



Gateway Load Balancers

Sistema di bilanciamento del carico elastico



Sistema di bilanciamento del carico elastico: Gateway Load Balancers

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è un Gateway Load Balancer?	1
Panoramica di Gateway Load Balancer	1
Fornitori di appliance	2
Nozioni di base	2
Prezzi	2
Nozioni di base	3
Panoramica	3
Routing	5
Prerequisiti	6
Fase 1: creare un Gateway Load Balancer	6
Fase 2: creazione di un servizio endpoint del Gateway Load Balancer	8
Fase 3: creare un endpoint del Gateway Load Balancer	9
Fase 4: configurazione del routing	10
Nozioni di base per l'utilizzo della CLI	12
Panoramica	12
Routing	5
Prerequisiti	15
Fase 1: creare un Gateway Load Balancer e registrare le destinazioni	15
Fase 2: creare un endpoint del Gateway Load Balancer	17
Fase 3: configurazione dell'instradamento	18
Sistemi di load balancer	20
Stato del sistema di bilanciamento del carico	20
Tipo di indirizzo IP	21
Attributi del sistema di bilanciamento del carico	22
Zone di disponibilità	22
Unità di trasmissione massima (MTU)	22
Deletion protection (Protezione da eliminazione)	23
Bilanciamento del carico su più zone	24
Flussi asimmetrici	24
Tempo di inattività	24
Creazione di un sistema di bilanciamento del carico	25
Prerequisiti	25
Creazione del sistema di bilanciamento del carico	25
Fasi successive importanti	26

Aggiornare il tipo di indirizzo	27
Aggiornamento dei tag	27
Eliminazione di un sistema di bilanciamento del carico	29
Listener	30
Gruppi target	31
Configurazione dell'instradamento	31
Target type (Tipo di destinazione)	32
Destinazioni registrate	32
Attributi dei gruppi di destinazione	33
Ritardo di annullamento della registrazione	34
Failover della destinazione	35
Persistenza del flusso	36
Creazione di un gruppo target	37
Configurazione dei controlli dello stato	39
Impostazioni del controllo dello stato	39
Stato di integrità della destinazione	41
Codici di motivo di controllo dello stato	42
Scenari di errore della destinazione	43
Controllo dello stato delle destinazioni	44
Modifica le impostazioni del controllo dell'integrità	45
Registrazione di destinazioni	45
Gruppi di sicurezza target	46
Liste di controllo accessi (ACL) di rete	46
Registrazione o annullamento della registrazione di destinazioni	46
Aggiornamento dei tag	48
Eliminazione di un gruppo target	49
Monitoraggio dei sistemi di bilanciamento del carico	51
CloudWatch metriche	52
Parametri di Gateway Load Balancer	52
Dimensioni di parametro per Gateway Load Balancer	54
Visualizza le CloudWatch metriche per il tuo Gateway Load Balancer	55
CloudTrail registri	57
Informazioni su Elastic Load Balancing in CloudTrail	57
Informazioni sulle voci dei file di log di Elastic Load Balancing	58
Quote	61
Cronologia dei documenti	63

..... lxxv

Cos'è un Gateway Load Balancer?

Il servizio di bilanciamento del carico elastico distribuisce automaticamente il traffico in ingresso su più destinazioni, in una o più zone di disponibilità. Monitora lo stato di integrità delle destinazioni registrate e instrada il traffico solo verso le destinazioni integre. Elastic Load Balancing ridimensiona il load balancer di volta in volta, in quanto il traffico in ingresso varia nel corso del tempo. Può ridimensionare le risorse per la maggior parte dei carichi di lavoro automaticamente.

Elastic Load Balancing supporta i seguenti bilanciatori del carico: Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. È possibile selezionare il tipo di load balancer più adatto alle proprie esigenze. In questa guida vengono illustrati i Gateway Load Balancer. Per ulteriori informazioni sugli altri sistemi di bilanciamento del carico, consulta la [Guida per l'utente sugli Application Load Balancer](#), la [Guida per l'utente sui Network Load Balancer](#), e la [Guida per l'utente sui Classic Load Balancer](#).

Panoramica di Gateway Load Balancer

I Gateway Load Balancer consentono di implementare, dimensionare e gestire appliance virtuali, come firewall, sistemi di prevenzione e rilevamento delle intrusioni e sistemi di ispezione approfondita dei pacchetti. Combina un gateway di rete trasparente (ovvero un unico punto di entrata e uscita per tutto il traffico) e distribuisce il traffico dimensionando le appliance virtuali in base alla domanda.

Un Gateway Load Balancer funziona al terzo livello del modello Open Systems Interconnection (OSI), il livello di rete. È in ascolto per tutti i pacchetti IP attraverso tutte le porte e inoltra il traffico al gruppo di destinazione specificato nella regola del listener. Mantiene l'[aderenza del flusso](#) a uno specifico dispositivo di destinazione utilizzando 5 tuple (impostazione predefinita), 3 tuple o 2 tuple. Il Gateway Load Balancer e le istanze dell'appliance virtuale registrate scambiano il traffico delle applicazioni utilizzando il protocollo [GENEVE](#) sulla porta 6081.

I Gateway Load Balancer utilizzano gli endpoint Gateway Load Balancer per scambiare in modo sicuro il traffico attraverso i confini VPC. Un endpoint Gateway Load Balancer è un endpoint VPC che fornisce connettività privata tra appliance virtuali nel VPC del provider di servizi e server delle applicazioni nel VPC consumer del servizio. Distribuisci il Gateway Load Balancer nello stesso VPC delle appliance virtuali. Registra le appliance virtuali con un gruppo di destinazione per il Gateway Load Balancer.

Il traffico da e verso un endpoint del Gateway Load Balancer viene configurato tramite le tabelle di routing. Il traffico scorre dal VPC consumatore del servizio sull'endpoint del Gateway Load Balancer

al Gateway Load Balancer nel VPC fornitore del servizio, per poi tornare al VPC consumatore. È necessario creare l'endpoint del Gateway Load Balancer e i server delle applicazioni in sottoreti diverse. In questo modo è possibile configurare l'endpoint del Gateway Load Balancer come hop successivo nella tabella di routing per la sottorete dell'applicazione.

Per ulteriori informazioni, consulta [Accesso alle appliance virtuali tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Fornitori di appliance

L'utente è responsabile della scelta e della qualificazione del software proveniente dai fornitori di appliance. È necessario affidarsi al software dell'appliance per ispezionare o modificare il traffico dal sistema di bilanciamento del carico. I fornitori di appliance elencati come [Elastic Load Balancing Partner](#) hanno integrato e qualificato il loro software di appliance con AWS. È possibile attribuire un grado di affidabilità maggiore ai software di appliance offerti dai fornitori presenti in questo elenco. Tuttavia, AWS non garantisce la sicurezza o l'affidabilità dei software di questi fornitori.

Nozioni di base

Per creare un Gateway Load Balancer utilizzando il AWS Management Console, vedere. [Nozioni di base](#) Per creare un Gateway Load Balancer utilizzando il AWS Command Line Interface, vedere. [Nozioni di base per l'utilizzo della CLI](#)

Prezzi

Con il load balancer paghi solo in base all'uso effettivo. Per ulteriori informazioni, consulta [Prezzi di Elastic Load Balancing](#).

Nozioni di base sui Gateway Load Balancer.

I Gateway Load Balancer semplificano distribuzione, dimensionamento e gestione delle appliance virtuali di terze parti, ad esempio quelle di sicurezza.

In questo tutorial implementeremo un sistema di ispezione utilizzando un Gateway Load Balancer e un endpoint del Gateway Load Balancer.

Indice

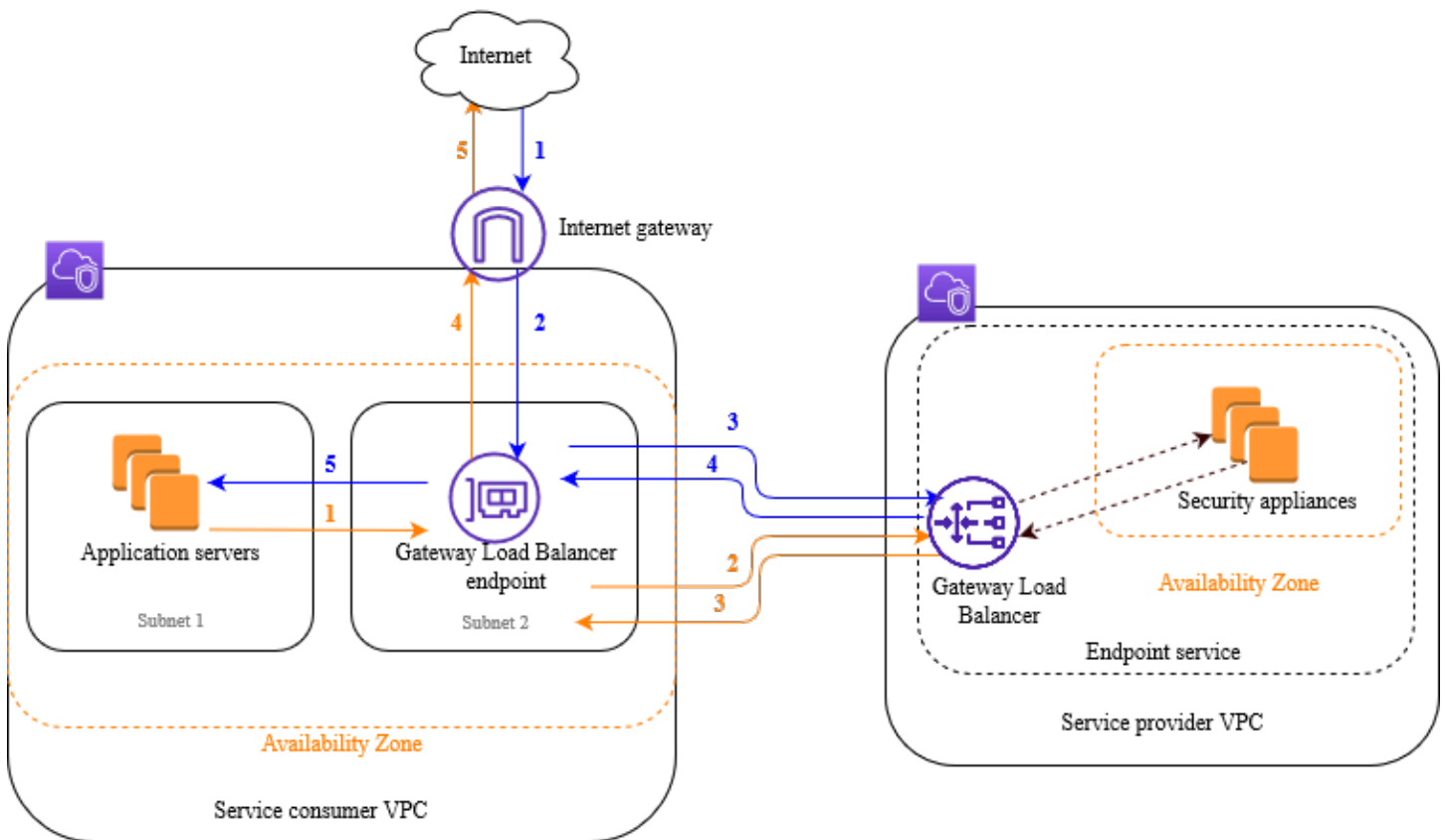
- [Panoramica](#)
- [Prerequisiti](#)
- [Fase 1: creare un Gateway Load Balancer](#)
- [Fase 2: creazione di un servizio endpoint del Gateway Load Balancer](#)
- [Fase 3: creare un endpoint del Gateway Load Balancer](#)
- [Fase 4: configurazione del routing](#)

Panoramica

Un endpoint Gateway Load Balancer è un endpoint VPC che fornisce connettività privata tra appliance virtuali nel VPC del provider di servizi e server delle applicazioni nel VPC consumer del servizio. Gateway Load Balancer viene distribuito nello stesso VPC delle appliance virtuali. Queste appliance vengono registrate come gruppo di destinazione del Gateway Load Balancer.

I server delle applicazioni vengono eseguiti in una sottorete (di destinazione) nel VPC del consumatore di servizi, mentre l'endpoint Gateway Load Balancer si trova in un'altra sottorete dello stesso VPC. Tutto il traffico che entra nel VPC dell'utente del servizio attraverso il gateway Internet viene innanzitutto instradato all'endpoint Gateway Load Balancer e poi instradato alla sottorete di destinazione.

Analogamente, tutto il traffico che esce dai server dell'applicazione (sottorete di destinazione) viene instradato sull'endpoint Gateway Load Balancer prima di essere instradato nuovamente attraverso Internet. Il seguente diagramma di rete è una rappresentazione visiva di come un endpoint del Gateway Load Balancer viene utilizzato per accedere a un servizio endpoint.



Gli articoli numerati di seguito evidenziano e spiegano gli elementi mostrati nell'immagine precedente.

Traffico in transito da Internet ai server dell'applicazione (frecche blu):

1. Il traffico entra nel VPC dell'utente del servizio attraverso il gateway Internet.
2. Il traffico viene inviato all'endpoint Gateway Load Balancer come risultato del routing in ingresso.
3. Il traffico viene inviato al Gateway Load Balancer che lo distribuisce a una delle appliance di sicurezza.
4. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione da parte dell'appliance di sicurezza.
5. Il traffico viene inviato ai server dell'applicazione (sottorete di destinazione).

Traffico in transito dall'applicazione a Internet (frecche arancioni):

1. Il traffico viene inviato all'endpoint Gateway Load Balancer come risultato dell'instradamento predefinito configurato nella sottorete del server dell'applicazione.

2. Il traffico viene inviato al Gateway Load Balancer che lo distribuisce a una delle appliance di sicurezza.
3. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione da parte dell'appliance di sicurezza.
4. Il traffico viene inviato al gateway Internet in base alla configurazione della tabella di instradamento.
5. Il traffico viene reindirizzato a Internet.

Routing

Questa tabella di routing per il gateway Internet deve disporre di una voce che invia il traffico destinato ai server dell'applicazione all'endpoint Gateway Load Balancer. Per specificare l'endpoint del Gateway Load Balancer utilizza l'ID dell'endpoint VPC. L'esempio seguente mostra le route per una configurazione dualstack.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
<i>CIDR IPv4 della sottorete 1</i>	<i>vpc-endpoint-id</i>
<i>CIDR IPv6 della sottorete 1</i>	<i>vpc-endpoint-id</i>

Questa tabella di routing per la sottorete con i server dell'applicazione deve disporre di voci che indirizzino tutto il traffico dai server dell'applicazione all'endpoint del Gateway Load Balancer.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
0.0.0.0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

La tabella di routing per la sottorete con l'endpoint del Gateway Load Balancer deve instradare il traffico dall'ispezione alla destinazione finale. Per il traffico proveniente da Internet, la route locale garantisce che raggiunga i server dell'applicazione. Per il traffico proveniente dai server dell'applicazione, aggiungi voci che indirizzino tutto il traffico al gateway Internet.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Prerequisiti

- Assicurati che il VPC consumatore del servizio disponga di almeno due sottoreti per ogni zona di disponibilità che contiene i server dell'applicazione. Una sottorete è destinata all'endpoint del Gateway Load Balancer e l'altra ai server dell'applicazione.
- Il Gateway Load Balancer e le destinazioni possono trovarsi nella stessa sottorete.
- Non è possibile utilizzare una sottorete condivisa da un altro account per distribuire il Gateway Load Balancer.
- Avvia almeno un'istanza dell'appliance di sicurezza in ogni sottorete nel VPC del provider di servizi. I gruppi di sicurezza per queste istanze devono permettere il traffico UDP sulla porta 6081.

Fase 1: creare un Gateway Load Balancer

Utilizza la procedura seguente per creare sistema di bilanciamento del carico, ascoltatore e gruppo di destinazione.

Per creare il sistema di bilanciamento del carico, l'ascoltatore e il gruppo target utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Load Balancing (Load balancer), scegliere Load Balancers (Load balancer).

3. Selezionare Create Load Balancer (Crea sistema di bilanciamento del carico).
4. Sotto a Gateway Load Balancer scegli Crea.
5. Configurazione di base
 - a. In Nome del sistema di bilanciamento del carico immetti un nome univoco per il sistema di bilanciamento del carico.
 - b. In IP address type (Tipo di indirizzo IP), seleziona ipv4 per supportare i soli indirizzi IPv4 oppure dualstack per supportare sia gli indirizzi IPv4 che IPv6.
6. Mappatura della rete
 - a. Per VPC, seleziona il VPC del fornitore del servizio.
 - b. Per le Mappature, seleziona tutte le zone di disponibilità in cui sono state avviate le istanze delle appliance di sicurezza e una sottorete per zona di disponibilità.
7. Routing dell'ascoltatore IP
 - a. Per Azione predefinita, seleziona un gruppo di destinazione esistente per ricevere il traffico. Questo gruppo di destinazione deve utilizzare il protocollo GENEVE.

Se non hai un gruppo di destinazione, seleziona Crea gruppo di destinazione, si aprirà una nuova scheda nel browser. Seleziona un tipo di destinazione, inserisci un nome per il gruppo di destinazione e mantieni il protocollo GENEVE. Seleziona il VPC con le istanze dell'appliance di sicurezza. Modifica le impostazioni del controllo dell'integrità secondo necessità e aggiungi i tag di cui hai bisogno. Seleziona Successivo. È possibile registrare le istanze dell'appliance di sicurezza con il gruppo di destinazione ora o dopo aver completato questa procedura. Seleziona Crea gruppo di destinazione, quindi torna alla scheda precedente del browser.
 - b. (Facoltativo) Espandi Tag dell'ascoltatore e aggiungi i tag di cui hai bisogno.
8. (Facoltativo) Espandi Tag del sistema di bilanciamento del carico e aggiungi i tag di cui hai bisogno.
9. Selezionare Create Load Balancer (Crea sistema di bilanciamento del carico).

Fase 2: creazione di un servizio endpoint del Gateway Load Balancer

Utilizza la procedura seguente per creare un servizio endpoint utilizzando un Gateway Load Balancer.

Creare di un servizio endpoint Gateway Load Balancer

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).
3. Seleziona Crea servizio endpoint ed effettua le seguenti operazioni:
 - a. Per Load balancer type (Tipo di load balancer), scegli Gateway.
 - b. In Available load balancers (Load balancer disponibili), seleziona il Gateway Load Balancer.
 - c. In Richiedi accettazione per l'endpoint, seleziona Accettazione richiesta per accettare manualmente le richieste di connessione al servizio endpoint. In caso contrario, queste vengono accettate automaticamente.
 - d. Per Supported IP address types (Tipi di indirizzo IP supportati), esegui una delle operazioni seguenti:
 - Seleziona IPv4 per consentire al servizio endpoint di accettare richieste IPv4.
 - Seleziona IPv6 per consentire al servizio endpoint di accettare richieste IPv6.
 - Seleziona IPv4 e IPv6 per consentire al servizio endpoint di accettare richieste IPv4 e IPv6.
 - e. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e inserisci la chiave e il valore del tag.
 - f. Scegli Crea. Il traffico viene inviato all'endpoint del Gateway Load Balancer.
4. Seleziona il proprio nuovo servizio endpoint e scegli Operazioni, Autorizza principali. Inserisci gli ARN dei consumatori del servizio che sono autorizzati a creare un endpoint per il servizio. Un consumatore del servizio può essere un utente, un ruolo IAM o Account AWS. Seleziona Allow principals (Consenti entità principali).

Fase 3: creare un endpoint del Gateway Load Balancer

Utilizza la procedura seguente per creare un endpoint Gateway Load Balancer che si connette al servizio endpoint del Gateway Load Balancer. Gli endpoint del Gateway Load Balancer sono zonali. È consigliabile creare un endpoint del Gateway Load Balancer per zona. Per ulteriori informazioni, consulta [Accesso alle appliance virtuali tramite AWS PrivateLink](#) nella Guida di AWS PrivateLink .

Per creare un endpoint Gateway Load Balancer

1. Accedere alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint ed effettua le seguenti operazioni:
 - a. In Service category (Categoria del servizio), scegli Other endpoint services (Altri servizi endpoint).
 - b. In Nome servizio, specifica il nome del servizio annotato precedentemente, quindi seleziona Verifica servizio.
 - c. Per VPC, seleziona il VPC del consumatore del servizio.
 - d. Per Sottoreti, seleziona una sottorete per l'endpoint del Gateway Load Balancer.
 - e. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
 - IPv4: consente di assegnare indirizzi IPv4 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
 - IPv6: consente di assegnare indirizzi IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
 - Dualstack: consente di assegnare sia indirizzi IPv4 che IPv6 alle interfacce di rete dell'endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.
 - f. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e inserisci la chiave e il valore del tag.
 - g. Seleziona Crea endpoint. Lo stato iniziale è pending acceptance.

Per accettare la richiesta di connessione all'endpoint, utilizza la seguente procedura.

1. Nel pannello di navigazione scegli Endpoint Services (Servizi endpoint).

2. Selezionare il servizio endpoint.
3. Dalla scheda Endpoint connections (Connessioni endpoint), seleziona la connessione endpoint.
4. Per accettare la richiesta di connessione, scegli Actions (Operazioni), Accept endpoint connection request (Accetta richiesta di connessione endpoint). Quando viene richiesta la conferma, immetti **accept** e seleziona Accept (Accetta).

Fase 4: configurazione del routing

Configura le tabelle di routing per il VPC consumatore del servizio come segue. Ciò consente alle appliance di sicurezza di eseguire ispezioni sul traffico in entrata destinato ai server dell'applicazione.

Configurazione del routing

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Seleziona la tabella di instradamento per il gateway Internet ed esegui le operazioni seguenti:
 - a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
 - b. Selezionare Add route (Aggiungi route). Per Destination (Destinazione), immetti il blocco CIDR IPv4 della sottorete per i server dell'applicazione. Per Target, seleziona l'endpoint VPC.
 - c. Se supporti IPv6, scegli Add route (Aggiungi route). Per Destination (Destinazione), immetti il blocco CIDR IPv6 della sottorete per i server dell'applicazione. Per Target, seleziona l'endpoint VPC.
 - d. Seleziona Salvataggio delle modifiche.
4. Seleziona la tabella di instradamento per la sottorete con i server dell'applicazione ed esegui le operazioni seguenti:
 - a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
 - b. Selezionare Add route (Aggiungi route). In Destination (Destinazione), immettere **0.0.0.0/0**. Per Target, seleziona l'endpoint VPC.
 - c. Se supporti IPv6, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **::/0**. Per Target, seleziona l'endpoint VPC.
 - d. Seleziona Salvataggio delle modifiche.

5. Seleziona la tabella di instradamento per la sottorete con l'endpoint Gateway Load Balancer ed esegui le operazioni seguenti:
 - a. Selezionare Actions (Operazioni), Edit routes (Modifica route).
 - b. Selezionare Add route (Aggiungi route). In Destination (Destinazione), immettere **0.0.0.0/0**. Per Target, seleziona il gateway Internet.
 - c. Se supporti IPv6, scegli Add route (Aggiungi route). In Destination (Destinazione), immettere **::/0**. Per Target, seleziona il gateway Internet.
 - d. Scegli Save changes (Salva modifiche).

Nozioni di base sui Gateway Load Balancer utilizzando la AWS CLI.

I Gateway Load Balancer semplificano distribuzione, dimensionamento e gestione delle appliance virtuali di terze parti, ad esempio quelle di sicurezza.

In questo tutorial implementeremo un sistema di ispezione utilizzando un Gateway Load Balancer e un endpoint del Gateway Load Balancer.

Indice

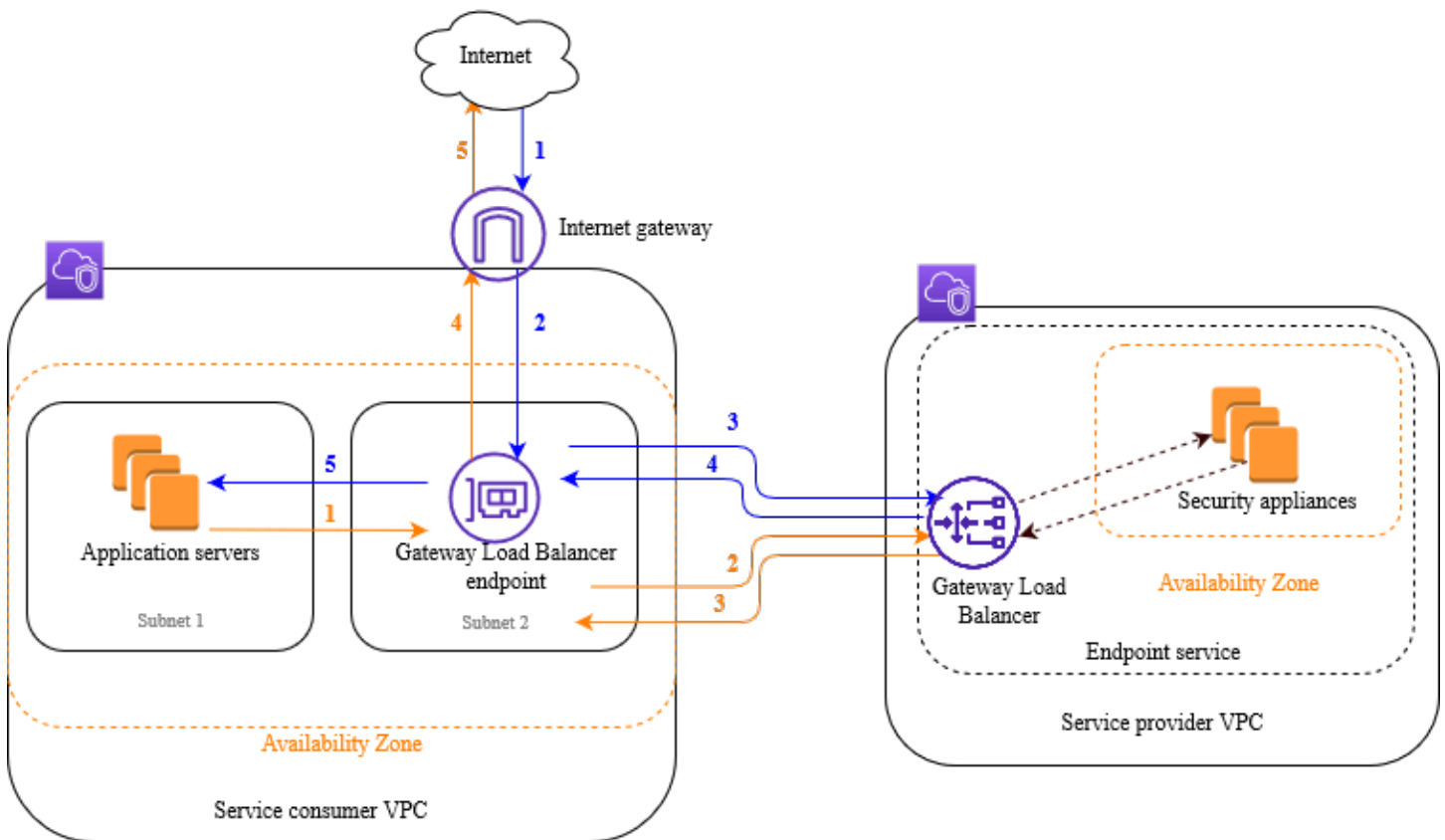
- [Panoramica](#)
- [Prerequisiti](#)
- [Fase 1: creare un Gateway Load Balancer e registrare le destinazioni](#)
- [Fase 2: creare un endpoint del Gateway Load Balancer](#)
- [Fase 3: configurazione dell'instradamento](#)

Panoramica

Un endpoint Gateway Load Balancer è un endpoint VPC che fornisce connettività privata tra appliance virtuali nel VPC del provider di servizi e server delle applicazioni nel VPC consumer del servizio. Gateway Load Balancer viene distribuito nello stesso VPC delle appliance virtuali. Queste appliance vengono registrate come gruppo di destinazione del Gateway Load Balancer.

I server delle applicazioni vengono eseguiti in una sottorete (di destinazione) nel VPC del consumatore di servizi, mentre l'endpoint Gateway Load Balancer si trova in un'altra sottorete dello stesso VPC. Tutto il traffico che entra nel VPC dell'utente del servizio attraverso il gateway Internet viene innanzitutto instradato all'endpoint Gateway Load Balancer e poi instradato alla sottorete di destinazione.

Analogamente, tutto il traffico che esce dai server dell'applicazione (sottorete di destinazione) viene instradato sull'endpoint Gateway Load Balancer prima di essere instradato nuovamente attraverso Internet. Il seguente diagramma di rete è una rappresentazione visiva di come un endpoint del Gateway Load Balancer viene utilizzato per accedere a un servizio endpoint.



Gli articoli numerati di seguito evidenziano e spiegano gli elementi mostrati nell'immagine precedente.

Traffico in transito da Internet ai server dell'applicazione (frecche blu):

1. Il traffico entra nel VPC dell'utente del servizio attraverso il gateway Internet.
2. Il traffico viene inviato all'endpoint Gateway Load Balancer come risultato del routing in ingresso.
3. Il traffico viene inviato al Gateway Load Balancer che lo distribuisce a una delle appliance di sicurezza.
4. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione da parte dell'appliance di sicurezza.
5. Il traffico viene inviato ai server dell'applicazione (sottorete di destinazione).

Traffico in transito dall'applicazione a Internet (frecche arancioni):

1. Il traffico viene inviato all'endpoint Gateway Load Balancer come risultato dell'instradamento predefinito configurato nella sottorete del server dell'applicazione.

2. Il traffico viene inviato al Gateway Load Balancer che lo distribuisce a una delle appliance di sicurezza.
3. Il traffico viene inviato nuovamente all'endpoint Gateway Load Balancer dopo l'ispezione da parte dell'appliance di sicurezza.
4. Il traffico viene inviato al gateway Internet in base alla configurazione della tabella di instradamento.
5. Il traffico viene reindirizzato a Internet.

Routing

Questa tabella di routing per il gateway Internet deve disporre di una voce che invia il traffico destinato ai server dell'applicazione all'endpoint Gateway Load Balancer. Per specificare l'endpoint del Gateway Load Balancer utilizza l'ID dell'endpoint VPC. L'esempio seguente mostra le route per una configurazione dualstack.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
<i>CIDR IPv4 della sottorete 1</i>	<i>vpc-endpoint-id</i>
<i>CIDR IPv6 della sottorete 1</i>	<i>vpc-endpoint-id</i>

Questa tabella di routing per la sottorete con i server dell'applicazione deve disporre di voci che indirizzino tutto il traffico dai server dell'applicazione all'endpoint del Gateway Load Balancer.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
0.0.0.0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

La tabella di routing per la sottorete con l'endpoint del Gateway Load Balancer deve instradare il traffico dall'ispezione alla destinazione finale. Per il traffico proveniente da Internet, la route locale garantisce che raggiunga i server dell'applicazione. Per il traffico proveniente dai server dell'applicazione, aggiungi voci che indirizzino tutto il traffico al gateway Internet.

Destinazione	Target
<i>CIDR IPv4 del VPC</i>	Locale
<i>CIDR IPv6 del VPC</i>	Locale
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Prerequisiti

- Installa la AWS CLI o aggiorna la versione corrente del AWS CLI se utilizzi una versione che non supporta i Gateway Load Balancer. Per ulteriori informazioni, consulta [Installazione dell'AWS Command Line Interface](#) nella Guida per l'utente di AWS Command Line Interface.
- Assicurati che il VPC consumatore del servizio disponga di almeno due sottoreti per ogni zona di disponibilità che contiene i server dell'applicazione. Una sottorete è destinata all'endpoint del Gateway Load Balancer e l'altra ai server dell'applicazione.
- Assicurati che il VPC del fornitore di servizi disponga di almeno due sottoreti per ogni zona di disponibilità che contiene i server delle appliance. Una sottorete è destinata al Gateway Load Balancer e l'altra alle istanze.
- Avvia almeno un'istanza dell'appliance di sicurezza in ogni sottorete nel VPC del provider di servizi. I gruppi di sicurezza per queste istanze devono permettere il traffico UDP sulla porta 6081.

Fase 1: creare un Gateway Load Balancer e registrare le destinazioni

Utilizza la procedura seguente per creare il sistema di bilanciamento del carico, l'ascoltatore, gruppi di destinazione e per registrare le istanze dell'appliance di sicurezza come destinazioni.

Creare un Gateway Load Balancer e registrare le destinazioni

1. Utilizzare il comando [create-load-balancer](#) per creare un sistema di bilanciamento del carico del tipo gateway. È possibile specificare una sottorete per ogni zona di disponibilità nella quale sono state lanciate le istanze dell'appliance di sicurezza.

```
aws elbv2 create-load-balancer --name my-load-balancer --type gateway --  
subnets provider-subnet-id
```

La modalità predefinita supporta solamente gli indirizzi IPv4. Per il supporto di entrambi gli indirizzi IPv4 e IPv6, aggiungi l'opzione `--ip-address-type dualstack`.

L'output include il nome della risorsa Amazon (ARN) del sistema di bilanciamento del carico, con il formato illustrato nel seguente esempio.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/gwy/my-load-  
balancer/1234567890123456
```

2. Utilizza il comando [create-target-group](#) per creare un gruppo di destinazione, specificando il VPC del provider di servizi in cui hai avviato le tue istanze.

```
aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --  
vpc-id provider-vpc-id
```

L'output include l'ARN del gruppo di destinazione, con il seguente formato.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-  
targets/0123456789012345
```

3. Utilizzare il comando [register-target \(registrare target\)](#) per registrare le istanze con il gruppo target.

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets  
Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. Utilizza il comando [create-listener](#) per creare un ascoltatore per il sistema di bilanciamento del carico con una regola predefinita che inoltra le richieste verso il gruppo target:

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions  
Type=forward,TargetGroupArn=targetgroup-arn
```

L'output contiene l'ARN dell'ascoltatore, con il formato seguente.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-load-  
balancer/1234567890123456/abc1234567890123
```

5. (Facoltativo) È possibile verificare l'integrità delle destinazioni registrate per il gruppo target utilizzando il seguente comando [describe-target-health](#).

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Fase 2: creare un endpoint del Gateway Load Balancer

Utilizza la procedura seguente per creare un endpoint del Gateway Load Balancer. Gli endpoint del Gateway Load Balancer sono zonali. È consigliabile creare un endpoint del Gateway Load Balancer per zona. Per ulteriori informazioni, consulta [Accesso alle appliance virtuali tramite AWS PrivateLink](#) nella Guida di .

Per creare un endpoint Gateway Load Balancer

1. Usa il comando [create-vpc-endpoint-service-configuration](#) per creare una configurazione del servizio di endpoint utilizzando il Gateway Load Balancer.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-  
arns loadbalancer-arn --no-acceptance-required
```

Per il supporto di entrambi gli indirizzi IPv4 e IPv6, aggiungi l'opzione `--supported-ip-address-types ipv4 ipv6`.

L'output contiene l'ID del servizio (ad esempio, `vpce-svc-12345678901234567`) e il nome del servizio (ad esempio, `com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567`).

2. Usa il comando [modify-vpc-endpoint-service-permissions](#) per consentire ai consumatori del servizio di creare un endpoint sul tuo servizio. Un consumatore del servizio può essere un utente, un ruolo IAM o Account AWS. L'esempio seguente aggiunge l'autorizzazione per l'Account AWS specificato.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root
```

3. Usa il comando [create-vpc-endpoint](#) per creare l'endpoint del Gateway Load Balancer per il tuo servizio.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-id --subnet-ids consumer-subnet-id
```

Per il supporto di entrambi gli indirizzi IPv4 e IPv6, aggiungi l'opzione `--ip-address-type dualstack`.

L'output contiene l'ID dell'endpoint del Gateway Load Balancer (ad esempio, `vpce-01234567890abcdef`).

Fase 3: configurazione dell'instradamento

Configura le tabelle di routing per il VPC consumatore del servizio come segue. Ciò consente alle appliance di sicurezza di eseguire ispezioni sul traffico in entrata destinato ai server dell'applicazione.

Configurazione del routing

1. Usa il comando [create-route](#) per aggiungere voci alla tabella di routing per il gateway Internet che instrada il traffico destinato ai server dell'applicazione all'endpoint del Gateway Load Balancer.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

Se supporti IPv6, aggiungi la route seguente.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

2. Usa il comando [create-route](#) per aggiungere una voce alla tabella di routing per la sottorete con i server dell'applicazione che instradano tutto il traffico dai server dell'applicazione all'endpoint del Gateway Load Balancer.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block  
0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

Se supporti IPv6, aggiungi la route seguente.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0  
--vpc-endpoint-id vpce-01234567890abcdef
```

3. Usa il comando [create-route](#) per aggiungere una voce alla tabella di routing per la sottorete con l'endpoint del Gateway Load Balancer che instrada tutto il traffico proveniente dai server dell'applicazione al gateway Internet.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block  
0.0.0.0/0 --gateway-id igw-01234567890abcdef
```

Se supporti IPv6, aggiungi la route seguente.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 --  
gateway-id igw-01234567890abcdef
```

4. Ripeti l'operazione per ogni tabella di routing della sottorete dell'applicazione in ogni zona.

Gateway Load Balancers

Utilizza un Gateway Load Balancer per implementare e gestire una parco istanze di appliance virtuali che supportano il protocollo GENEVE.

Un Gateway Load Balancer funziona al terzo livello del modello Open Systems Interconnection (OSI). È in ascolto per tutti i pacchetti IP attraverso tutte le porte e inoltra il traffico al gruppo di destinazione specificato nella regola dell'ascoltatore, usando il protocollo GENEVE sulla porta 6081.

È possibile aggiungere o rimuovere le destinazioni dal sistema di bilanciamento del carico in base alle proprie esigenze, senza interrompere il flusso di richieste. Elastic Load Balancing ridimensiona il load balancer di volta in volta, in quanto il traffico verso l'applicazione varia nel corso del tempo. Elastic Load Balancing è in grado di ridimensionare automaticamente le risorse per la maggior parte dei carichi di lavoro.

Indice

- [Stato del sistema di bilanciamento del carico](#)
- [Tipo di indirizzo IP](#)
- [Attributi del sistema di bilanciamento del carico](#)
- [Zone di disponibilità](#)
- [Unità di trasmissione massima \(MTU\)](#)
- [Deletion protection \(Protezione da eliminazione\)](#)
- [Bilanciamento del carico su più zone](#)
- [Flussi asimmetrici](#)
- [Tempo di inattività](#)
- [Crea un Gateway Load Balancer](#)
- [Tipi di indirizzi IP per il tuo Gateway Load Balancer](#)
- [Tag per il Gateway Load Balancer](#)
- [Elimina un Gateway Load Balancer](#)

Stato del sistema di bilanciamento del carico

Un Gateway Load Balancer può avere uno dei seguenti stati:

provisioning

Il Gateway Load Balancer è in fase di configurazione.

active

Il Gateway Load Balancer è completamente configurato e pronto a instradare il traffico.

failed

Il Gateway Load Balancer non può essere configurato.

Tipo di indirizzo IP

È possibile impostare i tipi di indirizzi IP che i server dell'applicazione possono utilizzare per accedere ai Gateway Load Balancer.

I Gateway Load Balancer supportano i seguenti tipi di indirizzi IP:

ipv4

È supportato solo IPv4.

dualstack

Sono supportati sia IPv4 che IPv6.

Considerazioni

- Il cloud privato virtuale (VPC, Virtual Private Cloud) e le sottoreti specificate per il sistema di bilanciamento del carico devono avere blocchi CIDR IPv6 associati.
- Le tabelle di routing per le sottoreti nel VPC del consumatore del servizio devono instradare il traffico IPv6 e le ACL di rete per queste sottoreti devono consentire il traffico IPv6.
- Un Gateway Load Balancer incapsula il traffico client IPv4 e IPv6 con un'intestazione IPv4 GENEVE e lo invia all'appliance. L'appliance incapsula il traffico client IPv4 e IPv6 con un'intestazione IPv4 GENEVE e lo invia al Gateway Load Balancer.

Per ulteriori informazioni sui tipi di indirizzi IP, vedere. [Tipi di indirizzi IP per il tuo Gateway Load Balancer](#)

Attributi del sistema di bilanciamento del carico

I seguenti sono gli attributi del sistema di bilanciamento del carico per il Gateway Load Balancer

`deletion_protection.enabled`

Indica se è abilitata la [protezione da eliminazione](#). Il valore predefinito è `false`.

`load_balancing.cross_zone.enabled`

Indica se è abilitato il [bilanciamento del carico tra zone](#). Il valore predefinito è `false`.

Zone di disponibilità

Quando si crea un Gateway Load Balancer, si abilitano una o più zone di disponibilità e si specifica la sottorete che corrisponde a ciascuna zona. Quando si abilitano più zone di disponibilità, si assicura che il sistema di bilanciamento del carico possa continuare a instradare il traffico anche se una zona di disponibilità non è più disponibile. Le sottoreti specificate devono avere a disposizione almeno 8 indirizzi IP ciascuna. Le sottoreti non possono essere rimosse dopo la creazione del load balancer. Per rimuovere una sottorete, è necessario creare un nuovo sistema di bilanciamento del carico.

Unità di trasmissione massima (MTU)

L'unità massima di trasmissione (MTU) è la dimensione del pacchetto di dati più grande che può essere trasmesso attraverso la rete. La MTU dell'interfaccia del Gateway Load Balancer supporta pacchetti fino a 8.500 byte. I pacchetti con una dimensione maggiore di 8.500 byte che arrivano al Gateway Load Balancer vengono eliminati.

Un Gateway Load Balancer incapsula il traffico client IP con un'intestazione GENEVE e lo invia all'appliance. Il processo di incapsulamento GENEVE aggiunge 64 byte al pacchetto originale. Pertanto, per supportare pacchetti fino a 8.500 byte, assicurati che l'impostazione MTU dell'appliance supporti pacchetti di almeno 8.564 byte.

I Gateway Load Balancer non supportano la frammentazione IP. Inoltre, i Gateway Load Balancer non generano il messaggio ICMP "Destinazione irraggiungibile: frammentazione necessaria e set DF". A causa di ciò, il percorso MTU Discovery (PMTUD) non è supportato.

Deletion protection (Protezione da eliminazione)

Per evitare che il Gateway Load Balancer venga eliminato accidentalmente, è possibile abilitare la protezione da eliminazione. Per impostazione predefinita, la protezione da eliminazione è disabilitata.

Se abiliti la protezione da eliminazione per il Gateway Load Balancer, devi disabilitarla prima di poterlo eliminare.

Per abilitare la protezione da eliminazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Gateway Load Balancer.
4. Seleziona Operazioni, Modifica attributi.
5. Nella pagina Edit load balancer attributes (Modifica attributi del sistema di bilanciamento del carico) seleziona Enable (Abilita) in Delete Protection (Elimina protezione) e poi scegli Save (Salva).

Per disabilitare la protezione da eliminazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Gateway Load Balancer.
4. Seleziona Operazioni, Modifica attributi.
5. Nella pagina Edit load balancer attributes (Modifica attributi del sistema di bilanciamento del carico) deseleziona Enable (Abilita) in Delete Protection (Elimina protezione) e poi scegli Save (Salva).

Per abilitare o disabilitare la protezione da eliminazione utilizzando il AWS CLI

Utilizza il comando [modify-load-balancer-attributes](#) con l'attributo `deletion_protection.enabled`.

Bilanciamento del carico su più zone

Per impostazione predefinita, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra i target registrati nella zona di disponibilità del sistema. Se attivi il bilanciamento del carico su più zone, ogni Gateway Load Balancer distribuisce le richieste nelle destinazioni registrate in tutte le zone di disponibilità attivate. Per ulteriori informazioni, consulta [Bilanciamento del carico su più zone](#) nella Guida per l'utente di Elastic Load Balancing.

Per abilitare il bilanciamento del carico su più zone utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Gateway Load Balancer.
4. Seleziona Operazioni, Modifica attributi.
5. Nella pagina Modifica gli attributi del sistema di bilanciamento del carico, seleziona Abilita per Bilanciamento del carico tra zone, quindi seleziona Salva.

Per abilitare il bilanciamento del carico tra zone utilizzando il AWS CLI

Utilizza il comando [modify-load-balancer-attributes](#) con l'attributo `load_balancing.cross_zone.enabled`.

Flussi asimmetrici

I Gateway Load Balancer supportano flussi asimmetrici quando il sistema di bilanciamento del carico elabora il pacchetto di flusso iniziale e il pacchetto di flusso di risposta non viene instradato attraverso il sistema di bilanciamento del carico. Il routing asimmetrico non è consigliato, in quanto può comportare una riduzione delle prestazioni di rete. I Gateway Load Balancer non supportano flussi asimmetrici quando il sistema di bilanciamento del carico non elabora il pacchetto di flusso iniziale e il pacchetto di flusso di risposta viene instradato attraverso il sistema di bilanciamento del carico.

Tempo di inattività

I Gateway Load Balancer supportano il timeout di inattività sia per i flussi TCP che per quelli non TCP.

- Il timeout di inattività per i flussi TCP è 350 secondi.
- Il timeout di inattività per i flussi non TCP è 120 secondi.

Nota: i valori di timeout di inattività per Gateway Load Balancer sono statici e non possono essere modificati.

Crea un Gateway Load Balancer

Un Gateway Load Balancer accetta richieste dai client e le distribuisce nei target di un gruppo target, ad esempio nelle istanze EC2.

Per creare un Gateway Load Balancer utilizzando AWS Management Console, completare le seguenti attività.

Attività

- [Prerequisiti](#)
- [Creazione del sistema di bilanciamento del carico](#)
- [Fasi successive importanti](#)

In alternativa, per creare un Gateway Load Balancer utilizzando il AWS CLI, vedere. [Nozioni di base per l'utilizzo della CLI](#)

Prerequisiti

Prima di iniziare, accertati che il cloud privato virtuale (VPC) per il tuo Gateway Load Balancer disponga di almeno una sottorete in ciascuna zona di disponibilità in cui si dispone di destinazioni.

Creazione del sistema di bilanciamento del carico

Utilizza la procedura seguente per creare il Gateway Load Balancer. Fornisci alcune informazioni di configurazione di base per il sistema di bilanciamento del carico, ad esempio un nome e un tipo di indirizzo IP. Successivamente, fornisci alcune informazioni relative alla rete e all'ascoltatore che indirizza il traffico verso le istanze. I Gateway Load Balancer richiedono gruppi di destinazione che utilizzano il protocollo GENEVE.

Per creare il load balancer e il listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.

2. Nel riquadro di navigazione, in Load Balancing (Load balancer), scegliere Load Balancers (Load balancer).
3. Selezionare Create Load Balancer (Crea sistema di bilanciamento del carico).
4. Sotto a Gateway Load Balancer scegli Crea.
5. Configurazione di base
 - a. In Nome del sistema di bilanciamento del carico immetti un nome univoco per il sistema di bilanciamento del carico. Ad esempio, **my-g1b**. Il nome del Gateway Load Balancer deve essere univoco all'interno del set di sistemi di bilanciamento del carico per la regione. I nomi possono avere un massimo di 32 caratteri e contenere solo caratteri alfanumerici e trattini. Inoltre non devono iniziare o finire con un carattere di sottolineatura.
 - b. Per tipo di indirizzo IP, seleziona IPv4 per supportare solo gli indirizzi IPv4, oppure Dualstack per supportare entrambi gli indirizzi IPv4 e IPv6.
6. Mappatura della rete
 - a. Per VPC, seleziona il VPC del fornitore del servizio.
 - b. Per le Mappature, seleziona tutte le zone di disponibilità in cui sono state avviate le istanze delle appliance di sicurezza e le sottoreti pubbliche corrispondenti.
7. Routing dell'ascoltatore IP
 - a. Per Azione predefinita, seleziona il gruppo di destinazione per ricevere il traffico. Se non hai un gruppo di destinazione, scegli Crea un gruppo di destinazione. Per ulteriori informazioni, consulta [Creazione di un gruppo target](#).
 - b. (Facoltativo) Espandi Tag dell'ascoltatore e aggiungi i tag di cui hai bisogno.
8. (Facoltativo) Espandi Tag del sistema di bilanciamento del carico e aggiungi i tag di cui hai bisogno.
9. Controlla la configurazione e scegli Crea sistema di bilanciamento del carico.

Fasi successive importanti

Dopo aver creato il sistema di bilanciamento del carico, verifica che le istanze EC2 abbiano superato il controllo dell'integrità iniziale. Per testare il sistema di bilanciamento del carico, devi creare un endpoint del Gateway Load Balancer e aggiornare la tabella di routing per fare in modo che l'endpoint del Gateway Load Balancer sia la fase successiva. Queste configurazioni sono impostate all'interno della console Amazon VPC. Per maggiori informazioni, vedi il tutorial [Nozioni di base](#).

Tipi di indirizzi IP per il tuo Gateway Load Balancer

È possibile configurare il Gateway Load Balancer in modo che i server delle applicazioni possano accedere al sistema di bilanciamento del carico utilizzando solo indirizzi IPv4 o utilizzando entrambi gli indirizzi IPv4 e IPv6 (dualstack). Il sistema di bilanciamento del carico comunica con le destinazioni in base al tipo di indirizzo IP del gruppo di destinazione. Per ulteriori informazioni, consulta [Tipo di indirizzo IP](#).

Per impostare il tipo di indirizzo IP al momento della creazione

Configura le impostazioni come descritto in [???](#).

Per aggiornare il tipo di indirizzo IP utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, sotto Load Balancing (Bilanciamento del carico), scegli Load Balancers (Load balancer).
3. Selezionare il load balancer.
4. Scegli Actions (Azioni), Edit IP address type (Modifica tipo di indirizzo IP).
5. In IP address type (Tipo di indirizzo IP), seleziona ipv4 per supportare i soli indirizzi IPv4 oppure dualstack per supportare sia gli indirizzi IPv4 che IPv6.
6. Selezionare Salva.

Per aggiornare il tipo di indirizzo IP utilizzando il AWS CLI

Utilizza il comando [set-ip-address-type](#).

Tag per il Gateway Load Balancer

I tag ti aiutano a classificare i bilanciatori del carico in modi diversi, ad esempio in base a scopo, proprietario o ambiente.

È possibile aggiungere più tag a ciascun sistema di bilanciamento del carico. Le chiavi dei tag devono essere univoche per ogni Gateway Load Balancer. Se aggiungi un tag con una chiave già associata al load balancer, il valore del tag viene aggiornato.

Quando il tag non è più necessario, è possibile eliminarlo dal Gateway Load Balancer.

Restrizioni

- Numero massimo di tag per risorsa: 50
- Lunghezza massima della chiave: 127 caratteri Unicode
- Lunghezza massima del valore: 255 caratteri Unicode
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali.
- Non utilizzate il `aws :` prefisso nei nomi o nei valori dei tag perché è riservato all' AWS uso. Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Per aggiornare i tag di un Gateway Load Balancer tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Gateway Load Balancer.
4. Scegliere Tags (Tag), Add/Edit Tags (Aggiungi/modifica tag) e quindi eseguire una o più delle operazioni seguenti:
 - a. Per aggiornare un tag, modificare i valori di Chiave e Valore.
 - b. Per aggiungere un nuovo tag, scegliere Create Tag (Crea tag). Digita un valore per Chiave e Valore.
 - c. Per eliminare un tag, scegliere l'icona di eliminazione (X) accanto al tag.
5. Una volta completato l'aggiornamento dei tag, scegli Salva.

Per aggiornare i tag per un Gateway Load Balancer utilizzando il AWS CLI

Utilizza i comandi [add-tags](#) e [remove-tags](#).

Elimina un Gateway Load Balancer

Non appena il Gateway Load Balancer diventa disponibile, ti verrà addebitata ogni ora o frazione di ora in cui lo mantieni in esecuzione. Se il Gateway Load Balancer non ti è più utile, puoi eliminarlo. Non appena il Gateway Load Balancer viene eliminato, i relativi addebiti vengono bloccati.

Non è possibile eliminare un Gateway Load Balancer, se è in uso da un altro servizio. Ad esempio, se il Gateway Load Balancer è associato a un servizio endpoint VPC, è necessario eliminare la configurazione del servizio endpoint prima di poter eliminare il Gateway Load Balancer associato.

L'eliminazione di un Gateway Load Balancer elimina anche i relativi ascoltatori. L'eliminazione di un Gateway Load Balancer non influisce sulle relative destinazioni registrate. Ad esempio, le istanze EC2 proseguono l'esecuzione e sono comunque registrate nei loro gruppi target. Per eliminare i gruppi target, consulta [Eliminazione di un gruppo target](#).

Eliminare un Gateway Load Balancer tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Gateway Load Balancer.
4. Scegli Operazioni > Elimina.
5. Quando viene richiesta la conferma, seleziona Sì, elimina.

Per eliminare un Gateway Load Balancer utilizzando il AWS CLI

Utilizza il comando [delete-load-balancer](#).

Ascoltatori dei Gateway Load Balancer

Quando crei il tuo Gateway Load Balancer, aggiungi un ascoltatore. Si definisce listener il processo che verifica la presenza di richieste di connessione.

Gli ascoltatori per Gateway Load Balancer ascoltano tutti i pacchetti IP su tutte le porte. Non è possibile specificare un protocollo o una porta quando si crea un ascoltatore per un Gateway Load Balancer.

Quando si crea un listener, è necessario specificare una regola per instradare le richieste. Questa regola inoltra le richieste verso il gruppo target indicato. È possibile aggiornare la regola dell'ascoltatore per inoltrare le richieste a un gruppo target diverso.

Per aggiornare il listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Selezionare il sistema del bilanciamento del carico e scegliere Listeners (Listener).
4. Scegli Modifica ascoltatore.
5. Per l'Inoltro al gruppo di destinazione, scegli un gruppo di destinazione.
6. Selezionare Salva.

Per aggiornare il tuo ascoltatore usando AWS CLI

Utilizza il comando [modify-listener](#).

Quota per i Gateway Load Balancer

Ogni gruppo target viene utilizzato per instradare le richieste a uno o più target registrati. Quando si crea un listener, si specifica un gruppo di destinazione per l'operazione predefinita. Il traffico viene inoltrato al gruppo di destinazione specificato nella regola dell'ascoltatore. È possibile creare diversi gruppi target per diversi tipi di richieste.

È possibile definire le impostazioni di controllo dell'integrità per il Gateway Load Balancer per ciascun gruppo target. Ogni gruppo target utilizza le impostazioni di controllo dello stato predefinite, a meno che non vengano sostituite al momento della creazione del gruppo target o modificate in un secondo momento. Dopo aver specificato un gruppo target in una regola per un ascoltatore, il Gateway Load Balancer monitora continuamente lo stato di tutti i target registrati con il gruppo di destinazione che si trovano in una zona di disponibilità abilitata per il Gateway Load Balancer. Il Gateway Load Balancer instrada le richieste alle destinazioni registrate con stato integro. Per ulteriori informazioni, consulta [Controlli dello stato per i gruppi target](#).

Indice

- [Configurazione dell'instradamento](#)
- [Target type \(Tipo di destinazione\)](#)
- [Destinazioni registrate](#)
- [Attributi dei gruppi di destinazione](#)
- [Ritardo di annullamento della registrazione](#)
- [Failover della destinazione](#)
- [Persistenza del flusso](#)
- [Creare un gruppo di destinazione per il Gateway Load Balancer](#)
- [Controlli dello stato per i gruppi target](#)
- [Registrazione di destinazioni con il gruppo target](#)
- [Tag per il gruppo target](#)
- [Eliminazione di un gruppo target](#)

Configurazione dell'instradamento

I gruppi di destinazione per Gateway Load Balancer supportano i seguenti protocolli e porte:

- Protocollo: GENEVE
- Porta: 6081

Target type (Tipo di destinazione)

Quando crei un gruppo target, devi specificare il tipo di target, che determina come vengono specificati i relativi oggetti target. Dopo aver creato un gruppo target, non è possibile modificarne il tipo di target.

I tipi di target possibili sono i seguenti:

`instance`

I target vengono specificati in base all'ID istanza.

`ip`

I target vengono specificati in base all'indirizzo IP.

Quando il tipo di target è `ip`, è possibile specificare gli indirizzi IP da uno dei blocchi CIDR seguenti:

- Sottoreti del VPC per il gruppo target
- 10.0.0.0/8 ([RFC 1918](#))
- 100.64.0.0/10 ([RFC 6598](#))
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Important

Non è possibile specificare indirizzi IP instradabili pubblicamente.

Destinazioni registrate

Il Gateway Load Balancer funge da singolo punto di contatto per i client e distribuisce il traffico in entrata tra le destinazioni registrati con stato integro. Ogni gruppo target deve avere almeno un

target registrato in ciascuna zona di disponibilità abilitata per il Gateway Load Balancer. È possibile registrare ogni target con uno o più gruppi target.

Se il carico di richieste per l'applicazione aumenta, puoi registrare destinazioni aggiuntive con uno o più gruppi di destinazione al fine di gestire le richieste. Il Gateway Load Balancer inizia a instradare il traffico a un nuovo target registrato non appena viene completato il processo di registrazione.

Se il carico di richieste diminuisce o devi eseguire la manutenzione delle destinazioni, puoi annullare la loro registrazione dai gruppi target. L'annullamento della registrazione di un target rimuove il target dal gruppo target, ma non influisce in altro modo sul target stesso. Il Gateway Load Balancer arresta l'instradamento del traffico a una destinazione non appena la sua registrazione viene annullata. Il target passa allo stato `draining` fino a quando non vengono completate le richieste in transito. Puoi registrare di nuovo il target con il gruppo target quando è possibile riprendere la ricezione del traffico.

Attributi dei gruppi di destinazione

Puoi utilizzare i seguenti attributi con i gruppi di destinazione:

`deregistration_delay.timeout_seconds`

La quantità di tempo che Elastic Load Balancing attende prima di modificare lo stato di un target di cui viene annullata la registrazione da `draining` a `unused`. L'intervallo è compreso tra 0 e 3600 secondi. Il valore predefinito è 300 secondi.

`stickiness.enabled`

Indica se la persistenza configurabile del flusso è abilitata per il gruppo di destinazione. I valori possibili sono `true` o `false`. Il valore predefinito è `false`. Quando l'attributo è impostato su `false`, viene utilizzato `5_tuple`.

`stickiness.type`

Indica il tipo di persistenza del flusso. I valori possibili per i gruppi di destinazione associati a Gateway Load Balancers sono:

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Indica il modo in cui il Gateway Load Balancer gestisce i flussi esistenti quando viene annullata la registrazione di una destinazione. I valori possibili sono `rebalance` e `no_rebalance`. Il

valore di default è `no_rebalance`. I due attributi (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) non possono essere impostati separatamente. Il valore impostato per entrambi gli attributi deve essere lo stesso.

`target_failover.on_unhealthy`

Indica il modo in cui il Gateway Load Balancer gestisce i flussi esistenti quando una destinazione non è integra. I valori possibili sono `rebalance` e `no_rebalance`. Il valore di default è `no_rebalance`. I due attributi (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) non possono essere impostati separatamente. Il valore impostato per entrambi gli attributi deve essere lo stesso.

Ritardo di annullamento della registrazione

Quando si annulla la registrazione di una destinazione, il Gateway Load Balancer gestisce i flussi verso tale destinazione nel modo seguente:

Nuovi flussi

Il Gateway Load Balancer interrompe l'invio di nuovi flussi.

Flussi esistenti

Il Gateway Load Balancer gestisce i flussi esistenti in base al protocollo:

- TCP: i flussi esistenti vengono chiusi se rimangono inattivi per più di 350 secondi.
- Altri protocolli: i flussi esistenti vengono chiusi se rimangono inattivi per più di 120 secondi.

Per favorire il drenaggio dei flussi esistenti, puoi abilitare il riequilibrio dei flussi per il tuo gruppo di destinazione. Per ulteriori informazioni, consulta [the section called “Failover della destinazione”](#).

Un obiettivo annullato indica che è `draining` fino alla scadenza del timeout. Dopo la scadenza del timeout, la destinazione passa allo stato `unused`.

Per aggiornare il valore di ritardo dell'annullamento della registrazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.

4. Nella pagina Dettagli del gruppo, all'interno della Attributi, scegliere Modifica.
5. Nella pagina Modifica attributi, modificare il valore di Intervallo annullamento registrazione secondo necessità.
6. Seleziona Salvataggio delle modifiche.

Per aggiornare il valore del ritardo di annullamento della registrazione utilizzando il AWS CLI

Utilizza il comando [modify-target-group-attributes](#).

Failover della destinazione

Con il failover della destinazione, si specifica il modo in cui il Gateway Load Balancer gestisce i flussi di traffico esistenti dopo che una destinazione diventa non integra o quando viene annullata la registrazione della destinazione. Per impostazione predefinita, il Gateway Load Balancer continua a inviare flussi esistenti alla stessa destinazione, anche se la destinazione ha avuto esito negativo o è stata annullata la registrazione. È possibile gestire questi flussi eseguendone un nuovo hashing (rebalance) o lasciandoli allo stato predefinito (no_rebalance).

Nessun ribilanciamento:

Il Gateway Load Balancer continua a inviare i flussi esistenti a destinazioni non integre o esaurite. Tuttavia, i nuovi flussi vengono inviati a destinazioni integre. Questo è il comportamento che segue di default.

Ribilanciamento:

Il Gateway Load Balancer rielabora i flussi esistenti e li invia a destinazioni integre dopo il timeout del ritardo di annullamento della registrazione.

Per le destinazioni annullate, il tempo minimo di failover dipenderà dal ritardo di annullamento della registrazione. La destinazione non viene contrassegnata come annullata fino al completamento del ritardo di annullamento della registrazione.

Per le destinazioni non integre, il tempo minimo di failover dipenderà dalla configurazione del controllo dello stato del gruppo di destinazione (soglia dei tempi di intervallo). Si tratta del periodo minimo prima del quale una destinazione viene contrassegnata come non integro. Trascorso questo periodo, il Gateway Load Balancer può impiegare diversi minuti a causa del tempo di propagazione aggiuntivo e del backoff della ritrasmissione TCP prima di reindirizzare i nuovi flussi verso destinazioni integre.

Per aggiornare il valore di failover di destinazione utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, modifica il valore di Failover della destinazione secondo necessità.
6. Seleziona Salvataggio delle modifiche.

Per aggiornare il valore di failover di destinazione utilizzando il AWS CLI

Utilizza il comando [modify-target-group-attributes](#), con le seguenti coppie chiave-valore:

- Chiave=`target_failover.on_deregistration` e Valore= `no_rebalance` (predefinito) o `rebalance`
- Chiave=`target_failover.on_unhealthy` e Valore= `no_rebalance` (predefinito) o `rebalance`

Note

Entrambi gli attributi (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) devono avere lo stesso valore.

Persistenza del flusso

Per impostazione predefinita, il Gateway Load Balancer mantiene la persistenza dei flussi verso un'appliance di destinazione specifica utilizzando 5-tuple (per flussi TCP/UDP). La 5-tuple include l'IP di origine, la porta di origine, l'IP di destinazione, la porta di destinazione e il protocollo di trasporto. È possibile utilizzare l'attributo di tipo di persistenza e per modificare l'impostazione predefinita (5-tuple) e scegliere 3-tuple (IP di origine, IP di destinazione e protocollo di trasporto) o 2-tuple (IP di origine e IP di destinazione).

Considerazioni sulla persistenza del flusso

- La persistenza del flusso viene configurata e applicata a livello di gruppo di destinazione e si applica a tutto il traffico diretto al gruppo di destinazione.
- La persistenza del flusso a 2-tuple e 3-tuple non è supportata quando la modalità appliance AWS Transit Gateway è attivata. Per utilizzare la modalità appliance sul tuo Gateway Load Balancer AWS Transit Gateway, utilizza la stabilità del flusso a 5 tuple
- La persistenza del flusso può portare a una distribuzione non uniforme di connessioni e flussi, che potrebbe influire sulla disponibilità delle destinazioni. Si consiglia di terminare o svuotare tutti i flussi esistenti prima di modificare il tipo di persistenza del gruppo di destinazione.

Aggiornare la persistenza del flusso utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, modifica il valore di Persistenza del flusso secondo necessità.
6. Seleziona Salvataggio delle modifiche.

Per abilitare o modificare la persistenza del flusso utilizzando il AWS CLI

Utilizza il comando [modify-target-group-attributes](#) con gli attributi del gruppo di destinazione `stickiness.enabled` e `stickiness.type`.

Creare un gruppo di destinazione per il Gateway Load Balancer

Registra le destinazioni per il vostro Gateway Load Balancer utilizzando un gruppo di destinazione.

Per instradare il traffico verso i target in un gruppo target, crea un listener e specifica il gruppo target nell'operazione predefinita per il listener. Per ulteriori informazioni, consulta [Listener](#).

È possibile aggiungere o rimuovere target dal gruppo target in qualsiasi momento. Per ulteriori informazioni, consulta [Registrazione di destinazioni](#). È anche possibile modificare le impostazioni di controllo dello stato per il gruppo target. Per ulteriori informazioni, consulta [Modifica le impostazioni del controllo dell'integrità](#).

Per creare un gruppo target tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Scegliere Crea gruppo target.
4. Configurazione di base
 - a. Per Scegli un tipo di destinazione, seleziona Istanze per specificare le destinazioni per ID dell'istanza, oppure seleziona Indirizzi IP per specificare le destinazioni per indirizzo IP.
 - b. Per Nome del gruppo di destinazione, inserisci un nome per il gruppo di destinazione. Questo nome deve essere unico per regione per ogni account, può avere un massimo di 32 caratteri, deve contenere solo caratteri alfanumerici o trattini e non deve iniziare o terminare con un trattino.
 - c. Verifica che il protocollo sia GENEVE e che la porta sia 6081. Non sono supportati altri protocolli o porte.
 - d. Per VPC, seleziona il cloud privato virtuale (VPC) con le istanze dell'appliance di sicurezza da includere nel gruppo di destinazione.
5. (Facoltativo) Per Controlli dell'integrità, modifica le impostazioni e le impostazioni avanzate secondo necessità. Se i controlli dell'integrità eccedono in modo consecutivo la Soglia di non integrità, il sistema di bilanciamento del carico considererà la destinazione fuori servizio. Se durante i controlli dell'integrità il numero di successi consecutivi supera la Soglia di integrità, il sistema di bilanciamento del carico considererà la destinazione nuovamente in servizio. Per ulteriori informazioni, consulta [Controlli dello stato per i gruppi target](#).
6. (Facoltativo) Espandi Tag e aggiungi i tag di cui hai bisogno.
7. Seleziona Successivo.
8. Per Registra destinazioni aggiungi una o più destinazioni come segue:
 - Se il tipo di destinazione è Istanze, seleziona una o più istanze, inserisci una o più porte e in seguito scegli Includi come in sospenso di seguito.
 - Se il tipo di destinazione è Indirizzi IP, seleziona la rete, inserisci indirizzo IP e porte, quindi seleziona Includi come in sospenso di seguito.
9. Scegliere Crea gruppo target.

Per creare un gruppo target utilizzando il AWS CLI

Utilizza il comando [create-target-group](#) per creare il gruppo target, il comando [add-tags](#) per aggiungere un tag al gruppo target e il comando [register-targets](#) per aggiungere target.

Controlli dello stato per i gruppi target


È possibile registrare i target con uno o più gruppi target. Il Gateway Load Balancer inizia a instradare le richieste a un nuovo target registrato non appena viene completato il processo di registrazione. Il completamento del processo di registrazione e l'avvio dei controlli dell'integrità possono richiedere alcuni minuti.

Il Gateway Load Balancer invia periodicamente una richiesta ad ogni destinatario registrato per controllare lo stato. Dopo il completamento di ciascun controllo dell'integrità, il Gateway Load Balancer chiude la connessione definita per il controllo dello stato.

Impostazioni del controllo dello stato

È possibile configurare controlli dell'integrità attivi per i target in un gruppo target utilizzando le seguenti impostazioni. Se i controlli di integrità superano il numero specificato di errori `UnhealthyThresholdCountconsecutivi`, il Gateway Load Balancer mette fuori servizio il target. Quando i controlli di integrità superano il numero specificato di successi `HealthyThresholdCountconsecutivi`, il Gateway Load Balancer rimette l'obiettivo in servizio.

Impostazione	Descrizione
<code>HealthCheckProtocol</code>	Il protocollo utilizzato dal sistema di bilanciamento del carico durante l'esecuzione dei controlli dell'integrità sulle destinazioni. I protocolli possibili sono HTTP, HTTPS e TCP. Il valore predefinito è TCP.
<code>HealthCheckPort</code>	La porta utilizzata dal Gateway Load Balancer durante l'esecuzione dei controlli dell'integrità sulle destinazioni. L'intervallo è compreso tra 1 e 65535. Il predefinito è 80.
<code>HealthCheckPath</code>	[Controlli di integrità HTTP/HTTPS] Il percorso dei controlli di integrità che è la destinazione

Impostazione	Descrizione
	degli obiettivi per i controlli sanitari. Il valore di default è /.
HealthCheckTimeoutSeconds	Il periodo di tempo, in secondi, durante il quale l'assenza di risposta da un target indica che un controllo dello stato non è riuscito. L'intervallo è compreso tra 2 e 120. Il predefinito è 5.
HealthCheckIntervalSeconds	<p>Il periodo di tempo approssimativo, in secondi, tra i controlli dell'integrità di una singola destinazione. L'intervallo è compreso tra 5 e 300. Il valore predefinito è 10 secondi. Questo valore deve essere maggiore o uguale a HealthCheckTimeoutSeconds</p> <div data-bbox="829 877 1507 1430" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>I controlli dell'integrità per i Gateway Load Balancer vengono distribuiti e utilizzano un meccanismo di consenso per determinare l'integrità della destinazione. Pertanto, è necessario aspettarsi che i dispositivi di destinazione ricevano diversi controlli dell'integrità entro l'intervallo di tempo configurato.</p></div>
HealthyThresholdCount	Il numero di controlli dello stato andati a buon fine consecutivi necessari prima di considerare integro un target non integro. L'intervallo è compreso tra 2 e 10. Il predefinito è 5.

Impostazione	Descrizione
UnhealthyThresholdCount	Numero di controlli dello stato consecutivi non andati a buon fine necessari prima di considerare un target non integro. L'intervallo è compreso tra 2 e 10. Il valore predefinito è 2.
Matcher	[Controlli dello stato HTTP/HTTPS] I codici HTTP da utilizzare durante la verifica di una risposta con esito positivo ricevuta da un target. Questo valore deve essere 200-399.

Stato di integrità della destinazione

Prima che il Gateway Load Balancer invii una richiesta di controllo dell'integrità a una destinazione, è necessario registrarlo con un gruppo di destinazione, specificare il gruppo di destinazione in una regola dell'ascoltatore e assicurarsi che la zona di disponibilità del target sia abilitata per il Gateway Load Balancer.

La tabella seguente descrive i valori possibili per lo stato di un target registrato.

Valore	Descrizione
<code>initial</code>	È in corso il processo di registrazione della destinazione o di esecuzione dei controlli dello stato iniziali della destinazione da parte del Gateway Load Balancer. Codici di motivo correlati: <code>Elb.RegistrationInProgress</code> <code>Elb.InitialHealthChecking</code>
<code>healthy</code>	Il target è integro. Codici di motivo correlati: Nessuno
<code>unhealthy</code>	Il target non ha risposto a un controllo di stato o il controllo dello stato non è andato a buon fine.

Valore	Descrizione
	Codice di motivo correlato: <code>Target.FailedHealthChecks</code>
<code>unused</code>	<p>La destinazione non è registrata con un gruppo di destinazione, il gruppo di destinazione non è utilizzato in una regola del listener, la destinazione è in una zona di disponibilità non abilitata oppure è nello stato arrestato o terminato.</p> <p>Codici di motivo correlati: <code>Target.NotRegistered</code> <code>Target.NotInUse</code> <code>Target.InvalidState</code> <code>Target.IpUnusable</code></p>
<code>draining</code>	<p>Il target viene revocato e la connection draining è in corso.</p> <p>Codice di motivo correlato: <code>Target.DeregistrationInProgress</code></p>
<code>unavailable</code>	<p>Lo stato della destinazione non è disponibile.</p> <p>Codice di motivo correlato: <code>Elb.InternalError</code></p>

Codici di motivo di controllo dello stato

Se lo stato di una destinazione è un valore diverso da `Healthy`, l'API restituisce un codice di motivo e una descrizione del problema e la console visualizza la stessa descrizione. I codici di motivo che iniziano con `Elb` vengono creati nella parte relativa al Gateway Load Balancer e i codici di motivo che iniziano con `Target` vengono creati nella parte relativa ai target.

Codice di motivo	Descrizione
<code>Elb.InitialHealthChecking</code>	Controlli dello stato iniziali in corso
<code>Elb.InternalError</code>	I controlli dello stato non andati a buon fine a causa di un errore interno

Codice di motivo	Descrizione
Elb.RegistrationInProgress	La registrazione del target è in corso
Target.DeregistrationInProgress	La revoca del target è in corso
Target.FailedHealthChecks	Controlli dello stato non andati a buon fine
Target.InvalidState	La destinazione è in stato di arresto La destinazione è in stato terminato I target sono in stato di arresto o terminato Il target è in uno stato non valido
Target.IpUnusable	L'indirizzo IP non può essere utilizzato come destinazione, poiché è in uso in un sistema di bilanciamento del carico.
Target.NotInUse	Il gruppo di destinazione non è configurato per la ricezione del traffico dal Gateway Load Balancer. Il target si trova in una zona di disponibilità che non è abilitata per il Gateway Load Balancer
Target.NotRegistered	Il target non è registrato nel gruppo target

Scenari di errore della destinazione del Gateway Load Balancer

Flussi esistenti: per impostazione predefinita, i flussi esistenti vanno alla stessa destinazione a meno che il flusso non scada o non venga ripristinato, indipendentemente dallo stato di integrità e di registrazione del target. Questo approccio facilita lo svuotamento della connessione e supporta firewall di terze parti che a volte non sono in grado di rispondere ai controlli dell'integrità a causa dell'elevato utilizzo della CPU. Per ulteriori informazioni, consulta [Target failover](#).

Nuovi flussi: i nuovi flussi vengono inviati a una destinazione integra. Una volta presa una decisione di bilanciamento del carico per un flusso, il Gateway Load Balancer invierà il flusso alla stessa destinazione anche se non integra o in presenza di altre destinazioni integre.

Quando tutti le destinazioni non sono integre, il Gateway Load Balancer sceglie una destinazione casuale e inoltra il traffico per l'intera durata del flusso, fino a quando non viene ripristinato o non scade il timeout. Poiché il traffico viene inoltrato a una destinazione non integra, il traffico viene interrotto finché tale destinazione non ricomincia a funzionare.

TLS 1.3: se un gruppo di destinazione è configurato con i controlli di integrità HTTPS, le destinazioni registrate non superano i controlli di integrità se supportano solo TLS 1.3. Queste destinazioni devono supportare una versione precedente di TLS, come TLS 1.2.

Bilanciamento del carico del carico tra zone: per impostazione predefinita, il bilanciamento del carico tra le zone di disponibilità è disabilitato. Se il bilanciamento del carico tra le zone è abilitato, ogni Gateway Load Balancer è in grado di vedere tutte le destinazioni in tutte le zone di disponibilità e vengono tutte trattate allo stesso modo, indipendentemente dalla zona.

Le decisioni relative al bilanciamento del carico e al controllo dell'integrità sono sempre indipendenti tra le zone. Anche quando il bilanciamento del carico tra le zone è abilitato, il comportamento dei flussi esistenti e dei nuovi flussi è lo stesso descritto sopra. Per ulteriori informazioni, consulta [Bilanciamento del carico su più zone](#) nella Guida per l'utente di Elastic Load Balancing.

Controllo dello stato delle destinazioni

È possibile controllare lo stato dei target registrato con i gruppi target.

Per controllare lo stato dei target utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Target, la colonna Stato indica lo stato di ogni destinazione.
5. Se lo stato di destinazione è un valore diverso da Healthy, la colonna Dettagli dello stato contiene ulteriori informazioni.

Per verificare lo stato di salute dei tuoi bersagli, utilizza il AWS CLI

Utilizza il comando [describe-target-health](#). L'output di questo comando contiene lo stato del target. Include un codice di motivo, se lo stato è un valore diverso da Healthy.

Per ricevere notifiche via e-mail su destinazioni non integre

Usa gli CloudWatch allarmi per attivare una funzione Lambda per inviare dettagli su obiettivi non sani. Per step-by-step istruzioni, consulta il seguente post sul blog: [Identificazione degli obiettivi non integri del sistema di bilanciamento del carico](#).

Modifica le impostazioni del controllo dell'integrità

È anche possibile modificare alcune delle impostazioni di controllo dello stato per il gruppo target.

Per modificare le impostazioni di controllo dello stato per un gruppo target utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Dettagli del gruppo, nella sezione Impostazioni del controllo dell'integrità, scegli Modifica.
5. Nella pagina Modifica le impostazioni del controllo dell'integrità, modificare le impostazioni secondo necessità, quindi scegliere Salva modifiche.

Per modificare le impostazioni del controllo dello stato di salute per un gruppo target utilizzando il AWS CLI

Utilizza il comando [modify-target-group](#).

Registrazione di destinazioni con il gruppo target

Quando la destinazione è pronta per gestire le richieste, è possibile registrarla con uno o più gruppi di destinazione. È possibile registrare i target in base a ID istanza o indirizzo IP. Il Gateway Load balancer inizia a instradare le richieste alla destinazione non appena viene completato il processo di registrazione e la destinazione supera i controlli dell'integrità iniziali. Il completamento del processo di registrazione e l'avvio dei controlli dello stato può richiedere alcuni minuti. Per ulteriori informazioni, consulta [Controlli dello stato per i gruppi target](#).

Se il carico di richieste per i target attualmente registrati aumenta, puoi registrare target aggiuntivi al fine di gestire le richieste. Se la richiesta sulle destinazioni registrate diminuisce, è possibile annullare

la registrazione delle destinazioni dal gruppo di destinazione. Il completamento del processo di annullamento della registrazione e l'interruzione delle richieste di instradamento alla destinazione da parte del Gateway Load balancer può richiedere alcuni minuti. Se successivamente la domanda aumenta, è possibile registrare nuovamente le destinazioni di cui si era annullata la registrazione con il gruppo di destinazione. Se è necessario eseguire la manutenzione di una destinazione, è possibile annullarne la registrazione e registrarla nuovamente al termine della manutenzione.

Quando annulli la registrazione di una destinazione, Elastic Load Balancing attende il completamento delle richieste in transito. Questo comportamento è noto come Connection Draining. Lo stato di un target è `draining` durante la fase di Connection Draining. Una volta completata l'annullamento della registrazione, lo stato del target diventa `unused`. Per ulteriori informazioni, consulta [Ritardo di annullamento della registrazione](#).

Gruppi di sicurezza target

Quando esegui la registrazione delle istanze EC2 come destinazione, devi assicurarti che i gruppi di sicurezza per queste istanze permettano il traffico in ingresso e in uscita sulla porta 6081.

I Gateway Load Balancer non hanno gruppi di sicurezza associati. Pertanto, i gruppi di sicurezza per i target devono utilizzare gli indirizzi IP per permettere il traffico dal sistema di bilanciamento del carico.

Liste di controllo accessi (ACL) di rete

Quando esegui la registrazione delle istanze EC2 come destinazione, devi assicurarti che le liste di controllo degli accessi (ACL) di rete per le sottoreti delle istanze permettano il traffico sulla porta 6081. L'ACL di rete predefinita per un VPC consente tutto il traffico in entrata e in uscita. Se crei liste di controllo accessi di rete personalizzate, verifica che consentano il traffico appropriato.

Registrazione o annullamento della registrazione di destinazioni

Ogni di destinazione deve avere almeno una destinazione registrata in ciascuna zona di disponibilità abilitata per il Gateway Load Balancer.

Il tipo di destinazione del gruppo di destinazioni determina il modo in cui si registrano le destinazioni con quel gruppo di destinazioni. Per ulteriori informazioni, consulta [Target type \(Tipo di destinazione\)](#).

Requisiti

- Non puoi registrare obiettivi tramite un peering VPC interregionale.

- Non puoi registrare istanze per ID di istanza su un peering VPC interregionale, ma puoi registrarle tramite indirizzo IP.

Indice

- [Registrazione o annullamento della registrazione di destinazioni in base all'ID istanza](#)
- [Registrazione o annullamento della registrazione di destinazioni in base all'indirizzo IP](#)
- [Registrazione o annullamento della registrazione di destinazioni tramite l' AWS CLI](#)

Registrazione o annullamento della registrazione di destinazioni in base all'ID istanza

Quando viene registrata, un'istanza deve essere nello stato `running`.

Per registrare le destinazioni o annullarne la registrazione in base all'ID istanza tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Per registrare le istanze, seleziona Registra destinazioni. Seleziona una o più istanze, quindi seleziona Includi come in sospenso di seguito. Dopo aver finito di aggiungere le istanze, seleziona Registra destinazioni in sospenso.
6. Per annullare la registrazione delle istanze, seleziona le istanze e poi scegli Annulla registrazione.

Registrazione o annullamento della registrazione di destinazioni in base all'indirizzo IP

Un indirizzo IP registrato deve provenire da uno dei seguenti blocchi CIDR:

- Sottoreti del VPC per il gruppo target
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Per registrare le destinazioni o annullarne la registrazione in base all'indirizzo IP tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Per registrare gli indirizzi IP, seleziona Registrare destinazioni. Per ogni indirizzo IP seleziona rete, zona di disponibilità, indirizzo IP e porta, quindi seleziona Includi come in sospeso di seguito. Dopo aver finito di specificare gli indirizzi, scegliere Registra destinazioni in sospeso.
6. Per annullare la registrazione degli indirizzi IP, seleziona gli indirizzi e scegliere Annulla registrazione. Se vi sono molti indirizzi IP registrati, può risultare utile aggiungere un filtro o modificare l'ordinamento.

Registrazione o annullamento della registrazione di destinazioni tramite l' AWS CLI

Utilizza il comando [register-targets](#) per aggiungere i target e il comando [deregister-targets](#) per rimuoverli.

Tag per il gruppo target

I tag ti aiutano a classificare i gruppi target in modi diversi, ad esempio in base a scopo, proprietario o ambiente.

È possibile aggiungere più tag a ciascun gruppo target. Le chiavi dei tag devono essere univoche per ogni gruppo target. Se aggiungi un tag con una chiave già associata al gruppo target, il valore del tag viene aggiornato.

Quando un tag non serve più, è possibile rimuoverlo.

Restrizioni

- Numero massimo di tag per risorsa: 50
- Lunghezza massima della chiave: 127 caratteri Unicode
- Lunghezza massima del valore: 255 caratteri Unicode
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali.

- Non utilizzate il aws : prefisso nei nomi o nei valori dei tag perché è riservato all'uso. AWS Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Per aggiornare i tag per un gruppo target tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Tag, scegli Aggiungi/modifica tag ed eseguire una o più delle operazioni seguenti:
 - a. Per aggiornare un tag, inserisci nuovi valori per Chiave e Valore.
 - b. Per aggiungere un tag, scegli Aggiungi tag e inserire valori per Chiave e Valore.
 - c. Per eliminare un tag, scegli Rimuovi accanto al tag.
5. Una volta completato l'aggiornamento dei tag, scegli Salva.

Per aggiornare i tag per un gruppo target utilizzando il AWS CLI

Utilizza i comandi [add-tags](#) e [remove-tags](#).

Eliminazione di un gruppo target

È possibile eliminare un gruppo di destinazione se non ci sono operazioni di inoltro di alcuna regola dell'ascoltatore che vi fanno riferimento. L'eliminazione di un gruppo target non influisce sui target registrati con il gruppo target. Se non hai più bisogno di un'istanza EC2 registrata, puoi arrestarla o terminarla.

Per eliminare un gruppo target tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Selezionare il gruppo target e scegliere Operazioni, Elimina.
4. Quando viene richiesta la conferma, seleziona Sì, elimina.

Per eliminare un gruppo target utilizzando il AWS CLI

Utilizza il comando [delete-target-group](#).

Monitora i Gateway Load Balancer

È possibile utilizzare le seguenti funzionalità per monitorare i Gateway Load Balancer per analizzare i modelli di traffico e risolvere i problemi. Tuttavia, il Gateway Load Balancer non genera log di accesso poiché è un sistema di bilanciamento del carico di livello 3 trasparente che non interrompe i flussi. Per ricevere i log di accesso, è necessario abilitare la registrazione degli accessi sulle appliance di destinazione del Gateway Load Balancer come firewall, IDS/IPS e appliance di sicurezza. Inoltre, puoi anche scegliere di abilitare i log di flusso VPC sui Gateway Load Balancer.

CloudWatch metriche

Puoi utilizzare Amazon CloudWatch per recuperare le statistiche sui punti dati per i tuoi Gateway Load Balancer e gli obiettivi sotto forma di set ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta [CloudWatch metriche per il tuo Gateway Load Balancer](#).

Log di flusso VPC

Puoi utilizzare i log di flusso VPC per acquisire informazioni dettagliate sul traffico in entrata e in uscita dal Gateway Load Balancer. Per ulteriori informazioni, consulta [Log di flusso VPC](#) nella Guida per l'utente di Amazon VPC.

Crea un log di flusso per ciascuna interfaccia di rete del Gateway Load Balancer. Esiste una sola interfaccia di rete per ogni sottorete. Per identificare le interfacce di rete di un Gateway Load Balancer, cerca il nome del Gateway Load Balancer nel campo descrizione dell'interfaccia di rete.

Per ogni connessione tramite Gateway Load Balancer sono disponibili due voci: una per la connessione front-end tra il client e il Gateway Load Balancer e l'altra per la connessione back-end tra il Gateway Load Balancer e la destinazione. Se il target è registrato dall'ID dell'istanza, la connessione appare sull'istanza come connessione dal client. Se il gruppo di sicurezza dell'istanza non consente le connessioni dal client ma queste sono permesse dalle liste di controllo degli accessi di rete della sottorete, i log dell'interfaccia di rete del Gateway Load Balancer mostrano "ACCEPT OK" per le connessioni front-end e back-end, mentre i log dell'interfaccia di rete dell'istanza mostrano "REJECT OK" per la connessione.

CloudTrail registri

Puoi utilizzarle AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate all'API Elastic Load Balancing e archivarle come file di registro in Amazon S3. È possibile

utilizzare questi CloudTrail registri per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata, quando è stata effettuata la chiamata e così via. Per ulteriori informazioni, consulta [Registrazione delle chiamate API per Gateway Load Balancer tramite AWS CloudTrail](#).

CloudWatch metriche per il tuo Gateway Load Balancer

Elastic Load Balancing pubblica punti dati su Amazon CloudWatch per i tuoi Gateway Load Balancer e i tuoi obiettivi. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a un parametro come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. Ad esempio, puoi monitorare il numero totale di target integri per un Gateway Load Balancer in un periodo di tempo specifico. 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 CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica non rientra in quello che consideri un intervallo accettabile.

Elastic Load Balancing riporta le metriche CloudWatch solo quando le richieste fluiscono attraverso il Gateway Load Balancer. Se ci sono delle richieste che passano, Elastic Load Balancing ne misura e invia i parametri a intervalli di 60 secondi. Se non vi sono richieste o in assenza di dati per un parametro, questa non viene segnalata.

Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

Indice

- [Parametri di Gateway Load Balancer](#)
- [Dimensioni di parametro per Gateway Load Balancer](#)
- [Visualizza le CloudWatch metriche per il tuo Gateway Load Balancer](#)

Parametri di Gateway Load Balancer

Lo spazio dei nomi AWS/GatewayELB include le metriche descritte di seguito.

Metrica	Descrizione
ActiveFlowCount	<p>Il numero totale di flussi simultanei (o connessioni) da client a target.</p> <p>Criteri di segnalazione: è presente un valore diverso da zero</p> <p>Statistiche: le statistiche più utili sono Average, Maximum e Minimum.</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
ConsumedLCUs	<p>Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico. Paghi per il numero di LCU che usi all'ora. Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing.</p> <p>Criteri di segnalazione: sempre segnalati</p> <p>Statistiche: tutte</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer
HealthyHostCount	<p>Il numero di target considerati integri.</p> <p>Criteri di segnalazione: segnalati se sono abilitati i controlli dello stato</p> <p>Statistiche: le statistiche più utili sono Maximum e Minimum.</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	<p>Il numero totale di nuovi flussi (o connessioni) stabiliti da client a target nel periodo di tempo.</p>

Metrica	Descrizione
	<p>Criteria di segnalazione: è presente un valore diverso da zero</p> <p>Statistiche: la statistica più utile è Sum.</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes	<p>Il numero totale di byte elaborati dal sistema di bilanciamento del carico. Questo conteggio include il traffico da e verso le destinazioni, ma non il traffico di controllo dell'integrità.</p> <p>Criteria di segnalazione: è presente un valore diverso da zero</p> <p>Statistiche: la statistica più utile è Sum.</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
UnHealthyHostCount	<p>Il numero di target considerati non integri.</p> <p>Criteria di segnalazione: segnalati se sono abilitati i controlli dello stato</p> <p>Statistiche: le statistiche più utili sono Maximum e Minimum.</p> <p>Dimensioni</p> <ul style="list-style-type: none"> • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup

Dimensioni di parametro per Gateway Load Balancer

Per filtrare i parametri relativi al tuo Gateway Load Balancer, usa le seguenti dimensioni.

Dimensione	Descrizione
AvailabilityZone	Consente di filtrare i dati del parametro per zona di disponibilità.
LoadBalancer	Consente di filtrare i dati del parametro per Gateway Load Balancer. Specificare il Gateway Load Balancer come segue: gateway/load-balancer-name/1234567890123456 (la parte finale dell'ARN).
TargetGroup	Consente di filtrare i dati del parametro per gruppo target. Specificare il gruppo target come segue: targetgroup/target-group-name/1234567890123456 (la parte finale dell'ARN del gruppo target).

Visualizza le CloudWatch metriche per il tuo Gateway Load Balancer

Puoi visualizzare i CloudWatch parametri per i tuoi Gateway Load Balancer utilizzando la console Amazon EC2. Tali parametri vengono visualizzati come grafici di monitoraggio. I grafici di monitoraggio mostrano punti di dati se il Gateway Load Balancer è attivo e riceve richieste.

In alternativa, puoi visualizzare le metriche per il tuo Gateway Load Balancer utilizzando CloudWatch la console.

Per visualizzare i parametri tramite la console

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Per visualizzare i parametri filtrati per gruppo target, procedi nel seguente modo:
 - a. Seleziona Gruppi di destinazioni nel riquadro di navigazione.
 - b. Scegliere il gruppo target e selezionare Monitoring (Monitoraggio).
 - c. (Opzionale) Per filtrare i risultati in base al tempo, seleziona un intervallo di tempo in Visualizzazione dati per.
 - d. Per ingrandire la visualizzazione di un singolo parametro, selezionarne il grafico.
3. Per visualizzare i parametri filtrati in base al Gateway Load Balancer, procedi nel seguente modo:
 - a. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
 - b. Scegli il Gateway Load Balancer e seleziona Monitoraggio.

- c. (Opzionale) Per filtrare i risultati in base al tempo, seleziona un intervallo di tempo in Visualizzazione dati per.
- d. Per ingrandire la visualizzazione di un singolo parametro, selezionarne il grafico.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Seleziona lo spazio dei nomi GatewayELB.
4. (Facoltativo) Per visualizzare tutte le dimensioni di un parametro, inserirne il nome nel campo di ricerca.

Per visualizzare le metriche utilizzando AWS CLI

Utilizza il seguente comando [list-metrics](#) per elencare i parametri disponibili:

```
aws cloudwatch list-metrics --namespace AWS/GatewayELB
```

Per ottenere le statistiche relative a una metrica, utilizzare il AWS CLI

Utilizzate il seguente [get-metric-statistics](#) comando get statistics per la metrica e la dimensione specificate. Tieni presente che CloudWatch considera ogni combinazione unica di dimensioni come una metrica separata. Non si possono recuperare le statistiche utilizzando combinazioni di dimensioni che non siano state specificamente pubblicate. Occorre specificare le stesse dimensioni utilizzate al momento della creazione dei parametri.

```
aws cloudwatch get-metric-statistics --namespace AWS/GatewayELB \  
--metric-name UnHealthyHostCount --statistics Average --period 3600 \  
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \  
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \  
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

Di seguito è riportato un output di esempio.

```
{  
  "Datapoints": [  
    {  
      "Timestamp": "2020-12-18T22:00:00Z",
```

```
        "Average": 0.0,  
        "Unit": "Count"  
    },  
    {  
        "Timestamp": "2020-12-18T04:00:00Z",  
        "Average": 0.0,  
        "Unit": "Count"  
    },  
    ...  
],  
"Label": "UnHealthyHostCount"  
}
```

Registrazione delle chiamate API per Gateway Load Balancer tramite AWS CloudTrail

Elastic Load Balancing è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Elastic Load Balancing. CloudTrail acquisisce tutte le chiamate API per Elastic Load Balancing come eventi. Le chiamate acquisite includono chiamate provenienti da AWS Management Console e chiamate di codice alle operazioni dell'API Elastic Load Balancing. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Elastic Load Balancing. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Elastic Load Balancing, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#).

Informazioni su Elastic Load Balancing in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Elastic Load Balancing, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Elastic Load Balancing, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon

S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

[Tutte le azioni Elastic Load Balancing per Gateway Load Balancer vengono registrate CloudTrail e documentate nella versione di riferimento dell'API Elastic Load Balancing 2015-12-01.](#) Ad esempio, le chiamate alle azioni e generano voci nei file di registro. `CreateLoadBalancer` `DeleteLoadBalancer` `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 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 AWS servizio.

Per ulteriori informazioni, vedete l'elemento [CloudTrailuserIdentity](#).

Informazioni sulle voci dei file di log di Elastic Load Balancing

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sull'azione richiesta, data e ora dell'azione, parametri richiesti e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

I file di registro includono gli eventi per tutte le chiamate AWS API per il tuo AWS account, non solo per le chiamate API Elastic Load Balancing. Puoi individuare le chiamate

all'API di Elastic Load Balancing controllando gli elementi `eventSource` con il valore `elasticloadbalancing.amazonaws.com`. Per visualizzare il record di un'operazione specifica, ad esempio `CreateLoadBalancer`, verifica la presenza di elementi `eventName` con il nome dell'operazione.

Di seguito sono riportati alcuni esempi di record di CloudTrail log per Elastic Load Balancing per un utente che ha creato un Gateway Load Balancer e poi lo ha eliminato utilizzando AWS CLI. Puoi identificare la CLI utilizzando gli elementi `userAgent`. Puoi identificare le chiamate API richieste utilizzando gli elementi `eventName`. Le informazioni relative all'utente (Alice) sono disponibili nell'elemento `userIdentity`.

Example Esempio: CreateLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2020-12-11T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-8360a9e7", "subnet-b7d581c0"],
    "name": "my-load-balancer",
    "type": "gateway"
  },
  "responseElements": {
    "loadBalancers": [{
      "type": "gateway",
      "loadBalancerName": "my-load-balancer",
      "vpcId": "vpc-3ac0fb5f",
      "state": {"code": "provisioning"},
      "availabilityZones": [
        {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"}
      ]
    }
  ]
}
```



```

        {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
    ],
    "createdTime": "Dec 11, 2020 5:23:50 PM",
    "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
    }]
},
"requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
"eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
"eventType": "AwsApiCall",
"apiVersion": "2015-12-01",
"recipientAccountId": "123456789012"
}

```

Example Esempio: DeleteLoadBalancer

```

{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2020-12-12T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "DeleteLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0"
  },
  "responseElements": null,
  "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
  "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-12-01",
  "recipientAccountId": "123456789012"
}

```

Quota per i load balancer del gateway

L'account AWS dispone delle seguenti quote predefinite, precedentemente definite limiti, per ogni servizio AWS. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per richiedere un incremento di quota, utilizza il [modulo per l'aumento dei limiti](#).

Sistemi di load balancer

Di seguito sono riportate le quote dell'account AWS in relazione ai Gateway Load Balancer.

Nome	Default	Adattabile
Gateway Load Balancer per regione	100	Sì
Gateway Load Balancer per VPC	100	Sì
ENI Gateway Load Balancer per VPC	300	Sì
Ascoltatori per Gateway Load Balancer	1	No

* Ogni Gateway Load Balancer utilizza un'interfaccia di rete per zona.

Gruppi target

Le quote elencate di seguito sono per i gruppi di destinazione.

Nome	Default	Adattabile
Gruppi di destinazione GENEVE per regione	100	Sì
Destinazioni per gruppo di destinazione	1.000	Sì
Destinazioni per zona di disponibilità per gruppo di destinazione GENEVE	300	No
Destinazioni per Gateway Load Balancer e per zona di disponibilità	300	No

Nome	Default	Adattabile
Destinazioni per Gateway Load Balancer	300	No

Larghezza di banda

Per impostazione predefinita, ogni endpoint VPC può supportare una larghezza di banda massima di 10 Gbps per zona di disponibilità e aumenta automaticamente fino a 100 Gbps. Se l'applicazione richiede una velocità effettiva più elevata, contatta il supporto AWS.

Cronologia dei documenti per i Gateway Load Balancer

La tabella seguente descrive i rilasci dei Gateway Load Balancer.

Modifica	Descrizione	Data
Supporto IPv6	È possibile configurare i servizi endpoint del Gateway Load Balancer in modo che supportino indirizzi IPv4 e IPv6.	12 dicembre 2022
Ribilanciamento del flusso	Questa versione aggiunge il supporto per definire il comportamento di gestione del flusso per Gateway Load Balancer in caso di errore o annullamento della registrazione degli obiettivi.	13 ottobre 2022
Persistenza del flusso configurabile	È possibile configurare l'hashing che mantiene la persistenza dei flussi verso una specifica appliance di destinazione.	25 agosto 2022
Disponibile in nuove regioni	Questa versione aggiunge il supporto per i Gateway Load Balancer nelle AWS GovCloud (US) regioni.	17 giugno 2021
Disponibile in nuove regioni	Questa versione aggiunge il supporto per Gateway Load Balancer nelle regioni Canada (Centrale), Asia Pacifico (Seoul) e Asia Pacifico (Osaka).	31 marzo 2021

[Disponibile in nuove regioni](#)

Questa versione aggiunge il supporto per Gateway Load Balancer negli Stati Uniti occidentali (California settentrionale), Europa (Londra), Europa (Parigi), Europa (Milano), Africa (Città del Capo), Medio Oriente (Bahrein), Asia Pacifico (Hong Kong), Asia Pacifico (Singapore) e Asia Pacifico (Mumbai).

19 marzo 2021

[Versione iniziale](#)

Questo rilascio di sistema di bilanciamento del carico elastico introduce i Gateway Load Balancer.

10 novembre 2020

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.