS per un servizio AWS con un altro servizio. I passaggi in questo capitolo descrivono come portare il proprio intervallo di indirizzi IP da utilizzare

solo in AWS Global Accelerator. Per informazioni sulla procedura per portare il proprio intervallo di indirizzi IP da utilizzare in Amazon EC2, consultaUtilizzare i propri indirizzi IP (BYOIP)Nella Guida per l'utente di Amazon EC2.

> **Important**
>
> È necessario smettere di pubblicizzare il proprio intervallo di indirizzi IP da altri percorsi prima di pubblicizzarlo tramite AWS. Se un intervallo di indirizzi IP è multihomed (ovvero, l'intervallo è pubblicizzato da più fornitori di servizi contemporaneamente), non possiamo garantire che il traffico verso l'intervallo di indirizzi entri nella nostra rete o che il flusso di lavoro pubblicitario BYOIP venga completato correttamente.

Dopo aver portato un intervallo di indirizzi ad AWS, viene visualizzato nell'account come un pool di indirizzi. Quando si crea un acceleratore, è possibile assegnargli un indirizzo IP dell'intervallo. Global Accelerator ti assegna un secondo indirizzo IP statico da un intervallo di indirizzi IP Amazon. Se si portano due intervalli di indirizzi IP ad AWS, è possibile assegnare un indirizzo IP da ogni intervallo all'acceleratore. Questa restrizione è dovuta al fatto che Global Accelerator assegna ogni intervallo di indirizzi a una zona di rete diversa, per una disponibilità elevata.

Per utilizzare un intervallo di indirizzi IP personalizzato con Global Accelerator, esaminare i requisiti e quindi seguire i passaggi descritti in questo argomento.

Argomenti

Requirements

Puoi portare fino a due intervalli di indirizzi IP idonei a AWS Global Accelerator per account AWS.

Per essere qualificato, l'intervallo di indirizzi IP deve soddisfare i seguenti requisiti:

- L'intervallo di indirizzi IP deve essere registrato in uno dei seguenti registri Internet regionali (RIR): American Registry for Internet Numeri (ARIN), Réseaux IP Européens Network Coordination Centre (RIPE) o Asia-Pacific Network Information Centre (APNIC). L'intervallo di indirizzi deve essere registrato in un'entità aziendale o istituzionale. Non può essere registrato per un individuo.
- L'intervallo di indirizzi più specifico che puoi portare è /24. I primi 24 bit dell'indirizzo IP specificano il numero di rete. Ad esempio, 198.51.100 è il numero di rete per l'indirizzo IP 198.51.100.0.
- Gli indirizzi IP nell'intervallo di indirizzi deve avere una cronologia pulita. Cioè, non possono avere una cattiva reputazione o essere associati a comportamenti dannosi. È opportuno rifiutare l'intervallo di indirizzi IP se esaminiamo la reputazione dell'intervallo di indirizzi IP e scopra che contiene un indirizzo IP che non ha una cronologia pulita.

Inoltre, sono necessari i seguenti tipi o stati di rete di allocazione e assegnazione, a seconda della posizione in cui è stato registrato l'intervallo di indirizzi IP:

- ARIN:`Direct Allocation` `Direct Assignment`Tipi di rete
- MATURI:`ALLOCATED PA`,`LEGACY`, e`ASSIGNED PI`Stati di allocazione
- APNIC:`ALLOCATED PORTABLE`e`ASSIGNED PORTABLE`Stati di allocazione

Preparazione per portare il proprio intervallo di indirizzi IP all'account AWS: Autorizzazione

Per garantire che solo tu possa portare lo spazio del tuo indirizzo IP ad Amazon, abbiamo bisogno di due autorizzazioni:

- Devi autorizzare Amazon a pubblicizzare l'intervallo di indirizzi IP.
- È necessario fornire la prova che si possiede l'intervallo di indirizzi IP e quindi avere l'autorità di portarlo ad AWS.

> **Note**
>
> Quando usi BYOIP per portare un intervallo di indirizzi IP in AWS, non puoi trasferire la proprietà di tale intervallo di indirizzi a un altro account o società mentre lo pubblicizziamo. Inoltre, non è possibile trasferire direttamente un intervallo di indirizzi IP da un account AWS a un altro account. Per trasferire la proprietà o per trasferire tra account AWS, è

necessario annullare il provisioning dell'intervallo di indirizzi e quindi il nuovo proprietario deve seguire i passaggi per aggiungere l'intervallo di indirizzi al proprio account AWS.

Per autorizzare Amazon a pubblicizzare l'intervallo di indirizzi IP, fornisci ad Amazon un messaggio di autorizzazione firmato. Utilizzare un'autorizzazione origine route (ROA) per fornire questa autorizzazione. Un ROA è un'istruzione crittografica relativa agli annunci route creati tramite il tuo registro Internet regionale (RIR). Un ROA contiene l'intervallo di indirizzi IP, gli Autonomous System Numeri (ASN) autorizzati a pubblicizzare l'intervallo di indirizzi IP e una data di scadenza. Il ROA autorizza Amazon a pubblicizzare un intervallo di indirizzi IP nell'ambito di un sistema autonomo specifico (AS).

Un ROA non autorizza il tuo account AWS a portare l'intervallo di indirizzi IP in AWS. Per fornire questa autorizzazione, è necessario pubblicare un certificato X.509 autofirmato nelle osservazioni Registry Data Access Protocol (RDAP) per l'intervallo di indirizzi IP. Il certificato contiene una chiave pubblica che AWS impiega per verificare la firma del contesto di autorizzazione fornito. Mantenere la chiave privata sicura e utilizzarla per firmare il messaggio del contesto di autorizzazione.

Le sezioni seguenti forniscono informazioni dettagliate su come completare queste attività di autorizzazione. I comandi di questi passaggi sono supportati su Linux. Se si utilizza Windows, è possibile accedere alSottosistema Windows per Linuxper eseguire i comandi Linux.

Passi per fornire l'autorizzazione

- Fase 1: Creazione di un oggetto ROA
- Fase 2: Creazione di un certificato autofirmato X.509
- Fase 3: Creazione di un messaggio di autorizzazione firmato

Fase 1: Creazione di un oggetto ROA

Crea un oggetto ROA per autorizzare Amazon ASN 16509 a pubblicizzare il tuo intervallo di indirizzi IP e gli ASN autorizzati a pubblicizzare l'intervallo di indirizzi IP. Il ROA deve contenere l'indirizzo IP /24 che si desidera portare in AWS ed è necessario impostare la lunghezza massima su /24.

Per ulteriori informazioni sulla creazione di una richiesta di ROA, vedere le sezioni seguenti, a seconda della posizione in cui è stato registrato l'intervallo di indirizzi IP:

- ARIN: Richieste ROA

- MATURI: Gestione di ROAS
- APNIC: Gestione delle route

Fase 2: Creazione di un certificato autofirmato X.509

Utilizzare una key pair e un certificato autofirmato X.509 e aggiungere il certificato al record RDAP per il RIR. Di seguito viene descritto come eseguire queste attività.

> **Note**
>
> Laopensslln questa procedura è necessario OpenSSL versione 1.0.2 o successive.

Per creare e aggiungere un certificato X.509

1. Generare una key pair RSA a 2048 bit utilizzando il comando seguente.

   ```
   openssl genrsa -out private.key 2048
   ```

2. Utilizzare il comando seguente per creare un certificato X.509 pubblico dalla key pair.

   ```
   openssl req -new -x509 -key private.key -days 365 | tr -d "\n" > publickey.cer
   ```

   In questo esempio, il certificato scade tra 365 giorni; dopo tale data diventa inaffidabile. Quando si esegue il comando, assicurarsi di impostare il valore`-days`al valore desiderato per la scadenza corretta. Quando viene richiesto di immettere altre informazioni, è possibile accettare i valori predefiniti.

3. Aggiorna il record RDAP per il tuo RIR con il certificato X.509 utilizzando la seguente procedura, a seconda del RIR.

   1. Visualizzare il certificato utilizzando il comando seguente.

      ```
      cat publickey.cer
      ```

   2. Aggiungere il certificato effettuando le seguenti operazioni:

> **Important**
>
> Assicurati di includere il`-----BEGIN CERTIFICATE-----`e`-----END CERTIFICATE-----`Dal certificato.

- Per ARIN, aggiungere il certificato nella`Public Comments`Per l'intervallo di indirizzi IP.
- Per RIPE, aggiungere il certificato come nuovo`descr`Per l'intervallo di indirizzi IP.
- Per APNIC, inviare la chiave pubblica via e-mail a`helpdesk@apnic.net`, il contatto autorizzato APNIC per gli indirizzi IP, per richiedere di aggiungerlo manualmente al`remarks`Campo.

Fase 3: Creazione di un messaggio di autorizzazione firmato

Crea il messaggio di autorizzazione firmato per consentire ad Amazon di pubblicizzare il tuo intervallo di indirizzi IP.

Il formato del messaggio è il seguente, in cui il valore`YYYYMMDD`data è la data di scadenza del messaggio.

```
1|aws|aws-account|address-range|YYYYMMDD|SHA256|RSAPSS
```

Per creare il messaggio di autorizzazione firmato

1. Crea un messaggio di autorizzazione in testo normale e archivialo in una variabile denominata`text_message`, come illustrato nell'esempio seguente. Sostituire il numero di account di esempio, l'intervallo di indirizzi IP e la data di scadenza con i valori preferiti.

   ```
   text_message="1|aws|123456789012|203.0.113.0/24|20191201|SHA256|RSAPSS"
   ```

2. Firma il messaggio di autorizzazione in`text_message`Utilizzando la key pair creata nella sezione precedente.
3. Memorizzare il messaggio in una variabile denominata`signed_message`, come illustrato nell'esempio seguente.

   ```
   signed_message=$(echo $text_message | tr -d "\n" | openssl dgst -sha256 -sigopt
   ```

```
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private.key -keyform
PEM | openssl base64 |
    tr -- '+=/' '-_~' | tr -d "\n")
```

Eseguire il provisioning dell'intervallo di indirizzi da utilizzare con AWS Global Accelerator

Quando effettui il provisioning di un intervallo di indirizzi per l'uso con AWS, confermi di essere il proprietario dell'intervallo di indirizzi e che autorizzi Amazon a pubblicizzarlo. Verifichiamo che tu sia il proprietario dell'intervallo di indirizzi.

È necessario eseguire il provisioning dell'intervallo di indirizzi utilizzando le operazioni CLI o Global Accelerator API. Questa funzionalità non è disponibile nella console AWS.

Per effettuare il provisioning dell'intervallo di indirizzi, utilizza quanto segueProvisionByoipCidrComando. La`--cidr-authorization-context`Utilizza le variabili create nella sezione precedente, non il messaggio ROA.

```
aws globalaccelerator provision-byoip-cidr --cidr address-range --cidr-authorization-
context Message="$text_message",Signature="$signed_message"
```

Di seguito è riportato un esempio di provisioning di un intervallo di indirizzi.

```
aws globalaccelerator provision-byoip-cidr
    --cidr 203.0.113.25/24
    --cidr-authorization-context Message="$text_message",Signature="$signed_message"
```

Il provisioning di un intervallo di indirizzi è un'operazione asincrona, pertanto la chiamata ritorna immediatamente. Tuttavia, l'intervallo di indirizzi non è pronto per l'uso fino a quando il suo stato non cambia da`PENDING_PROVISIONING`Da a`READY`: . Il completamento del processo di provisioning può richiedere fino a 3 settimane. Per monitorare lo stato degli intervalli di indirizzi di cui è stato eseguito il provisioning, utilizzare la seguenteListByoIPcidrsComando :

```
aws globalaccelerator list-byoip-cidrs
```

Per visualizzare un elenco degli stati per un intervallo di indirizzi IP, vedereByoIPCIDR: .

Quando viene eseguito il provisioning dell'intervallo di indirizzi IP, il`State`Il valore restituito da`list-byoip-cidrs`è`READY`: . Ad esempio:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "READY"
        }
    ]
}
```

Pubblicizzazione dell'intervallo di indirizzi attraverso AWS

Dopo aver eseguito il provisioning, l'intervallo di indirizzi è pronto per essere pubblicizzato. Deve essere pubblicizzato l'intervallo di indirizzi esatto oggetto del provisioning. Non può essere pubblicizzata solo una parte dell'intervallo di indirizzi oggetto del provisioning. È inoltre necessario smettere di pubblicizzare il proprio intervallo di indirizzi IP da altri percorsi prima di pubblicizzarlo tramite AWS.

Devi pubblicizzare (o interrompere la pubblicità) il tuo intervallo di indirizzi utilizzando le operazioni CLI o Global Accelerator API. Questa funzionalità non è disponibile nella console AWS.

> **Important**
>
> Assicurati che l'intervallo di indirizzi IP sia pubblicizzato da AWS prima di utilizzare un indirizzo IP del pool con Global Accelerator.

Per pubblicizzare l'intervallo di indirizzi, utilizza quanto segueAnnunciaByoIPCIDRComando.

```
aws globalaccelerator advertise-byoip-cidr --cidr address-range
```

Di seguito è riportato un esempio di richiesta di Global Accelerator per pubblicizzare un intervallo di indirizzi.

```
aws globalaccelerator advertise-byoip-cidr --cidr 203.0.113.0/24
```

Per monitorare lo stato degli intervalli di indirizzi pubblicati, utilizzare la seguenteListByoIPcidrsComando.

```
aws globalaccelerator list-byoip-cidrs
```

Quando il tuo intervallo di indirizzi IP viene pubblicizzato, il`State`Il valore restituito da`list-byoip-cidrs`è`ADVERTISING`: . Ad esempio:

```
{
    "ByoipCidrs": [
        {
            "Cidr": "203.0.113.0/24",
            "State": "ADVERTISING"
        }
    ]
}
```

Per smettere di pubblicizzare un intervallo di indirizzi, utilizza quanto segue`withdraw-byoip-cidr`Comando.

> **Important**
>
> Per interrompere la pubblicità dell'intervallo di indirizzi, è innanzitutto necessario rimuovere tutti gli acceleratori con indirizzi IP statici allocati dal pool di indirizzi. Per eliminare un acceleratore utilizzando la console o le operazioni API, vedere Eliminazione di un acceleratore: .

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

Di seguito è riportato un esempio di richiesta di Global Accelerator di ritirare un intervallo di indirizzi.

```
aws globalaccelerator withdraw-byoip-cidr
    --cidr 203.0.113.25/24
```

Annullamento del provisioning dell'intervallo di indirizzi

Per interrompere l'utilizzo dell'intervallo di indirizzi con AWS, è necessario rimuovere gli acceleratori con indirizzi IP statici allocati dal pool di indirizzi e interrompere la pubblicità dell'intervallo di indirizzi. Dopo aver completato questi passaggi, è possibile annullare il provisioning dell'intervallo di indirizzi.

È necessario interrompere la pubblicità e annullare il provisioning dell'intervallo di indirizzi utilizzando le operazioni CLI o Global Accelerator API. Questa funzionalità non è disponibile nella console AWS.

Fase 1: Eliminare gli acceleratori associati.Per eliminare un acceleratore utilizzando la console o le operazioni API, vedere Eliminazione di un acceleratore: .

Fase 2. Interrompi la pubblicità dell'intervallo di indirizzi. Per smettere di pubblicizzare un intervallo, utilizza quanto segueRelissoIpcidrComando.

```
aws globalaccelerator withdraw-byoip-cidr --cidr address-range
```

Fase 3. Annullamento del provisioning dell'intervallo di indirizzi Per annullare il provisioning dell'intervallo, utilizzare il seguenteDeprovisioning ByoIPCIDRComando.

```
aws globalaccelerator deprovision-byoip-cidr --cidr address-range
```

Crea un acceleratore con i tuoi indirizzi IP

Ora puoi creare un acceleratore con i tuoi indirizzi IP. Se hai portato un intervallo di indirizzi ad AWS, puoi assegnare un indirizzo IP all'acceleratore. Se sono stati portati due intervalli di indirizzi, è possibile assegnare un indirizzo IP da ogni intervallo di indirizzi all'acceleratore.

Sono disponibili diverse opzioni per creare un acceleratore utilizzando i propri indirizzi IP per gli indirizzi IP statici:

- Utilizzare la console Global Accelerator per creare un acceleratore. Per ulteriori informazioni, consulta Creazione o aggiornamento di un acceleratore standard e Creazione o aggiornamento di un acceleratore di routing personalizzato.
- Utilizzare l'API Global Accelerator per creare un acceleratore. Per ulteriori informazioni, inclusi esempi di utilizzo dell'interfaccia della riga di comando, consultaCreateAcceleratoreCreateCustomRoutingAcceleratorNella Riferimento per l'API di AWS Global Accelerator

Conservare gli indirizzi IP client in AWS Global Accelerator

Le opzioni per la conservazione e l'accesso all'indirizzo IP del client per AWS Global Accelerator dipendono dagli endpoint configurati con l'acceleratore. Esistono due tipi di endpoint che possono conservare l'indirizzo IP di origine del client nei pacchetti in ingresso: Application Load Balancers e istanze Amazon EC2.

- Quando si utilizza un Application Load Balancer con connessione Internet come endpoint con Global Accelerator, la conservazione degli indirizzi IP del client è abilitata per impostazione predefinita per i nuovi acceleratori. Ciò significa che l'indirizzo IP di origine del client originale viene mantenuto per i pacchetti che arrivano al bilanciamento del carico. È possibile scegliere di disabilitare l'opzione quando si crea l'acceleratore o modificando l'acceleratore in un secondo momento.
- Quando si utilizza un Application Load Balancer interno o un'istanza EC2 con Global Accelerator, l'endpoint ha sempre attivato la conservazione degli indirizzi IP del client.

> **Note**
>
> Global Accelerator non supporta la conservazione degli indirizzi IP del client per gli endpoint di Network Load Balancer e degli indirizzi IP elastici.

Quando si prevede di aggiungere la conservazione dell'indirizzo IP client, ricorda quanto segue:

- Prima di aggiungere e iniziare a instradare il traffico agli endpoint che conservano l'indirizzo IP del client, assicurarsi che tutte le configurazioni di protezione richieste, ad esempio i gruppi di sicurezza, vengano aggiornate per includere l'indirizzo IP del client utente negli elenchi consentiti.
- La conservazione dell'indirizzo IP del client è supportata solo in aree AWS specifiche. Per ulteriori informazioni, consulta Regioni AWS supportate per la conservazione degli indirizzi IP client.

Argomenti

- Regioni AWS supportate per la conservazione degli indirizzi IP client

Come abilitare la conservazione dell'indirizzo IP del client

Quando si crea un nuovo acceleratore, la conservazione degli indirizzi IP del client è abilitata, per impostazione predefinita, per gli endpoint supportati.

Ricorda quanto segue:

- I servizi di bilanciamento del carico delle applicazioni interne e le istanze EC2 hanno sempre attivato la conservazione degli indirizzi IP del client. Non è possibile disabilitare l'opzione per questi endpoint.
- Quando si utilizza la console AWS per creare un nuovo acceleratore, l'opzione per la conservazione degli indirizzi IP del client è abilitata per impostazione predefinita per gli endpoint Application Load Balancer. È possibile disabilitare l'opzione in qualsiasi momento se non si desidera mantenere l'indirizzo IP del client per un endpoint Application Load Balancer con connessione Internet.
- Quando si utilizza l'interfaccia della riga di comando AWS o un'azione API per creare un nuovo acceleratore e non si specifica l'opzione per la conservazione degli indirizzi IP del client, gli endpoint di Application Load Balancer con connessione Internet dispongono di conservazione dell'indirizzo IP del client attivata per impostazione predefinita.
- Global Accelerator non supporta la conservazione degli indirizzi IP del client per gli endpoint di Network Load Balancer e degli indirizzi IP elastici.

Per gli acceleratori esistenti, è possibile passare gli endpoint senza la conservazione dell'indirizzo IP del client a endpoint che conservano l'indirizzo IP del client. Gli endpoint di Application Load Balancer esistenti possono essere trasferiti a nuovi endpoint Application Load Balancer e gli endpoint degli indirizzi IP elastici esistenti possono essere trasferiti agli endpoint dell'istanza EC2. (Gli endpoint di Network Load Balancer non supportano la conservazione degli indirizzi IP del client.) Per passare ai nuovi endpoint, si consiglia di spostare lentamente il traffico da un endpoint esistente a un nuovo endpoint con conservazione degli indirizzi IP client eseguendo le operazioni seguenti:

- Per gli endpoint di Application Load Balancer esistenti, aggiungere prima a Global Accelerator un endpoint duplicato di Application Load Balancer che si rivolge agli stessi back-end e, se si tratta di un Application Load Balancer con connessione Internet, abilitare la conservazione degli indirizzi IP del client. Quindi regolare i pesi sugli endpoint per spostare lentamente il traffico dal bilanciamento

del carico che eseguenotavere la conservazione dell'indirizzo IP del client abilitata al servizio di bilanciamento del caricoconConservazione dell'indirizzo IP del client.

- Per un endpoint di indirizzo IP elastico esistente, è possibile spostare il traffico in un endpoint di istanza EC2 con la conservazione dell'indirizzo IP del client. Aggiungere innanzitutto un endpoint di istanza EC2 a Global Accelerator, quindi regolare i pesi sugli endpoint per spostare lentamente il traffico dall'endpoint dell'indirizzo IP elastico all'endpoint dell'istanza EC2.

Per istruzioni dettagliate sulla transizione, consulta Transizione degli endpoint per l'utilizzo della conservazione dell'indirizzo IP del client: .

Vantaggi della conservazione dell'indirizzo IP client

Per gli endpoint per i quali non è abilitata la conservazione degli indirizzi IP client, gli indirizzi IP utilizzati dal servizio Global Accelerator nella rete perimetrale sostituiscono l'indirizzo IP dell'utente richiedente come indirizzo di origine nei pacchetti in arrivo. Le informazioni di connessione del client originale, ad esempio l'indirizzo IP del client e la porta del client, non vengono conservate mentre il traffico viaggia verso i sistemi dietro un acceleratore. Questo funziona bene per molte applicazioni, in particolare quelle che sono disponibili per tutti gli utenti, come i siti Web pubblici.

Tuttavia, per altre applicazioni è possibile accedere all'indirizzo IP del client originale utilizzando endpoint con conservazione dell'indirizzo IP del client. Ad esempio, quando si dispone dell'indirizzo IP del client, è possibile raccogliere statistiche basate sugli indirizzi IP del client. È inoltre possibile utilizzare filtri basati su indirizzi IP comel gruppi di sicurezza su Application Load Balancerper filtrare il traffico. È possibile applicare una logica specifica per l'indirizzo IP di un utente nelle applicazioni eseguite sui server a livello Web dietro l'endpoint Application Load Balancer utilizzando il`X-Forwarded-For`, che contiene le informazioni sull'indirizzo IP del client originale. È inoltre possibile utilizzare la conservazione dell'indirizzo IP del client nelle regole dei gruppi di sicurezza nei gruppi di sicurezza associati al servizio di Application Load Balancer. Per ulteriori informazioni, consulta Come viene conservato l'indirizzo IP del client in AWS Global Accelerator. Per gli endpoint dell'istanza EC2, l'indirizzo IP del client originale viene mantenuto.

Per gli endpoint che non dispongono di conservazione dell'indirizzo IP del client, è possibile filtrare l'indirizzo IP di origine utilizzato da Global Accelerator quando inoltra il traffico dalla periferia. È possibile visualizzare informazioni sugli indirizzi IP di origine (che sono anche indirizzi IP client, quando è abilitata la conservazione degli indirizzi IP del client) dei pacchetti in ingresso esaminando i log dei flussi di Global Accelerator. Per ulteriori informazioni, consulta Intervalli di ubicazione e indirizzi IP dei server edge di Global Accelerator e Logdi flusso in AWS Global Accelerator.

Come viene conservato l'indirizzo IP del client in AWS Global Accelerator

AWS Global Accelerator conserva l'indirizzo IP di origine del client in modo diverso per le istanze Amazon EC2 e Application Load Balancers:

- Per un endpoint di istanza EC2, l'indirizzo IP del client viene conservato per tutto il traffico.
- Per un endpoint Application Load Balancer con conservazione degli indirizzi IP del client, Global Accelerator collabora con Application Load Balancer per fornire un`X-Forwarded`Intestazione,`X-Forwarded-For`, che include l'indirizzo IP del client originale in modo che il livello Web possa accedervi.

Le richieste e le risposte HTTP utilizzano i campi intestazione per inviare informazioni sui messaggi HTTP. I campi intestazione sono costituti da coppie nome-valore separati da due punti e intervallati da un ritorno a capo e un avanzamento riga. Un insieme standard di campi dell'intestazione HTTP è definito nella RFC 2616,Intestazioni dei messaggi: . Sono anche disponibili intestazioni HTTP non standard, ampiamente utilizzate dalle applicazioni. Alcune delle intestazioni HTTP non standard hanno`X-Forwarded`prefisso.

Poiché Application Load Balancer termina le connessioni TCP in ingresso e crea nuove connessioni alle destinazioni back-end, non mantiene gli indirizzi IP del client fino al codice di destinazione (ad esempio istanze, contenitori o codice Lambda). L'indirizzo IP di origine visualizzato nelle destinazioni nel pacchetto TCP è l'indirizzo IP di Application Load Balancer. Tuttavia, un Application Load Balancer conserva l'indirizzo IP del client originale rimuovendolo dall'indirizzo di risposta del pacchetto originale e inserendolo in un'intestazione HTTP prima di inviare la richiesta al back-end tramite una nuova connessione TCP.

La`X-Forwarded-For`l'intestazione della richiesta è formattata in questo modo:

```
X-Forwarded-For: client-ip-address
```

L'esempio seguente mostra un`X-Forwarded-For`Intestazione della richiesta per un client con l'indirizzo IP 203.0.113.7.

```
X-Forwarded-For: 203.0.113.7
```

Procedure consigliate per la conservazione degli indirizzi IP client

Quando si utilizza la conservazione degli indirizzi IP client in AWS Global Accelerator, tenere presente le informazioni e le procedure consigliate in questa sezione per le interfacce di rete elastiche e i gruppi di sicurezza.

Per supportare la conservazione degli indirizzi IP del client, Global Accelerator crea interfacce di rete elastiche nel tuo account AWS, una per ogni subnet in cui è presente un endpoint. Un'interfaccia di rete elastica è un componente di rete logico in un VPC che rappresenta una scheda di rete virtuale. Global Accelerator utilizza queste interfacce di rete elastiche per indirizzare il traffico agli endpoint configurati dietro un acceleratore. Gli endpoint supportati per il traffico di routing in questo modo sono Application Load Balancers (interno e connesso a Internet) e istanze Amazon EC2.

> **Note**
>
> Quando si aggiunge un Application Load Balancer interno o un endpoint di istanza EC2 in Global Accelerator, si abilita il flusso del traffico Internet direttamente da e verso l'endpoint in Virtual Private Cloud (VPC) tramite il targeting in una subnet privata. Per ulteriori informazioni, consulta Connessioni VPC sicure in AWS Global Accelerator.

Come Global Accelerator utilizza interfacce di rete elastiche

Quando si dispone di un servizio di Application Load Balancer con la conservazione degli indirizzi IP del client abilitata, il numero di subnet in cui si trova il servizio di bilanciamento del carico determina il numero di interfacce di rete elastiche create da Global Accelerator nell'account. Global Accelerator crea un'elastic network interface per ogni subnet in cui è presente almeno un'elastic network interface di Application Load Balancer che è diretta da un acceleratore nell'account.

Negli esempi seguenti viene illustrato il funzionamento.

- Esempio 1: Se un Application Load Balancer dispone di interfacce di rete elastiche nella subnet A e nella subnet B e quindi si aggiunge il bilanciamento del carico come endpoint di accelerazione, Global Accelerator crea due interfacce di rete elastiche, una in ogni subnet.
- Esempio 2: Se ad Accelerator1 si aggiunge, ad esempio, un ALB1 che dispone di interfacce di rete elastiche in SubNetA e SubNetB e quindi si aggiunge un ALB2 con interfacce di rete elastiche nella subnet A e subnet B ad Accelerator2, Global Accelerator crea solo due interfacce di rete elastiche: una in SubnetA e una in SubnetB.

- Esempio 3: Se si aggiunge un ALB1 con interfacce di rete elastiche in SubNetA e SubNetB ad Accelerator1 e quindi si aggiunge un ALB2 con interfacce di rete elastiche in SubNetA e SubNetC ad Accelerator2, Global Accelerator crea tre interfacce di rete elastiche: una in SubNetA, una in SubNetB e una in SubNetC. L'elastic network interface in SubNetA fornisce traffico attivo sia per Accelerator1 che per Accelerator2.

Come illustrato nell'esempio 3, le interfacce di rete elastiche vengono riutilizzate tra acceleratori se gli endpoint nella stessa subnet sono posizionati dietro più acceleratori.

Le interfacce di rete elastiche logiche create da Global Accelerator non rappresentano un singolo host, un collo di bottiglia della velocità effettiva o un singolo punto di errore. Come altri servizi AWS che appaiono come un'unica elastic network interface in una zona di disponibilità o subnet, servizi come un gateway NAT (Network Address Translation) o un sistema di bilanciamento del carico di rete, Global Accelerator viene implementato come servizio a disponibilità elevata e scalabilità orizzontale.

Valutare il numero di subnet utilizzate dagli endpoint negli acceleratori per determinare il numero di interfacce di rete elastiche create da Global Accelerator. Prima di creare un acceleratore, assicurarsi di disporre di spazio sufficiente per gli indirizzi IP per le interfacce di rete elastiche richieste, almeno un indirizzo IP libero per ogni subnet pertinente. Se non si dispone di spazio sufficiente per gli indirizzi IP, è necessario creare o utilizzare una subnet che disponga di spazio sufficiente per gli indirizzi IP disponibili per l'Application Load Balancer e le interfacce di rete elastiche di Global Accelerator associate.

Quando Global Accelerator determina che un'elastic network interface non viene utilizzata da nessuno degli endpoint negli acceleratori dell'account, Global Accelerator elimina l'interfaccia.

Gruppi di sicurezza creati da Global Accelerator

Esaminare le informazioni e le procedure consigliate seguenti quando si lavora con Global Accelerator e gruppi di sicurezza.

- Global Accelerator crea gruppi di sicurezza associati alle interfacce di rete elastiche. Sebbene il sistema non ti impedisca di farlo, non dovresti modificare nessuna delle impostazioni del gruppo di protezione per questi gruppi.
- Global Accelerator non elimina i gruppi di sicurezza creati. Tuttavia, Global Accelerator elimina un'elastic network interface se non viene utilizzata da nessuno degli endpoint negli acceleratori dell'account.

- È possibile utilizzare i gruppi di sicurezza creati da Global Accelerator come gruppo di origine in altri gruppi di sicurezza mantenuti, ma Global Accelerator inoltra solo il traffico alle destinazioni specificate nel VPC.
- Se si modificano le regole del gruppo di sicurezza create da Global Accelerator, l'endpoint potrebbe diventare non integro. In tal caso, contattaAWS SupportPer ricevere assistenza.
- Global Accelerator crea un gruppo di sicurezza specifico per ogni VPC. Le interfacce di rete elastiche create per gli endpoint all'interno di un VPC specifico utilizzano lo stesso gruppo di protezione, indipendentemente dalla subnet associata a un'elastic network interface.

Regioni AWS supportate per la conservazione degli indirizzi IP client

È possibile abilitare la conservazione dell'indirizzo IP del client per AWS Global Accelerator nelle seguenti aree AWS.

Nome della regione	Regione
US East (Ohio)	`us-east-2`
US East (N. Virginia)	`us-east-1`
US West (N. California)	`us-west-1 (except AZ usw1-az2)`
US West (Oregon)	`us-west-2`
Africa (Cape Town)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`
Asia Pacific (Mumbai)	`ap-south-1`
Asia Pacific (Osaka)	`ap-northeast-3`
Asia Pacific (Singapore)	`ap-southeast-1`
Asia Pacific (Sydney)	`ap-southeast-2`

Nome della regione	Regione
Asia Pacific (Tokyo)	`ap-northeast-1 (except AZ apne1-az3)`
Asia Pacific (Seoul)	`ap-northeast-2`
Canada (Central)	`ca-central-1 (except AZ cac1-az3)`
Europe (Frankfurt)	`eu-central-1`
Europe (Ireland)	`eu-west-1`
Europe (London)	`eu-west-2`
Europe (Milan)	`eu-south-1`
Europe (Paris)	`eu-west-3`
Europe (Stockholm)	`eu-north-1`
Middle East (Bahrain)	`me-south-1`
South America (São Paulo)	`sa-east-1`

Registrazione e monitoraggio in AWS Global Accelerator

Per monitorare l'acceleratore in AWS CloudTrail Global Accelerator, analizzare i modelli di traffico e risolvere i problemi relativi agli ascoltatori e agli endpoint, puoi utilizzare i registri di flusso.

Argomenti

Logdi flusso in AWS Global Accelerator

I log di flusso ti consentono di acquisire informazioni sul traffico degli indirizzi IP da e per le interfacce di rete nell'acceleratore in AWS Global Accelerator. I dati dei log di flusso vengono pubblicati su Amazon S3, dove puoi recuperare e visualizzare i dati dopo aver creato un log di flusso.

I log di flusso possono essere utili per diverse attività. Ad esempio, puoi risolvere i problemi relativi a traffico specifico che non raggiunge un endpoint, che a sua volta consente di diagnosticare regole del gruppo di sicurezza eccessivamente restrittive. Puoi anche utilizzare i log di flusso come uno strumento di sicurezza per monitorare il traffico che raggiunge i tuoi endpoint.

Un record di log di flusso rappresenta un flusso di rete nel log di flusso. Ogni record acquisisce l'interfaccia di rete per un 5 tuple specifico, per una finestra di acquisizione specifica. Una 5 tuple è un set di cinque diversi valori che specificano l'origine, la destinazione E il protocollo di un flusso IP. La finestra di acquisizione è un periodo di tempo durante il quale il servizio dei log di flusso aggrega i dati prima di pubblicare i record del log di flusso. La finestra di acquisizione è di circa 10 secondi, ma può richiedere fino a 1 minuto.

I costi di CloudWatch Logs si applicano quando si utilizzano log di flusso, anche quando i log vengono pubblicati direttamente su Amazon S3. Per ulteriori informazioni, consultaConsegna dei registri a S3allePrezzi Amazon CloudWatch: .

Argomenti

- Sintassi dei record di log

Pubblicazione di log di flusso su Amazon S3

I log di flusso per AWS Global Accelerator vengono pubblicati su Amazon S3 in un bucket S3 esistente specificato. I record di log di flusso vengono pubblicati in una serie di oggetti file di log archiviati nel bucket.

Per creare un bucket Amazon S3 da utilizzare con i registri di flusso, consulta Crea un bucket nella Guida introduttiva di Amazon Simple Storage Service.

File dei log di flusso

I log di flusso raccolgono record di log, li consolidano in file di log e pubblicano i file di log nel bucket Amazon S3 a intervalli di cinque minuti. Ogni file di log contiene record di log di flusso per il traffico degli indirizzi 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 il limite delle dimensioni del file entro il periodo di cinque minuti, il log di flusso smette di aggiungervi record di log di flusso, lo pubblica nel bucket Amazon S3 e crea un nuovo file di log.

I file di log vengono salvati nel bucket Amazon S3; utilizzando una struttura di cartelle che è determinata dall'ID del log di flusso, dalla regione e dalla loro data di creazione. La struttura di cartelle del bucket utilizza il seguente formato:

```
s3-bucket_name/s3-bucket-prefix/AWSLogs/aws_account_id/globalaccelerator/region/yyyy/mm/dd/
```

Analogamente, il nome del file di log è determinato dall'ID del log di flusso, dalla regione e dalla data e ora di creazione. I nomi file utilizzano il formato seguente:

```
aws_account_id_globalaccelerator_accelerator_id_flow_log_id_timestamp_hash.log.gz
```

Tenere presente quanto segue sulla struttura dei nomi delle cartelle e dei file per i file di registro:

- Il timestamp utilizza il formato YYYYMMDDTHHmmZ.
- Se si specifica la barra (/) per il prefisso bucket S3, la struttura della cartella bucket del file di registro includerà una doppia barra (//), come la seguente:

```
s3-bucket_name//AWSLogs/aws_account_id
```

L'esempio seguente mostra la struttura di cartelle e il nome file di un file di log per un log di flusso creato dall'account AWS123456789012per un acceleratore con un ID di1234abcd-abcd-1234-abcd-1234abcdefgh, il 23 novembre 2018 alle 00:05 UTC:

```
my-s3-bucket/prefix1/AWSLogs/123456789012/globalaccelerator/us-
west-2/2018/11/23/123456789012_globalaccelerator_1234abcd-abcd-1234-
abcd-1234abcdefgh_20181123T0005Z_1fb1234.log.gz
```

Un singolo file di log del flusso contiene voci interfogliate con più record a 5 tuple, ovveroclient_ip,client_port,accelerator_ip,accelerator_port,protocol: . Per visualizzare tutti i file di log del flusso per l'acceleratore, cercare le voci aggregate dalaccelerator_idE la tuaaccount_id: .

Ruoli IAM per la pubblicazione di log di flusso in Amazon S3

Un'entità principale IAM, ad esempio un utente IAM, deve disporre di autorizzazioni sufficienti per pubblicare log di flusso nel bucket Amazon S3. La policy IAM deve includere le autorizzazioni seguenti:

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

```
            "Resource": "*"
        },
        {
            "Sid": "s3Perms",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy"
            ],
            "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 mediante una policy di accesso.

Se l'utente che crea il log di flusso è il proprietario del bucket, il servizio collega automaticamente la seguente policy al bucket per concedere al log di flusso l'autorizzazione per pubblicare log in esso:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/
*",
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}
```

Se l'utente che crea il log di flusso non è il proprietario del bucket, o non dispone delle autorizzazioni `GetBucketPolicy` e `PutBucketPolicy` per il bucket, la creazione del log di flusso non va a buon fine. In questo caso, il proprietario del bucket deve aggiungere manualmente la policy precedente al bucket e specificare l'ID account AWS dell'autore del log di flusso. Per ulteriori informazioni, consultaIn che modo aggiungere una policy del bucket S3?nellaGuida alle operazioni di base di Amazon Simple Storage Service: . Se il bucket riceve log di flusso da più account, aggiungi una voce elemento `Resource` alla dichiarazione di policy `AWSLogDeliveryWrite` per ogni account.

Ad esempio, i criteri bucket seguenti consentono agli account AWS 123123123123 e 456456456456456456 di pubblicare log di flusso in una cartella denominata`flow-logs`In un bucket denominato`log-bucket`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": [
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/123123123123/*",
             "arn:aws:s3:::log-bucket/flow-logs/AWSLogs/456456456456/*"
             ],
            "Condition": {"StringEquals": {"s3:x-amz-acl": "bucket-owner-full-
control"}}
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::log-bucket"
        }
    ]
}
```

> **Note**
>
> Ti consigliamo di concedere laAWSLogDeliveryAclCheckeAWSLogDeliveryWriteLe autorizzazioni per l'entità principale del servizio di recapito log anziché singoli ARN di account AWS.

Policy chiave CMK necessarie per l'utilizzo con i bucket SSE/KMS

Se si abilita la crittografia lato server per il bucket Amazon S3 utilizzando chiavi gestite da AWS KMS (SSE-KMS) con una Customer Master Key (CMK) gestita dal cliente, è necessario aggiungere la seguente policy chiave per la CMK in modo che i log di flusso possano scrivere file di log nel bucket:

```
{
    "Sid": "Allow AWS Global Accelerator Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "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, consultaPanoramica delle liste di controllo accessi (ACL)nellaGuida alle operazioni di base di Amazon Simple Storage Service: .

Abilita i log di flusso di pubblicazione su Amazon S3

Per abilitare i log di flusso in AWS Global Accelerator, attenersi alla procedura descritta in questa procedura.

Per abilitare i log di flusso in AWS Global Accelerator

1. Crea un bucket Amazon S3 per i log di flusso nel tuo account AWS.
2. Aggiungere il criterio IAM richiesto per l'utente AWS che sta abilitando i registri di flusso. Per ulteriori informazioni, consulta Ruoli IAM per la pubblicazione di log di flusso in Amazon S3.
3. Eseguire il seguente comando AWS CLI, con il nome del bucket Amazon S3 e il prefisso che si desidera utilizzare per i file di registro:

```
aws globalaccelerator update-accelerator-attributes
       --accelerator-arn
 arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-
abcd-1234abcdefgh
       --region us-west-2
       --flow-logs-enabled
       --flow-logs-s3-bucket s3-bucket-name
       --flow-logs-s3-prefix s3-bucket-prefix
```

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.

Tempi di recapito file di log

AWS Global Accelerator fornisce i file di log dell'acceleratore configurato più volte ogni ora. In generale, un file di log contiene informazioni sulle richieste che l'acceleratore ha ricevuto durante un determinato periodo di tempo. Global Accelerator fornisce generalmente al tuo bucket Amazon S3 il file di log corrispondente a quel periodo nell'ora che segue gli eventi che appaiono nel log. Alcune o tutte le voci di file di log relative a un periodo di tempo possono talvolta essere ritardate fino a 24 ore. Quando le voci di log sono ritardate, Global Accelerator le salva in un file di log il cui nome di file include la data e l'ora del periodo in cui si sono verificate le richieste e non la data e l'ora in cui il file è stato recapitato.

Quando crei un file di log, Global Accelerator consolida le informazioni per l'acceleratore da tutte le edge location che hanno ricevuto richieste durante il periodo di tempo coperto dal file di log.

Global Accelerator inizia a consegnare file di log in modo affidabile all'incirca quattro ore dopo l'attivazione della registrazione. È possibile che tu ottenga alcuni file di log prima di quel momento.

> **Note**
>
> Se nessun utente si connette al tuo acceleratore durante il periodo di tempo, non riceverai alcun file di log per quel periodo.

Sintassi dei record di log

Un record di log di flusso è una stringa separata da spazi avente il seguente formato:

```
<version> <aws_account_id> <accelerator_id> <client_ip>
<client_port> <accelerator_ip> <accelerator_port> <endpoint_ip>
<endpoint_port> <protocol> <ip_address_type> <packets>
<bytes> <start_time> <end_time> <action> <log-status>
<globalaccelerator_source_ip> <globalaccelerator_source_port>
<endpoint_region> <globalaccelerator_region> <direction> <vpc_id>
```

Il formato versione 1.0 non include l'identificatore VPC,`vpc_id`: . Il formato della versione 2.0, che include`vpc_id`, viene generato quando Global Accelerator invia il traffico a un endpoint con conservazione dell'indirizzo IP del client.

La tabella di seguito descrive i campi di un record di log di flusso.

Campo	Descrizione
`version`	La versione dei registri di flusso.
`aws_account_id`	ID account di AWS per il log di flusso.
`accelerator_id`	L'ID dell'acceleratore per cui viene registrato il traffico.
`client_ip`	L'indirizzo IPv4 di origine.
`client_port`	La porta di origine.
`accelerator_ip`	L'indirizzo IP dell'acceleratore.

Campo	Descrizione
`accelerator_port`	Il porto dell'acceleratore.
`endpoint_ip`	L'indirizzo IP di destinazione del traffico.
`endpoint_port`	La porta di destinazione del traffico.
`protocol`	Il numero di protocollo IANA del traffico. Per ulteriori informazioni, consulta la sezione relativa ai numeri di protocollo Internet assegnati.
`ip_address_type`	IPv4.
`packets`	Il numero di pacchetti trasferiti durante la finestra di acquisizione.
`bytes`	Il numero di byte trasferiti durante la finestra di acquisizione.
`start_time`	L'ora, in secondi Unix, dell'inizio della finestra di acquisizione.
`end_time`	L'ora, in secondi Unix, della fine della finestra di acquisizione.
`action`	L'operazione associata al traffico: • `ACCEPT`: il traffico registrato è stato consentito dai gruppi di sicurezza o dalle liste di controllo accessi di rete. Il valore è attualmente sempre ACCEPT.

Campo	Descrizione
`log-status`	Lo stato di registrazione del log di flusso: • `OK`: dati registrati normalmente nelle destinazioni scelte. • `NODATA`: nessun traffico di rete da o per l'interfaccia di rete durante la finestra di acquisizione. • `SKIPDATA`: alcuni record del log di flusso sono stati ignorati durante la finestra di acquisizione. Ciò può essere causato da un vincolo di capacità interna o da un errore interno.
`globalaccelerator_source_ip`	Indirizzo IP utilizzato dall'interfaccia di rete Global Accelerator.
`globalaccelerator_source_port`	La porta utilizzata dall'interfaccia di rete Global Accelerator.
`endpoint_region`	La regione AWS in cui si trova l'endpoint.
`globalaccelerator_region`	La edge location (punto di presenza) che ha servito la richiesta. Ogni edge location ha un codice di tre lettere e un numero assegnato arbitrariamente, ad esempio DFW3. Il codice di tre lettere di solito corrisponde al codice aeroportuale della International Air Transport Association per l'aeroporto vicino alla edge location. (Queste abbreviazioni potrebbero cambiare in futuro).
`direction`	La direzione del traffico. Indica il traffico che entra nella rete Global Accelerator (`INGRESS`) o tornare al client (`EGRESS`).
`vpc_id`	L'identificatore VPC. Incluso nei log di flusso versione 2.0 quando Global Accelerator invia il traffico a un endpoint con conservazione dell'indirizzo IP del client.

Se un campo non è applicabile per un record specifico, il record visualizza un simbolo «-» per tale voce.

Utilizzo di Amazon CloudWatch con AWS Global Accelerator

AWS Global Accelerator pubblica punti dati su Amazon CloudWatch per i tuoi acceleratori. CloudWatch ti consente di recuperare le statistiche su quei punti di dati come set ordinato di dati di serie temporali, i cosiddettiParametri: . Pensa a una metrica come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. Ad esempio, puoi monitorare il traffico tramite un acceleratore in un periodo di tempo specificato. A ogni punto di dati sono associati un timestamp 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.

Global Accelerator segnala i parametri a CloudWatch solo quando le richieste passano attraverso l'acceleratore. Se le richieste passano attraverso l'acceleratore, Global Accelerator ne misura e invia i parametri a intervalli di 60 secondi. Se per l'acceleratore non passano richieste o in assenza di dati per un parametro, questa non viene segnalata.

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

Indice

Metriche di Global Accelerator

Lo spazio dei nomi `AWS/GlobalAccelerator` include i parametri descritti di seguito.

Parametro	Descrizione
`NewFlowCount`	Il numero totale di nuovi flussi (o connessioni) TCP e UDP stabiliti da client a endpoint nel periodo di tempo.

Parametro	Descrizione
	Criteri di segnalazione: Vi è un valore diverso da zero. Statistiche: L'unica statistica utile è`Sum`: . Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`
`ProcessedBytesIn`	Il numero totale di byte in ingresso elaborati dall'acceleratore, incluse le intestazioni TCP/IP. Questo conteggio include tutto il traffico verso gli endpoint. Criteri di segnalazione: Vi è un valore diverso da zero. Statistiche: L'unica statistica utile è`Sum`: . Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Parametro	Descrizione
`ProcessedBytesOut`	Il numero totale di byte in uscita elaborati dall'acceleratore, incluse le intestazioni TCP/IP. Questo conteggio include il traffico proveniente da endpoint, meno il traffico di controllo dello stato. Criteri di segnalazione: Vi è un valore diverso da zero. Statistiche: L'unica statistica utile è`Sum`: . Dimensions • `Accelerator` • `Accelerator, Listener` • `Accelerator, Listener, EndpointGroup` • `Accelerator, SourceRegion` • `Accelerator, DestinationEdge` • `Accelerator, TransportProtocol` • `Accelerator, AcceleratorIPAddress`

Dimensioni dei parametri per gli acceleratori

Per filtrare i parametri relativi all'acceleratore, usa le seguenti dimensioni.

Dimensione	Descrizione
`Accelerator`	Filtra i dati delle metriche per acceleratore. Specificare l'acceleratore in base all'ID dell'acceleratore (la parte finale dell'acceleratore ARN). Ad esempio, se l'ARN è`arn:aws:globalaccelerator::012345678901:accelerator/1234abcd-abcd-1234-abcd-1234abcdefgh` , occorre fornire le seguenti informazioni:**`1234abcd-abcd-1234-abcd-1234abcdefgh`** : .
`Listener`	Filtra i dati delle metriche per listener. Specificare il listener in base all'ID del listener (la parte finale del listener ARN). Ad esempio, se l'ARN è`arn:aws:globalaccelerator::012345678901:accel`

Dimensione	Descrizione
	`erator/1234abcd-abcd-1234-abcd-1234abcdefgh/listener/0123wxyz` , occorre fornire le seguenti informazioni:**`0123wxyz`**: .
`EndpointGroup`	Filtra i dati delle metriche per gruppo di endpoint. Specificare il gruppo di endpoint in base alla regione AWS, ad esempio**`us-east-1`** (tutti minuscoli).
`SourceRegion`	Filtra i dati delle metriche per area di origine, ovvero l'area geografica delle regioni AWS in cui sono in esecuzione gli endpoint dell'applicazione. L'area di origine è una delle seguenti informazioni: • NA — Stati Uniti e Canada • EU — Europa • AP — Asia Pacifico* • KR — Corea del Sud • IN — India • AU — Australia • ME — Medio Oriente Oriente Oriente • SA — Sud America Sud America *Esclusi Corea del Sud e India

Dimensione	Descrizione
`DestinationEdge`	Filtra i dati delle metriche per bordo di destinazione, ovvero l'area geografica delle posizioni perimetrali AWS che servono il traffico client. Il bordo di destinazione è uno dei seguenti valori: • NA — Stati Uniti e Canada • EU — Europa • AP — Asia Pacifico* • KR — Corea del Sud • IN — India • AU — Australia • ME — Medio Oriente Oriente Oriente • SA — Sud America Sud America • ZA — Sudafrica *Esclusi Corea del Sud e India
`Transport Protocol`	Filtra i dati delle metriche per protocollo di trasporto: UDP o TCP.
`AcceleratorIPAddress`	Filtra i dati delle metriche per indirizzo IP dell'acceleratore, ovvero uno degli indirizzi IP statici assegnati a un acceleratore.

Statistiche sulle metriche di Global Accelerator

CloudWatch fornisce statistiche basate sui punti di dati delle metriche pubblicati da Global Accelerator. Le statistiche sono aggregazioni di dati delle metriche in un periodo di tempo specificato. Quando richiedi le statistiche, il flusso di dati restituito viene identificato dal nome e dalla dimensione del parametro. Una dimensione è una coppia nome/valore che identifica un parametro in modo univoco. Ad esempio, è possibile richiedere i byte elaborati per un acceleratore in cui i byte vengono serviti da posizioni edge AWS in Europa (edge di destinazione è «EU»).

Di seguito sono riportati esempi di combinazioni metrice/quota che potrebbero essere utili:

- Visualizzare la quantità di traffico servita (ad esempio ProcessedBytesOut) da ciascuno dei due indirizzi IP dell'acceleratore per verificare che la configurazione DNS sia corretta.
- Visualizzare la distribuzione geografica del traffico utente e monitorare la quantità di esso è locale (ad esempio, dal Nord America al Nord America) o globale (ad esempio, Australia o India al Nord America). Per determinarlo, visualizzare le metriche ProcessedBytesIn o ProcessedBytesOut con le dimensioni DestinationEdge e SourceRegion impostate su valori specifici.

Visualizza le metriche di CloudWatch per i tuoi acceleratori

Puoi visualizzare le metriche di CloudWatch per i tuoi acceleratori usando la console CloudWatch o l'interfaccia della CLI AWS. Nella console, i parametri vengono visualizzati come grafici di monitoraggio. I grafici di monitoraggio mostrano punti di dati solo se l'acceleratore è attivo e riceve richieste.

Devi visualizzare le metriche di CloudWatch per Global Accelerator nella regione Stati Uniti occidentali (Oregon), sia nella console che quando usi l'interfaccia della CLI AWS. Quando si utilizza l'interfaccia della riga di comando AWS, specificare l'area Stati Uniti occidentali (Oregon) per il comando includendo il parametro seguente:`--region us-west-2`: .

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la console CloudWatch all'indirizzohttps://us-west-2.console.aws.amazon.com/cloudwatch/home?region=us-west-2: .
2. Nel riquadro di navigazione, selezionare Metrics (Parametri).
3. Selezionare ilGlobalAcceleratorSpazio dei nomi.
4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, digitarne il nome nel campo di ricerca.

Per visualizzare i parametri usando la AWS CLI

Utilizza il seguente comando list-metrics per elencare i parametri disponibili:

```
aws cloudwatch list-metrics --namespace AWS/GlobalAccelerator --region us-west-2
```

Per ottenere le statistiche su un parametro utilizzando AWS CLI

Utilizza il parametro seguenteget-metric-statisticsPer ottenere le statistiche su un determinato parametro e dimensione. Ricorda che CloudWatch tratta ogni combinazione univoca di dimensioni come un parametro distinto. Non puoi recuperare le statistiche usando combinazioni di dimensioni che non siano state specificamente pubblicate. Occorre specificare le stesse dimensioni utilizzate al momento della creazione dei parametri.

Nell'esempio seguente vengono elencati i byte totali elaborati, al minuto, per l'acceleratore che serve dal bordo di destinazione Nord America (NA).

```
aws cloudwatch get-metric-statistics --namespace AWS/GlobalAccelerator \
--metric-name ProcessedBytesIn \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=Accelerator,Value=1234abcd-abcd-1234-abcd-1234abcdefgh
 Name=DestinationEdge,Value=NA \
--start-time 2019-12-18T20:00:00Z --end-time 2019-12-18T21:00:00Z
```

Il seguente è un esempio di output del comando:

```
{
    "Label": "ProcessedBytesIn",
    "Datapoints": [
        {
            "Timestamp": "2019-12-18T20:45:00Z",
            "Sum": 2410870.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:47:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:46:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:42:00Z",
            "Sum": 1560.0,
            "Unit": "Bytes"
        },
```

```
        {
            "Timestamp": "2019-12-18T20:48:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:43:00Z",
            "Sum": 1343.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:49:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "Timestamp": "2019-12-18T20:44:00Z",
            "Sum": 35791560.0,
            "Unit": "Bytes"
        }
    ]
}
```

Utilizzo di AWS CloudTrail per registrare le chiamate API AWS Global Accelerator

AWS Global Accelerator è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, da un ruolo o da un servizio AWS in Global Accelerator. CloudTrail acquisisce tutte le chiamate API per Global Accelerator come eventi, tra cui le chiamate dalla console Global Accelerator e dalle chiamate di codice alle API di Global Accelerator. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per Global Accelerator. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi).

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

Informazioni su Global Accelerator in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in Global Accelerator, questa viene registrata in un evento CloudTrail insieme ad altri eventi di

servizio AWS inCronologia eventi: . È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi per Global Accelerator, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione di default, quando crei 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, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- 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 operazioni di Global Accelerator vengono registrate da CloudTrail e sono documentate nellaInformazioni di riferimento alle API di AWS Global Accelerator: . Ad esempio, le chiamate alle operazioni`CreateAccelerator`,`ListAccelerators`e`UpdateAccelerator`Le operazioni 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 IAM 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 l'argomento relativo all'elemento userIdentity di CloudTrail.

Informazioni sulle voci dei file di log di Global Accel

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 che specifichi. Ogni file di log CloudTrail formattato JSON può contenere una o più voci di log. Una voce di log rappresenta una singola richiesta proveniente da qualsiasi origine e include

informazioni sull'azione richiesta, inclusi eventuali parametri, la data e l'ora dell'azione e così via. Le voci di log non sono presentate in un particolare ordine e non costituiscono una traccia di stack ordinata delle chiamate API.

L'esempio seguente mostra una voce di log di CloudTrail che include queste operazioni di Global Accelerator.

- Elenco degli acceleratori per un account:`eventName`è`ListAccelerators`: .
- Creare un listener`eventName`è`CreateListener`: .
- Aggiornamento di un listener`eventName`è`UpdateListener`: .
- Descrizione di un listener`eventName`è`DescribeListener`: .
- Elenco dei listener per un account:`eventName`è`ListListeners`: .
- Eliminazione di un listener`eventName`è`DeleteListener`: .

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:14Z",
      "eventSource": "globalaccelerator.amazonaws.com",
```

```
      "eventName": "ListAccelerators",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "083cae81-28ab-4a66-862f-096e1example",
      "eventID": "fe8b1c13-8757-4c73-b842-fe2a3example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:04:49Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
        "portRanges": [
```

```
          {
            "fromPort": 80,
            "toPort": 80
          }
        ],
        "protocol": "TCP"
      },
      "responseElements": {
        "listener": {
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
      "eventID": "9cab44ef-0777-41e6-838f-f249example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
```

```
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:03:52Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "CreateAccelerator",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "name": "cloudTrailTest"
      },
      "responseElements": {
        "accelerator": {
          "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample",
          "name": "cloudTrailTest",
          "ipAddressType": "IPV4",
          "enabled": true,
          "ipSets": [
            {
              "ipFamily": "IPv4",
              "ipAddresses": [
                "192.0.2.213",
                "192.0.2.200"
              ]
            }
          ],
          "status": "IN_PROGRESS",
          "createdTime": "Nov 17, 2018 9:03:52 PM",
          "lastModifiedTime": "Nov 17, 2018 9:03:52 PM"
        }
      },
      "requestID": "d2d7f300-2f0b-4bda-aa2d-e67d6e4example",
      "eventID": "11f9a762-8c00-4fcc-80f9-848a29example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:27Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "UpdateListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
        "portRanges": [
          {
            "fromPort": 80,
            "toPort": 80
          },
          {
            "fromPort": 81,
            "toPort": 81
          }
        ]
      },
      "responseElements": {
        "listener": {
```

```
          "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234",
          "portRanges": [
            {
              "fromPort": 80,
              "toPort": 80
            },
            {
              "fromPort": 81,
              "toPort": 81
            }
          ],
          "protocol": "TCP",
          "clientAffinity": "NONE"
        }
      },
      "requestID": "008ef93c-b3a3-44b4-afb3-768example",
      "eventID": "85958f0d-63ff-4a2c-99e3-6ffbexample",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
```

```
      "eventTime": "2018-11-17T21:06:05Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DescribeListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
      },
      "responseElements": null,
      "requestID": "9980e368-82fa-40da-95a3-4b0example",
      "eventID": "885a02e9-2a60-4626-b1ba-57285example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:05:47Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "ListListeners",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
```

```
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "acceleratorArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample"
      },
      "responseElements": null,
      "requestID": "08e4b0f7-689b-4c84-af2d-47619example",
      "eventID": "f4fb8e41-ed21-404d-af9d-037c4example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/smithj",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2018-11-17T21:02:36Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "userName": "smithj"
          }
        }
      },
      "eventTime": "2018-11-17T21:06:24Z",
      "eventSource": "globalaccelerator.amazonaws.com",
      "eventName": "DeleteListener",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "aws-cli/1.16.34 Python/2.7.10 Darwin/16.7.0 botocore/1.12.24",
      "requestParameters": {
        "listenerArn":
 "arn:aws:globalaccelerator::111122223333:accelerator/0339bfd6-13bc-4d45-
a114-5d7fexample/listener/abcde1234"
```

```
      },
      "responseElements": null,
      "requestID": "04d37bf9-3e50-41d9-9932-6112example",
      "eventID": "afedb874-2e21-4ada-b1b0-2ddb2example",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Sicurezza AWS Global Accelerator

La sicurezza nel cloud è per AWS una priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce, inoltre, i servizi che puoi utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti nell'ambito dei programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Global Accelerator, consultaServizi AWS coperti dal programma di compliance: .
- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal servizio AWS utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Global Accelerator. I seguenti argomenti illustrano come configurare l'acceleratore globale per soddisfare gli obiettivi di sicurezza.

Argomenti

Identity and Access Management per AWS Global Accelerator

AWS Identity and Access Management (IAM) è un servizio AWS che permette agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS, incluse le risorse AWS Global Accelerator. Gli amministratori utilizzano IAM per controllare chi èAutenticazione(effettuato l'accesso)

eautorizzato(dispone delle autorizzazioni) per utilizzare le risorse di Global Accelerator. IAM è una caratteristica inclusa nel tuo account AWS senza costi aggiuntivi.

> **Important**
>
> Se non hai familiarità con IAM, consulta le informazioni introduttive in questa pagina e quindi consultaNozioni di base su IAM: . Facoltativamente, puoi fare riferimento agli argomenti, per ulteriori informazioni sull'autenticazione e sul controllo dell'accesso, consultaChe cos'è l'autenticazione?,Cos'è il controllo degli accessi?, eChe cosa sono le policy?: .

Argomenti

- Nozioni e termini
- Autorizzazioni necessarie per l'accesso alla console, la gestione dell'autenticazione e il controllo dell'accesso
- Capire come Global Accelerator funziona con IAM
- Risoluzione dei problemi di autenticazione e controllo degli accessi

Nozioni e termini

Autenticazione: per effettuare l'accesso ad AWS, devi utilizzare una delle seguenti credenziali: credenziali utente root (non consigliato), credenziali utente IAM o credenziali temporanee mediante i ruoli IAM. Per ulteriori informazioni su queste entità, consulta Che cos'è l'autenticazione?.

Controllo degli accessi: gli amministratori AWS utilizzano le policy per controllare l'accesso alle risorse AWS, ad esempio gli acceleratori in Global Accelerator. Per ulteriori informazioni, consulta Cos'è il controllo degli accessi? e Che cosa sono le policy?.

> **Important**
>
> Tutte le risorse in un account sono di proprietà di tale account, indipendentemente da chi le ha create. Per creare una risorsa, è necessario disporre dell'accesso. Tuttavia, il solo fatto di avere creato una risorsa non significa che automaticamente si dispone dell'accesso completo a tale risorsa. Un amministratore deve concedere in modo esplicito le autorizzazioni per ogni operazione che si desidera eseguire. L'amministratore può inoltre revocare tali autorizzazioni in qualsiasi momento.

Per ulteriori informazioni sulle nozioni di base relative al funzionamento di IAM, consulta i seguenti termini:

Risorse

I servizi AWS, ad esempio Global Accelerator e IAM, in genere includono oggetti denominati risorse. Nella maggior parte dei casi, è possibile creare, gestire ed eliminare queste risorse dal servizio. Le risorse IAM includono utenti, gruppi, ruoli e policy:

Utenti

Un utente IAM rappresenta la persona o l'applicazione che utilizza le credenziali per interagire con AWS. Un utente è composto da un nome, una password per effettuare l'accesso alla Console di gestione AWS e fino a due chiavi di accesso che possono essere utilizzate con l'interfaccia a riga di comando AWS o l'API AWS.

Gruppi

Un gruppo IAM è un insieme di utenti IAM. Gli amministratori possono utilizzare gruppi per specificare le autorizzazioni per gli utenti membri. Ciò semplifica la gestione delle autorizzazioni per più utenti per un amministratore.

Roles

A un ruolo IAM non sono associate credenziali a lungo termine (password o chiavi di accesso). Un ruolo può essere assunto da qualsiasi utente che lo richieda e che disponga delle autorizzazioni. Un utente IAM può assumere un ruolo per ottenere temporaneamente autorizzazioni diverse per un'attività specifica. Gli utenti federati possono assumere un ruolo utilizzando un provider di identità esterno mappato al ruolo. Alcuni servizi AWS possono assumere unRuolo del servizioPer accedere alle risorse AWS per conto tuo.

Policies

Le policy sono documenti JSON che definiscono le autorizzazioni per l'oggetto a cui sono collegate. AWS SupportPolicy basate su identitàCollegare alle identità (utenti, gruppi o ruoli). Alcuni servizi AWS consentono di allegarePolicy basate su risorseAlle risorse per controllare le operazioni che un principale (persona o applicazione) può eseguire su tale risorsa. Global Accelerator non supporta policy basate su risorse.

Identità

Le identità sono risorse IAM per le quali è possibile definire le autorizzazioni. Questi includono utenti, gruppi e ruoli.

Entità

Le entità sono risorse IAM che vengono utilizzate per l'autenticazione. Questi includono utenti e ruoli.

Principali

In AWS, un principale è una persona o un'applicazione che utilizza un'entità per accedere ed effettuare richieste ad AWS. Un principale può utilizzare AWS Management Console, l'interfaccia a riga di comando AWS oppure l'API AWS per eseguire un'operazione, ad esempio l'eliminazione di un acceleratore. Ciò crea una richiesta per tale operazione. La richiesta specifica l'operazione, la risorsa, il principale, l'account principale e qualsiasi altra informazione relativa alla richiesta. Tutte queste informazioni forniscono AWS concontextPer la tua richiesta. AWS controlla tutte le policy applicabili al contesto della richiesta. AWS autorizza la richiesta solo se ogni parte della richiesta è autorizzata in base alla policy.

Per visualizzare un diagramma del processo di autenticazione e controllo dell'accesso, consultaIntroduzione al funzionamento di IAMnellaGuida per l'utente di IAM: . Per ulteriori informazioni su come AWS determina se una richiesta è consentita, consultaLogica di valutazione delle policynellaGuida per l'utente di IAM: .

Autorizzazioni necessarie per l'accesso alla console, la gestione dell'autenticazione e il controllo dell'accesso

Per utilizzare Global Accelerator o per gestire l'autorizzazione e il controllo dell'accesso per sé stessi o gli altri utenti, è necessario disporre delle autorizzazioni corrette.

Autorizzazioni necessarie per creare un acceleratore globale

Per creare un acceleratore AWS Global Accelerator, gli utenti devono disporre dell'autorizzazione per creare ruoli collegati al servizio associati a Global Accelerator.

Per assicurarsi che gli utenti dispongano delle autorizzazioni corrette per creare acceleratori in Global Accelerator, allegare all'utente un criterio come il seguente.

> **Note**
>
> Se crei una policy di autorizzazioni basate sulle identità più restrittiva, gli utenti con tale policy non potranno creare un acceleratore.

```
{
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "globalaccelerator.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*"
    }
```

Autorizzazioni necessarie per l'uso della console Global Accelerator

Per accedere alla console AWS Global Accelerator, è necessario disporre di un set minimo di autorizzazioni che consentono di elencare e visualizzare i dettagli relativi alle risorse Global Accelerator nell'account AWS. Se crei una policy di autorizzazioni basate su identità più restrittiva delle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità associate a tale policy.

Per garantire che tali entità possano continuare a usare la console Global Accelerator o le operazioni API, collega anche una delle seguenti policy gestite da AWS all'utente, come descritto in[Creazione di policy nella scheda JSON](#):

```
        GlobalAcceleratorReadOnlyAccess
        GlobalAcceleratorFullAccess
```

Allegare il primo criterio,`GlobalAcceleratorReadOnlyAccess`, se gli utenti devono solo visualizzare le informazioni nella console o effettuare chiamate all'interfaccia della riga di comando AWS o all'API che utilizzano`List*`o`Describe*`operazioni.

Allegare la seconda politica,`GlobalAcceleratorFullAccess`, agli utenti che devono creare o aggiornare gli acceleratori. La policy di accesso completo includeFULLautorizzazioni per Global Accelerator edescribeautorizzazioni per Amazon EC2 e Elastic Load Balancing.

> **Note**
>
> Se crei un criterio di autorizzazione basato sull'identità che non include le autorizzazioni richieste per Amazon EC2 e Elastic Load Balancing, gli utenti con tale criterio non saranno in grado di aggiungere risorse Amazon EC2 e Elastic Load Balancing agli acceleratori.

Di seguito è riportato il criterio di accesso completo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

Permessi necessari per la gestione dell'autenticazione

Per gestire le credenziali, ad esempio la password, le chiavi di accesso e i dispositivi con autenticazione a più fattori, l'amministratore deve concedere le autorizzazioni richieste. Per visualizzare la policy che include questi autorizzazioni, consulta Consente agli utenti di gestire in modo autonomo le proprie credenziali.

Un amministratore AWS deve disporre dell'accesso completo a IAM in modo da poter creare e gestire utenti, gruppi, ruoli e policy in IAM. È consigliabile utilizzare l'opzioneAdministratorAccessPolicy gestita da AWS che include l'accesso completo a tutti AWS. Questa policy non fornisce l'accesso alla console Billing and Cost Management AWS oppure consente attività che richiedono le credenziali utente radice dell'account AWS. Per ulteriori informazioni, consultaAttività AWS che richiedono credenziali utente root dell'account AWSnellaRiferimenti generali AWS: .

> **Warning**
>
> Solo un utente amministratore deve disporre dell'accesso completo ad AWS. Chiunque associato a questa policy dispone dell'autorizzazione per la gestione completa dell'autenticazione e del controllo dell'accesso e per la modifica di tutte le risorse in AWS. Per scoprire come creare questo utente, consulta Creare l'utente amministratore IAM.

Autorizzazioni necessarie per il controllo degli

Se l'amministratore fornisce le credenziali utente IAM, tali credenziali associano policy all'utente IAM per controllare le risorse a cui l'utente può accedere. Per visualizzare le policy collegate all'identità utente nella Console di gestione AWS, devi disporre delle seguenti autorizzazioni:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
            "Sid": "ListUsersViewGroupsAndPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

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

Se sono necessarie ulteriori autorizzazioni, chiedi all'amministratore di aggiornare le policy in modo da consentirti di accedere alle operazioni richieste.

Capire come Global Accelerator funziona con IAM

I servizi possono funzionare con IAM in diversi modi:

Operazioni

Global Accelerator supporta l'utilizzo di operazioni in una policy. Ciò consente a un amministratore di controllare se un'entità è in grado di completare un'operazione in Global Accelerator. Ad esempio, per consentire a un'entità di chiamare il metodo`GetPolicy`Operazione API AWS per visualizzare una policy, un amministratore deve collegare una policy che consente la`iam:GetPolicy`Operazione .

Il seguente criterio di esempio consente a un utente di eseguire la`CreateAccelerator`per creare a livello di codice un acceleratore per il tuo account AWS:

```
{
   "Version": "2018-08-08",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "globalaccelerator:CreateAccelerator"
         ],
         "Resource":"*"
      }
   ]
}
```

Autorizzazioni a livello di risorsa

Global Accelerator supporta le autorizzazioni a livello di risorsa. Le autorizzazioni a livello di risorsa consentono di utilizzare gli ARN per specificare singole risorse nella policy.

Policy basate su risorse

Global Accelerator non supporta policy basate su risorse. Con policy basate sulle risorse, è possibile collegare una policy a una risorsa all'interno del servizio. Le policy basate su risorse includono un`Principal`Elemento per specificare quali identità IAM possono accedere a tale risorsa.

Autorizzazione basata tag

Global Accelerator supporta i tag basati sulle autorizzazioni. Questa caratteristica consente di usare i tag delle risorse nella condizione di una policy.

Credenziali temporanee

Global Accelerator supporta le credenziali temporanee. Con credenziali temporanee, puoi effettuare l'accesso utilizzando la federazione, assumere un ruolo IAM o assumere un ruolo multi-account. Per ottenere le credenziali di sicurezza temporanee, eseguire una chiamata a operazioni API AWS STS come`AssumeRole`o`GetFederationToken`: .

Ruoli collegati ai servizi

Global Accelerator supporta ruoli collegati ai servizi. Questa caratteristica consente a un servizio di assumere un ruolo collegato al servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'operazione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Ruoli dei servizi

Global Accelerator non supporta ruoli di servizio. Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'operazione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questa operazione potrebbe pregiudicare la funzionalità del servizio.

Risoluzione dei problemi di autenticazione e controllo degli accessi

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di IAM.

Argomenti

Non sono autorizzato a eseguire un'operazione in Global Accelerator

Se la Console di gestione AWS indica che non sei autorizzato a eseguire un'operazione, devi contattare l'amministratore e richiedere il nome utente e la password.

L'esempio seguente si verifica quando un utente IAM denominato`my-user-name`tenta di utilizzare la console per eseguire l'operazione`globalaccelerator:CreateAccelerator`ma non ha autorizzazioni:

```
User: arn:aws:iam::123456789012:user/my-user-name is not authorized to perform: aws-globalaccelerator:CreateAccelerator on resource: my-example-accelerator
```

In questo caso, devi contattare l'amministratore per l'aggiornamento delle policy in modo che venga autorizzato l'accesso allamy`-example-accelerator`utilizzando l'opzione`aws-globalaccelerator:CreateAccelerator`Operazione .

Sono un amministratore e desidero consentire ad altri utenti di accedere a Global Accelerator

Per consentire ad altri utenti di accedere ad Global Accelerator, devi creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che richiede l'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in Global Accelerator.

Per iniziare, consulta Nozioni di base su IAM.

Voglio capire IAM senza diventare un esperto

Per ulteriori informazioni su termini, concetti e procedure IAM di, consulta i seguenti argomenti:

- Che cos'è l'autenticazione?
- Cos'è il controllo degli accessi?
- Che cosa sono le policy?

Policy basate su tag

Durante la progettazione di policy IAM, potrebbe essere necessario impostare autorizzazioni granulari concedendo l'accesso a risorse specifiche. Poiché il numero di risorse che puoi gestire cresce, questa operazione diventa più difficile. Il tagging degli acceleratori e l'utilizzo di tag in condizioni di dichiarazione di policy possono semplificare questa attività. Puoi concedere l'accesso in blocco a qualsiasi acceleratore con un determinato tag. Quindi applicare ripetutamente questo tag a acceleratori pertinenti, quando crea l'acceleratore o aggiornando l'acceleratore in seguito.

> **Note**
>
> L'utilizzo di tag nelle condizioni è un modo per controllare l'accesso alle risorse e alle richieste. Per informazioni sul tagging in Global Accelerator, consultaTagging in AWS Global Accelerator: .

I tag possono essere collegati a una risorsa o trasferiti nella richiesta verso servizi che supportano il tagging. In Global Accelerator, solo gli acceleratori possono includere tag. Quando si crea una policy IAM, è possibile utilizzare le chiavi di condizione di tag per controllare:

- Quali utenti possono eseguire operazioni su un acceleratore in base ai tag di cui dispongono già.
- Quali tag possono essere passati in una richiesta di operazione;
- Se delle chiavi di tag specifiche possono essere utilizzate in una richiesta.

Per la sintassi completa e la semantica delle chiavi delle condizioni dei tag, consultaControllo dell'accesso tramite tag IAMnellaGuida per l'utente di IAM: .

Ad esempio, l'acceleratore globale`GlobalAcceleratorFullAccess`La policy utente gestita fornisce agli utenti autorizzazioni illimitate per eseguire qualsiasi operazione di Global Accelerator su qualsiasi risorsa. La policy seguente limita questa capacità e nega agli utenti non autorizzati l'autorizzazione a eseguire qualsiasi operazione di Global Accelerator su qualsiasiProduzioneAcceleratori L'amministratore di un cliente deve collegare questa policy IAM a utenti IAM non autorizzati oltre alla policy gestita dall'utente.

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

```
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:RequestTag/stage":"prod"
            }
         }
      },
      {
         "Effect":"Deny",
         "Action":"*",
         "Resource":"*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:ResourceTag/stage":"prod"
            }
         }
      }
   ]
}
```

Ruolo collegato ai servizi per Global Accelerator

AWS Global Accelerator utilizza AWS Identity and Access Management (IAM)Ruolo collegato ai servizi: . Un ruolo collegato ai servizi è un tipo univoco di ruolo IAM collegato direttamente a un servizio. I ruoli collegati ai servizi sono definiti automaticamente dal servizio stesso e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Global Accelerator usa il seguente ruolo collegato ai servizi IAM:

- AWSServiceroleForGlobalAccelerator: Global Accelerator utilizza questo ruolo per consentire a Global Accelerator di creare e gestire le risorse necessarie per la conservazione degli indirizzi IP del client.

Global Accelerator crea automaticamente un ruolo denominato AWSServiceroleForGlobalAccelerator quando il ruolo è richiesto per la prima volta per supportare un'operazione API Global Accelerator. Il ruolo AWSServiceroleForGlobalAccelerator consente a Global Accelerator di creare e gestire le risorse necessarie per la conservazione degli indirizzi IP del client. Questo ruolo è necessario per l'utilizzo degli acceleratori in Global Accelerator. L'ARN per il ruolo AWSServiceRoleForGlobalAccelerator è simile al seguente:

`arn:aws:iam::123456789012:role/aws-service-role/globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator`

Un ruolo collegato ai servizi semplifica la configurazione e l'utilizzo di Global Accelerator perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Global Accelerator definisce le autorizzazioni del relativo ruolo collegato ai servizi; solo Global Accelerator può assumere i propri ruoli. Le autorizzazioni definite includono policy di trust e di autorizzazioni. Queste ultime non possono essere collegate a nessun'altra entità IAM.

È necessario rimuovere qualsiasi risorsa associata a Global Accelerator prima di eliminare il ruolo collegato ai servizi. In questo modo è possibile proteggere le proprie risorse Global Accelerator assicurandosi che non venga rimosso un ruolo collegato ai servizi ancora necessario per accedere alle risorse attive.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione relativa ai servizi AWS che funzionano con IAM e cerca i servizi che nella colonna Service-Linked Role (Ruolo associato ai servizi) riportano Yes (Sì).

Autorizzazioni del ruolo collegato ai servizi per Global Accelerator

Global Accelerator usa un ruolo collegato ai servizi denominatoAWSServiceroleForGlobalAccelerator: . Nelle sezioni seguenti vengono descritte le autorizzazioni per il ruolo.

Autorizzazioni del ruolo collegato ai servizi

Questo ruolo collegato ai servizi consente a Global Accelerator di gestire le interfacce di rete elastiche EC2 e i gruppi di sicurezza e di facilitare la diagnosi degli errori.

Il ruolo collegato ai servizi AWSServiceRoleForGlobalAccelerator considera attendibile il seguente servizio per assumere il ruolo:

- `globalaccelerator.amazonaws.com`

La policy delle autorizzazioni del ruolo consente a Global Accelerator di eseguire le seguenti operazioni sulle risorse specificate, come mostrato nel policy:

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSecurityGroup",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSServiceName": "GlobalAccelerator"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
```

```
    ]
}
```

Devi configurare le autorizzazioni per consentire a un'entità IAM (ad esempio un utente, un gruppo o un ruolo) di eliminare il ruolo collegato ai servizi di Global Accelerator. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi per Global Accelerator

Non devi creare manualmente il ruolo collegato al servizio per Global Accelerator. Il servizio crea automaticamente il ruolo la prima volta che si crea un acceleratore. Se rimuovi le risorse Global Accelerator ed elimina il ruolo collegato ai servizi, il servizio crea di nuovo automaticamente il ruolo quando crea un nuovo acceleratore.

Modifica del ruolo collegato ai servizi Global Accelerator

Global Accelerator non consente di modificare il ruolo collegato ai servizi AWSServiceRoleForGlobalAccelerator. Dopo aver creato un ruolo collegato ai servizi, non puoi modificare il nome del ruolo perché varie entità possono farvi riferimento. Puoi tuttavia modificare la descrizione di un ruolo 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 Global Accelerator

Se non devi più utilizzare Global Accelerator, ti suggeriamo di eliminare il ruolo collegato ai servizi. In questo modo non saranno più presenti entità non utilizzate che non vengono monitorate e gestite attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse di Global Accelerator nel tuo account prima di poter eliminare manualmente i ruoli.

Dopo aver disabilitato ed eliminato i tasti di scelta rapida, è possibile eliminare il ruolo collegato ai servizi. Per ulteriori informazioni sull'eliminazione degli acceleratori, consulta Creazione o aggiornamento di un acceleratore standard: .

> **Note**
>
> Se gli acceleratori sono stati disattivati ed eliminati ma Global Accelerator non ha completato l'aggiornamento, l'eliminazione del ruolo collegato ai servizi potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti la procedura di eliminazione dei ruoli collegati ai servizi.

Per eliminare manualmente il ruolo collegato al servizio AWSServiceRoleForGlobalAccelerator

1. Accedere alla Console di gestione AWS e aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione della console IAM scegliere Roles (Ruoli). Quindi, seleziona la casella di controllo accanto al nome del ruolo che desideri eliminare, non il nome o la riga stessa.
3. In operazioni Role (Ruolo) nella parte superiore della pagina, seleziona Delete (Elimina) ruolo.
4. Nella finestra di dialogo di conferma, controlla gli ultimi dati del servizio a cui è stato effettuato l'accesso, che mostrano quando ognuno dei ruoli selezionati ha effettuato l'accesso a un servizio AWS. In questo modo potrai verificare se il ruolo è attualmente attivo. Se desideri procedere, seleziona Yes, Delete (Sì, elimina) per richiedere l'eliminazione del ruolo collegato ai servizi.
5. Controlla le notifiche della console IAM per monitorare lo stato dell'eliminazione del ruolo collegato ai servizi. Poiché l'eliminazione del ruolo collegato ai servizi IAM è asincrona, una volta richiesta l'eliminazione del ruolo, il task di eliminazione può essere eseguito correttamente o meno. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Aggiornamenti al ruolo collegato al servizio Global Accelerator (un criterio gestito AWS)

Visualizzare i dettagli sugli aggiornamenti del ruolo collegato al servizio per da quando il servizio ha iniziato a tenere traccia di queste modifiche. Per avvisi automatici sulle modifiche apportate a questa pagina, iscriviti al feed RSS su AWS Global AcceleratorCronologia dei documenti(Certificato creato).

Modifica	Descrizione	Data
AWSServiceroleForGlobalAccelerator— Aggiornamento della policy	Global Accelerator ha aggiunto una nuova autorizzazione per aiutare Global Accelerator a diagnosticare gli errori. Global Accelerator utilizza`aec2:DescribeRegions` per determinare la regione AWS in cui si	18 maggio 2021

Modifica	Descrizione	Data
	trova un cliente, che può aiutare Global Accelerator a risolvere gli errori.	
Global Accelerator ha iniziato a tenere traccia	Global Accelerator ha iniziato a monitorare le modifiche per i suoi criteri gestiti AWS.	18 maggio 2021

Regioni supportate per i ruoli collegati ai servizi di Global Accelerator

Global Accelerator supporta l'utilizzo di ruoli collegati ai servizi in regioni AWS in cui è supportato Global Accelerator.

Per un elenco delle regioni AWS in cui sono attualmente supportati Global Accelerator e altri servizi, consulta laTabella AWS: .

Panoramica sull'accesso e sull'autenticazione

Se non si è esperti di IAM, leggere i seguenti argomenti per iniziare a utilizzare l'autorizzazione e l'accesso in AWS.

Argomenti

- Che cos'è l'autenticazione?
- Cos'è il controllo degli accessi?
- Che cosa sono le policy?
- Nozioni di base su IAM

Che cos'è l'autenticazione?

L'autenticazione è la procedura di accesso ad AWS utilizzando le credenziali.

> **Note**
>
> Per iniziare, puoi ignorare questa sezione. Innanzi tutto, leggi le informazioni introduttive disponibili nella paginaIdentity and Access Management per AWS Global Acceleratore quindi vedereNozioni di base su IAM: .

In quanto preside, devi essereAutenticazione(connesso a AWS) utilizzando un'entità (utente root, utente IAM o ruolo IAM) per inviare una richiesta ad AWS. Un utente IAM può disporre di credenziali a lungo termine, ad esempio un nome utente e una password oppure un set di chiavi di accesso. Quando assumi un ruolo IAM, riceverai le credenziali di sicurezza temporanee.

Per ottenere l'autenticazione dalla console di gestione AWS come utente, devi effettuare l'accesso con il tuo nome utente e la password. Per eseguire l'autenticazione tramite l'interfaccia a riga di comando AWS o l'API AWS, devi fornire la chiave di accesso e la chiave segreta o le credenziali temporanee. AWS fornisce SDK e strumenti CLI per firmare la richiesta in maniera crittografica utilizzando le credenziali. Se non utilizzi gli strumenti di AWS, devi firmare la richiesta personalmente. Indipendentemente dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account.

In qualità di principale, puoi accedere ad AWS utilizzando le seguenti entità (utenti o ruoli):

Utente root dell'account AWS

Quando crei un account AWS per la prima volta, inizi con una singola identità di accesso che ha accesso completo a tutti i servizi e le risorse AWS nell'account. Tale identità è detta utente root dell'account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Rispetta piuttosto la best practice di utilizzare l'utente root soltanto per creare il tuo primo utente &IAM;. Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio.

Utente IAM

UnUtente IAMè un'entità all'interno del tuo account AWS che dispone di autorizzazioni specifiche. Global Accelerator supportaSignature Version 4, un protocollo per l'autenticazione di richieste API in entrata. Per ulteriori informazioni sull'autenticazione delle richieste API, consulta la sezione relativa al processo di firma Signature Version 4 nella Guida di riferimento generale di AWS.

Ruolo IAM

UnRuolo IAML'identità IAM che puoi creare nell'account che ha le autorizzazioni specifiche. Un ruolo IAM è simile a un utente IAM, in quanto è un'identità AWS con policy di autorizzazioni che determinano ciò che l'identità può e non può fare in AWS. Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque. Inoltre, un ruolo non ha credenziali a lungo termine standard associate (password o chiavi di accesso). Tuttavia, quando assumi un ruolo, vengono fornite le credenziali di sicurezza provvisorie per la sessione del ruolo. I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

Accesso utente federato

Anziché creare un utente IAM, è possibile utilizzare identità preesistenti da AWS Directory Service, dalla directory utente aziendale o da un provider di identità Web (IdP). Questi sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando è richiesto l'accesso tramite un provider di identità. Per ulteriori informazioni sugli utenti federati, consultare la sezione relativa a Utenti e ruoli federati nella Guida per l'utente di IAM.

Autorizzazioni temporanee

Un utente IAM può assumere un ruolo temporaneamente per ottenere autorizzazioni diverse per un'attività specifica.

Accesso tra account

Puoi utilizzare un ruolo IAM per permettere a un principale attendibile con un account diverso di accedere alle risorse nel tuo account. I ruoli sono lo strumento principale per concedere l'accesso tra account. Tuttavia, alcuni servizi AWS consentono di collegare una policy direttamente a una risorsa, invece di utilizzare un ruolo come proxy. Global Accelerator non supporta queste policy basate su risorse. Per ulteriori informazioni sulla scelta se utilizzare un ruolo o una policy basata sulle risorse per consentire l'accesso multiaccount, consulta Controllo dell'accesso ai principale in un account diverso.

Accesso al servizio AWS

Un ruolo di servizio è unRuolo IAMche un servizio assume per eseguire operazioni a nome dell'utente. I ruoli del servizio forniscono l'accesso all'interno del tuo account e non possono essere utilizzati per concedere l'accesso ai servizi in altri account. Un amministratore di IAM può creare, modificare ed eliminare un ruolo di servizio da IAM. Per ulteriori informazioni, consultare la sezione Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS nella Guida per l'utente di IAM.

Applicazioni in esecuzione su Amazon EC2

È possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste AWS CLI o API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consultare Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Cos'è il controllo degli accessi?

Dopo aver effettuato l'accesso (dopo l'autenticazione) ad AWS, l'accesso alle risorse e alle operazioni AWS è disciplinato dalle policy. Il controllo dell'accesso è noto anche come autorizzazione.

> **Note**
>
> Per iniziare, puoi ignorare questa pagina. Innanzi tutto, leggi le informazioni introduttive disponibili nella paginaIdentity and Access Management per AWS Global Acceleratore quindi vedereNozioni di base su IAM: .

Durante l'autorizzazione, AWS utilizza i valori dellaRichiesta di contestoPer verificare le policy applicabili. Quindi, utilizza le policy per determinare se accettare o rifiutare la richiesta. La maggior parte delle policy viene memorizzata in AWS sotto forma di documenti JSON e specifica le autorizzazioni concesse o negate per le entità principali. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON , consulta Che cosa sono le policy?.

Le policy consentono a un amministratore di specificare quali utenti hanno accesso alle risorse AWS e quali operazioni possono effettuare su tali risorse. Ogni entità IAM (utente o ruolo) inizialmente non dispone di autorizzazioni. Ovvero, per impostazione predefinita, gli utenti non possono eseguire alcuna operazione, neppure visualizzare le proprie chiavi di accesso. Per autorizzare un utente a eseguire operazioni, un amministratore deve collegare una policy di autorizzazioni a tale utente. In alternativa, può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore associa le autorizzazioni a un gruppo, tali autorizzazioni verranno assegnate a tutti gli utenti del gruppo.

Anche se disponi di credenziali valide per autenticare le richieste, non puoi creare né accedere a risorse AWS Global Accelerator se un amministratore non ti concede le autorizzazioni necessarie. Ad esempio, devi disporre di autorizzazioni esplicite per creare un acceleratore AWS Global Accelerator.

Un amministratore può scrivere una policy per controllare l'accesso ai seguenti elementi:

- Principali— Consente di controllare quali sono le persone o le applicazioni che effettuano la richiesta (laprincipale) è permesso di fare.
- Identità IAMConsente di controllare a quali identità IAM (gruppi, utenti e ruoli) è possibile accedere e come.
- Policy IAMControllo degli utenti possono creare, modificare ed eliminare le policy gestite dai clienti e quali utenti possono collegare e scollegare tutte le policy gestite.
- Risorse AWSControllo dell'accesso alle risorse mediante una policy basata sulle identità o una policy basata sulle risorse.
- Account AWS: consente di controllare se una richiesta è consentita solo per i membri di un determinato account.

Controllo dell'accesso per le entità principali

Le policy di autorizzazioni controllano le operazioni che un principale può eseguire. Un amministratore deve collegare una policy di autorizzazioni basata sulle identità all'identità (utente, gruppo o ruolo) che fornisce le autorizzazioni. Le policy di autorizzazioni consentono o negano l'accesso ad AWS. Gli amministratori possono inoltre impostare un limite alle autorizzazioni per un'entità IAM (utente o ruolo) per definire il numero massimo di autorizzazioni che è possibile concedere all'entità. I limiti delle autorizzazioni sono una caratteristica avanzata di IAM. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le identità IAM nella Guida per l'utente di IAM.

Per ulteriori informazioni e per un esempio di come controllare l'accesso AWS per i principali, consultaControllo dell'accesso per le entità principalinellaGuida per l'utente di IAM: .

Controllo dell'accesso ad identità

Gli amministratori controllano le operazioni che è possibile eseguire su un'identità IAM (utente, gruppo o ruolo) mediante la creazione di una policy che limita le operazioni che possono essere eseguite su un'identità o chi può accedervi. Possono quindi collegare tale policy all'identità che fornisce le autorizzazioni.

Ad esempio, un amministratore potrebbe permetterti di reimpostare la password per tre utenti specifici. A tale scopo, l'amministratore collega una policy all'utente IAM che ti autorizza a reimpostare la password solo per te stesso e per gli utenti con l'ARN dei tre utenti specificati. In questo modo potrai reimpostare la password dei membri del tuo team ma non di altri utenti IAM.

Per ulteriori informazioni e per un esempio di utilizzo di una policy per controllare l'accesso AWS alle identità, consultaControllo dell'accesso ad identitànellaGuida per l'utente di IAM: .

Controllo dell'accesso ai criteri

Gli amministratori possono controllare quali utenti possono creare, modificare ed eliminare le policy gestite dai clienti e quali utenti possono collegare e scollegare tutte le policy gestite. Quando si utilizza una policy, è possibile visualizzare il riepilogo della policy che include un riepilogo del livello di accesso per ciascun servizio nella policy. AWS categorizza ogni azione di servizio in una delle quattroLivelli di accessoin base a ciò che ogni azione fa:`List`,`Read`,`Write`, oppure`Permissions management`: . È possibile utilizzare questi livelli di accesso per determinare quali operazioni includere nelle policy. Per ulteriori informazioni, consultaInformazioni sui riepiloghi dei livelli di accesso all'interno di una policynellaGuida per l'utente di IAM: .

> **Warning**
>
> È consigliabile limitare`Permissions Management`Autorizzazioni a livello di accesso nel tuo account. In caso contrario, i membri del tuo account potrebbero creare policy per se stessi con livelli di autorizzazioni superiori a quelli consentiti. Oppure possono creare altri utenti con accesso completo ad AWS.

Per ulteriori informazioni e per un esempio di come controllare l'accesso AWS alle policy, consultaControllo dell'accesso ai criterinellaGuida per l'utente di IAM: .

Controllo dell'accesso alle risorse

Gli amministratori possono controllare chi ha accesso alle risorse utilizzando una policy basata sulle identità o una policy basata sulle risorse. In una policy basata sulle identità si collega la policy a un'identità e si specifica a quali risorse può accedere tale identità. In una policy basata sulle risorse, si collega una policy alla risorsa che si desidera controllare. Nella policy, è necessario specificare quali entità principali possono accedere a tale risorsa.

Per ulteriori informazioni, consultaControllo dell'accesso alle risorsenellaGuida per l'utente di IAM: .

I creatori di risorse non dispongono automaticamente delle autorizzazioni

Tutte le risorse in un account sono di proprietà di tale account, indipendentemente da chi le ha create. L'utente root dell'account AWS è il proprietario dell'account e quindidispone dell'autorizzazione per eseguire qualsiasi operazione su qualsiasi risorsa inclusa nell'account.

> **Important**
>
> È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Seguire invece laBest practice sull'utilizzo dell'utente root solo per creare il tuo primo utente IAM: . Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio. Per visualizzare le attività che richiedono l'accesso come utente root, consultaAttività AWS che richiedono l'utente root: .

Alle entità (utenti o ruoli) nell'account AWS deve essere concesso l'accesso per creare una risorsa. Tuttavia, il solo fatto di poter creare una risorsa non significa che automaticamente si dispone dell'accesso completo a tale risorsa. Gli amministratori devono concedere esplicitamente le autorizzazioni per ogni operazione. Inoltre, gli amministratori possono revocare le autorizzazioni in qualsiasi momento, a condizione che dispongano dell'accesso per la gestione di utenti e autorizzazioni del ruolo.

Controllo dell'accesso ai principale in un account diverso

Gli amministratori possono utilizzare policy basate su risorse AWS, ruoli multiaccount IAM o il servizio AWS Organizations per consentire ai principali in un altro account di accedere alle risorse nell'account corrente.

Per alcuni servizi AWS Services, gli amministratori possono concedere l'accesso per più account alle risorse. A tale scopo, un amministratore collega una policy direttamente alla risorsa da condividere, anziché utilizzare un ruolo come proxy. Se il servizio supporta questo tipo di policy, anche la risorsa condivisa dall'amministratore deve supportare le policy basate sulle risorse. A differenza di una policy basata sugli utenti, una policy basata sulle risorse specifica quali utenti (sotto forma di elenco di numeri ID account AWS) possono accedere a tale risorsa. Global Accelerator non supporta policy basate su risorse.

L'accesso per più account con una policy basata sulle risorse offre alcuni vantaggi rispetto a un ruolo. Con una risorsa accessibile tramite una policy basata sulle risorse, il principale (persona

o applicazione) continua a utilizzare l'account attendibile e non deve rinunciare alle proprie autorizzazioni utente al posto delle autorizzazioni di ruolo. In altre parole, il principale ha accesso alle risorse nell'account attendibile e nell'account trusting contemporaneamente. Ciò risulta per attività quali, ad esempio, la copia di informazioni da un account a un altro. Per ulteriori informazioni sull'utilizzo di ruoli tra account, consultaOfferta di un accesso a un utente IAM di un altro account AWS di proprietànellaGuida per l'utente di IAM: .

AWS Organizations ization offre gestione basata su policy per più account AWS di tua proprietà. Con Organizations, è possibile creare gruppi di account, automatizzare la creazione di account, nonché applicare e gestire policy per tali gruppi. Organizations consentono di gestire a livello centralizzato le policy tra più account, senza la necessità di script personalizzati e di processi manuali. Utilizzando AWS Organizations, è possibile creare policy di controllo dei servizi (SCP) che controllano centralmente l'utilizzo dei servizi AWS negli account AWS. Per ulteriori informazioni, consultaCos'è AWS Organizations?nellaGuida utente AWS Organizations: .

Che cosa sono le policy?

Per controllare l'accesso ad AWS è possibile creare policy e collegarle a identità IAM o risorse AWS.

> **Note**
>
> Per iniziare, puoi ignorare questa pagina. Innanzi tutto, leggi le informazioni introduttive disponibili nella paginaIdentity and Access Management per AWS Global Acceleratore quindi vedereNozioni di base su IAM: .

Una policy è un oggetto in AWS che, se associato a una entità o risorsa, ne definisce le relative autorizzazioni. AWS valuta queste policy quando un principale, come ad esempio un utente, invia una richiesta. Le autorizzazioni della policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene memorizzata in AWS sotto forma di documenti JSON.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente dal metodo utilizzato per eseguirla. Ad esempio, se un criterio consente l'opzioneGetUser, un utente con tale policy può ottenere informazioni utente dalla Console di gestione AWS, dall'interfaccia a riga di comando AWS oppure dall'API AWS. Nella creazione di un utente IAM, è possibile configurare l'utente consentendogli l'accesso programmatico o alla console. L'utente IAM può accedere alla console con un nome utente e una password oppure può usare le chiavi di accesso per utilizzare l'API o l'interfaccia a riga di comando.

I seguenti tipi di policy, elencati in ordine di frequenza, possono influenzare se una richiesta viene autorizzata o meno. Per ulteriori dettagli, consulta .Tipi di policynellaGuida per l'utente di IAM: .

Policy basate su identità

È possibile collegare policy inline e policy gestite a identità IAM (utenti, gruppi a cui appartengono gli utenti e ruoli).

Policy basate su risorse

Puoi collegare policy inline alle risorse in alcuni servizi AWS. Gli esempi più comuni di policy basate sulle risorse sono le policy dei bucket Amazon S3 e le policy di affidabilità dei ruoli IAM. Global Accelerator non supporta policy basate su risorse.

SCP delle Organizations

È possibile utilizzare una policy di controllo dei servizi (SCP) di AWS Organizations per applicare un limite delle autorizzazioni a un'organizzazione o a un'unità organizzativa (UO) in. Queste autorizzazioni vengono applicate a tutte le entità all'interno degli account membri.

Liste di controllo accessi di rete (ACL)

Puoi utilizzare le liste di controllo accessi per controllare quali entità principali possono accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, anche se sono l'unico tipo di policy che non utilizza la struttura del documento di policy JSON. Global Accelerator supporta OR non supporta ACL.

Questi tipi di policy possono essere classificati come policy di autorizzazione o limiti di autorizzazione.

Policy di autorizzazione

Puoi collegare le policy di autorizzazione a una risorsa in AWS per definire le autorizzazioni per tale oggetto. All'interno di un unico account, AWS valuta tutte le policy di autorizzazione insieme. Le policy di autorizzazione sono le più comuni. I seguenti tipi di policy possono essere utilizzati come policy di autorizzazione:

Policy basate su identità

Quando colleghi una policy inline o gestita a un utente, un gruppo o un ruolo IAM, la policy definisce le autorizzazioni per tale entità.

Policy basate su risorse

Quando si collega un documento di policy JSON a una risorsa, è possibile definire le autorizzazioni per tale risorsa. Il servizio deve supportare le policy basate su risorse.

Liste di controllo accessi di rete (ACL)

Quando si collega un ACL a una risorsa, è possibile definire un elenco di entità principali autorizzate ad accedere a tale risorsa. La risorsa deve supportare le ACL.

Limiti delle autorizzazioni

È possibile utilizzare le policy per definire il limite delle autorizzazioni per un'entità (utente o ruolo). Il limite di autorizzazione controlla il numero massimo di autorizzazioni di cui un'entità può disporre. I limiti delle autorizzazioni sono una caratteristica avanzata di AWS. Quando più di uno di questi limiti di autorizzazione è applicabile a una richiesta, AWS valuta ogni limite separatamente. È possibile applicare un limite delle autorizzazioni nelle situazioni seguenti:

Organizations

È possibile utilizzare una policy di controllo dei servizi (SCP) di AWS Organizations per applicare un limite delle autorizzazioni a un'organizzazione o a un'unità organizzativa (UO) in.

Utenti o ruoli IAM

È possibile utilizzare una policy gestita per un limite delle autorizzazioni di un utente o un ruolo. Per ulteriori informazioni, consultaLimiti delle autorizzazioni per le entità IAMnellaGuida per l'utente di IAM: .

Argomenti

- Policy basate su identità
- Policy basate su risorse
- Classificazioni a livello di accesso ai

Policy basate su identità

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

Allegare una policy di autorizzazioni a un utente o un gruppo nell'account

Per concedere a un utente le autorizzazioni per creare una risorsa AWS Global Accelerator, ad esempio un acceleratore, è possibile collegare una policy di autorizzazione a un utente o a un gruppo a cui appartiene l'utente.

Allegare una policy di autorizzazione a un ruolo (per concedere autorizzazioni multiaccount)

Per concedere autorizzazioni multiaccount, puoi collegare una policy di autorizzazione basata su identità a un ruolo IAM. Ad esempio, l'amministratore dell'account A può creare un ruolo per concedere autorizzazioni multi-account a un altro account AWS (ad esempio l'account B) oppure a un servizio AWS nel modo seguente:

1. Account Un amministratore crea un ruolo IAM e attribuisce una policy di autorizzazioni al ruolo che concede le autorizzazioni per le risorse nell'account A.
2. L'amministratore dell'account A collega una policy di attendibilità al ruolo, identificando l'account B come principale per tale ruolo.
3. L'amministratore dell'account B può quindi delegare le autorizzazioni per usare tale ruolo a qualsiasi utente nell'account B. In questo modo, gli utenti nell'account B possono creare risorse nell'account A o accedervi. Se si desidera concedere a un servizio AWS le autorizzazioni per usare il ruolo, l'entità principale nella policy di trust può essere anche un'entità principale del servizio AWS.

Per ulteriori informazioni sull'utilizzo di IAM per delegare le autorizzazioni, consultaGestione degli accessinellaGuida per l'utente di IAM: .

Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consulta Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Di seguito sono riportati due esempi di criteri che è possibile utilizzare con Global Accelerator Il primo criterio di esempio concede a un utente l'accesso a livello di programmazione a tutte le azioni Elenca e Descrivi per gli acceleratori nell'account AWS:

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

```
                "globalaccelerator:List*",
                "globalaccelerator:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Nell'esempio seguente viene concesso l'accesso a livello di programmazione alla`ListAccelerators`operazione:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "globalaccelerator:ListAccelerators",
            ],
            "Resource": "*"
        }
    ]
}
```

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Queste policy consentono di specificare quali operazioni può effettuare una determinata entità principale su tale risorsa e in quali condizioni. La policy basata su risorse più comune è quella di un bucket Amazon S3. Le policy basate sulle risorse sono policy che esistono solo nella risorsa. Non esistono policy basate su risorse gestite.

La concessione di autorizzazioni ai membri di altri account AWS mediante una policy basata sulle risorse presenta alcuni vantaggi rispetto a un ruolo IAM. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Classificazioni a livello di accesso ai

Nella console IAM, le operazioni sono raggruppate utilizzando le seguenti classificazioni a livello di accesso:

Elenco

Fornisce l'autorizzazione per elencare le risorse all'interno del servizio per determinare l'esistenza di un oggetto. Le operazioni con questo livello di accesso possono elencare gli oggetti, ma consentono di visualizzare i contenuti di una risorsa. La maggior parte delle operazioni all'interno del livello di accesso List (Elenco) non può essere eseguita su una risorsa specifica. Quando si crea una dichiarazione di policy con queste operazioni, è necessario specificare All resources (Tutte le risorse) ("*").

Leggi

Fornisce l'autorizzazione per leggere ma non per modificare i contenuti e gli attributi delle risorse del servizio. Ad esempio, le operazioni Amazon S3`GetObject`e`GetBucketLocation`Dispongono dellaLeggiLivello di accesso.

Write

Concede l'autorizzazione per creare, eliminare o modificare le risorse del servizio. Ad esempio, le operazioni Amazon S3`CreateBucket`,`DeleteBucket`, e`PutObject`Dispongono dellaWriteLivello di accesso.

Gestione delle autorizzazioni

Concede l'autorizzazione per concedere o modificare le autorizzazioni a livello di risorsa nel servizio. Ad esempio, la maggior parte delle operazioni policy di IAM e AWS Organizations ization hanno la proprietàGestione delle autorizzazioniLivello di accesso.

> **Tip**
>
> Per migliorare la sicurezza del tuo account AWS, limita o monitora regolarmente le policy che includono ilGestione delle autorizzazioniclassificazione a livello di accesso.

Applicazione di tag

Fornisce l'autorizzazione per creare, eliminare o modificare i tag collegati a una risorsa nel servizio. Ad esempio, Amazon EC2`CreateTags`e`DeleteTags`le operazioni hannoApplicazione di tagLivello di accesso.

Nozioni di base su IAM

AWS Identity and Access Management (IAM) è un servizio AWS che consente di gestire l'accesso ai servizi e alle risorse in modo sicuro. IAM è una caratteristica dell'account AWS offerta senza costi aggiuntivi.

> **Note**
>
> Prima di iniziare a utilizzare IAM, leggi le informazioni introduttive disponibili nellaIdentity and Access Management per AWS Global Accelerator: .

Quando crei un account AWS per la prima volta, inizi con una singola identità di accesso che ha accesso completo a tutti i servizi e le risorse AWS nell'account. Tale identità è detta utente root dell'account AWS e puoi accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Rispetta piuttosto la best practice di utilizzare l'utente root soltanto per creare il tuo primo utente &IAM;. Quindi conserva al sicuro le credenziali dell'utente root e utilizzale per eseguire solo alcune attività di gestione dell'account e del servizio.

Creare l'utente amministratore IAM

Per creare un utente amministratore per se stessi e aggiungere l'utente a un gruppo di amministratori (console)

1. Accedere alla console IAM come proprietario dell'account scegliendo Root user (Utente root) e immettendo l'indirizzo email dell'account AWS. Nella pagina successiva, inserisci la password.

   > **Note**
   >
   > È fortemente consigliato rispettare la best practice sull'utilizzo del**`Administrator`**Utente IAM che segue e blocca in un luogo sicuro le credenziali dell'utente root. Accedere come utente root solo per eseguire alcune attività di gestione dell'account e del servizio.

2. Nel riquadro di navigazione selezionare Users (Utenti), quindi selezionare Add user (Aggiungi utente).
3. In User name (Nome utente), immettere **`Administrator`**.

4. Selezionare la casella di controllo accanto a AWS Management Console access (Accesso a Console di gestione AWS). Quindi, selezionare Custom password (Password personalizzata)e immettere la nuova password nella casella di testo.
5. (Facoltativo) Per impostazione predefinita, AWS richiede che il nuovo utente crei una nuova password al primo accesso. Puoi deselezionare la casella di controllo accanto a User must create a new password at next sign-in (L'utente deve creare una nuova password al prossimo accesso) per consentire al nuovo utente di reimpostare la propria password dopo aver effettuato l'accesso.
6. ScegliereSuccessivo: Autorizzazioni.
7. In Set permissions (Imposta autorizzazioni), selezionare Add user to group (Aggiungi l'utente al gruppo).
8. Seleziona Create group (Crea gruppo).
9. Nella finestra di dialogo Create group (Crea gruppo), per Group name (Nome gruppo) immettere **`Administrators`**.
10. SceglierePolicy di filtroe quindi selezionareAWS gestito - funzione di lavoroper filtrare il contenuto della tabella.
11. Nell'elenco delle policy, selezionare la casella di controllo accanto ad AdministratorAccess. Seleziona quindi Create group (Crea gruppo).

> **Note**
>
> È necessario attivare l'accesso utente e ruolo IAM alla fatturazione prima di poter utilizzare le autorizzazioni `AdministratorAccess` per accedere alla console Fatturazione e gestione costi AWS. A questo scopo, seguire le istruzioni nella fase 1 del tutorial sulla delega dell'accesso alla console di fatturazione.

12. Nell'elenco dei gruppi seleziona la casella di controllo per il tuo nuovo gruppo. Se necessario, selezionare Refresh (Aggiorna) per visualizzare il gruppo nell'elenco.
13. ScegliereSuccessivo: Tags: .
14. (Facoltativo) Aggiungere metadati all'utente collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo di tag in IAM, consultare Tagging di utenti e ruoli IAM nella Guida per l'utente di IAM.
15. ScegliereSuccessivo: Review (Revisione)Per visualizzare l'elenco delle appartenenze ai gruppi da aggiungere al nuovo utente. Quando sei pronto per continuare, seleziona Create user (Crea utente).

È possibile utilizzare questa stessa procedura per creare altri gruppi e utenti e concedere agli utenti l'accesso alle risorse dell'account AWS. Per ulteriori informazioni sull'utilizzo di policy per limitare le autorizzazioni degli utenti alle risorse AWS, consulta Gestione degli accessi e Esempi di policy.

Creazione di utenti delegati per Global Accelerator

Per supportare più utenti nel tuo account AWS, devi delegare l'autorizzazione per consentire ad altri utenti di eseguire solo le operazioni che vuoi consentire. A tale scopo, crea un gruppo IAM con le autorizzazioni necessarie a questi utenti e aggiungi gli utenti IAM ai gruppi necessari al momento della creazione. Puoi utilizzare questa procedura per impostare i gruppi, gli utenti e le autorizzazioni per tutto il tuo account AWS. Questa soluzione è ottimale se utilizzata da organizzazioni di piccole e medie dimensioni in cui un amministratore AWS può gestire manualmente gli utenti e gruppi. Per le organizzazioni di grandi dimensioni, è possibile utilizzareRuoli IAM personalizzati,federazione, oppureSingle Sign-On: .

Nella procedura seguente vengono creati tre utenti denominati**arnav**,**carlos**, e**martha**e allegare un criterio che concede l'autorizzazione a creare un acceleratore denominato**my-example-accelerator**, ma solo entro i prossimi 30 giorni. Puoi utilizzare le fasi descritte qui per aggiungere utenti con autorizzazioni diverse.

Per creare un utente delegato per un'altra persona (console)

1. Accedere alla Console di gestione AWS e aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegliere Users (Utenti), quindi scegliere Add user (Aggiungi utente).
3. In User name (Nome utente), immettere **arnav**.
4. Scegliere Add another user (Aggiungi un altro utente) e immettere **carlos** per il secondo utente. Scegliere quindi Add another user (Aggiungi un altro utente) e immettere **martha** per il terzo utente.
5. Selezionare la casella di controllo accanto aAccesso alla console di gestione AWSe quindi selezionareAutogenerated password: .
6. Deselezionare la casella di controllo accanto a User must create a new password at next sign-in (L'utente deve creare una nuova password al prossimo accesso) per consentire al nuovo utente di reimpostare la propria password dopo aver effettuato l'accesso.
7. ScegliereSuccessivo: Autorizzazioni.

8. Scegli Attach existing policies directly (Collega direttamente le policy esistenti). Creerai una nuova policy gestita per gli utenti.
9. Seleziona Create Policy (Crea policy).

   La procedura guidata Create policy (Crea policy) viene visualizzata in una nuova scheda o in una nuova finestra del browser.
10. Nella scheda Visual editor (Editor visivo), selezionare Choose a Service (Scegli un servizio). Quindi scegliete Global Accelerator. È possibile utilizzare la casella di ricerca in alto per limitare i risultati nell'elenco di servizi.

    LaService (Servizio)si chiude e la sezioneOperazionisi apre automaticamente.
11. Scegliere le operazioni Acceleratore globale che si desidera consentire.
    Ad esempio, per concedere l'autorizzazione per creare un acceleratore, immettere**`globalaccelerator:CreateAccelerator`**nellaFiltra le azioniCasella di testo. Quando l'elenco di operazioni di acceleratore globale è filtrata, selezionare la casella di controllo accanto a**`globalaccelerator:CreateAccelerator`**: .

    Le operazioni Acceleratore globale sono raggruppate in base alla classificazione del livello di accesso per semplificare la definizione del livello di accesso di ogni operazione. Per ulteriori informazioni, consulta Classificazioni a livello di accesso ai.
12. Se le operazioni selezionate nelle fasi precedenti non supportano la scelta di risorse specifiche, l'opzioneA tutte le risorseè selezionato per te. In questo caso, non è possibile modificare questa sezione.

    Se si seleziona una o più operazioni che supportano le autorizzazioni a livello di risorsa, l'editor visivo elenca tali tipi di risorsa nella sezione Resources (Risorse). ScegliereHai scelto le azioni che richiedono ilAcceleratoreTipo di risorsaper scegliere se inserire un acceleratore specifico per il criterio.
13. Se si desidera consentire l'operazione `globalaccelerator:CreateAccelerator` per tutte le risorse, scegliere All resources (Tutte le risorse).

    Se si desidera specificare una risorsa, scegliere Add ARN (Aggiungi ARN). Specificare la regione e l'ID account (o l'ID account) (oppure selezionareQualsiasi), quindi immettere**`my-example-accelerator`**per la risorsa. Quindi scegliere Add (Aggiungi).
14. Scegliere Specify request conditions (optional) (Specifica le condizioni di richiesta (opzionale)).
15. ScegliereAggiungi condizionePer concedere l'autorizzazione per creare un acceleratoreentro i successivi 7 giorni. Supponiamo che la data odierna sia il 1° gennaio 2019.

16. Per Condition Key (Chiave di condizione), scegliere aws:CurrentTime. Questa chiave di condizione controlla la data e l'ora in cui l'utente effettua la richiesta. Restituisce True e pertanto consente l'operazione **`globalaccelerator:CreateAccelerator`** solo se la data e l'ora sono comprese nell'intervallo specificato.
17. PerQualifierMantenere il valore predefinito.
18. Per specificare l'inizio dell'intervallo di data e ora consentito, in Operator (Operatore) scegliere DateGreaterThan. In Value (Valore), immettere **`2019-01-01T00:00:00Z`**.
19. Scegliere Add (Aggiungi) per salvare la condizione.
20. Selezionare Add another condition (Aggiungi un'altra condizione) per specificare la data di fine.
21. Eseguire una procedura analoga per specificare la fine dell'intervallo di data e ora consentito. Per Condition Key (Chiave di condizione), scegliere aws:CurrentTime. In Operator (Operatore), scegliere DateLessThan. In Value (Valore), immettere **`2019-01-06T23:59:59Z`**, 7 giorni dopo la prima data. Scegliere Add (Aggiungi) per salvare la condizione.
22. (Facoltativo) Per visualizzare il documento di policy JSON per la policy in fase di creazione, scegliere la casella di controlloJSONScheda. È possibile passare tra le schede Visual editor (Editor visivo) e JSON in qualsiasi momento. Tuttavia, se si apportano modifiche o si sceglieEsamina policynellaVisual editor (Editor visivo)IAM potrebbe modificare la struttura della policy per ottimizzarla per l'editor visivo. Per ulteriori informazioni, consultaModifica della struttura delle policynellaGuida per l'utente di IAM: .
23. Al termine, selezionare Review policy (Rivedi policy).
24. SulEsamina policy, perNome, immettere**`globalaccelerator:CreateAcceleratorPolicy`**: . Per Descrizione, immettere **`Policy to grants permission to create an accelerator`**. Esaminare il riepilogo della policy per assicurarsi di aver concesso le autorizzazioni corrette e selezionare Create policy (Crea policy) per salvare la nuova policy.
25. Tornare alla scheda o alla finestra originale e aggiornare l'elenco di policy.
26. Nella casella di ricerca immetti **`globalaccelerator:CreateAcceleratorPolicy`**. Selezionare la casella di controllo accanto alla nuova policy. Quindi selezionare Next Step (Fase successiva).
27. ScegliereSuccessivo: Review (Revisione)Per visualizzare in anteprima i nuovi utenti. Quando si è pronti per continuare, selezionare Create users (Crea utenti).
28. Scaricare o copiare le password per i nuovi utenti e consegnarle agli utenti in modo sicuro. Separatamente, fornisci agli utenti uncollegamento alla pagina della console utente IAMe i nomi utente appena creati.

Consente agli utenti di gestire in modo autonomo le proprie credenziali

È necessario avere l'accesso fisico all'hardware che ospiterà il dispositivo MFA virtuale dell'utente per configurare MFA. Ad esempio, è possibile configurare MFA per un utente che utilizzerà un dispositivo MFA virtuale in esecuzione su uno smartphone. In questo caso, è necessario disporre di uno smartphone per completare la procedura guidata. Per questo motivo, è possibile consentire agli utenti di configurare e gestire i propri dispositivi MFA virtuali. In questo caso, è necessario concedere agli utenti le autorizzazioni per eseguire le necessarie operazioni IAM.

Per creare una policy che consenta l'autogestione delle credenziali (console)

1. Accedere alla Console di gestione AWS e aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, selezionare Policies (Policy) e Create Policy (Crea policy).
3. Selezionare la scheda JSON e copiare il testo dal documento della seguente policy JSON. Incollare il testo nella casella di testo JSON.

> **Important**
>
> Questo esempio di policy non consente agli utenti di modificare la password durante l'accesso. I nuovi utenti e gli utenti con una password scaduta potrebbero provare a farlo. Per consentire questa operazione, aggiungere `iam:ChangePassword` e `iam:CreateLoginProfile` all'istruzione `BlockMostAccessUnlessSignedInWithMFA`. Tuttavia, IAM sconsiglia di farlo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllUsersToListAccounts",
            "Effect": "Allow",
            "Action": [
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid":
"AllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation",
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword",
                "iam:CreateAccessKey",
                "iam:CreateLoginProfile",
                "iam:DeleteAccessKey",
                "iam:DeleteLoginProfile",
                "iam:GetLoginProfile",
                "iam:ListAccessKeys",
                "iam:UpdateAccessKey",
                "iam:UpdateLoginProfile",
                "iam:ListSigningCertificates",
                "iam:DeleteSigningCertificate",
                "iam:UpdateSigningCertificate",
                "iam:UploadSigningCertificate",
                "iam:ListSSHPublicKeys",
                "iam:GetSSHPublicKey",
                "iam:DeleteSSHPublicKey",
                "iam:UpdateSSHPublicKey",
                "iam:UploadSSHPublicKey"
            ],
            "Resource": "arn:aws:iam::*:user/${aws:username}"
        },
        {
            "Sid": "AllowIndividualUserToViewAndManageTheirOwnMFA",
            "Effect": "Allow",
            "Action": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:EnableMFADevice",
                "iam:ListMFADevices",
                "iam:ResyncMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
        {
```

```
            "Sid":
 "AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA",
            "Effect": "Allow",
            "Action": [
                "iam:DeactivateMFADevice"
            ],
            "Resource": [
                "arn:aws:iam::*:mfa/${aws:username}",
                "arn:aws:iam::*:user/${aws:username}"
            ],
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        },
        {
            "Sid": "BlockMostAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "NotAction": [
                "iam:CreateVirtualMFADevice",
                "iam:DeleteVirtualMFADevice",
                "iam:ListVirtualMFADevices",
                "iam:EnableMFADevice",
                "iam:ResyncMFADevice",
                "iam:ListAccountAliases",
                "iam:ListUsers",
                "iam:ListSSHPublicKeys",
                "iam:ListAccessKeys",
                "iam:ListServiceSpecificCredentials",
                "iam:ListMFADevices",
                "iam:GetAccountSummary",
                "sts:GetSessionToken"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "false"
                }
            }
        }
    ]
}
```

Che cosa fa questa policy?

- `LaAllowAllUsersToListAccounts`consente all'utente di visualizzare informazioni di base sull'account e i suoi utenti nella console IAM. Queste autorizzazioni devono essere nella propria istruzione perché non supportano o non devono specificare una risorsa ARN specifica e specificano invece `"Resource" : "*"`.
- `LaAllowIndividualUserToSeeAndManageOnlyTheirOwnAccountInformation`L'istruzione consente all'utente di gestire l'utente, la password, le chiavi di accesso, la firma di certificati, le chiavi pubbliche SSH e le informazioni MFA nella console IAM. Inoltre, consente agli utenti di effettuare l'accesso per la prima volta se un amministratore richiede di impostare una password per la prima volta. La risorsa ARN limita l'uso di queste autorizzazioni solo per l'entità utente IAM dell'utente.
- L'istruzione `AllowIndividualUserToViewAndManageTheirOwnMFA` consente all'utente di visualizzare o gestire il proprio dispositivo MFA. Si noti che gli ARN della risorsa in questa istruzione consentono l'accesso a un solo dispositivo MFA o utente con lo stesso nome dell'utente registrato al momento. Gli utenti non possono creare o modificare qualsiasi dispositivo MFA diverso dal proprio.
- L'istruzione `AllowIndividualUserToDeactivateOnlyTheirOwnMFAOnlyWhenUsingMFA` consente all'utente di disattivare solo il proprio dispositivo MFA e solo se l'utente ha effettuato l'accesso utilizzando MFA. Ciò impedisce ad altri con solo le chiavi di accesso (e non il dispositivo MFA) di disattivare il dispositivo MFA e accedere all'account.
- `LaBlockMostAccessUnlessSignedInWithMFA`utilizza una combinazione di`"Deny"e"NotAction"`per negare l'accesso a tutte le azioni tranne alcune in IAM e altri servizi AWSifl'utente non ha effettuato l'accesso con MFA. Per ulteriori informazioni sulla logica di questa istruzione, consultaNotAction con DenynellaGuida per l'utente di IAM: . Se l'utente ha effettuato l'accesso con MFA, il test `"Condition"` ha esito negativo e l'istruzione "deny" finale non ha effetto, quindi le altre policy o istruzioni per l'utente ne determinano le relative autorizzazioni. Questa istruzione garantisce che quando l'utente non ha effettuato l'accesso con MFA può eseguire solo le operazioni elencate e solo se un'altra istruzione o policy consente l'accesso a tali operazioni.

  La versione `...IfExists` dell'operatore `Bool` garantisce che se la chiave `aws:MultiFactorAuthPresent` manca, la condizione restituisce true. Questo significa che a un utente che accede a un'API con le credenziali di lungo termine, ad esempio con una chiave di accesso, viene negato l'accesso alle operazioni API non IAM.

4. Al termine, selezionare Review policy (Rivedi policy).
5. Nella pagina Review policy (Esamina policy), immettere **`Force_MFA`** come nome della policy. Per la descrizione del criterio, immetti**`This policy allows users to manage their own passwords and MFA devices but nothing else unless they authenticate with MFA.`**Consulta la policyRiepilogoPer visualizzare le autorizzazioni concesse dalla policy e selezionareCrea policyPer salvare il proprio lavoro.

   La nuova policy appare nell'elenco delle policy gestite ed è pronta a collegare.

Per collegare la policy a un utente (console)

1. Nel riquadro di navigazione, seleziona Users (Utenti).
2. Scegliere il nome (non la casella di controllo) dell'utente che si desidera modificare.
3. Nella scheda Permissions (Autorizzazioni), scegliere Add permissions (Aggiungi autorizzazioni).
4. Scegli Attach existing policies directly (Collega direttamente le policy esistenti).
5. Nella casella di ricerca, immettere **`Force`** e selezionare la casella di controllo accanto a Force_MFA nell'elenco. Quindi scegli Next (Successivo): Review (Revisione): .
6. Rivedere i dettagli e scegliere Add permissions (Aggiungi autorizzazioni).

Abilitare MFA per l'utente IAM

Per maggiore sicurezza, consigliamo a tutti gli utenti IAM di configurare l'autenticazione a più fattori o MFA (Multi-Factor Authentication) per favorire la protezione delle risorse Global Accelerator. L'autenticazione MFA garantisce una maggiore sicurezza poiché richiede agli utenti di fornire autenticazione univoca da un dispositivo MFA supportato da AWS in aggiunta alle normali credenziali di accesso. Il dispositivo AWS MFA più sicuro è la chiave di sicurezza U2F. Se la tua azienda dispone già di dispositivi U2F, ti consigliamo di abilitare quei dispositivi per AWS. In caso contrario, è necessario acquistare un dispositivo per ciascun utente e attendere l'arrivo dell'hardware. Per ulteriori informazioni, consultaAbilitazione di una chiave di sicurezza U2FnellaGuida per l'utente di IAM: .

Se non disponi di un dispositivo U2F, puoi iniziare a utilizzare il prodotto in modo semplice e rapido e a basso costo mediante l'abilitazione di un dispositivo MFA virtuale. Ciò richiede di installare un'applicazione software su un telefono esistente o su un altro dispositivo mobile. Il dispositivo genera un codice numerico di sei cifre basato su un algoritmo di password monouso sincronizzato nel tempo. Quando l'utente accede ad AWS, verrà richiesto di immettere un codice dal dispositivo. Ogni dispositivo MFA virtuale assegnato a un utente deve essere univoco. Per eseguire l'autenticazione,

gli utenti non possono immettere un codice generato dal dispositivo MFA virtuale di un altro utente. Per un elenco di alcune delle app supportate che puoi utilizzare come dispositivi MFA virtuali, consulta la pagina Multi-Factor Authentication.

> **Note**
>
> È necessario avere l'accesso fisico al dispositivo mobile che ospiterà il dispositivo MFA virtuale dell'utente per configurare MFA per un utente IAM.

Per abilitare un dispositivo MFA virtuale per un utente IAM (console)

1. Accedere alla Console di gestione AWS e aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Users (Utenti).
3. Nell'elenco Nome utente, selezionare il nome dell'utente MFA in questione.
4. Selezionare la scheda Security Credentials (Credenziali di sicurezza). Accanto ad Assigned MFA device (Dispositivo MFA assegnato), selezionare Gestione.
5. Nella procedura guidata Manage MFA Device (Gestisci dispositivo MFA), selezionare Virtual MFA device (Dispositivo MFA virtuale) e scegliere Continua.

   IAM genera e visualizza le informazioni di configurazione per il dispositivo MFA virtuale, tra cui il codice grafico QR. Il grafico è una rappresentazione della "chiave di configurazione segreta" disponibile per l'inserimento manuale sui dispositivi che non supportano i codici QR.
6. Aprire l'app MFA virtuale.

   Per un elenco delle app che è possibile utilizzare per ospitare i dispositivi MFA virtuali, consultare la pagina Multi-Factor Authentication. Se l'app MFA virtuale supporta più account (più dispositivi MFA virtuali), selezionare l'opzione che consente di creare un nuovo account (un nuovo dispositivo virtuale MFA).
7. Determinare se l'app MFA supporta i codici QR e procedere in uno dei seguenti modi:

   - Nella procedura guidata, scegliere Show QR code (Mostra codice QR) ed eseguire la scansione del codice QR tramite l'app. Ad esempio, è possibile selezionare l'icona della fotocamera o un'opzione simile a Scan code (Scannerizza codice) ed eseguire la scansione del codice tramite la fotocamera del dispositivo.

- Nella procedura guidata Manage MFA Device (Gestisci dispositivo MFA), selezionare Show secret key (Mostra chiave segreta) e quindi immettere la chiave segreta nell'app MFA.

Al termine, il dispositivo MFA virtuale avvia la generazione di password una tantum.

8. Nella procedura guidata Manage MFA Device (Gestisci dispositivo MFA), nella casella MFA code 1 (Codice MFA 1), immettere la password monouso visualizzata nel dispositivo MFA virtuale. Attendere fino a un massimo di 30 secondi prima che il dispositivo generi una nuova password una tantum. Immettere quindi la seconda password monouso nella casella MFA code 2 (Codice MFA 2). Scegliere Assign MFA (Assegna MFA).

> **Important**
>
> Inviare la richiesta immediatamente dopo la generazione dei codici. Se si generano i codici e si attende troppo a lungo per inviare la richiesta, il dispositivo MFA si associa correttamente con l'utente ma il dispositivo MFA non viene sincronizzato. Ciò accade perché le password monouso temporanee (TOTP) scadono dopo un breve periodo di tempo. Se ciò accade, è possibile sincronizzare nuovamente il dispositivo. Per ulteriori informazioni, consultaRisincronizzazione dei dispositivi MFA virtuali e hardwarenellaGuida per l'utente di IAM: .

Il dispositivo MFA virtuale ora è pronto per l'uso con AWS.

Connessioni VPC sicure in AWS Global Accelerator

Quando aggiungi un servizio di Application Load Balancer interno o un endpoint di istanza Amazon EC2 in AWS Global Accelerator, abiliti il flusso del traffico Internet direttamente da e verso l'endpoint nei cloud privati virtuali (VPC) impostandolo come target in una subnet privata. Il VPC che contiene il bilanciamento del carico o l'istanza EC2 deve avere ungateway Internetcollegato ad esso, per indicare che il VPC accetta traffico Internet. Tuttavia, non sono necessari indirizzi IP pubblici sul bilanciamento del carico o sull'istanza EC2. Inoltre, non è necessaria una route di gateway Internet associata per la subnet.

Questo è diverso dal tipico caso di utilizzo del gateway Internet in cui sia gli indirizzi IP pubblici che le route di gateway Internet sono necessari per il flusso del traffico Internet verso istanze o bilanciamento del carico in un VPC. Anche se le interfacce di rete elastiche delle destinazioni sono

presenti in una subnet pubblica (ovvero una subnet con una route di gateway Internet), quando si utilizza Global Accelerator per il traffico Internet, Global Accelerator sostituisce la tipica route Internet e tutte le connessioni logiche che arrivano attraverso il L'acceleratore ritorna anche tramite Global Accelerator anziché tramite il gateway Internet.

> **Note**
>
> L'utilizzo di indirizzi IP pubblici e l'utilizzo di una subnet pubblica per le istanze Amazon EC2 non sono tipici, sebbene sia possibile configurare la configurazione con esse. I gruppi di sicurezza si applicano a qualsiasi traffico che arriva alle istanze dell'utente, incluso il traffico proveniente da Global Accelerator e qualsiasi indirizzo IP pubblico o elastico assegnato all'istanza ENI. Utilizzare subnet private per garantire che il traffico venga recapitato solo da Global Accelerator.

Tenere presente queste informazioni quando si considerano i problemi del perimetro di rete e si configurano i privilegi IAM relativi alla gestione dell'accesso a Internet. Per ulteriori informazioni sul controllo dell'accesso a Internet al VPC, consulta questaEsempio di policy di controllo del servizio: .

Logging e monitoraggio in AWS Global Accelerator

Il monitoraggio è una parte importante per garantire la disponibilità e le prestazioni di Global Accelerator e delle soluzioni AWS. È necessario raccogliere i dati sul monitoraggio da tutte le parti della soluzione AWS per consentire un debug più facile di eventuali guasti in più punti. AWS fornisce diversi strumenti per il monitoraggio delle risorse e delle attività Global Accelerator e la risposta a potenziali incidenti.

Log di flusso AWS Global Accelerator

: I registri del flusso del server forniscono record dettagliati sul traffico che scorre attraverso un acceleratore fino a un endpoint. I log di flusso del server sono utili per numerose applicazioni. Ad esempio, le informazioni del log di flusso possono essere utili nei controlli di accesso e di sicurezza. Per ulteriori informazioni, consulta Logdi flusso in AWS Global Accelerator.

Metriche e allarmi Amazon CloudWatch

: Utilizzando CloudWatch, puoi monitorare, in tempo reale, le risorse AWS e le applicazioni che esegui su AWS. CloudWatch raccoglie e tiene traccia delle metriche, che sono variabili misurate nel tempo. Puoi creare allarmi con parametri di controllo specifici e inviare notifiche o apportare

automaticamente modifiche alle risorse che stai monitorando quando la metrica supera una determinata soglia per un periodo di tempo. Per ulteriori informazioni, consulta Utilizzo di Amazon CloudWatch con AWS Global Accelerator.

Log di AWS CloudTrail

CloudTrail fornisce un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in Global Accelerator. CloudTrail acquisisce tutte le chiamate API per Global Accelerator sotto forma di eventi, incluse le chiamate dalla console Global Accelerator e dalle chiamate di codice all'API Global Accelerator. Per ulteriori informazioni, consulta Utilizzo di AWS CloudTrail per registrare le chiamate API AWS Global Accelerator.

Convalida della conformità per AWS Global Accelerator

Revisori di terze parti valutano la sicurezza e la conformità di AWS Global Accelerator come parte di più programmi di conformità AWS. Sono inclusi SOC, PCI, HIPAA, GDPR, ISO ed ENS High.

Per un elenco di servizi AWS, tra cui Global Accelerator, nell'ambito di programmi di conformità specifici, consultaServizi AWS coperti dal programma di compliance: . Per informazioni generali, consulta Programmi per la conformità di AWS.

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consultaDownload di report in AWS Artifact: .

La tua responsabilità di conformità durante l'utilizzo di Global Accelerator è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e normative applicabili. AWS fornisce le seguenti risorse per facilitare la conformità:

- Guide Quick Start Sicurezza e compliance: queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Architecting for HIPAA Security and Compliance Whitepaper : questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- Risorse per la conformità AWS: questa raccolta di cartelle di lavoro e guide potrebbe essere utile per l'industria e la posizione.
- Valutazione delle risorse con le regole nella Guida per sviluppatori di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.

- AWS Security Hub: questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con standard industriali di sicurezza e best practice.

Resilienza in AWS Global Accelerator

L'infrastruttura globale di AWS è basata su regioni e zone di disponibilità AWS. Le regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle regioni e le zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Oltre al supporto dell'infrastruttura globale AWS, Global Accelerator offre le seguenti caratteristiche che supportano la resilienza dei dati:

- Una zona di rete gestisce gli indirizzi IP statici dell'acceleratore da una subnet IP univoca. Analogamente a una zona di disponibilità AWS, una zona di rete è un'unità isolata con un proprio set di infrastrutture fisiche. Quando si configura un acceleratore, Global Accelerator alloca due indirizzi IPv4. Se un indirizzo IP da una zona di rete diventa non disponibile a causa del blocco degli indirizzi IP da parte di determinate reti client o a causa di interruzioni di rete, le applicazioni client possono riprovare sull'indirizzo IP statico integro dall'altra zona di rete isolata.
- Global Accelerator monitora in modo costante lo stato di tutti gli endpoint. Quando si determina che un endpoint attivo non è integro, Global Accelerator inizia immediatamente a indirizzare il traffico verso un altro endpoint disponibile. Ciò consente di creare un'architettura ad alta disponibilità per le applicazioni su AWS.

Sicurezza dell'infrastruttura in AWS Global Accelerator

In qualità di servizio gestito, AWS Global Accelerator è protetto dalle procedure di sicurezza di rete globali AWS descritte nellaAmazon Web Services: Panoramica sui processi di sicurezzaWhite paper.

Utilizza le chiamate all'API pubblicate da AWS per accedere a Global Accelerator tramite la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile

TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni come Java 7 e versioni successive, supporta tali modalità. Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, puoi utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Quote per AWS Global Accelerator

L'account AWS dispone di quote specifiche, note anche limiti, correlate a AWS Global Accelerator.

La console Service Quotas fornisce le informazioni sulle quote Global Accelerator. Oltre a visualizzare le quote predefinite, è possibile utilizzare la console Service Quotas perrichiedere aumenti di quotaper quote regolabili. Si noti che è necessario essere in Stati Uniti orientali (N. Virginia) quando si richiedono aumenti di quota per Global Accelerator.

Argomenti

Quote generali

Di seguito sono riportate le quote complessive per Global Accelerator.

Entità	Quota
Accelerator per account AWS	20 È possibilePer richiedere un aumento delle quote: .
Listener per acceleratore	10 È possibilePer richiedere un aumento delle quote: .
Intervalli di porte per listener	10
Sostituzioni delle porte per gruppo di endpoint	10 È possibilePer richiedere un aumento delle quote: .

Quote per gli endpoint per gruppo di endpoint

Di seguito sono riportate quote Global Accelerator applicabili al numero di endpoint nei gruppi di endpoint.

Entità	Descrizione	Quota
Gruppi di endpoint con più tipi di endpoint	Numero di endpoint in un gruppo di endpoint contenente più di un tipo di endpoint.	10
Gruppi di endpoint con solo Application Load Balancers	Numero di Application Load Balancer in un gruppo di endpoint contenente solo gli endpoint di Application Load Balancer.	10
Gruppi di endpoint con solo Network Load Balancers	Numero di servizi di bilanciamento del carico di rete in un gruppo di endpoint contenente solo endpoint di Network Load Balancer.	10
Gruppi di endpoint con solo istanze Amazon EC2	Numero di istanze EC2 in un gruppo endpoint contenente solo endpoint di istanza EC2.	10 È possibilePer richiedere un aumento delle quote: .
Gruppi di endpoint con solo indirizzi IP elastici	Numero di indirizzi IP elastici in un gruppo di endpoint contenente solo endpoint di indirizzi IP elastici.	10 È possibilePer richiedere un aumento delle quote: .
Gruppi di endpoint con solo subnet Amazon Virtual Private Cloud	Numero di subnet Amazon VPC in un gruppo di endpoint contenente solo endpoint di subnet.	10 È possibilePer richiedere un aumento delle quote: .

Quote correlate

Oltre a quote in Global Accelerator, non ci sono quote che si applicano alle risorse utilizzate come endpoint per un acceleratore. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Quote di indirizzi IP elastici nella Guida per l'utente di Amazon EC2: .
- Quote di servizio Amazon EC2 nella Guida per l'utente di Amazon EC2: .
- Quote per i Network Load Balancer nella Guida per l'utente dei sistemi Network Load Balancer: .
- Quote per gli Application Load Balancer nella Guida per l'utente dei sistemi Application Load Balancer: .
- Quote Amazon VPC nella Guida per l'utente di Amazon VPC: .

Informazioni correlate AWS Global Accelerator

Le informazioni e le risorse elencate di seguito possono fornirti ulteriori informazioni su Global Accelerator.

Argomenti

- Documentazione di AWS Global Accelerator
- Ottenere il supporto
- Suggerimenti dal blog Amazon Web Services

Documentazione di AWS Global Accelerator

Le risorse correlate seguenti possono rivelarsi utili durante l'utilizzo di questo servizio.

- Il riferimento API AWS Global Accelerator: fornisce una descrizione completa di azioni, parametri e tipi di dati API e un elenco di errori generati dal servizio.
- Informazioni sul prodotto AWS Global Accelerator: la pagina Web principale con informazioni su Global Accelerator, tra cui caratteristiche e prezzi.
- Condizioni d'usoInformazioni dettagliate sul copyright e i marchi, sul tuo account, la tua licenza e l'accesso al sito e ad altri argomenti.

Ottenere il supporto

Il Support per Global Accelerator è disponibile in diverse forme.

- Forum di discussioneForum basato su community per sviluppatori per la discussione di questioni tecniche correlate a Global Accelerator.
- Centro AWS Support: questo sito raccoglie le informazioni sui tuoi casi di supporto recenti nonché i risultati di AWS Trusted Advisor e dei controlli dello stato. Fornisce inoltre collegamenti a forum di discussione, domande frequenti di natura tecnica, pannello di controllo stato servizi e informazioni sui piani di supporto AWS.
- Informazioni su AWS Premium Support: la pagina Web principale con informazioni su AWS Premium Support, un canale di supporto personale a risposta rapida per aiutarti a creare ed eseguire applicazioni in Servizi infrastrutturali AWS.

- Contattaci: collegamenti per domande su fatturazione o account. Per quesiti tecnici, utilizza i forum di discussione o i collegamenti di supporto elencati sopra.

Suggerimenti dal blog Amazon Web Services

Il blog AWS contiene vari post con informazioni utili sull'utilizzo dei servizi AWS. Ad esempio, consulta i seguenti blog su Global Accelerator:

- AWS Global Accelerator per disponibilità e prestazioni
- Gestione del traffico con AWS Global Accelerator
- Analisi e visualizzazione dei log di flusso di AWS Global Accelerator utilizzando Amazon Athena e Amazon QuickSight

Per un elenco completo dei blog AWS Global Accelerator, consultaAWS Global Acceleratornella categoria Networking & Content Delivery dei post del blog AWS.

Cronologia dei documenti

Le voci seguenti descrivono le modifiche importanti apportate alla documentazione AWS Global Accelerator.

- Versione API: ultima
- Ultimo aggiornamento della documentazione: 9 dicembre 2020

Modifica	Descrizione	Data
Aggiornamento al ruolo esistente collegato ai servizi di Global Accelerator	Global Accelerator ha aggiunto una nuova autorizzazione,`ec2:DescribeRegions` , per consentire a Global Accelerator di ottenere informazioni sulla regione AWS per facilitare la diagnosi degli errori. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/security-iam-awsmanpol-updates.html.	7 maggio 2021
Aggiunti acceleratori di routing personalizzati	Global Accelerator ha introdotto un nuovo tipo di acceleratori di routing personalizzati. Gli acceleratori di routing personalizzati funzionano bene per scenari in cui si desidera utilizzare la logica dell'applicazione personalizzata per indirizzare uno o più utenti verso una destinazione e una porta specifiche tra molti, pur ottenendo i	9 dicembre 2020

Modifica	Descrizione	Data
	vantaggi in termini di prestazioni di Global Accelerator. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/work-with-custom-routing-accelerators.html.	
Aggiunto supporto per override delle porte	Global Accelerator ora supporta l'override della porta listener utilizzata per il routing del traffico agli endpoint in modo da poter reindirizzare il traffico verso porte specifiche degli endpoint. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-port-override.html.	21 Ottobre 2020
Sono state aggiunte due nuove regioni	Ora Global Accelerator supporta Africa (Città del Capo) e UE (Milano). Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/preserve-client-ip-address.regions.html.	20 maggio 2020

Modifica	Descrizione	Data
Tagging e BYOIP	Questa versione aggiunge il supporto per aggiungere tag agli acceleratori e portare il proprio indirizzo IP a AWS Global Accelerator (BYOIP). Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/tagging-in-global-accelerator.html e https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html.	27 febbraio 2020
Capitolo sulla sicurezza aggiornato	Aggiunti contenuti per la conformità, la resilienza e la sicurezza dell'infrastruttura. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/security.html.	20 dicembre 2019

Modifica	Descrizione	Data
Support per istanze EC2 e nome DNS predefinito	AWS Global Accelerator ora supporta l'aggiunta di istanze EC2 nelle regioni AWS supportate. Inoltre, Global Accelerator crea un nome DNS predefinito mappato agli indirizzi IP statici dell'acce leratore. Per ulteriori informazi oni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html e https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.html#about-accelerators.dns-addressing.	29 ottobre 2019
Conservazione dell'indirizzo IP del client per i servizi di bilanciamento del carico delle applicazioni	È ora possibile scegliere di fare in modo che AWS Global Accelerator conservi l'indirizzo IP del client per i bilanciatori di carico delle applicazioni nelle aree AWS supportate. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works-client-ip.html.	28 agosto 2019

Modifica	Descrizione	Data
Versione del servizio AWS Global Accelerator	La Guida per gli sviluppatori AWS Global Accelerator fornisce informazioni sull'impostazione e l'utilizzo di acceleratori, ovvero gestori di traffico a livello di rete, che migliorano la disponibilità e le prestazioni delle applicazioni Internet che hanno un pubblico globale.	26 Novembre 2018

Glossario AWS

Per la terminologia AWS più recente, consulta il glossario AWS in Riferimenti generali AWS.

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.