aws

Network Load Balancers

Sistema di bilanciamento del carico elastico

Sistema di bilanciamento del carico elastico: Network Load Balancers

Table of Contents

Cos'è un Network Load Balancer?

Il servizio Elastic Load Balancing distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, 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 sistemi Network Load Balancer. Per ulteriori informazioni su altri sistemi di bilanciamento del carico, consulta la Guida per l'utente di Application Load Balancer, la Guida per l'utente di Gateway Load Balancer e la Guida per l'utente di Classic Load Balancer.

Componenti di un sistema Network Load Balancer

Un sistema di bilanciamento del carico funge da singolo punto di contatto per i client. Il sistema di bilanciamento del carico distribuisce automaticamente il traffico in ingresso tra più destinazioni, come le istanze Amazon EC2. Ciò aumenta la disponibilità dell'applicazione. Puoi aggiungere uno o più listener al load balancer.

Un listener controlla le richieste di connessione dai client, utilizzando il protocollo e la porta che configuri e inoltra le richieste a un gruppo target.

Un gruppo di destinazione instrada le richieste verso una o più destinazioni registrate, ad esempio istanze EC2, utilizzando il protocollo TCP e il numero di porta specificati dall'utente. I gruppi di destinazione del Network Load Balancer supportano i protocolli TCP, UDP, TCP_UDP e TLS. È possibile registrare un target a più gruppi target. È possibile configurare controlli dello stato per ciascun gruppo target. I controlli dello stato vengono eseguiti su tutti i target registrati a un gruppo target specificato in una regola di listener per il sistema di bilanciamento del carico.

Per ulteriori informazioni, consulta la seguente documentazione :

- Sistemi di load balancer
- Listener

- Gruppi di destinazione

Panoramica di Network Load Balancer

Un sistema Network Load Balancer funziona al quarto livello del modello Open Systems Interconnection (OSI). È in grado di gestire milioni di richieste al secondo. Dopo aver ricevuto una richiesta di connessione, il sistema di bilanciamento del carico seleziona un target dal gruppo target per la regola predefinita. Tenta quindi di aprire una connessione TCP per la destinazione selezionata sulla porta specificata nella configurazione del listener,

Quando abiliti una zona di disponibilità per il sistema di bilanciamento del carico, Elastic Load Balancing crea un nodo del sistema di bilanciamento del carico nella zona di disponibilità. 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 nodo di bilanciamento del carico distribuisce le richieste nei target registrati in tutte le zone di disponibilità attivate. Per ulteriori informazioni, consulta Zone di disponibilità.

Per aumentare la tolleranza agli errori delle applicazioni, puoi abilitare più zone di disponibilità per il sistema di bilanciamento del carico e assicurarti che ciascun gruppo di destinazione disponga di almeno una destinazione in ciascuna zona di disponibilità abilitata. Ad esempio, se uno o più gruppi target non hanno una target integro abilitato in una zona di disponibilità, rimuoviamo l'indirizzo IP per la sottorete corrispondente da DNS, ma il nodo del sistema di bilanciamento del carico nell'altra zona di disponibilità è ancora disponibile a instradare il traffico. Se un client non rispetta il time-to-live (TTL) e invia richieste all'indirizzo IP dopo che è stato rimosso dal DNS, le richieste hanno esito negativo.

Per il traffico TCP, un sistema di bilanciamento del carico seleziona un nodo target utilizzando un algoritmo di instradamento per l'hash del flusso, basato su protocollo, indirizzo IP di origine, porta di origine, indirizzo IP di destinazione, porta di destinazione e numero di sequenza TCP. Le connessioni TCP da un client dispongono di diverse porte di origine e numeri di sequenza e possono essere instradate a target differenti. Ogni singola connessione TCP viene instradata a un singolo target per tutta la durata della connessione.

Per il traffico UDP, un sistema di bilanciamento del carico seleziona un nodo target utilizzando un algoritmo di instradamento per l'hash del flusso, basato su protocollo, indirizzo IP di origine, porta di origine, indirizzo IP di destinazione e porta di destinazione. Un flusso UDP ha la stessa origine e destinazione, perciò è costantemente instradato a una sola destinazione per tutta la sua durata di vita. Diversi flussi UDP hanno diversi indirizzi IP di origine e porte, in modo che possano essere instradati a destinazioni differenti.

Elastic Load Balancing crea un'interfaccia di rete per ogni zona di disponibilità abilitata. Ogni nodo del sistema di bilanciamento del carico nella zona di disponibilità utilizza questa interfaccia di rete per ottenere un indirizzo IP statico. Quando crei un sistema di bilanciamento del carico connesso a Internet, puoi scegliere di associare un indirizzo IP elastico a ogni sottorete.

Quando crei un gruppo di destinazione, devi specificare il tipo di destinazione, che determina il modo in cui vengono registrate le destinazioni. Ad esempio, puoi registrare ID istanza, indirizzi IP o un Application Load Balancer. Il tipo di destinazione influisce anche sulla conservazione degli indirizzi IP client. Per ulteriori informazioni, consulta the section called “Conservazione dell'IP client”.

È possibile aggiungere e rimuovere le destinazioni dal sistema di bilanciamento del carico in base alle proprie esigenze, senza interrompere il flusso di richieste per l'applicazione. 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.

È possibile configurare controlli dello stato, che vengono utilizzati per monitorare lo stato dei target registrati in modo che il sistema di bilanciamento del carico è in grado di inviare le richieste solo per i target integri.

Per ulteriori informazioni consultare la guida Come funziona Elastic Load Balancing all'interno della Guida per l'utente di Elastic Load Balancing.

Vantaggi della migrazione da un Classic Load Balancer

L'utilizzo di Network Load Balancer invece di Classic Load Balancer comporta i seguenti vantaggi:

- Capacità di gestire carichi di lavoro volatili e ridimensionare milioni di richieste al secondo.
- Supporto per indirizzi IP statici per il sistema di bilanciamento del carico. È anche possibile assegnare un indirizzo IP elastico per ogni sottorete abilitata per il sistema di bilanciamento del carico.
- Supporto per la registrazione di target in base all'indirizzo IP, inclusi target all'esterno del VPC per il sistema di bilanciamento del carico.
- Supporto per le richieste di instradamento a più applicazioni su una singola istanza EC2. È possibile registrare ogni istanza o indirizzo IP con lo stesso gruppo target utilizzando più porte.
- Supporto per applicazioni containerizzate. Amazon Elastic Container Service (Amazon ECS) può selezionare una porta non utilizzata per la pianificazione di un'attività con un gruppo di destinazioni utilizzando questa porta. Ciò rende possibile un utilizzo efficiente dei cluster.

- Support per il monitoraggio dello stato di ciascun servizio in modo indipendente, poiché i controlli sanitari sono definiti a livello di gruppo target e molte CloudWatch metriche Amazon vengono riportate a livello di gruppo target. Il collegamento di un gruppo di destinazione a un gruppo con dimensionamento automatico consente di dimensionare ciascun servizio in modo dinamico in base alle esigenze.

Per ulteriori informazioni sulle caratteristiche supportate da ogni tipo di load balancer, vedere il Confronto di prodotti per Elastic Load Balancing.

Come iniziare

Per creare un Network Load Balancer, consulta uno dei seguenti tutorial:

- Nozioni di base sui sistemi Network Load Balancer
- Tutorial: creazione di un Network Load Balancer tramite AWS CLI

Per dimostrazioni di configurazioni comuni del sistema di bilanciamento del carico, consulta Demo di Elastic Load Balancing.

Prezzi

Per ulteriori informazioni, consulta Prezzi di Network Load Balancer.

Nozioni di base sui sistemi Network Load Balancer

Questo tutorial fornisce un'introduzione pratica ai Network Load Balancer tramite un'interfaccia basata sul Web AWS Management Console. Per creare il primo Network Load Balancer, completa le fasi seguenti.

Attività

Per dimostrazioni di configurazioni comuni del sistema di bilanciamento del carico, consulta Demo di Elastic Load Balancing.

Prima di iniziare

- Stabilire quali zone di disponibilità utilizzerai per le istanze EC2. Configurare il cloud privato virtuale (VPC) con almeno una sottorete pubblica in ciascuna di queste zone di disponibilità. Queste sottoreti pubbliche vengono utilizzate per configurare il sistema di bilanciamento del carico. È possibile avviare le istanze EC2 in altre sottoreti di queste zone di disponibilità.
- Avviare almeno una istanza EC2 in ciascuna zona di disponibilità. Verificare che i gruppi di sicurezza per queste istanze consentano l'accesso TCP dai client sulla porta del listener e le richieste di controllo dello stato dal VPC. Per ulteriori informazioni, consulta Gruppi di sicurezza target.

Fase 1: configurazione del gruppo di destinazione

Creare un gruppo target, che viene utilizzato nell'instradamento delle richieste. La regola per il listener instrada le richieste ai target registrati in questo gruppo target. Il bilanciamento del carico controlla lo stato dei target in questo gruppo target, utilizzando le impostazioni di controllo dello stato definite per il gruppo target.

Per configurare 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, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Scegliere Crea gruppo target.
4. Mantieni il tipo di destinazione istanze.
5. In Nome gruppo target, immetti un nome per il nuovo gruppo di destinazione.
6. In Protocollo scegli TCP e in Porta seleziona 80.
7. Per VPC, scegli il VPC contenente le istanze.
8. In Controlli dell'integrità, mantenere le impostazioni predefinite.
9. Seleziona Successivo.
10. Nella pagina Registra destinazioni, completa la seguente procedura. Si tratta di un passaggio facoltativo per la creazione di un gruppo di destinazione. Tuttavia, se vuoi testare il sistema di bilanciamento del carico e assicurarti che stia indirizzando il traffico verso le destinazioni, devi prima registrarle.
    a. Per Istanze disponibili, seleziona una o più istanze.
    b. Mantenere la porta 80 predefinita e scegliere Includi come in sospeso di seguito.
11. Scegliere Crea gruppo target.

Fase 2: scelta di un tipo di sistema di bilanciamento del carico

Elastic Load Balancing supporta diversi tipi di bilanciamento del carico. In questo tutorial viene creato un Network Load Balancer.

Per creare un Network Load Balancer utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Sulla barra di navigazione, seleziona una regione per il bilanciamento del carico. Assicurati di scegliere la stessa regione utilizzata per le istanze EC2.
3. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
4. Selezionare Create Load Balancer (Crea sistema di bilanciamento del carico).
5. Per Network Load Balancer, scegli Crea.

Fase 3: configurazione del sistema di bilanciamento del carico e dell'ascoltatore

Per creare un Network Load Balancer, devi innanzitutto fornire le informazioni di configurazione di base del sistema di bilanciamento del carico, ad esempio il nome, lo schema e il tipo di indirizzo IP. Successivamente, fornisci alcune informazioni relative alla rete e agli ascoltatori. Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e con una porta per le connessioni dai client al sistema di bilanciamento del carico. Per ulteriori informazioni sui protocolli e le porte supportati, consulta Configurazione dei listener.

Configurazione del sistema di bilanciamento del carico e dell'ascoltatore

1. In Nome del sistema di bilanciamento del carico immetti un nome univoco per il sistema di bilanciamento del carico. Ad esempio, `my-nlb`.
2. Per Schema e Tipo di indirizzo IP, mantenere i valori predefiniti.
3. In Mappatura di rete, seleziona il VPC utilizzato per le istanze EC2. Per ogni zona di disponibilità usata per avviare le istanze EC2, selezionare la zona di disponibilità e quindi una relativa sottorete pubblica.

   Per impostazione predefinita, AWS assegna un indirizzo IPv4 a ciascun nodo di bilanciamento del carico dalla sottorete per la relativa zona di disponibilità. In alternativa, se si crea un sistema di bilanciamento del carico collegato a Internet, è possibile selezionare un indirizzo IP elastico per ogni zona di disponibilità. Questo fornisce il sistema di bilanciamento del carico con indirizzi IP statici.
4. Per Gruppi di sicurezza viene preselezionato il gruppo di sicurezza predefinito per il VPC. Puoi selezionare altri gruppi di sicurezza in base alle esigenze. Se non disponi di un gruppo di sicurezza adatto, scegli Crea un nuovo gruppo di sicurezza e creane uno che soddisfi le tue esigenze di sicurezza. Per ulteriori informazioni, consulta Creazione di un gruppo di sicurezza nella Guida per l'utente di Amazon VPC.

   > **Warning**
   >
   > Se in questa fase decidi di non associare alcun gruppo di sicurezza al sistema di bilanciamento del carico, non potrai farlo in seguito.
5. In Listener e routing, mantieni il protocollo e la porta predefiniti, quindi seleziona il gruppo di destinazione dall'elenco. Questa operazione consente di configurare un ascoltatore in grado

di accettare il traffico TCP sulla porta 80 e inoltrarlo al gruppo di destinazione selezionato per impostazione predefinita.

6. (Facoltativo) Aggiungi tag per classificare il sistema di bilanciamento del carico. Le chiavi dei tag devono essere univoche per ogni load balancer. I caratteri consentiti sono lettere, spazi e numeri (in UTF-8) e i seguenti caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali. I valori di tag fanno distinzione tra maiuscole e minuscole.
7. Controlla la configurazione e scegli Crea sistema di bilanciamento del carico. Durante la creazione, vengono applicati alcuni attributi predefiniti al sistema di bilanciamento del carico. È possibile visualizzarli e modificarli dopo la creazione del sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Attributi del sistema di bilanciamento del carico.

Fase 4: test del sistema di bilanciamento del carico

Dopo aver creato il sistema di bilanciamento del carico, verificare l'invio del traffico verso le istanze di EC2.

Per verificare il sistema di bilanciamento del carico

1. Dopo la notifica di creazione del sistema di bilanciamento del carico, scegli Chiudi.
2. Nel riquadro di navigazione, sotto Bilanciamento del carico, scegli Gruppi di destinazioni.
3. Selezionare il gruppo target appena creato.
4. Scegliere Target e verificare che le istanze siano pronte. Se l'istanza è ancora nello stato `initial`, probabilmente si trova nella fase di registrazione o non ha superato il numero minimo di controlli dello stato per essere considerata integra. Se lo stato di almeno un'istanza è `healthy`, è possibile testare il sistema di bilanciamento del carico.
5. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
6. Seleziona il nome del sistema di bilanciamento del carico appena creato per aprirne la pagina dei dettagli.
7. Copia il nome DNS del load balancer (ad esempio, -1234567890abcdef. elb.us-east-2.amazonaws.com). my-load-balancer Incollare il nome DNS nel campo dell'indirizzo di un browser Web connesso a Internet. Se tutto funziona, il browser visualizza la pagina predefinita del server.

Fase 5: eliminazione del sistema di bilanciamento del carico (facoltativo)

Non appena il load balancer diventa disponibile, ti verrà addebitata ogni ora o frazione di ora in cui lo mantieni in esecuzione. Se il load balancer non ti è più utile, puoi eliminarlo. Non appena il load balancer viene eliminato, i relativi addebiti vengono bloccati. Si noti che l'eliminazione di un sistema di bilanciamento del carico non influisce sui target registrati con il sistema di bilanciamento del carico. Ad esempio, le istanze EC2 continuano a essere eseguite.

Per eliminare il sistema di bilanciamento del carico 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 la casella di controllo per il sistema di bilanciamento del carico e scegli Operazioni, Elimina.
4. Quando viene richiesta la conferma, digita **`confirm`** e scegli Elimina.

Tutorial: creazione di un Network Load Balancer tramite AWS CLI

Questo tutorial fornisce un'introduzione pratica ai sistemi Network Load Balancer tramite AWS CLI.

Prima di iniziare

- Installa l'AWS CLI o aggiorna la versione corrente dell'AWS CLI se utilizzi una versione che non supporta i sistemi Network Load Balancer. Per ulteriori informazioni, consulta Installazione dell'AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface.
- Stabilire quali zone di disponibilità utilizzerai per le istanze EC2. Configurare il cloud privato virtuale (VPC) con almeno una sottorete pubblica in ciascuna di queste zone di disponibilità.
- Decidi se creare un sistema di bilanciamento del carico IPv4 o dualstack. Utilizza IPv4 se desideri che i client utilizzino solo indirizzi IPv4 per comunicare con il sistema di bilanciamento del carico. Utilizza dualstack se desideri che i client utilizzino sia indirizzi IPv4 che IPv6 per comunicare con il sistema di bilanciamento del carico. Puoi anche utilizzare dualstack per comunicare con destinazioni di back-end, come applicazioni IPv6 o sottoreti dualstack, utilizzando IPv6.
- Avviare almeno una istanza EC2 in ciascuna zona di disponibilità. Verificare che i gruppi di sicurezza per queste istanze consentano l'accesso TCP dai client sulla porta del listener e le richieste di controllo dello stato dal VPC. Per ulteriori informazioni, consulta Gruppi di sicurezza target.

Creazione del sistema di bilanciamento del carico IPv4

Per creare il sistema di bilanciamento del carico, completare le fasi seguenti.

Per creare un sistema di bilanciamento del carico IPv4

1. Usa il create-load-balancercomando per creare un load balancer IPv4, specificando una sottorete pubblica per ogni zona di disponibilità in cui sono state avviate le istanze. Puoi specificare una sola sottorete per ogni zona di disponibilità.

   Per impostazione predefinita, quando i sistemi Network Load Balancer vengono creati tramite la AWS CLI, non utilizzano automaticamente il gruppo di sicurezza predefinito per il VPC. Se decidi di non associare alcun gruppo di sicurezza al sistema di bilanciamento del carico durante

la creazione, non potrai farlo in seguito. Ti consigliamo di specificare i gruppi di sicurezza per il sistema di bilanciamento del carico durante la creazione utilizzando l'opzione `--security-groups`.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

L'output include l'Amazon Resource Name (ARN) del load balancer, con il formato seguente:

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

2. Usa il create-target-groupcomando per creare un gruppo target IPv4, specificando lo stesso VPC che hai usato per le tue istanze EC2. I gruppi di destinazione IPv4 supportano le destinazioni di tipo IP e Istanza.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE
```

L'output include l'ARN del gruppo target, con questo formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Utilizzare il comando register-target per registrare le istanze nel gruppo di destinazioni:

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

4. Utilizzare 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 di destinazioni:

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --
port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

L'output contiene l'ARN del listener, con il formato seguente:

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

5. (Facoltativo) Puoi verificare lo stato dei target registrati per il tuo gruppo target utilizzando questo comando: describe-target-health

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

Creazione del sistema di bilanciamento del carico dualstack

Per creare il sistema di bilanciamento del carico, completare le fasi seguenti.

Per creare un sistema di bilanciamento del carico dualstack

1. Utilizzate il create-load-balancercomando per creare un sistema di bilanciamento del carico dualstack, specificando una sottorete pubblica per ogni zona di disponibilità in cui sono state avviate le istanze. Puoi specificare una sola sottorete per ogni zona di disponibilità.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

L'output include l'Amazon Resource Name (ARN) del load balancer, con il formato seguente:

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

2. Usa il create-target-groupcomando per creare un gruppo target, specificando lo stesso VPC che hai usato per le tue istanze EC2.

Devi utilizzare un gruppo di destinazione TCP o TLS con il sistema di bilanciamento del carico dualstack.

Puoi creare gruppi di destinazione IPv4 e IPv6 da associare ai sistemi di bilanciamento del carico dualstack. Il tipo di indirizzo IP del gruppo di destinazione determina la versione IP utilizzata dal sistema di bilanciamento del carico per comunicare con le destinazioni di back-end e controllarne lo stato.

I gruppi di destinazione IPv4 supportano le destinazioni di tipo IP e Istanza. Le destinazioni IPv6 supportano solo destinazioni IP.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE  --ip-address-type [ipv4 or ipv6]
```

L'output include l'ARN del gruppo target, con questo formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Utilizzare il comando register-target per registrare le istanze nel gruppo di destinazioni:

```
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 di destinazione. I sistemi di bilanciamento del carico dualstack devono disporre di ascoltatori TCP o TLS.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --
port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

L'output contiene l'ARN del listener, con il formato seguente:

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

5. (Facoltativo) Puoi verificare lo stato dei target registrati per il tuo gruppo target utilizzando questo comando: describe-target-health

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

Specifica dell'indirizzo IP elastico per il sistema di bilanciamento del carico

Quando crei un Network Load Balancer, puoi specificare un indirizzo IP elastico per ogni sottorete utilizzando una mappatura delle sottoreti.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

Eliminazione del sistema di bilanciamento del carico

Quando non è più necessario il sistema di bilanciamento del carico e il gruppo target, è possibile rimuoverli come segue:

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Network Load Balancers

Un sistema di bilanciamento del carico funge da singolo punto di contatto per i client. I client inviano le richieste al sistema di bilanciamento del carico e questo le invia ai target, ad esempio alle istanze EC2, in una o più zone di disponibilità.

Per configurare un sistema di bilanciamento del carico, devi creare gruppi target e poi registrare i target nei gruppi. Il sistema di bilanciamento del carico è più efficace se ogni zona di disponibilità abilitata dispone di almeno un target registrato. Puoi anche creare dei listener per verificare le richieste di connessione dai client e instradare le richieste dai client verso i target nel gruppo di target.

I Network Load Balancer supportano le connessioni dei client tramite peering VPC, AWS Direct Connect VPN AWS gestita e soluzioni VPN di terze parti.

Indice

Stato del sistema di bilanciamento del carico

Un sistema di bilanciamento del carico presenta uno dei seguenti stati:

`provisioning`

Il sistema di bilanciamento del carico è in fase di configurazione.

`active`

Il sistema di bilanciamento del carico è completamente configurato e pronto a instradare il traffico.

`failed`

Non è stato possibile configurare il sistema di bilanciamento del carico.

Attributi del sistema di bilanciamento del carico

Un sistema di bilanciamento del carico presenta gli attributi seguenti:

`access_logs.s3.enabled`

Indica se i log di accesso archiviati in Amazon S3 sono abilitati. Il valore predefinito è `false`.

`access_logs.s3.bucket`

Il nome del bucket Amazon S3 per i log di accesso. Questo attributo è obbligatorio se i log di accesso sono abilitati. Per ulteriori informazioni, consulta Requisiti del bucket.

`access_logs.s3.prefix`

Il prefisso della posizione nel bucket Amazon S3.

`deletion_protection.enabled`

Indica se è abilitata la protezione da eliminazione. Il valore predefinito è `false`.

`ipv6.deny_all_igw_traffic`

Blocca l'accesso tramite gateway Internet (IGW) al sistema di bilanciamento del carico, impedendo l'accesso involontario al sistema di bilanciamento del carico interno tramite un gateway Internet. È impostato su `false` per i sistemi di bilanciamento del carico connessi a Internet e su `true` per i sistemi di bilanciamento del carico interni. Questo attributo non impedisce l'accesso a Internet non IGW (ad esempio, tramite peering, AWS Direct Connect Transit Gateway o). AWS VPN

`load_balancing.cross_zone.enabled`

Indica se è abilitato il bilanciamento del carico tra zone. Il valore predefinito è `false`.

`dns_record.client_routing_policy`

Indica il modo in cui viene distribuito il traffico tra le zone di disponibilità del sistema di bilanciamento del carico. I valori possibili sono `availability_zone_affinity` con affinità di zona del 100%, `partial_availability_zone_affinity` con affinità di zona dell'85% e `any_availability_zone` con affinità di zona dello 0%.

Tipo di indirizzo IP

Puoi impostare i tipi di indirizzi IP che i client possono utilizzare con il sistema di bilanciamento del carico.

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

`ipv4`

I client devono connettersi al sistema di bilanciamento del carico utilizzando indirizzi IPv4 (ad esempio, 192.0.2.1). I sistemi di bilanciamento del carico compatibili con IPv4 (sia con connessione Internet che interni) supportano gli ascoltatori TCP, UDP, TCP_UDP e TLS.

`dualstack`

I client possono connettersi al sistema di bilanciamento del carico utilizzando entrambi gli indirizzi IPv4 (ad esempio 192.0.2.1) e gli indirizzi IPv6 (ad esempio, 2001:0db8:85a3:0:0:8a2e:0370:7334). I sistemi di bilanciamento del carico dualstack (sia con connessione Internet che interni) supportano gli ascoltatori TCP e TLS.

Considerazioni

- Il sistema di bilanciamento del carico comunica con le destinazioni in base al tipo di indirizzo IP del gruppo di destinazioni.
- Quando si attiva la modalità dualstack per il sistema di bilanciamento del carico, Elastic Load Balancing fornisce un record DNS AAAA per il sistema bilanciamento del carico. I client che comunicano con il sistema di bilanciamento del carico utilizzando indirizzi IPv4 risolvono il record DNS A. I client che comunicano con il sistema di bilanciamento del carico utilizzando indirizzi IPv6 risolvono il record DNS AAAA.

- L'accesso ai sistemi di bilanciamento del carico interni dualstack tramite il gateway Internet è bloccato per prevenire accessi non intenzionali a Internet. Tuttavia, ciò non impedisce altri accessi a Internet (ad esempio, tramite peering, Transit Gateway o AWS VPN). AWS Direct Connect

Per ulteriori informazioni sui tipi di indirizzi IP, vedereTipi di indirizzi IP per il Network Load Balancer.

Mappa delle risorse di Network Load Balancer

La mappa delle risorse di Network Load Balancer fornisce una visualizzazione interattiva dell'architettura del sistema di bilanciamento del carico, inclusi i listener, i gruppi target e i target associati. La mappa delle risorse evidenzia anche le relazioni e i percorsi di routing tra tutte le risorse, producendo una rappresentazione visiva della configurazione del sistema di bilanciamento del carico.

Per visualizzare la mappa delle risorse del Network Load Balancer utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare il load balancer.
4. Scegli la scheda Mappa delle risorse per visualizzare la mappa delle risorse del sistema di bilanciamento del carico.

Componenti della mappa delle risorse

Visualizzazioni della mappa

Nella mappa delle risorse di Network Load Balancer sono disponibili due visualizzazioni: Overview e Unhealthy Target Map. La panoramica è selezionata per impostazione predefinita e mostra tutte le risorse del sistema di bilanciamento del carico. Selezionando la visualizzazione Unhealthy Target Map verranno visualizzati solo gli obiettivi non sani e le risorse ad essi associate.

La visualizzazione Unhealthy Target Map può essere utilizzata per risolvere i problemi relativi agli obiettivi che non superano i controlli di integrità. Per ulteriori informazioni, consulta Risolvi i problemi relativi agli obiettivi non integri utilizzando la mappa delle risorse.

Colonne di risorse

La mappa delle risorse di Network Load Balancer contiene tre colonne di risorse, una per ogni tipo di risorsa. I gruppi di risorse sono Listener, Target groups e Targets.

Riquadri di risorse

Ogni risorsa all'interno di una colonna ha il proprio riquadro, che mostra i dettagli su quella risorsa specifica.

- Il passaggio del mouse su un riquadro di risorse evidenzia le relazioni tra tale risorsa e le altre risorse.
- La selezione di un riquadro delle risorse evidenzia le relazioni tra tale riquadro e le altre risorse e visualizza dettagli aggiuntivi su tale risorsa.
  - riepilogo sullo stato di salute del gruppo target: il numero di obiettivi registrati per ogni stato di salute.
  - stato di salute dell'obiettivo: lo stato di salute attuale e la descrizione dell'obiettivo.

> **Note**
>
> Puoi disattivare Mostra i dettagli delle risorse per nascondere dettagli aggiuntivi all'interno della mappa delle risorse.

- Ogni riquadro delle risorse contiene un link che, se selezionato, accede alla pagina dei dettagli della risorsa.
  - Listeners - Seleziona il protocollo dei listener:port. Ad esempio, `TCP:80`
  - Gruppi target - Seleziona il nome del gruppo target. Ad esempio, `my-target-group`
  - Obiettivi - Seleziona l'ID dei bersagli. Ad esempio, `i-1234567890abcdef0`

Esporta la mappa delle risorse

Selezionando Esporta è possibile esportare la visualizzazione corrente della mappa delle risorse di Network Load Balancer in formato PDF.

Zone di disponibilità

Quando crei un sistema di bilanciamento del carico, devi attivare una o più zone di disponibilità. Se attivi più zone di disponibilità in un sistema di bilanciamento del carico, la tolleranza ai guasti

delle applicazioni aumenta. Non è possibile disabilitare le zone di disponibilità per un Network Load Balancer dopo averle create, ma è possibile abilitare ulteriori zone di disponibilità.

Quando attivi una zona di disponibilità, devi specificare una sottorete per la zona. Elastic Load Balancing crea un nodo del sistema di bilanciamento del carico nella zona di disponibilità e un'interfaccia di rete per la sottorete (la descrizione inizia con "ELB net" e include il nome del sistema di bilanciamento del carico). Ogni nodo del sistema di bilanciamento del carico nella zona di disponibilità utilizza questa interfaccia di rete per ottenere un indirizzo IPv4. Tieni presente che puoi visualizzare l'interfaccia di rete, ma non puoi modificarla.

Quando crei un sistema di bilanciamento del carico connesso a Internet, puoi scegliere di specificare un indirizzo IP elastico per ogni sottorete. Se non scegli un tuo indirizzo IP elastico, Elastic Load Balancing fornisce automaticamente un indirizzo IP elastico per ogni sottorete. Questi indirizzi IP elastici forniscono al sistema di bilanciamento del carico gli indirizzi IP statici che non verranno modificati durante l'esecuzione del sistema di bilanciamento del carico. Non è possibile modificare questi indirizzi IP elastici dopo aver creato il sistema di bilanciamento del carico.

Quando crei un sistema di bilanciamento del carico interno, puoi scegliere di specificare un indirizzo IP privato per ogni sottorete. Se non specifichi un indirizzo IP dalla sottorete, Elastic Load Balancing ne sceglie uno automaticamente. Questi indirizzi IP privati forniscono al sistema di bilanciamento del carico gli indirizzi IP statici che non verranno modificati durante l'esecuzione del sistema di bilanciamento del carico. Non è possibile modificare questi indirizzi IP privati dopo aver creato il sistema di bilanciamento del carico.

Considerazioni

- Per i sistemi di bilanciamento del carico connessi a Internet, le sottoreti specificate devono avere a disposizione almeno 8 indirizzi IP. Per i sistemi di bilanciamento del carico interni, questa operazione è necessaria solo se si consente di AWS selezionare un indirizzo IPv4 privato dalla sottorete.
- Non è possibile specificare una sottorete in una zona di disponibilità vincolata. Il messaggio di errore indica che i sistemi di bilanciamento del carico di tipo "rete" non sono supportati in nome_az. È possibile specificare una sottorete in un'altra zona di disponibilità non vincolata e utilizzare il bilanciamento del carico tra più zone per distribuire il traffico a destinazioni nella zona di disponibilità vincolata.
- È possibile specificare le sottoreti condivise con l'utente.
- Non è possibile specificare una sottorete in una zona locale.

Dopo aver abilitato una zona di disponibilità, il sistema di bilanciamento del carico comincia a instradare le richieste ai target registrati in tale zona di disponibilità. Il sistema di bilanciamento del carico è più efficace se ogni zona di disponibilità abilitata dispone di almeno un target registrato.

Per aggiungere le zone di disponibilità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Mappatura di rete, scegli Modifica sottoreti.
5. Per abilitare una zona di disponibilità, seleziona la casella di controllo corrispondente. Se è presente una sola sottorete per la zona di disponibilità, viene selezionata. Se è presente più di una sottorete per la zona di disponibilità, dovrai selezionarne una. Ricorda che puoi selezionare solo una sottorete per ciascuna zona di disponibilità.

   Per un sistema di bilanciamento del carico collegato a Internet, è possibile selezionare un indirizzo IP elastico per ogni zona di disponibilità. Per un sistema di bilanciamento del carico interno, è possibile assegnare un indirizzo IP privato dall'intervallo di indirizzi IPv4 di ogni sottorete invece di permettere a Elastic Load Balancing di assegnarne uno.
6. Seleziona Salvataggio delle modifiche.

Per aggiungere zone di disponibilità utilizzando il AWS CLI

Utilizza il comando set-subnets.

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 tra zone, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico tra le destinazioni registrate in tutte le zone di disponibilità abilitate. Puoi anche attivare il bilanciamento del carico tra zone a livello di gruppo di destinazione. Per ulteriori informazioni, consulta the section called “Bilanciamento del carico tra zone” e Bilanciamento del carico tra zone nella Guida per l'utente di Elastic Load Balancing.

Deletion protection (Protezione da eliminazione)

Per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente, è possibile abilitare la protezione da eliminazione. Per impostazione predefinita, la protezione da eliminazioni è disabilitata nel sistema di bilanciamento del carico.

Se abiliti la protezione da eliminazione per il sistema di bilanciamento del carico, devi disabilitarla prima di poter eliminare il sistema.

Per abilitare la protezione da eliminazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Configurazione, attivare Protezione da eliminazione.
6. Seleziona Salvataggio delle modifiche.

Per disabilitare la protezione da eliminazione tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Configurazione, attivare Protezione da eliminazione.
6. Seleziona Salvataggio delle modifiche.

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`.

Timeout di inattività della connessione

Per ogni richiesta TCP eseguita da un client tramite un Network Load Balancer, viene monitorato lo stato della connessione. Se non vengono inviati dati tramite la connessione dal client o dal target

per un periodo superiore al tempo di inattività, la connessione viene chiusa. Se un client o una destinazione invia i dati dopo la scadenza del tempo di inattività, riceve un pacchetto RST TCP che indica che la connessione non è più valida.

Il valore di timeout di inattività per i flussi TCP è impostato su 350 secondi. Non è possibile modificare questo valore. I client o i target possono utilizzare i pacchetti keepalive TCP per ripristinare il tempo di inattività. I pacchetti Keepalive inviati per mantenere le connessioni TLS non possono contenere dati o payload.

Quando un ascoltatore TLS riceve un pacchetto Keepalive TCP da un client o da una destinazione, il sistema di bilanciamento del carico genera pacchetti Keepalive TCP e li invia alle connessioni front-end e back-end ogni 20 secondi. Non è possibile modificare questo comportamento.

Quando UDP è senza connessione, il sistema di bilanciamento del carico mantiene lo stato del flusso UDP basandosi sugli indirizzi IP di origine e di destinazione e sulle porte. Ciò garantisce che i pacchetti appartenenti allo stesso flusso siano regolarmente inviati alla stessa destinazione. Una volta trascorso il periodo di timeout di inattività, il sistema di bilanciamento del carico considera il pacchetto UDP in entrata come un nuovo flusso e lo instrada a una nuova destinazione. Elastic Load Balancing imposta il valore di timeout di inattività per i flussi UDP su 120 secondi.

Le istanze EC2 devono rispondere a una nuova richiesta entro 30 secondi per stabilire un percorso di ritorno.

Nome DNS

Ogni Network Load Balancer riceve un nome del sistema dei nomi di dominio (DNS) predefinito con la sintassi seguente: *name*-*id*.elb.*region*.amazonaws.com. Ad esempio, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com.

Se preferisci utilizzare un nome DNS più facile da ricordare, puoi creare un nome di dominio personalizzato e associarlo al nome DNS per il sistema di bilanciamento del carico. Quando un client invia una richiesta utilizzando questo nome di dominio personalizzato, il server DNS lo risolve nel nome DNS per il tuo load balancer.

In primo luogo, registra un nome di dominio con un registrar di nomi di dominio accreditato. Successivamente, utilizza il servizio DNS, come il registrar di dominio, per creare un record DNS per instradare le richieste al sistema di bilanciamento del carico. Per ulteriori informazioni, consulta la documentazione per il servizio DNS. Ad esempio, se utilizzi Amazon Route 53 come servizio

DNS, crea un record alias che punti al sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Instradamento del traffico a un sistema di bilanciamento del carico ELB nella Guida per gli sviluppatori di Amazon Route 53.

Il sistema di bilanciamento del carico dispone di un indirizzo IP per ogni zona di disponibilità abilitata. Questi sono gli indirizzi IP dei nodi del sistema di bilanciamento del carico. Il nome DNS del sistema di bilanciamento del carico si risolve in questi indirizzi. Ad esempio, supponiamo che il nome di dominio personalizzato per il sistema di bilanciamento del carico sia `example.networkloadbalancer.com`. Utilizzare il seguente comando dig o nslookup per determinare gli indirizzi IP dei nodi del sistema di bilanciamento del carico.

Linux o Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

Il sistema di bilanciamento del carico dispone di record DNS per i nodi del sistema di bilanciamento del carico. Puoi utilizzare nomi DNS con la seguente sintassi per determinare gli indirizzi IP dei nodi del sistema di bilanciamento del carico: *az*.*name*-*id*.elb.*region*.amazonaws.com.

Linux o Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Affinità DNS della zona di disponibilità

Quando si utilizza la policy di instradamento del client predefinita, le richieste inviate al nome DNS dei sistemi Network Load Balancer riceveranno tutti gli indirizzi IP dei sistemi di bilanciamento del carico integri. Ciò porta alla distribuzione delle connessioni client tra le zone di disponibilità dei sistemi di bilanciamento del carico. Con le policy di instradamento per affinità della zona di disponibilità, le

query DNS dei client favoriscono gli indirizzi IP dei sistemi di bilanciamento del carico nella propria zona di disponibilità. Ciò contribuisce a migliorare la latenza e la resilienza, poiché i client non devono attraversare i confini della zona di disponibilità per connettersi alle destinazioni.

Policy di instradamento del client disponibili per i Network Load Balancer che utilizzano il risolutore Route 53:

- Affinità della zona di disponibilità: affinità di zona al 100%

  Le query DNS dei client favoriranno l'indirizzo IP del sistema di bilanciamento del carico nella propria zona di disponibilità. Le query possono essere risolte in altre zone se non sono presenti indirizzi IP integri del sistema di bilanciamento del carico nella propria zona.
- Affinità parziale della zona di disponibilità: affinità di zona all'85%

  L'85% delle query DNS client favorirà gli indirizzi IP del sistema di bilanciamento del carico nella propria zona di disponibilità, mentre le query rimanenti si risolvono in qualsiasi zona integra. Le query possono essere risolte in altre zone integre se non sono presenti indirizzi IP integri nella zona. Se nessuna zona contiene IP integri, le query vengono risolte in qualsiasi zona.
- Qualsiasi zona di disponibilità (impostazione predefinita): affinità di zona al 0%

  Le query DNS dei client vengono risolte tra indirizzi IP integri del sistema di bilanciamento del carico in tutte le zone di disponibilità.

> **Note**
>
> Le policy di instradamento per affinità della zona di disponibilità si applicano solo ai client che risolvono il nome DNS dei sistemi Network Load Balancer utilizzando il risolutore Route 53. Per maggiori informazioni, consulta Cos'è Amazon Route 53 Resolver? nella Guida per gli sviluppatori di Amazon Route 53

L'affinità della zona di disponibilità favorisce l'instradamento delle richieste dal client al sistema di bilanciamento del carico, mentre il bilanciamento del carico tra zone viene utilizzato per indirizzare le richieste dal sistema di bilanciamento del carico alle destinazioni. Quando si utilizza l'affinità tra zone di disponibilità, è necessario disattivare il bilanciamento del carico tra zone, in modo da garantire che il traffico del load balancer dai client alle destinazioni rimanga all'interno della stessa zona di disponibilità. Con questa configurazione, il traffico client viene inviato alla stessa zona di disponibilità di Network Load Balancer, pertanto si consiglia di configurare l'applicazione per scalare

indipendentemente in ciascuna zona di disponibilità. Questa è una considerazione importante quando il numero di client per zona di disponibilità o il traffico per zona di disponibilità non sono gli stessi. Per ulteriori informazioni, consulta Bilanciamento del carico tra zone per gruppi di destinazione.

Quando una zona di disponibilità è considerata non integra o quando viene avviato uno spostamento zonale, l'indirizzo IP di zona viene considerato non integro e non viene restituito ai client a meno che non sia attivo il fail-open. L'affinità della zona di disponibilità viene mantenuta quando il record DNS è in modalità fail-open. Questo aiuta a mantenere indipendenti le zone di disponibilità e a prevenire potenziali errori tra zone.

Con l'affinità della zona di disponibilità si prevedono momenti di squilibrio tra le zone di disponibilità. Ti consigliamo di assicurarti che le destinazioni siano dimensionabili a livello di zona, per supportare il carico di lavoro delle zone di disponibilità. Nei casi in cui questi squilibri sono significativi, ti consigliamo di disattivare l'affinità della zona di disponibilità. Ciò consente una distribuzione uniforme delle connessioni client tra tutte le zone di disponibilità dei sistemi di bilanciamento del carico entro 60 secondi o il TTL DNS.

Prima di utilizzare l'affinità della zona di disponibilità, tieni presente le considerazioni seguenti:

- L'affinità della zona di disponibilità apporta modifiche a tutti i client dei sistemi Network Load Balancer che utilizzano il risolutore Route 53.
  - I client non sono in grado di decidere tra risoluzioni DNS di zona e multi-zona. Tale decisione viene presa dall'affinità della zona di disponibilità.
  - I client non dispongono di un metodo affidabile per determinare quando sono influenzati dall'affinità della zona di disponibilità o per sapere in quale zona di disponibilità si trova un determinato indirizzo IP.
- I client rimarranno assegnati all'indirizzo IP locale della zona fino a quando non saranno considerati completamente integri in base ai controlli dell'integrità del DNS e saranno rimossi dal DNS.
- L'utilizzo dell'affinità della zona di disponibilità con il bilanciamento del carico tra zone di disponibilità attivo può portare a una distribuzione sbilanciata delle connessioni client tra le zone di disponibilità. Ti consigliamo di configurare lo stack di applicazioni in modo da dimensionarlo in modo indipendente in ciascuna zona di disponibilità, assicurandoti che sia in grado di supportare il traffico dei client della zona.
- Se il bilanciamento del carico tra zone è attivo, il Network Load Balancer è soggetto all'impatto tra zone.
- Il carico su ciascuna delle zone di disponibilità dei Network Load Balancer sarà proporzionale ai percorsi di zona delle richieste dei client. Se non configuri il numero di client in esecuzione in una

determinata zona di disponibilità, dovrai dimensionare in modo indipendente ciascuna zona di disponibilità in modo reattivo.

Monitoraggio

Ti consigliamo di monitorare la distribuzione delle connessioni tra le zone di disponibilità utilizzando i parametri del sistema di bilanciamento del carico di zona. Puoi utilizzare i parametri per visualizzare il numero di connessioni nuove e attive per zona.

Ti consigliamo di monitorare i parametri seguenti:

- **`ActiveFlowCount`**: il numero totale di flussi simultanei (o connessioni) da client a target.
- **`NewFlowCount`**: il numero totale di nuovi flussi (o connessioni) stabiliti da client a target nel periodo di tempo.
- **`HealthyHostCount`**: il numero di target considerati integri.
- **`UnHealthyHostCount`**: il numero di target considerati non integri.

Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Network Load Balancer

Attivazione dell'affinità della zona di disponibilità

I passaggi di questa procedura descrivono come attivare l'affinità della zona di disponibilità utilizzando la console Amazon EC2.

Per attivare l'affinità della zona di disponibilità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Configurazione del routing della zona di disponibilità, Politica di instradamento del client (record DNS), seleziona Affinità della zona di disponibilità o Affinità parziale della zona di disponibilità.
6. Seleziona Salvataggio delle modifiche.

Per attivare l'affinità tra le zone di disponibilità, utilizzare il AWS CLI

Utilizza il comando modify-load-balancer-attributes con l'attributo `dns_record.client_routing_policy`.

Disattivazione dell'affinità della zona di disponibilità

I passaggi di questa procedura descrivono come disattivare l'affinità della zona di disponibilità utilizzando la console Amazon EC2.

Per disattivare l'affinità della zona di disponibilità utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Configurazione del routing della zona di disponibilità, Politica di instradamento del client (record DNS), seleziona Qualsiasi zona di disponibilità.
6. Seleziona Salvataggio delle modifiche.

Per disattivare l'affinità della zona di disponibilità utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes con l'attributo `dns_record.client_routing_policy`.

Creazione di un Network Load Balancer

Un sistema di bilanciamento del carico accetta richieste dai client e le distribuisce nei target di un gruppo target, ad esempio nelle istanze EC2.

Prima di iniziare, accertarsi che il cloud privato virtuale (VPC) per il tuo sistema di bilanciamento del carico disponga di almeno una sottorete pubblica in ciascuna zona di disponibilità in cui si dispone di destinazioni. Devi inoltre configurare un gruppo di destinazione e registrare almeno una destinazione da impostare come predefinita per indirizzare il traffico verso il gruppo di destinazione.

Per creare un sistema di bilanciamento del carico utilizzando il AWS CLI, vedere. Tutorial: creazione di un Network Load Balancer tramite AWS CLI

Per creare un sistema di bilanciamento del carico utilizzando il AWS Management Console, completa le seguenti attività.

Attività

- Fase 1: configurazione di un gruppo di destinazioni
- Fase 2: registrazione delle destinazioni
- Fase 3: configurazione di un sistema di bilanciamento del carico e di un ascoltatore
- Fase 4: test del sistema di bilanciamento del carico

Fase 1: configurazione di un gruppo di destinazioni

La configurazione di un gruppo di destinazioni consente di registrare destinazioni come le istanze EC2. Il gruppo di destinazioni configurato in questa fase viene utilizzato come gruppo di destinazioni nella regola dell'ascoltatore quando si configura il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Gruppi di destinazione per i Network Load Balancer.

Per configurare il gruppo target utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Gruppi di destinazioni nel riquadro di navigazione.
3. Scegliere Crea gruppo target.
4. Nel riquadro Configurazione di base, effettua le operazioni seguenti:
    a. In Scegli un tipo di destinazione, seleziona Istanze per registrare le destinazioni in base all'ID istanza, Indirizzi IP per registrare le destinazioni in base all'indirizzo IP o Application Load Balancer per registrare un Application Load Balancer come destinazione.
    b. In Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione.
    c. Per Protocol (Protocollo), scegliere un protocollo come segue:
        - Se il protocollo del listener è TCP, scegliere TCP o TCP_UDP.
        - Se il protocollo del listener è TLS, scegliere TCP o TLS.
        - Se il protocollo del listener è UDP, scegliere UDP o TCP_UDP.
        - Se il protocollo di listener è TCP_UDP, scegliere TCP_UDP.
    d. (Facoltativo) Per Port (Porta) modificare il valore predefinito in base alle esigenze.
    e. Per Tipo di indirizzo IP, scegli IPv4 o IPv6. Questa opzione è disponibile solo se il tipo di destinazione è Istanze o indirizzi IP e se il protocollo è TCP o TLS.

Devi associare un gruppo di destinazione IPv6 a un sistema di bilanciamento del carico dualstack. Tutte le destinazioni del gruppo di destinazione devono avere lo stesso tipo di indirizzo IP. Non è possibile modificare il tipo di indirizzo IP di un gruppo di destinazione dopo averlo creato.

f. Per VPC, seleziona il cloud privato virtuale (VPC) con le destinazioni da registrare.

5. Nel riquadro Controlli dell'integrità, modifica le impostazioni predefinite in base alle esigenze. In Impostazioni avanzate del controllo dello stato, scegli la porta per il controllo dell'integrità, il conteggio, il timeout, l'intervallo e i codici di successo. Se durante i controlli dell'integrità il numero di errori consecutivi supera la Soglia di mancata integrità, il sistema di bilanciamento del carico mette 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) Per aggiungere un tag, espandi Tag, scegli Aggiungi tag e inserisci la chiave e il valore del tag.
7. Seleziona Successivo.

Fase 2: registrazione delle destinazioni

Puoi registrare istanze EC2, indirizzi IP o un Application Load Balancer con il gruppo di destinazione. Si tratta di un passaggio facoltativo per creare un sistema di bilanciamento del carico. Tuttavia, per garantire che il sistema di bilanciamento del carico possa indirizzare il traffico verso le destinazioni, devi registrarle.

1. Nella pagina Registra destinazioni, aggiungi una o più destinazioni nel modo seguente:
   - Se il tipo di destinazione è Istanze, seleziona le istanze, inserisci le porte, quindi scegli Includi come in sospeso di seguito.
   - Se il tipo di destinazione è Indirizzi IP, seleziona la rete, inserisci gli indirizzi IP e le porte, quindi scegli Includi come in sospeso di seguito.
   - Se il tipo di destinazione è Application Load Balancer, seleziona un Application Load Balancer.
2. Scegliere Crea gruppo target.

Fase 3: configurazione di un sistema di bilanciamento del carico e di un ascoltatore

Per creare un Network Load Balancer, devi innanzitutto fornire le informazioni di configurazione di base del sistema di bilanciamento del carico, ad esempio il nome, lo schema e il tipo di indirizzo IP. Fornisci quindi informazioni sulla rete e su uno o più ascoltatori. Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e con una porta per le connessioni dai client al sistema di bilanciamento del carico. Per ulteriori informazioni sui protocolli e le porte supportati, consulta Configurazione dei listener.

Per configurare il sistema di bilanciamento del carico e il listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare Create Load Balancer (Crea sistema di bilanciamento del carico).
4. In Network Load Balancer (Sistema di bilanciamento del carico della rete), 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-nlb`**. Il nome del Network Load Balancer deve essere univoco all'interno del set di Application Load Balancer e Network Load Balancer per la regione. Può avere un massimo di 32 caratteri e contenere solo caratteri alfanumerici e trattini. Non può iniziare o terminare con un trattino o con `internal-`.
   b. In Schema, scegli Connesso a Internet o Interno. Un load balancer su Internet instrada le richieste dai client tramite Internet verso le destinazioni. Un load balancer interno instrada le richieste verso le destinazioni utilizzando indirizzi IP privati.
   c. Per Tipo di indirizzo IP, scegli IPv4 se i client utilizzano indirizzi IPv4 per comunicare con il sistema di bilanciamento del carico o Dualstack se i client utilizzano sia indirizzi IPv4 che IPv6 per tale comunicazione.
6. Mappatura della rete
   a. In VPC, seleziona il VPC utilizzato per le istanze EC2.

      Se hai selezionato Con connessione Internet in Schema, è possibile selezionare solo VPC con un gateway Internet.

b. In Mappature, seleziona una o più zone di disponibilità e le sottoreti corrispondenti. L'abilitazione di più zone di disponibilità aumenta la tolleranza agli errori delle applicazioni. È possibile specificare le sottoreti condivise con l'utente.

   Per i sistemi di bilanciamento del carico con connessione Internet, puoi selezionare un indirizzo IP elastico per ogni zona di disponibilità. Questo fornisce il sistema di bilanciamento del carico con indirizzi IP statici. In alternativa, per un sistema di bilanciamento del carico interno, puoi assegnare un indirizzo IP privato dall'intervallo IPv4 di ciascuna sottorete invece di lasciartene assegnare uno a te. AWS

7. Per Gruppi di sicurezza viene preselezionato il gruppo di sicurezza predefinito per il VPC. Puoi selezionare altri gruppi di sicurezza in base alle esigenze. Se non disponi di un gruppo di sicurezza adatto, scegli Crea un nuovo gruppo di sicurezza e creane uno che soddisfi le tue esigenze di sicurezza. Per ulteriori informazioni, consulta Creazione di un gruppo di sicurezza nella Guida per l'utente di Amazon VPC.

   > ⚠ Warning
   >
   > Se in questa fase decidi di non associare alcun gruppo di sicurezza al sistema di bilanciamento del carico, non potrai farlo in seguito.

8. Ascoltatori e instradamento

   a. L'ascoltatore predefinito accetta il traffico TCP sulla porta 80. Puoi mantenere le impostazioni predefinite dell'ascoltatore o modificare i parametri Protocollo e Porta, in base alle esigenze.

   b. Per Operazione predefinita, seleziona un gruppo di destinazione verso cui inoltrare il traffico. Se non hai creato un gruppo di destinazione in precedenza, creane uno ora. Puoi scegliere facoltativamente Aggiungi listener per aggiungere un altro ascoltatore (ad esempio, un ascoltatore TLS).

   c. (Facoltativo) Aggiungi tag per classificare l'ascoltatore.

   d. In Impostazioni listener sicuro (disponibile solo per gli ascoltatori TLS), esegui le operazioni seguenti:

      i. Per Policy di sicurezza, scegli una policy di sicurezza che soddisfi i requisiti.

      ii. Per ALPN policy (Policy ALPN), scegliere una policy per abilitare ALPN o scegliere None (Nessuna) per disabilitare ALPN.

iii. Per Certificato SSL predefinito, scegli Da ACM (impostazione consigliata) e seleziona un certificato. Se non sono disponibili certificati, è possibile importarne uno in ACM o utilizzare ACM per eseguirne il provisioning. Per ulteriori informazioni, consulta Rilascio e gestione dei certificati nella Guida per l'utente di AWS Certificate Manager .

9. (Facoltativo) Puoi utilizzare i servizi aggiuntivi con il tuo sistema di bilanciamento del carico. Ad esempio, puoi scegliere di AWS Global Acceleratorcreare un acceleratore per te e associare il tuo load balancer all'acceleratore. Il nome dell'acceleratore può contenere i seguenti caratteri (fino a 64 caratteri): a-z, A-Z, 0-9,. (punto) e - (trattino). Dopo aver creato l'acceleratore, vai alla AWS Global Acceleratorconsole per completare la configurazione. Per ulteriori informazioni, consulta Aggiungere un acceleratore quando si crea un sistema di bilanciamento del carico
10. Tag

    (Facoltativo) Aggiungi tag per classificare il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Tag.
11. Riepilogo

    Controlla la configurazione e scegli Crea sistema di bilanciamento del carico. Durante la creazione, vengono applicati alcuni attributi predefiniti al sistema di bilanciamento del carico. È possibile visualizzarli e modificarli dopo la creazione del sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Attributi del sistema di bilanciamento del carico.

Fase 4: test del sistema di bilanciamento del carico

Dopo aver creato il sistema di bilanciamento del carico, puoi verificare che le istanze EC2 abbiano superato il controllo dell'integrità iniziale e testare che il sistema di bilanciamento stia inviando traffico alle istanze EC2. Per eliminare il sistema di bilanciamento del carico, consulta Eliminazione di un Network Load Balancer.

Per effettuare un test del sistema di bilanciamento del carico

1. Dopo la creazione del sistema di bilanciamento del carico, scegli Chiudi.
2. Nel pannello di navigazione a sinistra, scegli Gruppi di destinazione.
3. Selezionare il nuovo gruppo di destinazione.
4. Scegliere Target e verificare che le istanze siano pronte. Se l'istanza è ancora nello stato `initial`, probabilmente si trova nella fase di registrazione o non ha superato il numero minimo di controlli dell'integrità per essere considerata integra. Se lo stato di almeno un'istanza è

healthy, è possibile testare il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Stato di integrità della destinazione.

5. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
6. Seleziona il nuovo sistema di bilanciamento del carico.
7. Copia il nome DNS del load balancer (ad esempio, my-load-balancer -1234567890abcdef.elb.us-east-2.amazonaws.com). Incollare il nome DNS nel campo dell'indirizzo di un browser Web connesso a Internet. Se tutto funziona, il browser visualizza la pagina predefinita del server.

Tipi di indirizzi IP per il Network Load Balancer

Puoi configurare il Network Load Balancer in modo che i client possano comunicare con il sistema di bilanciamento del carico utilizzando solo indirizzi IPv4 o 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.

Requisiti dualstack

- È possibile impostare il tipo di indirizzo IP quando si crea il sistema di bilanciamento del carico e lo si aggiorna in qualsiasi momento.
- 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. Per ulteriori informazioni, consulta Indirizzi IPv6 nella Guida per l'utente di Amazon EC2.
- Il sistema di bilanciamento del carico deve avere solo ascoltatori TCP e TLS.
- Le tabelle di routing per le sottoreti del sistema di bilanciamento del carico devono instradare il traffico IPv6.
- Le liste di controllo degli accessi di rete per le sottoreti del sistema di bilanciamento del carico devono consentire il traffico IPv6.

Per impostare il tipo di indirizzo IP al momento della creazione

Configura le impostazioni come descritto in Creazione di un sistema di bilanciamento del carico.

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. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.

3. Seleziona la casella di controllo relativa al sistema di bilanciamento del carico.
4. Scegli Actions (Azioni), Edit IP address type (Modifica tipo di indirizzo IP).
5. In Tipo di indirizzo IP, seleziona IPv4 per supportare soltanto gli indirizzi IPv4 o Dualstack per supportare sia gli indirizzi IPv4 che IPv6.
6. Seleziona Salvataggio delle modifiche.

Per aggiornare l'indirizzo IP, digitare utilizzando il AWS CLI

Utilizza il comando set-ip-address-type.

Gruppi di sicurezza per il Network Load Balancer

Puoi associare un gruppo di sicurezza al Network Load Balancer per controllare il traffico che può raggiungere e lasciare il sistema di bilanciamento del carico. Specifica le porte, i protocolli e le origini per consentire il traffico in entrata e le porte, i protocolli e le destinazioni per consentire il traffico in uscita. Se non assegni un gruppo di sicurezza al sistema di bilanciamento del carico, tutto il traffico client può raggiungere gli ascoltatori del sistema di bilanciamento del carico e tutto il traffico può uscire dal sistema di bilanciamento del carico.

Puoi aggiungere una regola ai gruppi di sicurezza associati alle destinazioni che faccia riferimento al gruppo di sicurezza associato al Network Load Balancer. Ciò consente ai client di inviare traffico alle destinazioni esclusivamente tramite il sistema di bilanciamento del carico, non in modo diretto. Il riferimento al gruppo di sicurezza associato al Network Load Balancer nei gruppi di sicurezza associati alle destinazioni garantisce che le destinazioni accettino il traffico proveniente dal sistema di bilanciamento del carico anche se si abilita la conservazione dell'IP client per il sistema di bilanciamento del carico.

Il traffico bloccato dalle regole in entrata dei gruppi di sicurezza non viene addebitato.

Indice

Considerazioni

- Puoi associare i gruppi di sicurezza a un Network Load Balancer al momento della creazione. Se non associ un gruppo di sicurezza a un Network Load Balancer al momento della creazione, non puoi associarlo in un secondo momento. Ti consigliamo di associare un gruppo di sicurezza al sistema di bilanciamento del carico al momento della creazione.
- Dopo aver creato un Network Load Balancer con i gruppi di sicurezza associati, puoi modificare i gruppi di sicurezza associati al sistema di bilanciamento del carico in qualsiasi momento.
- I controlli dell'integrità sono soggetti alle regole in uscita, ma non a quelle in entrata. Assicurati che le regole in uscita non blocchino il traffico relativo ai controlli dell'integrità. In caso contrario, il sistema di bilanciamento del carico considera le destinazioni non integre.
- È possibile controllare se il PrivateLink traffico è soggetto alle regole in entrata. Se abiliti le regole in entrata sul PrivateLink traffico, l'origine del traffico è l'indirizzo IP privato del client, non l'interfaccia dell'endpoint.

Esempio: filtraggio del traffico client

Le seguenti regole in entrata nel gruppo di sicurezza associato al Network Load Balancer consentono solo il traffico proveniente dall'intervallo di indirizzi specificato. Nel caso di un sistema di bilanciamento del carico interno, puoi specificare come origine un intervallo CIDR VPC, in modo da consentire solo il traffico proveniente da un VPC specifico. Nel caso di un sistema di bilanciamento del carico con connessione Internet che deve accettare traffico da qualsiasi punto della rete, puoi specificare 0.0.0.0/0 come origine.

In entrata

Protocollo	Origine	Intervallo porte	Commento
protocol	*intervallo di indirizzi IP client*	*porta dell'asco ltatore*	Consente il traffico in entrata dal CIDR di origine sulla porta dell'asco ltatore
ICMP	0.0.0.0/0	Tutti	Consente al traffico ICMP in entrata di supportare la MTU o il rilevamento della MTU del percorso †

† Per ulteriori informazioni, consulta Path MTU Discovery nella Amazon EC2 User Guide.

In uscita

Protocollo	Destinazione	Intervallo porte	Commento
Tutti	Ovunque	Tutti	Autorizza tutto il traffico in uscita

Esempio: accetta traffico solo dal sistema di bilanciamento del carico

Supponiamo che il Network Load Balancer disponga di un gruppo di sicurezza sg-111112222233333. Utilizza le seguenti regole nei gruppi di sicurezza associati alle istanze di destinazione per assicurarti che accettino traffico solo dal Network Load Balancer. Devi assicurarti che le destinazioni accettino il traffico dal sistema di bilanciamento del carico sia sulla porta di destinazione che sulla porta di controllo dell'integrità. Per ulteriori informazioni, consulta the section called “Gruppi di sicurezza target”.

In entrata

Protocollo	Origine	Intervallo porte	Commento
protocol	sg-111112222233333	*porta di destinazione*	Consente il traffico in entrata dal sistema di bilanciamento del carico sulla porta di destinazione
protocol	sg-111112222233333	*controllo dello stato*	Consente il traffico in entrata dal sistema di bilanciamento del carico sulla porta di controllo dell'integrità

In uscita

Protocollo	Destinazione	Intervallo porte	Commento
Tutti	Ovunque	Qualsiasi	Autorizza tutto il traffico in uscita

Aggiornamento dei gruppi di sicurezza associati

Se al momento della creazione hai associato almeno un gruppo di sicurezza a un sistema di bilanciamento del carico, puoi aggiornare i relativi gruppi di sicurezza in qualsiasi momento.

Per aggiornare i gruppi di sicurezza 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. Nella scheda Sicurezza, scegli Modifica.
5. Per associare un gruppo di sicurezza al sistema di bilanciamento del carico, selezionalo. Per rimuovere un gruppo di sicurezza dal sistema di bilanciamento del carico, deselezionalo.
6. Seleziona Salvataggio delle modifiche.

Per aggiornare i gruppi di sicurezza utilizzando il AWS CLI

Utilizza il comando set-security-group.

Aggiornamento delle impostazioni di sicurezza

Per impostazione predefinita, le regole in entrata del gruppo di sicurezza vengono applicate a tutto il traffico inviato al sistema di bilanciamento del carico. Tuttavia, potresti non voler applicare queste regole al traffico inviato al sistema di bilanciamento del carico AWS PrivateLink, che può provenire dalla sovrapposizione di indirizzi IP. In questo caso, puoi configurare il sistema di bilanciamento del carico in modo da non applicare le regole in entrata per il traffico inviato al sistema di bilanciamento del carico tramite. AWS PrivateLink

Per aggiornare le impostazioni di sicurezza 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. Nella scheda Sicurezza, scegli Modifica.
5. In Impostazioni di sicurezza, deseleziona Applica le regole in entrata al traffico. PrivateLink

6. Seleziona Salvataggio delle modifiche.

Per aggiornare le impostazioni di sicurezza utilizzando il AWS CLI

Utilizza il comando set-security-group.

Monitoraggio dei gruppi di sicurezza del sistema di bilanciamento del carico

Utilizza le `SecurityGroupBlockedFlowCount_Outbound` CloudWatch metriche `SecurityGroupBlockedFlowCount_Inbound` and per monitorare il conteggio dei flussi bloccati dai gruppi di sicurezza del load balancer. Il traffico bloccato non si riflette in altri parametri. Per ulteriori informazioni, consulta the section called “CloudWatch metriche”.

Utilizza i log di flusso VPC per monitorare il traffico accettato o rifiutato dai gruppi di sicurezza del sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

Tag per il Network Load Balancer

I tag ti aiutano a classificare i sistemi di bilanciamento del carico in diversi modi. Ad esempio, puoi assegnare tag a una risorsa in base allo scopo, al proprietario o all'ambiente.

È possibile aggiungere più tag a ciascun sistema di bilanciamento del carico. 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 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'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 di un sistema di bilanciamento del carico tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Tag scegliere Gestisci tag.
5. Per aggiungere un tag, scegli Aggiungi tag, quindi specifica la chiave e il valore del tag. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali. I valori di tag fanno distinzione tra maiuscole e minuscole.
6. Per aggiornare un tag, inserisci i nuovi valori in Chiave e Valore.
7. Per eliminare un tag, scegli il pulsante Rimuovi accanto al tag da eliminare.
8. Al termine, scegli Salva le modifiche.

Per aggiornare i tag per un sistema di bilanciamento del carico, utilizzare il AWS CLI

Utilizza i comandi add-tags e remove-tags.

Eliminazione di un Network Load Balancer

Non appena il load balancer diventa disponibile, ti verrà addebitata ogni ora o frazione di ora in cui lo mantieni in esecuzione. Se il sistema di bilanciamento del carico non ti è più utile, puoi eliminarlo. Non appena il load balancer viene eliminato, i relativi addebiti vengono bloccati.

Non è possibile eliminare un sistema di bilanciamento del carico se è abilitata la protezione da eliminazione. Per ulteriori informazioni, consulta Deletion protection (Protezione da eliminazione).

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

L'eliminazione di un sistema di bilanciamento del carico elimina anche i relativi listener. L'eliminazione di un sistema di bilanciamento del carico non influisce sui suoi target registrati. 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.

Per eliminare un sistema di bilanciamento del carico tramite la console

1. Se si dispone di un record DNS nel dominio che punta al sistema di bilanciamento del carico, puntare a una nuova posizione e attendere che il cambio di DNS abbia effetto prima di eliminare il sistema di bilanciamento del carico.

   Esempio:

   - Se il record è un record CNAME con un time-to-live (TTL) di 300 secondi, attendi almeno 300 secondi prima di passare alla fase successiva.
   - Se il record è un record Route 53 Alias(A), attendi almeno 60 secondi.
   - Se si utilizza Route 53, il cambiamento di record richiede 60 secondi per propagarsi in tutti i nomi server globali di Route 53. Aggiungi questo tempo al valore TTL del record in fase di aggiornamento.
2. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
3. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
4. Seleziona la casella di controllo relativa al sistema di bilanciamento del carico.
5. Seleziona Operazioni, Elimina sistema di bilanciamento del carico.
6. Quando viene richiesta la conferma, digita **`confirm`** e scegli Elimina.

Per eliminare un sistema di bilanciamento del carico utilizzando il AWS CLI

Utilizza il comando delete-load-balancer.

Spostamento zonale

Lo spostamento zonale è una funzionalità di Sistema di controllo Amazon Route 53 per il ripristino di applicazioni (Route53 ARC). Con lo spostamento zonale, è possibile spostare una risorsa di un sistema di bilanciamento del carico da una zona di disponibilità danneggiata con una singola operazione. In questo modo è possibile continuare a operare da altre zone di disponibilità integre in una Regione AWS.

Quando si avvia uno spostamento zonale, il sistema di bilanciamento del carico interrompe l'invio di traffico per la risorsa alla zona di disponibilità danneggiata. Route 53 ARC crea immediatamente lo spostamento zonale. Tuttavia, il completamento delle connessioni esistenti e in corso nella zona di

disponibilità danneggiata può richiedere un po' di tempo, generalmente fino a qualche minuto. Per ulteriori informazioni, consulta How a zonal shift works: health checks and zonal IP addresses nella Guida per gli sviluppatori di Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Gli spostamenti zonali sono supportati solo su Application Load Balancer e Network Load Balancer in cui il bilanciamento del carico tra zone è disattivato. Se si attiva il bilanciamento del carico tra zone, non è possibile avviare uno spostamento zonale. Per ulteriori informazioni, consulta Resources supported for zonal shifts nella Guida per gli sviluppatori di Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Prima di utilizzare uno spostamento zonale, consulta le seguenti informazioni:

- Gli spostamenti zonali non supportano il bilanciamento del carico tra zone. Per utilizzare questa funzionalità, è necessario disattivare il bilanciamento del carico tra zone.
- Lo spostamento zonale non è supportato quando si utilizza un Application Load Balancer come endpoint per l'acceleratore in AWS Global Accelerator.
- È possibile avviare uno spostamento zonale per uno specifico sistema di bilanciamento del carico solo per una singola zona di disponibilità. Non è possibile avviare uno spostamento zonale per più zone di disponibilità.
- AWS rimuove in modo proattivo gli indirizzi IP del sistema di bilanciamento del carico zonale dal DNS quando più problemi di infrastruttura influiscono sui servizi. Verificare sempre l'attuale capacità della zona di disponibilità prima di avviare uno spostamento zonale. Se i sistemi di bilanciamento del carico hanno il bilanciamento del carico tra zone disattivato e si utilizza uno spostamento zonale per rimuovere l'indirizzo IP zonale di un sistema di bilanciamento del carico, anche la zona di disponibilità coinvolta nello spostamento zonale perderà capacità di destinazione.
- Quando un Application Load Balancer è una destinazione di un Network Load Balancer, avviare sempre lo spostamento zonale dal Network Load Balancer. Se si avvia uno spostamento zonale dall'Application Load Balancer, il Network Load Balancer non riconoscerà lo spostamento e continuerà a inviare traffico all'Application Load Balancer.

Per ulteriori indicazioni e informazioni, consulta Best practices with Route 53 ARC zonal shifts nella Guida per gli sviluppatori del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Avviare uno spostamento zonale

I passaggi di questa procedura illustrano come avviare uno spostamento zonale utilizzando la console Amazon EC2. Per conoscere i passaggi per avviare uno spostamento zonale utilizzando la

console Route 53 ARC, consulta Starting a zonal shift nella Guida per gli sviluppatori del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Per avviare uno spostamento zonale tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Selezionare il nome del sistema di bilanciamento del carico.
4. Nella scheda Integrazioni, sotto Sistema di controllo Amazon Route 53 per il ripristino di applicazioni, scegli Avvia spostamento zonale.
5. Selezionare la zona di disponibilità dalla quale allontanare il traffico.
6. Scegliere o inserire una scadenza per lo spostamento zonale. Inizialmente è possibile impostare uno spostamento zonale per un tempo che va da 1 minuto a tre giorni (72 ore).

   Tutti gli spostamenti zonali sono temporanei. È necessario impostare una scadenza, ma è possibile aggiornare gli spostamenti attivi in un secondo momento e impostare una nuova scadenza.
7. Inserire un commento. Se lo si desidera, è possibile aggiornare lo spostamento zonale in un secondo momento e modificare il commento.
8. Selezionare la casella di controllo per accettare che l'avvio di uno spostamento zonale ridurrà la capacità dell'applicazione allontanando il traffico dalla zona di disponibilità.
9. Scegli Avvia.

Per avviare uno spostamento zonale utilizzando il AWS CLI

Per utilizzare lo spostamento zonale a livello di programmazione, consulta la Zonal Shift API Reference Guide.

Aggiornare uno spostamento zonale

I passaggi di questa procedura illustrano come aggiornare uno spostamento zonale utilizzando la console Amazon EC2. Per conoscere i passaggi per aggiornare uno spostamento zonale utilizzando la console del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni, consulta Updating a zonal shift nella Guida per gli sviluppatori del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Per aggiornare uno spostamento zonale tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Selezionare il nome di un sistema di bilanciamento del carico con uno spostamento zonale attivo.
4. Nella scheda Integrazioni, sotto Sistema di controllo Amazon Route 53 per il ripristino di applicazioni, scegli Aggiorna spostamento zonale.

   In questo modo si aprirà la console Route 53 ARC per proseguire l'aggiornamento.
5. Per Imposta scadenza dello spostamento zonale, seleziona o inserire facoltativamente una scadenza.
6. Per Commento, modificare il commento esistente o inserire un nuovo commento facoltativamente.
7. Scegli Aggiorna.

Per aggiornare uno spostamento zonale utilizzando il AWS CLI

Per utilizzare lo spostamento zonale a livello di programmazione, consulta la Zonal Shift API Reference Guide.

Annullare uno spostamento zonale

I passaggi di questa procedura illustrano come annullare uno spostamento zonale utilizzando la console Amazon EC2. Per conoscere i passaggi per annullare uno spostamento zonale utilizzando la console del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni, consulta Canceling a zonal shift nella Guida per gli sviluppatori del Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

Per annullare uno spostamento zonale tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Selezionare il nome di un sistema di bilanciamento del carico con uno spostamento zonale attivo.
4. Nella scheda Integrazioni, sotto Sistema di controllo Amazon Route 53 per il ripristino di applicazioni, scegli Annulla spostamento zonale.

In questo modo si aprirà la console Route 53 ARC per proseguire l'annullamento.

5. Scegliere Annulla spostamento zonale.
6. Nel dialogo di conferma, seleziona Elimina.

Per annullare uno spostamento zonale utilizzando il AWS CLI

Per utilizzare lo spostamento zonale a livello di programmazione, consulta la Zonal Shift API Reference Guide.

Ascoltatori per i sistemi Network Load Balancer

Un ascoltatore è un processo che controlla le richieste di connessione utilizzando il protocollo e la porta che hai configurato. Prima di iniziare a utilizzare il Network Load Balancer, è necessario aggiungere almeno un ascoltatore. Se il sistema di bilanciamento del carico non dispone di ascoltatori, non è in grado di ricevere traffico dai client. Le regole definite per un ascoltatore determinano il modo in cui il sistema di bilanciamento del carico instrada le richieste alle destinazioni registrate, come le istanze EC2.

Indice

Configurazione dei listener

I listener supportano i seguenti protocolli e porte:

- Protocolli: TCP, TLS, UDP, TCP_UDP
- Porte: 1-65535

È possibile utilizzare un listener TLS per deviare il lavoro di crittografia e decrittografia sul sistema di bilanciamento del carico, in modo che le applicazioni possano concentrarsi sulla logica di business. Se il listener utilizza un protocollo TLS, è necessario distribuire esattamente un certificato del server SSL sul listener. Per ulteriori informazioni, consulta Listener TLS per il Network Load Balancer.

Per garantire che la decrittografia del traffico TLS venga eseguita dalle destinazioni, e non dal sistema di bilanciamento del carico, puoi creare un ascoltatore TCP sulla porta 443 anziché creare un ascoltatore TLS. Con un ascoltatore TCP, il sistema di bilanciamento del carico trasmette il traffico crittografato alle destinazioni senza decrittografarlo.

Per supportare sia TCP e UDP sulla stessa porta, creare un listener TCP_UDP. I gruppi di destinazione per un listener TCP_UDP devono utilizzare il protocollo TCP_UDP.

Per i Network Load Balancer dualstack, sono supportati solo i protocolli TCP e TLS.

Puoi usarlo WebSockets con i tuoi ascoltatori.

Tutto il traffico di rete per un listener configurato è classificato come traffico volontario. Il traffico di rete che non corrisponde a un listener configurato è classificato come traffico involontario. Anche le richieste ICMP diverse da quelle di tipo 3 sono considerate traffico non intenzionale. I Network Load Balancer eliminano il traffico non intenzionale senza inoltrarlo alle destinazioni. I pacchetti di dati TCP inviati alla porta del listener per un listener configurato che non sono nuove connessioni o parte di una connessione TCP attiva vengono rifiutati con un ripristino TCP (RST).

Per ulteriori informazioni, consulta Instradamento della richiesta nella Guida per l'utente di Elastic Load Balancing.

Regole dei listener

Quando si crea un listener, è necessario specificare una regola per instradare le richieste. Questa regola inoltra le richieste verso il gruppo target indicato. Per aggiornare la regola, consulta Aggiornamento di un ascoltatore per il Network Load Balancer.

Creazione di un ascoltatore TLS per Network Load Balancer

Si definisce listener il processo che verifica la presenza di richieste di connessione. La definizione del listener avviene al momento della creazione di un sistema di bilanciamento del carico; si possono aggiungere listener al sistema in qualsiasi momento.

Prerequisiti

- È necessario specificare un gruppo target per la regola del listener. Per ulteriori informazioni, consulta Per creare un gruppo di destinazione per il Network Load Balancer.
- È necessario specificare un certificato SSL per un listener TLS. Il sistema di bilanciamento del carico utilizza il certificato per terminare la connessione e decrittografare le richieste provenienti dai client prima di inoltrarle alle destinazioni. Per ulteriori informazioni, consulta Certificati server.

Aggiunta di un listener

Il listener si configura con un protocollo e una porta per le connessioni dai client al sistema di bilanciamento del carico e con un gruppo target per la regola predefinita del listener. Per ulteriori informazioni, consulta Configurazione dei listener.

Per aggiungere un listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Aggiungi listener.
5. Per Protocollo, scegli TCP, UDP, TCP_UDP o TLS. Mantenere la porta predefinita o digitare una porta diversa. Per i Network Load Balancer dualstack, sono supportati solo i protocolli TCP e TLS.
6. Per Operazione predefinita, scegli un gruppo di destinazione disponibile.
7. [Listener TLS] In Security policy (Policy di sicurezza), si consiglia di mantenere la policy di sicurezza predefinita.
8. [Listener TLS] In Default SSL certificate (Certificato SSL predefinito), procedere in uno dei seguenti modi:
   - Se hai creato o importato un certificato utilizzando AWS Certificate Manager, scegli Da ACM e scegli il certificato.
   - Se hai caricato un certificato utilizzando IAM, scegli Da IAM e seleziona il certificato.
9. [Listener TLS] Per ALPN policy (Policy ALPN), scegliere una policy per abilitare ALPN o scegliere None (Nessuna) per disabilitare ALPN. Per ulteriori informazioni, consulta Policy ALPN.
10. Scegliere Aggiungi.
11. [Listener TLS] Per aggiungere un elenco di certificati opzionali da usare con il protocollo SNI, consulta Aggiunta di certificati all'elenco dei certificati.

Per aggiungere un ascoltatore utilizzando il AWS CLI

Utilizza il comando create-listener per creare il listener.

Listener TLS per il Network Load Balancer

Per utilizzare un listener TLS, occorre distribuire almeno un certificato server sul sistema di bilanciamento del carico. Il sistema di bilanciamento del carico utilizza il certificato del server per terminare la connessione front-end e quindi decrittografare le richieste provenienti dai client prima di inoltrarle ai target. Tieni presente che per trasmettere il traffico crittografato alle destinazioni senza decrittografia da parte del sistema di bilanciamento del carico, devi creare un ascoltatore TCP sulla porta 443 anziché un ascoltatore TLS. Il sistema di bilanciamento del carico trasmette la richiesta alla destinazione così com'è, senza decrittografarla.

Elastic Load Balancing utilizza una configurazione di negoziazione TLS, nota come policy di sicurezza, per negoziare le connessioni TLS tra un client e il sistema di bilanciamento del carico. Una policy di sicurezza è una combinazione di protocolli e codici. Il protocollo stabilisce una connessione sicura tra un client e un server e garantisce che tutti i dati trasferiti tra il client e il sistema di bilanciamento del carico siano privati. Un codice è un algoritmo di crittografia che utilizza chiavi di crittografia per creare un messaggio codificato. I protocolli utilizzano diversi codici per crittografare i dati su Internet. Durante il processo di negoziazione della connessione, il client e il sistema di bilanciamento del carico forniscono un elenco di crittografie e protocolli supportati, in ordine di preferenza. La prima crittografia nell'elenco del server che corrisponde a una qualsiasi delle crittografie del client viene selezionata per la connessione sicura.

I Network Load Balancer non supportano la rinegoziazione TLS o l'autenticazione TLS reciproca (mTLS). Per il supporto dell'autenticazione TLS reciproca, crea un ascoltatore TCP anziché un ascoltatore TLS. Il sistema di bilanciamento del carico trasmette la richiesta così com'è, in modo da poter implementare l'autenticazione TLS reciproca sulla destinazione.

Per creare un listener TLS, consulta Aggiunta di un listener. Per le demo correlate, consulta Supporto TLS su Network Load Balancer e Supporto SNI su Network Load Balancer.

Certificati server

Il sistema di bilanciamento del carico utilizza un certificato X.509 (certificato server). I certificati sono un modulo digitale di identificazione emesso da un'autorità di certificazione (CA). Un certificato contiene informazioni di identificazione, un periodo di validità, una chiave pubblica, un numero di serie e la firma digitale dell'emittente.

Quando si crea un certificato da utilizzare con il load balancer, occorre specificare un nome di dominio. Il nome di dominio sul certificato deve corrispondere al record del nome di dominio

personalizzato in modo che la connessione TLS possa essere verificata. Se i due nomi non corrispondono, il traffico non viene crittografato.

È necessario specificare un nome di dominio completo (FQDN) per il certificato, ad esempio `www.example.com` o un nome di dominio apex, ad esempio `example.com`. Per proteggere diversi nomi di siti nello stesso dominio, è inoltre possibile utilizzare un asterisco (*) come carattere jolly. Quando si fa richiesta di un certificato jolly, l'asterisco (*) deve essere nella posizione più a sinistra nel nome di dominio e può proteggere solo un livello di sottodominio. Ad esempio, `*.example.com` protegge `corp.example.com` e `images.example.com`, ma non può proteggere `test.login.example.com`. Si noti inoltre come `*.example.com` protegga solo i sottodomini di `example.com` e non il dominio essenziale o apex (`example.com`). Il nome con il carattere jolly appare nel campo Oggetto e nell'estensione Nome oggetto alternativo del certificato. Per ulteriori informazioni sui certificati pubblici, consulta Richiesta di un certificato pubblico nella Guida per l'utente di AWS Certificate Manager .

Ti consigliamo di utilizzare AWS Certificate Manager (ACM) per creare i certificati dei sistemi di bilanciamento del carico. ACM si integra con Elastic Load Balancing in modo da poter implementare il certificato sul load balancer. Per ulteriori informazioni, consulta la Guida per l'utente AWS Certificate Manager.

In alternativa, puoi utilizzare gli strumenti TLS per creare una richiesta di firma del certificato (CSR), quindi farla firmare da una CA per produrre un certificato, quindi importare il certificato in ACM o caricare il certificato su (IAM). AWS Identity and Access Management Per ulteriori informazioni, consulta Importazione di certificati nella Guida per l'utente di AWS Certificate Manager o Utilizzo dei certificati server nella Guida per l'utente di IAM.

Indice

Algoritmi chiave supportati

- RSA a 1024 bit
- RSA a 2048 bit
- RSA a 3072 bit

- ECDSA a 256 bit
- ECDSA a 384 bit
- ECDSA a 521 bit

Certificato predefinito

È necessario specificare un certificato predefinito al momento della creazione di un listener TLS. Questo certificato è noto come certificato predefinito. Puoi sostituire il certificato predefinito dopo aver creato il listener TLS. Per ulteriori informazioni, consulta Sostituzione del certificato predefinito.

Se definisci certificati aggiuntivi in un elenco di certificati, il certificato predefinito viene utilizzato solo se un client si collega senza utilizzare il protocollo Server Name Indication (SNI) per specificare un nome host o se non sono presenti certificati corrispondenti nel relativo elenco.

Se non specifichi certificati aggiuntivi, ma devi ospitare diverse applicazioni sicure attraverso un unico sistema di bilanciamento del carico, puoi usare un certificato jolly o aggiungere un Subject Alternative Name (SAN) per ogni dominio aggiuntivo al tuo certificato.

Elenco dei certificati

Una volta creato. il listener TLS include un certificato predefinito e un elenco di certificati vuoto. Facoltativamente, è possibile aggiungere certificati all'elenco certificati per il listener. In questo modo un sistema di bilanciamento del carico può supportare più domini sulla stessa porta e fornire un certificato diverso per ogni dominio. Per ulteriori informazioni, consulta Aggiunta di certificati all'elenco dei certificati.

Il sistema di bilanciamento del carico supporta inoltre un algoritmo intelligente di selezione dei certificati con SNI. Se il nome host fornito da un client corrisponde a un singolo certificato nell'elenco dei certificati, il sistema di bilanciamento del carico seleziona tale certificato. Se un nome host fornito da un client corrisponde a più certificati nell'elenco dei certificati, il sistema di bilanciamento del carico seleziona il miglior certificato che il client è in grado di supportare. La selezione del certificato si basa sui seguenti criteri nell'ordine seguente:

- Algoritmo hash (preferire SHA su MD5)
- Lunghezza della chiave (preferire la più lunga)
- Periodo di validità

Le voci nei log di accesso al sistema di bilanciamento del carico indicano il nome host specificato dal client e il certificato presentato al client. Per ulteriori informazioni, consulta Voci dei log di accesso.

Rinnovo del certificato

Ogni certificato include un periodo di validità. Devi assicurarti di rinnovare o sostituire il certificato per il sistema di bilanciamento del carico prima della fine del suo periodo di validità. Sono inclusi il certificato predefinito e i certificati presenti nel relativo elenco. Nota che il rinnovo o la sostituzione di un certificato non influenza le normali richieste che erano state ricevute da un nodo del sistema di bilanciamento del carico e che sono in attesa di essere instradate a una destinazione integra. Dopo il rinnovo di un certificato, le nuove richieste utilizzano il certificato rinnovato. Dopo la sostituzione di un certificato, le nuove richieste utilizzano il nuovo certificato.

È possibile gestire il rinnovo e la sostituzione del certificato come segue:

- I certificati forniti AWS Certificate Manager e distribuiti sul sistema di bilanciamento del carico possono essere rinnovati automaticamente. ACM cerca di rinnovare i certificati prima della scadenza. Per ulteriori informazioni, consulta Rinnovo gestito nella Guida per l'utente di AWS Certificate Manager .
- Se hai importato un certificato in ACM, la data di scadenza del certificato deve essere monitorata per rinnovarlo prima che scada. Per ulteriori informazioni, consulta Importazione di certificati nella Guida per l'utente di AWS Certificate Manager .
- Se si importa un certificato in IAM, è necessario creare un nuovo certificato, importare il nuovo certificato in ACM o IAM, aggiungere il nuovo certificato al sistema di bilanciamento del carico e rimuovere il certificato scaduto dal sistema di bilanciamento del carico.

Policy di sicurezza

Quando crei un listener TLS, devi selezionare una policy di sicurezza. Puoi aggiornare la policy di sicurezza in base alle esigenze. Per ulteriori informazioni, consulta Aggiornamento della policy di sicurezza.

Considerazioni:

- La `ELBSecurityPolicy-TLS13-1-2-2021-06` politica è la politica di sicurezza predefinita per i listener TLS creata utilizzando. AWS Management Console
  - Consigliamo la politica `ELBSecurityPolicy-TLS13-1-2-2021-06` di sicurezza, che include TLS 1.3 ed è retrocompatibile con TLS 1.2.

- La `ELBSecurityPolicy-2016-08` politica è la politica di sicurezza predefinita per i listener TLS creata utilizzando. AWS CLI
- È possibile scegliere la politica di sicurezza utilizzata per le connessioni front-end, ma non per le connessioni backend.
  - Per le connessioni back-end, se l'ascoltatore TLS utilizza una policy di sicurezza TLS 1.3, viene utilizzata la policy di sicurezza `ELBSecurityPolicy-TLS13-1-0-2021-06`. In caso contrario, la policy di sicurezza `ELBSecurityPolicy-2016-08` viene utilizzata per le connessioni back-end.
- Per soddisfare gli standard di conformità e sicurezza che richiedono la disabilitazione di determinate versioni del protocollo TLS o per supportare client legacy che richiedono cifrari obsoleti, puoi utilizzare una delle politiche di sicurezza. `ELBSecurityPolicy-TLS-` Puoi abilitare i log di accesso per informazioni sulle richieste TLS inviate al tuo Network Load Balancer, analizzare i modelli di traffico TLS, gestire gli aggiornamenti delle politiche di sicurezza e risolvere i problemi. Abilita la registrazione degli accessi per il tuo sistema di bilanciamento del carico ed esamina le voci del registro di accesso corrispondenti. Per ulteriori informazioni, consulta Log di accesso e Query di esempio di Network Load Balancer.
- Puoi limitare le policy di sicurezza disponibili per gli utenti in tutto il tuo Account AWS e AWS Organizations utilizzando le chiavi di condizione Elastic Load Balancing rispettivamente nelle tue policy IAM e service control (SCP). Per ulteriori informazioni, consulta le politiche di controllo dei servizi (SCP) nella Guida per l'utente AWS Organizations

Policy di sicurezza TLS 1.3

Elastic Load Balancing fornisce le seguenti politiche di sicurezza TLS 1.3 per Network Load Balancer:

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(Consigliato)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06`
- `ELBSecurityPolicy-TLS13-1-1-2021-06`
- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

Politiche di sicurezza FIPS

Il Federal Information Processing Standard (FIPS) è uno standard governativo statunitense e canadese che specifica i requisiti di sicurezza per i moduli crittografici che proteggono le informazioni sensibili. Per ulteriori informazioni, consulta Federal Information Processing Standard (FIPS) 140 nella pagina AWS Cloud Security Compliance.

Tutte le politiche FIPS sfruttano il modulo crittografico convalidato FIPS AWS-LC. Per saperne di più, consulta la pagina del modulo crittografico AWS-LC sul sito del NIST Cryptographic Module Validation Program.

Elastic Load Balancing fornisce le seguenti politiche di sicurezza FIPS per Network Load Balancer:

- `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`(Consigliato)
- `ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`

Policy FS supportate

Elastic Load Balancing fornisce le seguenti politiche di sicurezza supportate da FS (Forward Secrecy) per Network Load Balancer:

- `ELBSecurityPolicy-FS-1-2-Res-2020-10`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-2018-06`

Politiche di sicurezza TLS 1.0 - 1.2

Elastic Load Balancing fornisce le seguenti politiche di sicurezza TLS 1.0 - 1.2 per Network Load Balancer:

- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-2015-05`(identico a) **`ELBSecurityPolicy-2016-08`**

Protocolli e cifrari TLS

TLS 1.3

La tabella seguente descrive i protocolli e i codici TLS supportati per le politiche di sicurezza TLS 1.3 disponibili.

Nota: il `ELBSecurityPolicy-` prefisso è stato rimosso dai nomi delle politiche nella riga delle politiche di sicurezza.

Esempio: la politica di sicurezza `ELBSecurityPolicy-TLS13-1-2-2021-06` viene visualizzata come`TLS13-1-2-2021-06`.

Policy di sicurezza	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocolli TLS							
Protocollo-TLSv1							✓

Policy di sicurezza	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓
Protocollo-TLSv1.3	✓	✓	✓	✓	✓	✓	✓
Crittografie TLS							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓

Policy di sicurezza	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓			✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓			✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓
ECDHE-RSA-AES128-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓

Policy di sicurezza	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-RSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓
AES128-GCM-SHA256				✓	✓	✓	✓

Policy di sicurezza	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

Per creare un listener TLS che utilizzi una policy TLS 1.3 utilizzando la CLI

Utilizza il comando create-listener con qualsiasi politica di sicurezza TLS 1.3.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-TLS13-1-2-2021-06`

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Per modificare un listener TLS per utilizzare una politica TLS 1.3 utilizzando la CLI

Utilizza il comando modify-listener con qualsiasi politica di sicurezza TLS 1.3.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-TLS13-1-2-2021-06`

```
aws elbv2 modify-listener \
```

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Per visualizzare le politiche di sicurezza utilizzate da un listener utilizzando la CLI

Usa il comando describe-listener con il tuo listener. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Per visualizzare la configurazione di una politica di sicurezza TLS 1.3 utilizzando la CLI

Utilizza il describe-ssl-policiescomando con qualsiasi politica di sicurezza TLS 1.3.

L'esempio utilizza la politica `ELBSecurityPolicy-TLS13-1-2-2021-06` di sicurezza.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

> **Important**
>
> Le politiche `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` e `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` vengono fornite solo per la compatibilità con le versioni precedenti. Sebbene utilizzino la crittografia FIPS utilizzando il modulo FIPS140, potrebbero non essere conformi alle ultime linee guida NIST per la configurazione TLS.

La tabella seguente descrive i protocolli e i codici TLS supportati per le politiche di sicurezza FIPS disponibili.

Nota: il `ELBSecurityPolicy-` prefisso è stato rimosso dai nomi delle politiche nella riga delle politiche di sicurezza.

Esempio: la politica di sicurezza `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` viene visualizzata come`TLS13-1-2-FIPS-2023-04`.

Policy di sicurezza	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocolli TLS								
Protocollo-TLSv1								✓
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
Protocollo-TLSv1.3	✓	✓	✓	✓	✓	✓	✓	✓
Crittografie TLS								
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-		✓	✓	✓	✓	✓	✓	✓

Policy di sicurezza	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
SHA256								
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓	✓

Policy di sicurezza	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384			✓	✓	✓	✓	✓	✓

Policy di sicurezza	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓

Policy di sicurezza	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

Per creare un listener TLS che utilizzi una policy FIPS utilizzando la CLI

Utilizzate il comando create-listener con qualsiasi politica di sicurezza FIPS.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Per modificare un listener TLS per utilizzare una politica FIPS utilizzando la CLI

Utilizzate il comando modify-listener con qualsiasi politica di sicurezza FIPS.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Per visualizzare le politiche di sicurezza utilizzate da un listener utilizzando la CLI

Usa il comando describe-listener con il tuo listener. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Per visualizzare la configurazione di una politica di sicurezza FIPS utilizzando la CLI

Utilizzare il describe-ssl-policiescomando con qualsiasi politica di sicurezza FIPS.

L'esempio utilizza la politica `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` di sicurezza.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

La tabella seguente descrive i protocolli e i codici TLS supportati per le politiche di sicurezza supportate da FS disponibili.

Nota: il `ELBSecurityPolicy-` prefisso è stato rimosso dai nomi delle politiche nella riga delle politiche di sicurezza.

Esempio: la politica di sicurezza `ELBSecurityPolicy-FS-2018-06` viene visualizzata come`FS-2018-06`.

Policy di sicurezza	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocolli TLS						
Protocollo-TLSv1	✓					✓

Policy di sicurezza	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocol-TLSv1.1	✓				✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Crittografie TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓

Policy di sicurezza	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓		✓	✓	✓	✓

Policy di sicurezza	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					
AES256-GCM-SHA384	✓					

Policy di sicurezza	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-SHA256	✓					
AES256-SHA	✓					

Per creare un listener TLS che utilizzi una policy supportata da FS utilizzando la CLI

Utilizza il comando create-listener con qualsiasi politica di sicurezza supportata da FS.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-FS-2018-06`

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Per modificare un listener TLS per utilizzare una policy supportata da FS utilizzando la CLI

Usa il comando modify-listener con qualsiasi politica di sicurezza supportata da FS.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-FS-2018-06`

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Per visualizzare le politiche di sicurezza utilizzate da un listener utilizzando la CLI

Usa il comando describe-listener con il tuo listener. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Per visualizzare la configurazione di una politica di sicurezza supportata da FS utilizzando la CLI

Usa il describe-ssl-policiescomando con qualsiasi politica di sicurezza supportata da FS.

L'esempio utilizza la politica `ELBSecurityPolicy-FS-2018-06` di sicurezza.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

La tabella seguente descrive i protocolli e i codici TLS supportati per le politiche di sicurezza TLS 1.0-1.2 disponibili.

Nota: il `ELBSecurityPolicy-` prefisso è stato rimosso dai nomi delle politiche nella riga delle politiche di sicurezza.

Esempio: la politica di sicurezza `ELBSecurityPolicy-TLS-1-2-Ext-2018-06` viene visualizzata come`TLS-1-2-Ext-2018-06`.

Policy di sicurezza	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocolli TLS					
Protocollo-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓

Policy di sicurezza	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocol-TLSv1.2	✓	✓	✓	✓	✓
Crittografie TLS					
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	✓		✓	✓
ECDHE-RSA-AES128-SHA	✓	✓		✓	✓

Policy di sicurezza	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓	✓		✓	✓
ECDHE-ECDSA-AES256-SHA	✓	✓		✓	✓
AES128-GCM-SHA256	✓	✓	✓	✓	✓
AES128-SHA256	✓	✓	✓	✓	✓

Policy di sicurezza	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
AES128-SHA	✓	✓		✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓
DES-CBC3-SHA					✓

* Non utilizzare questa policy a meno che non si debba supportare un client legacy che richiede la crittografia DES-CBC3-SHA, che è una crittografia debole.

Per creare un listener TLS che utilizzi una policy TLS 1.0-1.2 utilizzando la CLI

Utilizza il comando create-listener con qualsiasi politica di sicurezza supportata da TLS 1.0-1.2.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-2016-08`

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Per modificare un listener TLS per utilizzare una politica TLS 1.0-1.2 utilizzando la CLI

Utilizza il comando modify-listener con qualsiasi politica di sicurezza supportata da TLS 1.0-1.2.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-2016-08`

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Per visualizzare le politiche di sicurezza utilizzate da un listener utilizzando la CLI

Usa il comando describe-listener con il tuo listener. `arn`

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Per visualizzare la configurazione di una politica di sicurezza TLS 1.0-1.2 utilizzando la CLI

Utilizza il describe-ssl-policiescomando con qualsiasi politica di sicurezza supportata da TLS 1.0-1.2.

L'esempio utilizza la politica di sicurezza. `ELBSecurityPolicy-2016-08`

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-2016-08
```

Policy ALPN

Application-Layer Protocol Negotiation (ALPN) è un'estensione TLS che viene inviata nei messaggi Hello di handshake TLS iniziali. ALPN consente al livello dell'applicazione di negoziare quali protocolli devono essere utilizzati su una connessione sicura, ad esempio HTTP/1 e HTTP/2.

Quando il client avvia una connessione ALPN, il sistema di bilanciamento del carico confronta l'elenco delle preferenze ALPN client con la relativa policy ALPN. Se il client supporta un protocollo dalla policy ALPN, il sistema di bilanciamento del carico stabilisce la connessione in base all'elenco delle preferenze della policy ALPN. In caso contrario, il sistema di bilanciamento del carico non utilizza ALPN.

Policy ALPN supportate

Di seguito sono riportati le policy ALPN supportate:

`HTTP10nly`

Negoziare solo HTTP/1.*. L'elenco delle preferenze ALPN è http/1.1, http/1.0.

`HTTP20nly`

Negoziare solo HTTP/2. L'elenco delle preferenze ALPN è h2.

`HTTP20ptional`

Preferire HTTP/1.* rispetto a HTTP/2 (che può essere utile per i test HTTP/2). L'elenco delle preferenze ALPN è http/1.1, http/1.0, h2.

`HTTP2Preferred`

Preferire HTTP/2 rispetto a HTTP/1.*. L'elenco delle preferenze ALPN è h2, http/1.1, http/1.0.

`None`

Non negoziare ALPN. Questa è l'impostazione predefinita.

Abilitare connessioni ALPN

È possibile abilitare le connessioni ALPN quando si crea o si modifica un listener TLS. Per ulteriori informazioni, consulta Aggiunta di un listener e Aggiornamento della policy ALPN.

Aggiornamento di un ascoltatore per il Network Load Balancer

È possibile aggiornare il protocollo dell'ascoltatore, la porta dell'ascoltatore o il gruppo di destinazione che riceve il traffico dall'operazione di inoltro. L'operazione predefinita, nota anche come regola predefinita, inoltra le richieste al gruppo di destinazione selezionato.

Se si modifica il protocollo da TCP o UDP a TLS, è necessario specificare una policy di sicurezza e un certificato server. Se si modifica il protocollo da TLS a TCP o UDP, la policy di sicurezza e il certificato server vengono rimossi.

Quando il gruppo di destinazione per l'operazione predefinita dell'ascoltatore viene aggiornato, le nuove connessioni vengono instradate al gruppo di destinazione appena configurato. Tuttavia, ciò non ha alcun effetto sulle connessioni attive create prima di questa modifica. Tali connessioni attive rimangono associate alla destinazione nel gruppo di destinazione originale per un massimo di un'ora, se viene inviato traffico, o fino allo scadere del periodo di inattività se non viene inviato traffico, a

seconda della condizione che si verifica per prima. Il parametro `Connection termination on deregistration` non viene applicato durante l'aggiornamento dell'ascoltatore, ma nel momento in cui si annulla la registrazione delle destinazioni.

Per aggiornare il listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Scegli Modifica.
6. (Facoltativo) Modifica i valori specificati in Protocollo e Porta in base alle esigenze.
7. (Facoltativo) Scegli un gruppo di destinazione diverso per Operazione predefinita.
8. (Facoltativo) Aggiungi, aggiorna o rimuovi tag in base alle esigenze.
9. Seleziona Salvataggio delle modifiche.

Per aggiornare il tuo listener usando il AWS CLI

Utilizza il comando modify-listener.

Aggiornamento di un ascoltatore TLS per il Network Load Balancer

Dopo aver creato un listener TLS, è possibile sostituire il certificato predefinito, aggiungere o rimuovere certificati dall'elenco di certificati, aggiornare la policy di sicurezza o aggiornare la policy ALPN.

Attività

- Sostituzione del certificato predefinito
- Aggiunta di certificati all’elenco dei certificati
- Rimozione di un certificato dall’elenco dei certificati
- Aggiornamento della policy di sicurezza
- Aggiornamento della policy ALPN

Sostituzione del certificato predefinito

È possibile sostituire il certificato predefinito per il listener TLS tramite la seguente procedura. Per ulteriori informazioni, consulta Certificato predefinito.

Per sostituire il certificato predefinito utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Per Certificato SSL predefinito, eseguire una delle seguenti operazioni:
   - Se hai creato o importato un certificato utilizzando AWS Certificate Manager, scegli Da ACM e scegli il certificato.
   - Se hai caricato un certificato utilizzando IAM, scegli Da IAM e seleziona il certificato.
6. Seleziona Salvataggio delle modifiche.

Per sostituire il certificato predefinito utilizzando il AWS CLI

Utilizzare il comando modify-listener con l'opzione --certificates.

Aggiunta di certificati all’elenco dei certificati

È possibile aggiungere certificati all'elenco di certificati per il listener tramite la seguente procedura. Quando crei un listener TLS per la prima volta, l’elenco di certificati è vuoto. Puoi aggiungere uno o più certificati. Puoi opzionalmente aggiungere il certificato predefinito per accertarti che questo certificato venga utilizzato con il protocollo SNI anche se viene sostituito come certificato predefinito. Per ulteriori informazioni, consulta Elenco dei certificati.

Aggiunta di certificati all’elenco certificati tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.

4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Seleziona la casella di controllo per l'ascoltatore e scegli Operazioni, Aggiungi certificati SSL per SNI.
6. Per aggiungere certificati già gestiti da ACM o IAM, seleziona le caselle di controllo per i certificati e scegli Includi come in sospeso di seguito.
7. Se disponi di un certificato non gestito da ACM o IAM, scegli Importa certificato, compila il modulo e seleziona Importa.
8. Scegliere Aggiungi certificati in sospeso.

Per aggiungere un certificato all'elenco dei certificati utilizzando il AWS CLI

Utilizza il comando add-listener-certificates.

Rimozione di un certificato dall’elenco dei certificati

È possibile rimuovere certificati dall'elenco di certificati per un listener TLS tramite la seguente procedura. Per rimuovere il certificato predefinito per un listener TLS consulta Sostituzione del certificato predefinito.

Per rimuovere i certificati dall’elenco certificati tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Seleziona la casella di controllo per l'ascoltatore e scegli Operazioni, Aggiungi certificati SSL per SNI.
6. Selezionare le caselle di controllo per i certificati e scegliere Remove (Rimuovi).
7. Quando viene richiesta la conferma, digita **`confirm`** e scegli Rimuovi.

Per rimuovere un certificato dall'elenco dei certificati utilizzando il AWS CLI

Utilizza il comando remove-listener-certificates.

Aggiornamento della policy di sicurezza

Al momento della creazione di un listener TLS, è possibile selezionare la policy di sicurezza più adatta alle proprie esigenze. Quando viene aggiunta una nuova policy di sicurezza, è possibile aggiornare l'ascoltatore TLS per utilizzare la nuova policy di sicurezza. I Network Load Balancer non supportano policy di sicurezza personalizzate. Per ulteriori informazioni, consulta Policy di sicurezza.

Per aggiungere una policy di sicurezza utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Scegli Modifica.
6. In Policy di sicurezza, scegli una policy di sicurezza.
7. Seleziona Salvataggio delle modifiche.

Per aggiornare la politica di sicurezza utilizzando il AWS CLI

Utilizzare il comando modify-listener con l'opzione --ssl-policy.

Aggiornamento della policy ALPN

Puoi aggiornare la policy ALPN per il listener TLS utilizzando la procedura seguente. Per ulteriori informazioni, consulta Policy ALPN.

Per aggiornare la policy ALPN utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli il testo nella colonna Protocol:Port per aprire la pagina dei dettagli dell'ascoltatore.
5. Scegli Modifica.

6. Per ALPN policy (Policy ALPN), scegliere una policy per abilitare ALPN o scegliere None (Nessuna) per disabilitare ALPN.
7. Seleziona Salvataggio delle modifiche.

Per aggiornare la politica ALPN utilizzando il AWS CLI

Utilizzare il comando modify-listener con l'opzione --alpn-policy.

Eliminazione di un ascoltatore TLS per il Network Load Balancer

Puoi eliminare un listener in qualsiasi momento.

Per eliminare un listener utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona la casella di controllo per il sistema di bilanciamento del carico.
4. Nella scheda Listener, seleziona la casella di controllo dell'ascoltatore, quindi scegli Operazioni, Elimina ascoltatore.
5. Quando viene richiesta la conferma, digita **`confirm`** e scegli Elimina.

Per eliminare un ascoltatore utilizzando il AWS CLI

Utilizza il comando delete-listener.

Gruppi di destinazione per i Network 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 del listener. È possibile creare diversi gruppi target per diversi tipi di richieste. Ad esempio, è possibile creare un gruppo target per le richieste generali e altri gruppi target per le richieste per i microservizi dell'applicazione. Per ulteriori informazioni, consulta Componenti di un sistema Network Load Balancer.

È possibile definire le impostazioni di controllo dello stato per il sistema di bilanciamento del carico 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 listener, il sistema di bilanciamento del carico monitora continuamente lo stato di tutti i target registrati con il gruppo target che si trovano in una zona di disponibilità abilitata per il sistema di bilanciamento del carico. Il sistema di bilanciamento del carico instrada le richieste ai target registrati con stato integro. Per ulteriori informazioni, consulta Controlli dello stato per i gruppi target.

Indice

- Tag per il gruppo target
- Eliminazione di un gruppo target

Configurazione dell'instradamento

Per impostazione predefinita, un sistema di bilanciamento del carico instrada le richieste ai target utilizzando il protocollo e il numero di porta specificati al momento della creazione del gruppo target. In alternativa, è possibile sostituire la porta utilizzata per l'instradamento del traffico a un target al momento della registrazione con il gruppo target.

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

- Protocolli: TCP, TLS, UDP, TCP_UDP
- Porte: 1-65535

Se un gruppo target è configurato con il protocollo TLS, il sistema di bilanciamento del carico stabilisce le connessioni TLS con le destinazioni utilizzando i certificati installati nelle destinazioni. Il sistema di bilanciamento del carico non convalida questi certificati. Pertanto, è possibile utilizzare certificati autofirmati o certificati scaduti. Poiché il sistema di bilanciamento del carico si trova in un cloud privato virtuale (VPC), il traffico tra il sistema di bilanciamento del carico e le destinazioni viene autenticato a livello di pacchetto, quindi non è a rischio man-in-the-middle di attacchi o spoofing anche se i certificati sulle destinazioni non sono validi.

La tabella seguente riepiloga le combinazioni supportate del protocollo di listener e le impostazioni del gruppo di destinazione.

Protocollo del listener	Protocollo del gruppo di destinazione	Tipo di gruppo di destinazione	Protocollo controllo dello stato
TCP	TCP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP
TCP	TCP	alb	HTTP | HTTPS
TLS	TCP | TLS	instance | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	instance | ip	HTTP | HTTPS | TCP

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 di destinazione, non è possibile modificarne il tipo di destinazione.

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.

`alb`

La destinazione è un sistema Application Load Balancer.

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.

Tutti i blocchi CIDR consentono di registrare le seguenti destinazioni in un gruppo di destinazioni:

- AWS risorse indirizzabili tramite indirizzo IP e porta (ad esempio database).
- Risorse locali collegate a una connessione VPN da sito a sito AWS Direct Connect o AWS tramite una connessione VPN.

Quando la conservazione dell'IP del client è disabilitata per i gruppi di destinazione, il sistema di bilanciamento del carico può supportare circa 55.000 connessioni al minuto per ogni combinazione di indirizzo IP del Network Load Balancer e destinazione univoca (indirizzo IP e porta). Se si superano queste connessioni, aumenta il rischio di errori di allocazione delle porte. Se si ottengono errori di allocazione di porta, aggiungere altri target al gruppo target.

Quando si avvia un Network Load Balancer in un Amazon VPC condiviso (come partecipante), è possibile registrare le destinazioni solo nelle sottoreti che sono state condivise con l'utente.

Quando il tipo di destinazione è `alb`, è possibile registrare un singolo Application Load Balancer come destinazione. Per ulteriori informazioni, consulta Application Load Balancer come destinazioni.

I Network Load Balancer non supportano il tipo di destinazione `lambda`. I sistemi Application Load Balancer sono gli unici sistemi di bilanciamento del carico che supportano il tipo di destinazione `lambda`. Per ulteriori informazioni, consulta Lambda functions as targets nella Guida per l'utente di Application Load Balancer.

Se sono presenti microservizi nelle istanze registrate con un Network Load Balancer, non è possibile utilizzare il sistema di bilanciamento del carico per permettere la comunicazione tra di essi, a meno che tale sistema non sia connesso a Internet o le istanze non siano registrate in base all'indirizzo IP. Per ulteriori informazioni, consulta Connessioni scadute per le richieste provenienti da un target al sistema di bilanciamento del carico.

Instradamento delle richieste e indirizzi IP

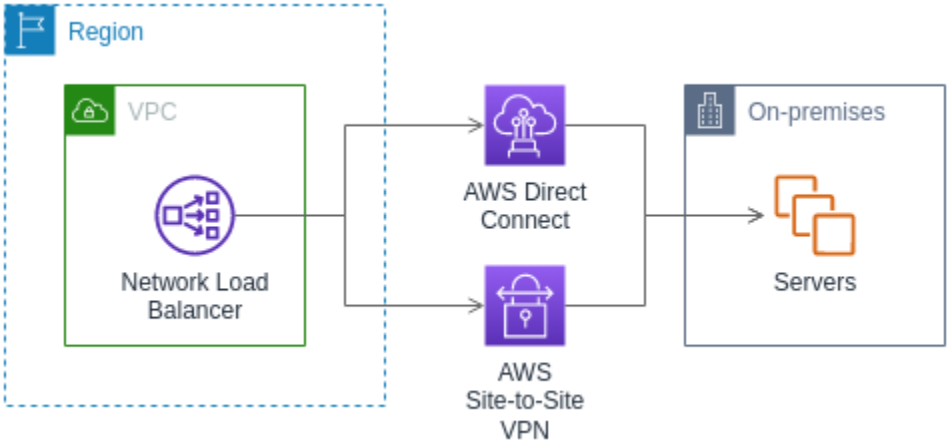
Se le destinazioni vengono specificate utilizzando un ID istanza, il traffico viene instradato alle istanze utilizzando l'indirizzo IP privato primario specificato nell'interfaccia di rete primaria per l'istanza. Il sistema di bilanciamento del carico riscrive l'indirizzo IP di destinazione dal pacchetto di dati prima di inoltrarlo all'istanza di destinazione.

Se i target vengono specificati utilizzando gli indirizzi IP, è possibile instradare il traffico a un'istanza utilizzando qualsiasi indirizzo IP privato di una o più interfacce di rete. Ciò consente a più applicazioni in un'istanza di utilizzare la stessa porta. Ogni interfaccia di rete può avere il proprio gruppo di sicurezza. Il sistema di bilanciamento del carico riscrive l'indirizzo IP di destinazione prima di inoltrarlo alla destinazione.

Per ulteriori informazioni su come consentire il traffico verso le istanze, consulta Gruppi di sicurezza target.

Risorse on-premise come destinazioni

Le risorse locali collegate tramite AWS Direct Connect o una connessione VPN da sito a sito possono fungere da destinazione, se il tipo di destinazione lo è. `ip`



Quando si utilizzano le risorse on-premise, gli indirizzi IP di tali destinazioni devono comunque provenire da uno dei seguenti blocchi CIDR:

- 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 ulteriori informazioni su AWS Direct Connect, consulta What is? AWS Direct Connect

Per ulteriori informazioni su AWS Site-to-Site VPN, vedi Cos'è AWS Site-to-Site VPN?

Tipo di indirizzo IP

Durante la creazione di un nuovo gruppo di destinazioni, è possibile seleziona il tipo di indirizzo IP del gruppo. Ciò consente di verificare la versione IP utilizzata per comunicare con le destinazioni e il relativo stato di integrità.

I Network Load Balancer supportano sia i gruppi di destinazione IPv4 che IPv6. L'opzione predefinita è IPv4. I gruppi di destinazione IPv6 possono essere associati solo a Network Load Balancer dualstack.

Considerazioni

- Tutti gli indirizzi IP all'interno di un gruppo di destinazioni devono avere lo stesso tipo di indirizzo IP. Ad esempio, non è possibile registrare una destinazione IPv4 con un gruppo di destinazione IPv6.
- I gruppi di destinazione IPv6 possono essere utilizzati solo con sistemi di bilanciamento del carico `dualstack` con ascoltatori TCP o TLS.
- I gruppi di destinazione IPv6 supportano le destinazioni di tipo IP e Istanza.

Destinazioni registrate

Il sistema di bilanciamento del carico funge da singolo punto di contatto per i client e distribuisce il traffico in entrata tra i target registrati con stato integro. Ogni gruppo target deve avere almeno un target registrato in ciascuna zona di disponibilità abilitata per il sistema di bilanciamento del carico. È possibile registrare ogni target con uno o più gruppi target.

Se il carico di richieste per l'applicazione aumenta, puoi registrare target aggiuntivi con uno o più gruppi target al fine di gestire le richieste. Il load balancer inizia a indirizzare il traffico verso una nuova destinazione registrata non appena il processo di registrazione viene completato e la destinazione supera il primo controllo di integrità iniziale, indipendentemente dalla soglia configurata.

Se il carico di richieste per l'applicazione diminuisce o devi eseguire la manutenzione delle destinazioni, puoi annullare la loro registrazione dai gruppi di destinazione. L'annullamento della registrazione di un target rimuove il target dal gruppo target, ma non influisce in altro modo sul target stesso. Il sistema di bilanciamento del carico arresta l'instradamento del traffico a un target 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.

Se stai eseguendo la registrazione delle destinazioni in base all'ID istanza, puoi utilizzare il sistema di bilanciamento del carico con un gruppo con dimensionamento automatico. Dopo aver collegato un gruppo di destinazioni a un gruppo con dimensionamento automatico, il dimensionamento automatico registra automaticamente le destinazioni nel gruppo di destinazioni al momento dell'avvio. Per maggiori informazioni, consulta Come allegare un sistema di bilanciamento del carico al gruppo con dimensionamento automatico nella Guida per l'utente di Dimensionamento automatico Amazon EC2.

Requisiti e considerazioni

- Non è possibile registrare le istanze in base all'ID istanza per i tipi di istanza seguenti: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1.
- Quando si registrano le destinazioni in base all'ID istanza per un gruppo di destinazione IPv6, è necessario assegnare alle destinazioni un indirizzo IPv6 primario. Per ulteriori informazioni, consulta gli indirizzi IPv6 nella Guida per l'utente di Amazon EC2
- Quando si registrano le destinazioni in base all'ID istanza, le istanze devono trovarsi nello stesso Amazon VPC del Network Load Balancer. Non è possibile registrare le istanze in base all'ID istanza se si trovano in un VPC collegato in peering al VPC del sistema di bilanciamento del carico (stessa regione o regione diversa). È possibile registrare queste istanze in base all'indirizzo IP.
- Se si registra una destinazione in base all'indirizzo IP e l'indirizzo IP si trova nello stesso VPC del sistema di bilanciamento del carico, il bilanciamento del carico verifica che provenga da una subnet che può raggiungere.
- Il sistema di bilanciamento del carico indirizza il traffico verso le destinazioni solo nelle zone di disponibilità abilitate. Le destinazioni nelle zone non abilitate non vengono utilizzate.
- Per i gruppi di destinazione UDP e TCP_UDP, non registrare le istanze in base all'indirizzo IP se risiedono all'esterno del VPC del sistema di bilanciamento del carico o se utilizzano uno dei seguenti tipi di istanza: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1. Le destinazioni che risiedono all'esterno del VPC del sistema di bilanciamento del carico o che utilizzano un tipo di istanza non supportato potrebbero ricevere traffico dal sistema di bilanciamento del carico ma non essere in grado di rispondere.

Attributi dei gruppi di destinazione

Di seguito sono elencati gli attributi dei gruppi di destinazione supportati. Puoi modificare questi attributi solo se il tipo di gruppo di destinazione è `instance` o `ip`. Se il tipo di gruppo di destinazione è `alb`, questi attributi utilizzano sempre i valori predefiniti.

`deregistration_delay.timeout_seconds`

La quantità di tempo che Elastic Load Balancing attende prima di modificare lo stato di una destinazione 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.

`deregistration_delay.connection_termination.enabled`

Indica se il sistema di bilanciamento del carico termina le connessioni alla fine del timeout di annullamento della registrazione. Il valore è `true` o `false`. Per i nuovi gruppi di destinazione UDP/TCP_UDP, l'opzione predefinita è `true`. In caso contrario, l'impostazione predefinita è `false`.

`load_balancing.cross_zone.enabled`

Indica se è abilitato il sistema di bilanciamento del carico tra zone. Il valore è `true`, `false` o `use_load_balancer_configuration`. Il valore predefinito è `use_load_balancer_configuration`.

`preserve_client_ip.enabled`

Indica se la conservazione dell'IP del client è abilitata. Il valore è `true` o `false`. L'impostazione predefinita è disabilitata se il tipo di gruppo target è l'indirizzo IP e il protocollo del gruppo target è TCP o TLS. In caso contrario, l'impostazione predefinita è abilitata. La conservazione dell'IP client non può essere disabilitata per i gruppi di destinazione UDP e TCP_UDP.

`proxy_protocol_v2.enabled`

Indica se il protocollo proxy versione 2 è abilitato. Per impostazione predefinita, il protocollo proxy è disabilitato.

`stickiness.enabled`

Indica se le sticky session sono abilitate.

`stickiness.type`

Il tipo di persistenza. Il valore possibile è `source_ip`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

Il numero minimo di destinazioni che devono essere integre. Se il numero di destinazioni integre è inferiore a questo valore, contrassegna la zona come non integra nel DNS, in modo che il traffico venga instradato solo in zone integre. I valori possibili sono `off` o un numero intero compreso tra 1 e il numero massimo di destinazioni. Quando il valore è `off`, il fail away DNS è disabilitato, il che significa che ogni gruppo di destinazioni contribuisce al failover DNS in modo indipendente. Il valore di default è 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

La percentuale minima di destinazioni che devono essere integre. Se la percentuale di destinazioni integre è inferiore a questo valore, contrassegna la zona come non integra nel DNS,

in modo che il traffico venga instradato solo in zone integre. I valori possibili sono `off` o un numero intero compreso tra 1 e 100. Il valore `off` indica che il failover DNS è disabilitato, il che significa che ogni gruppo di destinazione contribuisce in modo indipendente al failover DNS. Il valore di default è 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

Il numero minimo di destinazioni che devono essere integre. Se il numero di destinazioni integre è inferiore a questo valore, invia il traffico a tutte le destinazioni, incluse le destinazioni non integre. L'intervallo è compreso tra 1 e il numero massimo di destinazioni. Il valore di default è 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

La percentuale minima di destinazioni che devono essere integre. Se la percentuale di destinazioni integre è inferiore a questo valore, invia il traffico a tutte le destinazioni, incluse le destinazioni non integre. I valori possibili sono `off` o un numero intero compreso tra 1 e 100. Il valore predefinito è `off`.

`target_health_state.unhealthy.connection_termination.enabled`

Indica se il sistema di bilanciamento del carico termina le connessioni verso destinazioni non integre. Il valore è `true` o `false`. Il valore predefinito è `true`.

`target_health_state.unhealthy.draining_interval_seconds`

Il periodo di attesa di Elastic Load Balancing prima di modificare lo stato di un obiettivo non integro da a. `unhealthy.draining` `unhealthy` L'intervallo è compreso tra 0 e 360000 secondi. Il valore predefinito è 0 secondi.

Nota: questo attributo può essere configurato solo quando è. `target_health_state.unhealthy.connection_termination.enabled` `false`

Conservazione dell'IP client

I Network Load Balancer possono preservare l'indirizzo IP di origine dei client durante l'instradamento delle richieste verso destinazioni di back-end. Quando si disabilita la conservazione dell'IP client, l'indirizzo IP privato del Network Load Balancer diventa l'indirizzo IP client per tutto il traffico in entrata.

Per impostazione predefinita, la conservazione dell'IP client è abilitata (e non può essere disabilitata) per le istanze e i gruppi di destinazione di tipo IP con protocolli UDP e TCP_UDP. Tuttavia, puoi

abilitare o disabilitare la conservazione dell'IP client per i gruppi di destinazione TCP e TLS utilizzando l'attributo di gruppo di destinazione `preserve_client_ip.enabled`.

Impostazioni predefinite

- Gruppi di destinazione di tipo Istanza: abilitati
- Gruppi di destinazione di tipo IP (UDP, TCP_UDP): abilitati
- Gruppi di destinazione di tipo IP (TCP, TLS): disabilitati

Requisiti e considerazioni

- Quando la conservazione dell'IP client è abilitata, le destinazioni devono trovarsi nello stesso VPC del Network Load Balancer e il traffico deve fluire direttamente dal Network Load Balancer alla destinazione.
- La conservazione dell'IP client non è supportata quando il traffico tra il Network Load Balancer e la destinazione (istanza o IP) viene instradato attraverso un endpoint del sistema di bilanciamento del carico del gateway, anche se la destinazione si trova nello stesso VPC Amazon del Network Load Balancer.
- I seguenti tipi di istanza non supportano la conservazione dell'IP client: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 e T1. Ti consigliamo di registrare questi tipi di istanza come indirizzi IP, disattivando la conservazione dell'IP client.
- La conservazione dell'IP del client non ha alcun effetto sul traffico in entrata da AWS PrivateLink. L'IP di origine del AWS PrivateLink traffico è sempre l'indirizzo IP privato del Network Load Balancer.
- La conservazione dell'IP client non è supportata quando un gruppo di destinazione contiene ENI AWS PrivateLink o ENI di un altro Network Load Balancer. Ciò causerà la perdita di comunicazione con tali destinazioni.
- La conservazione dell'IP client non ha alcun effetto sul traffico convertito da IPv6 a IPv4. L'IP di origine di questo tipo di traffico è sempre l'indirizzo IP privato del Network Load Balancer.
- Quando si specificano le destinazioni in base al tipo di Application Load Balancer, l'IP client di tutto il traffico in entrata viene preservato dal Network Load Balancer e inviato all'Application Load Balancer. L'Application Load Balancer aggiunge quindi l'IP client all'intestazione della richiesta `X-Forwarded-For` prima di inviarlo alla destinazione.
- Le modifiche apportate alla conservazione dell'IP client vengono applicate solo per le nuove connessioni TCP.

- Il loopback NAT, noto anche come hairpinning, non è supportato quando è abilitata la conservazione dell'IP client. Quando abilitata, potrebbero verificarsi limitazioni delle connessioni TCP/IP legate al riutilizzo dei socket osservati sulle destinazioni. Queste limitazioni di connessione possono verificarsi quando un client, o un dispositivo NAT davanti al client, utilizza lo stesso indirizzo IP di origine e la stessa porta di origine quando si connette a più nodi del sistema di bilanciamento del carico contemporaneamente. Se il sistema di bilanciamento del carico indirizza queste connessioni alla stessa destinazione, le connessioni vengono visualizzate come se provenissero dallo stesso socket di origine, con conseguenti errori di connessione. In tal caso, i client possono tentare nuovamente l'operazione (se la connessione ha esito negativo) o riconnettersi (se la connessione viene interrotta). È possibile ridurre questo tipo di errore di connessione aumentando il numero di porte temporanee di origine o aumentando il numero di destinazioni per il sistema di bilanciamento del carico. È possibile prevenire questo tipo di errore di connessione disabilitando la conservazione dell'IP client o disabilitando il sistema di bilanciamento del carico tra zone.
- Quando la conservazione dell'IP client è disabilitata, il Network Load Balancer supporta 55.000 connessioni simultanee o circa 55.000 connessioni al minuto per ogni destinazione univoca (indirizzo IP e porta). Se si superano queste connessioni, aumenta il rischio di errori di allocazione delle porte, con conseguente impossibilità di stabilire nuove connessioni. Gli errori di allocazione delle porte possono essere tracciati utilizzando il parametro `PortAllocationErrorCount`. Per risolvere gli errori di allocazione delle porte, aggiungi altre destinazioni al gruppo di destinazione. Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Network Load Balancer.

Per configurare la conservazione dell'IP del client 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 aprire la relativa pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Per abilitare la conservazione dell'IP client, attiva Conserva indirizzi IP client. Per disabilitare la conservazione dell'IP client, disattiva Conserva indirizzi IP client.
6. Seleziona Salvataggio delle modifiche.

Per abilitare o disabilitare la conservazione dell'IP del client utilizzando AWS CLI

Utilizza il comando modify-target-group-attributes con l'attributo `preserve_client_ip.enabled`.

Ad esempio, utilizza il seguente comando per disabilitare la conservazione dell'IP client.

```
aws elbv2 modify-target-group-attributes --attributes
 Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

L'output visualizzato dovrebbe essere simile all'esempio seguente.

```
{
    "Attributes": [
      {
        "Key": "proxy_protocol_v2.enabled",
        "Value": "false"
      },
      {
        "Key": "preserve_client_ip.enabled",
        "Value": "false"
      },
      {
        "Key": "deregistration_delay.timeout_seconds",
        "Value": "300"
      }
    ]
}
```

Ritardo di annullamento della registrazione

Quando annulli la registrazione di una destinazione, il sistema di bilanciamento del carico interrompe la creazione di nuove connessioni verso la destinazione. Il sistema di bilanciamento del carico utilizza lo svuotamento della connessione per garantire che il traffico in corso venga completato sulle connessioni esistenti. Se la destinazione di cui è stata annullata la registrazione rimane integra e una connessione esistente non è inattiva, il sistema di bilanciamento del carico può continuare a inviare traffico alla destinazione. Per assicurarti che le connessioni esistenti siano chiuse, puoi eseguire una delle operazioni seguenti: abilitare l'attributo del gruppo di destinazione per la terminazione della connessione, verificare che l'istanza sia non integra prima di annullarne la registrazione oppure puoi chiudere periodicamente le connessioni client.

Lo stato iniziale di un target di cui viene annullata la registrazione è `draining`. Per impostazione predefinita, il sistema di bilanciamento del carico cambia lo stato di un target di cui viene annullata la registrazione in `unused` dopo 300 secondi. Per modificare la quantità di tempo di attesa da parte del sistema di bilanciamento del carico prima di modificare lo stato in `unused`, aggiorna il valore di ritardo

dell'annullamento della registrazione. È consigliabile specificare un valore di almeno 120 secondi per assicurare che le richieste vengano completate.

Se abiliti l'attributo del gruppo di destinazione per la terminazione delle connessioni, le connessioni alle destinazioni di cui è stata annullata la registrazione vengono chiuse poco dopo la fine del relativo timeout.

Per aggiornare gli attributi di annullamento della registrazione 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 aprire la relativa pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Per modificare il timeout di annullamento della registrazione, inserisci un nuovo valore per Ritardo annullamento della registrazione. Per garantire che le connessioni esistenti vengano chiuse dopo aver annullato la registrazione delle destinazioni, seleziona Termina le connessioni in fase di annullamento della registrazione.
6. Seleziona Salvataggio delle modifiche.

Per aggiornare gli attributi di annullamento della registrazione utilizzando AWS CLI

Utilizza il comando modify-target-group-attributes.

Protocollo proxy

I Network Load Balancer utilizzano il protocollo proxy versione 2 per inviare informazioni di connessione aggiuntive, ad esempio relative a origine e destinazione. Il protocollo proxy versione 2 fornisce una codifica binaria dell'intestazione del protocollo proxy stesso. Con gli ascoltatori TCP, il sistema di bilanciamento del carico antepone un'intestazione di protocollo proxy ai dati TCP. Non elimina o sovrascrive i dati esistenti, incluse le intestazioni di protocollo proxy in entrata inviate dal client o qualsiasi altro proxy, i sistemi di bilanciamento del carico o i server nel percorso di rete. Pertanto, è possibile ricevere più di un'intestazione di protocollo proxy. Inoltre, se è presente un altro percorso di rete per le destinazioni al di fuori del Network Load Balancer, la prima intestazione di protocollo proxy può non essere quella del Network Load Balancer.

Quando si specificano le destinazioni in base all'indirizzo IP, gli indirizzi IP di origine forniti alle applicazioni dipendono dal protocollo del gruppo di destinazione nel modo seguente:

- TCP e TLS: gli indirizzi IP di origine sono gli indirizzi IP privati dei nodi del sistema di bilanciamento del carico. Se sono necessari gli indirizzi IP dei client, abilita il protocollo proxy e ottieni gli indirizzi IP dei client dall'intestazione del protocollo proxy.
- UDP e TCP_UDP: gli indirizzi IP di origine sono gli indirizzi IP dei client.

Se i target vengono specificati in base all'ID istanza, gli indirizzi IP di origine forniti alle applicazioni sono gli indirizzi IP dei client. Tuttavia, se preferisci, puoi abilitare il protocollo proxy e ottenere gli indirizzi IP dei client dall'intestazione del protocollo proxy.

> **Note**
>
> Gli ascoltatori TLS non supportano le connessioni in entrata con intestazioni di protocollo proxy inviate dal client o da altri proxy.

Connessioni di controllo dello stato

Dopo avere abilitato il protocollo proxy, l'intestazione del protocollo proxy viene inclusa anche nelle connessioni di controllo dello stato dal sistema di bilanciamento del carico. Tuttavia, con le connessioni di controllo dello stato, le informazioni di connessione client non vengono inviate nell'intestazione del protocollo proxy.

Servizi endpoint VPC

Per il traffico proveniente dai consumer di servizi tramite un servizio endpoint VPC, gli indirizzi IP di origine forniti alle applicazioni sono gli indirizzi IP privati dei nodi del sistema di bilanciamento del carico. Se le applicazioni necessitano degli indirizzi IP dei consumer di servizi, abilita il protocollo proxy e ottieni tali indirizzi dall'intestazione del protocollo proxy.

L'intestazione del protocollo proxy include anche l'ID dell'endpoint. Queste informazioni sono codificate utilizzando un vettore Type-Length-Value (TLV) come indicato di seguito.

Campo	Lunghezza (in ottetti)	Descrizione
Type	1	PP2_TYPE_AWS (0xEA)
Lunghezza	2	Lunghezza del valore

Campo	Lunghezza (in ottetti)	Descrizione
Valore	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	Variabile (valore della lunghezza meno 1)	ID dell'endpoint

Per un esempio che analizza il tipo TLV 0xEA, consulta https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot.

Abilitazione del protocollo proxy

Prima di abilitare il protocollo proxy in un gruppo target, assicurati che le applicazioni prevedano e siano in grado di elaborare l'intestazione del protocollo proxy v2. In caso contrario potrebbe verificarsi un errore. Per ulteriori informazioni, consulta la pagina relativa a protocollo PROXY versioni 1 e 2.

Per abilitare il protocollo proxy v2 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 aprire la relativa pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, seleziona Protocollo proxy v2.
6. Seleziona Salvataggio delle modifiche.

Per abilitare il protocollo proxy v2 utilizzando il AWS CLI

Utilizza il comando modify-target-group-attributes.

Sessioni permanenti

Le sticky session costituiscono un meccanismo per instradare le richieste alla stessa destinazione in un gruppo di destinazioni. Questo meccanismo è utile per i server che conservano le informazioni sullo stato per fornire un'esperienza continua ai client.

Considerazioni

- L'utilizzo di sessioni sticky può portare a una distribuzione non uniforme di connessioni e flussi, che potrebbe influire sulla disponibilità degli obiettivi. Ad esempio, tutti i client dietro lo stesso dispositivo NAT hanno lo stesso indirizzo IP di origine. Di conseguenza, tutto il traffico proveniente da questi client viene instradato alla stessa destinazione.
- Il servizio di bilanciamento del carico potrebbe reimpostare le sessioni sticky per un gruppo di destinazione se lo stato di integrità di una delle sue destinazioni cambia o se si registrano o si annullano la registrazione delle destinazioni con il gruppo di destinazione.
- Quando l'attributo stickiness è attivato per un gruppo target, i controlli passivi dello stato di salute non sono supportati. Per ulteriori informazioni, consulta Health checks for your target group.
- Le sessioni permanenti non sono supportate per gli ascoltatori TLS.

Per abilitare le sticky session 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 aprire la relativa pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Configurazione della selezione della destinazione, attiva Adesione.
6. Seleziona Salvataggio delle modifiche.

Per abilitare le sessioni permanenti utilizzando il AWS CLI

Utilizza il comando modify-target-group-attributes con l'attributo `stickiness.enabled`.

Per creare un gruppo di destinazione per il Network Load Balancer

Le destinazioni per il Network Load Balancer vengono registrate con un gruppo di destinazione. Per impostazione predefinita, il sistema di bilanciamento del carico invia le richieste ai target registrati utilizzando la porta e il protocollo specificati per il gruppo target. È possibile sostituire questa porta al momento della registrazione di ogni target con il gruppo target.

Dopo la creazione di un gruppo target, è possibile aggiungere tag.

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 Regole dei listener. Puoi specificare lo stesso gruppo di destinazione per più ascoltatori solo se questi ultimi appartengono allo stesso Network Load Balancer. Per utilizzare un gruppo di destinazione con un sistema di bilanciamento del carico, devi verificare che il gruppo di destinazione non sia utilizzato dall'ascoltatore di un altro sistema di bilanciamento del carico.

È possibile aggiungere o rimuovere target dal gruppo target in qualsiasi momento. Per ulteriori informazioni, consulta Registrazione di destinazioni con il gruppo target. È anche possibile modificare le impostazioni di controllo dello stato per il gruppo target. Per ulteriori informazioni, consulta Modifica delle impostazioni di controllo dello stato di un gruppo target.

Per creare un gruppo target tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Gruppi di destinazioni nel riquadro di navigazione.
3. Scegliere Crea gruppo target.
4. Nel riquadro Configurazione di base, effettua le operazioni seguenti:

    a. In Scegli un tipo di destinazione, seleziona Istanze per registrare le destinazioni in base all'ID istanza, Indirizzi IP per registrare le destinazioni in base all'indirizzo IP o Application Load Balancer per registrare un Application Load Balancer come destinazione.

    b. In Nome gruppo di destinazione, immetti 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. Per Protocol (Protocollo), scegliere un protocollo come segue:

    - Se il protocollo del listener è TCP, scegliere TCP o TCP_UDP.
    - Se il protocollo del listener è TLS, scegliere TCP o TLS.
    - Se il protocollo del listener è UDP, scegliere UDP o TCP_UDP.
    - Se il protocollo di listener è TCP_UDP, scegliere TCP_UDP.

    d. (Facoltativo) Per Port (Porta) modificare il valore predefinito in base alle esigenze.

    e. Per Tipo di indirizzo IP, scegli IPv4 o IPv6. Questa opzione è disponibile solo se il tipo di destinazione è Istanze o indirizzi IP e se il protocollo è TCP o TLS.

Devi associare un gruppo di destinazione IPv6 a un sistema di bilanciamento del carico dualstack. Tutte le destinazioni del gruppo di destinazione devono avere lo stesso tipo di indirizzo IP. Non è possibile modificare il tipo di indirizzo IP di un gruppo di destinazione dopo averlo creato.

f. Per VPC, seleziona il cloud privato virtuale (VPC) con le destinazioni da registrare.

5. Nel riquadro Controlli dell'integrità, modifica le impostazioni predefinite in base alle esigenze. In Impostazioni avanzate del controllo dell'integrità, scegli la porta per il controllo dell'integrità, il conteggio, il timeout, l'intervallo e specifica i codici di successo. Se durante i controlli dell'integrità il numero di errori consecutivi supera 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) Per aggiungere un tag, espandi Tag, scegli Aggiungi tag e inserisci la chiave e il valore del tag.
7. Seleziona Successivo.
8. Nella pagina Registra destinazioni, aggiungi una o più destinazioni nel modo seguente:
   - Se il tipo di destinazione è Istanze, seleziona le istanze, inserisci le porte, quindi scegli Includi come in sospeso di seguito.

     Nota: le istanze devono avere un indirizzo IPv6 primario assegnato per essere registrate con un gruppo di destinazione IPv6.
   - Se il tipo di destinazione è Indirizzi IP, seleziona la rete, inserisci gli indirizzi IP e le porte, quindi scegli Includi come in sospeso 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 sistema di bilanciamento del carico 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 dello stato può richiedere alcuni minuti.

I sistemi Network Load Balancer utilizzano i controlli dell'integrità attivi e passivi per determinare se una destinazione è disponibile per gestire le richieste. Per impostazione predefinita, ogni nodo del sistema di bilanciamento del carico instrada le richieste ai target integri nella sua zona di disponibilità. Se attivi il bilanciamento del carico su più zone, ogni nodo di bilanciamento del carico instrada le richieste nei target registrati in tutte le zone di disponibilità attivate. Per ulteriori informazioni, consulta Bilanciamento del carico su più zone.

Con i controlli dello stato passivi, il sistema di bilanciamento del carico osserva come i target rispondono alle connessioni. I controlli dello stato passivi abilitano il sistema di bilanciamento del carico per rilevare un target non integro prima che sia segnalato come non integro dai controlli dello stato attivi. Non è possibile disabilitare, configurare o monitorare i controlli dello stato passivi. I controlli di integrità passivi non sono supportati per il traffico UDP e i gruppi target con viscosità attivata. Per ulteriori informazioni, consulta Sticky sessions.

Se una destinazione diventa non integra, il sistema di bilanciamento del carico invia un RST TCP per i pacchetti ricevuti sulle connessioni client associate alla destinazione, a meno che la destinazione non integra non provochi il fail-open da parte del sistema di bilanciamento del carico.

Se nei gruppi di destinazione non è presenta una destinazione integra in una zona di disponibilità abilitata, rimuoviamo l'indirizzo IP per la sottorete corrispondente da DNS, in modo che le richieste non possano essere instradate alla destinazione in quella zona di disponibilità. Se tutte le destinazioni non superano i controlli dell'integrità nello stesso momento in tutte le zone di disponibilità abilitate, il sistema di bilanciamento del carico attiva il fail-open. I Network Load Balancer non si aprono anche quando il gruppo target è vuoto. L'effetto del fail-open è quello di consentire il traffico verso tutte le destinazioni in tutte le zone di disponibilità abilitate, indipendentemente dal loro stato di integrità.

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

Per le richieste di controllo dello stato HTTP o HTTPS, l'intestazione host contiene l'indirizzo IP del nodo del sistema di bilanciamento del carico e la porta del listener anziché l'indirizzo IP della destinazione e la porta di controllo dello stato.

Se aggiungi un ascoltatore TLS al Network Load Balancer, viene eseguito un test di connettività dell'ascoltatore. Poiché la terminazione TLS termina anche una connessione TCP, viene stabilita una nuova connessione TCP tra il sistema di bilanciamento del carico e i target. Pertanto, è possibile

che le connessioni TCP per questo test vengano inviate dal sistema di bilanciamento del carico alle destinazioni registrate con il listener TLS. È possibile identificare queste connessioni TCP perché hanno l'indirizzo IP di origine del Network Load Balancer e le connessioni non contengono pacchetti di dati.

Per un servizio UDP, la disponibilità delle destinazioni può essere testata utilizzando i controlli dell'integrità diversi da UDP sul gruppo di destinazione. Puoi utilizzare qualsiasi controllo dell'integrità disponibile (TCP, HTTP o HTTPS) e qualsiasi porta sulla destinazione per verificare la disponibilità di un servizio UDP. Se il servizio sottoposto al controllo dell'integrità ha esito negativo, la destinazione è considerata non disponibile. Per migliorare la precisione dei controlli dell'integrità per un servizio UDP, configura il servizio in ascolto sulla porta di controllo dell'integrità in modo da monitorare lo stato del servizio UDP e terminare con esito negativo il controllo dell'integrità nel caso in cui il servizio non sia disponibile.

Impostazioni del controllo dello stato

È possibile configurare controlli dello stato attivi per i target in un gruppo target utilizzando le seguenti impostazioni. Se i controlli di integrità superano il UnhealthyThresholdnumero di errori consecutivi, il sistema di bilanciamento del carico mette il bersaglio fuori servizio. Quando i controlli di integrità superano il HealthyThresholdnumero di successi consecutivi, il sistema di bilanciamento del carico riattiva l'obiettivo.

Impostazione	Descrizione	Default
HealthCheckProtocollo	Il protocollo utilizzato dal load balancer durante l'esecuzione dei controlli dello stato sui target. I protocolli possibili sono HTTP, HTTPS e TCP. L'impostazione predefinita è il protocollo TCP. Se il tipo di destinazione è `alb`, i protocolli di controllo dell'integrità supportati sono HTTP e HTTPS.	TCP
HealthCheckPorto	La porta utilizzata dal load balancer durante l'esecuzione dei controlli dello stato sui target. L'impostazione predefinita è quella di utilizzar e la porta sulla quale ciascun target riceve il traffico dal sistema di bilanciamento del carico.	Porta sulla quale ciascuna destinazi one riceve il traffico dal

Impostazione	Descrizione	Default
		sistema di bilanciamento del carico.
HealthCheckSentiero	[Controlli di integrità HTTP/HTTPS] Il percorso dei controlli sanitari che è la destinazione 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 secondi. I valori predefiniti sono 6 secondi per i controlli dell'integrità HTTP e 10 secondi per i controlli dell'integrità TCP e HTTPS.	6 secondi per i controlli dell'integrità HTTP e 10 secondi per i controlli dell'integrità TCP e HTTPS.

Impostazione	Descrizione	Default
HealthCheckIntervalSeconds	Il periodo di tempo approssimativo, in secondi, tra i controlli dell'integrità di una singola destinazione. L'intervallo è compreso tra 5 e 300 secondi. Il valore predefinito è 30 secondi. **Important** I controlli dell'integrità per un Network Load Balancer vengono distribuiti e utilizzano un meccanismo di consenso per determinare lo stato di integrità della destinazione. Pertanto, i target ricevono più del numero configura to di controlli dello stato. Per ridurre l'impatto sui target se si stanno usando i controlli dello stato HTTP, usare una destinazione più semplice sui target, come un file HTML statico, oppure passare ai controlli dello stato TCP.	30 secondi
HealthyThresholdConta	Il numero di controlli dello stato andati a buon fine consecutivi necessari prima di considera re integro un target non integro. L'intervallo è compreso tra 2 e 10. Il predefinito è 5.	5
UnhealthyThresholdConta	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.	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. L'intervallo è compreso tra 200 e 599. Il valore predefinito è compreso tra 200 e 399.	200-399

Stato di integrità della destinazione

Prima che il sistema di bilanciamento del carico invii una richiesta di controllo dello stato a un target, è necessario registrarlo con un gruppo target, specificare il gruppo target in una regola del listener e assicurarsi che la zona di disponibilità del target sia abilitata per il sistema di bilanciamento del carico.

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

Valore	Descrizione
`initial`	È in corso il processo di registrazione del target o di esecuzione dei controlli dello stato iniziali del target da parte del sistema di bilanciamento del carico. Codici di motivo correlati: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	Il target è integro. Codici di motivo correlati: Nessuno
`unhealthy`	L'obiettivo non ha risposto a un controllo dello stato di salute, non ha superato il controllo dello stato o il bersaglio è in stato di arresto. Codice di motivo correlato: `Target.FailedHealthChecks`
`draining`	Il target viene revocato e la connection draining è in corso. Codice di motivo correlato: `Target.DeregistrationInProgress`
`unhealthy.draining`	L'obiettivo non ha risposto ai controlli sanitari o non ha superato i controlli sanitari ed entra in un periodo di tolleranza. La destinazione supporta le connessioni esistenti e non accetterà nuove connessioni durante questo periodo di prova.

Valore	Descrizione
	Codice di motivo correlato: `Target.FailedHealthChecks`
`unavailable`	Lo stato della destinazione non è disponibile. Codice di motivo correlato: `Elb.InternalError`
`unused`	La destinazione non è registrata presso un gruppo target, non viene utilizzato in una regola del listener o la destinazione si trova in una zona di disponibilità non abilitata. Codici di motivo correlati: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`

Codici di motivo di controllo dello stato

Se lo stato di una target 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 in un tooltip. Nota che i codici di motivo che iniziano con `Elb` hanno origine sul lato del sistema di bilanciamento del carico e i codici di motivo che iniziano con `Target` hanno origine sul lato del target.

Codice di motivo	Descrizione
`Elb.InitialHealthChecking`	Controlli dello stato iniziali in corso
`Elb.InternalError`	I controlli dello stato non andati a buon fine a causa di un errore interno
`Elb.RegistrationInProgress`	La registrazione del target è in corso
`Target.DeregistrationInProgress`	La revoca del target è in corso

Codice di motivo	Descrizione
`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 target non è configurato per la ricezione del traffico dal sistema di bilanciamento del carico. Il target si trova in una zona di disponibilità che non è abilitata per il sistema di bilanciamento del carico
`Target.NotRegistered`	Il target non è registrato nel gruppo target

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 aprire la relativa pagina dei dettagli.
4. Il riquadro Dettagli mostra il numero totale di destinazioni, più il numero di destinazioni per ogni stato di integrità.
5. Nella scheda Destinazioni, la colonna Stato di integrità indica lo stato di ogni destinazione.
6. Se lo stato di una destinazione è un valore diverso da `Healthy`, la colonna Dettagli sullo stato di integrità mostra ulteriori informazioni.

Per verificare lo stato dei tuoi obiettivi, utilizza il AWS CLI

Utilizzare 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 delle impostazioni di controllo dello stato di un gruppo target

Puoi modificare le impostazioni di controllo dello stato per il tuo gruppo di target in qualsiasi momento.

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 aprire la relativa pagina dei dettagli.
4. Nella scheda Controlli dello stato, seleziona Modifica.
5. Nella pagina Modifica le impostazioni di controllo dell'integrità, modifica le impostazioni secondo necessità, quindi scegli 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.

Bilanciamento del carico tra zone per gruppi di destinazione

I nodi del sistema di bilanciamento del carico distribuiscono le richieste dei client alle destinazioni registrate. Se il bilanciamento del carico tra zone è abilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico tra le destinazioni registrate in tutte le zone di disponibilità abilitate. Se il bilanciamento del carico tra zone è disabilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella relativa zona di disponibilità. È possibile utilizzare questa opzione se i domini di errore a livello di zona sono preferiti a quelli regionali, per

garantire che una zona integra non sia influenzata da una zona non integra o per migliorare la latenza complessiva.

Con i Network Load Balancer, il bilanciamento del carico tra zone è disattivato per impostazione predefinita a livello del sistema di bilanciamento del carico, ma puoi attivarlo in qualsiasi momento. Per i gruppi di destinazione, l'impostazione predefinita prevede l'utilizzo dell'impostazione del sistema di bilanciamento del carico, ma è possibile modificarla attivando o disattivando esplicitamente il bilanciamento del carico tra zone a livello di gruppo di destinazione.

Considerazioni

- Quando si abilita il bilanciamento del carico tra zone per un Network Load Balancer, vengono applicati i costi di trasferimento dati EC2. Per ulteriori informazioni, consulta Comprendere i costi di trasferimento dei dati nella Guida per l'AWS utente di Data Exports
- L'impostazione del gruppo di destinazione determina il comportamento del bilanciamento del carico per il relativo gruppo. Ad esempio, se il bilanciamento del carico tra zone è abilitato a livello di sistema di bilanciamento del carico e disabilitato a livello di gruppo di destinazione, il traffico inviato al gruppo di destinazione non viene instradato attraverso le zone di disponibilità.
- Quando il bilanciamento del carico tra zone è disattivato, assicurati che ogni zona di disponibilità del sistema di bilanciamento del carico abbia capacità sufficiente, in modo che possa servire il carico di lavoro associato.
- Quando il bilanciamento del carico tra zone è disattivato, assicurati che tutti i gruppi di destinazione partecipino alle stesse zone di disponibilità. Una zona di disponibilità vuota è considerata non integra.

Modifica del bilanciamento del carico tra zone per un sistema di bilanciamento del carico

Puoi abilitare o disabilitare il bilanciamento del carico tra zone del sistema di bilanciamento del carico in qualsiasi momento.

Per modificare il bilanciamento del carico tra zone per un sistema di bilanciamento del carico 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 nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, attiva o disattiva Bilanciamento del carico tra zone.
6. Seleziona Salvataggio delle modifiche.

Per modificare il bilanciamento del carico tra zone per il sistema di bilanciamento del carico, utilizzare il AWS CLI

Utilizza il comando modify-load-balancer-attributes con l'attributo `load_balancing.cross_zone.enabled`.

Modifica del bilanciamento del carico tra zone per un gruppo di destinazione

L'impostazione del bilanciamento del carico tra zone a livello di gruppo di destinazione sostituisce quella a livello di sistema di bilanciamento del carico.

Puoi abilitare o disabilitare il bilanciamento del carico tra zone a livello di gruppo di destinazione se il tipo di gruppo è `instance` o `ip`. Se il tipo di gruppo di destinazione è `alb`, tale gruppo eredita sempre l'impostazione di bilanciamento del carico tra zone dal sistema di bilanciamento del carico.

Per modificare il bilanciamento del carico tra zone per un gruppo 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, seleziona Gruppi di destinazione.
3. Seleziona il nome del gruppo di destinazione per aprire la relativa pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica gli attributi del gruppo di destinazione, seleziona Attivo per Bilanciamento del carico tra zone.
6. Seleziona Salvataggio delle modifiche.

Per modificare il bilanciamento del carico tra zone per un gruppo target utilizzando il AWS CLI

Utilizza il comando modify-target-group-attributes con l'attributo `load_balancing.cross_zone.enabled`.

Integrità del gruppo di destinazione

Per impostazione predefinita, un gruppo di destinazioni è considerato integro purché contenga almeno una destinazione integra. Se disponi di un parco istanze di grandi dimensioni, non è sufficiente avere una sola destinazione integra per la distribuzione del traffico. Al contrario, è possibile specificare un numero o percentuale minimi di destinazioni che devono essere integre e quali operazioni svolge il sistema di bilanciamento del carico quando le destinazioni integre scendono al di sotto della soglia specificata. In questo modo si migliora la disponibilità.

Operazioni per lo stato di non integrità

È possibile configurare soglie di integrità per le seguenti operazioni:

- Failover DNS: quando le destinazioni integre in una zona scendono al di sotto della soglia, gli indirizzi IP del nodo del sistema di bilanciamento del carico di tale zona vengono contrassegnati come non integri nel DNS. Pertanto, quando i client risolvono il nome DNS del sistema di bilanciamento del carico, il traffico viene instradato solo nelle zone integre.
- Failover di instradamento: quando le destinazioni integre in una zona scendono al di sotto della soglia, il sistema di bilanciamento del carico invia traffico a tutte le destinazioni disponibili nel nodo del sistema di bilanciamento del carico, comprese le destinazioni non integre. In questo modo si aumentano le possibilità di successo di una connessione client, soprattutto quando le destinazioni non superano temporaneamente i controlli dell'integrità, e si riduce il rischio di sovraccaricare le destinazioni integre.

Requisiti e considerazioni

- Se per un'operazione vengono specificati entrambi i tipi di soglia (numero e percentuale), il sistema di bilanciamento del carico esegue l'operazione quando viene superata una delle due soglie.
- Se viene specificata una soglia per entrambe le operazioni, la soglia per il failover DNS dev'essere maggiore o uguale alla soglia per il failover di instradamento, in modo che il failover DNS si verifichi insieme o prima rispetto al failover di instradamento.
- Se la soglia viene specificata in percentuale, il valore viene calcolato in modo dinamico, sulla base del numero totale di destinazioni registrato nei gruppi di destinazioni.
- Il numero totale di destinazioni si basa sull'attivazione o meno del bilanciamento del carico tra zone. Se il bilanciamento del carico tra zone è disattivato, ogni nodo invia il traffico solo alle destinazioni nella propria zona, il che significa che le soglie vengono applicate separatamente

al numero di destinazioni in ogni zona abilitata. Se il bilanciamento del carico tra zone è attivato, ogni nodo invia il traffico a tutte le destinazioni in tutte le zone abilitate, il che significa che le soglie specificate vengono applicate al numero totale di destinazioni in tutte le zone abilitate. Per ulteriori informazioni, consulta Bilanciamento del carico tra zone.

- Con il failover DNS, gli indirizzi IP delle zone non integre vengono rimossi dal nome host DNS del sistema di bilanciamento del carico. Tuttavia, la cache DNS del client locale potrebbe contenere questi indirizzi IP fino alla scadenza del time-to-live (TTL) nel record DNS (60 secondi).
- Quando si verifica un failover DNS, ciò influisce su tutti i gruppi di destinazioni associati al sistema di bilanciamento del carico. È necessario assicurarsi di disporre di capacità sufficiente nelle zone rimanenti per gestire il traffico aggiuntivo, soprattutto se il bilanciamento del carico tra zone è disattivato.
- Con il failover DNS, se tutte le zone del sistema di bilanciamento del carico sono considerate non integre, il sistema invia il traffico a tutte le zone, comprese quelle non integre.
- Oltre alla presenza di destinazioni integre sufficienti, vi sono altri fattori che possono portare al failover DNS, come l'integrità della zona.

Esempio

L'esempio seguente illustra come vengono applicate le impostazioni di integrità del gruppo di destinazioni.

Scenario

- Un sistema di bilanciamento del carico che supporta le due zone di disponibilità A e B
- Ogni zona di disponibilità contiene 10 destinazioni registrate
- Il gruppo di destinazioni dispone delle seguenti impostazioni di integrità del gruppo di destinazioni:
  - Failover DNS: 50%
  - Failover di instradamento: 50%
- Nella zona di disponibilità B non superano i controlli

Se il bilanciamento del carico tra zone è disattivato

- Il nodo del sistema di bilanciamento del carico in ogni zona di disponibilità può inviare il traffico solo alle 10 destinazioni presenti nella propria zona.

- Nella zona di disponibilità A sono presenti 10 destinazioni integre, che soddisfano la percentuale richiesta di destinazioni integre. Il sistema di bilanciamento del carico continua a distribuire il traffico nelle 10 destinazioni integre.
- Nella zona di disponibilità B sono presenti solo 4 zone integre, che rappresentano solo il 40% delle destinazioni per il nodo del sistema di bilanciamento del carico presente in tale zona. Dato che questa percentuale è inferiore a quella di destinazioni integre richiesta, il sistema di bilanciamento del carico esegue le seguenti operazioni:
  - Failover DNS: la zona di disponibilità B viene contrassegnata come non integra nel DNS. Dato che i client non possono risolvere il nome del sistema di bilanciamento del carico per ricavare il nodo del sistema nella zona di disponibilità B e la zona di disponibilità A è integra, i client inviano le nuove connessioni alla zona di disponibilità A.
  - Failover di instradamento: quando vengono inviate nuove connessioni esplicitamente alla zona di disponibilità B, il sistema di bilanciamento del carico distribuisce il traffico a tutte le destinazioni nella zona di disponibilità B, comprese quelle non integre. In questo modo si evitano interruzioni nelle destinazioni integre rimanenti.

Se il bilanciamento del carico tra zone è attivato

- Ogni nodo del sistema di bilanciamento del carico può inviare il traffico a tutte le 20 destinazioni registrate in entrambe le zone di disponibilità.
- Sono presenti 10 destinazioni integre nella zona di disponibilità A e 4 nella zona di disponibilità B, per un totale di 14 destinazioni integre. Si tratta del 70% delle destinazioni dei nodi del sistema di bilanciamento del carico in entrambe le zone di disponibilità, una percentuale di destinazioni integre che soddisfa quella richiesta.
- Il sistema di bilanciamento del carico distribuisce il traffico nelle 14 destinazioni integre in entrambe le zone di disponibilità.

Modifica delle impostazioni di integrità del gruppo di destinazioni

È possibile modificare le impostazioni di integrità del gruppo di destinazioni per tale gruppo come indicato di seguito.

Per modificare le impostazioni di integrità del gruppo di destinazioni 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 Attributi, scegli Modifica.
5. Verifica se il bilanciamento del carico tra zone è attivato o disattivato. Aggiorna questa impostazione secondo necessità per garantire di disporre di sufficiente capacità per gestire il traffico aggiuntivo se una zona diventa non integra.
6. Espandi Requisiti di integrità del gruppo di destinazioni.
7. Per Tipo di configurazione, consigliamo di scegliere Configurazione unificata, che imposta la stessa soglia per entrambe le operazioni.
8. Per Requisiti di stato di integrità, procedi in uno dei seguenti modi:
   - Scegli Numero minimo di destinazioni integre, poi inserisci un numero da 1 al numero massimo di destinazioni del gruppo di destinazioni.
   - Scegli Percentuale minima di destinazioni integre, poi inserisci un numero da 1 a 100.
9. Seleziona Salvataggio delle modifiche.

Per modificare le impostazioni relative allo stato di salute del gruppo target utilizzando il AWS CLI

Utilizza il comando modify-target-group-attributes. L'esempio seguente imposta la soglia di integrità al 50% per entrambe le operazioni relative allo stato di integrità.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Terminazione delle connessioni per le destinazioni non integre

La terminazione della connessione è abilitata per impostazione predefinita. Quando la destinazione di un Network Load Balancer non supera i controlli di integrità configurati ed è considerata non integra, il load balancer interrompe le connessioni stabilite e interrompe il routing di nuove connessioni verso la destinazione. Con l'interruzione della connessione disattivata, la destinazione viene comunque considerata non integra e non riceverà nuove connessioni, ma le connessioni stabilite vengono mantenute attive, permettendo loro di chiudersi senza problemi.

L'interruzione della connessione per destinazioni non integre può essere impostata individualmente per ciascun gruppo target.

Per modificare l'impostazione di terminazione delle connessioni 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. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. In Gestione dello stato non integro della destinazione, scegli se l'opzione Termina le connessioni quando le destinazioni diventano non integre è abilitata o disabilitata.
6. Seleziona Salvataggio delle modifiche.

Per modificare l'impostazione della terminazione della connessione utilizzando il AWS CLI

Utilizza il comando modify-target-group-attributes con l'attributo `target_health_state.unhealthy.connection_termination.enabled`.

Intervallo di drenaggio non salutare

> **Important**
>
> La terminazione della connessione deve essere disattivata prima di attivare un intervallo di drenaggio non corretto.

Le destinazioni nello `unhealthy.draining` stato sono considerate non integre, non ricevono nuove connessioni, ma mantengono le connessioni stabilite per l'intervallo configurato. L'intervallo di connessione non integro determina il periodo di tempo in cui la destinazione rimane `unhealthy.draining` nello stato precedente a quello in cui si trova. `unhealthy` Se la destinazione supera i controlli di integrità durante l'intervallo di connessione non integro, il suo stato torna a essere ripristinato. `healthy` Se viene attivata un'annullamento della registrazione, lo stato di destinazione diventa `draining` e inizia il timeout del ritardo di annullamento.

L'intervallo di drenaggio non salutare può essere impostato individualmente per ciascun gruppo target.

Per modificare l'intervallo di drenaggio non salutare 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 Attributi, scegli Modifica.
5. In Target unhealthy state management, assicurati che l'opzione Interrompi connessioni quando le destinazioni diventano inintegre sia disattivata.
6. Inserisci un valore per Intervallo di drenaggio non salutare.
7. Seleziona Salvataggio delle modifiche.

Per modificare l'intervallo di drenaggio non salutare, utilizzare il AWS CLI

Utilizza il comando modify-target-group-attributes con l'attributo `target_health_state.unhealthy.draining_interval_seconds`.

Utilizzo del failover DNS Route 53 per il sistema di bilanciamento del carico

Se utilizzi Route 53 per il routing delle query DNS al bilanciamento del carico, puoi anche configurare il failover DNS per il load balancer utilizzando Route 53. In una configurazione di failover, Route 53 controlla l'integrità delle destinazioni del gruppo di destinazioni registrate per il sistema di bilanciamento del carico per determinare se siano disponibili. Se non sono disponibili destinazioni integre registrate per il sistema di bilanciamento del carico, o se il sistema di bilanciamento del carico stesso non è integro, Route 53 esegue il routing del traffico a un'altra risorsa disponibile, come un sistema di bilanciamento del carico integro o un sito web statico in Amazon S3.

Ad esempio, supponiamo che tu disponga di un'applicazione web per `www.example.com` e che desideri istanze ridondanti in esecuzione dietro due bilanciatori del carico che risiedono in regioni diverse. Desideri che il routing del traffico avvenga principalmente verso il load balancer in una regione e vuoi utilizzare il bilanciamento del carico nell'altra regione come backup durante i guasti. Se configuri un failover di DNS, puoi specificare i bilanciatori del carico principale e secondario (backup). Route 53 indirizza il traffico verso il bilanciamento del carico principale, se è disponibile, in caso contrario, al load balancer secondario.

Utilizzo della valutazione dello stato di destinazione

- Quando la valutazione dello stato di destinazione è impostata su `Yes` su un record alias di un Network Load Balancer, Route 53 valuta l'integrità della risorsa specificata dal valore `alias`

`target`. Per un sistema Network Load Balancer, Route 53 utilizza i controlli dell'integrità del gruppo di destinazione associati al sistema di bilanciamento del carico.

- Quando tutti i gruppi di destinazione in un Network Load Balancer sono integri, Route 53 contrassegna il record alias come integro. Se un gruppo di destinazione contiene almeno una destinazione integra, il controllo dell'integrità ha esito positivo. Route 53 restituisce quindi i record in base alla policy di routing. Se viene utilizzata la policy di routing di failover, Route 53 restituisce il record principale.
- Se uno dei gruppi di destinazione di un Network Load Balancer non è integro, il record alias non supera il controllo dell'integrità di Route 53 (fail-open). Se si utilizza la valutazione dello stato di destinazione, la policy di routing di failover avrà esito negativo.
- Se tutti i gruppi di destinazione in un Network Load Balancer sono vuoti (nessuna destinazione), Route 53 considera il record non integro (fail-open). Se si utilizza la valutazione dello stato di destinazione, la policy di routing di failover avrà esito negativo.

Per ulteriori informazioni, consulta Configurazione di un failover DNS nella Guida per gli sviluppatori di Amazon Route 53.

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. Il tipo di destinazione del gruppo di destinazione determina la modalità di registrazione delle destinazioni. Ad esempio, puoi registrare ID istanza, indirizzi IP o un Application Load Balancer. Il sistema Network Load Balancer inizia a instradare le richieste verso le destinazioni non appena viene completato il processo di registrazione e le destinazioni superano 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 sistema di bilanciamento del carico 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.

Se stai eseguendo la registrazione delle destinazioni in base all'ID istanza, puoi utilizzare il sistema di bilanciamento del carico con un gruppo con dimensionamento automatico. Dopo aver collegato un gruppo di destinazione a un gruppo con dimensionamento automatico e aver impiegato la scalabilità orizzontale, le istanze avviate dal gruppo con dimensionamento automatico vengono registrate automaticamente con il gruppo di destinazione. Se scolleghi il sistema di bilanciamento del carico dal gruppo con dimensionamento automatico, viene automaticamente annullata la registrazione delle istanze dal gruppo di destinazione. Per maggiori informazioni, consulta Come allegare un sistema di bilanciamento del carico al gruppo con dimensionamento automatico nella Guida per l'utente di Dimensionamento automatico Amazon EC2.

Gruppi di sicurezza target

Prima di aggiungere le destinazioni al gruppo di destinazione, configura i gruppi di sicurezza associati in modo che accettino il traffico proveniente dal Network Load Balancer.

Consigli per i gruppi di sicurezza della destinazione se il sistema di bilanciamento del carico è associato a un gruppo di sicurezza

- Per consentire il traffico client: aggiungi una regola che fa riferimento al gruppo di sicurezza associato al sistema di bilanciamento del carico.
- Per consentire il PrivateLink traffico: se hai configurato il sistema di bilanciamento del carico per valutare le regole in entrata per il traffico inviato AWS PrivateLink, aggiungi una regola che accetti il traffico proveniente dal gruppo di sicurezza del bilanciamento del carico sulla porta di traffico. In caso contrario, aggiungi una regola che accetti il traffico proveniente dagli indirizzi IP privati del sistema di bilanciamento del carico sulla porta del traffico.
- Per accettare i controlli dell'integrità del sistema di bilanciamento del carico: aggiungi una regola che accetti il traffico dei controlli dell'integrità proveniente dai gruppi di sicurezza del sistema di bilanciamento del carico sulla porta di controllo dell'integrità.

Consigli per i gruppi di sicurezza della destinazione se il sistema di bilanciamento del carico non è associato a un gruppo di sicurezza

- Per consentire il traffico client: se il sistema di bilanciamento del carico conserva gli indirizzi IP client, aggiungi una regola che accetti il traffico proveniente dagli indirizzi IP dei client approvati sulla porta del traffico. In caso contrario, aggiungi una regola che accetti il traffico proveniente dagli indirizzi IP privati del sistema di bilanciamento del carico sulla porta del traffico.
- Per consentire PrivateLink il traffico: aggiungi una regola che accetti il traffico proveniente dagli indirizzi IP privati del sistema di bilanciamento del carico sulla porta di traffico.
- Per accettare i controlli dell'integrità del sistema di bilanciamento del carico: aggiungi una regola che accetti il traffico dei controlli dell'integrità proveniente dagli indirizzi IP privati del sistema di bilanciamento del carico sulla porta di controllo dell'integrità.

Come funziona la conservazione degli indirizzi IP client

I sistemi Network Load Balancer non conservano gli indirizzi IP client a meno che l'attributo `preserve_client_ip.enabled` non sia impostato su `true`. Inoltre, con i Network Load Balancer dualstack, conserviamo gli indirizzi IP dei client durante la traduzione degli indirizzi IPv4 in IPv6. Tuttavia, quando si traducono gli indirizzi IPv6 in IPv4, l'IP di origine è sempre l'indirizzo IP privato del Network Load Balancer.

Per trovare gli indirizzi IP privati del sistema di bilanciamento del carico, utilizzare la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Network Interfaces (Interfacce di rete).
3. Nel campo di ricerca digita il nome del Network Load Balancer. Esiste una sola interfaccia di rete per ogni sottorete del sistema di bilanciamento del carico.
4. Nella scheda Dettagli per ogni interfaccia di rete, copia l'indirizzo da Indirizzo IPv4 privato.

Per ulteriori informazioni, consulta Gruppi di sicurezza per il Network Load Balancer.

Liste di controllo accessi (ACL) di rete

Quando esegui la registrazione delle istanze EC2 come target, devi assicurarti che le liste di controllo accessi di rete per le subnet delle istanze permettano il traffico sia sulla porta del listener che su quella di controllo dello stato. La lista di controllo accessi (ACL) di rete predefinita per un VPC

permette tutto il traffico in entrata e in uscita. Se crei liste di controllo accessi di rete personalizzate, verifica che consentano il traffico appropriato.

Le liste di controllo accessi di rete associati alle sottoreti delle istanze devono consentire il traffico seguente per un sistema di bilanciamento del carico con connessione Internet.

Regole consigliate per le subnet delle istanze

Inbound

Origine	Protocollo	Port Range (Intervallo porte)	Commento
Indirizzi IP client	*ascoltatore*	*ascoltatore*	Autorizza il traffico del client (tipo di target `instance`)
CIDR VPC	*ascoltatore*	*ascoltatore*	Autorizza il traffico del client (tipo di target `ip`)
CIDR VPC	*controllo dello stato*	*controllo dello stato*	Autorizza il traffico del controllo dello stato dal sistema di bilanciamento del carico

Outbound

Destinazione	Protocollo	Port Range (Intervallo porte)	Commento
Indirizzi IP client	*ascoltatore*	*ascoltatore*	Autorizza le risposte ai client (tipo di target `instance`)
CIDR VPC	*ascoltatore*	*ascoltatore*	Autorizza le risposte ai client (tipo di target `ip`)

CIDR VPC	*controllo dello stato*	1024-65535	Autorizza il traffico del controllo dello stato

Le liste di controllo accessi di rete associati alle sottoreti del sistema di bilanciamento del carico devono consentire il traffico seguente per un sistema di bilanciamento del carico con connessione Internet.

Regole consigliate per le subnet del sistema di bilanciamento del carico

Inbound

Origine	Protocollo	Port Range (Intervallo porte)	Commento
Indirizzi IP client	*ascoltatore*	*ascoltatore*	Autorizza il traffico del client (tipo di target `instance`)
CIDR VPC	*ascoltatore*	*ascoltatore*	Autorizza il traffico del client (tipo di target `ip`)
CIDR VPC	*controllo dello stato*	1024-65535	Autorizza il traffico del controllo dello stato

Outbound

Destinazione	Protocollo	Port Range (Intervallo porte)	Commento
Indirizzi IP client	*ascoltatore*	*ascoltatore*	Autorizza le risposte ai client (tipo di target `instance`)
CIDR VPC	*ascoltatore*	*ascoltatore*	Autorizza le risposte ai client (tipo di target `ip`)

CIDR VPC	*controllo dello stato*	*controllo dello stato*	Autorizza il traffico del controllo dello stato
CIDR VPC	*controllo dello stato*	1024-65535	Autorizza il traffico del controllo dello stato

Per un sistema di bilanciamento del carico interno, le ACL di rete per le sottoreti delle istanze e per i nodi del sistema di bilanciamento del carico devono consentire il traffico in entrata e in uscita da e verso il CIDR VPC, sulla porta dell'ascoltatore e sulle porte temporanee.

Sottoreti condivise

I partecipanti possono creare un Network Load Balancer in un VPC condiviso. I partecipanti non possono registrare una destinazione che viene eseguita in una sottorete non condivisa con loro.

Le sottoreti condivise per Network Load Balancer sono supportate in tutte le regioni, ad eccezione di: AWS

- Asia Pacifico (Osaka) `ap-northeast-3`
- Asia Pacifico (Hong Kong) `ap-east-1`
- Medio Oriente (Bahrain) `me-south-1`
- AWS Cina (Pechino) `cn-north-1`
- AWS Cina (Ningxia) `cn-northwest-1`

Registrazione o annullamento della registrazione di destinazioni

Ogni gruppo target deve avere almeno un target registrato in ciascuna zona di disponibilità abilitata per il sistema di bilanciamento del carico.

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 e considerazioni

- Non è possibile registrare le istanze in base all'ID istanza per i tipi di istanza seguenti: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1.

- Quando si registrano le destinazioni in base all'ID istanza per un gruppo di destinazione IPv6, è necessario assegnare alle destinazioni un indirizzo IPv6 primario. Per ulteriori informazioni, consulta gli indirizzi IPv6 nella Guida per l'utente di Amazon EC2
- Quando si registrano le destinazioni in base all'ID istanza, le istanze devono trovarsi nello stesso Amazon VPC del Network Load Balancer. Non è possibile registrare le istanze in base all'ID istanza se si trovano in un VPC collegato in peering al VPC del sistema di bilanciamento del carico (stessa regione o regione diversa). È possibile registrare queste istanze in base all'indirizzo IP.
- Se si registra una destinazione in base all'indirizzo IP e l'indirizzo IP si trova nello stesso VPC del sistema di bilanciamento del carico, il bilanciamento del carico verifica che provenga da una subnet che può raggiungere.
- Per i gruppi di destinazione UDP e TCP_UDP, non registrare le istanze in base all'indirizzo IP se risiedono all'esterno del VPC del sistema di bilanciamento del carico o se utilizzano uno dei seguenti tipi di istanza: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1. Le destinazioni che risiedono all'esterno del VPC del sistema di bilanciamento del carico o che utilizzano un tipo di istanza non supportato potrebbero ricevere traffico dal sistema di bilanciamento del carico ma non essere in grado di rispondere.

Indice

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, scegli Registra destinazioni. Selezionare una o più istanze, inserisci la porta dell'istanza predefinita secondo necessità e poi scegli Includi come in sospeso di seguito. Dopo aver finito di aggiungere le istanze, scegli Registra destinazioni in sospeso.

Nota:

- le istanze devono aver assegnato un indirizzo IPv6 primario per essere registrate in un gruppo di destinazioni IPv6.
- I AWS GovCloud (US) Region non supportano l'assegnazione di un indirizzo IPv6 primario tramite la console. È necessario utilizzare l'API per assegnare gli indirizzi IPv6 primari in s. AWS GovCloud (US) Region

6. Per annullare la registrazione delle istanze, seleziona l'istanza, quindi scegli Annulla registrazione.

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

Destinazioni IPv4

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)

Il tipo di indirizzo IP non può essere modificato dopo la creazione del gruppo di destinazione.

Quando avvii un Network Load Balancer in un Amazon VPC condiviso come partecipante, puoi registrare le destinazioni solo nelle sottoreti che sono state condivise con te.

Destinazioni IPv6

- Gli indirizzi IP registrati devono trovarsi all'interno del blocco CIDR VPC o all'interno di un blocco CIDR VPC con peering.
- Il tipo di indirizzo IP non può essere modificato dopo la creazione del gruppo di destinazione.
- Puoi associare i gruppi di destinazione IPv6 solo a un sistema di bilanciamento del carico dualstack con ascoltatori TCP o TLS.

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, scegli Registra destinazioni. Per ogni indirizzo IP, seleziona la rete, la zona di disponibilità, l'indirizzo IP (IPv4 o IPv6) e la porta, quindi scegli Includi come in sospeso di seguito. Dopo aver specificato gli indirizzi, scegli Registra le 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.

Application Load Balancer come destinazioni

Puoi creare un gruppo di destinazione con un singolo Application Load Balancer come destinazione e configurare Network Load Balancer per inoltrare il traffico verso di esso. In questo scenario, il sistema Application Load Balancer assume la decisione di bilanciamento del carico non appena il traffico lo raggiunge. Questa configurazione combina le caratteristiche di entrambi i sistemi di bilanciamento del carico e offre i seguenti vantaggi:

- Puoi utilizzare la funzionalità di instradamento basato sulle richieste di livello 7 del sistema Application Load Balancer in combinazione con le funzionalità supportate da Network Load Balancer, come i servizi endpoint (AWS PrivateLink) e gli indirizzi IP statici.
- Puoi utilizzare questa configurazione per applicazioni che richiedono un singolo endpoint per più protocolli, come i servizi multimediali che utilizzano HTTP per la segnalazione e RTP per lo streaming di contenuti.

Puoi utilizzare questa funzionalità con un Application Load Balancer interno o connesso a Internet come destinazione di un Network Load Balancer interno o connesso a Internet.

Considerazioni

- Per associare un Application Load Balancer come destinazione di un Network Load Balancer, deve trovarsi nello stesso Amazon VPC all'interno dello stesso account.
- Puoi associare un Application Load Balancer come destinazione di più Network Load Balancer. A tale scopo, registra il sistema Application Load Balancer con un gruppo di destinazione separato per ogni singolo Network Load Balancer.
- Ogni sistema Application Load Balancer registrato con un Network Load Balancer riduce il numero massimo di destinazioni per zona di disponibilità per Network Load Balancer di 50 (se il bilanciamento del carico tra zone è disabilitato) o 100 (se il bilanciamento del carico tra zone è abilitato). Puoi disabilitare il bilanciamento del carico tra zone in entrambi i sistemi di bilanciamento del carico per ridurre al minimo la latenza ed evitare i costi di trasferimento dei dati regionali. Per ulteriori informazioni, consulta Quote per i Network Load Balancer.
- Se il tipo del gruppo di destinazione è `alb`, non puoi modificare gli attributi del gruppo di destinazione. Questi attributi utilizzano sempre i loro valori predefiniti.
- Dopo aver registrato un Application Load Balancer come destinazione, non è possibile eliminarlo finché non si annulla la registrazione da tutti i gruppi di destinazione.

Fase 1: creazione dell'Application Load Balancer

Prima di iniziare, configura i gruppi di destinazione che verranno utilizzati dal sistema Application Load Balancer. Assicurati di disporre di un cloud privato virtuale (VPC) con le destinazioni da registrare con il gruppo di destinazione. Questo VPC deve disporre come minimo di una sottorete pubblica in ogni zona di disponibilità utilizzata dalle destinazioni.

Per creare un Application Load Balancer 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 Create Load Balancer (Crea sistema di bilanciamento del carico).
4. In Application Load Balancer, scegli Crea.
5. Nella pagina Crea un application load balancer, in Configurazione di base, specifica i valori per Nome del sistema di bilanciamento del carico, Schema e Tipo di indirizzo IP.

6. In Listener, puoi creare un ascoltatore HTTP o HTTPS su qualsiasi porta. Tuttavia, devi assicurarti che il numero di porta di questo ascoltatore corrisponda alla porta del gruppo di destinazione in cui risiederà questo Application Load Balancer.
7. In Zone di disponibilità, procedi come segue:

   a. Per VPC, seleziona un cloud privato virtuale (VPC) con istanze o indirizzi IP che hai incluso come destinazioni dell'Application Load Balancer. Devi utilizzare lo stesso VPC impiegato per il Network Load Balancer in Fase 3: creazione di un Network Load Balancer e configurazione dell'Application Load Balancer come destinazione.

   b. Seleziona due o più Zone di disponibilità e le sottoreti corrispondenti. Assicurati che queste zone di disponibilità corrispondano a quelle abilitate per il Network Load Balancer per ottimizzare la disponibilità, la scalabilità e le prestazioni.
8. Puoi scegliere Assegna un gruppo di sicurezza al sistema di bilanciamento del carico creando un nuovo gruppo di sicurezza o selezionandone uno esistente.

   Il gruppo di sicurezza selezionato deve contenere una regola che consenta il traffico verso la porta dell'ascoltatore per questo sistema di bilanciamento del carico. Utilizza i blocchi CIDR (intervallo di indirizzi IP) dei computer client come origine del traffico nelle regole in entrata per i gruppi di sicurezza. Ciò consente ai client di inviare traffico tramite questo Application Load Balancer. Per ulteriori informazioni sulla configurazione dei gruppi di sicurezza per un Application Load Balancer come destinazione di un Network Load Balancer, consulta Gruppi di sicurezza per l'Application Load Balancer nella Guida per l'utente di Application Load Balancer.
9. In Configura instradamento, seleziona il gruppo di destinazione configurato per questo Application Load Balancer. Se non hai alcun gruppo di destinazione disponibile e desideri configurarne uno nuovo, consulta Creazione di un gruppo di destinazione nella Guida per l'utente di Application Load Balancer.
10. Controlla la configurazione e scegli Crea sistema di bilanciamento del carico.

Per creare l'Application Load Balancer utilizzando AWS CLI

Utilizza il comando create-load-balancer.

Fase 2: creazione del gruppo di destinazione con Application Load Balancer come destinazione

La creazione di un gruppo di destinazione ti consente di registrare un Application Load Balancer nuovo o esistente come destinazione. Puoi aggiungere solo un Application Load Balancer per gruppo

di destinazione. Lo stesso Application Load Balancer può essere utilizzato anche in un gruppo di destinazione separato, come destinazione di un massimo di due Network Load Balancer.

Per creare un gruppo target e registrare l'Application Load Balancer come destinazione, utilizzando la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Load balancing (Bilanciamento del carico) scegli Target Groups (Gruppi di destinazione).
3. Scegliere Crea gruppo target.
4. Nella pagina Specifica i dettagli del gruppo, in Configurazione di base, seleziona Application Load Balancer.
5. Per Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione di Application Load Balancer.
6. In Protocollo, è consentito solo il valore TCP. Seleziona la porta del gruppo di destinazione. Tale porta deve corrispondere alla porta ascoltatore dell'Application Load Balancer. In alternativa, puoi aggiungere o modificare la porta ascoltatore sull'Application Load Balancer in modo che corrispondano.
7. In VPC, seleziona il cloud privato virtuale (VPC) con l'Application Load Balancer per registrarlo con il gruppo di destinazione.
8. In Controlli dell'integrità, scegli HTTP o HTTPS come Protocollo di controllo dell'integrità. I controlli dell'integrità vengono inviati all'Application Load Balancer e inoltrati alle relative destinazioni utilizzando la porta, il protocollo e il percorso ping specificati. Assicurati che il sistema Application Load Balancer possa ricevere i controlli dell'integrità fornendo un ascoltatore con una porta e un protocollo che corrispondano alla porta e al protocollo dei controlli dell'integrità.
9. (Facoltativo) Aggiungi uno o più tag come richiesto.
10. Seleziona Successivo.
11. Nella pagina Registra destinazioni, scegli l'Application Load Balancer che desideri registrare come destinazione. L'Application Load Balancer scelto dall'elenco deve disporre di un ascoltatore sulla stessa porta del gruppo di destinazione che si sta creando. Puoi aggiungere o modificare un ascoltatore in questo sistema di bilanciamento del carico in modo che corrisponda alla porta del gruppo di destinazione o tornare al passaggio precedente e modificare la porta specificata per il gruppo di destinazione. Se non sei sicuro di quale Application Load Balancer

aggiungere come destinazione o non desideri aggiungerlo in questo momento, puoi scegliere di inserirlo in seguito.

12. Scegliere Crea gruppo target.

Per creare un gruppo di destinazione e registrare l'Application Load Balancer come destinazione tramite AWS CLI

Utilizza i comandi create-target-group e register-targets.

Fase 3: creazione di un Network Load Balancer e configurazione dell'Application Load Balancer come destinazione

Utilizza i seguenti passaggi per creare il Network Load Balancer e quindi configurare l'Application Load Balancer come destinazione utilizzando la console.

Per creare Network Load Balancer e listener 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 Create Load Balancer (Crea sistema di bilanciamento del carico).
4. In Network Load Balancer (Sistema di bilanciamento del carico della rete), scegli Crea.
5. Configurazione di base

   Nel riquadro Configurazione di base, configura i parametri Nome del sistema di bilanciamento del carico, Schema e Tipo di indirizzo IP.
6. Mappatura della rete

   a. Per VPC, seleziona lo stesso VPC utilizzato per la destinazione dell'Application Load Balancer. Se hai selezionato Con connessione Internet in Schema, è possibile selezionare solo VPC con un gateway Internet.

   b. In Mappature, seleziona una o più zone di disponibilità e le sottoreti corrispondenti. Ti consigliamo di selezionare le stesse zone di disponibilità della destinazione dell'Application Load Balancer per ottimizzare la disponibilità, la scalabilità e le prestazioni.

      (Facoltativo) Per utilizzare indirizzi IP statici, scegli Utilizza un indirizzo IP elastico nelle Impostazioni IPv4 per ogni zona di disponibilità. Grazie agli indirizzi IP statici puoi

aggiungere determinati indirizzi IP a un elenco di indirizzi consentiti per i firewall o puoi eseguire la codifica fissa degli indirizzi IP con i client.

7. Ascoltatori e instradamento

   a. L'ascoltatore predefinito accetta il traffico TCP sulla porta 80. Solo gli ascoltatori TCP possono inoltrare il traffico a un gruppo di destinazione dell'Application Load Balancer. Devi mantenere il Protocollo come TCP, ma puoi modificare la Porta in base alle esigenze.

      Con questa configurazione, puoi utilizzare gli ascoltatori HTTPS sull'Application Load Balancer per terminare il traffico TLS.

   b. Per Operazione predefinita, seleziona il gruppo di destinazione dell'Application Load Balancer per inoltrare il traffico. Se non viene visualizzato nell'elenco o non è possibile selezionare un gruppo di destinazione (in quanto già utilizzato da un altro Network Load Balancer), puoi creare un gruppo di destinazione dell'Application Load Balancer come mostrato in Fase 2: creazione del gruppo di destinazione con Application Load Balancer come destinazione.

8. Tag

   (Facoltativo) Aggiungi tag per classificare il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Tag.

9. Riepilogo

   Controlla la configurazione e scegli Crea sistema di bilanciamento del carico.

Per creare il Network Load Balancer utilizzando AWS CLI

Utilizza il comando create-load-balancer.

Fase 4: creazione di un servizio endpoint VPC (facoltativo)

Per utilizzare il Network Load Balancer configurato nel passaggio precedente come endpoint per la connettività privata, puoi abilitare AWS PrivateLink. In questo modo viene stabilita una connessione privata al sistema di bilanciamento del carico come servizio endpoint.

Per creare un servizio endpoint VPC utilizzando il Network Load Balancer

1. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
2. Seleziona il nome del Network Load Balancer per aprirne la pagina dei dettagli.

3. Nella scheda Integrazioni, espandi Servizi endpoint VPC (AWS PrivateLink).
4. Scegli Crea servizi endpoint per aprire la pagina Servizi endpoint. Per i passaggi rimanenti, consulta Creazione di un servizio endpoint nella Guida di AWS PrivateLink .

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' 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 per un gruppo target 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 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

Se le operazioni di inoltro di un ascoltatore non fanno riferimento al gruppo di destinazione, è possibile eliminare tale gruppo. 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 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. 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.

Monitoraggio dei Network Load Balancer

Per monitorare i sistemi di bilanciamento del carico, analizzare i modelli di traffico e risolvere i problemi relativi ai sistemi di bilanciamento del carico e ai target, puoi utilizzare le seguenti risorse.

CloudWatch metriche

Puoi utilizzare Amazon CloudWatch per recuperare le statistiche sui punti dati per i tuoi sistemi di bilanciamento del carico 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 Network 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 Network 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 sistema di bilanciamento del carico. Esiste una sola interfaccia di rete per ogni sottorete del sistema di bilanciamento del carico. Per identificare le interfacce di rete di un Network Load Balancer, cerca il nome del sistema di bilanciamento del carico nel campo descrizione dell'interfaccia di rete.

Per ogni connessione tramite Network Load Balancer sono disponibili due voci: una per la connessione front-end tra il client e il sistema di bilanciamento del carico e l'altra per la connessione back-end tra il sistema di bilanciamento del carico e la destinazione. Se l'attributo di conservazione dell'IP client del gruppo di destinazione è abilitato, la connessione viene visualizzata nell'istanza come una connessione proveniente dal client. In caso contrario, l'IP di origine della connessione è l'indirizzo IP privato del sistema di bilanciamento del carico. 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 del sistema di bilanciamento del carico, i log dell'interfaccia di rete del sistema 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.

Se un Network Load Balancer dispone di gruppi di sicurezza associati, i log di flusso presentano voci relative al traffico consentito o rifiutato dai gruppi di sicurezza. Per i Network Load Balancer con ascoltatori TLS, le voci dei log di flusso riflettono solo le voci rifiutate.

Log di accesso

È possibile usare i log di accesso per acquisire informazioni dettagliate sulle richieste TLS inviate al sistema di bilanciamento del carico. I file di log sono archiviati in Amazon S3. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi relativi alle destinazioni. Per ulteriori informazioni, consulta Log di accesso per il Network Load Balancer.

CloudTrail registri

Puoi utilizzarle AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate all'API Elastic Load Balancing e archiviarle come file di registro in Amazon S3. È possibile utilizzare questi CloudTrail registri per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata, quando è stata effettuata la chiamata e così via. Per ulteriori informazioni, consulta Registrazione delle chiamate API per Network Load Balancer tramite AWS CloudTrail.

CloudWatch metriche per il tuo Network Load Balancer

Elastic Load Balancing pubblica punti dati su Amazon CloudWatch per i tuoi sistemi di bilanciamento del carico e i tuoi obiettivi. CloudWatchti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a 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 sistema di bilanciamento del carico 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 nell'intervallo che consideri accettabile.

Elastic Load Balancing riporta le metriche CloudWatch solo quando le richieste fluiscono attraverso il sistema di bilanciamento del carico. Se ci sono delle richieste che passano attraverso il load balancer, Elastic Load Balancing ne misura e invia i parametri a intervalli di 60 secondi. Se per il load balancer non passano richieste o in assenza di dati su un parametro, questo non viene segnalato. Per i Network Load Balancer con gruppi di sicurezza, il traffico rifiutato dai gruppi di sicurezza non viene registrato nelle metriche. CloudWatch

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Parametri di Network Load Balancer

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

Metrica	Descrizione
`ActiveFlowCount`	Il numero totale di flussi simultanei (o connessioni) da client a target. Questo parametro include connessioni negli stati SYN_SENT ed ESTABLISHED. Le connessioni TCP non vengono terminate presso il sistema di bilanciamento del carico, pertanto un client che apre una connessione TCP su un target conta come un flusso singolo. Criteri di segnalazione: sempre segnalati. Statistiche: le statistiche più utili sono `Average`, `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TCP`	Il numero totale di flussi simultanei (o connessioni) TCP da client a target. Questo parametro include connessioni negli stati SYN_SENT ed ESTABLISHED. Le connessioni TCP non vengono terminate presso il sistema di bilanciamento del carico, pertanto un client che apre una connessione TCP su un target conta come un flusso singolo. Criteri di segnalazione: è presente un valore diverso da zero

Metrica	Descrizione
	Statistiche: le statistiche più utili sono `Average`, `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TLS`	Il numero totale di flussi simultanei (o connessioni) TLS da client a target. Questo parametro include connessioni negli stati SYN_SENT ed ESTABLISHED. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: le statistiche più utili sono `Average`, `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_UDP`	Il numero totale di flussi simultanei (o connessioni) UDP da client a target. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: le statistiche più utili sono `Average`, `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrica	Descrizione
`ClientTLSNegotiationErrorCount`	Il numero totale di handshake TLS non riusciti durante la negoziazione tra un client e un listener TLS. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer`
`ConsumedLCUs`	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. Criteri di segnalazione: sempre segnalati. Statistiche: tutte Dimensioni • `LoadBalancer`
`ConsumedLCUs_TCP`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico per TCP. Paghi per il numero di LCU che usi all'ora. Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: tutte Dimensioni • `LoadBalancer`

Metrica	Descrizione
`ConsumedLCUs_TLS`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico per TLS. Paghi per il numero di LCU che usi all'ora. Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: tutte Dimensioni • `LoadBalancer`
`ConsumedLCUs_UDP`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal tuo sistema di bilanciamento del carico per UDP. Paghi per il numero di LCU che usi all'ora. Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: tutte Dimensioni • `LoadBalancer`
`HealthyHostCount`	Il numero di target considerati integri. Questo parametro non include gli Application Load Balancer registrati come destinazioni. Criteri di segnalazione: segnalati se sono abilitati i controlli dell'integrità. Statistiche: le statistiche più utili sono `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Metrica	Descrizione
NewFlowCount	Il numero totale di nuovi flussi (o connessioni) stabiliti da client a target nel periodo di tempo. Criteri di segnalazione: sempre segnalati. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
NewFlowCount_TCP	Il numero totale di nuovi flussi (o connessioni) TCP stabiliti da client a target nel periodo di tempo. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
NewFlowCount_TLS	Il numero totale di nuovi flussi (o connessioni) TLS stabiliti da client a target nel periodo di tempo. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
NewFlowCount_UDP	Il numero totale di nuovi flussi (o connessioni) UDP stabiliti da client a target nel periodo di tempo. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
PeakPacketsPerSecond	Massima velocità media dei pacchetti (elaborati al secondo), calcolata ogni 10 secondi durante la finestra di campionamento. Questo parametro include il traffico relativo ai controlli dell'integrità. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Maximum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
PortAllocationErrorCount	Il numero totale di errori temporanei di allocazione delle porte durante un'operazione di conversione dell'IP client. Un valore diverso da zero indica l'interruzione delle connessioni client. Nota: i Network Load Balancer supportano 55.000 connessioni simultanee o circa 55.000 connessioni al minuto per ogni destinazione univoca (indirizzo IP e porta) durante la conversione dell'indirizzo client. Per risolvere gli errori di allocazione delle porte, aggiungi altre destinazioni al gruppo di destinazione. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes	Il numero totale di byte elaborati dal sistema di bilanciamento del carico, incluse le intestazioni TCP/IP. Questo conteggio include il traffico da e verso le destinazioni, meno il traffico di controllo dello stato. Criteri di segnalazione: sempre segnalati. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
`ProcessedBytes_TCP`	Il numero totale di byte elaborati dai listener TCP. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_TLS`	Il numero totale di byte elaborati dai listener TLS. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_UDP`	Il numero totale di byte elaborati dai listener UDP. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Metrica	Descrizione
ProcessedPackets	Il numero totale di pacchetti elaborati dal sistema di bilanciamento del carico. Questo conteggio include il traffico da e verso le destinazioni, incluso il traffico del controllo dell'integrità. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_ICMP	Il numero di nuovi messaggi ICMP rifiutati dalle regole in entrata dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_TCP	Il numero di nuovi flussi TCP rifiutati dalle regole in entrata dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
SecurityGroupBlockedFlowCount_Inbound_UDP	Il numero di nuovi flussi UDP rifiutati dalle regole in entrata dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_ICMP	Il numero di nuovi messaggi ICMP rifiutati dalle regole in uscita dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	Il numero di nuovi flussi TCP rifiutati dalle regole in uscita dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
SecurityGroupBlockedFlowCount_Outbound_UDP	Il numero di nuovi flussi UDP rifiutati dalle regole in uscita dei gruppi di sicurezza del sistema di bilanciamento del carico. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
TargetTLSNegotiationErrorCount	Il numero totale di handshake TLS non riusciti durante la negoziazione tra un listener TLS e un target. Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer
TCP_Client_Reset_Count	Il numero totale di pacchetti di ripristino (RST) inviati da un client a un target. Questi ripristini sono generati dal client e inoltrati dal sistema di bilanciamento del carico. Criteri di segnalazione: sempre segnalati. Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Metrica	Descrizione
`TCP_ELB_Reset_Count`	Il numero totale di pacchetti di ripristino (RST) generati dal sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Risoluzione dei problemi. Criteri di segnalazione: sempre segnalati. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`TCP_Target_Reset_Count`	Il numero totale di pacchetti di ripristino (RST) inviati da un target a un client. Questi ripristini sono generati dal target e inoltrati dal sistema di bilanciamento del carico. Criteri di segnalazione: sempre segnalati. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Il numero di target considerati non integri. Questo parametro non include gli Application Load Balancer registrati come destinazioni. Criteri di segnalazione: segnalati se sono abilitati i controlli dell'integrità. Statistiche: le statistiche più utili sono `Maximum` e `Minimum`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Metrica	Descrizione
`UnhealthyRoutingFlowCount`	Il numero di flussi (o connessioni) che vengono instradati utilizzando l'azione di failover dell'instradamento (fail open). Criteri di segnalazione: vi è un valore diverso da zero. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensioni di parametro per Network Load Balancer

Per filtrare i parametri relativi al tuo sistema di bilanciamento del carico, 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 load balancer. Specifica il sistema di bilanciamento del carico nel modo seguente: net/loda-balancer-name/1234567890123456 (la parte finale dell'ARN del sistema di bilanciamento del carico).
`TargetGroup`	Consente di filtrare i dati del parametro per gruppo target. Specifica il gruppo target nel modo seguente: targetgroup/target-group-name/1234567890123456 (la parte finale dell'ARN del gruppo target).

Statistiche per i parametri di Network Load Balancer

CloudWatch fornisce statistiche basate sui punti dati metrici pubblicati da Elastic Load Balancing. Le statistiche sono aggregazioni di dati del parametro in un determinato periodo di tempo. Quando richiedi le statistiche, il flusso di dati restituito viene identificato dal nome e dalla dimensione del

parametro. Una dimensione è una coppia nome/valore che identifica un parametro in modo univoco. Ad esempio, puoi richiedere le statistiche su tutte le istanze EC2 di un load balancer avviate in una determinata zona di disponibilità.

Le statistiche `Maximum` e `Minimum` riflettono il valore minimo e massimo dei punti dati restituiti dai singoli nodi del sistema di bilanciamento del carico in ciascuna finestra di campionatura. L'aumento del valore massimo di `HealthyHostCount` corrisponde alla diminuzione del valore minimo di `UnHealthyHostCount`. Ti consigliamo di monitorare il valore massimo di `HealthyHostCount`, richiamando l'allarme quando il valore massimo di `HealthyHostCount` scende al di sotto del minimo richiesto o è pari a `0`. In questo modo puoi verificare le destinazioni che non sono più integre. Ti consigliamo inoltre di monitorare il valore minimo di `UnHealthyHostCount`, richiamando l'allarme quando il valore minimo di `UnHealthyHostCount` supera lo `0`. Ciò ti consente di verificare quando non ci sono più destinazioni registrate.

La statistica `Sum` è il valore aggregato di tutti i nodi del load balancer. Poiché i parametri includono più report per ogni periodo, `Sum` si applica solo ai parametri aggregati in tutti i nodi del sistema di bilanciamento del carico.

La statistica `SampleCount` rappresenta il numero di campioni misurati. Poiché i parametri sono raccolti in base agli intervalli e agli eventi di campionamento, in genere questa statistica non è utile. Ad esempio, con `HealthyHostCount`, `SampleCount` si basa sul numero di campioni segnalato da ogni nodo del load balancer, non sul numero di host integri.

Visualizza le CloudWatch metriche per il tuo sistema di bilanciamento del carico

Puoi visualizzare i CloudWatch parametri per i tuoi sistemi di bilanciamento del carico utilizzando la console Amazon EC2. Tali parametri vengono visualizzati come grafici di monitoraggio. I grafici di monitoraggio mostrano punti di dati se il load balancer è attivo e riceve richieste.

In alternativa, puoi visualizzare i parametri per il tuo sistema di bilanciamento del carico utilizzando la console. CloudWatch

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 sistema di bilanciamento del carico, procedi nel seguente modo:

a. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
b. Scegliere il sistema di bilanciamento del carico 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.

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. Selezionare lo spazio dei nomi NetworkELB (NetworkELB).
4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, digitarne il nome nel campo di ricerca.

Per visualizzare le metriche utilizzando il AWS CLI

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

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

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

Utilizza il seguente comando get-metric-statistics per ottenere statistiche su un parametro e una dimensione specifici. 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/NetworkELB \
```

```
--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": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Log di accesso per il Network Load Balancer

Elastic Load Balancing fornisce log di accesso che raccolgono informazioni dettagliate sulle connessioni TLS stabilite con Network Load Balancer. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi che potresti incontrare.

> **Important**
>
> I log di accesso vengono creati solo quando Network Load Balancer dispone di un listener TLS e contengono informazioni solo sulle connessioni TLS.

La registrazione degli accessi è una funzionalità facoltativa di Elastic Load Balancing che viene disabilitata per impostazione predefinita. Dopo aver abilitato la registrazione degli accessi per il sistema di bilanciamento del carico, Elastic Load Balancing acquisisce i log come file compressi e li

archivia nel bucket Amazon S3 specificato. Puoi disabilitare la registrazione degli accessi in qualsiasi momento.

Puoi abilitare la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) o usare Key Management Service con chiavi gestite dal cliente (SSE-KMS CMK) per il bucket S3. Ogni file di log di accesso viene crittografato automaticamente prima di essere archiviato nel bucket S3 e decrittografato quando vi accedi. Non hai bisogno di intervenire in alcun modo in quanto non vi sono differenze nella modalità in cui accedi ai file di log crittografati e non crittografati. Ogni file di registro è crittografato con una chiave univoca, a sua volta crittografata con una chiave KMS che viene ruotata regolarmente. Per ulteriori informazioni, consulta Specificare la crittografia Amazon S3 (SSE-S3) e Specificare la crittografia lato server con (SSE-KMS) nella Guida per l'utente di Amazon AWS KMS S3.

Non sono previsti costi aggiuntivi per i log di accesso. Vengono addebitati i costi di archiviazione per Amazon S3, ma non per la larghezza di banda utilizzata da Elastic Load Balancing per inviare i file di log ad Amazon S3. Per ulteriori informazioni sui costi di storage, consultare Prezzi di Amazon S3.

File di log di accesso

Elastic Load Balancing pubblica un file di log per ciascun nodo del sistema di bilanciamento del carico ogni 5 minuti. La consegna dei log è caratterizzata da consistenza finale. Il load balancer è in grado di consegnare più log per lo stesso periodo. In genere questo accade se il sito è a traffico elevato.

I nomi dei file di log di accesso utilizzano il formato seguente:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

Nome del bucket S3.

prefisso

Il prefisso (gerarchia logica) nel bucket. Se non specifichi un prefisso, i log vengono collocati a livello di root del bucket.

aws-account-id

L' Account AWS ID del proprietario.

Regione

La regione del load balancer e del bucket S3.

yyyy/mm/dd

La data in cui il log è stato consegnato.

load-balancer-id

L'ID risorsa del sistema di bilanciamento del carico. Se l'ID risorsa contiene barre (/), queste sono sostituite da punti (.).

end-time

La data e l'ora di fine dell'intervallo dei log. Ad esempio, l'ora di fine 20181220T2340Z contiene le voci delle richieste effettuate tra le 23:35 e le 23:40.

random-string

Una stringa casuale generata dal sistema.

Di seguito è riportato un esempio di nome di file di log:

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

È possibile archiviare i file di log nel bucket per un periodo di tempo indeterminato, ma è anche possibile definire regole per il ciclo di vita di Amazon S3 per archiviare o eliminare automaticamente i file di log. Per ulteriori informazioni, consulta Gestione del ciclo di vita dello storage nella Guida per l'utente di Amazon S3.

Voci dei log di accesso

La seguente tabella descrive, in ordine, i campi di una voce di un log di accesso. Tutti i campi sono delimitati da spazi. Quando ne vengono introdotti di nuovi, i campi vengono aggiunti alla fine della voce del log. Quando si elaborano i file di log, consigliamo di ignorare eventuali campi inattesi alla fine della voce di log.

Campo	Descrizione
tipo	Il tipo di listener. Il valore supportato è `tls`.

Campo	Descrizione
version	La versione della voce di log. La versione corrente è 2.0.
time	L'ora registrata alla fine della connessione TLS, nel formato ISO 8601.
elb	L'ID risorsa del sistema di bilanciamento del carico.
ascoltatore	L'ID risorsa del listener TLS per la connessione.
client:port	L'indirizzo IP e la porta del client.
destination:port	L'indirizzo IP e la porta di destinazione. Se il client si connette direttame nte al sistema di bilanciamento del carico, la destinazione è il listener. Se il client si connette utilizzando un servizio endpoint VPC, la destinazione è l'endpoint VPC.
connection_time	Il tempo totale per il completamento della connessione, dall'inizio alla chiusura, in millisecondi.
tls_handshake_time	Il tempo totale per il completamento dell'handshake TLS dopo che la connessione TCP è stata stabilita, inclusi i ritardi lato client, in milliseco ndi. Questo tempo è incluso nel campo connection_time.
received_bytes	Il numero di byte ricevuti dal sistema di bilanciamento del carico dal client, dopo la decrittografia.
sent_bytes	Il numero di byte inviati dal sistema di bilanciamento del carico al client, prima della decrittografia.
incoming_tls_alert	Il valore intero degli avvisi TLS ricevuti dal sistema di bilanciamento del carico dal client, se presenti. In caso contrario, questo valore è impostato su -.
chosen_cert_arn	L'ARN del certificato servito al client. Se non viene inviato un messaggio di saluto client valido, questo valore è impostato su -.
chosen_cert_serial	Riservato per uso futuro. Questo valore è sempre impostato su -.

Campo	Descrizione
tls_cipher	La suite di crittografia negoziata con il client, nel formato OpenSSL. Se la negoziazione TLS non viene completata, questo valore è impostato su -.
tls_protocol_version	Il protocollo TLS negoziato con il client, in formato stringa. I valori possibili sono `tlsv10`, `tlsv11`, `tlsv12` e `tlsv13`. Se la negoziazione TLS non viene completata, questo valore è impostato su -.
tls_named_group	Riservato per uso futuro. Questo valore è sempre impostato su -.
domain_name	Il valore dell'estensione nome_server nel messaggio di saluto client. Questo valore è codificato in formato URL. Se non viene inviato un messaggio di saluto client valido o l'estensione non è presente, questo valore è impostato su -.
alpn_fe_protocol	Il protocollo dell’applicazione negoziato con il client, in formato stringa. I valori possibili sono `h2`, `http/1.1` e `http/1.0`. Se nel listener TLS non è configurata alcuna policy ALPN, non viene trovato alcun protocoll o corrispondente o non viene inviato alcun elenco di protocolli valido, questo valore è impostato su -.
alpn_be_protocol	Il protocollo dell’applicazione negoziato con il client, in formato stringa. I valori possibili sono `h2`, `http/1.1` e `http/1.0`. Se nel listener TLS non è configurata alcuna policy ALPN, non viene trovato alcun protocoll o corrispondente o non viene inviato alcun elenco di protocolli valido, questo valore è impostato su -.
alpn_client_preference_list	Il valore dell'estensione application_layer_protocol_negotiation nel messaggio di benvenuto del client. Questo valore è codificato in formato URL. Ogni protocollo è racchiuso tra virgolette e i protocolli sono separati da una virgola. Se nel listener TLS non è configurata alcuna policy ALPN, non viene inviato alcun messaggio di benvenuto del client valido o l'estensione non è presente, questo valore è impostato su -. La stringa viene troncata se è più lunga di 256 byte.
tls_connection_creation_time	L'ora registrata all'inizio della connessione TLS, nel formato ISO 8601.

Voci di log di esempio

Di seguito sono riportati esempi di voci di log; Il testo appare su più linee solo per semplificarne la lettura.

Di seguito è riportato un esempio per un listener TLS senza una policy ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

Di seguito è riportato un esempio per un listener TLS con una policy ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Requisiti del bucket

Quando abiliti la registrazione degli accessi, devi specificare un bucket S3 per i log di accesso. Il bucket può essere di proprietà di un account differente rispetto all'account proprietario del load balancer. Il bucket deve soddisfare i seguenti requisiti.

Requisiti

- Il bucket deve trovarsi nella stessa regione del load balancer.
- Il prefisso specificato non deve includere `AWSLogs`. Aggiungiamo la parte del nome del file che inizia con `AWSLogs` dopo il nome del bucket e il prefisso specificato.
- Il bucket deve disporre di una relativa policy che conceda l'autorizzazione a scrivere i log di accesso nel bucket. Le policy dei bucket sono una raccolta di istruzioni JSON scritte nella sintassi della policy di accesso per definire le autorizzazioni di accesso per il tuo bucket. Di seguito è riportata una policy di esempio.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["012345678912"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
                }
            }
        }
    ]
}
```

Nella policy precedente, per `aws:SourceAccount`, specifica l'elenco dei numeri di account per i quali i log vengono consegnati a questo bucket. Per `aws:SourceArn`, specifica l'elenco di ARN della risorsa che genera i log, nel formato `arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

Crittografia

Puoi abilitare la crittografia lato server per il bucket di log di accesso Amazon S3 in uno dei seguenti modi:

- Chiavi gestite da Amazon S3 (SSE-S3)
- AWS KMS chiavi memorizzate in AWS Key Management Service (SSE-KMS) †

† Con i log di accesso a Network Load Balancer, non è possibile utilizzare chiavi AWS gestite, ma solo chiavi gestite dal cliente.

Per ulteriori informazioni, consulta Specificare la crittografia Amazon S3 (SSE-S3) e Specificare la crittografia lato server con (SSE-KMS) nella Guida per l'utente di Amazon AWS KMS S3.

La policy della chiave deve consentire al servizio di crittografare e decrittografare i log. Di seguito è riportata una policy di esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Abilitazione della registrazione degli accessi

Quando abiliti la registrazione degli accessi per il sistema di bilanciamento del carico, devi specificare il bucket S3 in cui il sistema archivierà i log. Assicurati di esserne il proprietario e di avere configurato la policy del bucket richiesta. Per ulteriori informazioni, consulta Requisiti del bucket.

Per abilitare la registrazione degli accessi tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Edit load balancer attributes (Modifica gli attributi del sistema di bilanciamento del carico), procedere come segue:
   a. In Monitoraggio, attiva Log di accesso.
   b. Scegli Sfoglia S3 e seleziona il bucket da usare. In alternativa, inserisci il percorso del bucket S3, compreso l'eventuale prefisso.
   c. Seleziona Salvataggio delle modifiche.

Per abilitare la registrazione degli accessi utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Disabilitazione della registrazione degli accessi

Puoi disabilitare la registrazione degli accessi per il tuo sistema di bilanciamento del carico in qualsiasi momento. Dopo avere disabilitato la registrazione degli accessi, i log di accesso rimangono nel tuo bucket S3 finché non li elimini. Per ulteriori informazioni, consulta Utilizzo dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Per disabilitare la registrazione degli accessi tramite la console

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.

5. In Monitoraggio, disabilita Log di accesso.
6. Seleziona Salvataggio delle modifiche.

Per disabilitare la registrazione degli accessi utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Elaborazione dei file di log di accesso

I file di log di accesso sono compressi. Se li apri tramite la console Amazon S3, i file vengono decompressi e le informazioni visualizzate. Se scarichi i file, li devi decomprimere per visualizzare le informazioni.

Se il sito Web ha notevole quantità di domanda, il tuo load balancer può generare i file di log con i gigabyte di dati. Potrebbe non essere possibile elaborare una quantità così grande di dati utilizzando l' line-by-line elaborazione. Pertanto, potresti dover utilizzare gli strumenti di analisi che offrono soluzioni di elaborazione parallela. Ad esempio, puoi utilizzare i seguenti strumenti per analizzare ed elaborare i log di accesso:

- Amazon Athena è un servizio di query interattivo che semplifica l'analisi dei dati in Amazon S3 con SQL standard. Per ulteriori informazioni, consulta Esecuzione di query sui log di Network Load Balancer nella Guida per l'utente di Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Registrazione delle chiamate API per Network 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, un ruolo o un membro di Elastic Servizio AWS 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 Account AWS quando crei l'account. Quando si verifica un'attività in Elastic Load Balancing, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in. Account AWS Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi 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, puoi configurarne altri Servizi AWS 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 Network 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 Servizio AWS.

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 le tue chiamate Account AWS, 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 esempi di record di CloudTrail log per Elastic Load Balancing per un utente che ha creato un Network 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": "2016-04-01T15:31:48Z",
    "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"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "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": "2016-04-01T15:31:48Z",
    "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/net/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"
}
```

Risoluzione dei problemi relativi al Network Load Balancer

Le informazioni seguenti possono essere utili per risolvere i problemi relativi al Network Load Balancer.

Un target registrato non è in servizio

Se un oggetto richiede più tempo del previsto per inserire lo `InService` stato, è possibile che i controlli dello stato non siano stati superati. Il target non è in servizio finché non passa un controllo dello stato. Per ulteriori informazioni, consulta Controlli dello stato per i gruppi target.

Verificare che l'istanza non superi i controlli dello stato e quindi verificare le seguenti:

Un gruppo di sicurezza non consente il traffico

- I gruppi di sicurezza associati a un'istanza devono consentire il traffico dal sistema di bilanciamento del carico utilizzando la porta di controllo dello stato e il protocollo di controllo dello stato. Per ulteriori informazioni, consulta Gruppi di sicurezza target.

Una lista di controllo accessi di rete (ACL) non consente il traffico

- L'ACL di rete associata alle sottoreti delle istanze e alle sottoreti del sistema di bilanciamento del carico deve consentire il traffico e i controlli dell'integrità da parte del sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Liste di controllo accessi (ACL) di rete.

Le richieste vengono instradate ai target.

Verifica quanto segue:

Un gruppo di sicurezza non consente il traffico

- I gruppi di sicurezza associati con le istanze devono consentire il traffico sulla porta listener da indirizzi IP client (se i target sono specificati dall'ID istanza) o sui nodi di bilanciamento del carico (se i target sono specificati dall'indirizzo IP). Per ulteriori informazioni, consulta Gruppi di sicurezza target.

Una lista di controllo accessi di rete (ACL) non consente il traffico

- Le liste di controllo degli accessi di rete associati con le sottoreti per il VPC devono consentire la comunicazione da parte del sistema di bilanciamento del carico e del target in entrambe le

direzioni sulla porta listener. Per ulteriori informazioni, consulta Liste di controllo accessi (ACL) di rete.

I target si trovano in una zona di disponibilità non abilitata

Se si registrano target in una zona di disponibilità, ma non si abilita la zona di disponibilità, questi target registrati non sono in grado di ricevere traffico dal sistema di bilanciamento del carico.

L'istanza si trova in un VPC collegato in peering

Se in un VPC sono presenti istanze collegate in peering al VPC del sistema di bilanciamento del carico, è necessario registrarle con il sistema di bilanciamento del carico in base all'indirizzo IP e non all'ID istanza.

I target ricevono più richieste di controllo dello stato del previsto

I controlli dell'integrità per un Network Load Balancer vengono distribuiti e utilizzano un meccanismo di consenso per determinare lo stato di integrità della destinazione. Pertanto, i target ricevono più del numero di controlli dello stato configurato attraverso l'impostazione `HealthCheckIntervalSeconds`.

I target ricevono meno richieste di controllo dello stato del previsto

Controlla se `net.ipv4.tcp_tw_recycle` è abilitato. Questa impostazione è nota per causare problemi con i sistemi di bilanciamento del carico. L'impostazione `net.ipv4.tcp_tw_reuse` è considerata un'alternativa più sicura.

I target danneggiati ricevono richieste dal sistema di bilanciamento del carico

Ciò si verifica quando tutte le destinazioni registrate non sono integre. Se è presente almeno una destinazione registrata integra, il Network Load Balancer instrada le richieste solo verso tale destinazione.

Quando tutte le destinazioni sono non integre, il Network Load Balancer instrada le richieste verso tutte le destinazioni registrate, con una modalità denominata fail-open. Il Network Load Balancer esegue questa operazione invece di rimuovere tutti gli indirizzi IP dal DNS quando tutte le destinazioni non sono integre e le rispettive zone di disponibilità non dispongono di destinazioni integre a cui inviare le richieste.

Il target non riesce a controllare l'integrità HTTP o HTTPS a causa della mancata corrispondenza dell'intestazione dell’host

L'intestazione dell’host HTTP nella richiesta di controllo dello stato contiene l'indirizzo IP del nodo del sistema di bilanciamento del carico e la porta del listener anziché l'indirizzo IP della destinazione e la porta di controllo dello stato. Se si esegue il mapping delle richieste in ingresso per l’intestazione dell’host, è necessario assicurarsi che i controlli di integrità corrispondano a qualsiasi intestazione dell’host HTTP. Un'altra opzione consiste nell'aggiungere un servizio HTTP separato su una porta diversa e configurare il gruppo di destinazione in modo che utilizzi tale porta per i controlli di integrità. In alternativa, prendere in considerazione l'utilizzo dei controlli di integrità TCP.

Impossibile associare un gruppo di sicurezza a un sistema di bilanciamento del carico

Se il Network Load Balancer è stato creato senza gruppi di sicurezza, non è in grado di supportarli dopo la creazione. Puoi associare un gruppo di sicurezza a un sistema di bilanciamento del carico soltanto durante la creazione. In alternativa, puoi associarlo a un sistema di bilanciamento del carico esistente che è stato originariamente creato con gruppi di sicurezza.

Impossibile rimuovere tutti i gruppi di sicurezza

Se il Network Load Balancer è stato creato con gruppi di sicurezza, deve essere sempre associato almeno un gruppo di sicurezza. Non è possibile rimuovere tutti i gruppi di sicurezza dal sistema di bilanciamento del carico contemporaneamente.

Aumento del parametro TCP_ELB_Reset_Count

Per ogni richiesta TCP eseguita da un client tramite un Network Load Balancer, viene monitorato lo stato della connessione. Se non vengono inviati dati tramite la connessione dal client o dalla destinazione per un periodo superiore al tempo di inattività, la connessione viene chiusa. Se un client o un target invia i dati dopo la scadenza del tempo di inattività, riceve un pacchetto RST TCP che indica che la connessione non è più valida. Inoltre, se una destinazione diventa non integra, il sistema di bilanciamento del carico invia un RST TCP per i pacchetti ricevuti sulle connessioni client associate alla destinazione, a meno che la destinazione non integra non provochi il fail-open da parte del sistema di bilanciamento del carico.

Se noti un picco nel parametro `TCP_ELB_Reset_Count` poco prima o subito dopo l'incremento del parametro `UnhealthyHostCount`, è probabile che i pacchetti RST TCP siano stati inviati perché la destinazione presentava degli errori ma non era stata contrassegnata come non integra. Se noti aumenti persistenti nel parametro `TCP_ELB_Reset_Count` ma le destinazioni vengano contrassegnate ancora come integre, puoi controllare i log di flusso VPC per i client che inviano dati sui flussi scaduti.

Connessioni scadute per le richieste provenienti da un target al sistema di bilanciamento del carico

Verifica se la conservazione dell'IP client è abilitata sul gruppo di destinazione. Il loopback NAT, noto anche come hairpinning, non è supportato quando è abilitata la conservazione dell'IP client. Se un'istanza è un client di un sistema di bilanciamento del carico con cui è registrata e ha la conservazione dell'IP client abilitata, la connessione va a buon fine solo se la richiesta viene instradata a un'istanza diversa. Se la richiesta viene indirizzata alla stessa istanza da cui è stata inviata, la connessione scade perché gli indirizzi IP di origine e di destinazione sono gli stessi.

Se un'istanza deve inviare le richieste a un sistema di bilanciamento del carico registrato, procedere in uno dei seguenti modi:

- Disabilitare la conservazione dell'IP client.
- Verificare che i container che devono comunicare siano su diverse istanze di container.

Diminuzione delle prestazioni durante lo spostamento delle destinazioni verso un Network Load Balancer

Sia i Classic Load Balancer che gli Application Load Balancer utilizzano il multiplexing delle connessioni, al contrario dei Network Load Balancer. Pertanto, le destinazioni possono ricevere più connessioni TCP dietro un Network Load Balancer. Assicurati che i target siano preparati a gestire il volume di richieste di connessione che potrebbero ricevere.

Errori di allocazione delle porte durante la connessione AWS PrivateLink

Se il Network Load Balancer è associato a un servizio endpoint VPC, il sistema supporta 55.000 connessioni simultanee o circa 55.000 connessioni al minuto per ogni destinazione univoca

(indirizzo IP e porta). Se si superano queste connessioni, aumenta il rischio di errori di allocazione delle porte. Gli errori di allocazione delle porte possono essere tracciati utilizzando il parametro `PortAllocationErrorCount`. Per risolvere gli errori di allocazione delle porte, aggiungi altre destinazioni al gruppo di destinazione. Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Network Load Balancer.

Errore di connessione intermittente quando è abilitata la conservazione dell'IP client

Quando la conservazione dell'IP client è abilitata, potrebbero verificarsi limitazioni delle connessioni TCP/IP legate al riutilizzo dei socket osservati sulle destinazioni. Queste limitazioni di connessione possono verificarsi quando un client, o un dispositivo NAT davanti al client, utilizza lo stesso indirizzo IP di origine e la stessa porta di origine quando si connette a più nodi del sistema di bilanciamento del carico contemporaneamente. Se il sistema di bilanciamento del carico indirizza queste connessioni alla stessa destinazione, le connessioni vengono visualizzate come se provenissero dallo stesso socket di origine, con conseguenti errori di connessione. In tal caso, i client possono tentare nuovamente l'operazione (se la connessione ha esito negativo) o riconnettersi (se la connessione viene interrotta). È possibile ridurre questo tipo di errore di connessione aumentando il numero di porte temporanee di origine o aumentando il numero di destinazioni per il sistema di bilanciamento del carico. È possibile prevenire questo tipo di errore di connessione disabilitando la conservazione dell'IP client o disabilitando il sistema di bilanciamento del carico tra zone.

Inoltre, quando la conservazione dell'IP client è abilitata, la connettività potrebbe fallire se i client che si connettono al Network Load Balancer sono collegati anche a destinazioni dietro il sistema di bilanciamento del carico. Per risolvere questo problema, è possibile disabilitare la conservazione dell'IP client sui gruppi di destinazione interessati. In alternativa, i client possono connettersi solo al Network Load Balancer o solo alle destinazioni, ma non a entrambi.

Ritardi nella connessione TCP

Quando sono abilitati sia il bilanciamento del carico tra zone che la conservazione dell'IP client, un client che si connette a IP diversi sullo stesso sistema di bilanciamento del carico può essere indirizzato alla stessa destinazione. Se il client utilizza la stessa porta di origine per entrambe le connessioni, la destinazione riceverà quella che sembra essere una connessione duplicata, il che può causare errori di connessione e ritardi TCP nello stabilire nuove connessioni. È possibile prevenire questo tipo di errore di connessione disabilitando il sistema di bilanciamento del carico tra zone. Per ulteriori informazioni, consulta Bilanciamento del carico su più zone.

Potenziale errore durante il provisioning del sistema di bilanciamento del carico

L'utilizzo di un indirizzo IP già assegnato o allocato altrove (ad esempio, assegnato come indirizzo IP secondario per un'istanza EC2) potrebbe comportare la presenza di errori in un Network Load Balancer in fase di provisioning. Questo indirizzo IP impedisce la configurazione del sistema di bilanciamento del carico, con conseguente visualizzazione dello stato `failed`. Per risolvere questo problema, è possibile rimuovere l'allocazione dell'indirizzo IP associato e tentare nuovamente il processo di creazione.

La risoluzione dei nomi DNS contiene meno indirizzi IP rispetto alle zone di disponibilità abilitate

Idealmente, il Network Load Balancer fornisce un indirizzo IP per ogni zona di disponibilità abilitata quando è presente almeno un host integro. Quando non sono presenti host integri in una determinata zona di disponibilità e il bilanciamento del carico tra zone è disabilitato, l'indirizzo IP del Network Load Balancer corrispondente a quella zona di disponibilità verrà rimosso dal DNS.

Ad esempio, supponiamo che il Network Load Balancer abbia tre zone di disponibilità abilitate, tutte con almeno un'istanza di destinazione registrata integra.

- Se le istanze di destinazione registrate nella zona di disponibilità A non sono integre, l'indirizzo IP corrispondente a tale zona per il Network Load Balancer viene rimosso dal DNS.
- Se in due zone di disponibilità qualsiasi abilitate non sono presenti istanze di destinazione registrate integre, i rispettivi due indirizzi IP del Network Load Balancer verranno rimossi dal DNS.
- Se non sono presenti istanze di destinazione registrate integre in tutte le zone di disponibilità abilitate, verrà attivata la modalità fail-open e il DNS fornirà tutti gli indirizzi IP delle tre zone di disponibilità abilitate nel risultato.

Risolvi i problemi relativi agli obiettivi non integri utilizzando la mappa delle risorse

Se i tuoi obiettivi Network Load Balancer non superano i controlli di integrità, puoi utilizzare la mappa delle risorse per trovare obiettivi non integri e intraprendere azioni in base al codice del motivo dell'errore. Per ulteriori informazioni, consulta Mappa delle risorse di Network Load Balancer.

La mappa delle risorse offre due visualizzazioni: Overview e Unhealthy Target Map. La panoramica è selezionata per impostazione predefinita e mostra tutte le risorse del sistema di bilanciamento del carico. Selezionando la visualizzazione Unhealthy Target Map verranno visualizzati solo gli obiettivi non integri in ogni gruppo target associato al Network Load Balancer.

> **Note**
>
> L'opzione Mostra i dettagli delle risorse deve essere abilitata per visualizzare il riepilogo dei controlli di integrità e i messaggi di errore per tutte le risorse applicabili all'interno della mappa delle risorse. Se non è abilitato, è necessario selezionare ogni risorsa per visualizzarne i dettagli.

La colonna Gruppi target mostra un riepilogo degli obiettivi sani e non sani per ogni gruppo target. Questo può aiutare a determinare se tutti gli obiettivi non superano i controlli sanitari o se solo obiettivi specifici lo sono. Se tutti gli obiettivi di un gruppo target non superano i controlli sanitari, controlla le impostazioni del controllo dello stato del gruppo target. Seleziona il nome di un gruppo target per aprirne la pagina dei dettagli in una nuova scheda.

La colonna Target mostra il targetID e lo stato attuale del controllo dello stato di salute per ciascun bersaglio. Quando un bersaglio non è integro, viene visualizzato il codice del motivo dell'errore del controllo dello stato di salute. Quando un singolo bersaglio non supera un controllo di integrità, verifica che l'obiettivo disponga di risorse sufficienti. Seleziona l'ID di un oggetto per aprirne la pagina di dettaglio in una nuova scheda.

Selezionando Esporta hai la possibilità di esportare la visualizzazione corrente della mappa delle risorse di Network Load Balancer in formato PDF.

Verifica che l'istanza non superi i controlli di integrità e quindi, in base al codice del motivo dell'errore, verifica i seguenti problemi:

- Invalido: la richiesta è scaduta
  - Verifica i gruppi di sicurezza e le liste di controllo degli accessi alla rete (ACL) associati ai tuoi obiettivi e Network Load Balancer non bloccano la connettività.
  - Verificare che la destinazione disponga di una capacità sufficiente per accettare connessioni dal Network Load Balancer.

- Le risposte al controllo dello stato di Network Load Balancer possono essere visualizzate nei log delle applicazioni di ogni destinazione. Per ulteriori informazioni, consulta Codici motivo Health check.

- Malsano: FailedHealthChecks
  - Verifica che il bersaglio stia ascoltando il traffico sulla porta di controllo dello stato di salute.

    > Quando si utilizza un listener TLS
    >
    > Sei tu a scegliere quale politica di sicurezza utilizzare per le connessioni front-end. La politica di sicurezza utilizzata per le connessioni back-end viene selezionata automaticamente in base alla politica di sicurezza front-end in uso.
    >
    > - Se il listener TLS utilizza una politica di sicurezza TLS 1.3 per le connessioni front-end, la politica di sicurezza viene utilizzata per le connessioni back-end. `ELBSecurityPolicy-TLS13-1-0-2021-06`
    > - Se il listener TLS non utilizza una politica di sicurezza TLS 1.3 per le connessioni front-end, la politica di sicurezza viene utilizzata per le connessioni back-end. `ELBSecurityPolicy-2016-08`
    >
    > Per ulteriori informazioni, consulta Politiche di sicurezza.

  - Verifica che il destinatario fornisca un certificato e una chiave del server nel formato corretto specificato dalla politica di sicurezza.
  - Verifica che il target supporti uno o più codici corrispondenti e un protocollo fornito da Network Load Balancer per stabilire handshake TLS.

Quote per i Network Load Balancer

Il tuo Account AWS dispone di quote di default, 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 visualizzare le quote per i Network Load Balancer, apri la console Service Quotas. Nel riquadro di navigazione, scegli Servizi AWS e seleziona Elastic Load Balancing. È inoltre possibile utilizzare il comando describe-account-limits (AWS CLI) per Elastic Load Balancing.

Per richiedere un aumento delle quote, consulta Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizzare il modulo di aumento del limite di Elastic Load Balancing.

Sistema di bilanciamento del carico (load balancer)

Di seguito sono riportate le quote dell'Account AWS in relazione ai Network Load Balancer.

Nome	Default	Adattabile
Certificati per Network Load Balancer	25	Sì
Listener per Network Load Balancer	50	No
ENI di Network Load Balancer per VPC	1.200 [1]	Sì
Network Load Balancer per regione	50	Sì
Gruppi di destinazione per operazione per Network Load Balancer	1	No
Destinazioni per zona di disponibilità per Network Load Balancer	500 [2, 3]	Sì
Destinazioni per Network Load Balancer	3.000 [3]	Sì

[1] Ogni Network Load Balancer utilizza un'interfaccia di rete per zona. La quota viene impostata a livello di VPC. Quando si condividono sottoreti o VPC, l'utilizzo viene calcolato su tutti i tenant.

² Se una destinazione è registrata con N gruppi di destinazione, viene conteggiata come N destinazioni per questo limite. Ogni Application Load Balancer che è una destinazione del Network Load Balancer viene conteggiato come 50 destinazioni se il bilanciamento del carico tra zone è disabilitato o come 100 destinazioni se è abilitato.

³ Se il bilanciamento del carico tra zone è abilitato, il numero massimo è 500 destinazioni per sistema di bilanciamento del carico, indipendentemente dal numero di zone di disponibilità.

Gruppi target

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

Nome	Default	Adattabile
Gruppi di destinazione per regione	3.000 ¹	Sì
Destinazioni per gruppo di destinazione per regione (istanze o indirizzi IP)	1.000	Sì
Destinazioni per gruppo di destinazione per regione (Application Load Balancer)	1	No

¹ Questa quota è condivisa dai sistemi Application Load Balancer e Network Load Balancer.

Cronologia dei documenti per i sistemi Network Load Balancer

La tabella seguente descrive le versioni dei Network Load Balancer.

Modifica	Descrizione	Data
Certificati RSA 3072 bit ed ECDSA 256/384/521 bit	Questa versione aggiunge il supporto per i certificati RSA a 3072 bit e per i certificati Elliptic Curve Digital Signature Algorithm (ECDSA) a 256, 384 e 521 bit tramite (ACM). AWS Certificate Manager	19 gennaio 2024
Terminazione TLS FIPS 140-3	Questa versione aggiunge politiche di sicurezza che utilizzano moduli crittografici FIPS 140-3 per terminare le connessioni TLS.	20 novembre 2023
Affinità DNS zonale	Questa versione aggiunge il supporto per i client che risolvono il DNS del sistema di bilanciamento del carico in modo da ricevere un indirizzo IP nella stessa zona di disponibilità (AZ) in cui si trovano.	12 ottobre 2023
Disabilita la terminazione non corretta della connessione di destinazione	Questa versione aggiunge il supporto per mantenere le connessioni attive verso destinazioni che non superano i controlli di integrità.	12 ottobre 2023

Interruzione predefinita della connessione UDP	Per impostazione predefinita, questa versione aggiunge il supporto per terminare le connessioni UDP al termine del timeout di annullamento della registrazione.	12 ottobre 2023
Registra le destinazioni utilizzando IPv6	Questa versione aggiunge il supporto per registrare le istanze come destinazioni quando indirizzate tramite IPv6.	2 ottobre 2023
Gruppi di sicurezza per il Network Load Balancer	In questa versione è stato aggiunto il supporto per associare i gruppi di sicurezza ai Network Load Balancer al momento della creazione.	10 agosto 2023
Integrità del gruppo di destinazione	Questa versione aggiunge supporto per configurare il numero o la percentuale minimi di destinazioni che devono essere integre e quali operazioni il sistema di bilanciamento del carico quando la soglia non viene rispettata.	17 novembre 2022
Configurazione dei controlli dell'integrità	Questa versione apporta miglioramenti in merito alla configurazione dei controlli dell'integrità.	17 novembre 2022

Bilanciamento del carico su più zone	Questa versione aggiunge il supporto per configurare il bilanciamento del carico tra zone a livello di gruppo target.	17 novembre 2022
Gruppi di destinazioni IPv6	Questa versione aggiunge il supporto per configurare i gruppi di destinazione IPv6 per Network Load Balancer.	23 novembre 2021
Bilanciatori di carico interni IPv6	Questa versione aggiunge il supporto per configura re i gruppi target IPv6 per i Network Load Balancer.	23 novembre 2021
TLS 1.3	In questa versione sono state aggiunte policy di sicurezza che supportano la versione 1.3 di TLS.	14 ottobre 2021
Application Load Balancer come destinazioni	In questa versione è stato aggiunto il supporto per configurare un sistema Application Load Balancer come destinazione di un Network Load Balancer.	27 settembre 2021
Conservazione dell'IP client	In questa versione è stato aggiunto il supporto per configurare la conservazione dell'IP client.	4 febbraio 2021
Policy di sicurezza per FS che supporta la versione 1.2 di TLS	Questa versione aggiunge policy di sicurezza per Forward Secrecy (FS) per il supporto di TLS versione 1.2.	24 novembre 2020

Modalità dual-stack	In questa versione è stato aggiunto il supporto per la modalità dual-stack, che consente ai client di connetter si al sistema di bilanciam ento del carico utilizzando sia indirizzi IPv4 che IPv6.	13 Novembre 2020
Terminazione della connessio ne in fase di annullamento della registrazione	In questa versione è stato aggiunto il supporto per la chiusura delle connessioni alle destinazioni di cui è stata annullata la registrazione alla fine del relativo timeout.	13 Novembre 2020
Policy ALPN	Questa versione aggiunge il supporto per gli elenchi di preferenze ALPN (Application-Layer Protocol Negotiation).	27 maggio 2020
Sessioni permanenti	Questa versione aggiunge il supporto per le sessioni sticky basate su indirizzo IP di origine e protocollo.	28 febbraio 2020
Sottoreti condivise	In questa versione è stato aggiunto il supporto per la specifica delle sottoreti che sono state condivise da un altro Account AWS.	26 novembre 2019

Indirizzi IP privati	Questa versione consente di fornire un indirizzo IP privato dall'intervallo di indirizzi IPv4 della sottorete specificata quando si attiva una zona di disponibilità per un sistema di bilanciamento del carico interno.	25 novembre 2019
Aggiungere sottoreti	Questa versione aggiunge il supporto per l'attivazione di zone di disponibilità aggiuntive dopo la creazione del sistema di bilanciamento del carico.	25 novembre 2019
Politiche di sicurezza per FS	Questa versione aggiunge il supporto per tre ulteriori politiche di sicurezza predefini te relative alla segretezza avanzata.	8 ottobre 2019
Supporto SNI	Questa versione aggiunge il supporto del Server Name Indication (SNI).	12 settembre 2019
Protocollo UDP	Questa versione aggiunge il supporto per il protocollo UDP.	24 giugno 2019
Disponibile in una nuova regione	Questa versione aggiunge il supporto per Network Load Balancer nella regione Asia Pacifico (Osaka).	12 giugno 2019
Protocollo TLS	Questa versione aggiunge il supporto per il protocollo TLS.	24 gennaio 2019

Bilanciamento del carico tra zone	In questa versione è stato aggiunto il supporto per l'abilitazione del bilanciamento del carico tra zone.	22 febbraio 2018
Protocollo proxy	In questa versione è stato aggiunto il supporto per l'abilitazione del protocollo proxy.	17 Novembre 2017
Indirizzi IP come target	In questa versione è stato aggiunto il supporto per la registrazione di indirizzi IP come target.	21 settembre 2017
Nuovo tipo di sistema di bilanciamento del carico	Questa versione di Elastic Load Balancing introduce i sistemi Network Load Balancer.	7 settembre 2017

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.