Application Load Balancer

Sistema di bilanciamento del carico elastico

Sistema di bilanciamento del carico elastico: Application Load Balancer

Table of Contents

Cos'è un Application Load Balancer?

Elastic Load Balancing distribuisce automaticamente il traffico in entrata su più destinazioni, come EC2 istanze, contenitori 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 gli Application Load Balancer. Per ulteriori informazioni sugli altri sistemi di bilanciamento del carico, consulta la Guida per l'utente dei sistemi Network Load Balancer, la Guida per l'utente di Gateway Load Balancer, e la Guida per l'utente dei sistemi Classic Load Balancer.

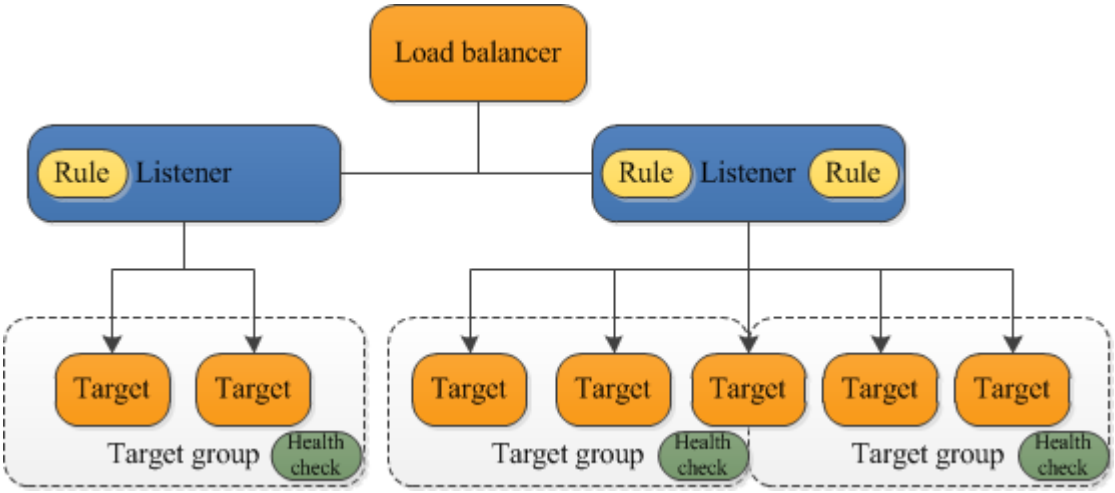
Componenti di Application Load Balancer

Un sistema di bilanciamento del carico funge da singolo punto di contatto per i client. Il load balancer distribuisce il traffico delle applicazioni in entrata su più destinazioni, ad esempio istanze, in più zone di disponibilità. EC2 Ciò aumenta la disponibilità dell'applicazione. Puoi aggiungere uno o più listener al load balancer.

Un listener è un processo che controlla le richieste di connessione dai client utilizzando il protocollo e la porta che hai configurato. Le regole definite per un listener determinano il modo in cui il sistema di bilanciamento del carico instrada le richieste alle destinazioni registrate. Ogni regola consiste in una priorità, una o più operazioni e una o più condizioni. Quando le condizioni di una regola vengono soddisfatte, l'operazione viene eseguita. Occorre definire una regola predefinita per ogni listener e opzionalmente è possibile definire regole aggiuntive.

Ogni gruppo target indirizza le richieste verso una o più destinazioni registrate, ad esempio EC2 le istanze, utilizzando il protocollo e il numero di porta specificati. 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.

Il seguente diagramma mostra le componenti essenziali. Da notare che tutti i listener contengono una regola predefinita, tranne uno, che contiene un'altra regola che instrada le richieste su un altro gruppo di target. Un target è registrato con due gruppi di destinazioni.



Per ulteriori informazioni, consulta la seguente documentazione :

- Sistemi di load balancer
- Listener
- Gruppi di destinazioni

Panoramica di Application Load Balancer

Un Application Load Balancer funziona a livello di applicazione, il settimo livello del modello Open Systems Interconnection (OSI). Una volta che il sistema di bilanciamento del carico ha ricevuto una richiesta, valuta le regole del listener in ordine di priorità per determinare quale di esse applicare, quindi seleziona un target dal gruppo di target per l'operazione della regola. È possibile configurare le regole del listener per instradare le richieste su diversi gruppi di destinazioni in base al contenuto del traffico delle applicazioni. L'instradamento avviene in maniera indipendente per ogni gruppo di destinazioni, anche nel caso in cui una destinazione sia registrata con più gruppi. È possibile configurare l'algoritmo di instradamento utilizzato a livello di gruppo di target. L'algoritmo di instradamento predefinito è round robin; in alternativa, puoi specificare l'algoritmo di instradamento per le richieste meno rilevanti.

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 Classic Load Balancer

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

- Supporto per Condizioni percorso. Puoi configurare le regole per il tuo listener in modo da inoltrare le richieste in base all'URL nella richiesta. Questo ti permette di strutturare la tua applicazione in servizi più piccoli, e di instradare le richieste al servizio giusto in base al contenuto dell'URL.
- Supporto per Condizioni host. Puoi configurare le regole per il tuo listener in modo da inoltrare le richieste in base al campo host nell'intestazione HTTP. Questo ti permette di instradare le richieste su più domini utilizzando un unico sistema di bilanciamento del carico.
- Supporto dell'instradamento basato sui campi nella richiesta, come Condizioni nell'intestazione HTTP e metodi, parametri di query e indirizzi IP di origine.
- Support per l'instradamento delle richieste verso più applicazioni su una singola EC2 istanza. È possibile registrare un'istanza o indirizzo IP con più gruppi di destinazioni, ognuno in una porta diversa.
- Supporto del reindirizzamento delle richieste da un URL all'altro.
- Supporto della restituzione di una risposta HTTP personalizzata.
- 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 della registrazione delle funzioni Lambda come target.
- Supporto della funzionalità del sistema di bilanciamento del carico di autenticare gli utenti delle applicazioni tramite le loro identità aziendali o social prima di instradare le richieste.
- 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 vengono riportate a

livello di gruppo target. Collegare un gruppo di destinazioni a un gruppo con dimensionamento automatico consente di dimensionare ciascun servizio in modo dinamico in base alle esigenze.

- I log di accesso contengono informazioni aggiuntive e vengono archiviati in formato compresso.
- Prestazioni del sistema di bilanciamento del carico migliorate.

Per ulteriori informazioni sulle funzionalità supportate da ciascun tipo di load balancer, consulta le funzionalità di Elastic Load Balancing.

Servizi correlati

Elastic Load Balancing funziona con i seguenti servizi per migliorare la disponibilità e la scalabilità delle applicazioni.

- Amazon EC2: server virtuali che eseguono le tue applicazioni nel cloud. Puoi configurare il tuo sistema di bilanciamento del carico per indirizzare il traffico verso le tue EC2 istanze.
- Amazon EC2 Auto Scaling: garantisce l'esecuzione del numero desiderato di istanze, anche in caso di guasto di un'istanza, e consente di aumentare o diminuire automaticamente il numero di istanze al variare della domanda delle istanze. Abilitando il dimensionamento automatico con Elastic Load Balancing, le istanze da esso avviate vengono registrate automaticamente nel gruppo di destinazioni, mentre e la registrazione delle istanze da esso terminate viene automaticamente annullata dal gruppo di destinazioni.
- AWS Certificate Manager: durante la creazione di un ascoltatore HTTPS, è possibile specificare i certificati forniti da ACM. Il sistema di bilanciamento del carico utilizza i certificati per terminare le connessioni e decriptare le richieste dei client. Per ulteriori informazioni, consulta Certificati SSL per il tuo Application Load Balancer.
- Amazon CloudWatch: ti consente di monitorare il tuo sistema di bilanciamento del carico e di intervenire secondo necessità. Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Application Load Balancer.
- Amazon ECS: consente di eseguire, arrestare e gestire contenitori Docker su un cluster di EC2 istanze. È possibile configurare il sistema di bilanciamento del carico per instradare il traffico sui propri contenitori. Per ulteriori informazioni, consulta Service load balancing nella Guida per gli sviluppatori di Amazon Elastic Container Service.
- AWS Global Accelerator: migliora la disponibilità e le prestazioni dell'applicazione. Utilizza un acceleratore per distribuire il traffico su più sistemi di bilanciamento del carico in una o più regioni. AWS Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Global Accelerator.

- Route 53: offre un modo affidabile ed economico per indirizzare i visitatori ai siti Web traducendo i nomi di dominio (ad esempio`www.example.com`) negli indirizzi IP numerici (ad esempio`192.0.2.1`) utilizzati dai computer per connettersi tra loro. AWS URLs assegna alle tue risorse, come i sistemi di bilanciamento del carico. Tuttavia, è possibile impostare un URL semplice da ricordare. Ad esempio, è possibile mappare il nome di dominio a un sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Routing del traffico a un load balancer ELB nella Guida per gli sviluppatori di Amazon Route 53.
- AWS WAF— Puoi utilizzarlo AWS WAF con il tuo Application Load Balancer per consentire o bloccare le richieste in base alle regole di una lista di controllo degli accessi Web (Web ACL). Per ulteriori informazioni, consulta AWS WAF.

Per visualizzare informazioni sui servizi integrati con il sistema di bilanciamento del carico, seleziona il sistema di bilanciamento del carico nella scheda AWS Management Console Servizi integrati.

Prezzi

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

Nozioni di base di Application Load Balancer

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

Indice

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

Prima di iniziare

- Decidi quali due zone di disponibilità utilizzare per le tue 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. Puoi invece avviare le tue EC2 istanze in altre sottoreti di queste zone di disponibilità.
- Avvia almeno un' EC2 istanza in ogni zona di disponibilità. Assicurati di installare un server Web, come Apache o Internet Information Services (IIS), su ogni EC2 istanza. Assicurarsi che i gruppi di sicurezza per queste istanze consentano l'accesso HTTP sulla porta 80.

Fase 1: configurazione del gruppo di destinazioni

Creare un gruppo target, che viene utilizzato nell'instradamento delle richieste. La regola predefinita per il listener instrada le richieste sui target registrati in questo gruppo di 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 EC2 console Amazon 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. In Configurazione di base, mantenere il Tipo di destinazione come istanza.
5. Per Nome gruppo di destinazioni inserire un nome per il nuovo gruppo di destinazioni.
6. Mantenere il protocollo (HTTP) e la porta (80) predefiniti.
7. Selezionare il VPC che contiene le istanze. Mantieni invariata la versione del protocollo HTTP1.
8. In Controlli dell'integrità, mantenere le impostazioni predefinite.
9. Scegli Next (Successivo).
10. Nella pagina Registra destinazioni, completare la seguente procedura. Questo è un passaggio facoltativo per la creazione di un sistema di bilanciamento del carico. Tuttavia, è necessario registrare questa destinazione se si desidera testare il sistema di bilanciamento del carico e assicurarsi che instradi il traffico verso questa destinazione.
    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, verrà creato un Application Load Balancer.

Per creare un Application Load Balancer utilizzando la console

1. Apri la EC2 console Amazon 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 che hai usato per le tue EC2 istanze.
3. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
4. Seleziona Crea sistema di bilanciamento del carico.
5. In Application Load Balancer, scegli Crea.

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

Per creare un Application Load Balancer, per prima cosa è necessario fornire informazioni di base della configurazione del sistema di bilanciamento del carico, come nome, schema e tipo di indirizzo IP. In seguito, è necessario fornire 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.

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-alb`.
2. Per Schema e Tipo di indirizzo IP, mantenere i valori predefiniti.
3. Per la mappatura della rete, seleziona il VPC che hai usato per EC2 le tue istanze. Selezionare almeno due zone di disponibilità e una sottorete per zona. Per ogni zona di disponibilità utilizzata per avviare EC2 le istanze, seleziona la zona di disponibilità, quindi seleziona una sottorete pubblica per quella zona di disponibilità.
4. Come Gruppi di sicurezza, selezioniamo il gruppo di sicurezza predefinito per il VPC selezionato nel passaggio precedente. È possibile scegliere un gruppo di sicurezza diverso. Il gruppo di sicurezza per deve consentire al sistema di bilanciamento del carico di comunicare con le destinazioni registrate sia sulla porta dell'ascoltatore che sulla porta del controllo dell'integrità. Per ulteriori informazioni, consulta Regole del gruppo di sicurezza.
5. Per Ascoltatore e instradamento, mantieni il protocollo e la porta predefiniti e seleziona il gruppo di destinazioni dall'elenco. In questo modo viene configurato un ascoltatore che accetta il traffico HTTP sulla porta 80 e inoltra il traffico al gruppo di destinazioni predefinito per impostazione predefinita. Per questo tutorial, non viene creato un listener HTTPS.
6. Per Operazione predefinita, seleziona il gruppo di destinazioni creato e registrato nella Fase 1: configurazione del gruppo di destinazioni.
7. (Facoltativo) Aggiungere un tag per categorizzare 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.

8. 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, verifica che stia inviando traffico alle tue istanze. 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. Selezionare il nuovo sistema di bilanciamento del carico.
7. Scegli Descrizione e 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.
8. (Facoltativo) Per definire ulteriori regole per i listener, consultare Aggiungere una regola.

Fase 5 (facoltativa): eliminare il sistema di bilanciamento del carico

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 EC2 istanze continuano a funzionare dopo l'eliminazione del load balancer creato in questa guida.

Per eliminare il sistema di bilanciamento del carico utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Selezionare la casella del sistema di bilanciamento del carico, quindi selezionare Operazioni e poi Elimina.
4. Quando viene richiesta la conferma, seleziona Sì, elimina.

Guida introduttiva agli Application Load Balancer utilizzando AWS CLI

Questo tutorial fornisce un'introduzione pratica agli Application Load Balancer tramite. AWS CLI

Indice

Prima di iniziare

- Utilizza il comando seguente per verificare di star eseguendo una versione della AWS CLI che supporta gli Application Load Balancer.

  ```
  aws elbv2 help
  ```

  Se ricevi un messaggio di errore che indica che elbv2 non è una scelta valida, aggiorna AWS CLI. Per ulteriori informazioni, vedere Installazione della versione più recente di AWS CLI nella Guida per l'utente.AWS Command Line Interface
- Avvia le tue EC2 istanze in un cloud privato virtuale (VPC). Accertati che i gruppi di sicurezza per queste istanze consentono l'accesso sulla porta del listener e sulla porta del controllo dello stato. Per ulteriori informazioni, consulta Gruppi di sicurezza target.
- Decidi se creare un sistema di bilanciamento del carico IPv4 o dualstack. Utilizzalo IPv4 se desideri che i client comunichino con il sistema di bilanciamento del carico utilizzando solo gli indirizzi. IPv4 Usa dualstack se desideri che i client comunichino con il sistema di bilanciamento del carico utilizzando gli indirizzi e. IPv4 IPv6 Puoi anche usare dualstack per comunicare con destinazioni di backend, come applicazioni o sottoreti dualstack, utilizzando. IPv6 IPv6
- Assicurati di installare un server web, come Apache o Internet Information Services (IIS), su ogni istanza. EC2 Assicurarsi che i gruppi di sicurezza per queste istanze consentano l'accesso HTTP sulla porta 80.

Creazione del sistema di bilanciamento del carico

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

Per creare un sistema di bilanciamento del carico

1. Utilizzate il create-load-balancercomando per creare un sistema di bilanciamento del carico. Occorre specificare due sottoreti che non si trovano nella stessa zona di disponibilità.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE
   ```

   Utilizzate il create-load-balancercomando per creare un **dualstack** bilanciamento del carico.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE --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/app/my-load-
   balancer/1234567890123456
   ```

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

   È possibile creare IPv4 e IPv6 indirizzare gruppi da associare ai sistemi di bilanciamento del carico dualstack. Il tipo di indirizzo IP del gruppo di destinazioni determina la versione IP che il sistema di bilanciamento del carico utilizzerà per comunicare con le destinazioni backend e controllarne l'integrità.

   ```
   aws elbv2 create-target-group --name my-targets --protocol HTTP --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-0abcdef1234567890 Id=i-1234567890abcdef0
```

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 HTTP --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/app/my-load-
balancer/1234567890123456/1234567890123456
```

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

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

Aggiunta di un ascoltatore HTTPS

Se disponi di un sistema di bilanciamento del carico con un listener HTTP, puoi aggiungere un listener HTTPS come descritto di seguito.

Per aggiungere un listener HTTPS al load balancer

1. Creare un certificato SSL per l'uso con il proprio sistema di bilanciamento del carico utilizzando uno dei seguenti metodi:

   - Crea o importa il certificato utilizzando AWS Certificate Manager (ACM). Per ulteriori informazioni, consulta Richiedere un certificato pubblico o Importare certificati nella Guida per l'AWS Certificate Manager utente.
   - Carica il certificato utilizzando AWS Identity and Access Management (IAM). Per ulteriori informazioni , consulta l'argomento relativo all'utilizzo dei certificati server nella Guida per l'utente IAM.

2. Utilizzare il comando create-listener per creare il listener con una regola predefinita che inoltra le richieste verso il gruppo target. È necessario specificare un certificato SSL al momento della creazione di un listener HTTPS. Si noti che è possibile specificare una policy SSL diversa da quella predefinita utilizzando l'opzione `--ssl-policy`.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol HTTPS --port 443  \
--certificates CertificateArn=certificate-arn \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Aggiunta dell'instradamento basato su percorso

Se disponi di un listener con una regola predefinita che inoltra le richieste a un gruppo di destinazione, puoi aggiungere una regola che inoltri le richieste a un altro gruppo di destinazione in base all'URL. Ad esempio, puoi instradare le richieste generali verso un gruppo di destinazione e le richieste di visualizzazione delle immagini verso un altro gruppo di destinazione.

Per aggiungere una regola a un listener con un modello di percorso

1. Usa il create-target-groupcomando per creare un gruppo target:

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

2. 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-0abcdef1234567890 Id=i-1234567890abcdef0
```

3. Utilizzare il comando create-rule per aggiungere una regola al listener che inoltri le richieste verso il gruppo di destinazione se l'URL contiene il modello specificato:

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values='/img/*' \
--actions Type=forward,TargetGroupArn=targetgroup-arn
```

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
```

Application Load Balancer

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 il sistema di bilanciamento del carico le invia a destinazioni, come EC2 le istanze. Per configurare un sistema di bilanciamento del carico, devi creare gruppi target e poi registrare i target nei gruppi. Puoi anche creare dei listener per verificare le richieste di connessione dai client e le regole dei listener per instradare le richieste dai client verso i target in uno o più gruppi target.

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

Indice

- Visualizza la mappa delle risorse di Application Load Balancer
- Prenotazioni di capacità per il tuo Application Load Balancer

Sottoreti per il sistema di bilanciamento del carico

Quando si crea un Application Load Balancer, è necessario abilitare le zone che contengono le destinazioni. Per abilitare una zona, specificare una sottorete che si trova al suo interno. Elastic Load Balancing crea un nodo del sistema di bilanciamento del carico in ogni zona specificata.

Considerazioni

- Il sistema di bilanciamento del carico è più efficace se ogni zona abilitata dispone di almeno una destinazione registrata.
- Se si registrano destinazioni in una zona, ma non si abilita tale zona, queste destinazioni registrate non sono in grado di ricevere traffico dal sistema di bilanciamento del carico.
- Se si abilitano più zone per il sistema di bilanciamento del carico, tali zone devono essere dello stesso tipo. Ad esempio, non è possibile abilitare sia una zona di disponibilità che una zona locale.
- È possibile specificare una sottorete condivisa con te.

Gli Application Load Balancer supportano i seguenti tipi di sottorete.

Tipi di sottorete

- Sottoreti della zone di disponibilità
- Sottoreti della zona locale
- Sottoreti Outpost

Sottoreti della zone di disponibilità

È necessario selezionare almeno due sottoreti delle zone di disponibilità. Le restrizioni si applicano come segue:

- Ogni sottorete deve essere in una zona di disponibilità diversa.
- Per garantire il corretto dimensionamento del sistema di bilanciamento del carico, verificare che ciascuna sottorete della zona di disponibilità del sistema disponga di un blocco CIDR con almeno una bitmask `/27` (ad esempio `10.0.0.0/27`) e almeno otto indirizzi IP liberi per sottorete. Gli otto

indirizzi IP sono necessari per consentire al sistema di bilanciamento del carico di dimensionare se necessario. Il sistema di bilanciamento del carico utilizza questi indirizzi IP per stabilire le connessioni con le destinazioni. Senza di essi, potrebbero verificarsi problemi coni tentativi di sostituzione del nodo dell'Application Load Balancer, comportando l'ingresso in uno stato non riuscito.

Nota: se una sottorete di un Application Load Balancer esaurisce gli indirizzi IP utilizzabili mentre cerca di dimensionarsi, l'Application Load Balancer sarà eseguito con capacità insufficiente. Durante questo periodo di tempo, i vecchi nodi continueranno a servire il traffico, ma il tentativo di dimensionamento bloccato potrebbe provocare errori 5xx o timeout dei tentativi di stabilire una connessione.

Sottoreti della zona locale

Si possono specificare una o più sottoreti della zona locale. Le seguenti funzioni non sono supportate:

- Funzioni Lambda come destinazioni
- Autenticazione TLS reciproca
- Sessioni permanenti
- AWS WAF integrazione

Sottoreti Outpost

È possibile specificare una sola sottorete Outpost. Le restrizioni si applicano come segue:

- Devi aver installato e configurato un Outpost nel data center locale. É necessaria una connessione di rete affidabile tra l'Outpost e la relativa Regione AWS . Per ulteriori informazioni, consulta la AWS Outposts Guida per l'utente di .
- Il sistema di bilanciamento del carico richiede due istanze `large` nell'Outpost per i nodi del sistema. I tipi di istanza supportati sono illustrati nella tabella seguente. Il sistema di bilanciamento del carico si dimensiona secondo necessità, ridimensionando i nodi una dimensione alla volta (da `large` a `xlarge`, poi da `xlarge` a `2xlarge` e infine da `2xlarge` a `4xlarge`). Dopo aver dimensionato i nodi alla dimensione di istanza più grande, il sistema di bilanciamento del carico aggiunge istanze `4xlarge` come nodi del sistema in caso di bisogno di capacità aggiuntiva. Se non si dispone di capacità di istanza o di indirizzi IP disponibili sufficienti per dimensionare il

sistema di bilanciamento del carico, il sistema stesso segnala un evento a AWS Health Dashboard e lo stato del sistema di bilanciamento del carico è `active_impaired`.

- È possibile registrare le destinazioni in base a ID istanza o indirizzo IP. Se si registrano obiettivi nella AWS regione per l'avamposto, questi non vengono utilizzati.
- Le seguenti funzioni non sono supportate:
  - AWS Global Accelerator integrazione
  - Funzioni Lambda come destinazioni
  - Autenticazione TLS reciproca
  - Sessioni permanenti
  - Autenticazione dell'utente
  - AWS WAF integrazione

Un Application Load Balancer può essere distribuito su istanze c5/c5d, m5/m5d o r5/r5d su Outpost. La tabella seguente illustra la dimensione e il volume EBS per tipo di istanza che il sistema di bilanciamento del carico può utilizzare in Outpost:

Tipo e dimensione dell'istanza	Volume EBS (GB)
c5/c5d	
large	50
xlarge	50
2xlarge	50
4xlarge	100
m5/m5d	
large	50
xlarge	50
2xlarge	100
4xlarge	100

Tipo e dimensione dell'istanza	Volume EBS (GB)
r5/r5d	
large	50
xlarge	100
2xlarge	100
4xlarge	100

Gruppi di sicurezza del sistema di bilanciamento del carico

Un gruppo di sicurezza agisce come un firewall che controlla il traffico consentito da e verso il sistema di bilanciamento del carico. Puoi scegliere le porte e i protocolli in modo da permettere il traffico sia in entrata sia in uscita.

Le regole dei gruppi di sicurezza associati al sistema di bilanciamento del carico devono permettere il traffico bidirezionale sia attraverso la porta dell'ascoltatore sia attraverso la porta di controllo dell'integrità. Quando aggiungi un listener a un sistema di bilanciamento del carico o aggiorni la porta di controllo dello stato per un gruppo target, devi rivedere le regole del gruppo di sicurezza in modo da permettere il traffico bidirezionale attraverso la nuova porta. Per ulteriori informazioni, consulta Regole consigliate.

Stato del sistema di bilanciamento del carico

Un sistema di bilanciamento del carico può avere 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.

`active_impaired`

Il sistema di bilanciamento del carico indirizza il traffico ma non dispone delle risorse necessarie per dimensionarsi.

`failed`

Il sistema di bilanciamento del carico non può essere configurato.

Attributi del sistema di bilanciamento del carico

È possibile configurare l'Application Load Balancer modificandone gli attributi. Per ulteriori informazioni, consulta Modifica gli attributi del load balancer.

Di seguito sono elencati gli attributi di sistema di bilanciamento del carico:

`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 Abilitare log di accesso.

`access_logs.s3.prefix`

Il prefisso della posizione nel bucket Amazon S3.

`client_keep_alive.seconds`

Il valore del client keepalive, in secondi. L'impostazione predefinita è 3600 secondi.

`deletion_protection.enabled`

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

`idle_timeout.timeout_seconds`

Il valore del tempo di inattività (in secondi). Il valore predefinito è 60 secondi.

`ipv6.deny_all_igw_traffic`

Blocca l'accesso del gateway Internet (IGW) al sistema di bilanciamento del carico, impedendo accessi non intenzionali 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, Transit Gateway o). AWS Direct Connect AWS VPN

`routing.http.desync_mitigation_mode`

Determina il modo in cui il sistema di bilanciamento del carico gestisce le richieste che potrebbero rappresentare un rischio per la sicurezza dell'applicazione. I valori possibili sono `monitor`, `defensive` e `strictest`. Il valore predefinito è `defensive`.

`routing.http.drop_invalid_header_fields.enabled`

Indica se le intestazioni HTTP con campi di intestazione non validi vengono rimosse dal sistema di bilanciamento del carico (`true`) o instradate alle destinazioni (`false`). Il valore predefinito è `false`. Elastic Load Balancing richiede che i nomi di intestazione HTTP validi siano conformi all'espressione regolare `[-A-Za-z0-9]+`, come descritto nel Registro dei nomi dei campi HTTP. Ogni nome è costituito da caratteri alfanumerici o trattini. Selezionare `true` se si desidera che le intestazioni HTTP non conformi a questo modello vengano rimosse dalle richieste.

`routing.http.preserve_host_header.enabled`

Indica se Application Load Balancer deve mantenere l'intestazione `Host` nella richiesta HTTP e inviarla alle destinazioni senza alcuna modifica. I valori possibili sono `true` e `false`. Il valore di default è `false`.

`routing.http.x_amzn_tls_version_and_cipher_suite.enabled`

Indica se le due intestazioni (`x-amzn-tls-version` e `x-amzn-tls-cipher-suite`), che contengono informazioni sulla versione TLS negoziata e sulla suite di cifratura, vengono aggiunte alla richiesta del client prima di inviarla alla destinazione. L'intestazione `x-amzn-tls-version` contiene informazioni sulla versione del protocollo TLS negoziata con il client e l'intestazione `x-amzn-tls-cipher-suite` contiene informazioni sulla suite di cifratura negoziata con il client. Entrambe le intestazioni sono in formato OpenSSL. I valori possibili per l'attributo sono `true` e `false`. Il valore predefinito è `false`.

`routing.http.xff_client_port.enabled`

Indica se l'intestazione `X-Forwarded-For` deve mantenere la porta di origine utilizzata dal client per connettersi al sistema di bilanciamento del carico. I valori possibili sono `true` e `false`. Il valore di default è `false`.

`routing.http.xff_header_processing.mode`

Consente di modificare, mantenere o rimuovere l'intestazione `X-Forwarded-For` nella richiesta HTTP prima che Application Load Balancer la invii alla destinazione. I valori possibili sono `append`, `preserve` e `remove`. Il valore predefinito è `append`.

- Se il valore è `append`, Application Load Balancer aggiunge l'indirizzo IP del client (dell'ultimo hop) all'intestazione `X-Forwarded-For` nella richiesta HTTP prima di inviarle alle destinazioni.
- Se il valore è `preserve`, Application Load Balancer mantiene l'intestazione `X-Forwarded-For` nella richiesta HTTP e la invia alle destinazioni senza alcuna modifica.
- Se il valore è `remove`, Application Load Balancer rimuove l'intestazione `X-Forwarded-For` nella richiesta HTTP prima di inviarla alle destinazioni.

`routing.http2.enabled`

Indica se la registrazione HTTP/2 è abilitata. Il valore predefinito è `true`.

`waf.fail_open.enabled`

Indica se consentire a un sistema di bilanciamento del carico AWS WAF abilitato a indirizzare le richieste verso destinazioni se non è in grado di inoltrare la richiesta a. AWS WAF I valori possibili sono `true` e `false`. Il valore di default è `false`.

> **Note**
>
> L'attributo `routing.http.drop_invalid_header_fields.enabled` è stato introdotto per offrire protezione dalla desincronizzazione HTTP. L'attributo `routing.http.desync_mitigation_mode` è stato aggiunto per fornire una protezione più completa dalla desincronizzazione HTTP per le applicazioni. Non è necessario utilizzare entrambi gli attributi ed è possibile scegliere uno dei due, a seconda dei requisiti dell'applicazione.

Tipo di indirizzo IP

È possibile impostare i tipi di indirizzi IP che i client possono utilizzare per accedere ai sistemi di bilanciamento del carico connessi a Internet e interni.

Gli Application Load Balancer supportano i seguenti tipi di indirizzi IP:

`ipv4`

I client devono connettersi al load balancer utilizzando IPv4 indirizzi (ad esempio, 192.0.2.1).

`dualstack`

I client possono connettersi al sistema di bilanciamento del carico utilizzando sia IPv4 gli indirizzi (ad esempio, 192.0.2.1) che gli indirizzi (ad esempio, 2001:0 db 8:85 a IPv6 3:0:0:8 a2e: 0370:7334).

`dualstack-without-public-ipv4`

I client devono connettersi al sistema di bilanciamento del carico utilizzando gli indirizzi (ad esempio, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334). IPv6

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 gli indirizzi risolvono il record DNS A. IPv4 I client che comunicano con il sistema di bilanciamento del carico utilizzando IPv6 gli indirizzi 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 l'accesso a Internet non IGW (ad esempio tramite peering, Transit Gateway o). AWS Direct Connect AWS VPN
- L'autenticazione Application Load Balancer è supportata solo IPv4 durante la connessione a un Identity Provider (IdP) o a un endpoint Amazon Cognito. Senza un IPv4 indirizzo pubblico, il load balancer non può completare il processo di autenticazione, con conseguenti errori HTTP 500.

Per ulteriori informazioni, consulta Aggiorna i tipi di indirizzi IP per il tuo Application Load Balancer.

Pool di indirizzi IP IPAM

Un pool di indirizzi IP IPAM è una raccolta di intervalli di indirizzi IP contigui (o CIDRs), all'interno di Amazon VPC IP Address Manager (IPAM). L'utilizzo dei pool di indirizzi IP IPAM con Application Load Balancer consente di organizzare IPv4 gli indirizzi in base alle esigenze di routing e sicurezza. I pool di indirizzi IP IPAM devono essere creati all'interno di IPAM prima di poter essere utilizzati dall'Application Load Balancer. Per ulteriori informazioni, consulta Bring your IP address to IPAM.

Considerazioni

- I pool di indirizzi IP IPAM non sono compatibili con i sistemi di bilanciamento del carico interni o con il Dualstack senza un tipo di indirizzo IP pubblico. IPv4
- Non è possibile eliminare un indirizzo IP in un pool di indirizzi IP IPAM se è attualmente utilizzato da un sistema di bilanciamento del carico.
- Durante la transizione verso un pool di indirizzi IP IPAM diverso, le connessioni esistenti vengono terminate in base alla durata keepalive del client HTTP del sistema di bilanciamento del carico.
- I pool di indirizzi IP IPAM possono essere condivisi tra più account. Per ulteriori informazioni, consulta Configurare le opzioni di integrazione per il tuo IPAM

I pool di indirizzi IP IPAM consentono di inserire alcuni o tutti gli intervalli di IPv4 indirizzi pubblici AWS e di utilizzarli con gli Application Load Balancer. Con un migliore controllo dell'assegnazione degli indirizzi IP, è possibile gestire e applicare in modo più efficace le policy e i controlli di sicurezza, beneficiando al contempo di costi inferiori. Non sono previsti costi aggiuntivi associati all'utilizzo dei pool di indirizzi IP IPAM con gli Application Load Balancer, tuttavia, potrebbero esserci costi associati all'IPAM a seconda del livello utilizzato. Per ulteriori informazioni, consulta i prezzi di Amazon VPC

Al pool di indirizzi IP IPAM viene sempre data priorità all'avvio di EC2 istanze e Application Load Balancer e quando gli indirizzi IP non sono più in uso, tornano immediatamente disponibili. Se non ci sono più indirizzi IP assegnabili nel pool di indirizzi IP IPAM, vengono assegnati gli indirizzi IP gestiti. AWS AWS gli indirizzi IP gestiti comportano costi aggiuntivi. Per aggiungere altri indirizzi IP, è possibile aggiungere nuovi intervalli di indirizzi IP a un pool di indirizzi IP IPAM esistente.

Connessioni di bilanciamento del carico

Durante l'elaborazione di una richiesta, il load balancer mantiene due connessioni: una connessione con il client e una connessione con una destinazione. La connessione tra il load balancer e il client viene anche definita connessione front-end. La connessione tra il load balancer e la destinazione viene anche definita connessione back-end.

Bilanciamento del carico su più zone

Con gli Application Load Balancer, il bilanciamento del carico tra zone è attivato per impostazione predefinita e non può essere modificato a livello di sistema di bilanciamento del carico. Per ulteriori informazioni, consulta la sezione Bilanciamento del carico tra zone nella Guida per l'utente di Elastic Load Balancing.

La disattivazione del bilanciamento del carico tra zone è possibile a livello di gruppo di destinazioni. Per ulteriori informazioni, consulta the section called “Disattivazione del bilanciamento del carico tra zone”.

Nome DNS

Ogni Application Load Balancer riceve un nome DNS (Domain Name System) predefinito con la seguente sintassi: - .elb. *name id region*.amazonaws.com. Ad esempio, -1234567890abcdef. elb.us-east-2.amazonaws.com my-load-balancer.

Se preferisci utilizzare un nome DNS più facile da ricordare, puoi creare un nome di dominio personalizzato e associarlo al nome DNS del tuo Application Load Balancer. Quando un client effettua una richiesta utilizzando questo nome di dominio personalizzato, il server DNS la risolve nel nome DNS dell'Application Load Balancer.

In primo luogo, registra un nome di dominio con un registrar di nomi di dominio accreditato. Successivamente, utilizza il tuo servizio DNS, ad esempio il registrar di domini, per creare un record DNS per indirizzare le richieste all'Application Load Balancer. Per ulteriori informazioni, consulta la documentazione per il servizio DNS. Ad esempio, se utilizzi Amazon Route 53 come servizio DNS, crei un record di alias che punta al tuo Application Load Balancer. Per ulteriori informazioni, consulta Routing del traffico a un load balancer ELB nella Guida per gli sviluppatori di Amazon Route 53.

L'Application Load Balancer dispone di un indirizzo IP per ogni zona di disponibilità abilitata. Questi sono gli indirizzi IP dei nodi Application Load Balancer. Il nome DNS dell'Application Load Balancer si risolve in questi indirizzi. Ad esempio, supponiamo che il nome di dominio personalizzato per l'Application Load `example.applicationloadbalancer.com` Balancer sia. Utilizzare il nslookup comando dig o il comando seguente per determinare gli indirizzi IP dei nodi Application Load Balancer.

Linux o Mac

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

Windows

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

L'Application Load Balancer dispone di record DNS per i suoi nodi. È possibile utilizzare nomi DNS con la seguente sintassi per determinare gli indirizzi IP dei nodi Application Load Balancer:. *az name*- .elb. *id 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
```

Creazione di un Application Load Balancer

Un sistema di bilanciamento del carico accetta richieste dai client e le distribuisce ai target di un gruppo target.

Prima di iniziare, accertarsi di avere un cloud privato virtuale (VPC, Virtual Private Cloud) con almeno una sottorete pubblica in ciascuna delle zone utilizzate dalle destinazioni. Per ulteriori informazioni, consulta the section called “Sottoreti per il sistema di bilanciamento del carico”.

Per creare un sistema di bilanciamento del carico utilizzando il, consulta. AWS CLIGuida introduttiva agli Application Load Balancer utilizzando 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 target consente di registrare destinazioni come EC2 le istanze. 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 destinazioni per gli Application Load Balancer.

Per configurare il gruppo target utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Gruppi di destinazioni nel riquadro di navigazione.
3. Scegliere Crea gruppo target.
4. Nella sezione Configurazione di base, impostare i seguenti parametri:

   a. Per Scegli tipo di destinazione, seleziona Istanze per specificare le destinazioni in base all'ID istanza oppure Indirizzi IP per specificarli in base all'indirizzo IP. Se il tipo di destinazione è una funzione Lambda, è possibile abilitare i controlli dell'integrità selezionando Abilità nella sezione Controlli dell'integrità.

   b. Per Nome gruppo di destinazioni immettere un nome per il gruppo di destinazioni.

   c. Modificare i valori Porta e Protocollo secondo necessità.

   d. Se il tipo di destinazione è Istanze o indirizzi IP, scegli IPv4o IPv6come tipo di indirizzo IP, altrimenti vai al passaggio successivo.

      Tieni presente che in questo gruppo di destinazioni possono essere incluse solo le destinazioni che hanno il tipo di indirizzo IP selezionato. Il tipo di indirizzo IP non può essere modificato dopo la creazione del gruppo di destinazioni.

   e. Per VPC, seleziona un cloud privato virtuale (VPC) con le destinazioni che si desiderano includere nel gruppo di destinazioni.

   f. Per la versione del protocollo, selezionare HTTP1quando il protocollo di richiesta è HTTP/1.1 o HTTP/2; selezionare HTTP2, quando il protocollo di richiesta è HTTP/2 o gRPC; e selezionare gRPC, quando il protocollo di richiesta è gRPC.

5. Nella sezione Controlli dell'integrità, mantenere le impostazioni predefinite. In Impostazioni avanzate del controllo dell'integrità, seleziona la porta, il conteggio, il timeout, l'intervallo del controllo dell'integrità e specificarne 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 di salute per i gruppi target di Application Load Balancer.
6. (Facoltativo) Aggiungere uno o più tag come illustrato di seguito:

a. Espandere la sezione Tag.
b. Selezionare Aggiungi tag.
c. Inserire il tag Chiave e il tag Valore. 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. Scegli Next (Successivo).

Fase 2: registrazione delle destinazioni

È possibile registrare EC2 istanze, indirizzi IP o funzioni Lambda come destinazioni in un gruppo di destinazione. Nella creazione di un sistema di bilanciamento del carico, questa è una fase facoltativa. Tuttavia, è necessario registrare gli obiettivi per garantire che il sistema di bilanciamento del carico vi indirizzi il traffico.

1. Nella pagina Registra destinazioni, aggiungere una o più destinazioni come segue:
   - Se il tipo di destinazione è Istanze, seleziona una o più istanze, inserisci una o più porte e in seguito scegli Includi come in sospeso di seguito.
   - Se il tipo di destinazione è Indirizzi IP, procedere nel seguente modo:
     a. Seleziona un rete VPC dall'elenco oppure scegli Altri indirizzi IP privati.
     b. Inserisci manualmente l'indirizzo IP oppure trova l'indirizzo utilizzando i dettagli dell'istanza. È possibile inserire fino a cinque indirizzi IP alla volta.
     c. Inserire le porte per l'instradamento del traffico verso l'indirizzo IP specificato.
     d. Seleziona Includi come in sospeso di seguito.
   - Se il tipo di destinazione è Lambda, seleziona una funzione Lambda o inserire l'ARN di una funzione Lambda e poi scegliere Includi come in sospeso di seguito.
2. Scegliere Crea gruppo target.

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

Per creare un Application Load Balancer, per prima cosa è necessario fornire informazioni di base della configurazione del sistema di bilanciamento del carico, come nome, schema e tipo di indirizzo IP. In seguito, è necessario fornire 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 EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona Create Load Balancer (Crea load balancer).
4. In Application Load Balancer, scegli Crea.
5. Configurazione di base
   a. In Nome del sistema di bilanciamento del carico immetti un nome univoco per il sistema di bilanciamento del carico. Ad esempio, **`my-alb`**. Il nome dell'Application Load Balancer deve essere univoco all'interno del set di Application Load Balancer e Network Load Balancer per la regione. I nomi possono avere un massimo di 32 caratteri e contenere solo caratteri alfanumerici e trattini. Non possono iniziare o terminare con un trattino o con `internal-`. Una volta creato l'Application Load Balancer, non è possibile modificarne il nome.
   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 il tipo di indirizzo IP IPv4, scegli Dualstack o Dualstack senza pubblico. IPv4 Scegli IPv4se i tuoi clienti utilizzano IPv4 gli indirizzi per comunicare con il sistema di bilanciamento del carico. Scegli Dualstack se i tuoi clienti utilizzano entrambi IPv6 gli indirizzi per comunicare con il IPv4 sistema di bilanciamento del carico. Scegli Dualstack without public IPv4 se i tuoi clienti utilizzano solo IPv6 indirizzi per comunicare con il load balancer.
6. Mappatura della rete
   a. Per VPC, seleziona il VPC che hai usato per le tue istanze. EC2 Se hai selezionato Internet-facing per Scheme, la selezione è disponibile solo VPCs con un gateway Internet.
   b. Per i pool di indirizzi IP IPAM è possibile scegliere di utilizzare il pool IPAM per gli indirizzi pubblici. IPv4 Per ulteriori informazioni, consulta Pool di indirizzi IP IPAM
   c. Per le zone di disponibilità e le sottoreti, abilita le zone per il tuo sistema di bilanciamento del carico selezionando le sottoreti come segue:
      - Sottoreti di due o più zone di disponibilità

- Sottireti di una o più zone locali
- Una sottorete Outpost

Per ulteriori informazioni, consulta the section called “Sottoreti per il sistema di bilanciamento del carico”.

Per i sistemi di bilanciamento del carico interni, gli IPv6 indirizzi IPv4 and vengono assegnati dalla sottorete CIDR.

Se hai abilitato la modalità Dualstack per il load balancer, seleziona le sottoreti con entrambi i blocchi e CIDR. IPv4 IPv6

7. Per Gruppi di sicurezza, seleziona un gruppo di sicurezza esistente o creane uno nuovo.

   Il gruppo di sicurezza per il load balancer deve permettergli di comunicare con i target registrati sia sulla porta del listener che sulla porta del controllo dello stato. La console può creare per tuo conto un gruppo di sicurezza per il load balancer con regole che permettono tale comunicazione. Puoi anche creare e selezionare un tuo gruppo di sicurezza. Per ulteriori informazioni, consulta Regole consigliate.

   (Facoltativo) Per creare un nuovo gruppo di sicurezza per il sistema di bilanciamento del carico, scegli Crea un nuovo gruppo di sicurezza.

8. In Ascoltatori e instradamento, l'ascoltatore predefinito accetta il traffico HTTP sulla porta 80. È possibile mantenere il protocollo e la porta predefiniti o sceglierli diversi. Per Nome, scegli il gruppo di destinazione creato. Puoi scegliere facoltativamente Aggiungi ascoltatore per aggiungere un altro ascoltatore (ad esempio un ascoltatore HTTPS).

9. (Facoltativo) Se si utilizza un listener HTTPS

   Come Policy di sicurezza, consigliamo di utilizzare sempre la policy di sicurezza predefinita più recente.

   a. Per il SSL/TLS certificato predefinito, sono disponibili le seguenti opzioni:

      - Se hai creato o importato un certificato utilizzando AWS Certificate Manager, seleziona Da ACM, quindi seleziona il certificato da Seleziona un certificato.
      - Se hai importato un certificato mediante IAM, scegli Da ACM, quindi seleziona il certificato da Seleziona un certificato.

- Se disponi di un certificato da importare ma ACM non è disponibile nella tua regione, seleziona Importa, quindi In IAM. Digita il nome del certificato nel campo Nome del certificato. In Chiave privata del certificato, copia e incolla il contenuto del file della chiave privata (con codifica PEM). In Corpo certificato, copia e incolla i contenuti del file della chiave pubblica (con codifica PEM). In Catena di certificati, copia e incolla i contenuti del file della catena di certificati (con codifica PEM), a meno che non utilizzi un certificato auto-firmato e non sia importante che i browser accettino implicitamente il certificato.

b. (Facoltativo) Per abilitare l'autenticazione reciproca, in Gestione dei certificati client abilita l'autenticazione reciproca (MTL).

   Se abilitata, la modalità TLS reciproca predefinita è passthrough.

   Se selezioni Verifica con Trust Store:

   - Per impostazione predefinita, le connessioni con certificati client scaduti vengono rifiutate. Per modificare questo comportamento, espandi le impostazioni Advanced MTLS, quindi in Scadenza del certificato client seleziona Consenti certificati client scaduti.
   - In Trust Store scegli un trust store esistente o scegli Nuovo trust store.
     - Se hai scelto Nuovo archivio attendibile, fornisci un nome di Trust Store, la posizione dell'Autorità di certificazione URI S3 e, facoltativamente, una posizione dell'elenco di revoca dei certificati URI S3.
   - (Facoltativo) Scegli se desideri abilitare TrustStore Advertise CA per i nomi dei soggetti.

10. (Facoltativo) Puoi integrare altri servizi con il tuo sistema di bilanciamento del carico durante la creazione, nella sezione Ottimizza con integrazioni di servizi.

    - Puoi scegliere di includere protezioni AWS WAFdi sicurezza per il tuo sistema di bilanciamento del carico, con un ACL web esistente o creato automaticamente. Dopo la creazione, il web ACLs può essere gestito nella console.AWS WAF Per ulteriori informazioni, consulta Associare o dissociare un ACL Web con una AWS risorsa nella Guida per gli sviluppatori.AWS WAF
    - 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, puoi gestirlo nella AWS Global Accelerator console. Per ulteriori informazioni, consulta Aggiungere un acceleratore quando si crea un sistema di bilanciamento del carico nella Guida per gli AWS Global Accelerator sviluppatori.

11. Taggare e creare

    a. (Facoltativo) Aggiungere un tag per categorizzare 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.

    b. 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 EC2 le istanze superino il controllo di integrità iniziale. Puoi quindi verificare che il load balancer stia inviando traffico alla tua istanza. EC2 Per eliminare il sistema di bilanciamento del carico, consulta Eliminazione di un Application 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. Seleziona Gruppi di destinazioni nel riquadro di navigazione.
3. Selezionare il gruppo target appena creato.
4. Scegliere Target e verificare che le istanze siano pronte. Se lo stato di un'istanza è `initial`, il motivo generalmente è che l'istanza è ancora in fase di registrazione. Questo stato può anche indicare che l'istanza 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. Selezionare il nuovo sistema di bilanciamento del carico.
7. Scegli Descrizione e copia il nome DNS del sistema di bilanciamento del carico interno o connesso a Internet (ad esempio, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com).

    - Per i sistemi di bilanciamento del carico connessi a Internet, incollare il nome DNS nel campo dell'indirizzo di un browser Web connesso alla rete Internet.

- Per i sistemi di bilanciamento del carico interni, incollare il nome DNS nel campo dell'indirizzo di un browser Web che ha una connessione privata al VPC.

Se tutto è stato configurato correttamente, il browser visualizza la pagina predefinita del server.

8. Se la pagina Web non viene visualizzata, consulta la seguente documentazione per ulteriore assistenza alla configurazione e passaggi per la risoluzione dei problemi.

   - Per ulteriori informazioni, consulta Routing del traffico a un load balancer ELB nella Guida per gli sviluppatori di Amazon Route 53.
   - Per le problematiche relative al sistema di bilanciamento del carico, consulta Risoluzione dei problemi degli Application Load Balancer.

Aggiorna le zone di disponibilità per il tuo Application Load Balancer

Puoi abilitare o disabilitare le zone di disponibilità per il tuo sistema di bilanciamento del carico in qualsiasi momento. 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. Per impostazione predefinita, gli Application Load Balancer hanno attivato il bilanciamento del carico tra zone di disponibilità, con il risultato che le richieste vengono instradate verso tutte le destinazioni registrate in tutte le zone di disponibilità. Quando il bilanciamento del carico tra zone è disattivato, il sistema di bilanciamento del carico indirizza la richiesta solo verso destinazioni nella stessa zona di disponibilità. Per ulteriori informazioni, consulta Bilanciamento del carico su più zone. Il sistema di bilanciamento del carico è più efficace se ogni zona di disponibilità abilitata dispone di almeno un target registrato.

Dopo avere disabilitato una zona di disponibilità, i target in tale zona rimangono registrati con il sistema di bilanciamento del carico, che però non instrada le richieste verso i target.

Per aggiornare le zone di disponibilità utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Mappatura di rete, scegli Modifica sottoreti.

5. Per abilitare una zona di disponibilità, seleziona la relativa casella di controllo e seleziona una sottorete. Se è presente solo una sottorete, viene già selezionata.
6. Per modificare la sottorete per una zona di disponibilità abilitata, scegli una delle altre sottoreti dall'elenco.
7. Per disabilitare una zona di disponibilità, deseleziona la relativa casella di controllo.
8. Scegli Save changes (Salva modifiche).

Per aggiornare le zone di disponibilità utilizzando il AWS CLI

Utilizza il comando set-subnets.

Gruppi di sicurezza per l'Application Load Balancer

Il gruppo di sicurezza dell'Application Load Balancer controlla il traffico a cui viene consentito di raggiungere e lasciare il sistema di bilanciamento del carico. Devi accertarti che il sistema di bilanciamento del carico sia in grado di comunicare con i target registrati sia attraverso la porta del listener sia attraverso la porta di controllo dello stato. Quando aggiungi un listener al tuo sistema di bilanciamento del carico o aggiorni la porta di controllo dello stato per un gruppo target di cui il sistema di bilanciamento del carico si serve per instradare le richieste, devi verificare che i gruppi di sicurezza associati al sistema di bilanciamento del carico permettano il traffico bidirezionale attraverso la nuova porta. Se così non è, è possibile modificare le regole per i gruppi di sicurezza attualmente associati o associare al sistema di bilanciamento del carico dei gruppi di sicurezza diversi. È possibile scegliere le porte e i protocolli da consentire. Ad esempio, puoi aprire connessioni ICMP (Internet Control Message Protocol) per il load balancer per rispondere a richieste di ping (tuttavia, le richieste di ping non vengono inoltrate a tutte le istanze).

Regole consigliate

Le regole seguenti sono consigliate per un sistema di bilanciamento del carico connesso a Internet.

Inbound		
Source	Port Range	Comment
0.0.0.0/0	*listener*	Consente tutto il traffico in entrata sulla porta del listener del load balancer

Outbound

Destination	Port Range	Comment
instance security group	*instance listener*	Consente il traffico in uscita verso le istanze sulla porta del listener dell'istanza
instance security group	*health check*	Permette il traffico in uscita verso le istanze attraverso la porta di controllo dello stato

Le seguenti regole sono consigliate per un sistema di bilanciamento del carico interno.

Inbound

Source	Port Range	Comment
VPC CIDR	*listener*	Consente il traffico in entrata dal CIDR VPC sulla porta del listener del load balancer.

Outbound

Destination	Port Range	Comment
instance security group	*instance listener*	Consente il traffico in uscita verso le istanze sulla porta del listener dell'istanza
instance security group	*health check*	Permette il traffico in uscita verso le istanze attraverso la porta di controllo dello stato

Le seguenti regole sono consigliate per un Application Load Balancer utilizzato come destinazione di un Network Load Balancer.

Inbound

Source	Port Range	Comment
client IP addresses/ CIDR	*alb listener*	Permette il traffico client in entrata sulla porta dell'asco ltatore del sistema di bilanciam ento del carico
VPC CIDR	*alb listener*	Consenti il traffico client in entrata tramite la porta AWS PrivateLink listener del sistema di bilanciamento del carico
VPC CIDR	*alb listener*	Autorizza il traffico integro in entrata dal Network Load Balancer

Outbound

Destination	Port Range	Comment
instance security group	*instance listener*	Consente il traffico in uscita verso le istanze sulla porta del listener dell'istanza
instance security group	*health check*	Permette il traffico in uscita verso le istanze attraverso la porta di controllo dello stato

Tenere presente che i gruppi di sicurezza dell'Application Load Balancer utilizza il monitoraggio della connessione per monitorare il traffico in arrivo dal Network Load Balancer. Questo si verifica a prescindere dalle regole del gruppo di sicurezza impostate per l'Application Load Balancer. Per ulteriori informazioni sul tracciamento delle EC2 connessioni Amazon, consulta Tracciamento delle connessioni dei gruppi di sicurezza nella Amazon EC2 User Guide.

Per garantire che i tuoi obiettivi ricevano traffico esclusivamente dal sistema di bilanciamento del carico, limita i gruppi di sicurezza associati ai tuoi obiettivi in modo che accettino il traffico esclusivamente dal sistema di bilanciamento del carico. Ciò può essere ottenuto impostando il gruppo di sicurezza del load balancer come origine nella regola di ingresso del gruppo di sicurezza della destinazione.

Ti consigliamo inoltre di consentire il traffico ICMP in entrata per supportare il rilevamento della MTU del percorso. Per ulteriori informazioni, consulta Path MTU Discovery nella Amazon EC2 User Guide.

Aggiornare i gruppi di sicurezza associati

Puoi aggiornare i gruppi di sicurezza associati al tuo sistema di bilanciamento del carico in qualsiasi momento.

Per aggiornare i gruppi di sicurezza utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Sicurezza, scegli Modifica.
5. Per associare un gruppo di sicurezza al sistema di bilanciamento del carico, selezionalo. Per rimuovere l'associazione a un gruppo di sicurezza, scegli l'icona X relativa a tale gruppo di sicurezza.
6. Scegli Save changes (Salva modifiche).

Per aggiornare i gruppi di sicurezza utilizzando il AWS CLI

Utilizza il comando set-security-groups.

Aggiorna i tipi di indirizzi IP per il tuo Application Load Balancer

È possibile configurare l'Application Load Balancer in modo che i client possano comunicare con il sistema di bilanciamento del carico utilizzando solo IPv4 gli indirizzi o utilizzando entrambi gli IPv6 indirizzi (IPv4 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) e le sottoreti specificati per il bilanciamento del carico devono avere blocchi CIDR associati. IPv6 Per ulteriori informazioni, IPv6consulta gli indirizzi nella Amazon EC2 User Guide.
- Le tabelle di routing per le sottoreti del load balancer devono indirizzare il traffico. IPv6
- I gruppi di sicurezza per il load balancer devono consentire il traffico. IPv6
- La rete ACLs per le sottoreti del load balancer deve 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 EC2 console Amazon 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. Nella scheda Mappatura di rete, scegli Modifica tipo di indirizzo IP.
5. Per il tipo di indirizzo IP, scegli IPv4di supportare solo IPv4 gli indirizzi, Dualstack per supportare entrambi IPv4 IPv6 gli indirizzi o Dualstack senza pubblico per supportare solo gli indirizzi. IPv4 IPv6
6. Scegli Save changes (Salva modifiche).

Per aggiornare il tipo di indirizzo IP utilizzando il AWS CLI

Utilizza il comando set-ip-address-type.

Aggiorna i pool di indirizzi IP IPAM per il tuo Application Load Balancer

I pool di indirizzi IP IPAM devono essere creati all'interno di IPAM prima di poter essere utilizzati dall'Application Load Balancer. Per ulteriori informazioni, consulta Bring your IP address to IPAM.

Per impostare i pool di indirizzi IP IPAM al momento della creazione

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

Per aggiornare i pool di indirizzi IP IPAM utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Mappatura della rete, scegli Modifica pool IP.
5. In Pool IP, attiva Usa il pool IPAM per gli indirizzi pubblici IPv4 .
6. In Pool IPv4 IPAM pubblico scegli il pool IPAM che desideri utilizzare.
7. Scegli Save changes (Salva modifiche).

Per aggiornare i pool di indirizzi IP IPAM utilizzando il AWS CLI

Utilizza il comando modify-ip-pools.

Integrazioni per il tuo Application Load Balancer

Puoi ottimizzare l'architettura dell'Application Load Balancer integrandola con diversi altri AWS servizi per migliorare le prestazioni, la sicurezza e la disponibilità dell'applicazione.

Integrazioni con Load Balancer

- Amazon Application Recovery Controller (ARC)
- CloudFront Amazon+ AWS WAF
- AWS Global Accelerator
- AWS Config
- AWS WAF

Amazon Application Recovery Controller (ARC)

Amazon Application Recovery Controller (ARC) ti aiuta a prepararti e a eseguire operazioni di ripristino più rapide per le applicazioni in AWS esecuzione. Lo spostamento di zona e lo spostamento automatico di zona sono funzionalità di Amazon Application Recovery Controller (ARC).

Con lo spostamento zonale, puoi spostare il traffico lontano da una zona di disponibilità ridotta con una sola azione. In questo modo è possibile continuare a operare da altre zone di disponibilità integre in una Regione AWS.

Con lo spostamento automatico zonale, autorizzi AWS a spostare il traffico di risorse di un'applicazione da una zona di disponibilità durante gli eventi, per tuo conto, per ridurre i tempi di ripristino. AWS avvia uno spostamento automatico quando il monitoraggio interno indica che esiste una violazione della zona di disponibilità che potrebbe avere un impatto potenziale sui clienti. Quando AWS inizia uno spostamento automatico, il traffico delle applicazioni verso le risorse che hai configurato per lo spostamento automatico zonale inizia a spostarsi dalla zona di disponibilità.

Quando si avvia uno spostamento zonale, il sistema di bilanciamento del carico interrompe l'invio di nuovo traffico per la risorsa alla zona di disponibilità interessata. ARC crea immediatamente lo spostamento zonale. Tuttavia, il completamento delle connessioni esistenti e in corso nella zona di disponibilità può richiedere poco tempo, a seconda del comportamento del client e del riutilizzo della connessione. A seconda delle impostazioni DNS e di altri fattori, le connessioni esistenti possono essere completate in pochi minuti o potrebbero richiedere più tempo. Per ulteriori informazioni, consulta Limita il tempo in cui i client rimangono connessi ai tuoi endpoint nella Amazon Application Recovery Controller (ARC) Developer Guide.

Per utilizzare le funzionalità di spostamento zonale su Application Load Balancers, devi avere l'attributo ARC zonal shift integration impostato su Enabled.

Prima di abilitare l'integrazione con Amazon Application Recovery Controller (ARC) e iniziare a utilizzare Zonal Shift, consulta quanto segue:

- 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 diversi 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.

Per ulteriori informazioni, consulta le migliori pratiche per i cambiamenti zonali in ARC nella Amazon Application Recovery Controller (ARC) Developer Guide.

Application Load Balancer abilitati per più zone

Quando viene avviato uno spostamento di zona su un Application Load Balancer con il bilanciamento del carico tra zone abilitato, tutto il traffico verso le destinazioni viene bloccato nella zona di disponibilità interessata e gli indirizzi IP zonali vengono rimossi dal DNS.

Vantaggi:

- Ripristino più rapido in caso di guasti nelle zone di disponibilità.
- La capacità di spostare il traffico verso una zona di disponibilità integra se vengono rilevati guasti in una zona di disponibilità.
- È possibile testare l'integrità delle applicazioni simulando e identificando gli errori per prevenire tempi di inattività non pianificati.

Sovrascrittura amministrativa del turno zonale

Le destinazioni che appartengono a un Application Load Balancer includeranno un nuovo statoAdministrativeOverride, indipendente dallo TargetHealth stato.

Quando viene avviato uno spostamento di zona per un Application Load Balancer, tutte le destinazioni all'interno della zona da cui viene allontanato vengono considerate sostituite dal punto di vista amministrativo. L'Application Load Balancer interromperà l'instradamento del nuovo traffico verso le destinazioni sostituite dal punto di vista amministrativo, tuttavia le connessioni esistenti rimangono intatte fino a quando non vengono chiuse organicamente.

Gli stati possibili sono: AdministrativeOverride

sconosciuto

Lo stato non può essere propagato a causa di un errore interno

no_override

Nessun override è attualmente attivo sulla destinazione

zonal_shift_active

Lo spostamento zonale è attivo nella zona di disponibilità di destinazione

CloudFront Amazon+ AWS WAF

Amazon CloudFront è un servizio web che aiuta a migliorare le prestazioni, la disponibilità e la sicurezza delle applicazioni che utilizzi AWS. CloudFront funge da punto di accesso unico e distribuito per le applicazioni Web che utilizzano Application Load Balancers. Estende la portata di Application Load Balancer a livello globale, consentendole di servire gli utenti in modo efficiente dalle edge location vicine, ottimizzando la distribuzione dei contenuti e riducendo la latenza per gli utenti di tutto il mondo. La memorizzazione automatica dei contenuti in queste edge location riduce significativamente il carico sull'Application Load Balancer, migliorandone le prestazioni e la scalabilità.

L'integrazione con un clic disponibile nella console Elastic Load Balancing crea CloudFront una distribuzione con le protezioni di sicurezza AWS WAF consigliate e la associa all'Application Load Balancer. Le AWS WAF protezioni bloccano gli exploit web più comuni prima di raggiungere il sistema di bilanciamento del carico. Puoi accedere alla CloudFront distribuzione e alla dashboard di sicurezza corrispondente dalla scheda Integrazioni del load balancer nella console. Per ulteriori informazioni, consulta Gestire le protezioni AWS WAF di sicurezza nella dashboard di CloudFront sicurezza nella Amazon CloudFront Developer Guide e Introducing Security Dashboard, a Unified CDN and CloudFront Security Experience all'indirizzo aws.amazon.com/blogs.

Come best practice in materia di sicurezza, configura i gruppi di sicurezza di Application Load Balancer con accesso a Internet in modo da consentire il traffico in entrata solo dall'elenco dei prefissi gestiti per e rimuovere qualsiasi altra regola in entrata. AWS CloudFront Per ulteriori informazioni, consulta Utilizzare l'elenco di prefissi CloudFront gestiti, CloudFront Configurare per aggiungere un'intestazione HTTP personalizzata alle richieste e Configurare un Application Load Balancer per inoltrare solo le richieste che contengono un'intestazione specifica nell' CloudFront Amazon Developer Guide >.

> **Note**
>
> CloudFront supporta solo i certificati ACM nella regione us-east-1 degli Stati Uniti orientali (Virginia settentrionale). Se l'Application Load Balancer dispone di un listener HTTPS configurato con un certificato ACM in una regione diversa da us-east-1, sarà necessario modificare la connessione di CloudFront origine da HTTPS a HTTP oppure fornire un certificato ACM nella regione Stati Uniti orientali (Virginia settentrionale) e collegarlo alla distribuzione. CloudFront

AWS Global Accelerator

Per ottimizzare la disponibilità, le prestazioni e la sicurezza delle applicazioni, crea un acceleratore per il bilanciamento del carico. L'acceleratore indirizza il traffico sulla rete AWS globale verso indirizzi IP statici che fungono da endpoint fissi nella regione più vicina al client. AWS Global Accelerator è protetto da Shield Standard, che riduce al minimo i tempi di inattività delle applicazioni e la latenza dagli attacchi S. DDo

Per ulteriori informazioni, consulta Aggiungere un acceleratore quando si crea un sistema di bilanciamento del carico nella Guida per gli sviluppatori.AWS Global Accelerator

AWS Config

Per ottimizzare il monitoraggio e la conformità del tuo sistema di bilanciamento del carico, configura. AWS Config AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo AWS account. Ciò include il modo in cui le risorse sono correlate tra loro e come sono state configurate in passato, in modo da poter vedere come le configurazioni e le relazioni cambiano nel tempo. AWS Config semplifica i controlli, la conformità e la risoluzione dei problemi.

Per ulteriori informazioni, consulta What Is? AWS Config nella Guida per gli AWS Config sviluppatori.

AWS WAF

Puoi utilizzarlo AWS WAF con il tuo Application Load Balancer per consentire o bloccare le richieste in base alle regole di una lista di controllo degli accessi Web (Web ACL).

Per impostazione predefinita, se il load balancer non riesce a ottenere una risposta AWS WAF, restituisce un errore HTTP 500 e non inoltra la richiesta. Se hai bisogno che il sistema di bilanciamento del carico inoltri le richieste alle destinazioni anche se non è in grado di contattare AWS WAF, puoi abilitare il AWS WAF fail-open.

Web predefinito ACLs

Quando abiliti AWS WAF l'integrazione, puoi scegliere di creare automaticamente un nuovo ACL web con regole predefinite. L'ACL web predefinito include tre regole AWS gestite che offrono protezioni contro le minacce alla sicurezza più comuni.

- `AWSManagedRulesAmazonIpReputationList`- Il gruppo di regole dell'elenco di reputazione IP di Amazon blocca gli indirizzi IP generalmente associati a bot o altre minacce. Per ulteriori

informazioni, consulta Amazon IP Reputation List managed rule group nella AWS WAF Developer Guide.

- `AWSManagedRulesCommonRuleSet`- Il gruppo di regole di base (CRS) fornisce protezione contro lo sfruttamento di un'ampia gamma di vulnerabilità, incluse alcune delle vulnerabilità ad alto rischio e più comuni descritte nelle pubblicazioni OWASP come OWASP Top 10. Per ulteriori informazioni, consulta il gruppo di regole gestito Core rule set (CRS) nella Developer Guide.AWS WAF
- `AWSManagedRulesKnownBadInputsRuleSet`- Il gruppo di regole Known bad inputs blocca i pattern di richiesta noti per non essere validi e associati allo sfruttamento o alla scoperta di vulnerabilità. Per ulteriori informazioni, consulta il gruppo di regole gestito da Known bad inputs nella Guida per gli sviluppatori.AWS WAF

Per ulteriori informazioni, consulta Using web ACLs in AWS WAF nella AWS WAF Developer Guide.

Modifica gli attributi per il tuo Application Load Balancer

Dopo aver creato un Application Load Balancer, è possibile modificarne gli attributi.

Attributi del sistema di bilanciamento del carico

- Timeout di inattività della connessione
- durata keepalive del client HTTP
- Deletion protection (Protezione da eliminazione)
- Modalità di mitigazione della desincronizzazione
- Conservazione dell'intestazione host

Timeout di inattività della connessione

Il timeout di inattività della connessione è il periodo di tempo in cui una connessione client o di destinazione esistente può rimanere inattiva, senza inviare o ricevere dati, prima che il load balancer chiuda la connessione.

Per garantire che operazioni lunghe come il caricamento di file abbiano il tempo di completare, invia almeno 1 byte di dati prima della scadenza di ogni periodo di timeout di inattività e aumenta la durata del periodo di inattività in base alle esigenze. Ti consigliamo inoltre di configurare il timeout di inattività dell'applicazione in modo che sia superiore al timeout di inattività configurato per il sistema di bilanciamento del carico. In caso contrario, se l'applicazione chiude la connessione TCP al sistema

di bilanciamento del carico in modo drastico, il sistema di bilanciamento del carico potrebbe inviare una richiesta all'applicazione prima di ricevere il pacchetto che indica che la connessione è chiusa. In tal caso, il sistema di bilanciamento del carico invia un errore HTTP 502 Gateway non valido al client.

Gli Application Load Balancer non supportano i frame PING HTTP/2. Questi non ripristinano il timeout di inattività della connessione.

Per impostazione predefinita, Elastic Load Balancing imposta il valore di timeout di inattività per il sistema di bilanciamento del carico su 60 secondi o 1 minuto. Utilizza la procedura seguente per impostare un valore di timeout per inattività diverso.

Per aggiornare il valore di timeout di inattività della connessione utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. In Configurazione del traffico, inserisci un valore per il timeout di inattività della connessione. L'intervallo valido è compreso tra 1 e 4000 secondi.
6. Scegli Save changes (Salva modifiche).

Per aggiornare il valore del timeout di inattività utilizzando il AWS CLI

Utilizzare il modify-load-balancer-attributescomando con l'attributo. `idle_timeout.timeout_seconds`

durata keepalive del client HTTP

La durata keepalive del client HTTP è il periodo di tempo massimo durante il quale un Application Load Balancer mantiene una connessione HTTP persistente a un client. Trascorsa la durata di keepalive del client HTTP configurato, l'Application Load Balancer accetta un'altra richiesta e quindi restituisce una risposta che chiude correttamente la connessione.

Il tipo di risposta inviata dal load balancer dipende dalla versione HTTP utilizzata dalla connessione client.

- Per i client connessi tramite HTTP 1.x, il load balancer invia un'intestazione HTTP contenente il campo. `Connection: close`

- Per i client connessi tramite HTTP/2, il load balancer invia un frame. `GOAWAY`

Per impostazione predefinita, Application Load Balancer imposta il valore di durata keepalive del client HTTP per i sistemi di bilanciamento del carico su 3600 secondi o 1 ora. La durata keepalive del client HTTP non può essere disattivata o impostata al di sotto del minimo di 60 secondi, ma è possibile aumentare la durata di keepalive del client HTTP, fino a un massimo di 604800 secondi o 7 giorni. Un Application Load Balancer inizia il periodo di durata keepalive del client HTTP quando viene inizialmente stabilita una connessione HTTP a un client. Il periodo di durata continua quando non c'è traffico e non viene ripristinato finché non viene stabilita una nuova connessione.

Quando il traffico del sistema di bilanciamento del carico viene spostato da una zona di disponibilità ridotta utilizzando lo spostamento zonale o lo spostamento automatico di zona, i client con connessioni aperte esistenti potrebbero continuare a effettuare richieste verso la posizione compromessa fino alla riconnessione dei client. Per supportare un ripristino più rapido, prendi in considerazione l'impostazione di un valore di durata keepalive inferiore, per limitare il tempo in cui i client rimangono connessi a un sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Limita il tempo in cui i client rimangono connessi ai tuoi endpoint nella Amazon Application Recovery Controller (ARC) Developer Guide.

> **Note**
>
> Quando il load balancer cambia il tipo di indirizzo IP dell'Application `dualstack-without-public-ipv4` Load Balancer su, il load balancer attende il completamento di tutte le connessioni attive. Per ridurre il tempo necessario per cambiare il tipo di indirizzo IP per il tuo Application Load Balancer, valuta la possibilità di ridurre la durata di keepalive del client HTTP.

L'Application Load Balancer assegna al client HTTP il valore di durata keepalive durante la connessione iniziale. Quando si aggiorna la durata keepalive del client HTTP, ciò può comportare connessioni simultanee con valori di durata keepalive del client HTTP diversi. Le connessioni esistenti mantengono il valore di durata keepalive del client HTTP applicato durante la connessione iniziale. Le nuove connessioni ricevono il valore di durata keepalive del client HTTP aggiornato.

Per aggiornare il valore di durata del client keepalive utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. In Configurazione del traffico, inserisci un valore per la durata di keepalive del client HTTP. L'intervallo valido è compreso tra 60 e 604800 secondi.
6. Scegli Save changes (Salva modifiche).

Per aggiornare il valore della durata di keepalive del client utilizzando il AWS CLI

Usa il modify-load-balancer-attributescomando con l'`client_keep_alive.seconds`attributo.

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 EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. In Configurazione, attivare Protezione da eliminazione.
6. Scegli Save changes (Salva modifiche).

Per disabilitare la protezione da eliminazione tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Configurazione, disattivare Protezione da eliminazione.
6. Scegli Save changes (Salva modifiche).

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

Utilizzare il modify-load-balancer-attributescomando con l'`deletion_protection.enabled`attributo.

Modalità di mitigazione della desincronizzazione

La modalità di attenuazione della desincronizzazione protegge l'applicazione da problemi dovuti alla desincronizzazione HTTP. Il load balancer classifica ogni richiesta in base al relativo livello di minaccia, consente le richieste sicure e quindi riduce i rischi come specificato dalla modalità di attenuazione specificata. Le modalità di attenuazione della desincronizzazione sono monitorate, difensive e più rigorose. L'impostazione predefinita è la modalità difensiva, che fornisce un'attenuazione duratura contro la desincronizzazione HTTP mantenendo la disponibilità dell'applicazione. È possibile passare alla modalità più rigorosa per garantire che l'applicazione riceva solo richieste conformi a RFC 7230.

La libreria http_desync_guardian analizza le richieste HTTP per prevenire gli attacchi di desincronizzazione HTTP. Per ulteriori informazioni, vedere HTTP Desync Guardian su GitHub.

Classificazioni

Le classificazioni sono le seguenti:

- Conformità: la richiesta è conforme a RFC 7230 e non presenta minacce per la sicurezza note.
- Accettabile: la richiesta non è conforme a RFC 7230 ma non presenta minacce per la sicurezza note.
- Ambigua: la richiesta non è conforme a RFC 7230 ma rappresenta un rischio, poiché vari server web e proxy potrebbero gestirla in modo diverso.
- Grave: la richiesta comporta un elevato rischio per la sicurezza. Il load balancer blocca la richiesta, fornisce una risposta 400 al client e chiude la connessione client.

Se una richiesta non è conforme a RFC 7230, il bilanciamento del carico incrementa il parametro `DesyncMitigationMode_NonCompliant_Request_Count`. Per ulteriori informazioni, consulta Parametri di Application Load Balancer.

La classificazione di ogni richiesta è inclusa nei log di accesso del sistema di bilanciamento del carico. Se la richiesta non è conforme, i log di accesso includono un codice del motivo della classificazione. Per ulteriori informazioni, consulta Motivi della classificazione.

Modalità

La tabella seguente descrive come gli Application Load Balancer trattano le richieste in base alla modalità e alla classificazione.

Classificazione	Modalità monitorata	Modalità difensiva	Modalità più rigorosa
Conforme	Consentito	Consentito	Consentito
Accettabile	Consentito	Consentito	Bloccato
Ambiguo	Consentito	Consentito[1]	Bloccato
Grave	Consentito	Bloccato	Bloccato

[1] Esegue il routing delle richieste ma chiude le connessioni client e target. È possibile incorrere in costi aggiuntivi se il sistema di bilanciamento del carico riceve un gran numero di richieste ambigue in modalità difensiva. Questo si verifica perché il numero crescente di nuove connessioni al secondo contribuisce al numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate all'ora. È possibile utilizzare il parametro `NewConnectionCount` per confrontare come il sistema di bilanciamento del carico stabilisce nuove connessioni in modalità monitoraggio e in modalità difensiva.

Per aggiornare la modalità di attenuazione della desincronizzazione tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. In Gestione pacchetti, per Modalità di attenuazione della desincronizzazione, scegli Difensiva, Più rigorosa o Monitoraggio.
6. Scegli Save changes (Salva modifiche).

Per aggiornare la modalità di mitigazione della desincronizzazione utilizzando il AWS CLI

Utilizzare il modify-load-balancer-attributescomando con l'`routing.http.desync_mitigation_mode`attributo impostato su `monitor`o. `defensive``strictest`

Conservazione dell'intestazione host

Quando si abilita l'attributo Conservazione dell'intestazione host, l'Application Load Balancer conserva l'intestazione `Host` nella richiesta HTTP e invia l'intestazione alle destinazioni senza alcuna modifica. Se l'Application Load Balancer riceve più intestazioni `Host`, le conserva tutte. Le regole dell'ascoltatore vengono applicate solo alla prima intestazione `Host` ricevuta.

Per impostazione predefinita, quando l'attributo Conservazione dell'intestazione host non è abilitato, l'Application Load Balancer modifica l'intestazione `Host` nel modo seguente:

Quando la conservazione dell'intestazione host non è abilitata e la porta dell'ascoltatore è una porta non predefinita: quando non si utilizzano le porte predefinite (80 o 443), il numero della porta viene aggiunto all'intestazione host se non è già aggiunto dal client. Ad esempio, l'intestazione `Host` nella richiesta HTTP con `Host: www.example.com`, sarebbe modificata in `Host: www.example.com:8080` se la porta dell'ascoltatore fosse una porta non predefinita come `8080`.

Quando la conservazione dell'intestazione host non è abilitata e la porta dell'ascoltatore è una porta predefinita (80 o 443): per le porte dell'ascoltatore predefinite (80 o 443), il numero della porta non viene aggiunto all'intestazione host in uscita. Qualsiasi numero di porta già presente nell'intestazione host viene rimosso.

La tabella seguente illustra ulteriori esempi di come Application Load Balancer tratta le intestazioni host nella richiesta HTTP basata sulla porta dell'ascoltatore.

Porta dell'ascoltatore	Richiesta di esempio	Intestazione host nella richiesta	Conservazione dell'intestazione host disabilitata (comportamento predefinito)	Conservazione dell'intestazione host abilitata
La richiesta viene inviata sul HTTP/HTTPS listener predefinito.	`GET /index.html HTTP/1.1 Host: example.com`	example.com	example.com	example.com

Porta dell'asco ltatore	Richiesta di esempio	Intestazione host nella richiesta	Conservazione dell'intestazione host disabilitata (comportamento predefinito)	Conservazione dell'intestazione host abilitata
La richiesta viene inviata sul listener HTTP predefinito e l'intestazione dell'host ha una porta (ad esempio, 80 o 443).	`GET / index.ht ml HTTP/1.1 Host: example.c om:80`	example.com:80	example.com	example.com:80
La richiesta ha un percorso assoluto.	`GET https:// dns_name/i ndex.html HTTP/1.1 Host: example.com`	example.com	dns_name	example.com
La richiesta viene inviata su una porta listener non predefinita (ad esempio 8080)	`GET / index.ht ml HTTP/1.1 Host: example.com`	example.com	example.c om:8080	example.com

Porta dell'asco ltatore	Richiesta di esempio	Intestazione host nella richiesta	Conservazione dell'intestazione host disabilitata (comportamento predefinito)	Conservazione dell'intestazione host abilitata
La richiesta viene inviata su una porta dell'ascoltatore non predefini ta e l'intesta zione host ha una porta (ad esempio, 8080).	`GET / index.ht ml HTTP/1.1 Host: example.c om:8080`	example.c om:8080	example.c om:8080	example.c om:8080

Per abilitare la conservazione dell'intestazione dell'host utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare il load balancer.
4. Nella scheda Attributi, scegli Modifica.
5. In Gestione pacchetti, attivare Conserva intestazione host.
6. Scegli Save changes (Salva modifiche).

Per abilitare la conservazione dell'intestazione dell'host utilizzando il AWS CLI

Utilizzate il modify-load-balancer-attributescomando con l'`routing.http.preserve_host_header.enabled`attributo `true` impostato su.

Etichetta un Application Load Balancer

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

È possibile aggiungere più tag a ciascun sistema di bilanciamento del carico. 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
- 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 AWS riservato all'uso. Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Per aggiornare i tag di un sistema di bilanciamento del carico tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Tag, scegli Gestisci tag, quindi eseguire una o più delle operazioni seguenti:
   a. Per aggiornare un tag, modificare i valori di Chiave e Valore.
   b. Per aggiungere un tag, scegli Aggiungi tag e poi inserisci valori per Chiave e Valore.
   c. Per eliminare un tag, scegli il pulsante Rimuovi accanto al tag da eliminare.
5. Una volta completato l'aggiornamento dei tag, scegli Salva.

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

Utilizza i comandi add-tags e remove-tags.

Eliminazione di un Application 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).

Ricorda che l'eliminazione di un sistema di bilanciamento del carico non influisce sui suoi target registrati. Ad esempio, le EC2 istanze continuano a funzionare e sono ancora registrate nei rispettivi gruppi target. Per eliminare i gruppi target, consulta Eliminare un gruppo target di Application Load Balancer.

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 EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
3. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
4. Seleziona il sistema di bilanciamento del carico, poi scegli Operazioni, Elimina sistema di bilanciamento del carico.
5. Quando viene richiesta la conferma, immettere **`confirm`** e quindi scegliere Elimina.

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

Utilizza il comando delete-load-balancer.

Visualizza la mappa delle risorse di Application Load Balancer

La mappa delle risorse di Application Load Balancer fornisce una visualizzazione interattiva dell'architettura del load balancer, inclusi i listener, le regole, 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 load balancer.

Per visualizzare la mappa delle risorse dell'Application Load Balancer utilizzando la console

1. Apri la EC2 console Amazon 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 Application 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.

Gruppi di risorse

La mappa delle risorse di Application Load Balancer contiene quattro gruppi di risorse, uno per ogni tipo di risorsa. I gruppi di risorse sono Listener, Rules, Target groups e Targets.

Riquadri di risorse

Ogni risorsa all'interno di un gruppo 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.
  - condizioni della regola: le condizioni per ogni regola.
  - riepilogo sullo stato di salute del gruppo destinatario: il numero di obiettivi registrati per ogni stato di salute.
  - stato di salute dell'obiettivo Lo stato di salute attuale e la descrizione degli obiettivi.

  > **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, `HTTP:80`
  - Regole - Seleziona l'azione delle regole. Ad esempio, `Forward to target group`
  - 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 Application Load Balancer in formato PDF.

Prenotazioni di capacità per il tuo Application Load Balancer

Le prenotazioni di Load Balancer Capacity Unit (LCU) consentono di riservare una capacità minima statica per il sistema di bilanciamento del carico. Gli Application Load Balancer si ridimensionano automaticamente per supportare i carichi di lavoro rilevati e soddisfare le esigenze di capacità. Quando viene configurata la capacità minima, il sistema di bilanciamento del carico continua a scalare verso l'alto o verso il basso in base al traffico ricevuto, ma impedisce anche che la capacità scenda al di sotto della capacità minima configurata.

Prendi in considerazione l'utilizzo della prenotazione LCU nelle seguenti situazioni:

- Hai un evento imminente che avrà un traffico improvviso e insolito e vuoi assicurarti che il sistema di bilanciamento del carico sia in grado di supportare l'improvviso picco di traffico durante l'evento.
- La natura del carico di lavoro comporta picchi di traffico imprevedibili per un breve periodo.
- Stai configurando il tuo sistema di bilanciamento del carico per integrare o migrare i tuoi servizi a un orario di avvio specifico e devi iniziare con una capacità elevata invece di aspettare che l'auto-scaling abbia effetto.
- È necessario mantenere una capacità minima per soddisfare gli accordi sui livelli di servizio o i requisiti di conformità.
- Stai migrando i carichi di lavoro tra sistemi di bilanciamento del carico e desideri configurare la destinazione in modo che corrisponda alla scala dell'origine.

Stima la capacità di cui hai bisogno

Per determinare la quantità di capacità da riservare al sistema di bilanciamento del carico, consigliamo di eseguire test di carico o di esaminare i dati storici sul carico di lavoro che rappresentano il traffico imminente previsto. Utilizzando la console Elastic Load Balancing, puoi stimare la capacità da riservare in base al traffico esaminato.

In alternativa, puoi utilizzare la CloudWatch metrica `PeakLCUs` per determinare il livello di capacità necessario. La `PeakLCUs` metrica tiene conto dei picchi del modello di traffico che il sistema di bilanciamento del carico deve scalare su tutte le dimensioni di scalabilità per supportare il carico di lavoro. La `PeakLCUs` metrica è diversa dalla `ConsumedLCUs` metrica, che aggrega solo le dimensioni di fatturazione del traffico. Si consiglia di utilizzare la `PeakLCUs` metrica per garantire che la prenotazione della LCU sia adeguata durante la scalabilità del sistema di bilanciamento del carico. Per la stima della capacità, utilizza un valore al minuto di. `Sum` `PeakLCUs`

Se non disponi di dati storici sul carico di lavoro a cui fare riferimento e non puoi eseguire test di carico, puoi stimare la capacità necessaria utilizzando il calcolatore di prenotazione LCU. Il calcolatore delle prenotazioni LCU utilizza dati basati sui carichi di lavoro storici AWS osservati e potrebbe non rappresentare il carico di lavoro specifico dell'utente. Per ulteriori informazioni, consulta Load Balancer Capacity Unit Reservation Calculator.

Quote per le prenotazioni LCU

Il tuo account ha quote relative a. LCUs Per ulteriori informazioni, consulta the section called “Unità di capacità Load Balancer”.

Richiedi la prenotazione della Load Balancer Capacity Unit per il tuo Application Load Balancer

Prima di utilizzare la prenotazione LCU, verifica quanto segue:

- La capacità è riservata a livello regionale ed è distribuita uniformemente tra le zone di disponibilità. Verifica di avere un numero sufficiente di obiettivi distribuiti in modo uniforme in ciascuna zona di disponibilità prima di attivare la prenotazione LCU.
- Le richieste di prenotazione LCU vengono soddisfatte in base al principio «primo arrivato, primo servito» e dipendono dalla capacità disponibile per una zona in quel momento. La maggior parte delle richieste viene in genere soddisfatta entro pochi minuti, ma può richiedere fino a qualche ora.
- Per aggiornare una prenotazione esistente, è necessario che la richiesta precedente sia stata effettuata o non sia riuscita. Puoi aumentare la capacità riservata tutte le volte che vuoi, tuttavia puoi diminuirla solo due volte al giorno.
- Continuerai a incorrere in addebiti per qualsiasi capacità riservata o fornita fino alla cessazione o alla cancellazione di tale capacità.

Richiedi una prenotazione LCU

I passaggi di questa procedura spiegano come richiedere una prenotazione LCU sul sistema di bilanciamento del carico.

Per richiedere una prenotazione LCU utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare il nome del sistema di bilanciamento del carico.
4. Nella scheda Capacità, scegli Modifica prenotazione LCU.
5. Seleziona Stima storica basata su riferimenti, quindi seleziona il sistema di bilanciamento del carico dall'elenco a discesa.
6. Seleziona il periodo di riferimento per visualizzare il livello LCU riservato consigliato.
7. Se non disponi di un carico di lavoro di riferimento storico, puoi scegliere Stima manuale e inserire il numero LCUs da prenotare.
8. Scegli Save (Salva).

Per richiedere una prenotazione LCU utilizzando AWS CLI

Utilizza il comando modify-capacity-reservation.

Aggiorna o termina le prenotazioni Load Balancer Capacity Unit per il tuo Application Load Balancer

Aggiornare o terminare una prenotazione LCU

I passaggi di questa procedura spiegano come aggiornare o terminare una prenotazione LCU sul sistema di bilanciamento del carico.

Per aggiornare o terminare una prenotazione LCU utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare il nome del sistema di bilanciamento del carico.
4. Nella scheda Capacità, conferma che lo stato della prenotazione è Fornito.
    a. Per aggiornare la prenotazione LCU, scegli Modifica prenotazione LCU.
    b. Per terminare la prenotazione LCU, scegli Annulla capacità.

Per aggiornare o terminare una prenotazione LCU utilizzando il AWS CLI

Utilizza il comando modify-capacity-reservation.

Monitora la prenotazione della Load Balancer Capacity Unit per il tuo Application Load Balancer

Stato della prenotazione

La prenotazione LCU ha quattro stati disponibili:

- in sospeso - Indica che la prenotazione è in fase di approvvigionamento.
- fornito - Indica che la capacità riservata è pronta e disponibile per l'uso.
- fallito - Indica che la richiesta non può essere completata in quel momento.
- ribilanciamento - Indica che è stata aggiunta o rimossa una zona di disponibilità e il bilanciamento del carico sta riequilibrando la capacità.

LCU riservata

La `ReservedLCUs` metrica viene riportata al minuto. La capacità è riservata su base oraria. Ad esempio, se hai una prenotazione LCU di 6.000, il totale per un'ora `ReservedLCUs` è 6.000 e il totale di un minuto è 100. Per determinare l'utilizzo riservato della LCU, fate riferimento alla metrica. `PeakLCUs` È possibile impostare CloudWatch allarmi per confrontare la capacità al minuto con il valore `Sum` della capacità riservata, oppure quella `PeakLCUs` oraria `Sum` di`ReservedLCUs`, per determinare se la capacità riservata è sufficiente per soddisfare le proprie esigenze.

Monitora la capacità riservata

I passaggi di questo processo spiegano come verificare lo stato di una prenotazione LCU sul sistema di bilanciamento del carico.

Per visualizzare lo stato di una prenotazione LCU utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Selezionare il nome del sistema di bilanciamento del carico.
4. Nella scheda Capacità, puoi visualizzare lo stato della prenotazione e il valore della LCU riservata.

Per monitorare lo stato della prenotazione LCU utilizzando AWS CLI

Utilizza il comando describe-capacity-reservation.

Ascoltatori per Application Load Balancer

Un ascoltatore è un processo che controlla le richieste di connessione utilizzando il protocollo e la porta configurata. Prima di iniziare a utilizzare l'Application Load Balancer, è necessario aggiungere almeno un ascoltatore. Se il sistema di bilanciamento del carico non ha un ascoltatore, non può ricevere traffico dai client. Le regole che definisci per i tuoi listener determinano il modo in cui il load balancer indirizza le richieste verso le destinazioni registrate, ad esempio le EC2 istanze.

Indice

Configurazione dei listener

I listener supportano i seguenti protocolli e porte:

- Protocolli: HTTP, HTTPS
- Porte: 1-65535

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

Se devi assicurarti che siano le destinazioni a decrittare il traffico HTTPS al posto del sistema di bilanciamento del carico, è possibile creare un Network Load Balancer con un ascoltatore TCP sulla porta 443. Con un ascoltatore TCP, il sistema di bilanciamento del carico passa il traffico crittografato alle destinazioni senza decrittarlo. Per ulteriori informazioni, consulta la Guida per l'utente dei Network Load Balancer.

WebSockets

Gli Application Load Balancer forniscono supporto nativo per. WebSockets È possibile aggiornare una connessione HTTP/1.1 esistente in una connessione WebSocket (`wsowss`) utilizzando un aggiornamento della connessione HTTP. Quando si esegue l'aggiornamento, la connessione TCP utilizzata per le richieste (al sistema di bilanciamento del carico e alla destinazione) diventa una WebSocket connessione persistente tra il client e la destinazione tramite il sistema di bilanciamento del carico. È possibile utilizzare sia WebSockets i listener HTTP che HTTPS. Le opzioni scelte per il listener si applicano sia alle WebSocket connessioni che al traffico HTTP. Per ulteriori informazioni, consulta How the WebSocket Protocol Works nella Amazon CloudFront Developer Guide.

HTTP/2

Gli Application Load Balancer forniscono supporto nativo per HTTP/2 con ascoltatori HTTPS. È possibile inviare fino a 128 richieste in parallelo utilizzando una sola connessione HTTP/2. È possibile utilizzare la versione del protocollo per inviare richieste alle destinazioni utilizzando HTTP/2. Per ulteriori informazioni, consulta Versione del protocollo. Poiché HTTP/2 utilizza connessioni front-end in modo più efficiente, si potrebbe notare un minor numero di connessioni tra i client e il sistema di bilanciamento del carico. Non è possibile usare la funzione server push di HTTP/2.

L'autenticazione TLS reciproca per Application Load Balancers supporta HTTP/2 sia in modalità passthrough che in modalità di verifica. Per ulteriori informazioni, consulta Autenticazione reciproca con TLS in Application Load Balancer.

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

Attributi del listener

Di seguito sono riportati gli attributi del listener per Application Load Balancers:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert-Serial-Number.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert-Issuer.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert-Sject.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert-Validity.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert-Leaf.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Mtls-Clientcert.

`routing.http.request.x_amzn_tls_version.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Tls-Version.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Consente di modificare il nome dell'intestazione dell'intestazione della richiesta HTTP X-Amzn-Tls-Cipher-Suite.

`routing.http.response.server.enabled`

Consente di consentire o rimuovere l'intestazione del server di risposta HTTP.

`routing.http.response.strict_transport_security.header_value`

Informa i browser che è necessario accedere al sito solo tramite HTTPS e che eventuali tentativi futuri di accedervi tramite HTTP devono essere automaticamente convertiti in HTTPS.

`routing.http.response.access_control_allow_origin.header_value`

Speciifica a quali origini è consentito accedere al server.

`routing.http.response.access_control_allow_methods.header_value`

Restituisce quali metodi HTTP sono consentiti quando si accede al server da un'origine diversa.

`routing.http.response.access_control_allow_headers.header_value`

Speciifica quali intestazioni possono essere utilizzate durante la richiesta.

`routing.http.response.access_control_allow_credentials.header_value`

Indica se il browser deve includere credenziali come i cookie o l'autenticazione quando effettua le richieste.

`routing.http.response.access_control_expose_headers.header_value`

Restituisce le intestazioni che il browser può esporre al client richiedente.

`routing.http.response.access_control_max_age.header_value`

Specifica per quanto tempo i risultati di una richiesta di preflight possono essere memorizzati nella cache, in secondi.

`routing.http.response.content_security_policy.header_value`

Speciifica le restrizioni applicate dal browser per ridurre al minimo il rischio di determinati tipi di minacce alla sicurezza.

`routing.http.response.x_content_type_options.header_value`

Indica se i tipi MIME pubblicizzati nelle intestazioni Content-Type devono essere seguiti e non modificati.

`routing.http.response.x_frame_options.header_value`

Indica se il browser è autorizzato a eseguire il rendering di una pagina in un frame, iframe, embed o oggetto.

Regole dei listener

Ogni ascoltatore ha un'operazione predefinita, nota anche come regola predefinita. La regola predefinita non può essere eliminata ed è sempre eseguita per ultima. È possibile creare regole aggiuntive e consistono in una priorità, una o più operazioni e una o più condizioni. Puoi aggiungere o modificare le regole in qualsiasi momento. Per ulteriori informazioni, consulta Modificare una regola.

Regole predefinite

Le operazioni per la regola predefinita vengono definite al momento della creazione del listener. Le regole predefinite non possono avere condizioni. Se non viene soddisfatta nessuna condizione per qualsiasi regola del listener, viene eseguita l'operazione per la regola predefinita.

Di seguito è riportato un esempio di una regola predefinita come illustrato nella console:

Priority	Conditions (If)	Actions (Then)
Last (default)	*If no other rule applies*	**Forward to target group** • my-targets: 1 (100%) • Group-level stickiness: Off

Priorità regola

Ogni regola ha una priorità. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima. È possibile modificare la priorità di una regola non predefinita in qualsiasi momento. Non è possibile modificare la priorità della regola di default. Per ulteriori informazioni, consulta Aggiornare la priorità delle regole.

Operazioni delle regole

Ogni operazione della regola dispone di un tipo, di una priorità e delle informazioni necessarie per eseguire l'operazione. Per ulteriori informazioni, consulta Tipi di operazioni delle regole.

Condizioni della regola

Ogni condizione della regola ha informazioni su tipo e configurazione. Quando le condizioni di una regola vengono soddisfatte, l'operazione viene eseguita. Per ulteriori informazioni, consulta Tipi di condizioni della regola.

Tipi di operazioni delle regole

I tipi di operazione supportati per una regola dell'ascoltatore sono i seguenti:

`authenticate-cognito`

[Ascoltatori HTTPS] Utilizzare Amazon Cognito per autenticare gli utenti. Per ulteriori informazioni, consulta Autenticazione degli utenti tramite Application Load Balancer.

`authenticate-oidc`

[Listener HTTPS] Utilizzare un provider di identità compatibile con OpenID Connect (OIDC) per autenticare gli utenti.

`fixed-response`

Restituire una risposta HTTP personalizzata. Per ulteriori informazioni, consulta Operazioni con risposta fissa.

`forward`

Inoltrare le richieste verso il gruppo di destinazioni indicato. Per ulteriori informazioni, consulta Operazioni di inoltro.

`redirect`

Reindirizzare le richieste da un URL a un altro. Per ulteriori informazioni, consulta Operazioni di reindirizzamento.

Viene eseguita per prima l'operazione con priorità minore. Ogni regola deve includere esattamente una delle seguenti operazioni: `forward`, `redirect` o `fixed-response` e deve essere l'ultima operazione da eseguire.

Se la versione del protocollo è gRPC o HTTP/2, le uniche operazioni supportate sono le operazioni `forward`.

Operazioni con risposta fissa

È possibile utilizzare le operazioni `fixed-response` per archiviare le richieste client e restituire una risposta HTTP personalizzata. È possibile utilizzare questa operazione per inviare un codice di risposta 2XX, 4XX o 5XX e un messaggio opzionale.

Quando viene eseguita un'operazione `fixed-response`, l'operazione e l'URL del target di reindirizzamento vengono registrate nei log di accesso. Per ulteriori informazioni, consulta Voci dei log di accesso. Il conteggio delle operazioni `fixed-response` avvenute con successo viene segnalato dal parametro `HTTP_Fixed_Response_Count`. Per ulteriori informazioni, consulta Parametri di Application Load Balancer.

Example Esempio di azione a risposta fissa per AWS CLI

Puoi specificare un'operazione quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. Le seguenti operazioni inviano una risposta fissa con il codice di stato specificato e il corpo del messaggio.

```
[
  {
      "Type": "fixed-response",
      "FixedResponseConfig": {
          "StatusCode": "200",
          "ContentType": "text/plain",
          "MessageBody": "Hello world"
      }
  }
]
```

Operazioni di inoltro

È possibile utilizzare le operazioni `forward` per instradare le richieste a uno o più gruppi di destinazioni. Se si specificano più gruppi di destinazioni per un'operazione `forward`, è necessario specificare un peso per ciascun gruppo di destinazioni. Ogni peso del gruppo di destinazioni è un valore compreso tra 0 e 999. Le richieste che corrispondono a una regola del listener con gruppi di destinazioni ponderati vengono distribuite a questi gruppi di destinazioni in base ai rispettivi pesi. Ad esempio, se specifichi due gruppi di destinazioni, ciascuno con un peso di 10, ogni gruppo di destinazioni riceve la metà delle richieste. Se specifichi due gruppi di destinazioni, uno con un peso di 10 e l'altro con un peso di 20, il gruppo di destinazioni con un peso di 20 riceve il doppio delle richieste rispetto all'altro gruppo di destinazioni.

Se si configura una regola per distribuire il traffico tra gruppi target ponderati e uno dei gruppi target è vuoto o contiene solo obiettivi non integri, il sistema di bilanciamento del carico non esegue automaticamente il failover su un gruppo target con obiettivi integri.

Per impostazione predefinita, la configurazione di una regola per distribuire il traffico tra gruppi di destinazioni ponderati non garantisce che le sticky session vengano rispettate. Per garantire che le sticky session siano rispettate, abilitare la persistenza del gruppo di destinazioni per la regola. Quando il load balancer indirizza per la prima volta una richiesta a un gruppo target ponderato, genera un cookie denominato AWSALBTG che codifica le informazioni sul gruppo di destinazione selezionato, crittografa il cookie e include il cookie nella risposta al client. Il client deve includere il cookie ricevuto nelle richieste successive al sistema di bilanciamento del carico. Quando il sistema di bilanciamento del carico riceve una richiesta che corrisponde a una regola con la persistenza del gruppo di destinazioni abilitata e contiene il cookie, la richiesta viene instradata al gruppo di destinazioni specificato nel cookie.

Gli Application Load Balancer non supportano i valori dei cookie codificati con URL.

Con le richieste CORS (cross-origin resource sharing), alcuni browser richiedono a `SameSite=None; Secure` di abilitare la stickness. In questo caso, Elastic Load Balancing genera un secondo cookie AWSALBTGCORS, che include le stesse informazioni dello stickiness cookie originale più questo attributo. `SameSite` I clienti ricevono entrambi i cookie.

Example Esempio di operazione di inoltro con un gruppo di destinazioni

Puoi specificare un'operazione quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente operazione inoltra le richieste al gruppo di destinazioni specificato.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067"
              }
          ]
      }
  }
]
```

Example Esempio di operazione di inoltro con due gruppi di destinazioni ponderati

L'operazione seguente inoltra le richieste ai due gruppi di destinazioni specificati, in base al peso di ciascun gruppo di destinazioni.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
                  "Weight": 10
              },
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                  "Weight": 20
              }
          ]
      }
  }
]
```

Example Esempio di operazione di inoltro con persistenza abilitata

Se si dispone di un'operazione di inoltro con più gruppi di destinazioni e per uno o più gruppi di destinazioni sono abilitate le sessioni permanenti, è necessario abilitare la persistenza del gruppo di destinazioni.

L'operazione seguente inoltra le richieste ai due gruppi di destinazioni specificati, con la persistenza del gruppo di destinazioni abilitata. Le richieste che non contengono il cookie AWSALBTG vengono instradate in base al peso di ciascun gruppo di destinazioni.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
```

```
                "Weight": 10
            },
            {
                "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                "Weight": 20
            }
        ],
        "TargetGroupStickinessConfig": {
            "Enabled": true,
            "DurationSeconds": 1000
        }
    }
  }
]
```

Operazioni di reindirizzamento

È possibile utilizzare le operazioni `redirect` per reindirizzare le richieste client da un URL a un altro. È possibile configurare i reindirizzamenti come temporanei (HTTP 302) o permanenti (HTTP 301) in base alle esigenze.

Un URI è costituito dai componenti seguenti:

```
protocol://hostname:port/path?query
```

È necessario modificare almeno uno dei componenti seguenti per evitare un reindirizzamento loop: protocollo, nome host, porta o percorso. I componenti che non vengono modificati mantengono i loro valori originali.

protocol

Il protocollo (HTTP o HTTPS). È possibile reindirizzare i protocolli HTTP a HTTP, HTTP a HTTPS e HTTPS a HTTPS. Non è possibile reindirizzare i protocolli HTTPS a HTTP.

hostname

Il nome host. Il nome host non prevede la distinzione tra lettere maiuscole e minuscole, può contenere fino a 128 caratteri di lunghezza e può contenere caratteri alfanumerici, caratteri jolly (* e ?) e trattini (-).

port

La porta (da 1 a 65535).

path

Il percorso assoluto, partendo da "/". Il percorso prevede la distinzione tra lettere maiuscole e minuscole, può contenere fino a 128 caratteri di lunghezza e può contenere caratteri alfanumerici, caratteri jolly (* e ?), & (con &) e i seguenti caratteri speciali: _-.$/~"'@:+

query

I parametri di query La lunghezza massima è 128 caratteri.

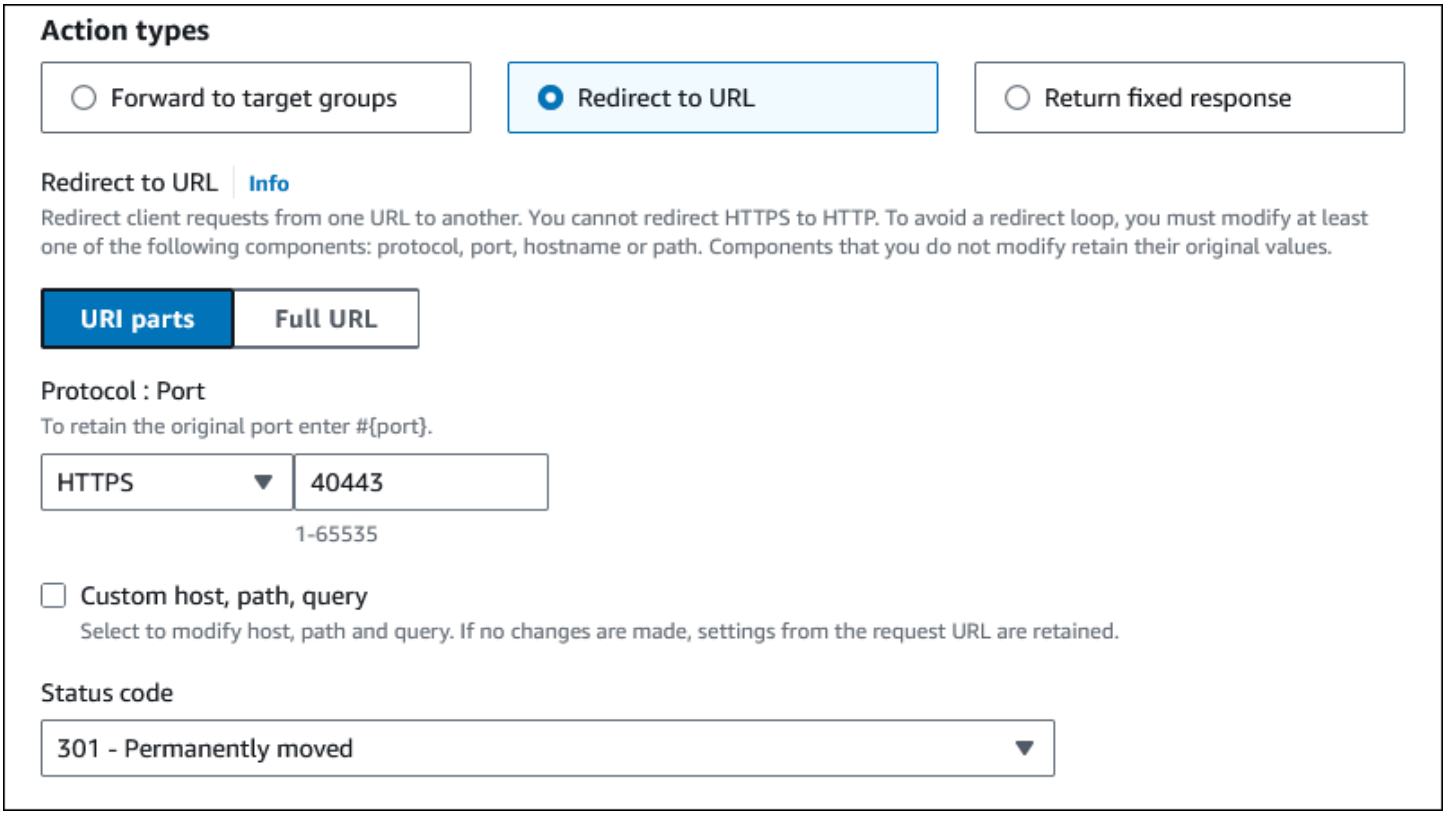
È possibile riutilizzare i componenti URI dell'URL originale nell'URL di destinazione utilizzando le seguenti parole chiave riservate:

- `#{protocol}` - Mantiene il protocollo. Utilizzare nel protocollo e nei componenti query.
- `#{host}` - Mantiene il dominio. Utilizzare nel nome host, nel percorso e nei componenti query.
- `#{port}` - Mantiene la porta. Utilizzare nella porta, nel percorso e nei componenti query.
- `#{path}` - Mantiene il percorso. Utilizzare nel percorso e nei componenti query.
- `#{query}` - Mantiene i parametri di query. Utilizzare nel componente query.

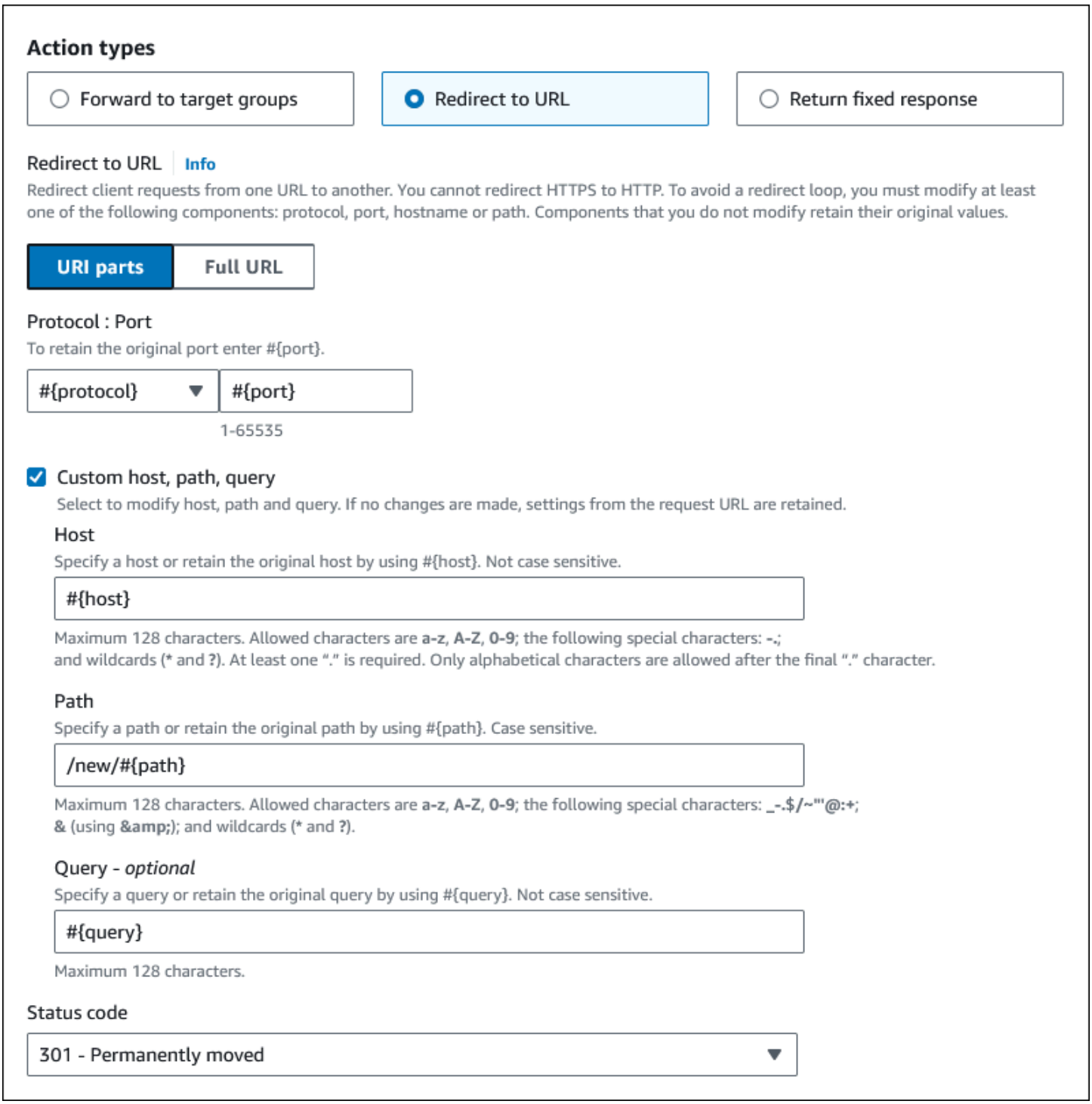
Quando viene eseguita un'operazione `redirect`, l'operazione viene registrata nei log di accesso. Per ulteriori informazioni, consulta Voci dei log di accesso. Il conteggio delle operazioni `redirect` avvenute con successo viene segnalato dal parametro `HTTP_Redirect_Count`. Per ulteriori informazioni, consulta Parametri di Application Load Balancer.

Example Esempio di operazioni di reindirizzamento tramite la console

Ad esempio, la regola seguente consente di configurare un reindirizzamento permanente a un URL che usa il protocollo HTTPS e la porta specificata (40443), ma mantiene il nome host, il percorso e i parametri di query originali. Questa schermata è equivalente a "https://#{host}:40443/#{path}?#{query}".



La regola seguente consente di configurare un reindirizzamento permanente a un URL che mantiene il protocollo, la porta, il nome host e i parametri di query originali e utilizza la parola chiave `#{path}` per creare un percorso modificato. Questa schermata è equivalente a "#{protocol}://#{host}:#{port}/new/#{path}?#{query}".



Example Esempio di azione di reindirizzamento per AWS CLI

Puoi specificare un'operazione quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente azione reindirizza una richiesta HTTP a una richiesta HTTP sulla porta 443, con lo stesso nome host, percorso e stringa di query della richiesta HTTOP:

```
[
  {
      "Type": "redirect",
      "RedirectConfig": {
          "Protocol": "HTTPS",
          "Port": "443",
          "Host": "#{host}",
          "Path": "/#{path}",
          "Query": "#{query}",
          "StatusCode": "HTTP_301"
      }
  }
]
```

Tipi di condizioni della regola

I tipi di operazione supportati per una regola sono i seguenti:

`host-header`

Instradamento basato sul nome host di ogni richiesta. Per ulteriori informazioni, consulta Condizioni host.

`http-header`

Instradamento basato sulle intestazioni HTTP per ogni richiesta. Per ulteriori informazioni, consulta Condizioni nell'intestazione HTTP.

`http-request-method`

Instradamento basato sul metodo della richiesta HTTP di ogni richiesta. Per ulteriori informazioni, consulta Condizioni del metodo di richiesta HTTP.

`path-pattern`

Percorso basato sui modelli di percorso indicati nella richiesta URLs. Per ulteriori informazioni, consulta Condizioni percorso.

`query-string`

Percorso basato su key/value coppie o valori nelle stringhe di query. Per ulteriori informazioni, consulta Condizioni delle stringhe di query.

`source-ip`

Instradamento basato sull'indirizzo IP di origine di ogni richiesta. Per ulteriori informazioni, consulta Condizioni indirizzo IP di origine.

Ogni regola può facoltativamente includere al massimo una delle seguenti condizioni: `host-header`, `http-request-method`, `path-pattern` e `source-ip`. Ogni regola può anche includere facoltativamente una o più delle seguenti condizioni: `http-header` e `query-string`.

Puoi specificare fino a tre valutazioni di corrispondenze per condizione. Ad esempio, per ogni condizione `http-header` è possibile specificare fino a tre stringhe da paragonare al valore dell'intestazione HTTP nella richiesta. La condizione è soddisfatta se una delle stringhe corrisponde al valore dell'intestazione HTTP. Per fare in modo che tutte le stringhe siano una corrispondenza, crea una condizione per valutazione di corrispondenza.

Puoi specificare fino a cinque valutazioni di corrispondenze per regola. Ad esempio, puoi creare una regola con cinque condizioni in cui ogni condizione ha una valutazione di corrispondenza.

Nelel valutazioni di corripondenza è possibile includere caratteri jolly per le condizioni `http-header`,`host-header`, `path-pattern` e `query-string`. Esiste un limite di cinque caratteri jolly per regola.

Le regole vengono applicate solo ai caratteri ASCII visibili; i caratteri di controllo (da 0x00 a 0x1f e 0x7f) sono esclusi.

Per le demo, consulta Instradamento avanzato delle richieste.

Condizioni nell'intestazione HTTP

Puoi usare le condizioni dell'intestazione HTTP per configurare le regole che instradano le richieste in base alle intestazioni HTTP per la richiesta. Puoi specificare i nomi dei campi delle intestazioni HTTP standard o personalizzate. Il nome dell'intestazione e la valutazione della corrispondenza non fanno distinzione tra lettere maiuscole e minuscole. I seguenti caratteri jolly sono supportati nelle stringhe di confronto: * (corrisponde a 0 o a più caratteri) e ? (corrisponde esattamente a 1 carattere). I caratteri jolly non sono supportati nel nome dell'intestazione.

Quando l'attributo Application Load Balancer `routing.http.drop_invalid_header_fields` è abilitato, eliminerà i nomi delle intestazioni che non sono conformi alle espressioni regolari (). `A-Z,a-z,0-9` È inoltre possibile aggiungere nomi di intestazione non conformi alle espressioni regolari.

Example Esempio di condizione di intestazione HTTP per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente condizione è soddisfatta dalle richieste con un'intestazione Utente-Agente che corrisponde a una delle stringhe specificate.

```
[
  {
      "Field": "http-header",
      "HttpHeaderConfig": {
          "HttpHeaderName": "User-Agent",
          "Values": ["*Chrome*", "*Safari*"]
      }
  }
]
```

Condizioni del metodo di richiesta HTTP

Puoi usare le condizioni del metodo di richiesta HTTP per configurare le regole che instradano le richieste in base al metodo di richiesta HTTP della richiesta. Puoi specificare metodi HTTP standard o personalizzati. La valutazione della corrispondenza prevede la distinzione tra lettere maiuscole e minuscole. I caratteri jolly non sono supportati; pertanto, il nome del metodo deve essere una corrispondenza esatta.

Consigliamo di instradare le richieste GET e HEAD nello stesso modo, perché la risposta alla richiesta HEAD può essere inserita nella cache.

Example Esempio di condizione del metodo HTTP per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La condizione seguente è soddisfatta dalle richieste che utilizzano il metodo specificato.

```
[
  {
      "Field": "http-request-method",
      "HttpRequestMethodConfig": {
          "Values": ["CUSTOM-METHOD"]
      }
  }
```

```
]
```

Condizioni host

È possibile utilizzare le condizioni host per definire regole in grado di inoltrare le richieste in base al nome host nell'intestazione host (noto anche come instradamento basato su host). In questo modo è possibile supportare più sottodomini e domini di primo livello diversi utilizzando un singolo sistema di bilanciamento del carico.

Un nome host non distingue tra maiuscole e minuscole, può avere una lunghezza massima di 128 caratteri e contenere qualsiasi carattere tra i seguenti:

- A-Z, a-z, 0-9
- - .
- * (corrisponde a 0 o più caratteri)
- ? (corrisponde esattamente a 1 carattere)

Si deve includere il carattere "." almeno una volta. Dopo l'ultimo carattere "." è possibile includere solo caratteri alfabetici.

Esempio di nomi host

- **`example.com`**
- **`test.example.com`**
- **`*.example.com`**

La regola **`*.example.com`** si applica a **`test.example.com`** ma non a **`example.com`**.

Example Esempio di condizione di intestazione dell'host per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente condizione è soddisfatta dalle richieste con un'intestazione host che corrisponde alla stringa specificata.

```
[
  {
      "Field": "host-header",
      "HostHeaderConfig": {
```

```
          "Values": ["*.example.com"]
      }
  }
]
```

Condizioni percorso

È possibile utilizzare le condizioni percorso per definire regole in grado di inoltrare le richieste in base all'URL nella richiesta (noto anche come instradamento basato su host).

Il modello di percorso viene applicato solo al percorso dell'URL, non ai suoi parametri di query. Viene applicato solo ai caratteri ASCII visibili; i caratteri di controllo (da 0x00 a 0x1f e 0x7f) sono esclusi.

La valutazione della regola viene eseguita solo dopo la normalizzazione dell'URI.

Un modello di percorso non distingue tra maiuscole e minuscole, può avere una lunghezza massima di 128 caratteri e contenere qualsiasi carattere tra i seguenti.

- A-Z, a-z, 0-9
- _ - . $ / ~ " ' @ : +
- & (utilizzo di &)
- * (corrisponde a 0 o più caratteri)
- ? (corrisponde esattamente a 1 carattere)

Se la versione del protocollo è gRPC, le condizioni possono essere specifiche per un pacchetto, un servizio o un metodo.

Esempio di modelli di percorso HTTP

- `/img/*`
- `/img/*/pics`

Esempio di modelli di percorso gRPC

- /package
- /package.service
- /package.service/method

Il modello di percorso viene utilizzato per instradare le richieste, ma non le modifica. Ad esempio, se una regola ha un modello di percorso `/img/*`, la regola inoltra una richiesta per `/img/picture.jpg` al gruppo target specificato come una richiesta per `/img/picture.jpg`.

Example Esempio di condizione del modello di percorso per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente condizione è soddisfatta dalle richieste con un URL che contiene la stringa specificata.

```
[
  {
      "Field": "path-pattern",
      "PathPatternConfig": {
          "Values": ["/img/*"]
      }
  }
]
```

Condizioni delle stringhe di query

È possibile utilizzare le condizioni della stringa di query per configurare le regole che instradano le richieste in base a key/value coppie o valori nella stringa di query. La valutazione della corrispondenza non prevede la distinzione tra lettere maiuscole e minuscole. I seguenti caratteri jolly sono supportati: * (corrisponde a 0 o a più caratteri) e ? (corrisponde esattamente a 1 carattere).

Example Esempio di condizione della stringa di query per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente condizione è soddisfatta dalle richieste con una stringa di query che include una key/value coppia di «version=v1" o qualsiasi chiave impostata su «example».

```
[
  {
      "Field": "query-string",
      "QueryStringConfig": {
          "Values": [
            {
                "Key": "version",
                "Value": "v1"
```

```
            },
            {
                "Value": "*example*"
            }
          ]
      }
  }
]
```

Condizioni indirizzo IP di origine

Puoi usare le condizioni dell'indirizzo IP di origine per configurare le regole che instradano le richieste in base all'indirizzo IP di origine della richiesta. L'indirizzo IP deve essere in formato CIDR. È possibile utilizzare entrambi gli indirizzi. IPv4 IPv6 I caratteri jolly non sono supportati. Non è possibile specificare il CIDR `255.255.255.255/32` come condizione della regola dell'IP di origine.

Se un client è al di là di un proxy, si tratta dell'indirizzo IP del proxy, non dell'indirizzo IP del client.

Questa condizione non è soddisfatta dagli indirizzi nell' X-Forwarded-Forintestazione. Per cercare gli indirizzi nell' X-Forwarded-Forintestazione, utilizza una `http-header` condizione.

Example Esempio di condizione IP di origine per AWS CLI

Puoi specificare le condizioni quando crei o modifichi una regola. Per ulteriori informazioni consulta i comandi create-rule e modify-rule. La seguente condizione è soddisfatta dalle richieste con un indirizzo IP di origine in uno dei blocchi CIDR specificati.

```
[
  {
      "Field": "source-ip",
      "SourceIpConfig": {
          "Values": ["192.0.2.0/24", "198.51.100.10/32"]
      }
  }
]
```

Intestazioni HTTP e Application Load Balancer

Le richieste e le risposte HTTP utilizzano i campi intestazione per inviare informazioni sui messaggi HTTP. Le intestazioni HTTP vengono aggiunte automaticamente. I campi intestazione sono costituti

da coppie nome-valore separati da due punti e intervallati da un ritorno a capo e un avanzamento riga. Un insieme standard di campi dell'intestazione HTTP è definito nella RFC 2616 intestazioni di messaggi. Sono anche disponibili intestazioni HTTP non standard che vengono aggiunte automaticamente e sono ampiamente utilizzate dalle applicazioni. Alcune delle intestazioni HTTP non standard hanno un prefisso `X-Forwarded`. Gli Application Load Balancer supportano le seguenti intestazioni `X-Forwarded`.

Per ulteriori informazioni sulle connessioni HTTP, consulta Routing della richiesta nella Guida per l'utente di Elastic Load Balancing.

Intestazioni X-Forwarded

- X-Forwarded-For
- X-Forwarded-Proto
- X-Forwarded-Port

X-Forwarded-For

L'intestazione della richiesta `X-Forwarded-For` consente di identificare l'indirizzo IP di un client quando utilizzi un sistema di bilanciamento del carico HTTP o HTTPS. Poiché i sistemi di bilanciamento del carico intercettano il traffico tra client e server, i log di accesso al server contengono solo l'indirizzo IP del sistema di bilanciamento del carico. Per visualizzare l'indirizzo IP del client, utilizza l'attributo `routing.http.xff_header_processing.mode`. Questo attributo consente di modificare, mantenere o rimuovere l'intestazione `X-Forwarded-For` nella richiesta HTTP prima che Application Load Balancer la invii alla destinazione. I valori possibili per questo attributo sono `append`, `preserve` e `remove`. Il valore predefinito per questo attributo è `append`.

> **Important**
>
> L'`X-Forwarded-For`intestazione deve essere utilizzata con cautela a causa dei potenziali rischi per la sicurezza. Le voci possono essere considerate affidabili solo se aggiunte da sistemi adeguatamente protetti all'interno della rete.

Append

Per impostazione predefinita, Application Load Balancer memorizza l'indirizzo IP del client nell'intestazione della richiesta `X-Forwarded-For` e passa l'intestazione al server. Se l'intestazione

della richiesta `X-Forwarded-For` non è inclusa nella richiesta originale, il sistema di bilanciamento del carico ne crea una con l'indirizzo IP del client come valore della richiesta. Altrimenti, il load balancer aggiunge l'indirizzo IP del client all'intestazione esistente e quindi passa l'intestazione al server. L'intestazione della richiesta `X-Forwarded-For` può contenere più indirizzi IP separati da virgole.

L'intestazione della richiesta `X-Forwarded-For` assume la seguente forma:

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

Di seguito è riportata un'intestazione della richiesta `X-Forwarded-For` di esempio per un client con l'indirizzo IP `203.0.113.7`.

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

Di seguito è riportato un esempio di intestazione di `X-Forwarded-For` richiesta per un client con un indirizzo di. IPv6 `2001:DB8::21f:5bff:febf:ce22:8a2e`

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

Quando l'attributo di conservazione della porta del client (`routing.http.xff_client_port.enabled`) è abilitato nel sistema di bilanciamento del carico, l'intestazione della richiesta `X-Forwarded-For` include il `client-port-number` aggiunto al `client-ip-address`, separato da due punti. L'intestazione assume così la seguente forma:

```
IPv4 -- X-Forwarded-For: client-ip-address:client-port-number
```

```
IPv6 -- X-Forwarded-For: [client-ip-address]:client-port-number
```

Si noti IPv6 infatti che quando il sistema di bilanciamento del carico aggiunge il `client-ip-address` all'intestazione esistente, racchiude l'indirizzo tra parentesi quadre.

Di seguito è riportato un esempio di intestazione di `X-Forwarded-For` richiesta per un client con un IPv4 indirizzo e un numero di porta di. `12.34.56.78` `8080`

```
X-Forwarded-For: 12.34.56.78:8080
```

Di seguito è riportato un esempio di intestazione di `X-Forwarded-For` richiesta per un client con un IPv6 indirizzo `2001:db8:85a3:8d3:1319:8a2e:370:7348` e un numero di porta di. `8080`

```
X-Forwarded-For: [2001:db8:85a3:8d3:1319:8a2e:370:7348]:8080
```

Preserve

La modalità `preserve` nell'attributo garantisce che l'intestazione `X-Forwarded-For` nella richiesta HTTP non venga modificato in alcun modo prima di essere inviata alle destinazioni.

Rimuovi

La modalità `remove` nell'attributo rimuove l'intestazione `X-Forwarded-For` nella richiesta HTTP prima di inviarla alle destinazioni.

> **Note**
>
> Se si abilita l'attributo di conservazione della porta del client (`routing.http.xff_client_port.enabled`) e inoltre si seleziona `preserve` o `remove` per l'attributo `routing.http.xff_header_processing.mode`, l'Application Load Balancer sovrascrive l'attributo di conservazione della porta del client. Mantiene l'intestazione `X-Forwarded-For` invariata o la rimuove, a seconda della modalità selezionata, prima di inviarla alle destinazioni.

La tabella seguente mostra esempi dell'intestazione `X-Forwarded-For` che la destinazione riceve quando si seleziona la modalità `append`, `preserve` o `remove`. In questo esempio, l'indirizzo IP dell'ultimo hop è `127.0.0.1`.

Descrizione della richiesta	Richiesta di esempio	XFF con modalità **append**	XFF con modalità **preserve**	XFF con modalità **remove**
La richiesta viene inviata senza intestazione XFF	`GET / index.html HTTP/1.1 Host: example.com`	`X-Forwarded-For: 127.0.0.1`	Non presente	Non presente

Descrizione della richiesta	Richiesta di esempio	XFF con modalità **append**	XFF con modalità **preserve**	XFF con modalità **remove**
La richiesta viene inviata con un'intestazione XFF e un indirizzo IP client.	`GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4`	`X-Forwarded-For: 127.0.0.4, 127.0.0.1`	`X-Forwarded-For: 127.0.0.4`	Non presente
La richiesta viene inviata con un'intestazione XFF con più indirizzi IP client.	`GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4, 127.0.0.8`	`X-Forwarded-For: 127.0.0.4, 127.0.0.8, 127.0.0.1`	`X-Forwarded-For: 127.0.0.4, 127.0.0.8`	Non presente

Per modificare, conservare o rimuovere l'intestazione X-Forwarded-For tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Attributi, scegli Modifica.
5. Nella sezione Configurazione del traffico, in Gestione dei pacchetti, per l'X-Forwarded-For intestazione scegli Aggiungi (impostazione predefinita), Conserva o Rimuovi.
6. Scegli Save changes (Salva modifiche).

Per modificare, conservare o rimuovere l'intestazione utilizzando il X-Forwarded-ForAWS CLI

Utilizzate il modify-load-balancer-attributescomando con l'`routing.http.xff_header_processing.mode`attributo.

X-Forwarded-Proto

L'intestazione della richiesta `X-Forwarded-Proto` consente di identificare il protocollo (HTTP o HTTPS) utilizzato da un client per connettersi al tuo load balancer. I log di accesso al server contengono solo il protocollo utilizzato tra il server e il load balancer; non contengono informazioni sul protocollo utilizzato tra il client e il load balancer. Per determinare il protocollo utilizzato tra il client e il load balancer, utilizzare l'intestazione della richiesta `X-Forwarded-Proto`. Elastic Load Balancing archivia il protocollo utilizzato tra il client e il load balancer nell'intestazione della richiesta `X-Forwarded-Proto` e passa l'intestazione al server.

La tua applicazione o il tuo sito Web può utilizzare il protocollo memorizzato nell'intestazione della richiesta `X-Forwarded-Proto` per eseguire il rendering di una risposta che reindirizza all'URL appropriato.

L'intestazione della richiesta `X-Forwarded-Proto` assume la seguente forma:

```
X-Forwarded-Proto: originatingProtocol
```

L'esempio seguente contiene un'intestazione della richiesta `X-Forwarded-Proto` per una richiesta originata dal client come richiesta HTTPS:

```
X-Forwarded-Proto: https
```

X-Forwarded-Port

L'intestazione della richiesta `X-Forwarded-Port` consente di identificare la porta di destinazione utilizzata dal client per connettersi al load balancer.

Creazione di un ascoltatore HTTP per Application Load Balancer

Un ascoltatore 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.

L'informazione in questa pagina consente di creare un listener HTTP per il sistema di bilanciamento del carico. Per aggiungere un listener HTTPS al sistema di bilanciamento del carico, consulta Creazione di un ascoltatore HTTPS per Application Load Balancer.

Prerequisiti

- Per aggiungere un'operazione di inoltro alla regola predefinita del listener, è necessario specificare un gruppo target disponibile. Per ulteriori informazioni, consulta Crea un gruppo target per il tuo Application Load Balancer.
- È possibile specificare lo stesso gruppo di destinazioni in più ascoltatori, che però devono appartenere allo stesso sistema di bilanciamento del carico. Per utilizzare un gruppo di destinazioni con un sistema di bilanciamento del carico, è necessario verificare non sia utilizzato da un ascoltatore per nessun altro sistema di bilanciamento del carico.

Aggiunta di un ascoltatore HTTP

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.

Aggiunta di un listener HTTP mediante la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, scegli Aggiungi ascoltatore.
5. In Protocollo : Porta, seleziona HTTP e usare la porta predefinita o inserire una porta diversa.
6. Per Operazioni predefinite, scegli una delle seguenti opzioni:

    - Inoltra a gruppi di destinazione: scegliere uno o più gruppi di destinazione a cui inoltrare il traffico. Per aggiungere gruppi di destinazione, scegli Aggiungi gruppo di destinazioni. Se si utilizza più di un gruppo di destinazioni, seleziona un peso per ogni gruppo e controllare la percentuale associata. Se è stata abilitata la persistenza per uno o più gruppi di destinazioni, è necessario abilitare la persistenza a livello di gruppo per una regola.
    - Reindirizza a URL: specificare l'URL verso cui verranno reindirizzate le richieste del client. È possibile farlo inserendo ogni parte separatamente nella scheda Parti URI, oppure inserendo

l'indirizzo completo nella scheda URL completo. Per Codice di stato, è possibile configurare i reindirizzamenti come temporanei (HTTP 302) o permanenti (HTTP 301) in base alle esigenze.

- Restituisci risposta fissa: specificare il Codice di risposta che verrà restituito alle richieste interrotte del client. Inoltre, è possibile specificare il Tipo di contenuto e il Corpo della risposta, ma non sono richiesti.

7. Scegliere Aggiungi.

Per aggiungere un listener HTTP utilizzando AWS CLI

Utilizzare il comando create-listener per creare il listener e la regola predefinita e il comando create-rule per definire regole di listener aggiuntive.

Certificati SSL per il tuo Application Load Balancer

Quando crei un listener sicuro per il tuo Application Load Balancer, devi distribuire almeno un certificato sul load balancer. Il sistema di bilanciamento del carico utilizza un certificato X.509 (certificati server SSL/TLS). 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 Richiedere un certificato pubblico nella Guida per l'utente.AWS Certificate Manager

Consigliamo di creare o importare certificati per il sistema di bilanciamento del carico utilizzando AWS Certificate Manager (ACM). Questa versione supporta certificati RSA con lunghezze di chiave 2048, 3072 e 4096 bit e tutti i certificati ECDSA. ACM si integra con Elastic Load Balancing in modo da poter implementare il certificato sul load balancer. Per ulteriori informazioni, consulta la AWS Certificate Manager Guida per l'utente di .

In alternativa, puoi utilizzare SSL/TLS gli strumenti 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 AWS Identity and Access Management (IAM). Per ulteriori informazioni sull'importazione di certificati in ACM, consulta Importazione di certificati nella Guida per l'utente di AWS Certificate Manager . Per ulteriori informazioni sul caricamento dei certificati in IAM, consulta Utilizzo dei certificati del server nella Guida per l'utente di IAM.

Certificato predefinito

È necessario specificare un certificato predefinito al momento della creazione di un listener HTTPS. Questo certificato è noto come certificato predefinito. Puoi sostituire il certificato predefinito dopo aver creato il listener HTTPS. 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

Dopo aver creato un listener HTTPS, puoi aggiungere certificati all'elenco dei certificati. Se hai creato il listener utilizzando il AWS Management Console, abbiamo aggiunto il certificato predefinito all'elenco dei certificati per te. Altrimenti, l'elenco dei certificati è vuoto. 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 chiave pubblica (preferire ECDSA su RSA)
- Scadenza (preferisco non scaduto)
- Algoritmo di hashing (preferire SHA a). MD5 Se sono presenti più certificati SHA, preferisci il numero SHA più alto.
- 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.

Politiche di sicurezza per il tuo Application Load Balancer

Elastic Load Balancing utilizza una configurazione di negoziazione Secure Socket Layer (SSL), nota come policy di sicurezza, per negoziare le connessioni SSL tra un client e il load balancer. 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. Per impostazione predefinita, la prima crittografia nell'elenco del server che corrisponde a una qualsiasi delle crittografie del client viene selezionata per la connessione sicura.

Considerazioni

- Gli Application Load Balancer supportano la rinegoziazione SSL solo per le connessioni di destinazione.
- Quando si crea un ascoltatore HTTPS, è necessario selezionare una policy di sicurezza.
- La `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` politica è la politica di sicurezza predefinita per i listener HTTPS creati utilizzando. AWS Management Console Questa politica supporta TLS 1.3 ed è retrocompatibile con TLS 1.2.
- La `ELBSecurityPolicy-2016-08` politica è la politica di sicurezza predefinita per i listener HTTPS creata utilizzando. AWS CLI
- Gli Application Load Balancer non supportano policy di sicurezza personalizzate.
- È possibile scegliere la politica di sicurezza utilizzata per le connessioni front-end, ma non per le connessioni backend.
  - Per le connessioni di backend, se uno dei listener HTTPS utilizza una politica di sicurezza TLS 1.3, viene utilizzata la politica di sicurezza. `ELBSecurityPolicy-TLS13-1-0-2021-06` In caso contrario, per le connessioni di back-end viene utilizzata la policy di sicurezza `ELBSecurityPolicy-2016-08`.
  - Nota: se si utilizza una politica FIPS TLS sul listener HTTPS, viene utilizzata per le connessioni di backend. `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
- 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-` Per

visualizzare la versione del protocollo TLS per le richieste all'Application Load Balancer, abilita la registrazione degli accessi per il tuo load balancer ed esamina le voci del registro di accesso corrispondenti. Per ulteriori informazioni, consulta Access logs for your Application 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 nelle tue policy IAM e service control (SCPs), rispettivamente. Per ulteriori informazioni, consulta Service control policies (SCPs) nella Guida per l'AWS Organizations utente
- Le politiche che supportano solo TLS 1.3 supportano Forward Secrecy (FS). Le politiche che supportano TLS 1.3 e TLS 1.2 che hanno solo cifrari del formato TLS_* ed ECDHE_* forniscono anche FS.
- Gli Application Load Balancer supportano la ripresa del TLS utilizzando PSK (TLS 1.3) e ticket di sessione (TLS 1.2 e versioni precedenti). IDs/session Le riprese sono supportate solo nelle connessioni allo stesso indirizzo IP di Application Load Balancer. La funzionalità 0-RTT Data e l'estensione early_data non sono implementate.
- Gli Application Load Balancer supportano l'estensione Extended Master Secret (EMS) per TLS 1.2.

È possibile descrivere i protocolli e i codici utilizzando il describe-ssl-policies AWS CLI comando o fare riferimento alle tabelle seguenti.

Policy di sicurezza

- Policy di sicurezza TLS
  - Protocolli per politica
  - Cifre per politica
  - Politiche per codice
- Politiche di sicurezza FIPS
  - Protocolli per politica
  - Cifre per politica
  - Politiche per codice
- Policy FS supportate
  - Protocolli per politica
  - Cifre per politica
  - Politiche per codice

Policy di sicurezza TLS

È possibile utilizzare le politiche di sicurezza TLS 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.

Le politiche che supportano solo TLS 1.3 supportano Forward Secrecy (FS). Le politiche che supportano TLS 1.3 e TLS 1.2 che hanno solo cifrari del formato TLS_* ed ECDHE_* forniscono anche FS.

Indice

Protocolli per politica

La tabella seguente descrive i protocolli supportati da ogni policy di sicurezza TLS.

Policy di sicurezza	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitica- -1-3-2021-06 TLS13	Sì	No	No	No
ELBSecurityPolitica- TLS13 -1-2-2021-06	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-Res-2021-06	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-Ext2-2021-06	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-Ext1-2021-06	Sì	Sì	No	No

Policy di sicurezza	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitica- TLS13 -1-1-2021-06	Sì	Sì	Sì	No
ELBSecurityPolitica- TLS13 -1-0-2021-06	Sì	Sì	Sì	Sì
ELBSecurityPolitica-TLS-1-2-EXT-2018-06	No	Sì	No	No
ELBSecurityPolitica-TLS-1-2-2017-01	No	Sì	No	No
ELBSecurityPolitica-TLS-1-1-2017-01	No	Sì	Sì	No
ELBSecurityPolitica - 2016-08	No	Sì	Sì	Sì
ELBSecurityPolitica - 2015-05	No	Sì	Sì	Sì

Cifre per politica

La tabella seguente descrive i codici supportati da ogni politica di sicurezza TLS.

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-3-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256
ELBSecurityPolitica- TLS13 -1-2-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256

Policy di sicurezza	Crittografie
	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityPolitica- -1-2-Res-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384

Policy di sicurezza	Crittografie
ELBSecurityPolitica- TLS13 -1-2-Ext2-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-2-Ext1-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-1-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-0-2021-06 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica-TLS-1-2-EXT-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica-TLS-1-2-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Policy di sicurezza	Crittografie
ELBSecurityPolitica-TLS-1-1-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica - 2016-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica - 2015-05	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- AES256 -SHA • ECDH-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politiche per codice

La tabella seguente descrive le politiche di sicurezza TLS che supportano ogni cifrario.

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — TLS_AES_128_GCM_ SHA256 IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-3-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-2021 -06	1301

Nome del cifrario	Policy di sicurezza	Suite di cifratura
	• ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06	
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-3-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06	1302

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 IANA — TLS_ CHACHA2 POLY13 0_05_ SHA256	• ELBSecurityPolitica- TLS13 -1-3-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res- 2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06	1303

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c02b

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-RSA-AESOpenSSL — 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH _AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c02f

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c023

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-RSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c-027
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c009

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c-013
ECDHE-ECDSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WI TH_AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c02c

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-RSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c030

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c-024

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-2021 -06 • ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c-028
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c00a

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	c014
AES128OpenSSL — -GCM- SHA256 IANA — TLS_RSA_CON_AES_12 8_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	9c

Nome del cifrario	Policy di sicurezza	Suite di cifratura
AES128OpenSSL — - SHA256 IANA — TLS_RSA_CON_AES_128_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	3c
AES128OpenSSL — -SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	2f

Nome del cifrario	Policy di sicurezza	Suite di cifratura
AES256OpenSSL — -GCM- SHA384 IANA — TLS_RSA_CON_AES_25 6_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2- EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	9d
AES256OpenSSL — - SHA256 IANA — TLS_RSA_WITH_AES_2 56_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-2-Ext1 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2- EXT-2018-06 • ELBSecurityPolitica-TLS-1-2-2017-01 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	3d

Nome del cifrario	Policy di sicurezza	Suite di cifratura
AES256OpenSSL — -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -2021-06 • ELBSecurityPolitica- TLS13 -1-1-2021 -06 • ELBSecurityPolitica- TLS13 -1-0-2021 -06 • ELBSecurityPolitica-TLS-1-2-EXT-2018-06 • ELBSecurityPolitica-TLS-1-1-2017-01 • ELBSecurityPolitica - 2016-08	35

Politiche di sicurezza FIPS

> **Important**
>
> Tutti i listener sicuri collegati a un Application Load Balancer devono utilizzare policy di sicurezza FIPS o policy di sicurezza non FIPS; non possono essere combinate. Se un Application Load Balancer esistente ha due o più listener che utilizzano policy non FIPS e desideri che i listener utilizzino invece policy di sicurezza FIPS, rimuovi tutti i listener finché non ce n'è uno solo. Modificate la politica di sicurezza del listener in FIPS, quindi create listener aggiuntivi utilizzando le politiche di sicurezza FIPS. In alternativa, è possibile creare un nuovo Application Load Balancer con nuovi listener utilizzando solo le policy 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.

> **Important**
>
> Le politiche `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` e sono fornite solo per la compatibilità con `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` le versioni precedenti. Sebbene utilizzino la crittografia FIPS utilizzando il modulo FIPS14 0, potrebbero non essere conformi alle ultime linee guida NIST per la configurazione TLS.

Indice

Protocolli per politica

La tabella seguente descrive i protocolli supportati da ogni politica di sicurezza FIPS.

Policy di sicurezza	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitica- -1-3-FIPS-2023-04 TLS13	Sì	No	No	No
ELBSecurityPolitica- TLS13 -1-2-FIPS-2023-04	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-res-FIPS-2023-04	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-EXT2-FIPS-2023-04	Sì	Sì	No	No

Policy di sicurezza	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04	Sì	Sì	No	No
ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04	Sì	Sì	Sì	No
ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	Sì	Sì	Sì	Sì

Cifre per politica

La tabella seguente descrive i codici supportati da ogni politica di sicurezza FIPS.

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-3-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384
ELBSecurityPolitica- -1-2-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-2-RES-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384
ELBSecurityPolitica- TLS13 -1-2-EXT2-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-2-ext1-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256
ELBSecurityPolitica- -1-2-Ext0-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-1-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica- -1-0-FIPS-2023-04 TLS13	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politiche per codice

La tabella seguente descrive le politiche di sicurezza FIPS che supportano ogni cifrario.

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-3-FIPS -2023-04	1301

Nome del cifrario	Policy di sicurezza	Suite di cifratura
IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-res-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-3-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-res-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	1302

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c02b
ECDHE-RSA-AESOpenSSL — 128-GCM- SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c02f

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	c023
ECDHE-RSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	c027

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c009
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c013

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c02c
ECDHE-RSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c030

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	c024
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	c028

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c00a
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext0-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	c014
AES128OpenSSL — -GCM- SHA256 IANA — TLS_RSA_CON_AES_128_GCM_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS-2023-04	9 c

Nome del cifrario	Policy di sicurezza	Suite di cifratura
AES128OpenSSL — - SHA256 IANA — TLS_RSA_CON_AES_12 8_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1- FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	3c
AES128OpenSSL — -SHA IANA — TLS_RSA_WITH_AES_1 28_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	2 f
AES256OpenSSL — -GCM- SHA384 IANA — TLS_RSA_CON_AES_25 6_GCM_ SHA384	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1- FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	9d

Nome del cifrario	Policy di sicurezza	Suite di cifratura
AES256OpenSSL — - SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-2-ext1-FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	3d
AES256OpenSSL — -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica- TLS13 -1-2-Ext2 -FIPS-2023-04 • ELBSecurityPolitica- TLS13 -1-1-FIPS -2023-04 • ELBSecurityPolitica- TLS13 -1-0-FIPS -2023-04	35

Policy FS supportate

Le politiche di sicurezza supportate da FS (Forward Secrecy) forniscono ulteriori garanzie contro l'intercettazione di dati crittografati, attraverso l'uso di una chiave di sessione casuale unica. Ciò impedisce la decodifica dei dati acquisiti, anche se la chiave segreta a lungo termine è compromessa.

Le politiche in questa sezione supportano FS e «FS» è incluso nei loro nomi. Tuttavia, queste non sono le uniche politiche che supportano FS. Le politiche che supportano solo TLS 1.3 supportano FS. Le politiche che supportano TLS 1.3 e TLS 1.2 che hanno solo cifrari del formato TLS_* ed ECDHE_* forniscono anche FS.

Indice

Protocolli per politica

La tabella seguente descrive i protocolli supportati da ogni policy di sicurezza supportata da FS.

Policy di sicurezza	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-FS-1-2-res-2020-10	No	Sì	No	No
ELBSecurityPolitica-FS-1-2-res-2019-08	No	Sì	No	No
ELBSecurityPolitica-FS-1-2-2019-08	No	Sì	No	No
ELBSecurityPolitica-FS-1-1-2019-08	No	Sì	Sì	No
ELBSecurityPolitica-FS-2018-06	No	Sì	Sì	Sì

Cifre per politica

La tabella seguente descrive i codici supportati da ogni politica di sicurezza supportata da FS.

Policy di sicurezza	Crittografie
ELBSecurityPolicy-FS-1-2-res-2020-10	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384
ELBSecurityPolitica-FS-1-2-RES-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256

Policy di sicurezza	Crittografie
	• ECDHE-ECDSA- -GCM AES256 - SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityPolitica-FS-1-2-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA
ELBSecurityPolitica-FS-1-1-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA

Policy di sicurezza	Crittografie
ELBSecurityPolitica-FS-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDH-RSA- AES128 -GCM- SHA256 • ECDHE-ECSA AES128 - - SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- AES128 -SHA • ECDH-RSA- -SHA AES128 • ECDHE-ECDSA- AES256 -GCM- SHA384 • ECDH-RSA- AES256 -GCM- SHA384 • ECDHE-ECSA AES256 - - SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- AES256 -SHA • ECDHE-ECDSA- AES256 -SHA

Politiche per codice

La tabella seguente descrive le politiche di sicurezza supportate da FS che supportano ogni cifrario.

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 128-GCM- SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitica-FS-1-2-RES-2020-10 • ELBSecurityPolitica-FS-1-2-res-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c02b
ECDHE-RSA-AESOpenSSL — 128-GCM- SHA256	• ELBSecurityPolitica-FS-1-2-RES-2020-10	c02f

Nome del cifrario	Policy di sicurezza	Suite di cifratura
IANA — TLS_ECDHE_RSA_WITH _AES_128_GCM_ SHA256	• ELBSecurityPolitica-FS-1-2-res-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	
ECDHE-ECDSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_ SHA256	• ELBSecurityPolitica-FS-1-2-RES-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c023
ECDHE-RSA-AESOpenSSL — 128-SHA256 IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_ SHA256	• ELBSecurityPolitica-FS-1-2-RES-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c027
OpenSSL — ECDHE-ECDSA-AES 128-SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_SHA	• ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c009
OpenSSL — ECDHE-RSA-AES 128-SHA IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_SHA	• ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c013

Nome del cifrario	Policy di sicurezza	Suite di cifratura
ECDHE-ECDSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitica-FS-1-2-RES-2020-10 • ELBSecurityPolitica-FS-1-2-res-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c02c
ECDHE-RSA-AESOpenSSL — 256-GCM- SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitica-FS-1-2-RES-2020-10 • ELBSecurityPolitica-FS-1-2-res-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c030
ECDHE-ECDSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitica-FS-1-2-RES-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c024
ECDHE-RSA-AESOpenSSL — 256-SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitica-FS-1-2-RES-2019-08 • ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c028

Nome del cifrario	Policy di sicurezza	Suite di cifratura
OpenSSL — ECDHE-ECDSA-AES 256-SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c00a
OpenSSL — ECDHE-RSA-AES 256-SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitica-FS-1-2-2019-08 • ELBSecurityPolitica-FS-1-1-2019-08 • ELBSecurityPolitica-FS-2018-06	c014

Creazione di un ascoltatore HTTPS per Application Load Balancer

Un ascoltatore 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.

Per creare un listener HTTPS, è necessario distribuire almeno un certificato del server SSL 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 alle destinazioni. È inoltre necessario specificare una politica di sicurezza, che viene utilizzata per negoziare connessioni sicure tra i client e il sistema di bilanciamento del carico.

Se è necessario passare traffico crittografato alle destinazioni senza una decrittazione da parte del sistema di bilanciamento del carico, è possibile creare un Network Load Balancer o un Classic Load Balancer con un ascoltatore TCP sulla porta 443. Con un ascoltatore TCP, il sistema di bilanciamento del carico passa il traffico crittografato alle destinazioni senza decrittarlo.

L'informazione in questa pagina consente di creare un listener HTTPS per il sistema di bilanciamento del carico. Per aggiungere un listener HTTP al sistema di bilanciamento del carico consulta Creazione di un ascoltatore HTTP per Application Load Balancer.

Prerequisiti

- Per creare un listener HTTPS, è necessario specificare un certificato e una policy di sicurezza. 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. Il sistema di bilanciamento del carico utilizza la policy di sicurezza durante le negoziazioni delle connessioni SSL con i client.

  Gli Application Load Balancer non supportano le chiavi. ED25519
- Per aggiungere un'operazione di inoltro alla regola predefinita del listener, è necessario specificare un gruppo target disponibile. Per ulteriori informazioni, consulta Crea un gruppo target per il tuo Application Load Balancer.
- È possibile specificare lo stesso gruppo di destinazioni in più ascoltatori, che però devono appartenere allo stesso sistema di bilanciamento del carico. Per utilizzare un gruppo di destinazioni con un sistema di bilanciamento del carico, è necessario verificare non sia utilizzato da un ascoltatore per nessun altro sistema di bilanciamento del carico.

Aggiunta di un ascoltatore HTTPS

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.

Aggiunta di un listener HTTPS mediante la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, scegli Aggiungi ascoltatore.
5. In Protocollo : Porta, seleziona HTTPS e usare la porta predefinita o inserire una porta diversa.
6. (Facoltativo) Per abilitare l'autenticazione, in Autenticazione seleziona Usa OpenID o Amazon Cognito e indica le informazioni richieste. Per ulteriori informazioni, consulta Autenticazione degli utenti tramite Application Load Balancer.
7. Per le azioni di routing, esegui una delle seguenti operazioni:

- Inoltra ai gruppi target: scegli i gruppi target a cui inoltrare il traffico. Per aggiungere gruppi di destinazione, scegli Aggiungi gruppo di destinazioni. Se si utilizza più di un gruppo di destinazioni, seleziona un peso per ogni gruppo e controllare la percentuale associata. Se è stata abilitata la persistenza per uno o più gruppi di destinazioni, è necessario abilitare la persistenza a livello di gruppo per una regola.
- Reindirizza all'URL: inserisci l'URL a cui verranno reindirizzate le richieste del cliente. È possibile farlo inserendo ogni parte separatamente nella scheda Parti URI, oppure inserendo l'indirizzo completo nella scheda URL completo. Per Codice di stato, è possibile configurare i reindirizzamenti come temporanei (HTTP 302) o permanenti (HTTP 301) in base alle esigenze.
- Restituisci una risposta fissa: inserisci il codice di risposta per tornare alle richieste dei client abbandonate. Facoltativamente, puoi specificare il tipo di contenuto e il corpo della risposta.

8. Come Policy di sicurezza, consigliamo di utilizzare sempre la policy di sicurezza predefinita più recente.
9. Per SSL/TLS Certificato predefinito, scegli il certificato predefinito. Aggiungiamo anche il certificato predefinito all'elenco SNI. Puoi selezionare il certificato da una delle seguenti fonti:

   - Se hai creato o importato un certificato utilizzando AWS Certificate Manager, scegli Da ACM, quindi scegli il certificato da Certificato (da ACM).
   - Se hai importato un certificato utilizzando IAM, scegli Da IAM, quindi scegli il certificato da Certificate (da IAM).
   - Se hai un certificato, scegli Importa certificato. Scegli Importa in ACM o Importa in IAM. Per la chiave privata del certificato, copia e incolla il contenuto del file della chiave privata (con codifica PEM). Per Certificate Body, copia e incolla il contenuto del file di certificato a chiave pubblica (con codifica PEM). Per Certificate Chain, copia e incolla il contenuto del file della catena del certificato (con codifica PEM), a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.

10. (Facoltativo) Per abilitare l'autenticazione reciproca, in Gestione dei certificati Client, abilita l'autenticazione reciproca (MTL).

    Se abilitata, la modalità TLS reciproca predefinita è passthrough.

    Se selezioni Verifica con Trust Store:

    - Per impostazione predefinita, le connessioni con certificati client scaduti vengono rifiutate. Per modificare questo comportamento, espandi le impostazioni Advanced MTLS, quindi in Scadenza del certificato client seleziona Consenti certificati client scaduti.

- In Trust Store scegli un trust store esistente o scegli Nuovo trust store.
  - Se hai scelto Nuovo archivio attendibile, fornisci un nome di Trust Store, la posizione dell'Autorità di certificazione URI S3 e, facoltativamente, una posizione dell'elenco di revoca dei certificati URI S3.
- (Facoltativo) Scegli se desideri abilitare TrustStore Advertise CA per i nomi dei soggetti.

11. Scegli Aggiungi.
12. Per aggiungere certificati all'elenco dei certificati opzionali, consultaAggiunta di certificati all'elenco dei certificati.

Per aggiungere un listener HTTPS utilizzando AWS CLI

Utilizzare il comando create-listener per creare il listener e la regola predefinita e il comando create-rule per definire regole di listener aggiuntive.

Regole dell'ascoltatore per Application Load Balancer

Le regole definite per un listener determinano il modo in cui il sistema di bilanciamento del carico instrada le richieste ai target in uno o più gruppi target.

Ogni regola consiste in una priorità, una o più operazioni e una o più condizioni. Per ulteriori informazioni, consulta Regole dei listener.

Requisiti

- Ogni regola deve includere esattamente una delle seguenti operazioni: `forward`, `redirect` o `fixed-response` e deve essere l'ultima operazione da eseguire.
- Ogni regola può includere uno zero o una delle seguenti condizioni: `host-header`, `http-request-method`, `path-pattern` e `source-ip` e zero o una o più delle seguenti condizioni: `http-header` e `query-string`.
- Puoi specificare fino a tre stringhe di confronto per condizione e fino a cinque per regola.
- Un'operazione `forward` instrada le richieste verso il gruppo target. Prima di aggiungere un'operazione `forward`, crea il gruppo target e aggiungi i target. Per ulteriori informazioni, consulta Crea un gruppo target per il tuo Application Load Balancer.

Aggiungere una regola

È possibile definire una regola predefinita al momento della creazione di un listener, ed è possibile definire regole aggiuntive non predefinite in qualsiasi momento.

Per aggiungere una regola tramite la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona il sistema di bilanciamento del carico per visualizzarne i dettagli.
4. Nella scheda Ascoltatori e regole, eseguire una delle seguenti operazioni:

   a. Selezionare il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.

      Nella scheda Regole scegliere Aggiungi regola.

   b. Selezionare l'ascoltatore al quale si desidera aggiungere una regola.

      Scegliere Gestisci regole, poi Aggiungi regola.
5. È possibile specificare un nome per la regola nella sezione Nome e tag, anche se non è obbligatorio.

   Per aggiungere altri tag, seleziona il testo Aggiungi altri tag.
6. Scegli Next (Successivo).
7. Scegliere Aggiungi condizione.
8. Aggiungere una o più delle seguenti condizioni:

   - Intestazione host: definire l'intestazione dell'host. Ad esempio: `*.example.com`. Scegliere Conferma per salvare la condizione.

     Massimo 128 caratteri. Non prevede una distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono a-z, A-Z, 0-9, i caratteri speciali -_. e i caratteri jolly (* e ?). Si deve includere il carattere "." almeno una volta. Dopo l'ultimo carattere "." è possibile includere solo caratteri alfabetici.
   - Percorso: definire il percorso. Ad esempio: `/item/*` . Scegliere Conferma per salvare la condizione.

Massimo 128 caratteri. Distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono a-z, A-Z, 0-9, i caratteri speciali _-.$/~"'@:+; & e i caratteri jolly (* e ?).

- Metodo di richiesta HTTP: definire il metodo di richiesta HTTP. Scegliere Conferma per salvare la condizione.

  Massimo 40 caratteri. Distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono A-Z e i caratteri speciali -_. I caratteri jolly non sono supportati.

- IP sorgente: definire l'indirizzo IP sorgente in formato CIDR. Scegliere Conferma per salvare la condizione.

  Entrambi IPv4 IPv6 CIDRs sono consentiti. I caratteri jolly non sono supportati.

- Intestazione HTTP: inserire il nome dell'intestazione e aggiungere una o più stringhe di confronto. Scegli Conferma per salvare la condizione.

  - Nome dell'intestazione HTTP: la regola valuterà le richieste che contengono questa intestazione per confermare i valori corrispondenti.

    Massimo 40 caratteri. Non prevede una distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono a-z, A-Z, 0-9 e i caratteri speciali *?-!#$%&'+.^_`|~. I caratteri jolly non sono supportati.

  - Valore dell'intestazione HTTP: inserire stringhe da confrontare rispetto al valore dell'intestazione HTTP.

    Massimo 128 caratteri. Non prevede una distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono a-z, A-Z, 0-9; gli spazi; i seguenti caratteri speciali:!» #$%&' () +,. /:; <=>@ [] ^_` {|} ~-; e caratteri jolly (* e?).

- Stringa di query: instradare le richieste sulla base di coppie chiave:valore nella stringa di query. Scegli Conferma per salvare la condizione.

  Massimo 128 caratteri. Non prevede una distinzione tra lettere maiuscole e minuscole. I caratteri consentiti sono a-z, A-Z, 0-9, i caratteri speciali _-.$/~"'@:+&()!,;= e i caratteri jolly (* e ?).

9. Scegli Next (Successivo).
10. Definire una delle seguenti operazioni per la regola:

    - Inoltra a gruppi di destinazione: scegliere uno o più gruppi di destinazione a cui inoltrare il traffico. Per aggiungere gruppi di destinazione, scegli Aggiungi gruppo di destinazioni. Se si

utilizza più di un gruppo di destinazioni, seleziona un peso per ogni gruppo e controllare la percentuale associata. Se è stata abilitata la persistenza per uno o più gruppi di destinazioni, è necessario abilitare la persistenza a livello di gruppo per una regola.

- Reindirizza a URL: specificare l'URL verso cui verranno reindirizzate le richieste del client. È possibile farlo inserendo ogni parte separatamente nella scheda Parti URI, oppure inserendo l'indirizzo completo nella scheda URL completo. Per Codice di stato, è possibile configurare i reindirizzamenti come temporanei (HTTP 302) o permanenti (HTTP 301) in base alle esigenze.
- Restituisci risposta fissa: specificare il Codice di risposta che verrà restituito alle richieste interrotte del client. Inoltre, è possibile specificare il Tipo di contenuto e il Corpo della risposta, ma non sono richiesti.

11. Scegli Next (Successivo).
12. Specificate la priorità della regola inserendo un valore compreso tra 1 e 50000.
13. Scegli Next (Successivo).
14. Verificare tutti i dettagli e le impostazioni attualmente configurati per la nuove regola. Una volta effettuate tutte le selezioni, scegli Crea.

Per aggiungere una regola usando il AWS CLI

Utilizzare il comando create-rule per creare la regola. Utilizzare il comando describe-rules per visualizzare le informazioni sulla regola.

Modificare una regola

È possibile modificare l'operazione e le condizioni per una regola in qualsiasi momento. Gli aggiornamenti delle regole non hanno effetto immediato, pertanto è possibile che le richieste vengano instradate utilizzando la configurazione della regola precedente per un breve periodo dopo l'aggiornamento di una regola. Eventuali richieste in transito vengono completate.

Per modificare una regola tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, eseguire una delle seguenti operazioni:

- Selezionare il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.

  i. Nella scheda Regole, nella sezione Regole dell'ascoltatore, seleziona il testo nella colonna Nome tag corrispondente alla regola che si desidera modificare.

     Scegliere Operazioni, quindi Modifica regola.

  ii. Nella scheda Regole, nella sezione Regole dell'ascoltatore, seleziona la regola che si desidera modificare.

     Scegliere Operazioni, quindi Modifica regola.

5. Modifica il nome e i tag secondo necessità. Per aggiungere altri tag, seleziona il testo Aggiungi altri tag.
6. Seleziona Next (Successivo).
7. Modificate le condizioni in base alle esigenze. È possibile aggiungere, modificare una condizione esistente o eliminare.
8. Seleziona Next (Successivo).
9. Modificate le azioni in base alle esigenze.
10. Seleziona Next (Successivo).
11. Modificare la priorità della regola in base alle esigenze. È possibile inserire un valore compreso tra 1 e 50000.
12. Seleziona Next (Successivo).
13. Controlla tutti i dettagli e le impostazioni aggiornate configurate per la tua regola. Quando sei soddisfatto delle tue selezioni, scegli Salva modifiche.

Per modificare una regola utilizzando il AWS CLI

Utilizzare il comando modify-rule.

Aggiornare la priorità delle regole

Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima. È possibile modificare la priorità di una regola non predefinita in qualsiasi momento. Non è possibile modificare la priorità della regola di default.

Per aggiornare la priorità delle regole utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, eseguire una delle seguenti operazioni:
   a. Selezionare il testo nelle colonne Protocollo:Porta o Regole per aprire la pagina dei dettagli dell'ascoltatore.
      i. Scegliere Operazioni, quindi Riassegna priorità alle regole.
      ii. Nella scheda Regole, nella sezione Regole dell'ascoltatore, scegli Operazioni e poi Riassegna priorità alle regole.
   b. Selezionare l'ascoltatore.
      - Scegliere Gestisci regole, quindi Riassegna priorità alle regole.
5. Nella sezione Regole dell'ascoltatore, la colonna Priorità mostra l'attuale priorità delle regole. Puoi aggiornare la priorità di una regola inserendo un valore compreso tra 1 e 50000.
6. Una volta effettuate tutte le modifiche, scegli Salva modifiche.

Per aggiornare le priorità delle regole utilizzando il AWS CLI

Utilizza il comando set-rule-priorities.

Eliminare una regola

È possibile eliminare le regole non predefinite per un listener in qualsiasi momento. Non è possibile eliminare la regola predefinita per un listener. Quando si elimina un listener, vengono eliminate anche tutte le sue regole.

Per eliminare una regola utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, eseguire una delle seguenti operazioni:

a. Selezionare il testo nelle colonne Protocollo:Porta o Regole per aprire la pagina dei dettagli dell'ascoltatore.

   i. Selezionare la regola da eliminare.

   ii. Scegliere Operazioni, quindi Elimina regola

   iii. Digitare `confirm` nel campo di testo, quindi scegliere Elimina.

b. Selezionare il testo nella colonna Nome tag per aprire la pagina dei dettagli della regola.

   i. Scegli Operazioni, quindi Elimina regola.

   ii. Digitare `confirm` nel campo di testo, quindi scegliere Elimina.

Per eliminare una regola utilizzando il AWS CLI

Utilizzare il comando delete-rule.

Creazione di un ascoltatore HTTPS per Application Load Balancer

Dopo aver creato un listener HTTPS, puoi sostituire il certificato predefinito, aggiornare l'elenco di certificati o sostituire la policy di sicurezza.

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
- Modifica dell'intestazione HTTP

Sostituzione del certificato predefinito

È possibile sostituire il certificato predefinito per il listener tramite la seguente procedura. Per ulteriori informazioni, consulta Certificati SSL per il tuo Application Load Balancer.

Per sostituire il certificato predefinito utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, scegli il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.
5. Nella scheda Certificati, scegli Modifica predefinito.
6. Nella tabella Certificati ACM e IAM, seleziona un nuovo certificato predefinito.
7. Scegliere Salva come predefinito.

Per sostituire il certificato predefinito utilizzando il AWS CLI

Utilizza il comando modify-listener.

Aggiunta di certificati all’elenco dei certificati

È possibile aggiungere certificati all'elenco di certificati per il listener tramite la seguente procedura. Se hai creato il listener utilizzando il AWS Management Console, abbiamo aggiunto il certificato predefinito all'elenco dei certificati per te. Altrimenti, l'elenco dei certificati è vuoto. L'aggiunta del certificato predefinito all'elenco dei certificati garantisce che questo certificato venga utilizzato con il protocollo SNI anche se viene sostituito come certificato predefinito. Per ulteriori informazioni, consulta Certificati SSL per il tuo Application Load Balancer.

Aggiunta di certificati all’elenco certificati tramite la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, scegli il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.
5. Nella pagina Certificati, scegli Aggiungi certificato.
6. Per aggiungere certificati già gestiti da ACM o IAM, seleziona le caselle di controllo relative ai certificati, quindi scegli Includi come in sospeso di seguito.
7. Se si dispone di un certificato non gestito da ACM o IAM, scegli Importa certificato, completare il modulo e scegliere 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 HTTPS tramite la seguente procedura. Dopo aver rimosso un certificato, il listener non può più creare connessioni utilizzando quel certificato. Per assicurarti che i client non siano interessati, aggiungi un nuovo certificato all'elenco e conferma che le connessioni funzionino prima di rimuovere un certificato dall'elenco.

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 EC2 console Amazon 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. Nella scheda Ascoltatori e regole, seleziona il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.
5. Nella scheda Certificati, seleziona le caselle di controllo per i certificati e scegliere Rimuovi.
6. Quando viene richiesta la conferma, immetti **`confirm`** e seleziona Rifiuta.

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 HTTPS, è possibile selezionare la policy di sicurezza in grado di soddisfare le proprie esigenze. Quando viene aggiunta una nuova policy di sicurezza, è possibile aggiornare l'ascoltatore HTTPS perché utilizzi la nuova policy di sicurezza. Gli Application Load Balancer non supportano policy di sicurezza personalizzate. Per ulteriori informazioni, consulta Politiche di sicurezza per il tuo Application Load Balancer.

L'aggiornamento della politica di sicurezza può causare interruzioni se il sistema di bilanciamento del carico gestisce un volume di traffico elevato. Per ridurre la possibilità di interruzioni quando il sistema

di bilanciamento del carico gestisce un volume di traffico elevato, crea un sistema di bilanciamento del carico aggiuntivo che aiuti a gestire il traffico o richiedi una prenotazione LCU.

Utilizzo delle politiche FIPS sull'Application Load Balancer

Tutti i listener sicuri collegati a un Application Load Balancer devono utilizzare policy di sicurezza FIPS o policy di sicurezza non FIPS; non possono essere combinate. Se un Application Load Balancer esistente ha due o più listener che utilizzano policy non FIPS e desideri che i listener utilizzino invece policy di sicurezza FIPS, rimuovi tutti i listener finché non ce n'è uno solo. Modificate la politica di sicurezza del listener in FIPS, quindi create listener aggiuntivi utilizzando le politiche di sicurezza FIPS. In alternativa, è possibile creare un nuovo Application Load Balancer con nuovi listener utilizzando solo le policy di sicurezza FIPS.

Per aggiungere una policy di sicurezza utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, seleziona il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.
5. Nella pagina Dettagli, scegli Operazioni, poi Modifica ascoltatore.
6. Nella sezione Impostazioni Secure listener, in Politica di sicurezza, scegli una nuova politica di sicurezza.
7. Scegli Save changes (Salva modifiche).

Per aggiornare la politica di sicurezza utilizzando il AWS CLI

Utilizza il comando modify-listener.

Modifica dell'intestazione HTTP

La modifica dell'intestazione HTTP consente di rinominare intestazioni specifiche generate dal load balancer, inserire intestazioni di risposta specifiche e disabilitare l'intestazione di risposta del server. Gli Application Load Balancer supportano la modifica dell'intestazione sia per le intestazioni di richiesta che per quelle di risposta.

Per ulteriori informazioni, consulta Abilita la modifica dell'intestazione HTTP per il tuo Application Load Balancer.

Autenticazione reciproca con TLS in Application Load Balancer

L'autenticazione TLS reciproca è una variante del Transport Layer Security (TLS). Il TLS tradizionale stabilisce comunicazioni sicure tra un server e un client, in cui il server deve fornire la propria identità ai propri client. Con il TLS reciproco, un load balancer negozia l'autenticazione reciproca tra il client e il server mentre negozia TLS. Quando si utilizza Mutual TLS con Application Load Balancer, si semplifica la gestione dell'autenticazione e si riduce il carico sulle applicazioni.

Utilizzando il protocollo TLS reciproco con Application Load Balancer, il sistema di bilanciamento del carico può gestire l'autenticazione dei client per garantire che solo client affidabili comunichino con le applicazioni di backend. Quando si utilizza questa funzionalità, Application Load Balancer autentica i client con certificati di autorità di certificazione (CA) di terze parti o utilizzando il AWS Private Certificate Authority (PCA), facoltativamente, con controlli di revoca. Application Load Balancer trasmette le informazioni sul certificato client al backend, che le applicazioni possono utilizzare per l'autorizzazione. Utilizzando il protocollo TLS reciproco in Application Load Balancer, è possibile ottenere un'autenticazione integrata, scalabile e gestita per le entità basate su certificati, che utilizza librerie consolidate.

Mutual TLS for Application Load Balancers offre le due opzioni seguenti per la convalida dei certificati client X.509v3:

Nota: i certificati client X.509v1 non sono supportati.

- Passthrough TLS reciproco: quando si utilizza la modalità passthrough TLS reciproca, Application Load Balancer invia l'intera catena di certificati client alla destinazione utilizzando intestazioni HTTP. Quindi, utilizzando la catena di certificati client, è possibile implementare l'autenticazione del load balancer corrispondente e la logica di autorizzazione Target nell'applicazione.
- Verifica TLS reciproca: quando si utilizza la modalità di verifica TLS reciproca, Application Load Balancer esegue l'autenticazione del certificato client X.509 per i client quando un sistema di bilanciamento del carico negozia connessioni TLS.

Per iniziare a utilizzare il TLS reciproco in Application Load Balancer utilizzando il passthrough, è sufficiente configurare il listener in modo che accetti qualsiasi certificato dai client. Per utilizzare il TLS reciproco con verifica, devi fare quanto segue:

- Crea una nuova risorsa Trust Store.
- Carica il tuo pacchetto di autorità di certificazione (CA) e, facoltativamente, gli elenchi di revoca.
- Collega il trust store al listener configurato per verificare i certificati client.

Per step-by-step le procedure per configurare la modalità di verifica TLS reciproca con Application Load Balancer, vedere. Configurazione del TLS reciproco su un Application Load Balancer

Prima di iniziare a configurare il TLS reciproco sull'Application Load Balancer

Prima di iniziare a configurare Mutual TLS sul tuo Application Load Balancer, tieni presente quanto segue:

Quote

Gli Application Load Balancer includono alcuni limiti relativi alla quantità di trust store, certificati CA ed elenchi di revoca dei certificati in uso all'interno dell'account. AWS

Per ulteriori informazioni, consulta Quotas for your Application Load Balancers.

Requisiti per i certificati

Gli Application Load Balancer supportano quanto segue per i certificati utilizzati con l'autenticazione TLS reciproca:

- Certificato supportato: X.509v3
- Chiavi pubbliche supportate: RSA 2K — 8K o ECDSA secp256r1, secp384r1, secp521r1
- Algoritmi di SHA256 firma supportati: 384, 512 con 256.384.512 hash con RSA/SHA256, 384, 512 with EC/SHA RSASSA-PSS con MGF1

Pacchetti di certificati CA

Quanto segue si applica ai pacchetti di autorità di certificazione (CA):

- Gli Application Load Balancer caricano ogni pacchetto di certificati dell'autorità di certificazione (CA) come batch. Gli Application Load Balancer non supportano il caricamento di singoli certificati. Se è necessario aggiungere nuovi certificati, è necessario caricare il file del pacchetto dei certificati.
- Per sostituire un pacchetto di certificati CA, utilizza l'ModifyTrustStoreAPI.

Ordine di certificati per il passthrough

Quando si utilizza il passthrough TLS reciproco, Application Load Balancer inserisce delle intestazioni per presentare la catena di certificati dei client alle destinazioni di backend. L'ordine di presentazione inizia con i certificati leaf e termina con il certificato root.

Ripresa della sessione

La ripresa della sessione non è supportata durante l'utilizzo del passthrough TLS reciproco o delle modalità di verifica con un Application Load Balancer.

Intestazioni HTTP

Gli Application Load Balancer utilizzano le `X-Amzn-Mtls` intestazioni per inviare le informazioni sui certificati quando negozia le connessioni client tramite TLS reciproco. Per ulteriori informazioni ed esempi di intestazioni, vedere. Intestazioni HTTP e TLS reciproco

File di certificato CA

I file di certificato CA devono soddisfare i seguenti requisiti:

- Il file di certificato deve utilizzare il formato PEM (Privacy Enhanced Mail).
- Il contenuto del certificato deve essere racchiuso entro i limiti `-----BEGIN CERTIFICATE-----` e`-----END CERTIFICATE-----`.
- I commenti devono essere preceduti da un # carattere e non devono contenere alcun carattere. -
- Non possono esserci righe vuote.

Esempio di certificato non accettato (non valido):

```
# comments

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 01
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Validity
            Not Before: Jan 11 23:57:57 2024 GMT
            Not After : Jan 10 00:57:57 2029 GMT
        Subject: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    00:01:02:03:04:05:06:07:08
                ASN1 OID: secp384r1
                NIST CURVE: P-384
```

```
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                00:01:02:03:04:05:06:07:08
            X509v3 Subject Alternative Name:
                URI:EXAMPLE.COM
    Signature Algorithm: ecdsa-with-SHA384
         00:01:02:03:04:05:06:07:08
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Esempi di certificati accettati (validi):

1. Certificato singolo (con codifica PEM):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

2. Certificati multipli (con codifica PEM):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Intestazioni HTTP e TLS reciproco

Questa sezione descrive le intestazioni HTTP utilizzate dagli Application Load Balancer per inviare informazioni sui certificati durante la negoziazione di connessioni con i client tramite TLS reciproco.

Le `X-Amzn-Mtls` intestazioni specifiche utilizzate da Application Load Balancer dipendono dalla modalità TLS reciproca che hai specificato: modalità passthrough o modalità di verifica.

Per informazioni su altre intestazioni HTTP supportate da Application Load Balancers, consulta. Intestazioni HTTP e Application Load Balancer

Intestazione HTTP per la modalità passthrough

Per il TLS reciproco in modalità passthrough, gli Application Load Balancer utilizzano l'intestazione seguente.

X-Amzn-Mtls-Clientcert

Questa intestazione contiene il formato PEM con codifica URL dell'intera catena di certificati client presentata nella connessione, con caratteri sicuri. `+=/`

Contenuto dell'intestazione di esempio:

```
X-Amzn-Mtls-Clientcert: -----BEGIN%20CERTIFICATE-----%0AMIID<...reduced...>do0g
%3D%3D%0A-----END%20CERTIFICATE-----%0A-----BEGIN%20CERTIFICATE-----
%0AMIID1<...reduced...>3eZlyKA%3D%3D%0A-----END%20CERTIFICATE-----%0A
```

Intestazioni HTTP per la modalità di verifica

Per il TLS reciproco in modalità di verifica, gli Application Load Balancer utilizzano le seguenti intestazioni.

X-Amzn-Mtls-Clientcert-Serial-Number

Questa intestazione contiene una rappresentazione esadecimale del numero di serie del certificato Leaf.

Contenuto dell'intestazione di esempio:

```
X-Amzn-Mtls-Clientcert-Serial-Number: 03A5B1
```

X-Amzn-Mtls-Clientcert-Issuer

Questa intestazione contiene una rappresentazione in formato stringa del nome distinto (DN) dell'emittente RFC2253 .

Contenuto dell'intestazione di esempio:

```
X-Amzn-Mtls-Clientcert-Issuer:
 CN=rootcamtls.com,OU=rootCA,O=mTLS,L=Seattle,ST=Washington,C=US
```

X-Amzn-Mtls-Clientcert-Subject

Questa intestazione contiene una rappresentazione in RFC2253 formato stringa del nome distinto (DN) del soggetto.

Contenuto dell'intestazione di esempio:

```
X-Amzn-Mtls-Clientcert-Subject: CN=client_.com,OU=client-3,O=mTLS,ST=Washington,C=US
```

X-Amzn-Mtls-ClientCert-Validity

Questa intestazione contiene il formato 01 della data e. ISO86 `notBefore` `notAfter`

Contenuto dell'intestazione di esempio:

```
X-Amzn-Mtls-Clientcert-Validity:
 NotBefore=2023-09-21T01:50:17Z;NotAfter=2024-09-20T01:50:17Z
```

X-Amzn-Mtls-Clientcert-Leaf

Questa intestazione contiene un formato PEM con codifica URL del certificato leaf, con caratteri sicuri. `+=/`

Esempio di contenuto dell'intestazione:

```
X-Amzn-Mtls-Clientcert-Leaf: -----BEGIN%20CERTIFICATE-----%0AMIIG<...reduced...>NmrUlw
%0A-----END%20CERTIFICATE-----%0A
```

Pubblicizza il nome del soggetto della Certificate Authority (CA)

Advertising Certificate Authority (CA) dei nomi dei soggetti migliora il processo di autenticazione aiutando i clienti a determinare quali certificati saranno accettati durante l'autenticazione TLS reciproca.

Quando abiliti Advertise CA Subject names, Application Load Balancer pubblicizzerà l'elenco dei nomi di soggetti delle Autorità di Certificazione CAs () di cui si fida, in base al trust store a cui è associato. Quando un client si connette a una destinazione tramite Application Load Balancer, riceve l'elenco dei nomi di soggetti CA attendibili.

Durante l'handshake TLS, quando Application Load Balancer richiede un certificato client, include un elenco di CA Distinguished Names DNs () affidabili nel messaggio di richiesta di certificato. Questo aiuta i client a selezionare certificati validi che corrispondano ai nomi dei soggetti CA pubblicizzati, semplificando il processo di autenticazione e riducendo gli errori di connessione.

È possibile abilitare Advertise CA Subject Name sui listener nuovi ed esistenti. Per ulteriori informazioni, consulta Aggiunta di un ascoltatore HTTPS.

Registri di connessione per Application Load Balancers

Elastic Load Balancing fornisce log di connessione che acquisiscono gli attributi delle richieste inviate agli Application Load Balancer. I log di connessione contengono informazioni come l'indirizzo IP e la porta del client, le informazioni sul certificato del client, i risultati della connessione e i codici TLS utilizzati. Questi log di connessione possono quindi essere utilizzati per esaminare i modelli di richiesta e altre tendenze.

Per ulteriori informazioni sui log di connessione, consulta Log di connessione per l'Application Load Balancer

Configurazione del TLS reciproco su un Application Load Balancer

Questa sezione include le procedure per configurare la modalità di verifica TLS reciproca per l'autenticazione sugli Application Load Balancer.

Per utilizzare la modalità passthrough TLS reciproca, è sufficiente configurare il listener in modo che accetti qualsiasi certificato dai client. Quando si utilizza il passthrough TLS reciproco, Application Load Balancer invia l'intera catena di certificati client alla destinazione utilizzando intestazioni HTTP, che consentono di implementare la logica di autenticazione e autorizzazione corrispondente nell'applicazione. Per ulteriori informazioni, consulta Creare un listener HTTPS per l'Application Load Balancer.

Quando si utilizza il protocollo TLS reciproco in modalità di verifica, Application Load Balancer esegue l'autenticazione del certificato client X.509 per i client quando un sistema di bilanciamento del carico negozia connessioni TLS.

Per utilizzare la modalità di verifica TLS reciproca, effettuate le seguenti operazioni:

- Crea una nuova risorsa Trust Store.
- Carica il tuo pacchetto di autorità di certificazione (CA) e, facoltativamente, gli elenchi di revoca.
- Collega il trust store al listener configurato per verificare i certificati client.

Segui le procedure in questa sezione per configurare la modalità di verifica TLS reciproca sul tuo Application Load Balancer in. AWS Management Console Per configurare il TLS reciproco utilizzando le operazioni API anziché la console, consulta la Application Load Balancer API Reference Guide.

Attività

- Crea un trust store
- Associa un trust store
- Visualizza i dettagli del Trust Store
- Modifica un trust store
- Eliminare un trust store

Crea un trust store

Esistono tre modi per creare un trust store: quando si crea un Application Load Balancer, quando si crea un listener sicuro e utilizzando la console Trust Store. Quando aggiungi un trust store quando crei un load balancer o un listener, il trust store viene automaticamente associato al nuovo listener. Quando crei un trust store utilizzando la console Trust Store, devi associarlo tu stesso a un listener.

Questa sezione descrive la creazione di un trust store utilizzando la console Trust Store, ma i passaggi utilizzati durante la creazione di un Application Load Balancer o di un listener sono gli stessi. Per maggiori informazioni, consulta Configurare un load balancer e un listener e Creare un listener HTTPS.

Prerequisiti:

- Per creare un trust store, devi disporre di un pacchetto di certificati rilasciato dalla tua Autorità di Certificazione (CA).

Per creare un trust store utilizzando la console

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

2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona Crea trust store.
4. Configurazione del Trust Store

   a. Per il nome del Trust Store, inserisci un nome per il tuo Trust Store.

   b. Per il pacchetto di autorità di certificazione, inserisci il percorso Amazon S3 verso il pacchetto di certificati ca che desideri venga utilizzato dal tuo trust store.

      Facoltativo: utilizza la versione dell'oggetto per selezionare una versione precedente del pacchetto di certificati ca. Altrimenti viene utilizzata la versione corrente.
5. Per le revoche puoi facoltativamente aggiungere un elenco di revoche dei certificati al tuo trust store.

   - In Elenco di revoca dei certificati, inserisci il percorso di Amazon S3 all'elenco di revoca dei certificati che desideri venga utilizzato dal tuo trust store.

     Facoltativo: utilizza la versione dell'oggetto per selezionare una versione precedente dell'elenco di revoca dei certificati. Altrimenti viene utilizzata la versione corrente.
6. Per i tag Trust Store puoi facoltativamente inserire fino a 50 tag da applicare al tuo Trust Store.
7. Seleziona Crea trust store.

Associa un trust store

Dopo aver creato un trust store, è necessario associarlo a un listener prima che l'Application Load Balancer possa iniziare a utilizzare il trust store. È possibile associare un solo trust store a ciascuno dei listener sicuri, ma un trust store può essere associato a più listener.

Questa sezione tratta l'associazione di un trust store a un listener esistente. In alternativa, è possibile associare un trust store durante la creazione di un Application Load Balancer o di un listener. Per maggiori informazioni, consulta Configurare un load balancer e un listener e Creare un listener HTTPS.

Per associare un trust store utilizzando la console

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

4. Nella scheda Listener and rules, scegli il link nella colonna Protocol:Port per aprire la pagina dei dettagli del listener sicuro.
5. Nella scheda Sicurezza, scegli Modifica le impostazioni del listener sicuro.
6. (Facoltativo) Se il TLS reciproco non è abilitato, seleziona Autenticazione reciproca (MTLS) in Gestione dei certificati del client, quindi scegli Verifica con trust store.
7. In Trust store, scegli il trust store che hai creato.
8. Scegli Save changes (Salva modifiche).

Visualizza i dettagli del Trust Store

Pacchetti di certificati CA

Il pacchetto di certificati CA è un componente obbligatorio del trust store. È una raccolta di certificati root e intermedi affidabili che sono stati convalidati da un'autorità di certificazione. Questi certificati convalidati garantiscono che il client possa fidarsi che il certificato presentato sia di proprietà del sistema di bilanciamento del carico.

Puoi visualizzare il contenuto dell'attuale pacchetto di certificati CA nel tuo trust store in qualsiasi momento.

Visualizza un pacchetto di certificati CA

Per visualizzare un pacchetto di certificati CA utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzare la pagina dei dettagli.
4. Scegli Azioni, quindi Get CA bundle.
5. Scegli Condividi link o Scarica.

Elenchi di revoca dei certificati

Facoltativamente, è possibile creare un elenco di revoca dei certificati per un archivio attendibile. Gli elenchi di revoca vengono rilasciati dalle autorità di certificazione e contengono dati relativi ai certificati che sono stati revocati. Gli Application Load Balancer supportano solo gli elenchi di revoca dei certificati in formato PEM.

Quando un elenco di revoca dei certificati viene aggiunto a un archivio attendibile, gli viene assegnato un ID di revoca. Le revoche IDs aumentano per ogni elenco di revoche aggiunto al trust store e non possono essere modificate. Se un elenco di revoca dei certificati viene eliminato da un archivio attendibile, viene eliminato anche il relativo ID di revoca e non viene riutilizzato per tutta la durata dell'archivio attendibile.

> **Note**
>
> Application Load Balancers non può revocare certificati con un numero di serie negativo, all'interno di un elenco di revoche di certificati.

Visualizza un elenco di revoca dei certificati

Per visualizzare un elenco di revoche utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzare la pagina dei dettagli.
4. Nella scheda Elenchi di revoca dei certificati, seleziona Azioni, quindi Ottieni elenco di revoca.
5. Scegli Condividi link o Scarica.

Modifica un trust store

Un trust store può contenere solo un pacchetto di certificati CA alla volta, ma è possibile sostituire il bundle di certificati CA in qualsiasi momento dopo la creazione del trust store.

Sostituisci un pacchetto di certificati CA

Per sostituire un pacchetto di certificati CA utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzare la pagina dei dettagli.
4. Scegli Azioni, quindi Sostituisci il pacchetto CA.
5. Nella pagina Replace CA bundle, in Certificate Authority bundle inserisci la posizione Amazon S3 del pacchetto CA desiderato.

6. (Facoltativo) Utilizza la versione dell'oggetto per selezionare una versione precedente dell'elenco di revoca dei certificati. Altrimenti viene utilizzata la versione corrente.
7. Seleziona Replace CA bundle.

Aggiungi un elenco di revoca dei certificati

Per aggiungere un elenco di revoche utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzarne la pagina dei dettagli.
4. Nella scheda Elenchi di revoca dei certificati, seleziona Azioni, quindi Aggiungi elenco di revoca.
5. Nella pagina Aggiungi elenco di revoche, in Elenco di revoca dei certificati, inserisci la posizione Amazon S3 dell'elenco di revoca dei certificati desiderato
6. (Facoltativo) Utilizza la versione dell'oggetto per selezionare una versione precedente dell'elenco di revoca dei certificati. Altrimenti viene utilizzata la versione corrente.
7. Seleziona Aggiungi elenco di revoca

Eliminare un elenco di revoca dei certificati

Per eliminare un elenco di revoche utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzare la pagina dei dettagli.
4. Nella scheda Elenchi di revoca dei certificati, seleziona Azioni, quindi Elimina elenco di revoca.
5. Conferma l'eliminazione digitando. `confirm`
6. Seleziona Elimina.

Eliminare un trust store

Quando non è più possibile utilizzare un archivio attendibile, è possibile eliminarlo.

Nota: non è possibile eliminare un trust store attualmente associato a un listener.

Per eliminare un trust store utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, scegli Trust Stores.
3. Seleziona il Trust Store per visualizzarne la pagina dei dettagli.
4. Scegli Azioni, quindi Elimina trust store.
5. Conferma l'eliminazione `confirm` digitando.
6. Seleziona Elimina

Condividi il tuo trust store Elastic Load Balancing per Application Load Balancer

Elastic Load Balancing si integra con AWS Resource Access Manager (AWS RAM) per abilitare la condivisione di trust store. AWS RAM è un servizio che consente di condividere in modo sicuro le risorse Account AWS del trust store Elastic Load Balancing all'interno e all'interno dell'organizzazione o delle unità OUs organizzative (). Se disponi di più account, puoi creare un trust store una sola volta e utilizzarlo AWS RAM per renderlo utilizzabile da altri account. Se il tuo account è gestito da AWS Organizations, puoi condividere gli archivi fiduciari con tutti gli account dell'organizzazione o solo con gli account all'interno di unità organizzative specificate (OUs).

Con AWS RAM, condividi le risorse di tua proprietà creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. In questo modello, il Account AWS proprietario del trust store (proprietario) lo condivide con altri Account AWS (consumatori). I consumatori possono associare i trust store condivisi ai propri listener di Application Load Balancer nello stesso modo in cui associano i trust store nel proprio account.

Il proprietario di un trust store può condividere un trust store con:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Indice

- Condividi un trust store
- Smetti di condividere un trust store
- Fatturazione e misurazione

Prerequisiti per la condivisione del trust store

- È necessario creare una condivisione di risorse utilizzando AWS Resource Access Manager. Per ulteriori informazioni, consulta Creare una condivisione di risorse nella Guida AWS RAM per l'utente.
- Per condividere un trust store, devi possederlo nel tuo Account AWS. Non puoi condividere un trust store che è stato condiviso con te.
- Per condividere un trust store con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Autorizzazioni per gli archivi di fiducia condivisi

Affidati ai proprietari di negozi

- I proprietari di negozi fiduciari possono creare un trust store.
- I proprietari di Trust Store possono utilizzare un trust store con sistemi di bilanciamento del carico nello stesso account.
- I proprietari di Trust Store possono condividere un Trust Store con altri AWS account oppure. AWS Organizations
- I proprietari di Trust Store possono annullare la condivisione di un trust store da qualsiasi AWS account o AWS Organizations.
- I proprietari di Trust Store non possono impedire ai sistemi di bilanciamento del carico di utilizzare un trust store nello stesso account.
- I proprietari di Trust Store possono elencare tutti gli Application Load Balancer utilizzando un trust store condiviso.
- I proprietari di Trust Store possono eliminare un trust store se non ci sono associazioni correnti.
- I proprietari di trust store possono eliminare le associazioni con un trust store condiviso.
- I proprietari di negozi fiduciari ricevono CloudTrail i log quando viene utilizzato un archivio di fiducia condiviso.

Fidati dei consumatori del negozio

- I consumatori di Trust Store possono visualizzare i trust store condivisi.
- I consumatori di Trust Store possono creare o modificare gli ascoltatori utilizzando un trust store nello stesso account.
- I consumatori di Trust Store possono creare o modificare gli ascoltatori utilizzando un trust store condiviso.
- I consumatori di Trust Store non possono creare un listener utilizzando un trust store che non è più condiviso.
- I consumatori di Trust Store non possono modificare un trust store condiviso.
- I consumatori di Trust Store possono visualizzare l'ARN di un trust store condiviso se associato a un listener.
- I consumatori di Trust Store ricevono CloudTrail i log quando creano o modificano un listener utilizzando un trust store condiviso.

Autorizzazioni gestite

Quando si condivide un trust store, la condivisione delle risorse utilizza le autorizzazioni gestite per controllare quali azioni sono consentite dal consumatore del trust store. Puoi utilizzare le autorizzazioni gestite predefiniteAWSRAMPermissionElasticLoadBalancingTrustStore, che includono tutte le autorizzazioni disponibili, o creare autorizzazioni gestite dai clienti personalizzate. Le `DescribeTrustStoreAssociations` autorizzazioni `DescribeTrustStoresDescribeTrustStoreRevocations`, e sono sempre abilitate e non possono essere rimosse.

Le seguenti autorizzazioni sono supportate per le condivisioni di risorse Trust Store:

bilanciamento elastico del carico: CreateListener

Può collegare un trust store condiviso a un nuovo listener.

bilanciamento elastico del carico: ModifyListener

Può collegare un trust store condiviso a un listener esistente.

bilanciamento elastico del carico: GetTrustStoreCaCertificatesBundle

Può scaricare il pacchetto di certificati ca associato allo shared trust store.

bilanciamento elastico del carico: GetTrustStoreRevocationContent

Può scaricare il file di revoca associato all'archivio di fiducia condiviso.

elasticloadbalancing: (impostazione predefinita) DescribeTrustStores

Può elencare tutti i trust store posseduti e condivisi con l'account.

elasticloadbalancing: (impostazione predefinita) DescribeTrustStoreRevocations

Può elencare tutto il contenuto della revoca per il trust store arn specificato.

elasticloadbalancing: (impostazione predefinita) DescribeTrustStoreAssociations

Può elencare tutte le risorse nell'account consumer del trust store associate al trust store condiviso.

Condividi un trust store

Per condividere un archivio attendibile, è necessario aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che consente di condividere le risorse tra Account AWS. Una condivisione di risorse specifica le risorse da condividere, i consumatori con cui vengono condivise e le azioni che i responsabili possono eseguire. Quando condividi un trust store utilizzando la EC2 console Amazon, lo aggiungi a una condivisione di risorse esistente. Per aggiungere il trust store a una nuova condivisione di risorse, devi prima creare la condivisione di risorse utilizzando la AWS RAM console.

Quando condividi un trust store di tua proprietà con altri Account AWS, consenti a tali account di associare i rispettivi listener di Application Load Balancer ai trust store del tuo account.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al trust store condiviso. In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso allo Shared Trust Store dopo aver accettato l'invito.

Puoi condividere un trust store di tua proprietà utilizzando la EC2 console Amazon, la AWS RAM console o il AWS CLI.

Per condividere un trust store di tua proprietà utilizzando la EC2 console Amazon

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

2. Nel pannello di navigazione, in Load Balancing, scegli Trust Stores.
3. Seleziona il nome del Trust Store per visualizzarne la pagina dei dettagli.
4. Nella scheda Condivisione, scegli Share trust store.
5. Nella pagina Share Trust Store, in Condivisioni di risorse, seleziona le condivisioni di risorse con cui condividere il trust store.
6. (Facoltativo) Se devi creare una nuova condivisione di risorse, seleziona il link Crea una condivisione di risorse nella console RAM.
7. Seleziona Share trust store.

Per condividere un trust store di tua proprietà utilizzando la AWS RAM console

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

Per condividere un trust store di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Smetti di condividere un trust store

Per interrompere la condivisione di un archivio attendibile di cui sei proprietario, devi rimuoverlo dalla condivisione di risorse. Le associazioni esistenti persistono dopo l'interruzione della condivisione del trust store, tuttavia non sono consentite nuove associazioni a un trust store precedentemente condiviso. Quando il proprietario del Trust Store o il consumatore del Trust Store elimina un'associazione, questa viene eliminata da entrambi gli account. Se un consumatore di Trust Store desidera abbandonare una condivisione di risorse, deve chiedere al proprietario della condivisione di risorse di rimuovere l'account.

> **Eliminazione di associazioni**
>
> I proprietari di Trust Store possono eliminare forzatamente le associazioni di archivi fiduciari esistenti utilizzando il DeleteTrustStoreAssociationcomando. Quando un'associazione viene eliminata, tutti gli ascoltatori del sistema di bilanciamento del carico che utilizzano il trust store non possono più verificare i certificati client e falliranno gli handshake TLS.

Puoi interrompere la condivisione di un trust store utilizzando la EC2 console Amazon, la AWS RAM console o il AWS CLI.

Per interrompere la condivisione di un trust store di tua proprietà utilizzando la EC2 console Amazon

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Load Balancing, scegli Trust Stores.
3. Seleziona il nome del Trust Store per visualizzarne la pagina dei dettagli.
4. Nella scheda Condivisione, in Condivisione delle risorse, seleziona le condivisioni di risorse con cui interrompere la condivisione.
5. Scegli Rimuovi.

Per interrompere la condivisione di un trust store di tua proprietà utilizzando la AWS RAM console

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

Per interrompere la condivisione di un trust store di tua proprietà, utilizza AWS CLI

Utilizza il comando disassociate-resource-share.

Fatturazione e misurazione

Gli archivi trust condivisi prevedono la stessa tariffa standard di trust store, fatturata all'ora, per associazione di trust store con un Application Load Balancer.

Per ulteriori informazioni, inclusa la tariffa specifica per regione, consulta i prezzi di Elastic Load Balancing

Autenticazione degli utenti tramite Application Load Balancer

È possibile configurare un Application Load Balancer per autenticare in modo sicuro gli utenti nel momento in cui accedono alle proprie applicazioni. Ciò consente di deviare il lavoro di autenticazione degli utenti per il sistema di bilanciamento del carico, in modo che le applicazioni possano concentrarsi sulla loro logica di business.

Sono supportati i seguenti casi d'uso:

- Autenticazione degli utenti tramite un provider di identità (IdP) compatibile con OpenID Connect (OIDC).
- Autentica gli utenti tramite social IdPs, come Amazon, Facebook o Google, tramite i pool di utenti supportati da Amazon Cognito.

- Autentica gli utenti tramite identità aziendali, utilizzando SAML, OpenID Connect (OIDC) OAuth o tramite i pool di utenti supportati da Amazon Cognito.

Preparazione all'uso di un provider di identità compatibile con OIDC

Eseguire le seguenti operazioni se si utilizza un provider di identità compatibile con OIDC con Application Load Balancer:

- Creazione di una nuova app OIDC nel provider di identità. Il DNS del provider di identità dev'essere risolvibile pubblicamente.
- È necessario configurare un ID client e un segreto client.
- Ottieni i seguenti endpoint pubblicati dal provider di identità: autorizzazione, token e info sull'utente. È possibile inserire queste informazioni nella config.
- Gli endpoint dei certificati dei provider di identità devono essere emessi da un'autorità di certificazione pubblica considerata attendibile.
- Le voci DNS per gli endpoint devono essere risolvibili pubblicamente, anche se risolvono indirizzi IP privati.
- Consenti uno dei seguenti reindirizzamenti URLs nella tua app IdP, a seconda di quello utilizzato dagli utenti, dove DNS è il nome di dominio del tuo sistema di bilanciamento del carico e CNAME è l'alias DNS dell'applicazione:
  - https://oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse

Preparazione all'uso di Amazon Cognito

Regioni disponibili

L'integrazione di Amazon Cognito per Application Load Balancers è disponibile nelle seguenti regioni:

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)
- US West (Oregon)
- Canada (Centrale)

- Canada occidentale (Calgary)
- Europa (Stoccolma)
- Europa (Milano)
- Europa (Francoforte)
- Europa (Zurigo)
- Europa (Irlanda)
- Europe (London)
- Europa (Parigi)
- Europa (Spagna)
- Sud America (San Paolo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Tokyo)
- Asia Pacifico (Seoul)
- Asia Pacifico (Osaka-Locale)
- Asia Pacifico (Mumbai)
- Asia Pacific (Hyderabad)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Medio Oriente (Emirati Arabi Uniti)
- Medio Oriente (Bahrein)
- Africa (Città del Capo)
- Israele (Tel Aviv)

Eseguire le seguenti operazioni se si utilizzano pool di utenti di Amazon Cognito con Application Load Balancer:

- Crea un pool di utenti. Per ulteriori informazioni, consulta Pool di utenti di Amazon Cognito nella Guida per gli sviluppatori di Amazon Cognito.

- Creazione di un client pool di utenti È necessario configurare il client per generare un client secret, utilizzare il Code Grant Flow e supportare gli stessi OAuth ambiti utilizzati dal sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Configurare un client app pool di utenti nella Guida per gli sviluppatori di Amazon Cognito.
- Creazione di un dominio pool di utenti. Per ulteriori informazioni, consulta Configurare un dominio di pool di utenti nella Amazon Cognito Developer Guide.
- Verificare che l'ambito richiesto restituisca un token ID. Ad esempio, l'ambito predefinito, `openid` restituisce un token ID, ma l'ambito `aws.cognito.signin.user.admin` non lo restituisce.
- Per effettuare la federazione con un provider di identità social o aziendale, abilitare il provider di identità nella sezione di federazione. Per ulteriori informazioni, consulta Accesso al pool di utenti con un provider di identità di terze parti nella Amazon Cognito Developer Guide.
- Consenti il seguente reindirizzamento URLs nel campo URL di callback per Amazon Cognito, dove DNS è il nome di dominio del tuo sistema di bilanciamento del carico e CNAME è l'alias DNS dell'applicazione (se ne utilizzi uno):
  - https://oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse
- Consentire nella whitelist il dominio pool di utenti nell'URL di richiamo dell'app del provider di identità. Utilizzare il formato per il provider di identità. Per esempio:
  - https:*domain-prefix*//.auth. *region*.amazoncognito. com/saml2/idpresponse
  - *user-pool-domain*https://saml2/idpresponse

L'URL di richiamo nelle impostazioni dell'app client dev'essere in lettere minuscole.

Per consentire a un utente di configurare un sistema di bilanciamento del carico per autenticare gli utenti tramite Amazon Cognito, è necessario concedere all'utente l'autorizzazione di chiamare l'operazione `cognito-idp:DescribeUserPoolClient`.

Preparati a usare Amazon CloudFront

Abilita le seguenti impostazioni se utilizzi una CloudFront distribuzione davanti all'Application Load Balancer:

- Inoltra le intestazioni delle richieste (tutte): garantisce che CloudFront non vengano memorizzate nella cache le risposte per le richieste autenticate. Questo impedisce che vangano serviti dalla cache dopo che la sessione di autenticazione è scaduta. In alternativa, per ridurre questo rischio mentre la memorizzazione nella cache è abilitata, i proprietari di una CloudFront distribuzione

possono impostare la scadenza del valore time-to-live (TTL) prima della scadenza del cookie di autenticazione.

- Inoltro e caching delle stringhe di query (tutte): assicura che il sistema di bilanciamento del carico abbia accesso ai parametri della stringa di query richiesti per l'autenticazione dell'utente con il provider di identità.
- Inoltro dei cookie (tutti): assicura che tutti i cookie di autenticazione vengano CloudFront inoltrati al sistema di bilanciamento del carico.
- Quando configuri l'autenticazione OpenID Connect (OIDC) insieme ad CloudFront Amazon, assicurati che la porta HTTPS 443 venga utilizzata in modo coerente lungo l'intero percorso di connessione. In caso contrario, possono verificarsi errori di autenticazione perché il reindirizzamento OIDC del client URLs non corrisponde al numero di porta dell'URI generato originariamente.

Configurazione dell'autenticazione utente

È possibile creare un'operazione di autenticazione per una o più regole di listener per configurare l'autenticazione utente. I tipi di operazione `authenticate-cognito` e `authenticate-oidc` sono supportati solo con i listener HTTPS. Per le descrizioni dei campi corrispondenti, consulta AuthenticateCognitoActionConfige AuthenticateOidcActionConfignella versione di riferimento dell'API Elastic Load Balancing 2015-12-01.

Il servizio di bilanciamento del carico invia un cookie di sessione al client per mantenere lo stato di autenticazione. Questo cookie contiene sempre l'attributo `secure`, perché l'autenticazione utente richiede un listener HTTPS. Questo cookie contiene l'attributo `SameSite=None` con le richieste CORS (cross-origin resource sharing).

Per un sistema di bilanciamento del carico che supporta più applicazioni che richiedono l'autenticazione client indipendente, ogni ascoltatore con un'operazione di autenticazione deve avere un nome di cookie univoco. Ciò garantisce che i client siano sempre autenticati tramite il provider di identità prima di essere instradato verso il gruppo di destinazioni specificato nella regola.

Gli Application Load Balancer non supportano i valori dei cookie codificati con URL.

Per impostazione predefinita, il campo `SessionTimeout` è impostato su 7 giorni. Se si desiderano sessioni più brevi, è possibile configurare un timeout della sessione di 1 secondo. Per ulteriori informazioni, consulta Timeout della sessione.

Impostare il campo `OnUnauthenticatedRequest` più appropriato per l'applicazione. Per esempio:

- Applicazioni che richiedono all'utente di effettuare l'accesso utilizzando un'identità social o aziendale: queste applicazioni sono supportate dall'opzione predefinita, `authenticate`. Se l'utente non è connesso, il sistema di bilanciamento del carico reindirizza la richiesta all'endpoint di autorizzazione del provider di identità e il provider di identità richiede all'utente di effettuare l'accesso utilizzando la sua interfaccia utente.
- Applicazioni che forniscono una vista personalizzata a un utente che ha eseguito l'accesso o una vista generale a un utente che non è connesso: per supportare questo tipo di applicazione, utilizzare l'opzione `allow`. Se l'utente è connesso, il sistema di bilanciamento del carico fornisce le richieste dell'utente e l'applicazione può fornire una vista personalizzata. Se l'utente non è connesso, il sistema di bilanciamento del carico inoltra la richiesta senza le istanze degli utenti e l'applicazione può fornire la vista generale.
- Applicazioni a pagina singola JavaScript che vengono caricate ogni pochi secondi: se si utilizza l'`deny`opzione, il sistema di bilanciamento del carico restituisce un errore HTTP 401 Unauthorized alle chiamate AJAX prive di informazioni di autenticazione. Ma se l'utente ha informazioni di autenticazione scadute, reindirizza il client all'endpoint di autenticazione del provider di identità.

Il sistema di bilanciamento del carico deve essere in grado di comunicare con l'endpoint del token del provider di identità (`TokenEndpoint`) e con l'endpoint delle info sull'utente del provider di identità (`UserInfoEndpoint`). Gli Application Load Balancer supportano solo la comunicazione con questi endpoint. IPv4 Se il tuo IdP utilizza indirizzi pubblici, assicurati che i gruppi di sicurezza per il tuo load balancer e la rete per il ACLs tuo VPC consentano l'accesso agli endpoint. Quando si utilizza un sistema di bilanciamento del carico interno o il tipo di indirizzo IP`dualstack-without-public-ipv4`, un gateway NAT può consentire al sistema di bilanciamento del carico di comunicare con gli endpoint. Per ulteriori informazioni, consulta Nozioni di base sul gateway NAT nella Guida per l'utente di Amazon VPC.

Utilizzare il seguente comando create-rule per configurare l'autenticazione utente.

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values="/login" --actions file://actions.json
```

Di seguito è riportato un esempio del file `actions.json` che specifica un'operazione `authenticate-oidc` e un'operazione `forward`. `AuthenticationRequestExtraParams` consente di passare parametri extra a un provider di identità durante l'autenticazione. Seguire la documentazione fornita dal provider di identità per determinare quali campi sono supportati.

```
[{
```

```
    "Type": "authenticate-oidc",
    "AuthenticateOidcConfig": {
        "Issuer": "https://idp-issuer.com",
        "AuthorizationEndpoint": "https://authorization-endpoint.com",
        "TokenEndpoint": "https://token-endpoint.com",
        "UserInfoEndpoint": "https://user-info-endpoint.com",
        "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "ClientSecret": "1234567890123456789012345678 90",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Di seguito è riportato un esempio di un file `actions.json` che specifica un'operazione `authenticate-cognito` e un'operazione `forward`.

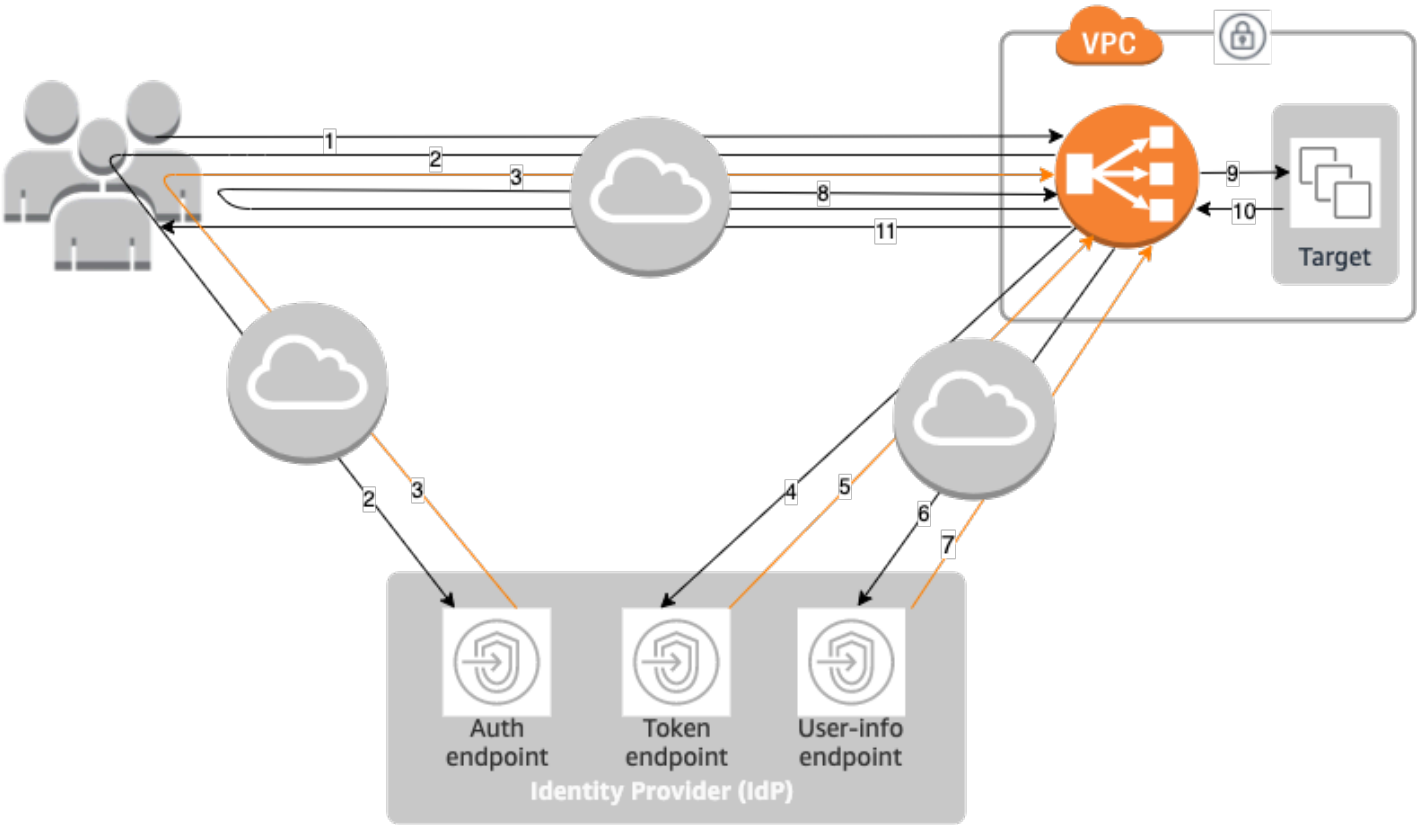
```
[{
    "Type": "authenticate-cognito",
    "AuthenticateCognitoConfig": {
        "UserPoolArn": "arn:aws:cognito-idp:region-code:account-id:userpool/user-pool-
id",
        "UserPoolClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "UserPoolDomain": "userPoolDomain1",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
```

```
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Per ulteriori informazioni, consulta Regole dei listener.

Flusso di autenticazione

Il seguente diagramma di rete è una rappresentazione visiva di come un Application Load Balancer utilizza OIDC per autenticare gli utenti.



Gli articoli numerati di seguito evidenziano e spiegano gli elementi mostrati nel diagramma di rete precedente.

1. L'utente invia una richiesta HTTPS a un sito Web ospitato dietro un Application Load Balancer. Quando le condizioni di una regola con un'operazione di autenticazione sono soddisfatte, il sistema di bilanciamento del carico verifica se nelle intestazioni delle richieste è presente un cookie di sessione per l'autenticazione.
2. Se il cookie non è presente, il sistema di bilanciamento del carico reindirizza l'utente all'endpoint di autorizzazione del provider di identità in modo che il provider di identità possa autenticare l'utente.
3. Dopo che l'utente si è autenticato, il provider di identità invia l'utente al sistema di bilanciamento del carico con un codice di autorizzazione.
4. Il sistema di bilanciamento del carico presenta il codice per la concessione dell'autorizzazione all'endpoint del token del provider di identità.
5. Dopo aver ricevuto un codice per la concessione dell'autorizzazione valido, il provider di identità fornisce il token ID token e il token di accesso all'Application Load Balancer.
6. In seguito, l'Application Load Balancer invia il token di accesso all'endpoint di informazioni dell'utente.
7. L'endpoint di informazioni dell'utente scambia il token di accesso con le richieste dell'utente.
8. L'Application Load Balancer reindirizza l'utente con il cookie di autenticazione della sessione `AWSELB` all'URI originale. Poiché la maggior parte dei browser limita le dimensioni dei cookie a 4 K, il sistema di bilanciamento del carico suddivide ciascun cookie superiore a 4 K in più cookie. Se la dimensione totale delle richieste dell'utente e dei token di accesso ricevuti dal provider di identità è superiore a 11K byte, il sistema di bilanciamento del carico restituisce al client un errore HTTP 500 e incrementa il parametro `ELBAuthUserClaimsSizeExceeded`.
9. L'Application Load Balancer convalida il cookie e inoltre le informazioni dell'utente alle destinazioni nelle intestazioni HTTP `X-AMZN-OIDC-*` impostate. Per ulteriori informazioni, consulta Codifica delle richieste dell'utente e verifica della firma.
10. La destinazione invia una risposta all'Application Load Balancer.
11. L'Application Load Balancer invia la risposta finale all'utente.

Ogni nuova richiesta segue i passaggi da 1 a 11, mentre le richieste successive seguono i passaggi da 9 a 11. Ciò significa che ogni richiesta successiva inizia al passaggio 9 purché il cookie non sia scaduto.

Il cookie `AWSALBAuthNonce` viene aggiunto all'intestazione della richiesta dopo l'autenticazione dell'utente da parte del provider di identità. Questo non modifica il modo in cui l'Application Load Balancer elabora le richieste di reindirizzamento del provider di identità.

Se il provider di identità fornisce un token di aggiornamento valido nel token ID, il sistema di bilanciamento del carico salva il token di aggiornamento e lo utilizza per aggiornare le richieste dell'utente ogni volta che il token di accesso scade, fino a quando la sessione scade o l'aggiornamento del provider di identità ha esito negativo. Se l'utente si disconnette, l'aggiornamento ha esito negativo e il sistema di bilanciamento del carico reindirizza l'utente all'endpoint di autorizzazione del provider di identità. In questo modo il sistema di bilanciamento del carico archivia le sessioni dopo la disconnessione dell'utente. Per ulteriori informazioni, consulta Timeout della sessione.

> **Note**
>
> La scadenza del cookie è diversa da quella della sessione di autenticazione. La scadenza del cookie è un attributo del cookie ed è impostata su 7 giorni. La durata effettiva della sessione di autenticazione viene determinata dal timeout della sessione configurato nell'Application Load Balancer per la funzionalità di autenticazione. Il timeout della sessione è incluso nel valore del cookie Auth, anch'esso crittografato.

Codifica delle richieste dell'utente e verifica della firma

Dopo che il sistema di bilanciamento del carico è riuscito ad autenticare un utente, invia alla destinazione le richieste dell'utente ricevute dal provider di identità. Il sistema di bilanciamento del carico firma le richieste dell'utente in modo che le applicazioni possano verificare la firma e verificare che le richieste siano state inviate dal sistema di bilanciamento del carico.

Il sistema di bilanciamento del carico aggiunge le seguenti intestazioni HTTP:

`x-amzn-oidc-accesstoken`

Il token di accesso dall'endpoint del token, in testo normale.

`x-amzn-oidc-identity`

Il campo oggetto (`sub`) dall'endpoint delle informazioni sull'utente, in testo normale.

Nota: l'attestazione sub è il modo migliore per identificare un determinato utente.

`x-amzn-oidc-data`

Le richieste dell'utente, nel formato dei token Web JSON (JWT).

I token di accesso e le richieste dell'utente sono diverse dai token ID. I token di accesso e le richieste dell'utente consentono l'accesso solo alle risorse del server, mentre i token ID contengono informazioni aggiuntive per autenticare un utente. L'Application Load Balancer crea un nuovo token di accesso durante l'autenticazione di un utente e passa solo i token di accesso e le attestazioni al backend, tuttavia non trasmette le informazioni sul token ID.

Tali token seguono il formato JWT, ma non sono token ID. Il formato JWT include un'intestazione, un payload e una firma con codifica URL base64, oltre ai caratteri padding alla fine.. Un Application Load Balancer utilizza ES256 (ECDSA utilizza P-256 e SHA256) per generare la firma JWT.

L'intestazione JWT è un oggetto JSON con i seguenti campi:

```
{
   "alg": "algorithm",
   "kid": "12345678-1234-1234-1234-123456789012",
   "signer": "arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/
app/load-balancer-name/load-balancer-id",
   "iss": "url",
   "client": "client-id",
   "exp": "expiration"
}
```

Il carico utile JWT è un oggetto JSON che contiene le richieste dell'utente ricevute dall'endpoint delle informazioni sull'utente del provider di identità.

```
{
   "sub": "1234567890",
   "name": "name",
   "email": "alias@example.com",
   ...
}
```

Se desideri che il sistema di bilanciamento del carico crittografi le dichiarazioni degli utenti, devi configurare il tuo gruppo target in modo che utilizzi HTTPS. Inoltre, come best practice di sicurezza, ti consigliamo di limitare i tuoi obiettivi alla ricezione del solo traffico dall'Application Load Balancer. Puoi raggiungere questo obiettivo configurando il gruppo di sicurezza dei tuoi target in modo che faccia riferimento all'ID del gruppo di sicurezza del load balancer.

Per garantire la sicurezza, è necessario verificare la firma prima di eseguire qualsiasi autorizzazione in base alle affermazioni e verificare che il `signer` campo nell'intestazione JWT contenga l'ARN Application Load Balancer previsto.

Per ottenere la chiave pubblica, ottenere la chiave ID dall'intestazione JWT e utilizzarla per cercare la chiave pubblica dall'endpoint. L'endpoint per ogni regione AWS è il seguente:

```
https://public-keys.auth.elb.region.amazonaws.com/key-id
```

Infatti AWS GovCloud (US), gli endpoint sono i seguenti:

```
https://s3-us-gov-west-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-west-1/key-id
https://s3-us-gov-east-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-east-1/key-id
```

AWS fornisce una libreria che puoi utilizzare per verificare la JWTs firma firmata da Amazon Cognito, Application Load Balancers e altri dispositivi compatibili con OIDC. IDPs Per ulteriori informazioni, consulta JWT Verify.AWS

Timeout

Timeout della sessione

Il token di aggiornamento e il timeout della sessione funzionano congiuntamente come segue:

- Se il timeout della sessione è inferiore alla scadenza del token di accesso, il sistema di bilanciamento del carico mantiene il timeout della sessione. Se l'utente dispone di una sessione attiva con IdP, è possibile che non venga richiesto di accedere nuovamente. In caso contrario, l'utente viene reindirizzato all'accesso.
  - Se il timeout della sessione del provider di identità è più lungo di quello dell'Application Load Balancer, l'utente non deve fornire nuovamente le credenziali per effettuare l'accesso. Al contrario, il provider di identità reindirizza all'Application Load Balancer con un nuovo codice per la concessione dell'autorizzazione. I codici per la concessione dell'autorizzazione sono monouso, anche se non si effettua nuovamente l'accesso.
  - Se il timeout della sessione del provider di identità è uguale a quello dell'Application Load Balancer, all'utente viene richiesto di fornire le credenziali per effettuare l'accesso. Dopo l'accesso dell'utente, il provider di identità reindirizza all'Application Load Balancer con un nuovo codice per la concessione dell'autorizzazione e il resto del flusso di autenticazione prosegue fino a quando la richiesta raggiunge il back-end.
- Se il timeout della sessione è superiore alla scadenza del token di accesso e il provider di identità non supporta i token di aggiornamento, il sistema di bilanciamento del carico mantiene la sessione di autenticazione fino alla sua scadenza. Dopodiché, l'utente deve effettuare nuovamente l'accesso.

- Se il timeout della sessione supera la scadenza del token di accesso e il provider di identità supporta i token di aggiornamento, il sistema di bilanciamento del carico aggiorna la sessione dell'utente ogni volta che il token di accesso scade. Il sistema di bilanciamento del carico richiede all'utente di accedere nuovamente solo dopo che la sessione di autenticazione è scaduta o il flusso di aggiornamento ha avuto esito negativo.

Timeout di accesso client

Un client deve avviare e completare il processo di autenticazione entro 15 minuti. Se un client non riesce a completare l'autenticazione entro il limite di 15 minuti, riceve un errore HTTP 401 dal sistema di bilanciamento del carico. Non è possibile modificare o rimuovere questo timeout.

Ad esempio, se un utente carica la pagina di accesso tramite l'Application Load Balancer, deve completare il processo di accesso entro 15 minuti. Se l'utente aspetta e prova a effettuare l'accesso dopo la scadenza del timeout di 15 minuti, il sistema di bilanciamento del carico restituisce un errore HTTP 401. L'utente dovrà aggiornare la pagina e riprovare a effettuare l'accesso.

Autenticazione di disconnessione

Quando un'applicazione deve disconnettere un utente autenticato, è necessario impostare la data di scadenza del cookie di sessione per l'autenticazione su -1 e reindirizzare il client all'endpoint di disconnessione del provider di identità (se il provider di identità lo supporta). Per impedire agli utenti di riutilizzare un cookie eliminato, è consigliabile configurare un periodo di scadenza ragionevolmente breve per il token di accesso. Se un client fornisce al load balancer un cookie di sessione con un token di accesso scaduto con un token di aggiornamento non NULL, il load balancer contatta l'IdP per determinare se l'utente è ancora connesso.

Le pagine di destinazione per il logout del client non sono autenticate. Ciò significa che non possono essere responsabili di una regola Application Load Balancer che richiede l'autenticazione.

- Quando viene inviata una richiesta alla destinazione, l'applicazione deve impostare la scadenza su -1 per tutti i cookie di autenticazione. Gli Application Load Balancer supportano cookie di dimensioni massime di 16 K, quindi possono creare fino a 4 partizioni da inviare poi al client.
  - Se il provider di identità ha un endpoint di disconnessione, deve emettere un reindirizzamento verso l'endpoint di disconnessione del provider di identità, ad esempio l'Endpoint LOGOUT documentato nella Guida per gli sviluppatori di Amazon Cognito.
  - Se il provider di identità non dispone di un endpoint di disconnessione, la richiesta ritorna alla pagina di destinazione di disconnessione del client e il processo di accesso ricomincia.

- Supponendo che il provider di identità abbia un endpoint di disconnessione, il provider deve far scadere i token di accesso e i token di aggiornamento e reindirizzare l'utente alla pagina di destinazione di disconnessione del client.
- Le richieste successive seguono il flusso di autenticazione originale.

Tag per i listener e le regole di Application Load Balancer

I tag aiutano a categorizzare gli ascoltatori e le regole in modi diversi. Ad esempio, è possibile aggiungere un tag a una risorsa in base a scopo, proprietario o ambiente.

È possibile aggiungere più tag per ogni ascoltatore e regola. Le chiavi dei tag devono essere univoche per ciascun ascoltatore e regola. Se aggiungi un tag con una chiave già associata all'ascoltatore e alla regola, 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
- 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 AWS riservato all'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.

Aggiornare i tag dell'ascoltatore

Per aggiornare i tag per un ascoltatore tramite la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.

3. Scegliere il nome del sistema di bilanciamento del carico che contiene l'ascoltatore che si desidera aggiornare per aprire la pagina dei dettagli.
4. Nella scheda Ascoltatori e regole, eseguire una delle seguenti operazioni:

   a. Selezionare il testo nella colonna Protocollo:Porta per aprire la pagina dei dettagli dell'ascoltatore.

      Nella scheda Tag scegliere Gestisci tag.

   b. Selezionare l'ascoltatore per cui si desidera aggiornare i tag.

      Scegliere Gestisci ascoltatore, poi Gestisci tag.

   c. Selezionare il testo nella colonna Tag per aprire la pagina dei dettagli dell'ascoltatore nella scheda tag.

      Scegliere Gestisci tag.
5. Nella pagina Gestisci tag, eseguire una o più delle seguenti operazioni:

   a. Per aggiornare un tag, inserisci nuovi valori per Chiave e Valore.
   b. Per aggiungere un tag, scegli Aggiungi nuovo tag e inserire valori per Chiave e Valore.
   c. Per eliminare un tag, scegli Rimuovi accanto al tag.
6. Una volta completato l'aggiornamento dei tag, scegli Salva.

Per aggiornare i tag per un ascoltatore utilizzando il AWS CLI

Utilizza i comandi add-tags e remove-tags.

Aggiornare i tag della regola

Per aggiornare i tag per una regola tramite la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Scegliere il nome del sistema di bilanciamento del carico che contiene la regola che si desidera aggiornare per aprire la pagina dei dettagli.

4. Nella scheda Ascoltatori e regole, seleziona il testo nella colonna Protocollo:Porta dell'ascoltatore che contiene la regola che si desidera aggiornare aprire la pagina dei dettagli dell'ascoltatore.
5. Nella pagina dei dettagli dell'ascoltatore, completare una delle seguenti operazioni:
   a. Selezionare il testo nella colonna Nome tag per aprire la pagina dei dettagli della regola.

      Nella pagina dei dettagli della regola, scegli Gestisci tag.
   b. Selezionare il testo nella colonna Tag per la regola che si desidera aggiornare.

      Nella finestra popup di riepilogo dei tag, scegli Gestisci tag.
6. Nella pagina Gestisci tag, eseguire una o più delle seguenti operazioni:
   a. Per aggiornare un tag, inserisci nuovi valori per Chiave e Valore.
   b. Per aggiungere un tag, scegli Aggiungi nuovo tag e inserire valori per Chiave e Valore.
   c. Per eliminare un tag, scegli Rimuovi accanto al tag.
7. Una volta completato l'aggiornamento dei tag, scegli Salva.

Per aggiornare i tag di una regola utilizzando il AWS CLI

Utilizza i comandi add-tags e remove-tags.

Eliminare un ascoltatore per Application Load Balancer

Puoi eliminare un listener in qualsiasi momento. Quando elimini un sistema di bilanciamento del carico, vengono eliminati anche tutti i suoi listener.

Per eliminare un listener utilizzando la console

1. Apri la EC2 console Amazon 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. Nella scheda Ascoltatori e regole, seleziona la casella di controllo dell'ascoltatore e scegliere Gestisci ascoltatore, Elimina ascoltatore.
5. Quando viene richiesta la conferma, immettere **`confirm`** e quindi scegliere Elimina.

Per eliminare un listener utilizzando il AWS CLI

Utilizza il comando delete-listener.

Modifica dell'intestazione HTTP per il tuo Application Load Balancer

La modifica dell'intestazione HTTP è supportata da Application Load Balancers, sia per le intestazioni di richiesta che per quelle di risposta. Senza dover aggiornare il codice dell'applicazione, la modifica dell'intestazione consente un maggiore controllo sul traffico e sulla sicurezza dell'applicazione.

Per abilitare la modifica dell'intestazione, consulta. Abilita la modifica dell'intestazione

Rinominare mTLS/TLS le intestazioni

La funzionalità di ridenominazione delle intestazioni consente di configurare i nomi delle intestazioni MTLS e TLS che Application Load Balancer genera e aggiunge alle richieste.

Questa capacità di modificare le intestazioni HTTP consente all'Application Load Balancer di supportare facilmente le applicazioni che utilizzano intestazioni di richiesta e risposta formattate in modo specifico.

Header	Descrizione
X-Amzn-Mtls-Clientcert-Serial-Number	Assicura che il target possa identificare e verificare il certificato specifico presentato dal client durante l'handshake TLS.
X-Amzn-Mtls-Clientcert-Issuer	Aiuta il destinatario a convalidare e autentica re il certificato client identificando l'autorità di certificazione che ha emesso il certificato.
X-Amzn-Mtls-Clientcert-Subject	Fornisce all'obiettivo informazioni dettagliate sull'entità a cui è stato rilasciato il certificato client, il che aiuta nell'identificazione, nell'aute nticazione, nell'autorizzazione e nella registraz ione durante l'autenticazione MTLS.
X-Amzn-Mtls-Clientcert-Validity	Consente al destinatario di verificare che il certificato client utilizzato rientri nel periodo di

Header	Descrizione
	validità definito, assicurando che il certificato non sia scaduto o utilizzato prematuramente.
X-Amzn-Mtls-Clientcert-Leaf	Fornisce il certificato client utilizzato nell'hand shake MTLS, che consente al server di autenticare il client e convalidare la catena di certificati. Ciò garantisce che la connessione sia sicura e autorizzata.
X-Amzn-Mtls-Clientcert	Contiene il certificato client completo. Consente al destinatario di verificare l'autenticità del certificato, convalidare la catena di certifica ti e autenticare il client durante il processo di handshake mTLS.
X-Amzn-TLS-Version	Indica la versione del protocollo TLS utilizzat a per una connessione. Facilita la determina zione del livello di sicurezza della comunicaz ione, la risoluzione dei problemi di connessione e la garanzia della conformità.
X-Amzn-TLS-Cipher-Suite	Indica la combinazione di algoritmi crittogra fici utilizzati per proteggere una connessio ne in TLS. Ciò consente al server di valutare la sicurezza della connessione, facilitare la risoluzione dei problemi di compatibilità e garantire la conformità alle politiche di sicurezza.

Aggiungi intestazioni di risposta

Utilizzando gli insert header, puoi configurare l'Application Load Balancer per aggiungere intestazioni relative alla sicurezza alle risposte. Con questi attributi, è possibile inserire intestazioni tra cui HSTS, CORS e CSP.

Per impostazione predefinita, queste intestazioni sono vuote. Quando ciò accade, l'Application Load Balancer non modifica questa intestazione di risposta.

Quando abiliti un'intestazione di risposta, Application Load Balancer aggiunge l'intestazione con il valore configurato a tutte le risposte. Se la risposta di target include l'intestazione di risposta HTTP, il load balancer aggiorna il valore dell'intestazione in modo che sia il valore configurato. Altrimenti, il load balancer aggiunge l'intestazione di risposta HTTP alla risposta con il valore configurato.

Header	Descrizione
Strict-Transport-Security	Implica le connessioni solo HTTPS da parte del browser per una durata specificata, contribue ndo a proteggere da man-in-the-middle attacchi, downgrade del protocollo ed errori degli utenti. Garantisce che tutte le comunicaz ioni tra il client e la destinazione siano crittogra fate.
Access-Control-Allow-Origin	Controlla se è possibile accedere alle risorse su una destinazione da origini diverse. Ciò consente interazioni sicure tra origini diverse, impedendo al contempo l'accesso non autorizzato.
Access-Control-Allow-Methods	Speciifica i metodi HTTP consentiti quando si effettuano richieste tra origini diverse alla destinazione. Fornisce il controllo su quali azioni possono essere eseguite da origini diverse.
Access-Control-Allow-Headers	Speciifica quali intestazioni personalizzate o non semplici possono essere incluse in una richiesta multiorigine. Questa intestazione consente ai target di controllare quali intestazi oni possono essere inviate da client di origini diverse.

Header	Descrizione
Access-Control-Allow-Credentials	Speciifica se il client deve includere credenziali come cookie, autenticazione HTTP o certificati client nelle richieste tra origini diverse.
Access-Control-Expose-Headers	Consente al target di specificare a quali intestazioni di risposta aggiuntive può accedere il client nelle richieste multiorigine.
Access-Control-Max-Age	Definisce per quanto tempo il browser può memorizzare nella cache il risultato di una richiesta di preflight, riducendo la necessità di ripetuti controlli di preflight. Ciò aiuta a ottimizza re le prestazioni riducendo il numero di richieste OPTIONS necessarie per determinate richieste tra origini diverse.
Content-Security-Policy	Funzionalità di sicurezza che previene gli attacchi di iniezione di codice come XSS controllando quali risorse come script, stili, immagini, ecc. possono essere caricate ed eseguite da un sito Web.
X-Content-Type-Options	Con la direttiva no-sniff, migliora la sicurezza web impedendo ai browser di indovinare il tipo MIME di una risorsa. Garantisce che i browser interpretino il contenuto solo in base al Content-Type dichiarato
X-Frame-Options	Meccanismo di sicurezza delle intestazioni che aiuta a prevenire gli attacchi di clickjack ing controllando se una pagina Web può essere incorporata nei frame. Valori come DENY e SAMEORIGIN possono garantire che i contenuti non siano incorporati in siti Web dannosi o non affidabili.

Disabilita le intestazioni

Utilizzando disable header, puoi configurare l'Application Load Balancer per disabilitare `server:awselb/2.0` l'intestazione dalle risposte. Ciò riduce l'esposizione delle informazioni specifiche del server, aggiungendo al contempo un ulteriore livello di protezione all'applicazione.

Il nome dell'attributo è`routing.http.response.server.enabled`. I valori disponibili sono `true` o`false`. Il valore predefinito è `true`.

Limitazioni

- I valori dell'intestazione possono contenere i seguenti caratteri
  - Caratteri alfanumerici:`a-z`, e `A-Z` `0-9`
  - Caratteri speciali: `_ :;.,\/'?!(){}[]@<>=-+*#&`|~^%`
- Il valore dell'attributo non può superare la dimensione di 1.000 byte.
- Elastic Load Balancing esegue convalide di input di base per verificare che il valore dell'intestazione sia valido. Tuttavia, la convalida non è in grado di confermare se il valore è supportato per un'intestazione specifica.
- L'impostazione di un valore vuoto per qualsiasi attributo farà sì che Application Load Balancer torni al comportamento predefinito.

Abilita la modifica dell'intestazione HTTP per il tuo Application Load Balancer

La modifica dell'intestazione è disattivata per impostazione predefinita e deve essere abilitata su ogni listener.

Per abilitare la modifica dell'intestazione utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Seleziona Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona Application Load Balancer.
4. Nella scheda Listener e regole, seleziona il protocollo e la porta per aprire la pagina dei dettagli del tuo listener.
5. Nella scheda Attributi, seleziona Modifica.

Gli attributi del listener sono organizzati in gruppi. Sceglierai quali funzionalità abilitare.

6. [Listener HTTPS] Nomi di intestazione modificabili mTLS/TLS

   a. Espandi i nomi delle intestazioni modificabili. mTLS/TLS

   b. Abilita le intestazioni della richiesta per modificarle e fornisci i loro nomi. Per ulteriori informazioni, consulta the section called “Rinominare mTLS/TLS le intestazioni”.

7. Aggiungi intestazioni di risposta

   a. Espandi Aggiungi intestazioni di risposta.

   b. Abilita le intestazioni di risposta per aggiungere e fornire valori. Per ulteriori informazioni, consulta the section called “Aggiungi intestazioni di risposta”.

8. Intestazione di risposta del server ALB

   - Abilita o disabilita l'intestazione del server.

9. Scegli Save changes (Salva modifiche).

Per abilitare la modifica dell'intestazione utilizzando il AWS CLI

Utilizzate il modify-listener-attributescomando con i seguenti attributi:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert-Serial-Number.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert-Issuer.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert-Subject.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert-Validity.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert-Leaf.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Modifica il nome dell'intestazione di X-Amzn-Mtls-Clientcert.

`routing.http.request.x_amzn_tls_version.header_name`

Modifica il nome dell'intestazione di X-Amzn-Tls-Version.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Modifica il nome dell'intestazione di X-Amzn-Tls-Cipher-Suite.

`routing.http.response.server.enabled`

Indica se consentire o rimuovere l'intestazione del server di risposta HTTP.

`routing.http.response.strict_transport_security.header_value`

Aggiungi l'intestazione Strict-Transport-Security per informare i browser che è necessario accedere al sito solo tramite HTTPS e che eventuali tentativi futuri di accedervi tramite HTTP devono essere convertiti automaticamente in HTTPS.

`routing.http.response.access_control_allow_origin.header_value`

Aggiungi l'intestazione Access-Control-Allow-Origin per specificare a quali origini è consentito accedere al server.

`routing.http.response.access_control_allow_methods.header_value`

Aggiungi l'intestazione Access-Control-Allow-Methods per specificare quali metodi HTTP sono consentiti quando si accede al server da un'origine diversa.

`routing.http.response.access_control_allow_headers.header_value`

Aggiungi l'intestazione Access-Control-Allow-Headers per specificare quali intestazioni sono consentite durante una richiesta multiorigine.

`routing.http.response.access_control_allow_credentials.header_value`

Aggiungi l'intestazione Access-Control-Allow-Credentials per indicare se il browser deve includere credenziali come i cookie o l'autenticazione nelle richieste tra origini diverse.

`routing.http.response.access_control_expose_headers.header_value`

Aggiungi l'intestazione Access-Control-Expose-Headers per indicare quali intestazioni il browser può esporre al client richiedente.

`routing.http.response.access_control_max_age.header_value`

Aggiungi l'intestazione Access-Control-Max-Age per specificare per quanto tempo i risultati di una richiesta di preflight possono essere memorizzati nella cache, in secondi.

`routing.http.response.content_security_policy.header_value`

Aggiungete l'intestazione Content-Security-Policy per specificare le restrizioni applicate dal browser per ridurre al minimo il rischio di determinati tipi di minacce alla sicurezza.

`routing.http.response.x_content_type_options.header_value`

Aggiungete l'intestazione X-Content-Type-Options per indicare se i tipi MIME pubblicizzati nelle intestazioni Content-Type devono essere seguiti e non modificati.

`routing.http.response.x_frame_options.header_value`

Aggiungete l'intestazione X-Frame-Options per indicare se il browser è autorizzato a renderizzare una pagina in un frame, iframe, embed o oggetto.

Gruppi di destinazioni per gli Application Load Balancer

I gruppi di destinazione instradano le richieste verso singole destinazioni registrate, ad esempio EC2 le istanze, utilizzando il protocollo e il numero di porta specificati. 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.

Ogni gruppo target viene utilizzato per instradare le richieste a uno o più target registrati. Al momento della creazione di ciascuna regola del listener, è necessario specificare un gruppo target e le condizioni. Quando una condizione di una regola viene soddisfatta, il traffico viene instradato al gruppo target corrispondente. 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. È possibile utilizzare ogni gruppo di destinazioni con un solo sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Componenti di Application 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.

Indice

- Crea un gruppo target per il tuo Application Load Balancer
- Aggiorna le impostazioni di integrità per il tuo gruppo target di Application Load Balancer
- Controlli dello stato di salute per i gruppi target di Application Load Balancer
- Modifica gli attributi del gruppo target per il tuo Application Load Balancer
- Registra gli obiettivi con il tuo gruppo target di Application Load Balancer
- Usa le funzioni Lambda come obiettivi di un Application Load Balancer
- Tag per il gruppo target di Application Load Balancer
- Eliminare un gruppo target di Application Load Balancer

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 destinazioni supportano i seguenti protocolli e porte:

- Protocolli: HTTP, HTTPS
- Porte: 1-65535

Quando un gruppo target è configurato con il protocollo HTTPS o utilizza i controlli di integrità HTTPS, se un listener HTTPS utilizza una politica di sicurezza TLS 1.3, la politica di `ELBSecurityPolicy-TLS13-1-0-2021-06` sicurezza verrà utilizzata per le connessioni di destinazione. Altrimenti, viene utilizzata la politica `ELBSecurityPolicy-2016-08` di sicurezza. 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 e le sue destinazioni si trovano 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. Il traffico in uscita non AWS avrà le stesse protezioni e potrebbero essere necessarie ulteriori misure per proteggere ulteriormente il traffico.

Target type (Tipo di destinazione)

Quando si crea un gruppo di destinazioni, occorre specificare il relativo tipo, che determina il tipo di destinazione specificato al momento della registrazione delle destinazioni con tale gruppo di destinazioni. 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`

Le destinazioni sono indirizzi IP.

`lambda`

La destinazione è una funzione Lambda.

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:

- Istanze in un VPC collegato in peering al VPC del sistema di bilanciamento del carico (nella stessa regione o in una regione diversa).
- AWS risorse indirizzabili tramite indirizzo IP e porta (ad esempio database).

- Risorse locali collegate AWS tramite AWS Direct Connect o una Site-to-Site connessione VPN.

> **Note**
>
> Per gli Application Load Balancer distribuiti all'interno di una zona locale, gli `ip` di destinazione devono trovarsi nella stessa zona per ricevere traffico.
> Per ulteriori informazioni, consulta What is AWS Local Zones?

Se i target vengono specificati 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. 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.

Se il tipo di destinazione del gruppo è `lambda`, è possibile registrare una singola funzione Lambda. Quando riceve una richiesta per la funzione Lambda, il sistema di bilanciamento del carico chiama la funzione Lambda. Per ulteriori informazioni, consulta Usa le funzioni Lambda come obiettivi di un Application Load Balancer.

Puoi configurare Amazon Elastic Container Service (Amazon ECS) come destinazione dell'Application Load Balancer. Per ulteriori informazioni, consulta Use an Application Load Balancer for Amazon ECS nella Amazon Elastic Container Service Developer Guide.

Tipo di indirizzo IP

Durante la creazione di un nuovo gruppo di destinazioni, è possibile seleziona il tipo di indirizzo IP del gruppo. In questo modo è possibile controllare la versione IP utilizzata per comunicare con le destinazioni e verificarne lo stato di integrità.

I gruppi target per i tuoi Application Load Balancer supportano i seguenti tipi di indirizzi IP:

`ipv4`

Il load balancer comunica con i target utilizzando. IPv4

`ipv6`

Il sistema di bilanciamento del carico comunica con i target utilizzando. IPv6

Considerazioni

- Il sistema di bilanciamento del carico comunica con le destinazioni in base al tipo di indirizzo IP del gruppo di destinazioni. Le destinazioni di un gruppo IPv4 target devono accettare il IPv4 traffico proveniente dal sistema di bilanciamento del carico e le destinazioni di un gruppo IPv6 target devono accettare il IPv6 traffico proveniente dal sistema di bilanciamento del carico.
- Non è possibile utilizzare un gruppo IPv6 target con un sistema di bilanciamento del `ipv4` carico.
- Non è possibile registrare una funzione Lambda con un gruppo IPv6 target.

Versione del protocollo

Per impostazione predefinita, gli Application Load Balancer inviano richieste alle destinazioni utilizzando HTTP/1.1. È possibile utilizzare la versione del protocollo per inviare richieste alle destinazioni utilizzando HTTP/2 o gRPC.

La tabella seguente riassume il risultato per le combinazioni di protocollo della richiesta e versione del protocollo del gruppo di destinazioni.

Protocollo della richiesta	Versione del protocollo	Risultato
HTTP/1.1	HTTP/1.1	Riuscito
HTTP/2	HTTP/1.1	Riuscito
gRPC	HTTP/1.1	Errore
HTTP/1.1	HTTP/2	Errore
HTTP/2	HTTP/2	Riuscito
gRPC	HTTP/2	Riuscito se le destinazioni supportano gRPC
HTTP/1.1	gRPC	Errore
HTTP/2	gRPC	Riuscito se la richiesta è POST
gRPC	gRPC	Riuscito

Considerazioni sulla versione del protocollo gRPC

- L'unico protocollo dell'ascoltatore supportato è HTTPS.
- L'unico tipo di operazione supportato per le regole dell'ascoltatore è `forward`.
- Gli unici tipi di istanza supportati sono `instance` e `ip`.
- Il sistema di bilanciamento del carico analizza le richieste gRPC e instrada le chiamate gRPC ai gruppi di destinazioni appropriati in base al pacchetto, al servizio e al metodo.
- Il sistema di bilanciamento del carico supporta lo streaming unario lato client, lo streaming lato server e lo streaming bidirezionale.
- È necessario fornire un metodo di controllo dell'integrità personalizzato con il formato `/package.service/method`.
- È necessario specificare i codici di stato gRPC da utilizzare durante la verifica di una risposta positiva ricevuta da una destinazione.
- Non puoi usare le funzioni Lambda come obiettivi.

Considerazioni sulla versione del protocollo HTTP/2

- L'unico protocollo dell'ascoltatore supportato è HTTPS.
- L'unico tipo di operazione supportato per le regole dell'ascoltatore è `forward`.
- Gli unici tipi di istanza supportati sono `instance` e `ip`.
- Il sistema di bilanciamento del carico supporta lo streaming unario lato client, lo streaming lato server e lo streaming bidirezionale. Il numero massimo di stream per connessione HTTP/2 client è 128.

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

Se stai eseguendo la registrazione dei target 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 ulteriori informazioni, consulta Collegare un sistema di bilanciamento del carico al gruppo Auto Scaling nella Amazon Auto Scaling User EC2 Guide.

Limiti

- Non è possibile registrare gli indirizzi IP di un altro Application Load Balancer nello stesso VPC. Se l'altro Application Load Balancer si trova in un VPC in peering al VPC del sistema di bilanciamento del carico, è possibile registrarne gli indirizzi IP.
- Non puoi registrare le istanze in base all'ID dell'istanza se si trovano in un VPC collegato al VPC del sistema di bilanciamento del carico (stessa regione o regione diversa). È possibile registrare queste istanze in base all'indirizzo IP.

Attributi dei gruppi di destinazione

È possibile configurare un gruppo target modificandone gli attributi. Per ulteriori informazioni, consulta Modifica gli attributi del gruppo target.

I seguenti attributi del gruppo di destinazioni sono supportati se il tipo di gruppo di destinazioni è `instance` o `ip`:

`deregistration_delay.timeout_seconds`

Il tempo che Elastic Load Balancing deve aspettare prima di annullare la registrazione di una destinazione. L'intervallo è compreso tra 0 e 3600 secondi. Il valore predefinito è 300 secondi.

`load_balancing.algorithm.type`

L'algoritmo di bilanciamento del carico determina il modo in cui il sistema di bilanciamento del carico seleziona le destinazioni durante l'instradamento delle richieste. Il valore è `round_robin`e `least_outstanding_requests`, o `weighted_random`. Il valore predefinito è `round_robin`.

`load_balancing.algorithm.anomaly_mitigation`

Disponibile solo quando lo `load_balancing.algorithm.type` è `weighted_random`. Indica se la mitigazione delle anomalie è abilitata. Il valore è `on` o `off`. Il valore predefinito è `off`.

`load_balancing.cross_zone.enabled`

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

`slow_start.duration_seconds`

L'intervallo di tempo in secondi durante il quale il sistema di bilanciamento del carico invia a una destinazione appena registrata una quantità di traffico in aumento lineare verso il gruppo di destinazioni. L'intervallo è compreso tra 30 e 900 secondi (15 minuti). L'impostazione predefinita è 0 secondi (disattivata).

`stickiness.enabled`

Indica se le sticky session sono abilitate. Il valore è `true` o `false`. Il valore predefinito è `false`.

`stickiness.app_cookie.cookie_name`

Il nome del cookie dell'applicazione. Il nome del cookie dell'applicazione non può avere i seguenti prefissi:`AWSALB`,`AWSALBAPP`, oppure`AWSALBTG`; sono riservati all'uso da parte del load balancer.

`stickiness.app_cookie.duration_seconds`

Il periodo di scadenza dei cookie basati sull'applicazione, in secondi. Al termine di questo periodo, il cookie è considerato obsoleto. Il valore minimo è 1 secondo e il valore massimo è 7 giorni (604800 secondi). Il valore predefinito è 1 giorno (86400 secondi).

`stickiness.lb_cookie.duration_seconds`

Il periodo di scadenza dei cookie basati sulla durata, in secondi. Al termine di questo periodo, il cookie è considerato obsoleto. Il valore minimo è 1 secondo e il valore massimo è 7 giorni (604800 secondi). Il valore predefinito è 1 giorno (86400 secondi).

`stickiness.type`

Il tipo di persistenza. I valori possibili sono `lb_cookie` e `app_cookie`.

`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 il nodo come non integro nel DNS, in modo che il traffico venga indirizzato solo verso nodi integri. I valori possibili sono `off` o un numero intero compreso tra 1 e il numero massimo di destinazioni. Quando `off` il DNS fail away è disabilitato, il che significa che anche se tutte le destinazioni del gruppo di destinazione non sono integre, il nodo non viene rimosso dal DNS. 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 il nodo come non integro nel DNS, in modo che il traffico venga indirizzato solo verso nodi integri. I valori possibili sono `off` o un numero intero compreso tra 1 e 100. Quando `off` il DNS fail away è disabilitato, il che significa che anche se tutte le destinazioni del gruppo di destinazione non sono integre, il nodo non viene rimosso dal DNS. Il valore predefinito è `off`.

`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`.

Il seguente attributo del gruppo di destinazioni è supportato se il tipo di gruppo di destinazioni è `lambda`:

`lambda.multi_value_headers.enabled`

Indica se le intestazioni di richieste e risposte scambiate tra il sistema di bilanciamento del carico e la funzione Lambda includono array di valori o stringhe. I valori possibili sono `true` o `false`. Il valore predefinito è `false`. Per ulteriori informazioni, consulta Intestazioni con più valori.

Algoritmi di routing

Un algoritmo di routing è il metodo utilizzato dal load balancer per determinare quali destinazioni riceveranno le richieste. L'algoritmo di routing round robin viene utilizzato di default per indirizzare le richieste a livello di gruppo target. In base alle esigenze dell'applicazione, sono disponibili anche le richieste meno in sospeso e gli algoritmi di routing casuale ponderati. Un gruppo target può avere solo un algoritmo di routing attivo alla volta, tuttavia l'algoritmo di routing può essere aggiornato ogni volta che è necessario.

Se abiliti le sessioni permanenti, l'algoritmo di routing selezionato viene utilizzato per la selezione iniziale del target. Le richieste future dello stesso client verranno inoltrate allo stesso target, ignorando l'algoritmo di routing selezionato.

Round robin

- L'algoritmo di routing round robin indirizza le richieste in modo uniforme tra i target sani del gruppo target, in ordine sequenziale.
- Questo algoritmo viene comunemente utilizzato quando le richieste ricevute hanno una complessità simile, le destinazioni registrate hanno capacità di elaborazione simili o se è necessario distribuire equamente le richieste tra le destinazioni.

Richieste meno rilevanti

- L'algoritmo di routing delle richieste con il minor numero di richieste in sospeso indirizza le richieste verso le destinazioni con il minor numero di richieste in corso.
- Questo algoritmo viene comunemente utilizzato quando le richieste ricevute variano in complessità e le destinazioni registrate variano nella capacità di elaborazione.
- Quando un sistema di bilanciamento del carico che supporta HTTP/2 utilizza obiettivi che supportano solo HTTP/1.1, converte la richiesta in più richieste HTTP/1.1. In questa configurazione, l'algoritmo di richieste meno in sospeso tratterà ogni richiesta HTTP/2 come richiesta multipla.

- Durante l'utilizzo WebSockets, la destinazione viene selezionata utilizzando l'algoritmo delle richieste meno in sospeso. Una volta selezionato, il load balancer crea una connessione alla destinazione e invia tutti i messaggi tramite questa connessione.
- L'algoritmo di routing delle richieste meno in sospeso non può essere utilizzato con la modalità di avvio lento.

Ponderato casualmente

- L'algoritmo di routing casuale ponderato indirizza le richieste in modo uniforme tra i target sani del gruppo target, in ordine casuale.
- Questo algoritmo supporta la mitigazione delle anomalie Automatic Target Weights (ATW).
- L'algoritmo di routing casuale ponderato non può essere utilizzato con la modalità di avvio lento.
- L'algoritmo di routing casuale ponderato non può essere utilizzato con sessioni permanenti.

Modifica l'algoritmo di routing di un gruppo target

Puoi modificare l'algoritmo di routing per il tuo gruppo target in qualsiasi momento.

Per modificare l'algoritmo di routing utilizzando la nuova console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina dei dettagli del gruppo target, nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica gli attributi del gruppo target, nella sezione Configurazione del traffico, in Algoritmo di bilanciamento del carico, scegli Round robin, Least Outstanding requests o Weighted random.
6. Scegli Save changes (Salva modifiche).

Per modificare l'algoritmo di routing utilizzando AWS CLI

Utilizzare il modify-target-group-attributescomando con l'`load_balancing.algorithm.type`attributo.

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. Ciò migliora la disponibilità dell'applicazione.

Indice

Operazioni per lo stato di non integrità

È possibile configurare soglie di integrità per le seguenti operazioni:

- Failover DNS: quando gli obiettivi integri in una zona scendono al di sotto della soglia, nel DNS contrassegniamo gli indirizzi IP del nodo di bilanciamento del carico relativo alla zona come non integri. Pertanto, quando i client risolvono il nome DNS del sistema di bilanciamento del carico, il traffico viene instradato solo nelle zone integre.
- Failover di routing: quando gli obiettivi integri in una zona scendono al di sotto della soglia, il load balancer invia il traffico a tutte le destinazioni disponibili per il nodo 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

- Non è possibile utilizzare questa funzionalità con i gruppi di destinazioni quando la destinazione è una funzione Lambda. Se l'Application Load Balancer è la destinazione di un Network Load Balancer o Global Accelerator, non configurare una soglia per il failover DNS.

- 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 per i gruppi target di Application Load Balancer.
- Quando si verifica il failover DNS, influisce su tutti i gruppi target associati al load balancer. 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, rimuoviamo gli indirizzi IP delle zone non integre dal nome host DNS del load balancer. 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).
- Con il failover DNS, se ci sono più gruppi target collegati a un Application Load Balancer e un gruppo target non è integro in una zona, i controlli di integrità del DNS hanno esito positivo se almeno un altro gruppo target è integro in quella zona.
- 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.

Monitoraggio

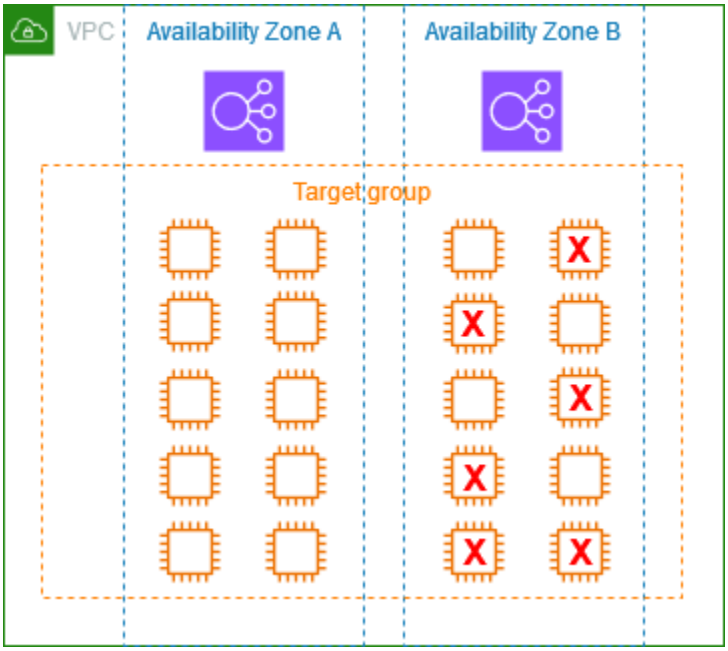
Per monitorare lo stato dei gruppi target, consulta le CloudWatch metriche relative allo stato del gruppo target.

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.

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.

Come funziona Value Target Health

- Se la valutazione dello stato dell'obiettivo è impostata `Yes` su un record di alias per un Application Load Balancer, Route 53 valuta lo stato della risorsa specificata dal valore. `alias target` Route 53 utilizza i controlli di integrità del gruppo target.
- Se tutti i gruppi target collegati a un Application Load Balancer sono integri, Route 53 contrassegna il record di alias come integro. Se hai configurato una soglia per un gruppo target e questo raggiunge la soglia, supera i controlli di integrità. Altrimenti, se un gruppo target contiene almeno un bersaglio sano, supera i controlli sanitari. Se i controlli sanitari vengono superati, Route 53 restituisce i record in base alla politica di routing. Se viene utilizzata una politica di routing di failover, Route 53 restituisce il record principale.
- Se uno dei gruppi target collegati a un Application Load Balancer non è integro, il record di alias non supera il controllo di integrità della Route 53 (fail-open). Se si utilizza assessment target health, la policy di routing di failover reindirizza il traffico verso la risorsa secondaria.
- Se tutti i gruppi target collegati a un Application Load Balancer sono vuoti (nessun target), Route 53 considera il record non integro (fail-open). Se si utilizza assessment target health, la policy di routing di failover reindirizza il traffico verso la risorsa secondaria.

Per ulteriori informazioni, consulta la sezione Utilizzo delle soglie di integrità del gruppo target del sistema di bilanciamento del carico per migliorare la disponibilità nel AWS blog e Configurazione del failover DNS nella Amazon Route 53 Developer Guide.

Crea un gruppo target per il tuo Application Load Balancer

Puoi registrare le destinazioni con un gruppo di destinazioni. 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 le destinazioni in un gruppo, specifica il gruppo in un'operazione al momento della creazione di un listener oppure crea una regola per il listener. Per ulteriori informazioni, consulta Regole dei listener. È possibile specificare lo stesso gruppo di destinazioni in più ascoltatori, che però devono appartenere allo stesso Application Load Balancer. Per utilizzare un gruppo di destinazioni con un sistema di bilanciamento del carico, è necessario verificare che tale gruppo non sia utilizzato da un ascoltatore per nessun altro sistema di bilanciamento del carico.

È possibile aggiungere o rimuovere target dal gruppo target in qualsiasi momento. Per ulteriori informazioni, consulta Registra gli obiettivi con il tuo gruppo target di Application Load Balancer. È anche possibile modificare le impostazioni di controllo dello stato per il gruppo target. Per ulteriori informazioni, consulta Aggiornare le impostazioni del controllo dello stato di un gruppo target di Application Load Balancer.

Per creare un gruppo target tramite la console

1. Apri la EC2 console Amazon 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. In Scegli tipo di target, seleziona Istanze per registrare le destinazioni per ID istanza, Indirizzi IP per registrare le destinazioni per indirizzo IP o Funzione Lambda per registrare una funzione Lambda come destinazione.
5. Per Nome gruppo di destinazioni digitare un nome per il gruppo di destinazioni. 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.
6. (Facoltativo) Per Protocollo e Porta, modificare i valori predefiniti come necessario.
7. Se il tipo di destinazione è Istanze o indirizzi IP, scegli IPv4o IPv6come tipo di indirizzo IP, altrimenti vai al passaggio successivo.

   Tieni presente che in questo gruppo di destinazioni possono essere incluse solo le destinazioni che hanno il tipo di indirizzo IP selezionato. Il tipo di indirizzo IP non può essere modificato dopo la creazione del gruppo di destinazione.
8. Per VPC, selezionare un cloud privato virtuale (VPC, Virtual Private Cloud). Tieni presente che per i tipi di destinazione degli indirizzi IP, i tipi di destinazione VPCs disponibili per la selezione sono quelli che supportano il tipo di indirizzo IP scelto nel passaggio precedente.
9. (Facoltativo) Per Versione del protocollo, modifica i valori predefiniti secondo necessità.

10. (Facoltativo) Nella sezione Controlli dell'integrità, modifica le impostazioni predefinite in base alle esigenze.
11. Se il tipo di destinazione è Funzione Lambda, puoi abilitare i controlli dell'integrità selezionando Abilita nella sezione Controlli dell'integrità.
12. (Facoltativo) Aggiungere uno o più tag come illustrato di seguito:
    a. Espandere la sezione Tag.
    b. Selezionare Aggiungi tag.
    c. Immetti una chiave e un valore per il tag.
13. Scegli Next (Successivo).
14. (Facoltativo) Aggiungere una o più destinazioni come illustrato di seguito:
    - Se il tipo di destinazione è Istanze, seleziona una o più istanze, inserisci una o più porte e in seguito scegli Includi come in sospeso di seguito.

      Nota: le istanze devono avere un IPv6 indirizzo principale assegnato per essere registrate presso un gruppo IPv6 target.
    - Se il tipo di destinazione è Indirizzi IP, procedere nel seguente modo:
      a. Seleziona un rete VPC dall'elenco oppure scegli Altri indirizzi IP privati.
      b. Inserisci manualmente l'indirizzo IP oppure trova l'indirizzo utilizzando i dettagli dell'istanza. È possibile inserire fino a cinque indirizzi IP alla volta.
      c. Inserire le porte per l'instradamento del traffico verso l'indirizzo IP specificato.
      d. Seleziona Includi come in sospeso di seguito.
    - Se il tipo di destinazione è una Funzione Lambda, specifica una singola funzione Lambda oppure salta questo passaggio e specificane uno in seguito.
15. Scegliere Crea gruppo target.
16. (Facoltativo) È possibile specificare il gruppo di destinazione in una regola listener. Per ulteriori informazioni, vedere Regole listener.

Per creare un gruppo target utilizzando il AWS CLI

Utilizzate il create-target-groupcomando per creare il gruppo target, il comando add-tags per etichettare il gruppo target e il comando register-targets per aggiungere obiettivi.

Aggiorna le impostazioni di integrità per il tuo gruppo target di Application Load Balancer

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 EC2 console Amazon 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. Scegli Save changes (Salva 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 illustra come impostare la soglia di integrità per entrambe le operazioni per gli stati di non integrità al 50%.

```
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
```

Controlli dello stato di salute per i gruppi target di Application Load Balancer

L'Application Load Balancer invia periodicamente delle richieste alle destinazioni registrate per testare il loro stato. Questi test sono chiamati controlli dello stato.

Ogni nodo del sistema di bilanciamento del carico instrada le richieste solamente sui target integri all'interno delle zone di disponibilità abilitate per il sistema di bilanciamento del carico. Ogni nodo del sistema di bilanciamento del carico controlla lo stato dei target, utilizzando le impostazioni di controllo dello stato per i gruppi di target con i quali il target è registrato. Una volta che un target viene registrato, deve essere sottoposto a un controllo dello stato per essere considerato integro. Dopo il completamento di ciascun controllo dello stato, il nodo del sistema di bilanciamento del carico chiude la connessione definita per il controllo dello stato.

Se un gruppo di destinazione contiene solo destinazioni non integre registrate, il sistema di bilanciamento del carico instrada le richieste a tutte le destinazioni, a prescindere dal loro stato di integrità. Questo significa che tutte le destinazioni non superano i controlli dell'integrità allo stesso tempo in tutte le zone di disponibilità abilitate, nel sistema di bilanciamento del carico si verifica un fail open. L'effetto del fail-open è quello di consentire il traffico verso tutte le destinazioni in tutte le zone di disponibilità abilitate, a prescindere dal loro stato di integrità, sulla base dell'algoritmo del sistema di bilanciamento del carico.

I controlli sanitari non supportano WebSockets.

Per ulteriori informazioni, consulta the section called “Integrità del gruppo di destinazione”.

Impostazioni del controllo dello stato

È possibile configurare controlli dell'integrità per le destinazioni all'interno di un gruppo di destinazioni come viene descritto nella tabella seguente. I nomi delle impostazioni utilizzati nella tabella sono i nomi usati nell'API. Il load balancer invia una richiesta di controllo dello stato a ciascun target registrato ogni HealthCheckIntervalSecondssecondo, utilizzando la porta, il protocollo e il percorso di controllo dello stato specificati. Ogni richiesta di controllo dello stato è indipendente e il risultato dura per l'intero intervallo. Il tempo di risposta del target non influenza l'intervallo per la richiesta di controllo dello stato successiva. Se i controlli di integrità superano gli errori UnhealthyThresholdCountconsecutivi, il load balancer mette fuori servizio l'obiettivo. Quando i controlli di integrità superano i successi HealthyThresholdCountconsecutivi, il load balancer rimette in servizio l'obiettivo.

Tieni presente che quando annulli la registrazione di un obiettivo, questa diminuisce HealthyHostCountma non aumenta. UnhealthyHostCount

Impostazione	Descrizione
HealthCheckProtocol	Il protocollo utilizzato dal load balancer durante l'esecuzione dei controlli dello stato sui target. Per gli Application Load Balancer i protocolli possibili sono HTTP e HTTPS. L'impostazione predefinita è il protocollo HTTP. Questi protocolli utilizzano il metodo HTTP GET per inviare richieste di controllo dell'integrità.
HealthCheckPort	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.
HealthCheckPath	La destinazione dei controlli dell'integrità sulle destinazioni. Se la versione del protocollo è HTTP/1.1 o HTTP/2, specificare un URI valido (/path?query). Il valore di default è /. Se la versione del protocollo è gRPC, specifica re il percorso di un metodo personalizzato per il controllo dell'integrità con il formato `/package.service/method` . Il valore predefinito è `/AWS.ALB/healthcheck` .
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. L'impostazione predefinita è 5 secondi se il tipo di destinazione

Impostazione	Descrizione
	è `instance` oppure `ip` e 30 secondi se il tipo di destinazione è `lambda`.
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. L'impostazione predefinita è 30 secondi se il tipo di destinazione è `instance` oppure `ip` e 35 secondi se il tipo di destinazione è `lambda`.
HealthyThresholdCount	Il numero di controlli dello stato andati a buon fine consecutivi necessari prima di considerare integro un target non integro. L'intervallo è compreso tra 2 e 10. Il predefinito è 5.
UnhealthyThresholdCount	Numero di controlli dello stato consecutivi non andati a buon fine necessari prima di considerare un target non integro. L'intervallo è compreso tra 2 e 10. Il valore predefinito è 2.

Impostazione	Descrizione
Matcher	I codici da utilizzare durante la verifica di una risposta con esito positivo ricevuta da una destinazione. Tali codici si chiamano Codici di successo nella console. Se la versione del protocollo è HTTP/1.1 o HTTP/2, i valori possibili sono compresi tra 200 e 499. Puoi specificare più valori (ad esempio "200,202") o un intervallo di valori (ad esempio "200-299"). Il valore predefinito è 200. Se la versione del protocollo è gRPC, i valori possibili sono compresi tra 0 e 99. Puoi specificare più valori (ad esempio "0,1") o un intervallo di valori (ad esempio "0-5"). Il valore predefinito è 12.

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. Prima che un target possa ricevere richieste dal sistema di bilanciamento del carico, deve superare i controlli dello stato iniziali. Una volta che il target ha superato i controlli dello stato iniziali, il suo stato è `Healthy`.

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.

Valore	Descrizione
	Codici di motivo correlati: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	Il target è integro. Codici di motivo correlati: Nessuno
`unhealthy`	Il target non ha risposto a un controllo di stato o il controllo dello stato non è andato a buon fine. Codici di motivo correlati: `Target.ResponseCodeMismatch` | `Target.Timeout` | `Target.FailedHealthChecks` | `Elb.InternalError`
`unused`	La destinazione non è registrata con un gruppo di destinazione, il gruppo di destinazione non è utilizzato in una regola del listener, la destinazione è in una zona di disponibilità non abilitata oppure è nello stato arrestato o terminato. Codici di motivo correlati: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`
`draining`	Il target viene revocato e la connection draining è in corso. Codice di motivo correlato: `Target.DeregistrationInProgress`
`unavailable`	I controlli dello stato sono disabilitati per il gruppo di destinazione. Codice di motivo correlato: `Target.HealthCheckDisabled`

Codici di motivo di controllo dello stato

Se lo stato di una destinazione è un valore diverso da `Healthy`, l'API restituisce un codice di motivo e una descrizione del problema e la console visualizza la stessa descrizione. I codici di motivo che iniziano con `Elb` vengono creati nella parte relativa al sistema di bilanciamento del carico e i codici di motivo che iniziano con `Target` vengono creati nella parte relativa ai target. Per ulteriori informazioni sulle possibili cause per cui un controllo dell'integrità non va a buon fine, consulta Risoluzione dei problemi.

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
`Target.FailedHealthChecks`	Controlli dello stato non andati a buon fine
`Target.HealthCheckDisabled`	I controlli dello stato sono disabilitati
`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.

Codice di motivo	Descrizione
`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
`Target.ResponseCodeMismatch`	I controlli dello stato non sono andati a buon fine con questi codici: [codice]
`Target.Timeout`	Richiesta scaduta

Verifica lo stato dei tuoi obiettivi di Application Load Balancer

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

Per controllare lo stato dei target utilizzando la console

1. Apri la EC2 console Amazon 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 Target, la colonna Stato indica lo stato di ogni destinazione.
5. Se lo stato ha un valore diverso da `Healthy`, la colonna Dettagli dello stato contiene ulteriori informazioni. Per assistenza con i controlli dell'integrità che non vanno a buon fine, consulta Risoluzione dei problemi.

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

Utilizza il comando describe-target-health. L'output di questo comando contiene lo stato del target. Se lo stato è un valore diverso da `Healthy`, il risultato comprende anche un codice di motivo.

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.

Aggiornare le impostazioni del controllo dello stato di un gruppo target di Application Load Balancer

Puoi aggiornare le impostazioni del controllo sanitario per il tuo gruppo target in qualsiasi momento.

Per aggiornare le impostazioni del controllo sanitario di un gruppo target utilizzando la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, nella sezione Impostazioni del controllo dell'integrità, scegli Modifica.
5. Nella pagina Modifica le impostazioni del controllo dell'integrità, modificare le impostazioni secondo necessità, quindi scegliere Salva modifiche.

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

Utilizza il comando modify-target-group.

Modifica gli attributi del gruppo target per il tuo Application Load Balancer

Dopo aver creato un gruppo target per l'Application Load Balancer, puoi modificarne gli attributi del gruppo target.

Attributi dei gruppi di destinazione

- Ritardo di annullamento della registrazione
- Modalità di avvio lento
- Bilanciamento del carico tra zone per i gruppi target di Application Load Balancer
- Automatic Target Weights (ATW)
- Sessioni permanenti per l'Application Load Balancer

Ritardo di annullamento della registrazione

Elastic Load Balancing smette di inviare le richieste alle destinazioni per le quali è in corso l'annullamento della registrazione. Per impostazione predefinita, Elastic Load Balancing attende 300 secondi prima di completare l'annullamento della registrazione, favorendo il completamento delle richieste in transito verso la destinazione. Per modificare il tempo di attesa di Elastic Load Balancing, aggiorna il valore di ritardo dell'annullamento della registrazione.

Lo stato iniziale di un target di cui viene annullata la registrazione è `draining`. Allo scadere del tempo richiesto per l'annullamento della registrazione, tale processo viene completato e lo stato della destinazione diventa `unused`. Se fa parte di un gruppo con dimensionamento automatico, la destinazione può essere terminata e sostituita.

Se una destinazione la cui registrazione è in fase di annullamento non ha richieste in transito né connessioni attive, Elastic Load Balancing completa immediatamente il processo di annullamento senza attendere la scadenza del tempo previsto. Tuttavia, anche se l'annullamento della registrazione della destinazione è completato, lo stato della destinazione risulta `draining` fino allo scadere del timeout previsto per il completamento del processo. Dopo la scadenza del timeout, la destinazione passa allo stato `unused`.

Se una destinazione la cui registrazione è in fase di annullamento termina la connessione prima dello scadere del tempo previsto per il processo, il client riceve un errore di livello 500.

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

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, modificare il valore di Intervallo annullamento registrazione secondo necessità.
6. Scegli Save changes (Salva modifiche).

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

Utilizzate il modify-target-group-attributescomando con l'attributo. `deregistration_delay.timeout_seconds`

Modalità di avvio lento

Per impostazione predefinita, una destinazione inizia a ricevere la quantità completa di richieste non appena viene registrata con un gruppo di destinazioni e supera un controllo dello stato iniziale. Grazie alla modalità di avvio lento, le destinazioni hanno il tempo di prepararsi prima che il sistema di bilanciamento del carico invii loro una quantità completa di richieste.

Dopo aver abilitato l'avvio lento per un gruppo di destinazioni, le destinazioni entrano in modalità avvio lento quando vengono considerati integre dal gruppo di destinazioni. Una destinazione in modalità di avvio lento esce dalla modalità di avvio lento quando scade il periodo di durata dell'avvio lento configurato o se la destinazione diventa non integra. Il sistema di bilanciamento del carico aumenta in modo lineare il numero di richieste che è in grado di inviare a una destinazione nella modalità di avvio lento. Una volta che una destinazione integra è uscita dalla modalità di avvio lento, il sistema di bilanciamento del carico può inviarle una quantità completa di richieste.

Considerazioni

- Quando abiliti la modalità di avvio lento per un gruppo di destinazioni, le destinazioni integre registrate con il gruppo non entrano in questa modalità.
- Quando abiliti la modalità di avvio lento per un gruppo di destinazioni vuoto e quindi registri destinazioni con un'unica operazione, tali destinazioni non entrano in questa modalità. Le destinazioni appena registrate entrano nella modalità di avvio lento solo se è presente almeno una destinazione integra registrata che non si trova in questa modalità.
- Se annulli la registrazione di una destinazione che si trova nella modalità di avvio lento, la destinazione esce da questa modalità. Se si registra di nuovo la stessa destinazione, essa entra in modalità di avvio lento quando viene considerata integra dal gruppo di destinazione.
- Se una destinazione in modalità di avvio lento diventa non integra esce dalla modalità di avvio lento. Quando diventa integra, entra di nuovo in modalità di avvio lento.
- Non è possibile abilitare la modalità di avvio lento quando si utilizzano le richieste meno in sospeso o gli algoritmi di routing casuale ponderati.

Per aggiornare il valore della durata dell'avvio lento tramite la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, modificare il valore di Durata avvio lento secondo necessità. Per disabilitare la modalità di avvio lento, impostare la durata su 0.
6. Scegli Save changes (Salva modifiche).

Per aggiornare il valore della durata dell'avvio lento utilizzando il AWS CLI

Utilizzate il modify-target-group-attributescomando con l'`slow_start.duration_seconds`attributo.

Bilanciamento del carico tra zone per i gruppi target di Application Load Balancer

I nodi del sistema di bilanciamento del carico distribuiscono le richieste dei client alle destinazioni registrate. Se il bilanciamento del carico tra zone è attivato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico tra le destinazioni registrate in tutte le zone di disponibilità registrate. Se il bilanciamento del carico tra zone è disattivato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella propria zona di disponibilità. Questo potrebbe verificarsi se i domini con errori di zona vengono preferiti a quelli regionali, garantendo che una zona integra non venga influenzata da una zona non integra, oppure per ottenere miglioramenti di latenza generali.

Con gli Application Load Balancer, il bilanciamento del carico tra zone è sempre attivato a livello di sistema di bilanciamento del carico e non può essere disattivato. Per i gruppi di destinazioni, l'impostazione predefinita è l'utilizzo dell'impostazione del sistema di bilanciamento del carico, ma è possibile sovrascrivere tale impostazione disattivando esplicitamente il bilanciamento del carico tra zone a livello di gruppo di destinazioni.

Considerazioni

- La persistenza della destinazione non è supportata quando il bilanciamento del carico tra zone è disattivato.
- Le funzioni Lambda non sono supportate come destinazioni quando il bilanciamento del carico tra zone è disattivato.
- Il tentativo di disattivazione del bilanciamento del carico tra zone tramite l'API `ModifyTargetGroupAttributes` restituisce un errore se una qualsiasi delle destinazioni ha il parametro `AvailabilityZone` impostato su `all`.

- Durante la registrazione delle destinazioni, il parametro `AvailabilityZone` è obbligatorio. Valori specifici per le zone di disponibilità sono consentiti solo quando il bilanciamento del carico tra zone è disattivato. In caso contrario, il parametro viene ignorato e gestito come `all`.

Best practice

- Pianificare una sufficiente capacità di destinazione in tutte le zone di disponibilità che si prevede di utilizzare, per gruppo di destinazioni. Se non è possibile pianificare una capacità sufficiente per tutte le zone di disponibilità partecipanti, consigliamo di mantenere attivo il bilanciamento del carico tra zone.
- Quando si configura un Application Load Balancer con più gruppi di destinazioni, assicurarsi che tutti i gruppi di destinazioni partecipino nella stessa zona di disponibilità, all'interno della regione configurata. In questo modo si evita che la zona di disponibilità sia vuota quando il bilanciamento del carico tra zone è disattivato, il che provoca un errore 503 per tutte le richieste HTTP che entrano nella zona di disponibilità vuota.
- Evitare di creare sottoreti vuote. Gli Application Load Balancer espongono gli indirizzi IP zonali tramite DNS per le sottoreti vuote, il che provoca errori 503 per le richieste HTTP.
- In alcuni casi, un gruppo di destinazioni in cui il bilanciamento del carico è disattivato dispongono di capacità pianificata sufficiente per ogni zona di disponibilità, ma tutte le destinazioni in una zona di disponibilità diventano non integre. Quando è presente almeno un gruppo di destinazioni in cui tutte le destinazioni sono non integre, gli indirizzi IP del nodo del sistema di bilanciamento del carico vengono rimosse dal DNS. Una volta che il gruppo di destinazioni ha almeno una destinazione integra, gli indirizzi IP vengono ripristinate nel DNS.

Disattivazione del bilanciamento del carico tra zone

È possibile disattivare il bilanciamento del carico tra zone per i gruppi di destinazioni dell'Application Load Balancer in qualsiasi momento.

Per disattivare il bilanciamento del carico tra zone tramite la console

1. Apri la EC2 console Amazon 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 visualizzarne i dettagli.
4. Nella scheda Attributi, seleziona Modifica.

5. Nella pagina Modifica attributi dei gruppi di destinazione, seleziona Disattivato per Bilanciamento del carico tra zone.
6. Scegli Save changes (Salva modifiche).

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

Utilizzate il modify-target-group-attributescomando e impostate l'`load_balancing.cross_zone.enabled`attributo su. `false`

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=false
```

Di seguito è riportata una risposta di esempio:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "false"
        },
    ]
}
```

Attivazione del bilanciamento del carico tra zone

È possibile attivare il bilanciamento del carico tra zone per i gruppi di destinazioni dell'Application Load Balancer in qualsiasi momento. L'impostazione del bilanciamento del carico tra zone a livello di gruppo di destinazioni sovrascrive l'impostazione a livello di sistema di bilanciamento del carico.

Per attivare il bilanciamento del carico tra zone tramite la console

1. Apri la EC2 console Amazon 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 visualizzarne i dettagli.
4. Nella scheda Attributi, seleziona Modifica.
5. Nella pagina Modifica attributi dei gruppi di destinazione, seleziona Attivato per Bilanciamento del carico tra zone.
6. Scegli Save changes (Salva modifiche).

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

Utilizzate il modify-target-group-attributescomando e impostate l'`load_balancing.cross_zone.enabled`attributo su. `true`

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=true
```

Di seguito è riportata una risposta di esempio:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "true"
        },
    ]
}
```

Automatic Target Weights (ATW)

Automatic Target Weights (ATW) monitora costantemente i target che eseguono le applicazioni, rilevando deviazioni significative delle prestazioni, note come anomalie. ATW offre la possibilità di regolare dinamicamente la quantità di traffico indirizzata verso gli obiettivi, attraverso il rilevamento delle anomalie dei dati in tempo reale.

Automatic Target Weights (ATW) esegue automaticamente il rilevamento delle anomalie su ogni Application Load Balancer del tuo account. Quando vengono identificati obiettivi anomali, ATW può tentare automaticamente di stabilizzarli riducendo la quantità di traffico che vengono instradati, operazione nota come mitigazione delle anomalie. ATW ottimizza continuamente la distribuzione del traffico per massimizzare le percentuali di successo per target e ridurre al minimo le percentuali di fallimento del gruppo target.

Considerazioni:

- Il rilevamento delle anomalie attualmente monitora i codici di risposta HTTP 5xx provenienti dagli obiettivi e gli errori di connessione verso di essi. Il rilevamento delle anomalie è sempre attivo e non può essere disattivato.
- ATW non è supportato quando si utilizza Lambda come destinazione.

Rilevamento anomalie

Il rilevamento delle anomalie ATW monitora tutti gli obiettivi che mostrano una deviazione significativa nel comportamento rispetto agli altri bersagli del rispettivo gruppo target. Queste deviazioni, chiamate anomalie, vengono determinate confrontando la percentuale di errori di un obiettivo con la percentuale di errori di altri target del gruppo target. Questi errori possono essere sia errori di connessione che codici di errore HTTP. Gli obiettivi che riportano risultati significativamente più alti rispetto ai loro omologhi vengono quindi considerati anomali.

Il rilevamento delle anomalie richiede un minimo di tre obiettivi sani nel gruppo target. Quando un target è registrato in un gruppo target, deve prima superare i controlli di integrità per iniziare a ricevere traffico. Una volta che il bersaglio riceve il bersaglio, ATW inizia a monitorarlo e pubblica continuamente il risultato dell'anomalia. Per i bersagli senza anomalie, il risultato dell'anomalia è. `normal` Per gli obiettivi con anomalie, il risultato dell'anomalia è. `anomalous`

Il rilevamento delle anomalie ATW funziona indipendentemente dai controlli sanitari del gruppo target. Un bersaglio può superare tutti i controlli sanitari del gruppo bersaglio, ma essere comunque contrassegnato come anomalo a causa di un elevato tasso di errore. Il fatto che i bersagli diventino anomali non influisce sullo stato dei controlli sanitari del gruppo bersaglio.

Stato di rilevamento delle anomalie

ATW pubblica continuamente lo stato dei rilevamenti di anomalie che esegue sugli obiettivi. È possibile visualizzare lo stato corrente in qualsiasi momento utilizzando o. AWS Management Console AWS CLI

Per visualizzare lo stato di rilevamento delle anomalie utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina dei dettagli dei gruppi target, scegli la scheda Target.
5. Nella tabella Obiettivi registrati, è possibile visualizzare lo stato di anomalia di ciascun target nella colonna Risultati del rilevamento delle anomalie.

   Se non è stata rilevata alcuna anomalia, il risultato è. `normal`

   Se sono state rilevate anomalie, il risultato è. `anomalous`

Per visualizzare i risultati del rilevamento delle anomalie utilizzando AWS CLI

Utilizzare il describe-target-healthcomando con il valore dell'`Include.member.`Nattributo `AnomalyDetection` impostato su.

Attenuazione delle anomalie

> **Important**
>
> La funzione di mitigazione delle anomalie di ATW è disponibile solo quando si utilizza l'algoritmo di routing casuale Weighted.

La mitigazione delle anomalie ATW allontana automaticamente il traffico dagli obiettivi anomali, offrendo loro l'opportunità di riprendersi.

Durante la mitigazione:

- ATW regola periodicamente la quantità di traffico indirizzata verso obiettivi anomali. Attualmente, il periodo è ogni cinque secondi.
- ATW riduce la quantità di traffico indirizzata verso obiettivi anomali alla quantità minima richiesta per eseguire la mitigazione delle anomalie.
- Agli obiettivi che non vengono più rilevati come anomali verrà indirizzato gradualmente più traffico verso gli obiettivi, fino a raggiungere la parità con gli altri obiettivi normali del gruppo bersaglio.

Attiva la mitigazione delle anomalie ATW

Puoi attivare la mitigazione delle anomalie in qualsiasi momento.

Per attivare la mitigazione delle anomalie utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina dei dettagli del gruppo target, nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica gli attributi del gruppo target, nella sezione Configurazione del traffico, in Algoritmo di bilanciamento del carico, assicurati che sia selezionato Weighted random.

Nota: quando l'algoritmo casuale ponderato è selezionato inizialmente, il rilevamento delle anomalie è attivo per impostazione predefinita.

6. In Attenuazione delle anomalie, assicurati che sia selezionata l'opzione Attiva mitigazione delle anomalie.
7. Scegli Save changes (Salva modifiche).

Per attivare la mitigazione delle anomalie utilizzando il AWS CLI

Utilizzare il modify-target-group-attributescomando con l'attributo. `load_balancing.algorithm.anomaly_mitigation`

Stato di mitigazione delle anomalie

Ogni volta che ATW esegue la mitigazione su un obiettivo, è possibile visualizzare lo stato corrente in qualsiasi momento utilizzando o. AWS Management Console AWS CLI

Per visualizzare lo stato di mitigazione delle anomalie utilizzando la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella pagina dei dettagli dei gruppi target, scegli la scheda Target.
5. Nella tabella Obiettivi registrati, è possibile visualizzare lo stato di mitigazione delle anomalie di ciascun target nella colonna Mitigazione in effetto.

   Se la mitigazione non è in corso, lo stato è. `yes`

   Se la mitigazione è in corso, lo stato è. `no`

Per visualizzare lo stato di mitigazione delle anomalie utilizzando il AWS CLI

Utilizzare il describe-target-healthcomando con il valore dell'`Include.member.`Nattributo impostato su. `AnomalyDetection`

Sessioni permanenti per l'Application Load Balancer

Per impostazione predefinita, un Application Load Balancer instrada ogni richiesta in modo indipendente verso una destinazione registrata in base all'algoritmo di bilanciamento del carico

scelto. Tuttavia, è possibile usare la funzionalità sessione permanente (nota anche come affinità di sessione), per consentire al sistema di bilanciamento del carico di associare una sessione utente a una destinazione specifica. Questo garantisce che durante la sessione tutte le richieste dell'utente vengano inviate alla stessa destinazione. Questa funzionalità è utile per i server che conservano le informazioni sullo stato per fornire un'esperienza continua ai client. Per usare le sessioni permanenti, i client devono supportare i cookie.

Gli Application Load Balancer supportano sia i cookie basati sulla durata che i cookie basati sull'applicazione. Le sessioni permanenti sono abilitate a livello di gruppo di destinazioni. È possibile utilizzare una combinazione di permanenza basata sulla durata, permanenza basata sull'applicazione e nessuna permanenza nei gruppi.

La chiave per la gestione delle sessioni permanenti consiste nel determinare per quanto tempo il sistema di bilanciamento del carico deve instradare costantemente la richiesta dell'utente verso la stessa destinazione. Se l'applicazione ha il proprio cookie di sessione, è possibile utilizzare la permanenza basata sull'applicazione e il cookie di sessione del sistema di bilanciamento del carico rispetta la durata specificata dal cookie di sessione dell'applicazione. Se l'applicazione non ha il proprio cookie di sessione, è possibile utilizzare la permanenza basata sulla durata per generare un cookie di sessione del sistema di bilanciamento del carico della durata specificata.

Il contenuto dei cookie generati dal sistema di bilanciamento del carico viene crittografato utilizzando una chiave di rotazione. Non è possibile decrittografare o modificare i cookie generati dal sistema di bilanciamento del carico.

Per entrambi i tipi di permanenza, l'Application Load Balancer reimposta la scadenza dei cookie che genera dopo ogni richiesta. Se un cookie scade, la sessione non è più persistente e il client dovrebbe rimuovere il cookie dal rispettivo archivio.

Requisiti

- Un HTTP/HTTPS sistema di bilanciamento del carico.
- Almeno un'istanza integra in ciascuna zona di disponibilità.

Considerazioni

- Le sessioni permanenti non sono supportate se il bilanciamento del carico tra zone è disabilitato. Il tentativo di abilitare le sessioni permanenti quando il bilanciamento del carico tra zone è disabilitato non andrà a buon fine.

- Per i cookie basati sulle applicazioni, i nomi dei cookie devono essere specificati individualmente per ogni gruppo di destinazioni. Al contrario, per i cookie basati sulla durata, `AWSALB` è l'unico nome utilizzato in tutti i gruppi di destinazioni.
- Se si utilizzano più livelli per gli Application Load Balancer, è possibile abilitare le sessioni permanenti in tutti i livelli con i cookie basati sull'applicazione. Al contrario, con i cookie basati sulla durata, è possibile abilitare le sessioni permanenti solo in un livello, poiché `AWSALB` è l'unico nome disponibile.
- Se l'Application Load Balancer riceve sia un `AWSALBCORS` cookie di permanenza che uno `AWSALB` basato sulla durata, il valore inserito avrà la precedenza. `AWSALBCORS`
- La permanenza basata sull'applicazione non funziona con i gruppi di destinazioni ponderati.
- Se si dispone di un'operazione di inoltro con più gruppi di destinazioni e le sessioni permanenti sono abilitate per uno o più gruppi di destinazioni, è necessario abilitare la persistenza a livello di gruppo di destinazioni.
- WebSocket le connessioni sono intrinsecamente persistenti. Se il client richiede un aggiornamento della connessione a WebSockets, la destinazione che restituisce un codice di stato HTTP 101 per accettare l'aggiornamento della connessione è la destinazione utilizzata nella WebSockets connessione. Una volta completato l' WebSockets aggiornamento, la persistenza basata sui cookie non viene utilizzata.
- Gli Application Load Balancer utilizzano l'attributo `Expires` nell'intestazione del cookie invece dell'attributo `Max-Age`.
- Gli Application Load Balancer non supportano i valori dei cookie codificati con URL.
- Se l'Application Load Balancer riceve una nuova richiesta mentre la destinazione si sta esaurendo a causa dell'annullamento della registrazione, la richiesta viene indirizzata a una destinazione integra.

Persistenza basata sulla durata

La persistenza basata sulla durata instrada le richieste verso la stessa destinazione all'interno di un gruppo di destinazioni utilizzando un cookie generato dal sistema di bilanciamento del carico (`AWSALB`). Il cookie viene utilizzato per mappare la sessione verso la destinazione. Se l'applicazione non dispone del proprio cookie di sessione, è possibile specificare la durata della persistenza e gestire per quanto tempo il sistema di bilanciamento del carico dovrebbe instradare la richiesta dell'utente verso la stessa destinazione in modo sistematico.

Quando un sistema di bilanciamento del carico riceve per la prima volta una richiesta da un client, la instrada verso una destinazione (sulla base dell'algoritmo scelto) e genera un cookie chiamato `AWSALB`. Codifica le informazioni sulla destinazione selezionata, crittografa il cookie e lo include nella risposta al cliente. Il cookie generato dal sistema di bilanciamento del carico ha una scadenza di 7 giorni non configurabile.

Nelle richieste successive, il client deve includere il cookie `AWSALB`. Quando il sistema di bilanciamento del carico riceve una richiesta da un client che contiene il cookie, rileva e instrada la richiesta verso la stessa destinazione. Se il cookie è presente ma non può essere decodificato o se si riferisce a un target che è stato cancellato o non è integro, il load balancer seleziona una nuova destinazione e aggiorna il cookie con le informazioni sulla nuova destinazione.

Per le richieste CORS (Cross-Origin Resource Sharing), alcuni browser richiedono l'attivazione della persistenza. `SameSite=None; Secure` Per supportare questi browser, il load balancer genera sempre un secondo cookie di adesività`AWSALBCORS`, che include le stesse informazioni del cookie di persistenza originale, oltre all'attributo. `SameSite` I client ricevono entrambi i cookie, incluse le richieste non CORS.

Per abilitare la persistenza basata sulla durata tramite la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, procedere nel modo seguente:
    a. Seleziona Persistenza.
    b. Per Tipo di persistenza, seleziona Cookie generato dal sistema di bilanciamento del carico.
    c. Per Durata persistenza, specificare un valore compreso tra 1 secondo e 7 giorni.
    d. Scegli Save changes (Salva modifiche).

Per abilitare la viscosità basata sulla durata utilizzando il AWS CLI

Utilizzate il modify-target-group-attributescomando con gli attributi and. `stickiness.enabled` `stickiness.lb_cookie.duration_seconds`

Utilizzare il seguente comando per abilitare la persistenza basata sulla durata.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true
 Key=stickiness.lb_cookie.duration_seconds,Value=time-in-seconds
```

L'output visualizzato dovrebbe essere simile al seguente esempio.

```
    {
       "Attributes": [
          ...
           {
                "Key": "stickiness.enabled",
                "Value": "true"
             },
             {
                 "Key": "stickiness.lb_cookie.duration_seconds",
                 "Value": "86500"

             },
          ...
        ]
     }
```

Persistenza basata sull'applicazione

La persistenza basata sull'applicazione offre la flessibilità di impostare i propri criteri per la persistenza client-destinazione. Quando si abilita la persistenza basata sull'applicazione, il sistema di bilanciamento del carico instrada la prima richiesta verso una destinazione all'interno del gruppo di destinazioni sulla base dell'algoritmo scelto. La destinazione dovrebbe impostare un cookie dell'applicazione personalizzato che corrisponda al cookie configurato nel sistema di bilanciamento del carico per abilitare la persistenza. Questo cookie personalizzato può includere qualsiasi attributo di cookie richiesto dall'applicazione.

Quando l'Application Load Balancer riceve il cookie dell'applicazione personalizzato dalla destinazione, genera automaticamente un nuovo cookie dell'applicazione crittografato per acquisire informazioni sulla persistenza. Questo cookie dell'applicazione generato dal sistema di bilanciamento del carico acquisisce informazioni sulla persistenza per ogni gruppo di destinazioni che ha abilitato la persistenza basata sull'applicazione.

Il cookie dell'applicazione generato dal sistema di bilanciamento del carico non copia gli attributi del cookie personalizzato impostato dalla destinazione. Ha una scadenza di 7 giorni non configurabile.

Nella risposta al client, l'Application Load Balancer valida solamente il nome con cui il cookie personalizzato è stato configurato a livello di gruppo di destinazioni e non il suo valore o attributo di scadenza. Finché il nome corrisponde, il sistema di bilanciamento del carico invia entrambi i cookie, quello personalizzato impostato dalla destinazione e quello dell'applicazione generato dal sistema di bilanciamento del carico in risposta al client.

Nelle richieste successive, i client devono restituire entrambi i cookie per mantenere la persistenza. Il sistema di bilanciamento del carico decritta il cookie dell'applicazione e verifica se la durata configurata della pertinenza è ancora valida. In seguito, utilizza le informazioni contenute nel cookie per inviare la richiesta alla stessa destinazione all'interno del gruppo di destinazioni per mantenere la pertinenza. Inoltre, il sistema di bilanciamento del carico delega il cookie dell'applicazione personalizzato alla destinazione senza ispezionarlo o modificarlo. Nelle risposte successive, la scadenza del cookie dell'applicazione generato dal sistema di bilanciamento del carico e la durata della persistenza configurata nel sistema di bilanciamento del carico vengono reimpostate. Per mantenere la persistenza tra client e target, la scadenza del cookie e la durata della persistenza non devono trascorrere.

Se una destinazione non va a buon fine o diventa non integra, il sistema di bilanciamento del carico interrompe l'instradamento delle richieste a quella destinazione e ne sceglie una nuova integra in base all'algoritmo di bilanciamento del carico esistente. Il sistema di bilanciamento del carico tratta la sessione come se fosse bloccata sulla nuova destinazione integra e continua a instradare le richieste verso la nuova destinazione integra, anche se quella non andata a buon fine ritorna.

Per abilitare la persistenza con le richieste cross-origin resource sharing (CORS), il sistema di bilanciamento del carico aggiunge gli attributi `SameSite=None; Secure` al cookie dell'applicazione generato dal sistema di bilanciamento del carico solo se la versione utente-agente è Chromium80 o superiore.

Poiché la maggior parte dei browser limita a 4 K le dimensioni dei cookie, il sistema di bilanciamento del carico suddivide ciascun cookie dell'applicazione superiore a 4 K in più cookie. Gli Application Load Balancer supportano cookie di dimensioni massime di 16 K, quindi possono creare fino a 4 partizioni che invia poi al client. Il nome del cookie dell'applicazione visualizzato dal client inizia con «AWSALBAPP-» e include un numero di frammento. Ad esempio, se la dimensione del cookie è 0-4K, il client vede -0. AWSALBAPP Se la dimensione del cookie è 4-8k, il client vede AWSALBAPP -0 e -1 e AWSALBAPP così via.

Per abilitare la persistenza basata sull'applicazione tramite la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Nella pagina Modifica attributi, procedere nel modo seguente:

    a. Seleziona Persistenza.
    b. Per Tipo di persistenza, seleziona Cookie basato sull'applicazione.
    c. Per Durata persistenza, specificare un valore compreso tra 1 secondo e 7 giorni.
    d. Per Nome del cookie dell'applicazione, inserisci un nome per il cookie basato sull'applicazione.

        Non utilizzare `AWSALB`, `AWSALBAPP` o `AWSALBTG` come nome del cookie, poiché il loro uso è riservato per il sistema di bilanciamento del carico.
    e. Scegli Save changes (Salva modifiche).

Per abilitare l'adesività basata sulle applicazioni utilizzando il AWS CLI

Utilizzate il modify-target-group-attributescomando con i seguenti attributi:

- `stickiness.enabled`
- `stickiness.type`
- `stickiness.app_cookie.cookie_name`
- `stickiness.app_cookie.duration_seconds`

Utilizzare il seguente comando per abilitare la persistenza basata sull'applicazione.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true Key=stickiness.type,Value=app_cookie
 Key=stickiness.app_cookie.cookie_name,Value=my-cookie-name
 Key=stickiness.app_cookie.duration_seconds,Value=time-in-seconds
```

L'output visualizzato dovrebbe essere simile al seguente esempio.

```
      {
           "Attributes": [
```

```
            ...
            {
                "Key": "stickiness.enabled",
                "Value": "true"
            },
            {
                "Key": "stickiness.app_cookie.cookie_name",
                "Value": "MyCookie"
            },
            {
                "Key": "stickiness.type",
                "Value": "app_cookie"
            },
            {
                "Key": "stickiness.app_cookie.duration_seconds",
                "Value": "86500"
            },
            ...
        ]
    }
```

Ribilanciamento manuale

In caso di dimensionamento, se il numero di destinazioni aumenta considerevolmente, potrebbe potenzialmente verificarsi una distribuzione disomogenea del carico per via della persistenza. In questo scenario, è possibile ribilanciare il carico verso le destinazioni utilizzando le due opzioni seguenti:

- Impostare una scadenza per il cookie generato dall'applicazione precedente alla data e ora attuali. Ciò impedirà ai client di inviare il cookie all'Application Load Balancer, che riavvierà il processo di definizione della persistenza.
- Impostare una durata molto breve, ad esempio 1 secondo, nella configurazione della persistenza basata sull'applicazione del sistema di bilanciamento del carico. In questo modo, l'Application Load Balancer è costretto a ridefinire la persistenza anche se il cookie impostato dalla destinazione non è scaduto.

Registra gli obiettivi con il tuo gruppo target di Application Load Balancer

Puoi registrare le destinazioni con un gruppo di destinazioni. Quando crei un gruppo di destinazioni, devi specificare il tipo di destinazione, che determina come vengono registrate le relative destinazioni. Ad esempio, puoi registrare istanze IDs, indirizzi IP o funzioni Lambda. Per ulteriori informazioni, consulta Gruppi di destinazioni per gli Application Load Balancer.

Se il carico di richieste per i target attualmente registrati aumenta, puoi registrare target aggiuntivi al fine di gestire le richieste. Quando il target è pronto per gestire le richieste, registralo con il gruppo target. Il sistema di bilanciamento del carico inizia a instradare le richieste al target non appena viene completato il processo di registrazione e il target supera i controlli dello stato iniziali.

Se il carico di richieste per i target registrati diminuisce o devi eseguire la manutenzione di un target, puoi annullarne registrazione dal gruppo target. Il sistema di bilanciamento del carico arresta l'instradamento delle richieste a un target non appena la sua registrazione viene annullata. Quando il target è pronto per ricevere le richieste, è possibile registrarlo di nuovo con il gruppo target.

Quando annulli la registrazione di una destinazione, il sistema di bilanciamento del carico 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.

Quando annulli la registrazione di una destinazione che è stata registrata in base all'indirizzo IP, devi attendere lo scadere della durata dell'annullamento della registrazione prima di poter registrare nuovamente lo stesso indirizzo IP.

Se stai eseguendo la registrazione dei target in base all'ID istanza, puoi utilizzare il sistema di bilanciamento del carico con un gruppo con dimensionamento automatico. Quando colleghi un gruppo di destinazioni a un gruppo con dimensionamento automatico e il gruppo si dimensiona orizzontalmente, le istanze avviate dal gruppo con dimensionamento automatico vengono registrate automaticamente nel gruppo di destinazioni. Se distacchi il gruppo di destinazioni dal gruppo con dimensionamento automatico, viene automaticamente annullata la registrazione delle istanze dal gruppo di destinazioni. Per ulteriori informazioni, consulta Collegare un sistema di bilanciamento del carico al gruppo Auto Scaling nella Amazon Auto Scaling User EC2 Guide.

Quando chiudi un'applicazione su una destinazione, devi prima annullare la registrazione della destinazione dal relativo gruppo di destinazione e attendere che le connessioni esistenti si esauriscano. È possibile monitorare lo stato dell'annullamento della registrazione utilizzando il

comando describe-target-health CLI o aggiornando la visualizzazione del gruppo di destinazione in. AWS Management Console Dopo aver confermato che la registrazione dell'obiettivo è stata annullata, è possibile procedere con l'arresto o la chiusura dell'applicazione. Questa sequenza impedisce agli utenti di riscontrare errori 5XX quando le applicazioni vengono terminate mentre è ancora in corso l'elaborazione del traffico.

Gruppi di sicurezza target

Quando si registrano EC2 le istanze come destinazioni, è necessario assicurarsi che i gruppi di sicurezza delle istanze consentano al sistema di bilanciamento del carico di comunicare con le istanze sia sulla porta listener che sulla porta di controllo dello stato.

Regole consigliate

Inbound

Source	Port Range	Comment
load balancer security group	*instance listener*	Consente il traffico dal load balancer sulla porta del listener dell'istanza
load balancer security group	*health check*	Autorizza il traffico dal load balancer sulla porta di controllo dello stato

Ti consigliamo inoltre di consentire il traffico ICMP in entrata per supportare il rilevamento della MTU del percorso. Per ulteriori informazioni, consulta Path MTU Discovery nella Amazon EC2 User Guide.

Sottoreti condivise

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

Registrazione o annullamento della registrazione di destinazioni

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).

Indice

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

> **Note**
>
> Quando si registrano le destinazioni per ID di istanza per un gruppo IPv6 target, alle destinazioni deve essere assegnato un indirizzo principale IPv6 . Per ulteriori informazioni, IPv6 consulta gli indirizzi nella Amazon EC2 User Guide

L'istanza deve trovarsi nel cloud privato virtuale (VPC, Virtual Private Cloud) specificato per il gruppo di destinazioni. Quando la registri, l'istanza deve inoltre trovarsi nello stato `running`.

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

1. Apri la EC2 console Amazon 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 avere un IPv6 indirizzo principale assegnato per essere registrate presso un gruppo IPv6 target.
   - AWS GovCloud (US) Region s non supporta l'assegnazione di un IPv6 indirizzo principale tramite la console. È necessario utilizzare l'API per assegnare IPv6 gli indirizzi primari in AWS GovCloud (US) Region s.

6. Per annullare la registrazione delle istanze, seleziona le istanze e poi scegliere Annullare registrazione.

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

IPv4 obiettivi

Gli indirizzi IP registrati devono 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)

Non è possibile registrare gli indirizzi IP di un altro Application Load Balancer nello stesso VPC. Se l'altro Application Load Balancer si trova in un VPC in peering al VPC del sistema di bilanciamento del carico, è possibile registrarne gli indirizzi IP.

IPv6 obiettivi

- Gli indirizzi IP registrati devono essere all'interno del blocco CIDR VPC o all'interno di un blocco CIDR VPC con peering.

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

1. Apri la EC2 console Amazon 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 Registrare destinazioni. Per ogni indirizzo IP, seleziona la rete, inserisci l'indirizzo IP e la porta, quindi scegli Includi come in sospeso di seguito.
6. Facoltativo: se l'indirizzo IP è esterno al VPC selezionato, è necessario specificare una zona di disponibilità.
7. Dopo aver finito di specificare gli indirizzi, scegli Registra destinazioni in sospeso.

8. 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 una funzione Lambda

È possibile registrare una singola funzione Lambda in ogni gruppo di destinazioni. Elastic Load Balancing deve disporre delle autorizzazioni per richiamare la funzione Lambda. Se non hai più bisogno di inviare traffico alla funzione Lambda, puoi annullare la relativa registrazione. Dopo avere annullato la registrazione di una funzione Lambda, le richieste in transito hanno esito negativo con 5XX errori HTTP. Per sostituire una funzione Lambda, risulta più conveniente creare invece un nuovo gruppo di destinazioni. Per ulteriori informazioni, consulta Usa le funzioni Lambda come obiettivi di un Application Load Balancer.

Per registrare o annullare la registrazione di una funzione Lambda utilizzando la console

1. Apri la EC2 console Amazon 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. Se non vi sono funzioni Lambda registrate, scegli Registra. Selezionare la funzione Lambda e scegliere Registra.
6. Per annullare la registrazione di una funzione Lambda, scegli Annulla registrazione. Quando viene richiesta la conferma, seleziona Annulla registrazione.

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.

Usa le funzioni Lambda come obiettivi di un Application Load Balancer

Puoi registrare le tue funzioni Lambda come destinazioni e configurare una regola del listener per inoltrare le richieste al gruppo di destinazioni della funzione Lambda. Quando inoltra la richiesta a un gruppo di destinazioni con una funzione Lambda come destinazione, il sistema di bilanciamento del

carico richiama la funzione Lambda e trasferisce i contenuti della richiesta alla funzione Lambda, nel formato JSON.

Limiti

- La funzione Lambda e il gruppo di destinazioni devono trovarsi nello stesso account e nella stessa regione.
- Le dimensioni massime del corpo della richiesta che puoi inviare a una funzione Lambda sono di 1 MB. Per i limiti correlati delle dimensioni, consulta HTTP header limits.
- Le dimensioni massime dell'oggetto JSON di risposta che può inviare la funzione Lambda sono di 1 MB.
- WebSockets non sono supportati. Le richieste di aggiornamento vengono rifiutate con un codice HTTP 400.
- Le zone locali non sono supportate.
- Automatic Target Weights (ATW) non è supportato.

Indice

Per una demo, consulta Lambda target on Application Load Balancer.

Preparazione della funzione Lambda

Le seguenti raccomandazioni si applicano se utilizzi la funzione Lambda con un Application Load Balancer.

Autorizzazioni a richiamare la funzione Lambda

Se crei il gruppo di destinazioni e registri la funzione Lambda tramite la AWS Management Console, questa aggiunge automaticamente le autorizzazioni richieste alla tua policy delle funzioni

Lambda. Altrimenti, dopo aver creato il gruppo target e registrato la funzione utilizzando AWS CLI, è necessario utilizzare il comando add-permission per concedere a Elastic Load Balancing l'autorizzazione a richiamare la funzione Lambda. Consigliamo di includere le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per limitare l'invocazione della funzione al gruppo di destinazioni specificato. Per ulteriori informazioni, consulta Problema del "confused deputy" nella Guida per l'utente IAM.

```
aws lambda add-permission \
--function-name lambda-function-arn-with-alias-name \
--statement-id elb1 \
--principal elasticloadbalancing.amazonaws.com \
--action lambda:InvokeFunction \
--source-arn target-group-arn \
--source-account target-group-account-id
```

Controllo delle versioni della funzione Lambda

Puoi registrare una funzione Lambda per gruppo di destinazioni. Per accertarti di poter cambiare la funzione Lambda e che il sistema di bilanciamento del carico richiami sempre la versione corrente della funzione Lambda, crea un alias della funzione e includilo nell'ARN della funzione al momento della registrazione della funzione con il sistema di bilanciamento del carico. Per ulteriori informazioni, consulta gli alias delle AWS Lambda funzioni nella Guida per gli sviluppatori.AWS Lambda

Timeout della funzione

Il sistema di bilanciamento del carico attende finché la funzione Lambda non risponde o scade. Ti consigliamo di configurare il timeout della funzione Lambda in base al runtime previsto. Per informazioni sul valore di timeout predefinito e su come modificarlo, consulta Configurare il timeout della funzione Lambda. Per informazioni sul valore di timeout massimo che puoi configurare, vedi quote.AWS Lambda

Creazione di un gruppo di destinazioni per la funzione Lambda

Creare un gruppo target, che viene utilizzato nell'instradamento delle richieste. Se il contenuto della richiesta corrisponde a una regola del listener con un'operazione per l'inoltro al gruppo di destinazioni, il sistema di bilanciamento del carico richiama la funzione Lambda registrata.

Per creare un gruppo target e registrare la funzione Lambda utilizzando la console

1. Apri la EC2 console Amazon 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. Per Seleziona destinazione, scegli Funzione Lambda.
5. Per Nome gruppo di destinazioni digitare un nome per il gruppo di destinazioni.
6. (Facoltativo) Per abilitare i controlli dell'integrità, scegli Controllo dell'integrità, Abilita.
7. (Facoltativo) Aggiungere uno o più tag come illustrato di seguito:
   a. Espandere la sezione Tag.
   b. Selezionare Aggiungi tag.
   c. Immetti una chiave e un valore per il tag.
8. Scegli Next (Successivo).
9. Specificare una singola funzione Lambda oppure saltare questo passaggio e specificare una funzione Lambda in seguito.
10. Scegliere Crea gruppo target.

Per creare un gruppo di destinazioni e registrare la funzione Lambda tramite AWS CLI

Usa i comandi create-target-groupe register-targets.

Ricezione di eventi dal sistema di bilanciamento del carico

Il sistema di bilanciamento del carico supporta l'invocazione Lambda per le richieste sia da HTTP che HTTPS. Il sistema di bilanciamento del carico invia un evento in formato JSON. Il sistema di bilanciamento del carico aggiunge le seguenti intestazioni a ogni richiesta: `X-Amzn-Trace-Id`, `X-Forwarded-For`, `X-Forwarded-Port` e `X-Forwarded-Proto`.

Se è presente l'intestazione `content-encoding`, il sistema di bilanciamento del carico Base64 codifica il corpo e imposta `isBase64Encoded` su `true`.

Se l'intestazione `content-encoding` non è presente, la codifica Base64 dipende dal tipo di contenuto. Per i seguenti tipi, il load balancer invia il corpo così com'è e lo imposta `isBase64Encoded` su: text/*,. `false` application/json, application/javascript, and application/xml In caso contrario, il sistema di bilanciamento del carico Base64 codifica il corpo e imposta `isBase64Encoded` su `true`.

Di seguito è riportato un esempio di evento.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
    "path": "/",
    "queryStringParameters": {parameters},
    "headers": {
        "accept": "text/html,application/xhtml+xml",
        "accept-language": "en-US,en;q=0.8",
        "content-type": "text/plain",
        "cookie": "cookies",
        "host": "lambda-846800462-us-east-2.elb.amazonaws.com",
        "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)",
        "x-amzn-trace-id": "Root=1-5bdb40ca-556d8b0c50dc66f0511bf520",
        "x-forwarded-for": "72.21.198.66",
        "x-forwarded-port": "443",
        "x-forwarded-proto": "https"
    },
    "isBase64Encoded": false,
    "body": "request_body"
}
```

Risposta al sistema di bilanciamento del carico

La risposta dalla funzione Lambda deve includere lo stato della codifica Base64, il codice di stato e le intestazioni. Puoi omettere il corpo della risposta.

Per includere un contenuto binario nel corpo della risposta, devi sottoporre a codifica Base64 il contenuto e impostare `isBase64Encoded` su `true`. Il sistema di bilanciamento del carico decodifica il contenuto per recuperare la parte binaria e inviarla al client nel corpo della risposta HTTP.

Il sistema di bilanciamento del carico non rispetta le hop-by-hop intestazioni, come o. `Connection` `Transfer-Encoding` Puoi omettere l'intestazione `Content-Length` in quanto il sistema di bilanciamento del carico la calcola prima di inviare le risposte ai client.

Di seguito è riportata una risposta di esempio da una funzione Lambda basata su nodejs.

```
{
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

Per i modelli di funzioni Lambda che funzionano con Application Load Balancer, vedi application-load-balancer-serverless -app su github. In alternativa, aprire la console Lambda, scegli Applicazioni, Crea applicazione e seleziona una delle seguenti opzioni da AWS Serverless Application Repository:

- Obiettivo Lambda ALB - S3 UploadFileto
- Obiettivo ALB-Lambda- BinaryResponse
- ALB-Lambda-Target IP WhatisMy

Intestazioni con più valori

Se le richieste provenienti da un client o le risposte da una funzione Lambda contengono intestazioni con più valori o la stessa intestazione più volte oppure parametri di query con più valori per la stessa chiave, puoi abilitare il supporto della sintassi delle intestazioni con più valori. Dopo aver abilitato le intestazioni con più valori, le intestazioni e i parametri di query scambiati tra il sistema di bilanciamento del carico e la funzione Lambda utilizzano array anziché stringhe. Se non abiliti la sintassi delle intestazioni con più valori e un intestazione o un parametro di query dispongono di più valori, il sistema di bilanciamento del carico utilizza l'ultimo valore ricevuto.

Indice

Richieste con intestazioni con più valori

I nomi dei campi utilizzati per le intestazioni e i parametri delle stringhe di query sono diversi a seconda se sono abilitate le intestazioni multivalore per il gruppo target.

La seguente richiesta di esempio ha due parametri di query con la stessa chiave:

```
http://www.example.com?&myKey=val1&myKey=val2
```

Con il formato predefinito, il sistema di bilanciamento del carico utilizza l'ultimo valore inviato dal client e invia un evento che include parametri di stringhe di query tramite `queryStringParameters`. Per esempio:

```
"queryStringParameters": { "myKey": "val2"},
```

Con le intestazioni con più valori, il sistema di bilanciamento del carico utilizza entrambi i valori della chiave inviati dal client e invia un evento che include parametri di stringhe di query tramite `multiValueQueryStringParameters`. Per esempio:

```
"multiValueQueryStringParameters": { "myKey": ["val1", "val2"] },
```

Analogamente, supponiamo che il client invii una richiesta con due cookie nell'intestazione:

```
"cookie": "name1=value1",
"cookie": "name2=value2",
```

Con il formato predefinito, il sistema di bilanciamento del carico utilizza l'ultimo cookie inviato dal client e invia un evento che include intestazioni tramite `headers`. Per esempio:

```
"headers": {
    "cookie": "name2=value2",
    ...
},
```

Con le intestazioni con più valori, il sistema di bilanciamento del carico utilizza entrambi i cookie inviati dal client e invia un evento che include le intestazioni tramite `multiValueHeaders`. Per esempio:

```
"multiValueHeaders": {
```

```
    "cookie": ["name1=value1", "name2=value2"],
    ...
},
```

Se i parametri di query sono codificati in formato URL, il sistema di bilanciamento del carico non li decodifica. Devi decodificarli nella funzione Lambda.

Risposte con intestazioni con più valori

I nomi dei campi utilizzati per le intestazioni sono diversi a seconda se sono abilitate le intestazioni multivalore per il gruppo target. Devi utilizzare `multiValueHeaders` se hai abilitato le intestazioni multivalore e `headers` in caso contrario.

Con il formato predefinito, puoi specificare un singolo cookie:

```
{
  "headers": {
      "Set-cookie": "cookie-name=cookie-value;Domain=myweb.com;Secure;HttpOnly",
      "Content-Type": "application/json"
  },
}
```

Con le intestazioni con più valori, è necessario specificare più cookie come segue:

```
{
  "multiValueHeaders": {
      "Set-cookie": ["cookie-name=cookie-
value;Domain=myweb.com;Secure;HttpOnly","cookie-name=cookie-value;Expires=May 8,
 2019"],
      "Content-Type": ["application/json"]
  },
}
```

Il sistema di bilanciamento del carico potrebbe inviare le intestazioni al client in un ordine diverso rispetto a quello specificato nel payload della risposta di Lambda. Pertanto, non fare affidamento sul fatto che le intestazioni verranno restituite in un ordine specifico.

Abilitazione delle intestazioni con più valori

Puoi abilitare o disabilitare le intestazioni con più valori per un gruppo di destinazioni con tipo `lambda`.

Per abilitare le intestazioni con più valori tramite la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, all'interno della Attributi, scegli Modifica.
5. Seleziona o deseleziona Intestazioni con più valori.
6. Scegli Save changes (Salva modifiche).

Per abilitare le intestazioni multivalore utilizzando AWS CLI

Utilizzate il modify-target-group-attributescomando con l'`lambda.multi_value_headers.enabled`attributo.

Abilitazione dei controlli dell'integrità

Per impostazione predefinita, i controlli dello stato sono disabilitati per i gruppi di destinazioni di tipo `lambda`. È possibile abilitare i controlli dell'integrità per implementare il failover DNS con Amazon Route 53. La funzione Lambda è in grado di verificare l'integrità di un servizio downstream prima di rispondere alla richiesta di controllo dello stato. Se la risposta dalla funzione Lambda indica un errore del controllo dell'integrità, l'errore viene trasmesso a Route 53. Puoi configurare Route 53 affinché esegua il failover sullo stack di un'applicazione di backup.

Ti verrà addebitato il costo per i controlli dello stato, allo stesso modo che per qualsiasi invocazione della funzione Lambda.

Di seguito è riportato il formato dell'evento di controllo dello stato inviato alla funzione Lambda. Per controllare se un evento è un evento di controllo dello stato, controlla il valore del campo utente-agente. L'agente utente per i controlli dello stato è `ELB-HealthChecker/2.0`.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
```

```
    "path": "/",
    "queryStringParameters": {},
    "headers": {
        "user-agent": "ELB-HealthChecker/2.0"
    },
    "body": "",
    "isBase64Encoded": false
}
```

Per abilitare i controlli sanitari per un gruppo target utilizzando la console

1. Apri la EC2 console Amazon 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 Dettagli del gruppo, nella sezione Impostazioni del controllo dell'integrità, scegli Modifica.
5. In Controlli dell'integrità, scegli Abilita.
6. Scegli Save changes (Salva modifiche).

Per abilitare i controlli sanitari per un gruppo target utilizzando il AWS CLI

Utilizzare il comando modify-target-group con l'opzione `--health-check-enabled`.

Annullamento della registrazione della funzione Lambda

Se non hai più bisogno di inviare traffico alla funzione Lambda, puoi annullare la relativa registrazione. Dopo avere annullato la registrazione di una funzione Lambda, le richieste in transito hanno esito negativo con 5XX errori HTTP.

Per sostituire una funzione Lambda, ti consigliamo di creare un nuovo gruppo di destinazioni, registrare la nuova funzione con il nuovo gruppo e aggiornare le regole del listener per utilizzare il nuovo gruppo di destinazioni invece di quello esistente.

Per annullare la registrazione della funzione Lambda utilizzando la console

1. Apri la EC2 console Amazon 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 Destinazioni, scegli Annulla registrazione.
5. Quando viene richiesta la conferma, seleziona Annulla registrazione.

Per annullare la registrazione della funzione Lambda utilizzando AWS CLI

Utilizza il comando deregister-targets.

Tag per il gruppo target di Application Load Balancer

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

Per aggiornare i tag per un gruppo target tramite la console

1. Apri la EC2 console Amazon 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.

Eliminare un gruppo target di Application Load Balancer

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

Per eliminare un gruppo target tramite la console

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Bilanciamento del carico scegli Gruppi di destinazione.
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 degli Application 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 Application Load Balancer.

Log di accesso

Puoi utilizzare i log di accesso per acquisire informazioni dettagliate sulle richieste effettuate al sistema di bilanciamento del carico e per archiviarle come file di log 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 dell'Application Load Balancer.

Log delle connessioni

Puoi utilizzare i log di connessione per acquisire gli attributi relativi alle richieste inviate al tuo sistema di bilanciamento del carico e archiviarli come file di registro in Amazon S3. Puoi utilizzare questi log di connessione per determinare l'indirizzo IP e la porta del client, le informazioni sul certificato del client, i risultati della connessione e i codici TLS utilizzati. Questi log di connessione possono quindi essere utilizzati per esaminare i modelli di richiesta e altre tendenze. Per ulteriori informazioni, consulta Log di connessione per l'Application Load Balancer.

Tracciamento delle richieste

Puoi utilizzare il tracciamento delle richieste per tenere traccia delle richieste HTTP. Il sistema di bilanciamento del carico aggiunge un'intestazione con un identificatore di traccia per ciascuna richiesta che riceve. Per ulteriori informazioni, consulta Richiesta del tracciamento sull'Application 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 Registrare le chiamate API per l'utilizzo di Elastic Load Balancing. CloudTrail

CloudWatch metriche per il tuo Application 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.

Le metriche per Application Load Balancers escludono le richieste di controllo dello stato.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Parametri di Application Load Balancer

- Integrità del gruppo di destinazioni
- Funzioni Lambda
- Autenticazione dell'utente

Il namespace `AWS/ApplicationELB` include i seguenti parametri per i sistemi di bilanciamento del carico.

Parametro	Descrizione
`ActiveConnectionCount`	Il numero totale di connessioni TCP attive dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico ai target. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`AnomalousHostCount`	Il numero di host rilevati con anomalie. Criteri di segnalazione: sempre segnalati Statistiche: le statistiche più utili sono `Average`, `Minimum` e `Maximum`. Dimensioni • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`
`BYoIPUtilPercentage`	La percentuale di utilizzo del pool IP. Criteri di segnalazione: l' BYoIP è abilitato sul load balancer. Statistiche: l'unica statistica significativa è `Average`.

Parametro	Descrizione
	Dimensioni • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `TargetGroup` , `AvailabilityZone`
`ClientTLSNegotiationErrorCount`	Il numero di connessioni TLS avviate dal client che non hanno stabilito una sessione con il sistema di bilanciamento del carico. Le possibili cause includono una mancata corrispondenza di crittografia o protocolli o il client non riesce a verificare il certificato del server e chiudere la connessione. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `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 LCUs quello che usi all'ora. Quando la prenotazione LCU è attiva, Consumed LCUs segnalerà `0` se l'utilizzo è inferiore alla capacità riservata e riporterà i valori superiori `0` se l'utilizzo supera la capacità riservata. LCUs Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing. Criteri di segnalazione: sempre segnalati Statistiche: tutte Dimensioni • `LoadBalancer`

Parametro	Descrizione
`PeakLCUs`	Il numero massimo di unità di capacità di bilanciamento del carico (LCU) utilizzate dal sistema di bilanciamento del carico in un determinato momento. Applicabile solo quando si utilizza LCU Reservation. Criteri di segnalazione: sempre Statistiche: le statistiche più utili sono `Sum` e `Max`. Dimensioni • `LoadBalancer`
`ReservedLCUs`	Una metrica di fatturazione che riporta la capacità riservata su base al minuto. L'importo totale riservato LCUs per qualsiasi periodo è l'importo LCUs che ti verrà addebitato. Ad esempio, se LCUs ne vengono prenotati 500 per un'ora, la metrica al minuto sarà 8,33. LCUs Per ulteriori informazioni, consulta Monitora la prenotazione. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: tutte Dimensioni • `LoadBalancer`
`DesyncMitigationMode_NonCompliant_Request_Count`	Il numero di richieste che non sono conformi a RFC 7230. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`DroppedInvalidHeaderRequestCount`	Numero di richieste in cui il sistema di bilanciamento del carico ha rimosso le intestazioni HTTP con campi di intestazione non validi prima di instradare la richiesta. Il sistema di bilanciamento del carico rimuove queste intestazioni solo se l'attributo `routing.http.drop_invalid_header_fields.enabled` è impostato su `true`. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: tutte Dimensioni • `AvailabilityZone` , `LoadBalancer`
`MitigatedHostCount`	Il numero di obiettivi oggetto di mitigazione. Criteri di segnalazione: sempre segnalati Statistiche: le statistiche più utili sono `Average`, `Minimum` e `Maximum`. Dimensioni • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
ForwardedInvalidHeaderRequestCount	Numero di richieste instradate dal sistema di bilanciamento del carico con intestazioni HTTP con campi di intestazione non validi. Il sistema di bilanciamento del carico inoltra le richieste con queste intestazioni solo se l'attributo routing.http.drop_invalid_header_fields.enabled è impostato su false. Criteri di segnalazione: sempre segnalati Statistiche: tutte Dimensioni • AvailabilityZone , LoadBalancer
GrpcRequestCount	Il numero di richieste gRPC elaborate su IPv4 e. IPv6 Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Minimum, Maximum e Average restituiscono 1. Dimensioni • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup • TargetGroup • AvailabilityZone , TargetGroup
HTTP_Fixed_Response_Count	Il numero di operazioni a risposta fissa completate. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Parametro	Descrizione
`HTTP_Redirect_Count`	Il numero di operazioni di reindirizzamento completate. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AavailabilityZone` , `LoadBalancer`
`HTTP_Redirect_Url_Limit_Exceeded_Count`	Il numero di operazioni di reindirizzamento che non è possibile completare perché l'URL nell'intestazione Location della risposta è più grande di 8 K. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`HTTPCode_ELB_3XX_Count`	Il numero di codici di reindirizzamento 3XX HTTP provenienti dal sistema di bilanciamento del carico. Questo numero non comprende i codici di risposta generati dalle destinazioni. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
HTTPCode_ELB_4XX_Count	Il numero di codici di errore client HTTP 4XX provenienti dal sistema di bilanciamento del carico. Questo numero non comprende i codici di risposta generati dalle destinazioni. Gli errori client vengono generati quando le richieste sono malformate o incomplete. Queste richieste non sono state ricevute dalla destinazione, tranne nel caso in cui il sistema di bilanciamento del carico restituisce un codice di errore HTTP 460. Questo numero non comprende i codici di risposta generati dai target. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Minimum, Maximum e Average restituiscono 1. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_5XX_Count	Il numero di codici di errore server HTTP 5XX provenienti dal sistema di bilanciamento del carico. Questo numero non comprende i codici di risposta generati dai target. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Minimum, Maximum e Average restituiscono 1. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Parametro	Descrizione
`HTTPCode_ELB_500_Count`	Il numero di codici di errore HTTP 500 provenienti dal sistema di bilanciamento del carico. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`HTTPCode_ELB_502_Count`	Il numero di codici di errore HTTP 500 provenienti dal sistema di bilanciamento del carico. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`HTTPCode_ELB_503_Count`	Il numero di codici di errore HTTP 503 provenienti dal sistema di bilanciamento del carico. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
HTTPCode_ELB_504_Count	Il numero di codici di errore HTTP 504 provenienti dal sistema di bilanciamento del carico. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
IPv6ProcessedBytes	Il numero totale di byte elaborati dal sistema di bilanciamento del carico. IPv6 Questo conteggio è incluso in ProcessedBytes . Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer
IPv6RequestCount	Il numero di IPv6 richieste ricevute dal load balancer. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Minimum, Maximum e Average restituiscono 1. Dimensioni • LoadBalancer • AvailabilityZone , LoadBalancer

Parametro	Descrizione
`NewConnectionCount`	Il numero totale di nuove connessioni TCP stabilite dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico ai target. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`NonStickyRequestCount`	Il numero di richieste in cui il sistema di bilanciamento del carico ha scelto una nuova destinazione perché non è stato in grado di utilizzare una sticky session esistente. Ad esempio, la richiesta è stata la prima da un nuovo client e non erano presenti cookie di persistenza, un cookie di persistenza è stato presentato ma non specificava una destinazione registrata con il gruppo di destinazioni, il cookie di persistenza era errato o scaduto oppure un errore interno ha impedito al sistema di bilanciamento del carico di leggere il cookie di persistenza. Criteri di segnalazione: la persistenza è abilitata nel gruppo di destinazioni. Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`ProcessedBytes`	Il numero totale di byte elaborati dal load balancer su IPv4 e IPv6 (intestazione HTTP e payload HTTP). Questo conteggio include il traffico da e verso i client e le funzioni Lambda, nonché il traffico proveniente da un Identity Provider (IdP) se l'autenticazione dell'utente è abilitata. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedConnectionCount`	Il numero di connessioni respinte perché il sistema di bilanciamento del carico ha raggiunto il numero massimo di connessioni. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`RequestCount`	Il numero di richieste elaborate su e. IPv4 IPv6 Questo parametro viene incrementato solo per le richieste in cui il nodo del sistema di bilanciamento del carico è riuscito a scegliere una destinazione. Le richieste che vengono rifiutate prima della scelta di una destinazione non si riflettono in questo parametro. Criteri di segnalazione: segnalato se ci sono obiettivi registrati. Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `LoadBalancer` , `AvailabilityZone` • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`
`RuleEvaluations`	Il numero di regole valutate dal load balancer durante l'elaborazione delle richieste. La regola predefinita non viene conteggiata. In questo conteggio sono incluse le 10 valutazioni gratuite delle regole per richiesta. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer`

Parametro	Descrizione
`ZonalShiftedHostCount`	Il numero di obiettivi considerati disabilitati a causa dello spostamento di zona. Criteri di segnalazione: segnalato quando è presente un valore Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` , `TargetGroup` . • `AvailabilityZone` , `LoadBalancer` , `TargetGroup` .

Il namespace `AWS/ApplicationELB` include i seguenti parametri per i target.

Parametro	Descrizione
`HealthyHostCount`	Il numero di target considerati integri. Criteri di segnalazione: segnalato se ci sono obiettivi registrati. Statistiche: le statistiche più utili sono `Average`, `Minimum` e `Maximum`. Dimensioni • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`
`HTTPCode_Target_2XX_Count` , `HTTPCode_Target_3XX_Count` , `HTTPCode_Target_4XX_Count` , `HTTPCode_Target_5XX_Count`	Il numero di codici di risposta HTTP generati dai target. Questo non comprende i codici di risposta generati dal sistema di load balancer. Criteri di segnalazione: segnalato se ci sono obiettivi registrati. Statistiche: la statistica più utile è `Sum`. `Minimum`, `Maximum` e `Average` restituiscono 1.

Parametro	Descrizione
	Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`
`RequestCountPerTarget`	Il numero medio di richieste per target, in un gruppo target. È necessario specificare il gruppo target utilizzando la dimensione `TargetGroup` . Questo parametro non è applicabile se la destinazione è una funzione Lambda. Questo conteggio utilizza il numero totale di richieste ricevute dal gruppo target, diviso per il numero di target sani presenti nel gruppo target. Se non ci sono obiettivi sani nel gruppo target, viene diviso per il numero totale di obiettivi registrati. Criteri di segnalazione: sempre segnalati Statistiche: l'unica statistica valida è `Sum`. Questo valore rappresenta la media, non la somma. Dimensioni • `TargetGroup` • `TargetGroup` , `AvailabilityZone` • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`

Parametro	Descrizione
`TargetConnectionErrorCount`	Il numero di connessioni che non sono state stabilite con successo tra il sistema di bilanciamento del carico e il target. Questo parametro non è applicabile se la destinazione è una funzione Lambda. Questa metrica non viene incrementata in caso di connessioni con controlli sanitari non riusciti. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`
`TargetResponseTime`	Il tempo trascorso, in secondi, dal momento in cui la richiesta ha lasciato il sistema di bilanciamento del carico prima che la destinazione inizi a inviare le intestazioni di risposta. È l'equivalente del campo `target_processing_time` nei log di accesso. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali). Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`TargetTLSNegotiationErrorCount`	Il numero di connessioni TLS avviate dal sistema di bilanciamento del carico che non hanno stabilito una sessione con il target. Tra le possibili cause vi è una mancata corrispondenza tra crittografie o protocolli. Questo parametro non è applicabile se la destinazione è una funzione Lambda. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`
`UnHealthyHostCount`	Il numero di target considerati non integri. Quando si annulla la registrazione di un obiettivo, questo valore diminuisce ma non aumenta. `HealthyHostCount` `UnhealthyHostCount` Criteri di segnalazione: segnalato se ci sono obiettivi registrati. Statistiche: le statistiche più utili sono `Average`, `Minimum` e `Maximum`. Dimensioni • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`

Lo spazio dei nomi `AWS/ApplicationELB` include i seguenti parametri per i l'integrità del gruppo di destinazioni. Per ulteriori informazioni, consulta the section called “Integrità del gruppo di destinazione”.

Parametro	Descrizione
`HealthyStateDNS`	Il numero di zone che soddisfano i requisiti di stato di integrità del DNS. Statistiche: la statistica più utile è `Max`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`HealthyStateRouting`	Il numero di zone che soddisfano i requisiti di stato di integrità dell'instradamento. Statistiche: la statistica più utile è `Max`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyRoutingRequestCount`	Il numero di richieste che vengono instradate utilizzando l'operazione di failover dell'instradamento (fail open). Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyStateDNS`	Il numero di zone che non soddisfano i requisiti di stato di integrità del DNS e che pertanto sono state contrassegnate come non integre nel DNS. Statistiche: la statistica più utile è `Min`.

Parametro	Descrizione
	Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyStateRouting`	Il numero di zone che non soddisfano i requisiti di stato di integrità dell'instradamento. Pertanto, il sistema di bilanciamento del carico distribuisce il traffico verso tutte le destinazioni della zona, comprese quelle non integre. Statistiche: la statistica più utile è `Min`. Dimensioni • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Lo spazio dei nomi `AWS/ApplicationELB` include i parametri seguenti per le funzioni Lambda registrate come destinazioni.

Parametro	Descrizione
`LambdaInternalError`	Il numero di richieste a una funzione Lambda che non sono riuscite a causa di un problema interno del sistema di bilanciamento del carico o AWS Lambda. Per ottenere i codici di errore, controllare il campo error_reason del log di accesso. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `TargetGroup` • `TargetGroup` , `LoadBalancer`

Parametro	Descrizione
LambdaTargetProcessedBytes	Il numero totale di byte elaborati dal sistema di bilanciamento del carico per le richieste a una funzione Lambda e le risposte da essa. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è Sum. Dimensioni • LoadBalancer
LambdaUserError	Il numero di richieste a una funzione Lambda che non sono riuscite a causa di un problema con la funzione Lambda. Ad esempio, il sistema di bilanciamento del carico non aveva l'autorizzazione a invocare la funzione; l'oggetto JSON ricevuto dal sistema di bilanciamento del carico è errato o privo dei campi obbligatori oppure le dimensioni del corpo della richiesta o la risposta superavano il limite di 1 MB. Per ottenere i codici di errore, controllare il campo error_reason del log di accesso. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è Sum. Dimensioni • TargetGroup • TargetGroup , LoadBalancer

Il namespace AWS/ApplicationELB include i seguenti parametri per l'autenticazione utente.

Parametro	Descrizione
ELBAuthError	Il numero di autenticazioni utente che non possono essere completate perché un'operazione di configurazione non è stata correttamente configurata, il sistema di bilanciamento del carico non ha potuto

Parametro	Descrizione
	stabilire una connessione con l'IdP o il sistema di bilanciamento del carico non è riuscito a completare il flusso di autenticazioni a causa di un errore interno. Per ottenere i codici di errore, controllare il campo error_reason del log di accesso. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthFailure`	Il numero di autenticazioni utente che non sono state completate perché l'IdP ha negato l'accesso all'utente o un codice di autorizza zione è stato utilizzato più di una volta. Per ottenere i codici di errore, controllare il campo error_reason del log di accesso. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`ELBAuthLatency`	Il tempo trascorso, in millisecondi, per eseguire una query all'IdP per il token dell'ID e le informazioni utente. Se una o più di queste operazioni non vanno a buon fine, è il momento giusto per un fallimento. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: tutte le statistiche sono significative. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthRefreshTokenSuccess`	Il numero di volte in cui il sistema di bilanciamento del carico ha aggiornato correttamente le richieste dell'utente utilizzando un token di aggiornamento fornito dal provider di identità. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Parametro	Descrizione
`ELBAuthSuccess`	Il numero di operazioni di autenticazione riuscite. Questo parametro aumenta alla fine del flusso di lavoro di autenticazione, dopo che il sistema di bilanciamento del carico ha recuperato le richieste dell'utente dall'IdP. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthUserClaimsSizeExceeded`	Il numero di volte in cui un provider di identità configurato ha restituito le richieste dell'utente che superavano 11 Kbyte di dimensioni. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: l'unica statistica significativa è `Sum`. Dimensioni • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensioni di parametro per Application Load Balancer

Per filtrare i parametri relativi all'Application Load Balancer, usa le seguenti dimensioni.

Dimensione	Descrizione
`AvailabilityZone`	Consente di filtrare i dati del parametro per zona di disponibilità.

Dimensione	Descrizione
`LoadBalancer`	Consente di filtrare i dati del parametro per load balancer. Specificare il load balancer come segue: load-balancer-nameapp/ 1234567890123456 (la parte finale dell'ARN del load balancer).
`TargetGroup`	Consente di filtrare i dati del parametro per gruppo target. Specificare il gruppo target come segue: targetgroup/ target-group-name/123456789 0123456 (la parte finale dell'ARN del gruppo target).

Statistiche per i parametri dell'Application 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 statistiche per tutte le EC2 istanze integre di un sistema di bilanciamento del carico avviato in una zona di disponibilità specifica.

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. Ad esempio, supponiamo che l'Application Load Balancer sia costituito da 2 nodi del sistema di bilanciamento del carico. Un nodo ha un `HealthyHostCount` con un `Minimum` di 2, un `Maximum` di 10 e una `Average` di 6, mentre l'altro ha un `HealthyHostCount` con un `Minimum` di 1, un `Maximum` di 5 e una `Average` di 3. Pertanto il load balancer ha un `Minimum` di 1, un `Maximum` di 10 e una `Average` di circa 4.

Consigliamo di monitorare un `UnHealthyHostCount` con valore diverso da zero nella statistica `Minimum` e di impostare un allarme in caso di valori diversi da zero per più di un punto dati. L'utilizzo del `Minimum` consente di rilevare quando le destinazioni sono considerate non integre da ogni nodo e zona di disponibilità del sistema di bilanciamento del carico. Impostare un allarme per `Average` o `Maximum` è utile per ricevere un avviso in caso di potenziali problemi e consigliamo ai clienti di esaminare questo parametro e indagare sulle occorrenze di valori diversi da zero. La mitigazione automatica degli errori può essere eseguita seguendo le migliori pratiche di utilizzo del load balancer health check in Amazon EC2 Auto Scaling o Amazon Elastic Container Service (Amazon ECS).

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.

Un percentile indica lo stato relativo di un valore in un set di dati. Puoi specificare qualsiasi percentile, utilizzando fino a due decimali (ad esempio, p95,45). Ad esempio, il 95° percentile indica che il 95% dei dati è al di sotto di questo valore e il 5% al di sopra. I percentili sono spesso utilizzati per isolare le anomalie. Ad esempio, supponiamo che un'applicazione serva la maggior parte delle richieste da una cache in 1-2 ms, ma in 100-200 ms se la cache è vuota. Il valore massimo riflette il caso più lento, attorno ai 200 ms. La media non indica la distribuzione dei dati. I percentili forniscono una visione più significativa delle prestazioni delle applicazioni. Utilizzando il 99° percentile come trigger o CloudWatch allarme per l'Auto Scaling, è possibile fare in modo che l'elaborazione di non più dell'1% delle richieste richieda più di 2 ms.

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

Puoi visualizzare le CloudWatch metriche 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 del sistema tramite la console CloudWatch.

Per visualizzare i parametri tramite la console

1. Apri la EC2 console Amazon 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. Seleziona il gruppo di destinazioni, quindi scegli la scheda 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. Seleziona il sistema di bilanciamento del carico, quindi la scheda 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 ApplicationELB.
4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, inseriscine il nome nel campo di ricerca.
5. (Facoltativo) Per filtrare per dimensione, selezionare una delle opzioni seguenti:

   - Per visualizzare solo i parametri segnalati per i sistemi di bilanciamento del carico, scegli Per parametri AppELB. Per visualizzare i parametri di un singolo sistema di bilanciamento del carico, inseriscine il nome nel campo di ricerca.
   - Per visualizzare solo i parametri segnalati per i gruppi di destinazioni, scegli Per parametri AppELB, GD. Per visualizzare i parametri di un singolo gruppo di destinazioni, inserisci il relativo nome nel campo di ricerca.
   - Per visualizzare solo i parametri segnalati per i sistemi di bilanciamento del carico per zona di disponibilità, scegli Per parametri AppELB, AZ. Per visualizzare i parametri di un singolo sistema di bilanciamento del carico, inseriscine il nome nel campo di ricerca. Per visualizzare i parametri di una singola zona di disponibilità, inseriscine il nome nel campo di ricerca.
   - Per visualizzare solo i parametri segnalati per i sistemi di bilanciamento del carico per zona di disponibilità e gruppo di destinazioni, scegli Per parametri AppELB, AZ, GD. Per visualizzare i parametri di un singolo sistema di bilanciamento del carico, inseriscine il nome nel campo di ricerca. Per visualizzare i parametri di un singolo gruppo di destinazioni, inserisci il relativo nome nel campo di ricerca. Per visualizzare i parametri di una singola zona di disponibilità, inseriscine 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/ApplicationELB
```

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

Utilizzate il seguente get-metric-statisticscomando get statistics per la metrica e la dimensione specificate. 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/ApplicationELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=app/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2016-04-18T00:00:00Z --end-time 2016-04-21T00:00:00Z
```

Di seguito è riportato un output di esempio:

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2016-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Log di accesso dell'Application Load Balancer

Elastic Load Balancing fornisce log di accesso che acquisiscono informazioni dettagliate sulle richieste inviate al tuo load balancer. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi che potresti incontrare.

I log di accesso sono una funzionalità facoltativa di Elastic Load Balancing che viene disabilitata per impostazione predefinita. Dopo aver abilitato i log di accesso per il sistema di bilanciamento del carico, Elastic Load Balancing acquisisce i log e li archivia nel bucket Amazon S3 specificato come file compressi. Puoi disabilitare i log di accesso in qualsiasi momento.

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, consulta Prezzi di Amazon S3.

Indice

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_app.load-balancer-id_end-time_ip-address_random-string.log.gz
```

bucket

Nome del bucket S3.

prefisso

(Facoltativo) Il prefisso (gerarchia logica) per il bucket. Il prefisso specificato non deve includere la stringa `AWSLogs`. Per ulteriori informazioni, consulta Organizzazione degli oggetti utilizzando i prefissi.

`AWSLogs`

Aggiungiamo la parte del nome del file che inizia con `AWSLogs` dopo il nome del bucket e il prefisso facoltativo specificato.

aws-account-id

L'ID AWS dell'account 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 20140215T2340Z contiene le voci delle richieste effettuate tra le 23:35 e le 23:40 UTC o GMT.

ip-address

L'indirizzo IP del nodo del load balancer che ha gestito la richiesta. Per un load balancer interno, si tratta di un indirizzo IP privato.

random-string

Una stringa casuale generata dal sistema.

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

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-
east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/
us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_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 la gestione del ciclo di vita degli oggetti nella Guida per l'utente di Amazon S3.

Voci dei log di accesso

Elastic Load Balancing registra le richieste inviate al sistema di bilanciamento del carico, incluse le richieste mai arrivate alla destinazione. Ad esempio, se un client invia una richiesta errata o se non sono presenti destinazioni integre a rispondere alla richiesta, questa viene comunque registrata. Elastic Load Balancing non registra le richieste di controllo dell'integrità.

Ogni voce di registro contiene i dettagli di una singola richiesta (o connessione nel caso di WebSockets) effettuata al sistema di bilanciamento del carico. Infatti WebSockets, una voce viene scritta solo dopo la chiusura della connessione. Se non è possibile stabilire la connessione aggiornata, la voce è la medesima di una richiesta HTTP o HTTPS.

> **Important**
>
> Elastic Load Balancing registra le richieste nel miglior modo possibile. Ti consigliamo di utilizzare i log di accesso per comprendere la natura delle richieste e non come resoconto completo di tutte le richieste.

Indice

Sintassi

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. Ti consigliamo di ignorare i campi inattesi alla fine della voce di log.

Campo	Descrizione
type	Il tipo di richiesta o di connessione. I valori possibili sono i seguenti (ignora eventuali altri valori): • `http`: HTTP • `https`: HTTP su TLS • `h2`: HTTP/2 su TLS • `grpcs`: gRPC su TLS • `ws` — WebSockets • `wss`— WebSockets tramite TLS
time	L'ora in cui il sistema di bilanciamento del carico ha generato una risposta al client, nel formato ISO 8601. Perché WebSockets, questo è il momento in cui la connessione viene chiusa.
elb	L'ID risorsa del sistema di bilanciamento del carico. Se state analizzan do le voci del registro di accesso, tenete presente che le risorse IDs possono contenere barre (/).
client:port	L'indirizzo IP e la porta del client che esegue la richiesta. Se il sistema di bilanciamento del carico ha un proxy, questo campo contiene l'indirizzo IP del proxy.
target:port	L'indirizzo IP e la porta della destinazione che ha elaborato la richiesta.

Campo	Descrizione
	Se il client non ha inviato una richiesta completa, il sistema di bilanciamento del carico non è in grado di inviare la richiesta a una destinazione e questo valore è impostato su -. Se la destinazione è una funzione Lambda, questo valore è impostato su -. Se la richiesta è bloccata da AWS WAF, questo valore è impostato su -.
request_processing_time	Il tempo totale trascorso (in secondi, con precisione al millisecondo) dal momento in cui il sistema di bilanciamento del carico ha ricevuto la richiesta al momento in cui l'ha inviata a una destinazione. Questo valore è impostato su -1 se il sistema di bilanciamento del carico non è in grado di inviare la richiesta a una destinazione. Questo può accadere se la destinazione chiude la connessione prima del timeout di inattività o se il client invia una richiesta errata. Questo valore può essere impostato su -1 anche se non è possibile stabilire una connessione TCP con la destinazione prima del raggiungimento del timeout di connessione TCP di 10 secondi. Se AWS WAF è abilitato per l'Application Load Balancer o il tipo di destinazione è una funzione Lambda, viene conteggiato il tempo impiegato dal client per inviare i dati richiesti per le richieste POST. `request_processing_time`

Campo	Descrizione
target_processing_time	Il tempo totale trascorso (in secondi, con precisione al millisecondo) dal momento in cui il sistema di bilanciamento del carico ha inviato la richiesta a una destinazione fino a quando la destinazione non ha iniziato a inviare le intestazioni di risposta. Questo valore è impostato su -1 se il sistema di bilanciamento del carico non è in grado di inviare la richiesta a una destinazione. Questo può accadere se la destinazione chiude la connessione prima del timeout di inattività o se il client invia una richiesta errata. Questo valore può anche essere impostata su -1 se la destinazione registrata non risponde prima del timeout di inattività. Se non AWS WAF è abilitato per l'Application Load Balancer, viene conteggiato il tempo impiegato dal client per inviare i dati richiesti per le richieste POST. `target_processing_time`
response_processing_time	Il tempo totale trascorso (in secondi, con precisione al millisecondo) dal momento in cui il sistema di bilanciamento del carico ha ricevuto l'intestazione di risposta dalla destinazione finché non ha iniziato a inviare la risposta al client. Sono inclusi sia il tempo di inserimento nella coda del load balancer che il tempo di acquisizione della connessione dal load balancer al client. Questo valore è impostato su -1 se il sistema di bilanciamento del carico non riceve una risposta da una destinazione. Questo può accadere se la destinazione chiude la connessione prima del timeout di inattività o se il client invia una richiesta errata.
elb_status_code	Il codice di stato della risposta generata dal load balancer, dalla regola di risposta fissa o dal codice di risposta AWS WAF personalizzato per le azioni di blocco.
target_status_code	Il codice di stato della risposta dalla destinazione. Questo valore viene registrato solo se è stata stabilita una connessione con la destinazione e quest'ultima ha inviato una risposta. Altrimenti il valore è impostato su -.

Campo	Descrizione
received_bytes	Le dimensioni della richiesta, in byte, ricevuta dal client (richiedente). Per le richieste HTTP, sono incluse le intestazioni. Infatti WebSockets, questo è il numero totale di byte ricevuti dal client sulla connessione.
sent_bytes	Le dimensioni della risposta, in byte, inviata al client (richiedente). Per le richieste HTTP, questo include le intestazioni e il corpo della risposta. Infatti WebSockets, questo è il numero totale di byte inviati al client durante la connessione. Le intestazioni TCP e il payload di handshake TLS non vengono conteggiati e non hanno alcuna correlazione con in. `DataTransfer-Out-Bytes` AWS Cost Explorer
"request"	La richiesta di riga dal client, tra virgolette doppie e registrata utilizzan do il formato: metodo HTTP + protocollo://host:port/uri + versione HTTP. Il load balancer conserva l'URL inviato dal client così com'è quando registra l'URI della richiesta. Non imposta il tipo di contenuto per il file di log di accesso. Quando elabori questo campo, considera in che modo il client ha inviato l'URL.
"user_agent"	Una stringa utente-agente che identifica il client che ha originato la richiesta, racchiusa tra virgolette doppie. La stringa è composta da uno o più identificatori di prodotto, prodotto[/versione]. Se la stringa è più lunga di 8 KB viene troncata.
ssl_cipher	[Listener HTTPS] La crittografia SSL. Questo valore è impostato su - se il listener non è un listener HTTPS.
ssl_protocol	[Listener HTTPS] Il protocollo SSL. Questo valore è impostato su - se il listener non è un listener HTTPS.
target_group_arn	L'Amazon Resource Name (ARN) del gruppo di destinazioni.
"trace_id"	Il contenuto dell'intestazione X-Amzn-Trace-Id, racchiuso tra virgolette doppie.

Campo	Descrizione
"domain_name"	[Listener HTTPS] Il dominio SNI fornito dal client durante l'handshake TLS, racchiuso tra virgolette doppie. Questo valore viene impostato su - se il client non supporta SNI o il dominio non corrisponde a un certificato e il certificato predefinito viene presentato al client.
"chosen_cert_arn"	[Listener HTTPS] L'ARN del certificato presentato al client, racchiuso tra virgolette doppie. Questo valore è impostato su `session-reused` se la sessione è riutilizzata. Questo valore è impostato su - se il listener non è un listener HTTPS.
matched_rule_priority	Il valore di priorità della regola che corrisponde alla richiesta. Se era presente una regola corrispondente, si tratta di un valore da 1 a 50.000. Se non erano presenti regole corrispondenti ed è stata effettuata l'operazione predefinita, il valore è impostato su 0. Se si verifica un errore durante la valutazione delle regole, il valore è impostato su -1; per qualsiasi altro errore, è impostato su -.
request_creation_time	L'ora in cui il sistema di bilanciamento del carico ha ricevuto la richiesta dal client, nel formato ISO 8601.
"actions_executed"	Le operazioni effettuate durante l'elaborazione della richiesta, racchiuse tra virgolette doppie. Questo valore è un elenco separato da virgole che può includere i valori descritti in Operazioni intraprese. Se non è stata effettuata alcuna operazione, come per una richiesta errata, il valore è impostato su -.
"redirect_url"	L'URL della destinazione di reindirizzamento per l'intestazione Location della risposta HTTP, racchiuso tra virgolette doppie. Se non è stata effettuata alcuna operazione di reindirizzamento, il valore è impostato su -.
"error_reason"	Il codice di motivo errore, racchiuso tra virgolette doppie. Se la richiesta non è riuscita, si tratta di uno dei codici di errore descritti in Codici dei motivi degli errori. Se le azioni intraprese non includono un'operazione di autenticazione o il target non è una funzione Lambda, questo valore è impostato su - .

Campo	Descrizione
"target:port_list"	Un elenco delimitato da spazi di indirizzi IP e porte per le destinazioni che hanno elaborato questa richiesta, racchiuse tra virgolette doppie. Attualmente, questo elenco può contenere un elemento e corrisponde al campo target:port. Se il client non ha inviato una richiesta completa, il sistema di bilanciam ento del carico non è in grado di inviare la richiesta a una destinazione e questo valore è impostato su -. Se la destinazione è una funzione Lambda, questo valore è impostato su -. Se la richiesta è bloccata da AWS WAF, questo valore è impostato su -.
"target_status_cod e_list"	Un elenco delimitato da spazi di codici di stato dalle risposte delle destinazioni, racchiuse tra virgolette doppie. Attualmente, questo elenco può contenere un elemento e corrisponde al campo target_status_code. Questo valore viene registrato solo se è stata stabilita una connessione con la destinazione e quest'ultima ha inviato una risposta. Altrimenti il valore è impostato su -.
"classification"	La classificazione della mitigazione della desincronizzazione, racchiusa tra virgolette doppie. Se la richiesta non è conforme a RFC 7230, i valori possibili sono Accettabile, Ambiguo e Grave. Se la richiesta è conforme a RFC 7230, questo valore è impostato su -.
"classification_reason"	Il codice del motivo della classificazione, racchiuso tra virgolette doppie. Se la richiesta non è conforme a RFC 7230, si tratta di uno dei codici di classificazione descritti in Motivi della classificazione. Se la richiesta è conforme a RFC 7230, questo valore è impostato su -.

Campo	Descrizione
conn_trace_id	L'ID di tracciabilità della connessione è un ID opaco univoco utilizzato per identificare ogni connessione. Dopo aver stabilito una connessione con un client, le richieste successive di questo client conterranno questo ID nelle rispettive voci del registro di accesso. Questo ID funge da chiave esterna per creare un collegamento tra la connessione e i log di accesso.

Operazioni intraprese

Il sistema di bilanciamento del carico archivia le operazioni intraprese nel campo actions_executed del log di accesso.

- `authenticate`: il sistema di bilanciamento del carico ha convalidato la sessione, autenticato l'utente e aggiunto le informazioni dell'utente alle intestazioni della richiesta, come specificato dalla configurazione della regola.
- `fixed-response`: il sistema di bilanciamento del carico ha generato una risposta fissa, come specificato dalla configurazione della regola.
- `forward`: il sistema di bilanciamento del carico ha inoltrato la richiesta a una destinazione, come specificato dalla configurazione della regola.
- `redirect`: il sistema di bilanciamento del carico ha reindirizzato la richiesta a un altro URL, come specificato dalla configurazione della regola.
- `waf`: il sistema di bilanciamento del carico ha inoltrato la richiesta a AWS WAF per determinare se la richiesta deve essere inoltrata alla destinazione. Se questa è l'azione finale, AWS WAF stabilisce che la richiesta deve essere rifiutata. Per impostazione predefinita, le richieste rifiutate da AWS WAF verranno registrate come «403" nel campo. `elb_status_code` Se AWS WAF è configurato per rifiutare le richieste con un codice di risposta personalizzato, il `elb_status_code` campo rifletterà il codice di risposta configurato.
- `waf-failed`— Il sistema di bilanciamento del carico ha tentato di inoltrare la richiesta a AWS WAF, ma questo processo non è riuscito.

Motivi della classificazione

Se una richiesta non è conforme a RFC 7230, il sistema di bilanciamento del carico archivia uno dei seguenti codici nel campo classification_reason del log di accesso. Per ulteriori informazioni, consulta Modalità di mitigazione della desincronizzazione.

Codice	Descrizione	Classificazione
`AmbiguousUri`	L'URI della richiesta contiene caratteri di controllo.	Ambiguo
`BadContentLength`	L'intestazione Content-Length contiene un valore che non può essere analizzato o non è un numero valido.	Grave
`BadHeader`	Un'intestazione contiene un carattere nullo o un'andata a capo.	Grave
`BadTransferEncoding`	L'intestazione Transfer-Encoding contiene un valore non valido.	Grave
`BadUri`	L'URI della richiesta contiene un carattere nullo o un'andata a capo.	Grave
`BadMethod`	Il formato del metodo di richiesta è errato.	Grave
`BadVersion`	Il formato della versione della richiesta è errato.	Grave
`BothTeClPresent`	La richiesta contiene sia un'intestazione Transfer-Encoding che un'intestazione Content-Length.	Ambiguo
`DuplicateContentLength`	Esistono più intestazioni Content-Length con lo stesso valore.	Ambiguo
`EmptyHeader`	Un'intestazione è vuota o c'è una riga con solo spazi.	Ambiguo

Codice	Descrizione	Classificazione
`GetHeadZeroContentLength`	Esiste un'intestazione Content-Length con un valore pari a 0 per una richiesta GET o HEAD.	Accettabile
`MultipleContentLength`	Esistono più intestazioni Content-Length con valori diversi.	Grave
`MultipleTransferEncodingChunked`	Esistono più Transfer-Encoding: intestazioni a blocchi.	Grave
`NonCompliantHeader`	Un'intestazione contiene un carattere non ASCII o di controllo.	Accettabile
`NonCompliantVersion`	La versione della richiesta contiene un valore non valido.	Accettabile
`SpaceInUri`	L'URI della richiesta contiene uno spazio che non ha codifica URL.	Accettabile
`SuspiciousHeader`	C'è un'intestazione che può essere normalizzata per Transfer-Encoding o Content-Length utilizzando tecniche comuni di normalizzazione del testo.	Ambiguo
`SuspiciousTeClPresent`	La richiesta contiene sia un'intestazione Transfer-Encoding che un'intestazione Content-Length, di cui almeno una è sospetta.	Grave
`UndefinedContentLengthSemantics`	Esiste un'intestazione Content-Length definita per una richiesta GET o HEAD.	Ambiguo
`UndefinedTransferEncodingSemantics`	Esiste un'intestazione Transfer-Encoding definita per una richiesta GET o HEAD.	Ambiguo

Codici dei motivi degli errori

Se il sistema di bilanciamento del carico non può completare un'operazione di autenticazione, il sistema di bilanciamento del carico archivia uno dei seguenti codici di motivo nel campo error_reason del log di accesso. Il load balancer incrementa anche la metrica corrispondente. CloudWatch Per ulteriori informazioni, consulta Autenticazione degli utenti tramite Application Load Balancer.

Codice	Descrizione	Parametro
`AuthInvalidCookie`	Il cookie di autenticazione non è valido.	`ELBAuthFailure`
`AuthInvalidGrantError`	Il codice per la concessione delle autorizzazioni dall'endpoint del token non è valido.	`ELBAuthFailure`
`AuthInvalidIdToken`	Il token dell'ID non è valido.	`ELBAuthFailure`
`AuthInvalidStateParam`	Il parametro dello stato non è valido.	`ELBAuthFailure`
`AuthInvalidTokenResponse`	La risposta dall'endpoint del token non è valida.	`ELBAuthFailure`
`AuthInvalidUserinfoResponse`	La risposta dall'endpoint di informazione dell'utente non è valida.	`ELBAuthFailure`
`AuthMissingCodeParam`	La risposta di autenticazione dall'endpoint di autorizzazione non ha un parametro di query denominato "codice".	`ELBAuthFailure`
`AuthMissingHostHeader`	La risposta di autenticazione dall'endpoint di autorizzazione non ha un campo di intestazione host.	`ELBAuthError`

Codice	Descrizione	Parametro
`AuthMissingStateParam`	La risposta di autenticazione dall'endpoint di autorizzazione non ha un campo di intestazione host.	`ELBAuthFailure`
`AuthTokenEpRequestFailed`	C'è una risposta di errore (non-2XX) dall'endpoint del token.	`ELBAuthError`
`AuthTokenEpRequestTimeout`	Il load balancer non è in grado di comunicare con l'endpoint del token o l'endpoint del token non risponde entro 5 secondi.	`ELBAuthError`
`AuthUnhandledException`	Il sistema di bilanciamento del carico ha incontrato un'eccezione non gestita.	`ELBAuthError`
`AuthUserinfoEpRequestFailed`	C'è una risposta di errore (non 2XX) dall'endpoint di informazione dell'utente IdP	`ELBAuthError`
`AuthUserinfoEpRequestTimeout`	Il load balancer non è in grado di comunicare con l'endpoint IdP user info oppure l'endpoint User Info non risponde entro 5 secondi.	`ELBAuthError`
`AuthUserinfoResponseSizeExceeded`	La dimensione delle richieste restituite dall'IdP supera i 11K byte.	`ELBAuthUserClaimsSizeExceeded`

Se una richiesta a un gruppo di destinazioni ponderato ha esito negativo, il sistema di bilanciamento del carico archivia uno dei seguenti codici di errore nel campo error_reason del log di accesso.

Codice	Descrizione
`AWSALBTGCookieInvalid`	Il AWSALBTG cookie, utilizzato con gruppi target ponderati, non è valido. Ad esempio, il bilanciamento del carico restituisce questo errore quando i valori dei cookie sono URL codificati.

Codice	Descrizione
`WeightedTargetGroupsUnhandledException`	Il sistema di bilanciamento del carico ha incontrato un'eccezione non gestita.

Se una richiesta a una funzione Lambda ha esito negativo, il sistema di bilanciamento del carico archivia uno dei seguenti codici di motivo nel campo error_reason del log di accesso. Il load balancer incrementa anche la metrica corrispondente. CloudWatch Per ulteriori informazioni, consultare l'operazione Lambda Invoke.

Codice	Descrizione	Parametro
`LambdaAccessDenied`	Il sistema di bilanciamento del carico non aveva l'autorizzazione a chiamare la funzione Lambda.	`LambdaUserError`
`LambdaBadRequest`	Invocazione Lambda non riuscita perché le intestazioni o il corpo della richiesta client non contenevano solo caratteri UTF-8.	`LambdaUserError`
`LambdaConnectionError`	Il sistema di bilanciamento del carico non è in grado di connettersi a Lambda.	`LambdaInternalError`
`LambdaConnectionTimeout`	Un tentativo di connessione a Lambda è scaduto.	`LambdaInternalError`
`LambdaEC2AccessDeniedException`	Amazon EC2 ha negato l'accesso a Lambda durante l'inizializzazione della funzione.	`LambdaUserError`
`LambdaEC2ThrottledException`	Amazon ha EC2 limitato Lambda durante l'inizializzazione della funzione.	`LambdaUserError`

Codice	Descrizione	Parametro
`LambdaEC2UnexpectedException`	Amazon EC2 ha riscontrato un'eccezione inaspettata durante l'inizializzazione della funzione.	`LambdaUserError`
`LambdaENILimitReachedException`	Lambda non è stato in grado di creare un'interfaccia di rete nel VPC specificato nella configurazione della funzione Lambda poiché è stato superato il limite di interfacce di rete.	`LambdaUserError`
`LambdaInvalidResponse`	La risposta dalla funzione Lambda è errata o non sono presenti i campi obbligatori.	`LambdaUserError`
`LambdaInvalidRuntimeException`	La versione specificata del runtime di Lambda non è supportata.	`LambdaUserError`
`LambdaInvalidSecurityGroupIDException`	L'ID del gruppo di sicurezza specificato nella configurazione della funzione Lambda non è valido.	`LambdaUserError`
`LambdaInvalidSubnetIDException`	L'ID della sottorete specificato nella configurazione della funzione Lambda non è valido.	`LambdaUserError`
`LambdaInvalidZipFileException`	Lambda non è stato in grado di decomprimere il file zip della funzione specificato.	`LambdaUserError`
`LambdaKMSAccessDeniedException`	Lambda non è stato in grado di decrittare le variabili di ambiente poiché è stato rifiutato l'accesso alla chiave KMS. Verifica le autorizzazioni KMS della funzione Lambda.	`LambdaUserError`

Codice	Descrizione	Parametro
`LambdaKMSDisabledException`	Lambda non è stato in grado di decrittare le variabili di ambiente poiché la chiave KMS specificata è disabilitata. Verifica le autorizzazioni della chiave KMS della funzione Lambda.	`LambdaUserError`
`LambdaKMSInvalidStateException`	Lambda non è stato in grado di decrittare le variabili di ambiente poiché lo stato della chiave KMS non è valido. Verifica le autorizzazioni della chiave KMS della funzione Lambda.	`LambdaUserError`
`LambdaKMSNotFoundException`	Lambda non è stato in grado di decrittare le variabili di ambiente poiché non è stata trovata la KMS. Verifica le autorizzazioni della chiave KMS della funzione Lambda.	`LambdaUserError`
`LambdaRequestTooLarge`	Le dimensioni del corpo della richiesta hanno superato 1 MB.	`LambdaUserError`
`LambdaResourceNotFound`	La funzione Lambda non è stata trovata.	`LambdaUserError`
`LambdaResponseTooLarge`	Le dimensioni della risposta hanno superato 1 MB.	`LambdaUserError`
`LambdaServiceException`	Lambda ha riscontrato un errore interno.	`LambdaInternalError`
`LambdaSubnetIPAddressLimitReachedException`	Lambda non è stato in grado di configurare l'accesso VPC per la funzione Lambda poiché una o più sottoreti non hanno indirizzi IP disponibili.	`LambdaUserError`
`LambdaThrottling`	La funzione Lambda è stata sottoposta a throttling a causa di troppe richieste.	`LambdaUserError`

Codice	Descrizione	Parametro
`LambdaUnhandled`	La funzione Lambda ha riscontrato un'eccezione non gestita.	`LambdaUserError`
`LambdaUnhandledException`	Il sistema di bilanciamento del carico ha incontrato un’eccezione non gestita.	`LambdaInternalError`
`LambdaWebsocketNotSupported`	WebSockets non sono supportati con Lambda.	`LambdaUserError`

Se il load balancer rileva un errore durante l'inoltro delle richieste a AWS WAF, memorizza uno dei seguenti codici di errore nel campo error_reason del log di accesso.

Codice	Descrizione
`WAFConnectionError`	Il sistema AWS WAF di bilanciamento del carico non può connettersi a.
`WAFConnectionTimeout`	La connessione a è AWS WAF scaduta.
`WAFResponseReadTimeout`	Una richiesta da AWS WAF scadere.
`WAFServiceError`	AWS WAF ha restituito un errore 5XX.
`WAFUnhandledException`	Il sistema di bilanciamento del carico ha incontrato un’eccezione non gestita.

Voci di log di esempio

Di seguito sono riportati esempi di voci di log; Nota che il testo di esempio viene visualizzato su più righe solo per facilitarne la lettura.

Esempio di voce HTTP

Nell'esempio seguente viene mostrata una voce di log di un listener HTTP (da porta 80 a porta 80):

```
http 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337262-36d228ad5d99923122bbe354" "-" "-"
0 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.0.1:80" "200" "-" "-"
 TID_1234abcd5678ef90
```

Esempio di voce HTTPS

Nell'esempio seguente viene mostrata una voce di log di un listener HTTPS (da porta 443 a porta 80):

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-
east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" "10.0.0.1:80" "200" "-"
 "-" TID_1234abcd5678ef90
```

Esempio di voce HTTP/2

Nell'esempio seguente viene mostrata una voce di log di un flusso HTTP/2

```
h2 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.1.252:48160 10.0.0.66:9000 0.000 0.002 0.000 200 200 5 257
"GET https://10.0.2.105:773/ HTTP/2.0" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337327-72bd00b0343d75b906739c42" "-" "-"
1 2018-07-02T22:22:48.364000Z "redirect" "https://example.com:80/" "-" "10.0.0.66:9000"
 "200" "-" "-" TID_1234abcd5678ef90
```

Esempio WebSockets di inserimento

Di seguito è riportato un esempio di voce di registro per una WebSockets connessione.

```
ws 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:40914 10.0.1.192:8010 0.001 0.003 0.000 101 101 218 587
"GET http://10.0.0.30:80/ HTTP/1.1" "-" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.1.192:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Esempio di immissione protetta WebSockets

Di seguito è riportato un esempio di voce di registro per una connessione protetta WebSockets.

```
wss 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:44244 10.0.0.171:8010 0.000 0.001 0.000 101 101 218 786
"GET https://10.0.0.30:443/ HTTP/1.1" "-" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.0.171:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Esempio di voci delle funzioni Lambda

Nell'esempio seguente viene mostrata una voce di log di una richiesta a una funzione Lambda che ha avuto esito positivo:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "-" "-" "-" "-" "-" TID_1234abcd5678ef90
```

Nell'esempio seguente viene mostrata una voce di log di una richiesta a una funzione Lambda che ha avuto esito negativo:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 502 - 34 366
```

```
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "LambdaInvalidResponse" "-" "-" "-" "-"
 TID_1234abcd5678ef90
```

Elaborazione dei file di log di accesso

I file di log di accesso sono compressi. 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. Potresti non essere in grado di elaborare una quantità così grande di dati utilizzando l' line-by-lineelaborazione. 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 la sezione relativa all'Esecuzione di query nei log di Application Load Balancer nella Guida per l'utente di Amazon Athena.
- Loggly
- Splunk
- Sumo logic

Abilitazione dei log di accesso dell'Application Load Balancer

Quando abiliti i log di accesso per il sistema di bilanciamento del carico, devi specificare il nome del bucket S3 in cui il sistema archivierà i log. Il bucket deve avere una policy di bucket che concede a Elastic Load Balancing l'autorizzazione a scrivere nel bucket.

Attività

- Fase 1: Crea un bucket S3
- Fase 2: collegamento di una policy al bucket S3
- Fase 3: configurazione dei log di accesso
- Fase 4: verifica delle autorizzazioni del bucket
- Risoluzione dei problemi

Fase 1: Crea un bucket S3

Quando si abilitano i log di accesso, è necessario specificare un bucket S3 per tali log. È possibile utilizzare un bucket esistente o creare un bucket specifico per i log di accesso. Il bucket deve soddisfare i seguenti requisiti.

Requisiti

- Il bucket deve trovarsi nella stessa regione del load balancer. Il bucket e il load balancer possono essere di proprietà di account differenti.
- L'unica opzione di crittografia lato server supportata è data dalle chiavi gestite da Amazon S3 (SSE-S3). Per ulteriori informazioni, consulta Chiavi di crittografia gestite da Amazon S3 (SSE-S3).

Per creare un bucket S3 utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona Crea bucket.
3. Nella pagina Crea bucket, segui questi passaggi:
   a. In Nome bucket, immettere il nome del bucket. Il nome deve essere univoco rispetto a tutti i nomi di bucket esistenti in Amazon S3. In alcune regioni , possono esistere restrizioni aggiuntive sui nomi bucket. Per ulteriori informazioni, consulta Restrizioni e limitazioni di Bucket nella Amazon S3 User Guide.
   b. Per Regione AWS , seleziona la regione in cui è stato creato il sistema di bilanciamento del carico.
   c. Per la crittografia predefinita, scegli le chiavi gestite da Amazon S3 (SSE-S3).
   d. Seleziona Crea bucket.

Fase 2: collegamento di una policy al bucket S3

Il bucket S3 deve avere una policy che conceda a Elastic Load Balancing 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. Ogni istruzione include informazioni su una singola autorizzazione e contiene una serie di elementi.

Se utilizzi un bucket esistente che ha già una policy collegata, puoi aggiungere alla policy l'istruzione per i log di accesso di Elastic Load Balancing. In questo caso, ti consigliamo di valutare il set di

autorizzazioni risultante per accertarti che queste siano appropriate agli utenti che devono accedere al bucket per i log di accesso.

Policy di bucket disponibili

La policy bucket che utilizzerai dipende dalla zona Regione AWS e dal tipo di zona.

Regioni disponibili a partire da agosto 2022

Questa policy concede le autorizzazioni al servizio di consegna dei log specificato. Utilizza questa politica per i sistemi di bilanciamento del carico nelle seguenti regioni:

- Asia Pacific (Hyderabad)
- Asia Pacifico (Malesia)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Taipei)
- Asia Pacifico (Tailandia)
- Canada occidentale (Calgary)
- Europa (Spagna)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente (Emirati Arabi Uniti)
- Messico (centrale)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
```

```
  ]
}
```

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Regioni disponibili prima di agosto 2022

Questa policy concede le autorizzazioni all'ID dell'account del sistema di bilanciamento del carico elastico specificato. Utilizza questa politica per i sistemi di bilanciamento del carico nelle regioni elencate di seguito.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
```

```
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Per`Principal`, sostituisci *`elb-account-id`* con l'ID dell'account Elastic Load Balancing per la regione del load balancer:

- Stati Uniti orientali (Virginia settentrionale): 127311923021
- Stati Uniti orientali (Ohio): 033677994240
- Stati Uniti occidentali (California settentrionale): 027434742980
- Stati Uniti occidentali (Oregon): 797873946194
- Africa (Città del Capo): 098369216593
- Asia Pacifico (Hong Kong): 754344448648
- Asia Pacifico (Giacarta) – 589379963580
- Asia Pacifico (Mumbai): 718504428378
- Asia Pacifico (Osaka-Locale): 383597477331
- Asia Pacifico (Seoul): 600734575887
- Asia Pacifico (Singapore): 114774131450
- Asia Pacifico (Sydney): 783225319266
- Asia Pacifico (Tokyo): 582318560864
- Canada (Centrale): 985666609251
- Europa (Francoforte): 054676820928
- Europa (Irlanda): 156460612806
- Europa (Londra): 652711504416
- Europa (Milano): 635631232127
- Europa (Parigi): 009996457667
- Europa (Stoccolma): 897822967062
- Medio Oriente (Bahrein): 076674570225
- Sud America (San Paolo): 507241528517

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regioni

Questa policy concede le autorizzazioni all'ID dell'account del sistema di bilanciamento del carico elastico specificato. Utilizza questa politica per i sistemi di bilanciamento del carico nelle AWS GovCloud (US) regioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
```

```
  ]
}
```

Per`Principal`, sostituisci *`elb-account-id`* con l'ID dell'account Elastic Load Balancing per la regione del load balancer:

- AWS GovCloud (Stati Uniti occidentali) — 048591011584
- AWS GovCloud (Stati Uniti orientali) — 190560391635

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN del bucket S3 specificato dipende dal fatto che si intenda includere un prefisso quando si abilita il collegamento ai log di accesso (passaggio 3).

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Zone Outpost

La policy seguente concede le autorizzazioni al servizio di consegna dei log specificato. Utilizzare questa policy per i sistemi di bilanciamento del carico nelle zone Outpost.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
```

```
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN del bucket S3 specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

> **Ottimizzazione della sicurezza**
>
> Utilizza i seguenti suggerimenti per migliorare la sicurezza del tuo bucket S3.

Rivedi la tua politica sui bucket

- Utilizza il percorso completo delle risorse, inclusa la parte relativa all'ID dell'account dell'ARN del bucket S3. Non utilizzare caratteri jolly (*) nella parte relativa all'ID dell'account dell'ARN del bucket S3.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
```

- Utilizzalo `aws:SourceArn` per assicurarti che solo i sistemi di bilanciamento del carico della regione e dell'account specificati possano utilizzare il tuo bucket.

```
"Condition": {
    "ArnLike": {
        "aws:SourceArn":
 "arn:aws:elasticloadbalancing:region:123456789012:loadbalancer/*"
    }
}
```

- Usa `aws:SourceOrgId` with `aws:SourceArn` per assicurarti che solo i sistemi di bilanciamento del carico dell'organizzazione specificata possano utilizzare il tuo bucket.

```
"Condition": {
    "StringEquals": {
        "aws:SourceOrgId": "o-1234567890"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    }
}
```

- Se hai una `Deny` dichiarazione per impedire l'accesso ai principali di servizio ad eccezione di quelli esplicitamente consentiti, assicurati di aggiungerli `logdelivery.elasticloadbalancing.amazonaws.com` all'elenco dei principali di servizio consentiti. Ad esempio, se hai utilizzato la `aws:PrincipalServiceNamesList` condizione, aggiungi `logdelivery.elasticloadbalancing.amazonaws.com` quanto segue:

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Condition": {
      "StringNotEqualsIfExists": {
          "aws:PrincipalServiceNamesList": [
              "logdelivery.elasticloadbalancing.amazonaws.com",
              "service.amazonaws.com"
          ]
      }
  }
```

```
}
```

Se hai usato l'`NotPrincipal`elemento, aggiungi `logdelivery.elasticloadbalancing.amazonaws.com` quanto segue. Tieni presente che ti consigliamo di utilizzare la chiave di `aws:PrincipalServiceNamesList` condizione `aws:PrincipalServiceName` o per consentire esplicitamente i principali del servizio invece di utilizzare l'`NotPrincipal`elemento. Per ulteriori informazioni, consulta NotPrincipal.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "service.amazonaws.com"
    ]
  }
},
```

Collegamento di una policy del bucket per i log di accesso al bucket utilizzando la console di Amazon S3.

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il nome del bucket per aprirne la pagina dei dettagli.
3. Scegli Autorizzazioni quindi seleziona Policy del bucket, Modifica.
4. Crea o aggiorna la policy del bucket per concedere le autorizzazioni richieste.
5. Scegli Save changes (Salva modifiche).

Fase 3: configurazione dei log di accesso

Utilizza la seguente procedura per configurare i log di accesso per acquisire le informazioni sulle richieste e inviare i file di registro al tuo bucket S3.

Requisiti

Il bucket deve soddisfare i requisiti descritti nella fase 1 e devi collegare una policy di bucket come descritto nella fase 2. Se includi un prefisso, questo non deve includere la stringa "». AWSLogs

Per abilitare i log di accesso per il load balancer mediante la console

1. Apri la EC2 console Amazon 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, abilita Log di accesso.
6. In URI S3, inserisci l'URI S3 per i tuoi file di log. L'URI specificato dipende dall'utilizzo di un prefisso.
   - URI con prefisso: s3:///*amzn-s3-demo-logging-bucketlogging-prefix*
   - URI senza prefisso: s3://*amzn-s3-demo-logging-bucket*
7. Scegli Save changes (Salva modifiche).

Per abilitare i log di accesso utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Per gestire il bucket S3 per i log di accesso

Assicurati di disabilitare i log di accesso prima di eliminare il bucket configurato. In caso contrario, se sono presenti un nuovo bucket con lo stesso nome e la policy del bucket richiesta creata però in un account Account AWS non di tua proprietà, Elastic Load Balancing potrebbe scrivere i log di accesso per il sistema di bilanciamento del carico in questo nuovo bucket.

Fase 4: verifica delle autorizzazioni del bucket

Dopo avere abilitato i log di accesso per il load balancer, Elastic Load Balancing convalida il bucket S3 e crea un file di test per garantire che la policy del bucket specifichi le autorizzazioni richieste. Puoi utilizzare la console Amazon S3 per verificare che il file di test sia stato creato. Il file di test non è un file di log di accesso reale: non contiene i record di esempio.

Per verificare che nel bucket sia stato creato un file di test utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il nome del bucket che hai specificato per i log di accesso.
3. Accedi al file di test, `ELBAccessLogTestFile`. La posizione dipende dall'utilizzo di un prefisso.

- Posizione con prefisso:*amzn-s3-demo-logging-bucket*//*logging-prefix*/AWSLogs*123456789012*ELBAccessLogTestFile
- Posizione senza prefisso:*amzn-s3-demo-logging-bucket*///AWSLogs*123456789012*ELBAccessLogTestFile

Risoluzione dei problemi

L'errore di accesso negato può essere provocato da una delle cause elencate di seguito:

- Il bucket deve avere una policy collegata che concede al sistema di bilanciamento del carico elastico l'autorizzazione a scrivere nel bucket. Verifica di utilizzare la policy di bucket corretta per la regione. Verifica che la risorsa ARN utilizzi lo stesso nome di bucket specificato quando i log di accesso sono abilitati. Verifica che la risorsa ARN non includa un prefisso se non hai specificato un prefisso, quando i log di accesso sono abilitati.
- Il bucket utilizza un'opzione di crittografia lato server non supportata. Il bucket deve utilizzare chiavi gestite da Amazon S3 (SSE-S3).

Disabilitazione dei log di accesso dell'Application Load Balancer

Puoi disabilitare i log di accesso per il tuo load balancer in qualsiasi momento. Dopo avere disabilitato i log di accesso, tali log rimangono nel tuo bucket S3 finché non li elimini. Per ulteriori informazioni, consulta Creazione, configurazione e utilizzo dei bucket S3 nella Amazon S3 User Guide.

Disabilitazione dei log di accesso tramite la console

1. Apri la EC2 console Amazon 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. Scegli Save changes (Salva modifiche).

Per disabilitare i log di accesso utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Log di connessione per l'Application Load Balancer

Elastic Load Balancing fornisce log di connessione che raccolgono informazioni dettagliate sulle richieste inviate al sistema di bilanciamento del carico. Ogni registro contiene informazioni come l'indirizzo IP e la porta del client, la porta del listener, il codice TLS e il protocollo utilizzati, la latenza dell'handshake TLS, lo stato della connessione e i dettagli del certificato del client. È possibile utilizzare questi log di connessione per analizzare i modelli di richiesta e risolvere i problemi.

I log di connessione sono una funzionalità opzionale di Elastic Load Balancing che è disabilitata per impostazione predefinita. Dopo aver abilitato i log di connessione per il sistema di bilanciamento del carico, Elastic Load Balancing acquisisce i log e li archivia nel bucket Amazon S3 specificato, come file compressi. Puoi disabilitare i log di connessione in qualsiasi momento.

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, consulta Prezzi di Amazon S3.

Indice

File di registro delle connessioni

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 dei registri delle connessioni utilizzano il seguente formato:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/
conn_log_aws-account-id_elasticloadbalancing_region_app.load-balancer-id_end-time_ip-
address_random-string.log.gz
```

bucket

Nome del bucket S3.

prefisso

(Facoltativo) Il prefisso (gerarchia logica) per il bucket. Il prefisso specificato non deve includere la stringa `AWSLogs`. Per ulteriori informazioni, consulta Organizzazione degli oggetti utilizzando i prefissi.

`AWSLogs`

Aggiungiamo la parte del nome del file che inizia con `AWSLogs` dopo il nome del bucket e il prefisso facoltativo specificato.

aws-account-id

L'ID AWS dell'account 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 20140215T2340Z contiene le voci delle richieste effettuate tra le 23:35 e le 23:40 UTC o GMT.

ip-address

L'indirizzo IP del nodo del load balancer che ha gestito la richiesta. Per un load balancer interno, si tratta di un indirizzo IP privato.

random-string

Una stringa casuale generata dal sistema.

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

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/
conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_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 la gestione del ciclo di vita degli oggetti nella Guida per l'utente di Amazon S3.

Voci di log del registro di connessione

Ogni tentativo di connessione ha una voce in un file di registro della connessione. Il modo in cui vengono inviate le richieste dei client è determinato dal fatto che la connessione sia persistente o non persistente. Le connessioni non persistenti hanno un'unica richiesta, che crea una singola voce nel registro degli accessi e nel registro delle connessioni. Le connessioni persistenti hanno più richieste, il che crea più voci nel registro degli accessi e una singola voce nel registro delle connessioni.

Indice

Sintassi

La tabella seguente descrive i campi di una voce del registro delle connessioni, in ordine. Tutti i campi sono delimitati da spazi. Quando ne vengono introdotti di nuovi, i campi vengono aggiunti alla fine della voce del log. Ti consigliamo di ignorare i campi inattesi alla fine della voce di log.

Campo	Descrizione
timestamp	L'ora, in formato ISO 8601, in cui il sistema di bilanciamento del carico ha stabilito o non è riuscito a stabilire una connessione.

Campo	Descrizione
client_ip	L'indirizzo IP del client richiedente.
client_port	La porta del client richiedente.
listener_port	La porta del listener del load balancer che riceve la richiesta del client.
tls_protocol	[HTTPS listener] Il SSL/TLS protocollo usato durante le strette di mano. Questo campo è impostato - per non richieste. SSL/TLS
tls_cipher	[HTTPS listener] Il SSL/TLS protocollo usato durante le strette di mano. Questo campo è impostato - per non richieste. SSL/TLS
tls_handshake_latency	[HTTPS listener] Il tempo totale in secondi, con una precisione di millisecondi, è trascorso durante la creazione di una stretta di mano riuscita. Questo campo è impostato su quando: - • La richiesta in arrivo non è una SSL/TLS richiesta. • La stretta di mano non è stata stabilita correttamente.
leaf_client_cert_subject	[HTTPS listener] Il nome dell'oggetto del certificato del client leaf. Questo campo è impostato su - quando: • La richiesta in arrivo non è una SSL/TLS richiesta. • Il listener di load balancer non è configurato con MTL abilitato. • Il server non è in grado di ricevere load/parse il certificato Leaf Client.
leaf_client_cert_idity	[HTTPS listener] La validità, con `not-before` e `not-after` in formato ISO 8601, del certificato del client leaf. Questo campo è impostato su quando: - • La richiesta in arrivo non è una SSL/TLS richiesta. • Il listener di load balancer non è configurato con MTL abilitato. • Il server non è in grado di ricevere load/parse il certificato Leaf Client.

Campo	Descrizione
leaf_client_cert_serial_number	[HTTPS listener] Il numero di serie del certificato del client leaf. Questo campo è impostato su - quando: • La richiesta in arrivo non è una SSL/TLS richiesta. • Il listener di load balancer non è configurato con MTL abilitato. • Il server non è in grado di ricevere load/parse il certificato Leaf Client.
tls_verify_status	[HTTPS listener] Lo stato della richiesta di connessione. Questo valore è `Success` se la connessione è stata stabilita correttamente. In caso di connessione non riuscita, il valore è`Failed:$error_code` .
conn_trace_id	L'ID di tracciabilità della connessione è un ID opaco univoco utilizzato per identificare ogni connessione. Dopo aver stabilito una connessione con un client, le richieste successive di questo client contengono questo ID nelle rispettive voci del registro di accesso. Questo ID funge da chiave esterna per creare un collegamento tra la connessione e i log di accesso.

Codici dei motivi degli errori

Se il sistema di bilanciamento del carico non è in grado di stabilire una connessione, memorizza uno dei seguenti codici motivo nel registro delle connessioni.

Codice	Descrizione
`ClientCertMaxChainDepthExceeded`	La profondità massima della catena di certificati del client è stata superata
`ClientCertMaxSizeExceeded`	La dimensione massima del certificato client è stata superata
`ClientCertCrlHit`	Il certificato client è stato revocato dalla CA

Codice	Descrizione	
`ClientCertCrlProcessingError`	Errore di elaborazione CRL	
`ClientCertUntrusted`	Il certificato client non è attendibile	
`ClientCertNotYetValid`	Il certificato client non è ancora valido	
`ClientCertExpired`	Il certificato client è scaduto	
`ClientCertTypeUnsupported`	Il tipo di certificato client non è supportato	
`ClientCertInvalid`	Il certificato client non è valido	
`ClientCertPurposeInvalid`	Lo scopo del certificato client non è valido	
`ClientCertRejected`	Il certificato client viene rifiutato dalla convalida personalizzata del server	
`UnmappedConnectionError`	Errore di connessione in runtime non mappato	

Voci di log di esempio

Di seguito sono riportati alcuni esempi di voci del registro di connessione. Si noti che il testo di esempio viene visualizzato su più righe solo per facilitarne la lettura.

Di seguito è riportato un esempio di voce di registro relativa a una connessione riuscita con un listener HTTPS con la modalità di verifica TLS reciproca abilitata sulla porta 443.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 4.036
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Success TID_3180a73013c8ca4bac2f731159d4b0fe
```

Di seguito è riportato un esempio di voce di registro relativa a una connessione non riuscita con un listener HTTPS con la modalità di verifica TLS reciproca abilitata sulla porta 443.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 -
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Failed:ClientCertUntrusted TID_1c71a68d70587445ad5127ff8b2687d7
```

Elaborazione dei file di registro della connessione

I file di registro delle connessioni 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. Potresti non essere in grado di elaborare una quantità così grande di dati utilizzando l' line-by-lineelaborazione. Pertanto, potresti dover utilizzare gli strumenti di analisi che offrono soluzioni di elaborazione parallela. Ad esempio, è possibile utilizzare i seguenti strumenti analitici per analizzare ed elaborare i registri di connessione:

- Amazon Athena è un servizio di query interattivo che semplifica l'analisi dei dati in Amazon S3 con SQL standard.
- Loggly
- Splunk
- Sumo logic

Abilita i log di connessione per il tuo Application Load Balancer

Quando abiliti i log di connessione per il tuo load balancer, devi specificare il nome del bucket S3 in cui il load balancer memorizzerà i log. Il bucket deve avere una policy di bucket che concede a Elastic Load Balancing l'autorizzazione a scrivere nel bucket.

Attività

- Fase 1: Crea un bucket S3
- Fase 2: collegamento di una policy al bucket S3
- Fase 3: Configurazione dei log di connessione
- Fase 4: verifica delle autorizzazioni del bucket
- Risoluzione dei problemi

Fase 1: Crea un bucket S3

Quando abiliti i log di connessione, devi specificare un bucket S3 per i log di connessione. È possibile utilizzare un bucket esistente o creare un bucket specifico per i log di connessione. Il bucket deve soddisfare i seguenti requisiti.

Requisiti

- Il bucket deve trovarsi nella stessa regione del load balancer. Il bucket e il load balancer possono essere di proprietà di account differenti.
- L'unica opzione di crittografia lato server supportata è data dalle chiavi gestite da Amazon S3 (SSE-S3). Per ulteriori informazioni, consulta Chiavi di crittografia gestite da Amazon S3 (SSE-S3).

Per creare un bucket S3 utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona Crea bucket.
3. Nella pagina Crea bucket, segui questi passaggi:
    a. In Nome bucket, immettere il nome del bucket. Il nome deve essere univoco rispetto a tutti i nomi di bucket esistenti in Amazon S3. In alcune regioni , possono esistere restrizioni aggiuntive sui nomi bucket. Per ulteriori informazioni, consulta Restrizioni e limitazioni di Bucket nella Amazon S3 User Guide.
    b. Per Regione AWS , seleziona la regione in cui è stato creato il sistema di bilanciamento del carico.
    c. Per la crittografia predefinita, scegli le chiavi gestite da Amazon S3 (SSE-S3).
    d. Seleziona Crea bucket.

Fase 2: collegamento di una policy al bucket S3

Il bucket S3 deve avere una policy relativa ai bucket che conceda a Elastic Load Balancing l'autorizzazione a scrivere i log di connessione 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. Ogni istruzione include informazioni su una singola autorizzazione e contiene una serie di elementi.

Se utilizzi un bucket esistente a cui è già associata una policy, puoi aggiungere l'istruzione per i log di connessione Elastic Load Balancing alla policy. In tal caso, ti consigliamo di valutare il set di autorizzazioni risultante per assicurarti che siano appropriate per gli utenti che devono accedere al bucket per i log di connessione.

Policy di bucket disponibili

La policy del bucket che utilizzerai dipende dalla Regione AWS e dal tipo di zona.

⚠ Migliora la sicurezza utilizzando un ARNs bucket S3 preciso.

- Utilizza il percorso completo delle risorse, non solo l'ARN del bucket S3.
- Includi la parte relativa all'ID dell'account dell'ARN del bucket S3.
- Non utilizzare caratteri jolly (*) nella parte relativa all'ID dell'account dell'ARN del bucket S3.

Regioni disponibili a partire da agosto 2022

Questa policy concede le autorizzazioni al servizio di consegna dei log specificato. Utilizza questa politica per i sistemi di bilanciamento del carico nelle seguenti regioni:

- Asia Pacific (Hyderabad)
- Asia Pacifico (Malesia)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Tailandia)
- Canada occidentale (Calgary)
- Europa (Spagna)
- Europa (Zurigo)
- Israele (Tel Aviv)

- Medio Oriente (Emirati Arabi Uniti)
- Messico (centrale)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN del bucket S3 specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Usare when è NotPrincipalEffectDeny

Se la policy sui bucket di Amazon S3 utilizza `Effect` il valore `Deny` e include `NotPrincipal` come mostrato nell'esempio seguente, assicurati che `logdelivery.elasticloadbalancing.amazonaws.com` sia incluso nell'elenco. `Service`

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

Regioni disponibili prima di agosto 2022

Questa politica concede le autorizzazioni all'account Elastic Load Balancing specificato. Utilizza questa politica per i sistemi di bilanciamento del carico nelle regioni elencate di seguito.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Per`Principal`, sostituisci *`elb-account-id`* con l'ID dell'account Elastic Load Balancing per la regione del load balancer:

- Stati Uniti orientali (Virginia settentrionale): 127311923021
- Stati Uniti orientali (Ohio): 033677994240
- Stati Uniti occidentali (California settentrionale): 027434742980
- Stati Uniti occidentali (Oregon): 797873946194
- Africa (Città del Capo): 098369216593
- Asia Pacifico (Hong Kong): 754344448648
- Asia Pacifico (Giacarta) – 589379963580
- Asia Pacifico (Mumbai): 718504428378
- Asia Pacifico (Osaka-Locale): 383597477331
- Asia Pacifico (Seoul): 600734575887
- Asia Pacifico (Singapore): 114774131450
- Asia Pacifico (Sydney): 783225319266
- Asia Pacifico (Tokyo): 582318560864
- Canada (Centrale): 985666609251
- Europa (Francoforte): 054676820928
- Europa (Irlanda): 156460612806
- Europa (Londra): 652711504416
- Europa (Milano): 635631232127
- Europa (Parigi): 009996457667
- Europa (Stoccolma): 897822967062
- Medio Oriente (Bahrein): 076674570225
- Sud America (San Paolo): 507241528517

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN del bucket S3 specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regioni

Questa politica concede le autorizzazioni all'account Elastic Load Balancing specificato. Utilizza questo criterio per i sistemi di bilanciamento del carico nelle zone di disponibilità o nelle zone locali nelle AWS GovCloud (US) regioni elencate di seguito.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
  ]
}
```

Da `Principal` sostituire *`elb-account-id`* con l'ID dell'account Elastic Load Balancing per la regione del load balancer:

- AWS GovCloud (Stati Uniti occidentali) — 048591011584

- AWS GovCloud (Stati Uniti orientali) — 190560391635

Per`Resource`, immettere l'ARN della posizione per i log di accesso, utilizzando il formato mostrato nella politica di esempio. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Garantisce che i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN del bucket S3 che specifichi dipende dal fatto che intendi includere un prefisso quando abiliti i log di accesso.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Zone Outpost

La policy seguente concede le autorizzazioni al servizio di consegna dei log specificato. Utilizzare questa policy per i sistemi di bilanciamento del carico nelle zone Outpost.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
```

```
    }
}
```

Per`Resource`, inserire l'ARN della posizione per i log di accesso. Includi sempre l'ID dell'account con il sistema di bilanciamento del carico nel percorso delle risorse dell'ARN del bucket S3. Ciò garantisce che solo i sistemi di bilanciamento del carico dell'account specificato possano scrivere i log di accesso al bucket S3.

L'ARN specificato dipende dal fatto che si intenda includere un prefisso quando si abilitano i log di accesso nel passaggio 3.

Esempio ARN del bucket S3 con un prefisso

Il nome del bucket S3 è e il prefisso è. amzn-s3-demo-logging-bucket logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Esempio di ARN per bucket S3 senza prefisso

Il nome del bucket S3 è. amzn-s3-demo-logging-bucket Non è presente alcuna porzione di prefisso nell'ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Usare when è NotPrincipalEffectDeny

Se la policy sui bucket di Amazon S3 utilizza `Effect` il valore `Deny` e include `NotPrincipal` come mostrato nell'esempio seguente, assicurati che `logdelivery.elasticloadbalancing.amazonaws.com` sia incluso nell'elenco. `Service`

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

Per allegare una policy bucket per i log di connessione al tuo bucket utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il nome del bucket per aprirne la pagina dei dettagli.
3. Scegli Autorizzazioni quindi seleziona Policy del bucket, Modifica.
4. Crea o aggiorna la policy del bucket per concedere le autorizzazioni richieste.
5. Scegli Save changes (Salva modifiche).

Fase 3: Configurazione dei log di connessione

Utilizza la seguente procedura per configurare i log di connessione per acquisire e inviare i file di registro al tuo bucket S3.

Requisiti

Il bucket deve soddisfare i requisiti descritti nella fase 1 e devi collegare una policy di bucket come descritto nella fase 2. Se si specifica un prefisso, questo non deve includere la stringa "». AWSLogs

Per abilitare i registri di connessione per il sistema di bilanciamento del carico utilizzando la console

1. Apri la EC2 console Amazon 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. Per il monitoraggio, attiva i registri di connessione.
6. In URI S3, inserisci l'URI S3 per i tuoi file di log. L'URI specificato dipende dall'utilizzo di un prefisso.
   - URI con prefisso: `s3://bucket-name/prefix`
   - URI senza prefisso: `s3://bucket-name`
7. Scegli Save changes (Salva modifiche).

Per abilitare i registri di connessione utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Per gestire il bucket S3 per i log di connessione

Assicurati di disabilitare i log di connessione prima di eliminare il bucket che hai configurato per i log di connessione. Altrimenti, se esiste un nuovo bucket con lo stesso nome e la policy del bucket richiesta ma creato in un bucket di Account AWS cui non sei proprietario, Elastic Load Balancing potrebbe scrivere i log di connessione del tuo load balancer su questo nuovo bucket.

Fase 4: verifica delle autorizzazioni del bucket

Dopo aver abilitato i log di connessione per il sistema di bilanciamento del carico, Elastic Load Balancing convalida il bucket S3 e crea un file di test per garantire che la policy del bucket specifichi le autorizzazioni richieste. Puoi utilizzare la console Amazon S3 per verificare che il file di test sia stato creato. Il file di test non è un vero file di registro delle connessioni; non contiene record di esempio.

Per verificare che Elastic Load Balancing abbia creato un file di test nel bucket S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il nome del bucket che hai specificato per i log di connessione.
3. Accedi al file di test, `ELBConnectionLogTestFile`. La posizione dipende dall'utilizzo di un prefisso.

   - Posizione con prefisso:*amzn-s3-demo-logging-bucket*///*prefix*AWSLogs*123456789012*ELBConnectionLogTestFile
   - Posizione senza prefisso:*amzn-s3-demo-logging-bucket*/// AWSLogs*123456789012*ELBConnectionLogTestFile

Risoluzione dei problemi

L'errore di accesso negato può essere provocato da una delle cause elencate di seguito:

- La policy del bucket non concede a Elastic Load Balancing l'autorizzazione a scrivere i log di connessione nel bucket. Verifica di utilizzare la policy di bucket corretta per la regione. Verifica che l'ARN della risorsa utilizzi lo stesso nome di bucket specificato quando hai abilitato i log di connessione. Verifica che l'ARN della risorsa non includa un prefisso se non hai specificato un prefisso quando hai abilitato i log di connessione.
- Il bucket utilizza un'opzione di crittografia lato server non supportata. Il bucket deve utilizzare chiavi gestite da Amazon S3 (SSE-S3).

Disattiva i log di connessione per il tuo Application Load Balancer

Puoi disabilitare i registri di connessione per il tuo sistema di bilanciamento del carico in qualsiasi momento. Dopo aver disabilitato i log di connessione, i log di connessione rimangono nel bucket S3 finché non li elimini. Per ulteriori informazioni, consulta Creazione, configurazione e utilizzo dei bucket nella Guida per l'utente di Amazon S3.

Per disabilitare i log di connessione utilizzando la console

1. Apri la EC2 console Amazon 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. Per il monitoraggio, disattiva i registri di connessione.
6. Scegli Save changes (Salva modifiche).

Per disabilitare i registri di connessione utilizzando il AWS CLI

Utilizza il comando modify-load-balancer-attributes.

Richiesta del tracciamento sull'Application Load Balancer

Quando il sistema di bilanciamento del carico riceve una richiesta da un client, aggiunge o aggiorna l'intestazione X-Amzn-Trace-Id prima di inviare la richiesta alla destinazione. Anche qualsiasi servizio o applicazione tra il sistema di bilanciamento del carico e la destinazione può aggiungere o aggiornare questa intestazione.

Puoi utilizzare il tracciamento delle richieste per tenere traccia delle richieste HTTP effettuate dai client verso le destinazioni o altri servizi. Se abiliti i log di accesso, i contenuti dell'intestazione X-Amzn-Trace-Id vengono registrati. Per ulteriori informazioni, consulta Log di accesso dell'Application Load Balancer.

Sintassi

L'intestazione X-Amzn-Trace-Id contiene campi con il seguente formato:

```
Field=version-time-id
```

Campo

Il nome del campo. I valori supportati sono `Root` e `Self`.

Un'applicazione può aggiungere campi arbitrari per i propri scopi. Il sistema di bilanciamento del carico conserva tali campi ma non li utilizza.

version

Il numero di versione. Questo valore è 1.

time

L'ora nel formato epoca (Unix epoch) in secondi. Questo valore è composto da 8 cifre esadecimali.

id

L'identificatore di traccia. Questo valore è composto da 24 cifre esadecimali.

Esempi

Se in una richiesta in entrata non è presente l'intestazione X-Amzn-Trace-Id, il sistema di bilanciamento del carico genera un'intestazione con un campo `Root` e inoltra la richiesta. Per esempio:

```
X-Amzn-Trace-Id: Root=1-67891233-abcdef012345678912345678
```

Se l'intestazione X-Amzn-Trace-Id è presente e dispone di un campo `Root`, il sistema di bilanciamento del carico inserisce un campo `Self` e inoltra la richiesta. Per esempio:

```
X-Amzn-Trace-Id: Self=1-67891233-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678
```

Se un'applicazione aggiunge un'intestazione con un campo `Root` e un campo personalizzato, il sistema di bilanciamento del carico mantiene entrambi i campi, inserisce un campo `Self` e inoltra la richiesta:

```
X-Amzn-Trace-Id: Self=1-67891233-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678;CalledFrom=app
```

Se l'intestazione X-Amzn-Trace-Id è presente e dispone di un campo `Self`, il sistema di bilanciamento del carico aggiorna il valore del campo `Self`.

Limitazioni

- Il sistema di bilanciamento del carico aggiorna l'intestazione quando riceve una richiesta in entrata, non quando riceve una risposta.
- Se le intestazioni HTTP sono superiori a 7 KB, il sistema di bilanciamento del carico riscrive l'intestazione X-Amzn-Trace-Id con un campo `Root`.
- Con WebSockets, è possibile tracciare solo fino all'esito positivo della richiesta di aggiornamento.

Risoluzione dei problemi degli Application Load Balancer

Le informazioni seguenti possono essere utili per risolvere i problemi con l'Application Load Balancer.

Problemi

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 di salute per i gruppi target di Application Load Balancer.

Verificare che l'istanza non superi i controlli dell'integrità e quindi verificare le seguenti problematiche:

Un gruppo di sicurezza non consente il traffico

Il gruppo di sicurezza associato a un'istanza deve consentire il traffico dal sistema di bilanciamento del carico utilizzando la porta di controllo dello stato e il protocollo di controllo dello

stato. È possibile aggiungere una regola al gruppo di sicurezza dell'istanza per consentire tutto il traffico dal sistema di bilanciamento del carico per il gruppo di sicurezza. Inoltre, il gruppo di sicurezza del sistema di bilanciamento del carico deve consentire il traffico verso le istanze.

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

L'ACL di rete associato con le sottoreti per le istanze deve consentire il traffico in entrata sulla porta di controllo dello stato e di traffico in uscita su porte temporanee (1024-65535). L'ACL di rete associato con le sottoreti per i nodi del sistema di bilanciamento del carico deve consentire il traffico in entrata su porte temporanee e il traffico in uscita sul controllo dello stato e su porte temporanee.

Il percorso ping non esiste

Creare una pagina di destinazione per il controllo dello stato e specificare il relativo percorso come percorso ping.

La connessione scade

In primo luogo, verificare che sia possibile connettersi alla destinazione direttamente dalla rete utilizzando l'indirizzo IP privato della destinazione e il protocollo del controllo dello stato. Se non è possibile connettersi, verificare che l'istanza non sia utilizzata eccessivamente, e aggiungere ulteriori destinazioni al gruppo di destinazioni se è troppo occupato per rispondere. Se non è possibile connettersi, è probabile che la pagina di destinazione non stia rispondendo prima del timeout del controllo dello stato. Scegliere una pagina di destinazione del controllo dello stato più semplice o regolare le impostazioni del controllo dello stato.

La destinazione non ha restituito un codice di risposta positiva

Per impostazione predefinita, il codice di successo è 200, ma è possibile specificare ulteriori codici al momento della configurazione dei controlli dello stato. Verificare i codici di successo relativi al sistema di bilanciamento del carico e accertarsi che l'applicazione sia configurata per restituire tali codici in caso di esito positivo.

Il codice di risposta della destinazione era difettoso o si è verificato un errore di connessione alla destinazione

Verifica che l'applicazione risponda alle richieste di controllo dell'integrità del sistema di bilanciamento del carico. Alcune applicazioni richiedono una configurazione aggiuntiva per rispondere ai controlli dell'integrità, come la configurazione dell'host virtuale per rispondere all'intestazione HTTP dell'host inviata dal sistema di bilanciamento del carico. Il valore dell'intestazione dell'host contiene l'indirizzo IP privato della destinazione, seguito dalla porta

per il controllo dello stato quando non si utilizza una porta predefinita. Se la destinazione utilizza una porta di controllo dello stato predefinita, il valore dell'intestazione dell'host contiene solo l'indirizzo IP privato della destinazione. Ad esempio, se l'indirizzo IP privato della destinazione è `10.0.0.10` e la porta per il controllo dello stato è`8080`, l'intestazione HTTP Host inviata dal load balancer durante i controlli di integrità è. `Host: 10.0.0.10:8080` Se l'indirizzo IP privato della destinazione è `10.0.0.10` e la porta per il controllo dello stato è`80`, l'intestazione HTTP Host inviata dal load balancer durante i controlli di integrità è. `Host: 10.0.0.10` Per eseguire correttamente un controllo dell'integrità dell'applicazione potrebbero essere necessari una configurazione dell'host virtuale per rispondere a tale host o una configurazione predefinita. Le richieste di controllo dell'integrità hanno i seguenti attributi: l'`User-Agent` è impostato su `ELB-HealthChecker/2.0`, il terminatore di riga per i campi messagge-header è la sequenza CRLF e l'intestazione termina alla prima riga vuota seguita da una CRLF.

I client non sono in grado di connettersi a un sistema di bilanciamento del carico connesso a Internet

Se il sistema di bilanciamento del carico non risponde alle richieste, verifica la presenza dei problemi seguenti:

Il tuo load balancer connesso a Internet è associato a una sottorete privata

Assicurati di avere specificato sottoreti pubbliche per il sistema di bilanciamento del carico. Una sottorete pubblica include una route all'Internet gateway per il tuo cloud privato virtuale (VPC, Virtual Private Cloud).

Un gruppo di sicurezza o una lista di controllo degli accessi di rete non consente il traffico

Il gruppo di sicurezza per il load balancer e qualsiasi rete ACLs per le sottoreti del load balancer devono consentire il traffico in entrata dai client e il traffico in uscita verso i client sulle porte del listener.

Le richieste inviate a un dominio personalizzato non vengono ricevute dal sistema di bilanciamento del carico

Se il sistema di bilanciamento del carico non riceve le richieste inviate a un dominio personalizzato, verifica la presenza dei problemi seguenti:

Il nome di dominio personalizzato non si risolve all'indirizzo IP del sistema di bilanciamento del carico

- Conferma a quale indirizzo IP si risolve il nome di dominio personalizzato utilizzando un'interfaccia della linea di comando.
  - Linux, macOS o Unix: puoi utilizzare il comando `dig` all'interno del terminale. Es. `dig example.com`
  - Windows: è possibile utilizzare il comando `nslookup` all'interno del prompt dei comandi. Es. `nslookup example.com`
- Conferma a quale indirizzo IP si risolve il nome DNS del sistema di bilanciamento del carico utilizzando un'interfaccia della linea di comando.
- Confronta i risultati dei due output. Gli indirizzi IP devono corrispondere.

Se si utilizza Route 53 per ospitare il dominio personalizzato, consulta Il mio dominio non è disponibile su Internet nella Guida per gli sviluppatori di Amazon Route 53.

Le richieste HTTPS inviate al sistema di bilanciamento del carico restituiscono "NET::ERR_CERT_COMMON_NAME_INVALID"

Se le richieste HTTPS ricevono l'errore `NET::ERR_CERT_COMMON_NAME_INVALID` dal sistema di bilanciamento del carico, verifica le seguenti possibili cause:

- Il nome di dominio utilizzato nella richiesta HTTPS non corrisponde al nome alternativo specificato nel certificato ACM associato agli ascoltatori.
- Viene utilizzato il nome DNS predefinito del sistema di bilanciamento del carico. Il nome DNS predefinito non può essere utilizzato per effettuare richieste HTTPS poiché non è possibile richiedere un certificato pubblico per il dominio `*.amazonaws.com`.

Il sistema di bilanciamento del carico mostra tempi di elaborazione lunghi

Il sistema di bilanciamento del carico calcola i tempi di elaborazione in modo diverso sulla base della configurazione.

- Se AWS WAF è associato all'Application Load Balancer e un client invia una richiesta HTTP POST, il tempo necessario per inviare i dati per le richieste POST si riflette nel

`request_processing_time` campo dei log di accesso del load balancer. Si tratta di un comportamento previsto per le richieste POST.

- Se non AWS WAF è associato all'Application Load Balancer e un client invia una richiesta HTTP POST, il tempo necessario per inviare i dati per le richieste POST si riflette nel `target_processing_time` campo dei log di accesso del load balancer. Si tratta di un comportamento previsto per le richieste POST.

Il bilanciamento del carico invia un codice di risposta di 000

Con le connessioni HTTP/2, se il numero di richieste servite tramite una connessione supera le 10.000, il load balancer invia un frame GOAWAY e chiude la connessione con un TCP FIN.

Il sistema di bilanciamento del carico genera un errore HTTP

I seguenti errori HTTP vengono generati dal sistema di bilanciamento del carico. Il sistema di bilanciamento del carico invia il codice HTTP al client, salva la richiesta nel log degli accessi e incrementa il parametro `HTTPCode_ELB_4XX_Count` o `HTTPCode_ELB_5XX_Count`.

Errori

- HTTP 400: Bad request
- HTTP 401: Unauthorized
- HTTP 403: Forbidden
- HTTP 405: Method not allowed
- HTTP 408: Request timeout
- HTTP 413: Payload too large
- HTTP 414: URI too long
- HTTP 460
- HTTP 463
- HTTP 464
- HTTP 500: Internal server error
- HTTP 501: Not implemented
- HTTP 502: Bad Gateway

- HTTP 503: Service Unavailable
- HTTP 504: Gateway Timeout
- HTTP 505: Version not supported
- HTTP 507: spazio di archiviazione insufficiente
- HTTP 561: Unauthorized

HTTP 400: Bad request

Possibili cause:

- Il client ha inviato una richiesta con un formato errato che non soddisfa le specifiche HTTP.
- L'intestazione della richiesta ha superato il limite di 16 K per riga della richiesta, 16K per singola intestazione o 64 K per l'intera intestazione della richiesta.
- Il client ha chiuso la connessione prima di inviare l'intero corpo della richiesta.

HTTP 401: Unauthorized

È stata configurata una regola del listener per autenticare gli utenti, ma una delle condizioni seguenti è vera:

- È stato configurato `OnUnauthenticatedRequest` per rifiutare gli utenti non autenticati o il provider di identità ha rifiutato l'accesso.
- Le dimensioni delle dichiarazioni restituite dal provider di identità hanno superato il limite massimo supportato dal sistema di bilanciamento del carico.
- Un client ha inoltrato una richiesta HTTP/1.0 senza un'intestazione host e il sistema di bilanciamento del carico non è stato in grado di generare un URL di reindirizzamento.
- L'ambito richiesto non restituisce un token ID.
- Il processo di accesso non è stato completato prima della scadenza del timeout di accesso del client. Per ulteriori informazioni, consulta Client login timeout.

HTTP 403: Forbidden

Hai configurato una AWS WAF lista di controllo degli accessi Web (Web ACL) per monitorare le richieste all'Application Load Balancer e questa ha bloccato una richiesta.

HTTP 405: Method not allowed

Il client ha utilizzato il metodo TRACE che non è supportato dagli Application Load Balancer.

HTTP 408: Request timeout

Il client non ha inviato i dati prima della scadenza del periodo di timeout di inattività. L'invio di un keepalive TCP non impedisce il timeout. Invia almeno 1 byte di dati prima che scada ciascun periodo di timeout di inattività. Aumenta la durata del periodo di timeout di inattività in base alle esigenze.

HTTP 413: Payload too large

Possibili cause:

- Il target è una funzione Lambda e il corpo della richiesta supera il limite di 1 MB.
- L'intestazione della richiesta ha superato il limite di 16 K per riga della richiesta, 16K per singola intestazione o 64 K per l'intera intestazione della richiesta.

HTTP 414: URI too long

Le dimensioni dell'URL della richiesta o dei parametri della stringa di query superano i limiti previsti.

HTTP 460

Il sistema di bilanciamento del carico ha ricevuto una richiesta da un client, ma il client ha chiuso la connessione con il sistema di bilanciamento del carico prima dello scadere del timeout di inattività.

Accertarsi che il periodo di timeout del client sia superiore al periodo di timeout di inattività del sistema di bilanciamento del carico. Accertarsi che la destinazione fornisca una risposta al client prima che il relativo periodo di timeout scada oppure aumentare questo periodo di tempo affinché corrisponda al timeout di inattività del sistema di bilanciamento del carico, se il client lo supporta.

HTTP 463

Il sistema di bilanciamento del carico ha ricevuto un'intestazione X-Forwarded-For della richiesta con troppi indirizzi IP. Il limite massimo di indirizzi IP è 30.

HTTP 464

Il sistema di bilanciamento del carico ha ricevuto un protocollo di richiesta in entrata incompatibile con la versione di configurazione del protocollo del gruppo di destinazioni.

Possibili cause:

- Il protocollo della richiesta è HTTP/1.1, mentre la versione del protocollo del gruppo di destinazioni è gRPC o HTTP/2.
- Il protocollo della richiesta è gRPC, mentre la versione del protocollo del gruppo di destinazioni è HTTP/1.1.
- Il protocollo della richiesta è HTTP/2 è la richiesta non è POST, mentre la versione del protocollo del gruppo di destinazioni è gRPC.

HTTP 500: Internal server error

Possibili cause:

- È stata configurata una AWS WAF lista di controllo degli accessi Web (Web ACL) e si è verificato un errore durante l'esecuzione delle regole Web ACL.
- Il sistema di bilanciamento del carico non è in grado di comunicare con l'endpoint del token del provider di identità o con l'endpoint delle info sull'utente del provider di identità.
  - Verifica che il DNS del provider di identità sia risolvibile pubblicamente.
  - Verifica che i gruppi di sicurezza per il tuo sistema di bilanciamento del carico e la rete ACLs per il tuo VPC consentano l'accesso in uscita a questi endpoint.
  - Verificare che il VPC abbia accesso a Internet. Se si dispone di un sistema di bilanciamento del carico interno, utilizzare un gateway NAT per abilitare l'accesso interno.
- L'attestazione dell'utente ricevuta dal provider di identità è di dimensione maggiore di 11 KB.
- L'endpoint del token IdP o l'endpoint IdP user info impiega più di 5 secondi per rispondere.

HTTP 501: Not implemented

Il sistema di bilanciamento del carico ha ricevuto un'intestazione Transfer-Encoding con un valore non supportato. I valori supportati per Transfer-Encoding sono `chunked` e `identity`. In alternativa, è possibile utilizzare l'intestazione Content-Encoding.

HTTP 502: Bad Gateway

Possibili cause:

- Il sistema di bilanciamento del carico ha ricevuto un pacchetto RST TCP dalla destinazione durante il tentativo di stabilire una connessione.
- Il sistema di bilanciamento del carico ha ricevuto una risposta imprevista dalla destinazione, ad esempio "ICMP Destination unreachable (Host unreachable)" ("Destinazione ICMP non raggiungibile (host non raggiungibile)") durante un tentativo di stabilire una connessione. Accertarsi che sia consentito il traffico dalle sottoreti del sistema di bilanciamento del carico verso le destinazioni sulla porta di destinazione.
- La destinazione ha chiuso la connessione con un pacchetto RST TCP o FIN TCP mentre il sistema di bilanciamento del carico aveva una richiesta rilevante per la destinazione. Controllare se la durata keep-alive della destinazione è inferiore al valore del timeout di inattività del sistema di bilanciamento del carico.
- La risposta della destinazione non è valida o contiene intestazioni HTTP che non sono valide.
- L'intestazione della risposta della destinazione è di dimensione superiore a 32 K per l'intera intestazione.
- L'intervallo di tempo per l'annullamento della registrazione è scaduto per una richiesta gestita da una destinazione la cui registrazione era stata annullata. Aumentare l'intervallo di tempo in modo che sia possibile completare le operazioni che richiedono più tempo.
- Il target è una funzione Lambda e il corpo della richiesta supera il limite di 1 MB.
- La destinazione è una funzione Lambda che non ha risposto prima che sia stato raggiunto il suo timeout configurato.
- La destinazione è una funzione Lambda che ha restituito un errore, oppure la funzione è stata limitata dal servizio Lambda.
- Il load balancer ha riscontrato un errore di handshake SSL durante la connessione a una destinazione.

Per ulteriori informazioni, consulta Come risolvere gli errori HTTP 502 di Application Load Balancer nel Support Knowledge Center. AWS

HTTP 503: Service Unavailable

I gruppi target per il load balancer non hanno obiettivi registrati oppure tutti i target registrati si trovano in uno stato. `unused`

HTTP 504: Gateway Timeout

Possibili cause:

- Il sistema di bilanciamento del carico non è stato in grado di stabilire una connessione con la destinazione prima dello scadere del timeout della connessione (10 secondi).
- Il sistema di bilanciamento del carico ha stabilito una connessione con la destinazione, ma la destinazione non ha risposto prima dello scadere del timeout di inattività.
- L'ACL o SecurityGroup le politiche della rete non consentivano il traffico dai target ai nodi di bilanciamento del carico sulle porte temporanee (1024-65535).
- La destinazione ha restituito un'intestazione content-length più grande del corpo dell'entità. Il sistema di bilanciamento del carico è scaduto in attesa di byte mancanti.
- La destinazione è una funzione Lambda e il servizio Lambda non ha risposto prima della scadenza del timeout della connessione.
- Il sistema di bilanciamento del carico ha rilevato un timeout dell'handshake SSL (10 secondi) durante la connessione a una destinazione.

HTTP 505: Version not supported

Il sistema di bilanciamento del carico ha ricevuto una versione della richiesta HTTP inaspettata. Ad esempio, il sistema di bilanciamento del carico ha stabilito una connessione HTTP/1, ma ha ricevuto una richiesta HTTP/2.

HTTP 507: spazio di archiviazione insufficiente

L'URL di reindirizzamento è troppo lungo.

HTTP 561: Unauthorized

È stata configurata una regola del listener per autenticare gli utenti, ma il provider di identità ha restituito un codice di errore durante l'autenticazione dell'utente. Controlla i log di accesso per trovare il relativo codice di motivo errore.

Una destinazione genera un errore HTTP

Il sistema di bilanciamento del carico inoltra risposte HTTP valide dalle destinazioni al client, inclusi gli errori HTTP. Gli errori HTTP generati da una destinazione vengono registrati nei parametri `HTTPCode_Target_4XX_Count` e `HTTPCode_Target_5XX_Count`.

Un AWS Certificate Manager certificato non è disponibile per l'uso

Quando si decide di utilizzare un listener HTTPS con Application Load Balancer AWS Certificate Manager , è necessario convalidare la proprietà del dominio prima di emettere un certificato. Se durante la configurazione viene saltato questo passaggio, il certificato rimane nello stato `Pending Validation` e non sarà disponibile per l'uso fino a quando non sarà convalidato.

- Se si utilizza la convalida e-mail, consulta Convalida e-mail nella Guida per l'utente di AWS Certificate Manager .
- Se si utilizza la convalida DNS, consulta Convalida DNS nella Guida per l'utente di AWS Certificate Manager .

Le intestazioni a più righe non sono supportate

Gli Application Load Balancer non supportano le intestazioni a più righe, incluse le intestazioni con tipo di supporto `message/http`. Quando viene fornita un'intestazione a più righe, l'Application Load Balancer aggiunge un carattere due punti, "`:`", prima di passarla alla destinazione.

Risolvi i problemi relativi agli obiettivi non integri utilizzando la mappa delle risorse

Se i tuoi obiettivi Application 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 Visualizza la mappa delle risorse di Application 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 i target non integri in ogni gruppo target associato all'Application Load Balancer.

> **Note**
>
> È necessario abilitare Mostra i dettagli delle risorse 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 abilitata, 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 di integrità, controlla la configurazione del gruppo target. Seleziona il nome di un gruppo target per aprirne la pagina di dettaglio 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 oggetto non supera il controllo di integrità, verifica che l'oggetto disponga di risorse sufficienti e conferma che le applicazioni in esecuzione sull'oggetto siano disponibili. Seleziona l'ID di un target per aprirne la pagina di dettaglio in una nuova scheda.

Selezionando Esporta è possibile esportare la visualizzazione corrente della mappa delle risorse di Application 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:

- Insalubre: mancata corrispondenza della risposta HTTP
  - Verifica che l'applicazione in esecuzione sulla destinazione stia inviando la risposta HTTP corretta alle richieste di controllo dello stato di Application Load Balancer.
  - In alternativa, puoi aggiornare la richiesta di controllo dello stato di Application Load Balancer in modo che corrisponda alla risposta dell'applicazione in esecuzione sulla destinazione.
- Non integro: la richiesta è scaduta
  - Verifica che i gruppi di sicurezza e gli elenchi di controllo degli accessi alla rete (ACL) associati ai tuoi obiettivi e Application Load Balancer non blocchino la connettività.
  - Verifica che la destinazione disponga di risorse sufficienti per accettare connessioni dall'Application Load Balancer.
  - Verifica lo stato di tutte le applicazioni in esecuzione sulla destinazione.

- Le risposte al controllo dello stato di Application Load Balancer possono essere visualizzate nei log delle applicazioni di ogni destinazione. Per ulteriori informazioni, consulta Codici motivo Health check.

- Malsano: FailedHealthChecks
  - Verifica lo stato di tutte le applicazioni in esecuzione sulla destinazione.
  - Verifica che il bersaglio stia ascoltando il traffico sulla porta di controllo dello stato.

    > Quando si utilizza un listener HTTPS
    >
    > 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 HTTPS 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 HTTPS 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 Application Load Balancer per stabilire handshake TLS.

Quote per gli Application Load Balancer

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, 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 gli Application Load Balancer, apri la Console Service Quotas. Nel riquadro di navigazione, scegliere Servizi AWS e selezionare Elastic Load Balancing. Puoi anche usare il comando describe-account-limits(AWS CLI) per Elastic Load Balancing.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, invia una richiesta di aumento della quota di servizio.

Quote

- Sistemi di load balancer
- Gruppi target
- Regolamento
- Negozi fiduciari
- Certificati
- Intestazioni HTTP
- Unità di capacità Load Balancer

Sistemi di load balancer

Il tuo AWS account ha le seguenti quote relative agli Application Load Balancers.

Nome	Predefinita	Adattabile
Application Load Balancer per regione	50	Sì
Certificati per Application Load Balancer (esclusi i certificati predefiniti)	25	Sì
Listener per Application Load Balancer	50	Sì

Nome	Predefinita	Adattabile
Gruppi di destinazione per operazione per Application Load Balancer	5	No
Gruppi di destinazione per Application Load Balancer	100	No
Destinazioni per Application Load Balancer	1.000	Sì

Gruppi target

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

Nome	Predefinita	Adattabile
Gruppi di destinazione per regione	3.000*	Sì
Destinazioni per gruppo di destinazioni per regione (istanze o indirizzi IP)	1.000	Sì
Destinazioni per gruppo di destinazioni per regione (funzioni Lambda)	1	No
Sistemi di bilanciamento del carico per gruppo di destinazione	1	No

* Questa quota è condivisa da Application Load Balancer e Network Load Balancer.

Regolamento

Le seguenti quote sono per le regole.

Nome	Predefinita	Adattabile
Regole per Application Load Balancer (escluse le regole predefinite)	100	Sì

Nome	Predefinita	Adattabile
Valori delle condizioni per regola	5	No
Caratteri jolly delle condizioni per regola	5	No
Valutazione corrispondenze per regola	5	No

Negozi fiduciari

Le seguenti quote si riferiscono ai negozi fiduciari.

Nome	Predefinita	Adattabile
Trust Stores per account	20	Sì
Numero di ascoltatori che utilizzano MTL in modalità di verifica, per sistema di bilanciamento del carico.	2	No

Certificati

Le seguenti quote si applicano ai certificati, compresi i nomi dei certificati CA pubblicitari e gli elenchi di revoca dei certificati.

Nome	Predefinita	Adattabile
Dimensione del certificato CA	16 KB	No
Certificati CA per trust store	25	Sì
Dimensione del soggetto dei certificati CA per archivio attendibile	10.000	Sì
Profondità massima della catena di certificati	4	No
Voci di revoca per trust store	500.000	Sì

Nome	Predefinita	Adattabile
Dimensione del file dell'elenco di revoca	50 MB	No
Elenchi di revoca per archivio di fiducia	30	Sì
Dimensioni dei messaggi TLS	64 K	No

Intestazioni HTTP

Di seguito sono elencati i limiti di dimensione per le intestazioni HTTP.

Nome	Predefinita	Adattabile
Riga della richiesta	16 K	No
Intestazione singola	16 K	No
Intestazione della risposta intera	32 K	No
Intestazione della richiesta intera	64 K	No

Unità di capacità Load Balancer

Le seguenti quote si riferiscono alle Load Balancer Capacity Units (LCU).

Nome	Predefinita	Adattabile
Unità di capacità riservate per Application Load Balancer (LCUs) per Application Load Balancer	15.000	Sì
Unità di capacità di Application Load Balancer (LCU) riservate per regione	0	Sì

Cronologia dei documenti per gli Application Load Balancer

La tabella seguente descrive le versioni degli Application Load Balancer.

Modifica	Descrizione	Data
Modifica dell'intestazione HTTP	Questa versione aggiunge il supporto per la modifica dell'intestazione HTTP per tutti i codici di risposta. In precedenza, questa funzionalità era limitata ai codici di risposta 2xx e 3xx.	28 febbraio 2025
Prenotazione dell'unità di capacità	Questa versione aggiunge il supporto per impostare una capacità minima per il sistema di bilanciamento del carico.	20 novembre 2024
Mappa delle risorse	Questa versione aggiunge il supporto per visualizzare le risorse e le relazioni del sistema di bilanciamento del carico in un formato visivo.	8 marzo 2024
WAF con un clic	Questa versione aggiunge il supporto per la configurazione del comportamento del sistema di bilanciamento del carico se si integra con un clic. AWS WAF	6 febbraio 2024
TLS reciproco	Questa versione aggiunge il supporto per l'autenticazione TLS reciproca.	26 novembre 2023

Pesi target automatici	Questa versione aggiunge il supporto per l'algoritmo automatico dei pesi target.	26 novembre 2023
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
Registra gli obiettivi utilizzando IPv6	Questa versione aggiunge il supporto per registrare le istanze come destinazioni quando indirizzate da IPv6.	2 ottobre 2023
Politiche di sicurezza che supportano TLS 1.3	Questa versione aggiunge il supporto per le politiche di sicurezza predefinite di TLS 1.3.	22 marzo 2023
Spostamento zonale	Questa versione aggiunge il supporto per indirizzare il traffico lontano da una singola zona di disponibilità ridotta attraverso l'integrazione con. Amazon Application Recovery Controller (ARC)	28 novembre 2022
Disattiva il bilanciamento del carico tra zone	Questa versione aggiunge il supporto per disattivare il bilanciamento del carico tra zone.	28 novembre 2022

Integrità del gruppo di destinazioni	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.	28 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
IPv6 gruppi target	Questa versione aggiunge il supporto per configurare i gruppi IPv6 target per Applicati on Load Balancer.	23 novembre 2021
IPv6 bilanciatori di carico interni	Questa versione aggiunge il supporto per configurare i gruppi IPv6 target per Applicati on Load Balancer.	23 novembre 2021
AWS PrivateLink e indirizzi IP statici	Questa versione aggiunge il supporto per l'uso AWS PrivateLink e l'esposizione di indirizzi IP statici inoltrand o il traffico direttamente dai Network Load Balancer agli Application Load Balancer.	27 settembre 2021

Conservazione della porta del client	Questa versione aggiunge un attributo per conservare la porta di origine che il client ha utilizzato per connettersi al sistema di bilanciamento del carico.	29 luglio 2021
Intestazioni TLS	Questa versione aggiunge un attributo per indicare che le intestazioni TLS, che contengono informazioni sulla versione TLS negoziata e sulla suite di crittografia, vengono aggiunte alla richiesta del client prima di inviarla alla destinazione.	21 luglio 2021
Certificati ACM aggiuntivi	Questa versione supporta certificati RSA con lunghezze di chiave 2048, 3072 e 4096 bit e tutti i certificati ECDSA.	14 luglio 2021
Persistenza basata sull'applicazione	Questa versione aggiunge un cookie basato sull'applicazione per supportare le sessioni permanenti per il sistema di bilanciamento del carico.	8 febbraio 2021
Policy di sicurezza FS per il supporto di TLS versione 1.2	Questa versione aggiunge policy di sicurezza per Forward Secrecy (FS) per il supporto di TLS versione 1.2.	24 novembre 2020

Supporto WAF fail open	Questa versione aggiunge il supporto per la configura zione del comportamento del sistema di bilanciamento del carico, se si integra con. AWS WAF	13 Novembre 2020
Supporto gRPC e HTTP/2	Questa versione aggiunge il supporto per carichi di lavoro gRPC e HTTP/2. end-to-end	29 ottobre 2020
Supporto Outpost	Puoi effettuare il provision ing di un Application Load Balancer sul tuo. AWS Outposts	8 settembre 2020
Modalità di mitigazione della desincronizzazione	Questa release aggiunge il supporto della modalità di mitigazione della desincron izzazione.	17 agosto 2020
Richieste meno rilevanti	Questa versione aggiunge il supporto dell'algoritmo per le richieste meno rilevanti.	25 novembre 2019
Gruppi di destinazioni ponderate	Questa versione aggiunge il supporto per le operazion i di inoltro con più gruppi di destinazioni. Le richieste vengono distribuite a questi gruppi di destinazioni in base al peso specificato per ciascun gruppo di destinazioni.	19 novembre 2019
New Attribute (Nuovo attributo)	Questa versione aggiunge il supporto per l'attributo routing.http.drop_invalid_h eader_fields.enabled.	15 novembre 2019

Politiche di sicurezza per FS	Questa versione aggiunge il supporto per tre ulteriori politiche di sicurezza predefinite relative alla segretezza avanzata.	8 ottobre 2019
Instradamento avanzato delle richieste	Questa versione aggiunge il supporto per tipi di condizione aggiuntivi per le regole dell'ascoltatore.	27 marzo 2019
Funzioni Lambda come destinazioni	Questa versione aggiunge il supporto della funzionalità di registrazione delle funzioni Lambda come target	29 novembre 2018
Operazioni di reindirizzamento	Questa versione aggiunge il supporto della funzionalità del sistema di bilanciamento del carico di reindirizzare le richieste a un URL diverso.	25 luglio 2018
Operazioni con risposta fissa	Questa versione aggiunge il supporto della funzionalità del sistema di bilanciamento del carico di restituire una risposta HTTP personalizzata.	25 luglio 2018
Policy di sicurezza per FS e TLS 1.2	Questa versione aggiunge il supporto di due policy di sicurezza predefinite aggiuntive.	6 giugno 2018

Autenticazione dell'utente	Questa versione aggiunge il supporto della funzionalità del sistema di bilanciamento del carico di autenticare gli utenti delle proprie applicazioni tramite le loro identità aziendali o social prima di instradare le richieste.	30 maggio 2018
Autorizzazioni a livello di risorsa	Questa versione aggiunge il supporto delle autorizzazioni a livello di risorsa e delle chiavi per le condizioni di tagging.	10 maggio 2018
Modalità di avvio lento	Questa versione aggiunge il supporto della modalità slow start, che aumenta gradualmente la condivisione di richieste che il sistema di bilanciamento del carico invia a un target appena registrato mano a mano che si riscalda.	24 marzo 2018
Supporto SNI	Questa versione aggiunge il supporto del Server Name Indication (SNI).	10 Ottobre 2017
Indirizzi IP come target	In questa versione è stato aggiunto il supporto per la registrazione di indirizzi IP come target.	31 agosto 2017
Routing basato su host	Questa versione aggiunge il supporto delle richieste di instradamento basato sui nomi dell'host all'interno dell'interstazione dell'host.	5 Aprile 2017

Politiche di sicurezza per TLS 1.1 e TLS 1.2	Questa versione aggiunge policy di sicurezza per TLS 1.1 e TLS 1.2.	6 febbraio 2017
IPv6 supporto	Questa versione aggiunge il supporto per IPv6 gli indirizzi.	25 gennaio 2017
Tracciamento delle richieste	Questa versione aggiunge il supporto del tracciamento delle richieste.	22 Novembre 2016
Supporto dei percentili per la metrica TargetResponseTime	Questa versione aggiunge il supporto per le nuove statistic he percentili supportate da Amazon CloudWatch.	17 Novembre 2016
Nuovo tipo di sistema di bilanciamento del carico	Questa versione di Elastic Load Balancing introduce gli Application Load Balancer.	11 agosto 2016

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.