aws

Classic Load Balancer

Sistema di bilanciamento del carico elastico

Sistema di bilanciamento del carico elastico: Classic Load Balancer

Table of Contents

Cos'è un Classic 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 i Classic Load Balancer. Per ulteriori informazioni sugli altri bilanciatori del carico, consultare la Guida per l'utente sugli Application Load Balancer, la Guida per l'utente sui Network Load Balancer, e la Guida per l'utente sui Gateway Load Balancer.

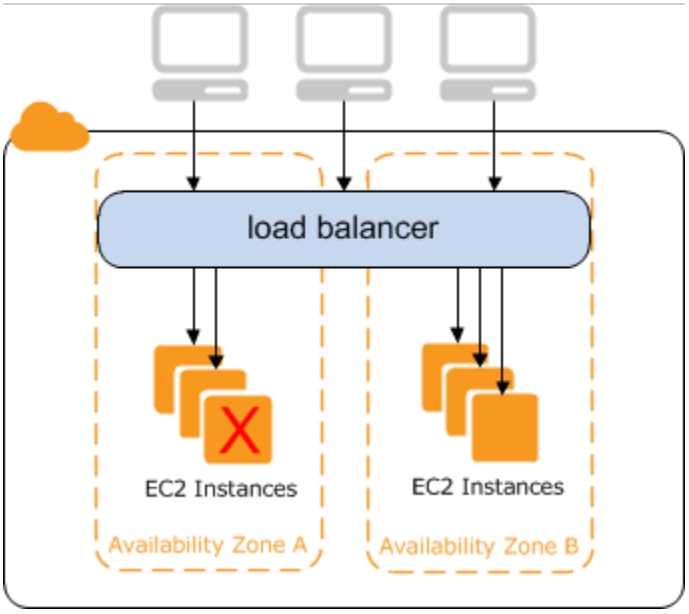
Panoramica di Classic Load Balancer

Un sistema di bilanciamento del carico distribuisce il traffico delle applicazioni in entrata su più istanze in più zone di disponibilità. EC2 Questo aumenta la tolleranza ai guasti delle applicazioni. Elastic Load Balancing rileva le istanze non integre e instrada il traffico solo verso le istanze integre.

Il load balancer funge da singolo punto di contatto per i client. Ciò aumenta la disponibilità dell'applicazione. È possibile aggiungere e rimuovere istanze dal load balancer in base alle esigenze, senza interrompere il flusso generico 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.

Un listener controlla le richieste di connessione inviate dai client, utilizzando il protocollo e la porta configurati e inoltra le richieste a una o più istanze registrate utilizzando il protocollo e il numero di porta configurati. Puoi aggiungere uno o più listener al load balancer.

Puoi configurare controlli dello stato, che vengono utilizzati per monitorare lo stato delle istanze registrate in modo che il load balancer invii richieste solo alle stanze integre.



Per assicurarti che le tue istanze registrate siano in grado di gestire il carico di richieste in ciascuna zona di disponibilità, è importante tenere circa lo stesso numero di istanze in ciascuna zona di disponibilità registrato con il load balancer. Se, ad esempio, disponi di dieci istanze nella zona di disponibilità us-west-2a e di due istanze nella zona us-west-2b, le richieste vengono distribuite in modo uniforme tra le due zone di disponibilità. Di conseguenza, le due istanze nella zona us-west-2b servono la stessa quantità di traffico delle dieci istanze nella zona us-west-2a. È invece necessario disporre di sei istanze in ogni zona di disponibilità.

Per impostazione predefinita, il load balancer distribuisce il traffico in modo uniforme su tutte le zone di disponibilità abilitate per il tuo load balancer. Per distribuire il traffico in modo uniforme su tutte le istanze registrate in tutte le zone di disponibilità, attiva il bilanciamento del carico tra zone sul tuo load balancer. Tuttavia, ti consigliamo di mantenere comunque numeri di istanze più o meno equivalenti in ciascuna zona di disponibilità per migliorare la tolleranza ai guasti.

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

Vantaggi

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

- Support per TCP e SSL ascoltatori
- Supporto per le sticky session mediante i cookie generati dall'applicazione

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

Come iniziare

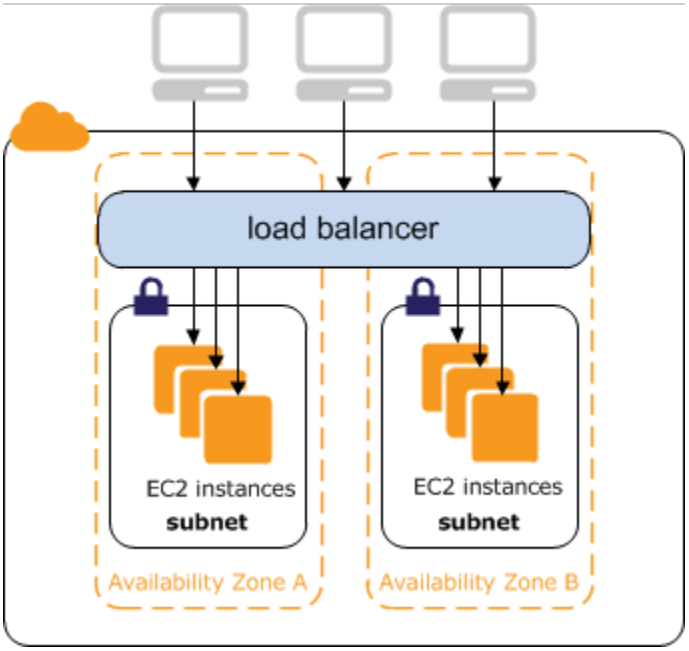
- Per informazioni su come creare un Classic Load Balancer e registrare EC2 istanze con esso, consulta. Crea un Classic Load Balancer con accesso a Internet
- Per informazioni su come creare un sistema di HTTPS bilanciamento del carico e registrarne EC2 le istanze, consulta. Crea un Classic Load Balancer con un listener HTTPS
- Per informazioni su come utilizzare le varie funzionalità supportate da Classic Load Balancers, consulta. Configura il Classic Load Balancer

Prezzi

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

Classic Load Balancer connessi a Internet

Quando crei un Classic Load Balancer, puoi renderlo un load balancer interno o un load balancer connesso a Internet. Un sistema di bilanciamento del carico connesso a Internet ha un DNS nome risolvibile pubblicamente, quindi può instradare le richieste dai client su Internet alle istanze registrate con il sistema di bilanciamento del carico. EC2



Il DNS nome di un sistema di bilanciamento del carico interno è risolvibile pubblicamente negli indirizzi IP privati dei nodi. Pertanto, i sistemi di bilanciamento del carico interni possono instradare solo le richieste dei client con accesso al sistema di bilanciamento del carico per il VPC sistema. Per ulteriori informazioni, consulta bilanciatori del carico interni.

Indice

DNSNomi pubblici per il sistema di bilanciamento del carico

Quando il load balancer viene creato, riceve un DNS nome pubblico che i client possono utilizzare per inviare richieste. I DNS server risolvono il DNS nome del sistema di bilanciamento del carico negli indirizzi IP pubblici dei nodi del sistema di bilanciamento del carico. Ogni nodo del load balancer è connesso alle istanze di back-end utilizzando indirizzi IP privati.

La console visualizza un DNS nome pubblico con il seguente formato:

```
name-1234567890.region.elb.amazonaws.com
```

Crea un Classic Load Balancer con accesso a Internet

Quando si crea un sistema di bilanciamento del carico, si configurano i listener, si configurano i controlli di integrità e si registrano le istanze di back-end. Per configurare un listener, specifica un protocollo e una porta per connessioni front-end (dal client al load balancer) e una porta per connessioni back-end (dal load balancer alle istanze di back-end). Puoi configurare più listener per il load balancer.

Questo tutorial fornisce un'introduzione pratica ai Classic Load Balancers tramite un'interfaccia basata sul Web. AWS Management Console Creerai un sistema di bilanciamento del carico che riceve il HTTP traffico pubblico e lo invia alle tue istanze. EC2

Per creare un sistema di bilanciamento del carico con un HTTPS listener, consulta. Crea un Classic Load Balancer con un listener HTTPS

Attività

- Prima di iniziare
- Crea un Classic Load Balancer utilizzando il AWS Management Console

Prima di iniziare

- Crea un cloud privato virtuale ()VPC. Per ulteriori informazioni, consulta Raccomandazioni per il tuo VPC.
- Avvia le EC2 istanze che intendi registrare con il sistema di bilanciamento del carico. Assicurati che i gruppi di sicurezza per queste istanze consentano HTTP l'accesso alla porta 80.
- Installa un server Web, come Apache o Internet Information Services (IIS), su ogni istanza, inserisci il DNS nome nel campo dell'indirizzo di un browser Web connesso a Internet e verifica che il browser visualizzi la pagina predefinita del server.

Crea un Classic Load Balancer utilizzando il AWS Management Console

Utilizza la procedura seguente per creare il Classic Load Balancer. Fornisci alcune informazioni di configurazione di base per il sistema di bilanciamento del carico, ad esempio un nome e uno schema. Successivamente, fornisci alcune informazioni relative alla rete e all'ascoltatore che indirizza il traffico verso le istanze.

Per creare un Classic 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 selezionare la stessa regione che hai selezionato per le tue EC2 istanze.
3. Nel pannello di navigazione, sotto Load Balancing (Bilanciamento del carico), scegli Load Balancers (Load balancer).
4. Seleziona Create Load Balancer (Crea load balancer).
5. Espandi la sezione Classic Load Balancer, quindi scegli Crea.
6. Configurazione di base
   a. In Nome del sistema di bilanciamento del carico, immetti un nome per il sistema di bilanciamento del carico.

      Il nome del Classic Load Balancer deve essere univoco nel set di Classic Load Balancer della regione, può essere composto da un massimo di 32 caratteri, può contenere solo caratteri alfanumerici e trattini e non deve iniziare o finire con un trattino.
   b. In Schema, seleziona Con connessione Internet.
7. Mappatura della rete
   a. Per VPC, seleziona la stessa VPC che hai selezionato per le tue istanze.
   b. In Mappature, seleziona innanzitutto una zona di disponibilità, quindi scegli una sottorete pubblica tra quelle disponibili. Puoi selezionare solo una sottorete per ogni zona di disponibilità. Per migliorare la disponibilità del sistema di bilanciamento del carico, seleziona più zone di disponibilità e sottoreti.
8. Gruppi di sicurezza
   - Per i gruppi di sicurezza, seleziona un gruppo di sicurezza esistente configurato per consentire il HTTP traffico richiesto sulla porta 80.
9. Ascoltatori e instradamento

a. In Listener, assicurati che il protocollo sia `HTTP` e che la porta sia `80`.

b. In Istanza, assicurati che il protocollo sia `HTTP` e che la porta sia `80`.

10. Controlli dell'integrità

a. In Protocollo Ping, assicurati che il protocollo sia `HTTP`.

b. In Porta Ping, assicurati che la porta sia `80`.

c. In Percorso ping, assicurati che il percorso sia `/`.

d. In Impostazioni avanzate del controllo dell'integrità, utilizza i valori predefiniti.

11. Istanze

a. Seleziona Aggiungi istanze per visualizzare la schermata di selezione delle istanze.

b. In Istanze disponibili puoi selezionare le istanze attualmente disponibili per il sistema di bilanciamento del carico, in base alle impostazioni di rete in uso.

c. Dopo aver effettuato le selezioni, scegli Conferma per aggiungere le istanze da registrare al sistema di bilanciamento del carico.

12. Attributes

- Mantieni i valori predefiniti per Abilita il sistema di bilanciamento del carico tra zone, Abilita svuotamento della connessione e Timeout (intervallo di svuotamento).

13. Tag del sistema di bilanciamento del carico (facoltativo)

a. Il campo Chiave è obbligatorio.

b. Il campo Valore è facoltativo.

c. Per aggiungere un altro tag, seleziona Aggiungi nuovo tag, quindi inserisci i valori nel campo Chiave e facoltativamente nel campo Valore.

d. Per rimuovere un tag esistente, seleziona Rimuovi accanto al tag da rimuovere.

14. Riepilogo e creazione

a. Se hai bisogno di modificare le impostazioni, seleziona Modifica accanto all'impostazione da cambiare.

b. Dopo aver verificato le impostazioni mostrate nel riepilogo, seleziona Crea sistema di bilanciamento del carico per iniziare a creare il sistema di bilanciamento del carico.

c. Nella pagina di creazione finale, seleziona Visualizza sistema di bilanciamento del carico per visualizzare il sistema di bilanciamento del carico nella console AmazonEC2.

15. Verify

    a. Seleziona il nuovo load balancer.

    b. Nella scheda Istanze di destinazione, verifica la colonna Stato di integrità. Dopo che almeno una delle tue EC2 istanze è in servizio, puoi testare il tuo sistema di bilanciamento del carico.

    c. Nella sezione Dettagli, copia il DNSnome del sistema di bilanciamento del carico, che sarà simile a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`

    d. Incolla il DNSnome del sistema di bilanciamento del carico nel campo dell'indirizzo di un browser web pubblico connesso a Internet. Se il sistema di bilanciamento del carico funziona correttamente, verrà visualizzata la pagina predefinita del server.

16. Rimozione (facoltativa)

    a. Se hai un CNAME record per il tuo dominio che punta al sistema di bilanciamento del carico, indirizzalo verso una nuova posizione e attendi che la DNS modifica abbia effetto prima di eliminare il sistema di bilanciamento del carico.

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

    c. Selezionare il load balancer.

    d. Seleziona Operazioni, Elimina sistema di bilanciamento del carico.

    e. Quando viene richiesta la conferma, digita `confirm`, quindi scegli Elimina.

    f. Dopo aver eliminato un sistema di bilanciamento del carico, le EC2 istanze registrate con il sistema di bilanciamento del carico continuano a funzionare. Verranno addebitate le spese per ogni ora parziale o intera in cui continuano a funzionare. Quando non hai più bisogno di un'EC2istanza, puoi interromperla o terminarla per evitare di incorrere in costi aggiuntivi.

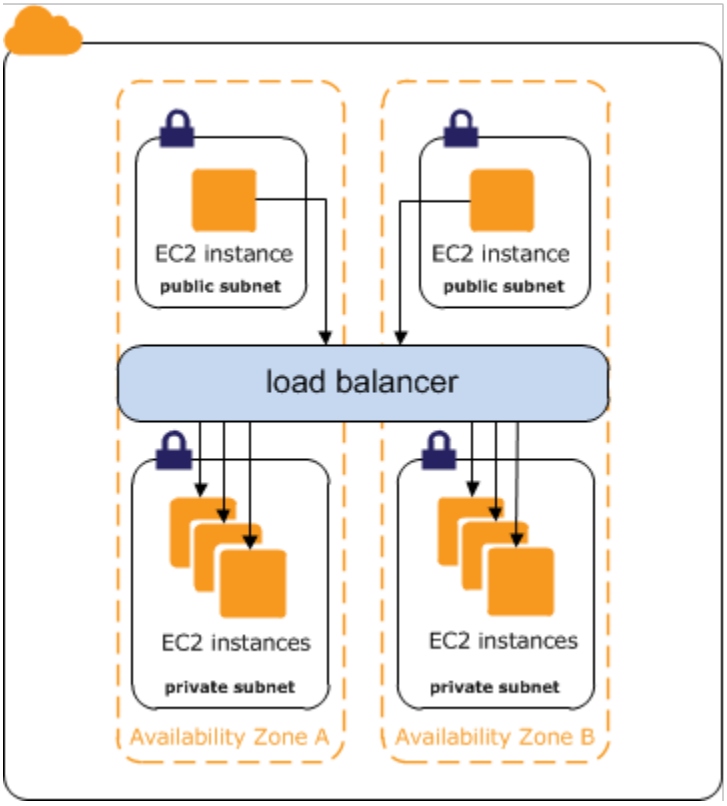
Classic Load Balancer interni

Quando crei un sistema di bilanciamento del carico, devi scegliere se renderlo un sistema di bilanciamento del carico interno o connesso a Internet.

I nodi di un load balancer con connessione Internet dispongono di indirizzi IP pubblici. Il DNS nome di un sistema di bilanciamento del carico connesso a Internet è risolvibile pubblicamente negli indirizzi IP pubblici dei nodi. Di conseguenza, i bilanciatori del carico connessi a Internet possono instradare le richieste dai client tramite Internet. Per ulteriori informazioni, consulta Classic Load Balancer connessi a Internet.

I nodi di un load balancer interno dispongono solo di indirizzi IP privati. Il DNS nome di un load balancer interno è risolvibile pubblicamente negli indirizzi IP privati dei nodi. Pertanto, i sistemi di bilanciamento del carico interni possono instradare solo le richieste dei client con accesso al sistema di bilanciamento del carico per il VPC sistema.

Se l'applicazione dispone di più livelli, ad esempio server web che devono essere connessi a Internet e server di database che sono connessi solo ai server web, puoi progettare un'architettura che utilizza bilanciatori del carico sia interni che connessi a Internet. Crea un load balancer connesso a Internet e registra il server Web insieme ad esso. Crea un load balancer interno e registra il server di database insieme ad esso. I server Web ricevono le richieste dal load balancer connesso a Internet e inviano le richieste per i server di database al load balancer interno. I server di database ricevono le richieste dal load balancer interno.



Indice

DNSNome pubblico per il sistema di bilanciamento del carico

Quando viene creato un load balancer interno, riceve un DNS nome pubblico con il seguente formato:

```
internal-name-123456789.region.elb.amazonaws.com
```

I DNS server risolvono il DNS nome del sistema di bilanciamento del carico negli indirizzi IP privati dei nodi di bilanciamento del carico per il bilanciamento del carico interno. Ogni nodo del load balancer è connesso agli indirizzi IP privati delle istanze di back-end utilizzando interfacce di rete elastiche. Se il bilanciamento del carico tra zone è abilitato, ogni nodo è connesso a ciascuna istanza di back-end, a prescindere dalla zona di disponibilità. In caso contrario, ogni nodo è connesso solo alle istanze che si trovano nella sua zona di disponibilità.

Creazione di un Classic Load Balancer interno

Puoi creare un sistema di bilanciamento del carico interno per distribuire il traffico verso le tue EC2 istanze dai client con accesso al sistema di bilanciamento del carico VPC per il sistema.

Indice

Prerequisiti

- Se non ne hai ancora creato uno VPC per il tuo sistema di bilanciamento del carico, devi crearlo prima di iniziare. Per ulteriori informazioni, consulta Raccomandazioni per il tuo VPC.
- Avvia le EC2 istanze che intendi registrare con il sistema di bilanciamento del carico interno. Assicurati di avviarle in sottoreti private nell'area VPC prevista per il bilanciamento del carico.

Creazione di un load balancer interno mediante la console

Utilizza la procedura seguente per creare il Classic Load Balancer interno. Fornisci alcune informazioni di configurazione di base per il sistema di bilanciamento del carico, ad esempio un nome e uno schema. Successivamente, fornisci alcune informazioni relative alla rete e all'ascoltatore che indirizza il traffico verso le istanze.

Per creare un Classic Load Balancer interno 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 selezionare la stessa regione che hai selezionato per le tue EC2 istanze.
3. Nel pannello di navigazione, sotto Load Balancing (Bilanciamento del carico), scegli Load Balancers (Load balancer).
4. Seleziona Create Load Balancer (Crea load balancer).
5. Espandi la sezione Classic Load Balancer, quindi scegli Crea.
6. Configurazione di base

a. In Nome del sistema di bilanciamento del carico, immetti un nome per il sistema di bilanciamento del carico.

   Il nome del Classic Load Balancer deve essere univoco nel set di Classic Load Balancer della regione, può essere composto da un massimo di 32 caratteri, può contenere solo caratteri alfanumerici e trattini e non deve iniziare o finire con un trattino.

b. In Schema, seleziona Interno.

7. Mappatura della rete

   a. Per VPC, seleziona la stessa VPC che hai selezionato per le tue istanze.

   b. In Mappature, seleziona innanzitutto una zona di disponibilità, quindi scegli una sottorete tra quelle disponibili. Puoi selezionare solo una sottorete per ogni zona di disponibilità. Per migliorare la disponibilità del sistema di bilanciamento del carico, seleziona più zone di disponibilità e sottoreti.

8. Per i gruppi di sicurezza, seleziona un gruppo di sicurezza esistente configurato per consentire il HTTP traffico richiesto sulla porta 80. In alternativa, puoi creare un nuovo gruppo di sicurezza se l'applicazione utilizza porte e protocolli diversi.

9. Ascoltatori e instradamento

   a. In Listener, assicurati che il protocollo sia `HTTP` e che la porta sia `80`.

   b. In Istanza, assicurati che il protocollo sia `HTTP` e che la porta sia `80`.

10. Controlli dell'integrità

    a. In Protocollo ping, il valore predefinito è `HTTP`.

    b. In Porta ping, il valore predefinito è `80`.

    c. In Percorso ping, il valore predefinito è `/`.

    d. In Impostazioni avanzate del controllo dell'integrità, utilizza i valori predefiniti o inserisci valori specifici per la tua applicazione.

11. Istanze

    a. Seleziona Aggiungi istanze per visualizzare la schermata di selezione delle istanze.

    b. In Istanze disponibili puoi selezionare le istanze attualmente disponibili per il sistema di bilanciamento del carico, in base alle impostazioni di rete selezionate in precedenza.

    c. Dopo aver effettuato le selezioni, scegli Conferma per aggiungere le istanze da registrare al sistema di bilanciamento del carico.

12. Attributes

    - Mantieni i valori predefiniti per Abilita il sistema di bilanciamento del carico tra zone, Abilita svuotamento della connessione e Timeout (intervallo di svuotamento).

13. Tag del sistema di bilanciamento del carico (facoltativo)

    a. Il campo Chiave è obbligatorio.
    b. Il campo Valore è facoltativo.
    c. Per aggiungere un altro tag, seleziona Aggiungi nuovo tag, quindi inserisci i valori nel campo Chiave e facoltativamente nel campo Valore.
    d. Per rimuovere un tag esistente, seleziona Rimuovi accanto al tag da rimuovere.

14. Riepilogo e creazione

    a. Se hai bisogno di modificare le impostazioni, seleziona Modifica accanto all'impostazione da cambiare.
    b. Dopo aver verificato le impostazioni mostrate nel riepilogo, seleziona Crea sistema di bilanciamento del carico per iniziare a creare il sistema di bilanciamento del carico.
    c. Nella pagina di creazione finale, seleziona Visualizza sistema di bilanciamento del carico per visualizzare il sistema di bilanciamento del carico nella console AmazonEC2.

15. Verify

    a. Seleziona il nuovo load balancer.
    b. Nella scheda Istanze di destinazione, verifica la colonna Stato di integrità. Dopo che almeno una delle tue EC2 istanze è in servizio, puoi testare il tuo sistema di bilanciamento del carico.
    c. Nella sezione Dettagli, copia il DNSnome del sistema di bilanciamento del carico, che sarà simile a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`
    d. Incolla il DNSnome del sistema di bilanciamento del carico nel campo dell'indirizzo di un browser web pubblico connesso a Internet. Se il sistema di bilanciamento del carico funziona correttamente, verrà visualizzata la pagina predefinita del server.

16. Rimozione (facoltativa)

    a. Se hai un CNAME record per il tuo dominio che punta al sistema di bilanciamento del carico, indirizzalo verso una nuova posizione e attendi che la DNS modifica abbia effetto prima di eliminare il sistema di bilanciamento del carico.
    b. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.

c. Selezionare il load balancer.

d. Seleziona Operazioni, Elimina sistema di bilanciamento del carico.

e. Quando viene richiesta la conferma, digita `confirm`, quindi scegli Elimina.

f. Dopo aver eliminato un sistema di bilanciamento del carico, le EC2 istanze registrate con il sistema di bilanciamento del carico continuano a funzionare. Verranno addebitate le spese per ogni ora parziale o intera in cui continuano a funzionare. Quando non hai più bisogno di un'EC2istanza, puoi interromperla o terminarla per evitare di incorrere in costi aggiuntivi.

Crea un sistema di bilanciamento del carico interno utilizzando il AWS CLI

Per impostazione predefinita, Elastic Load Balancing crea un load balancer connesso a Internet. Utilizza la procedura seguente per creare un bilanciamento del carico interno e registrare EC2 le istanze con il bilanciamento del carico interno appena creato.

Per creare un load balancer interno

1. Utilizzate il create-load-balancercomando con l'`--scheme`opzione impostata su`internal`, come segue:

```
aws elb create-load-balancer --load-balancer-name my-internal-loadbalancer --
listeners Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80
 --subnets subnet-4e05f721 --scheme internal --security-groups sg-b9ffedd5
```

   Di seguito è riportata una risposta di esempio. Notare che il nome indica che questo è un load balancer interno.

```
{
    "DNSName": "internal-my-internal-loadbalancer-786501203.us-
west-2.elb.amazonaws.com"
}
```

2. Utilizzate il seguente comando register-instances-with-load-balancer per aggiungere istanze:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-internal-
loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

   Di seguito è riportata una risposta di esempio:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

3. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare il bilanciamento del carico interno:

```
aws elb describe-load-balancers --load-balancer-name my-internal-loadbalancer
```

La risposta include i campi `DNSName` e `Scheme`, che indicano che questo è un load balancer interno.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "DNSName": "internal-my-internal-loadbalancer-1234567890.us-
west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-b9ffedd5"
            ],
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": []
            },
            "LoadBalancerName": "my-internal-loadbalancer",
            "CreatedTime": "2014-05-22T20:32:19.920Z",
            "AvailabilityZones": [
                "us-west-2a"
            ],
            "Scheme": "internal",
            ...
        }
```

```
    ]
}
```

Configura il Classic Load Balancer

Dopo aver creato un Classic Load Balancer, puoi modificarne la configurazione. Ad esempio, è possibile aggiornare gli attributi del load balancer, le sottoreti e i gruppi di sicurezza.

Attributi del sistema di bilanciamento del carico

Drenaggio della connessione

Se abilitata, il load balancer consente il completamento delle richieste esistenti prima che trasferisca il traffico da un'istanza non integra o la cui registrazione è stata annullata.

Bilanciamento del carico su più zone

Se abilitata, il load balancer instrada il traffico richiesto in modo uniforme su tutte le istanze, a prescindere dalle zone di disponibilità.

Modalità di migrazione Desync

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`.

Timeout di inattività

Se abilitata, il load balancer consente alle connessioni di rimanere inattive (i dati non vengono inviati sulla connessione) per la durata specificata. Il valore predefinito è 60 secondi.

Sessioni permanenti

I Load Balancer Classic supportano la persistenza delle sessioni in base alla durata e all'applicazione.

Dettagli del sistema di bilanciamento del carico

Gruppi di sicurezza

I gruppi di sicurezza del sistema di bilanciamento del carico devono consentire il traffico sulle porte listener e health check.

Sottoreti

È possibile espandere la capacità del sistema di bilanciamento del carico a sottoreti aggiuntive.

Protocollo proxy

Se abilitata, aggiungiamo un'intestazione con le informazioni di connessione che vengono inviate all'istanza.

Tag

Puoi aggiungere tag per classificare i tuoi sistemi di bilanciamento del carico.

Configura il timeout per connessione inattiva per il Classic Load Balancer

Per ogni richiesta che un client fa attraverso un Classic Load Balancer, questo gestisce due connessioni: La connessione front-end è tra il client e il load balancer. La connessione back-end avviene tra il load balancer e un'istanza registrata. EC2 Il load balancer ha configurato un periodo di timeout di inattività che si applica anche alle sue connessioni. Se allo scadere di questo periodo di timeout di inattività non vengono inviati o ricevuti dati, il load balancer chiude la connessione. Per garantire tempo sufficiente per il completamento delle operazioni di lunga durata (ad esempio il caricamento di file), invia almeno 1 byte di dati prima dello scadere di ogni periodo di timeout di inattività e aumenta la durata del periodo in base alle esigenze.

Se utilizzi i HTTPS listener HTTP and, ti consigliamo di abilitare l'opzione HTTP keep-alive per le tue istanze. Puoi abilitare keep-alive nelle impostazioni del server Web per le tue istanze. Keep-alive, quando abilitato, consente al load balancer di riutilizzare le connessioni back-end fino alla scadenza del timeout keep-alive. Per assicurarti che il load balancer sia responsabile della chiusura delle connessioni all'istanza, assicurati che il valore impostato per il tempo di HTTP keep-alive sia maggiore dell'impostazione del timeout di idle configurata per il bilanciamento del carico.

Tieni presente che le sonde TCP keep-alive non impediscono al load balancer di interrompere la connessione perché non inviano dati nel payload.

Indice

Configura il tempo di inattività utilizzando la console

Per impostazione predefinita, Elastic Load Balancing imposta il tempo di inattività per il load balancer su 60 secondi. Utilizzare la procedura seguente per impostare un valore diverso per il timeout di inattività.

Per configurare l'impostazione del timeout di inattività 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. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del traffico, digita un valore in Tempo di inattività. L'intervallo per il timeout di inattività è compreso tra 1 e 4.000 secondi.
6. Scegli Save changes (Salva modifiche).

Configura il tempo di inattività utilizzando la AWS CLI

Usa il seguente modify-load-balancer-attributescomando per impostare il timeout di inattività per il tuo sistema di bilanciamento del carico:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionSettings\":{\"IdleTimeout\":30}}"
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerAttributes": {
        "ConnectionSettings": {
            "IdleTimeout": 30
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Configura il load balancer tra zone per il Classic Load Balancer

Con il bilanciamento del carico su più zone, ogni nodo del load balancer per Classic Load Balancer distribuisce le richieste in modo uniforme su istanze registrate in tutte le zone di disponibilità abilitate. Se il load balancer su più zone non è attivo, ogni nodo di load balancer distribuisce le richieste in modo uniforme sulle istanze registrate solo nella relativa zona di disponibilità. Per ulteriori informazioni, consulta Bilanciamento del carico su più zone nella Guida per l'utente di Elastic Load Balancing.

Il load balancer tra zone riduce la necessità di mantenere numeri equivalenti di istanze in ciascuna zona di disponibilità abilitata e migliora le capacità della tua applicazione di gestire la perdita di una o più istanze. Tuttavia, consigliamo di mantenere comunque numeri di istanze più o meno equivalenti in ciascuna zona di disponibilità abilitata per una maggiore tolleranza ai guasti.

Per gli ambienti in cui i client memorizzano nella cache DNS le ricerche, le richieste in arrivo potrebbero favorire una delle zone di disponibilità. Utilizzando il load balancer su più zone, questo squilibrio nel carico di richieste viene distribuito su tutte le istanze disponibili della regione, riducendo l'impatto dei client malfunzionanti.

Quando si crea un Classic Load Balancer, l'impostazione predefinita per il load balancer tra zone dipende dal modo in cui crei il load balancer. Con l'opzione API oCLI, il bilanciamento del carico tra zone è disabilitato per impostazione predefinita. Con AWS Management Console, l'opzione per abilitare il bilanciamento del carico tra zone è selezionata per impostazione predefinita. Dopo aver creato un Classic Load Balancer, è possibile abilitare o disabilitare il load balancer tra zone in qualsiasi momento.

Indice

Abilita il load balancer tra zone

Puoi abilitare il load balancer tra zone per il tuo Classic Load Balancer in qualsiasi momento.

Per abilitare il bilanciamento del carico su più zone utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del routing della zona di disponibilità, abilita Bilanciamento del carico tra zone.
6. Scegli Save changes (Salva modifiche).

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

1. Utilizzate il seguente modify-load-balancer-attributescomando per impostare l'`CrossZoneLoadBalancing`attributo del vostro sistema di bilanciamento del carico su: `true`

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
```

   Di seguito è riportata una risposta di esempio:

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": true
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Facoltativo) Utilizzate il seguente describe-load-balancer-attributescomando per verificare che il bilanciamento del carico tra zone sia abilitato per il sistema di bilanciamento del carico:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

   Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
```

```
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Disabilita il load balancer tra zone

Puoi disabilitare l'opzione di bilanciamento del carico tra per il tuo load balancer in qualsiasi momento.

Per disabilitare il load balancer tra zone utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del routing della zona di disponibilità, disabilita Bilanciamento del carico tra zone.
6. Scegli Save changes (Salva modifiche).

Per disabilitare il bilanciamento del carico tra zone, impostare l'attributo `CrossZoneLoadBalancing` del load balancer su `false`.

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

1. Utilizzando il seguente comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":false}}"
```

Di seguito è riportata una risposta di esempio:

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": false
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Facoltativo) Utilizzate il seguente describe-load-balancer-attributescomando per verificare che il bilanciamento del carico tra zone sia disabilitato per il sistema di bilanciamento del carico:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": false
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Configura il Connection Draining per il Classic Load Balancer

Per garantire che un Classic Load Balancer interrompa l'invio di richieste alle istanze non integre o di cui è in corso l'annullamento della registrazione, mantenendo aperte le connessioni esistenti, utilizza Connection Draining. In questo modo il load balancer può completare le richieste in transito effettuate per le istanze non integre o per le quali si sta eseguendo l'annullamento della registrazione.

Quando si abilita Connection Draining, è possibile specificare un intervallo di tempo massimo durante il quale il load balancer mantiene le connessioni attive prima di segnalare l'istanza come con registrazione annullata. Il valore di timeout massimo può essere impostato tra 1 e 3.600 secondi (l'impostazione predefinita è 300 secondi). Quando viene raggiunto il limite massimo, il load balancer chiude forzatamente le connessioni all'istanza con registrazione annullata.

Mentre vengono gestite le richieste in transito, il load balancer segnala lo stato di un'istanza come `InService: Instance deregistration currently in progress`. Quando l'istanza di cui è in corso l'annullamento della registrazione ha finito di gestire tutte le richieste in transito, o quando viene raggiunto il limite massimo di timeout, il load balancer segnala l'istanza come `OutOfService: Instance is not currently registered with the LoadBalancer`.

Se un'istanza diventa non integra, il load balancer segnala il rispettivo stato come `OutOfService`. Eventuali richieste in transito effettuate all'istanza non integra verranno completate. Il limite massimo di timeout non è valido per le connessioni alle istanze non integre.

Se le istanze fanno parte di un gruppo Auto Scaling e per il load balancer è abilitato Connection Draining, Auto Scaling attende il completamento delle richieste in transito o la scadenza del timeout massimo, prima di terminare le istanze a causa di un evento di dimensionamento o della sostituzione del controllo dello stato.

È possibile disabilitare Connection Draining se si desidera che il load balancer chiuda immediatamente le connessioni alle istanze di cui è in corso l'annullamento della registrazione o che sono diventate non integre. Quando Connection Draining è disabilitato, le richieste in transito effettuate alle istanze non integre o di cui è in corso l'annullamento della registrazione non vengono completate.

Indice

Abilita Connection Draining

Puoi abilitare Connection Draining per il tuo load balancer in qualsiasi momento.

Per abilitare Connection Draining utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del traffico, seleziona Abilita svuotamento della connessione.
6. (Facoltativo) Per Timeout (intervallo di svuotamento), digita un valore compreso tra 1 e 3.600 secondi. In caso contrario, viene utilizzato il valore predefinito di 300 secondi.
7. Scegli Save changes (Salva modifiche).

Per abilitare il drenaggio della connessione utilizzando il AWS CLI

Utilizzando il seguente comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout\":300}}"
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": true,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Disabilita Connection Draining

Puoi disabilitare Connection Draining per il tuo load balancer in qualsiasi momento.

Per disabilitare Connection Draining utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del traffico, deseleziona Abilita svuotamento della connessione.
6. Scegli Save changes (Salva modifiche).

Per disabilitare il drenaggio della connessione utilizzando il AWS CLI

Utilizzando il seguente comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":false}}"
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Configura le sticky session per il Classic Load Balancer

Per impostazione predefinita, un Classic Load Balancer esegue il routing di ogni richiesta in modo indipendente all'istanza registrata con il carico minore. Tuttavia, è possibile usare la caratteristica

sticky session (nota anche come affinità di sessione), che consente al load balancer di associare una sessione utente a un'istanza specifica. Questo garantisce che durante la sessione tutte le richieste dell'utente vengano inviate alla stessa istanza.

La chiave per la gestione delle sticky session consiste nel determinare per quanto tempo il tuo load balancer deve instradare costantemente la richiesta dell'utente verso la stessa istanza. Se la tua applicazione ha il proprio cookie di sessione, puoi configurare Elastic Load Balancing in modo che il cookie della sessione rispetti la durata specificata dal cookie della sessione dell'applicazione. Se la tua applicazione non ha un proprio cookie di sessione, puoi configurare Elastic Load Balancing per creare un cookie della sessione specificando la durata della persistenza.

Elastic Load Balancing crea un cookie, denominato AWSELB, che viene utilizzato per mappare la sessione all'istanza.

Requisiti

- Un sistema di HTTPS bilanciamento del caricoHTTP/.
- Almeno un'istanza integra in ciascuna zona di disponibilità.

Compatibilità

- La proprietà RFC for the path di un cookie consente i caratteri di sottolineatura. Tuttavia, Elastic Load Balancing URI codifica i caratteri di sottolineatura `%5F` perché alcuni browser, come Internet Explorer 7, prevedono che i caratteri di sottolineatura vengano codificati come. URI `%5F` A causa del potenziale impatto sui browser attualmente funzionanti, Elastic Load Balancing continua a URI codificare i caratteri di sottolineatura. Ad esempio, se il cookie presenta la proprietà `path=/my_path`, Elastic Load Balancing modifica questa proprietà nella richiesta inoltrata a `path=/my%5Fpath`.
- Non è possibile impostare il flag `secure` o `HttpOnly` sui cookie di persistenza della sessione basati sulla durata. Tuttavia, questi cookie non contengono informazioni sensibili. Tieni presente che se imposti il `secure` flag o il `HttpOnly` flag su un cookie di persistenza della sessione controllato dall'applicazione, questo viene impostato anche sul cookie. AWSELB
- Se nel campo `Set-Cookie` di un cookie di applicazione è presente un punto e virgola finale, il load balancer ignora il cookie.

Indice

- Persistenza della sessione controllata dalle applicazioni

Persistenza della sessione basata sulla durata

Il load balancer utilizza un cookie speciale per tracciare l'istanza di ogni richiesta a ciascun listener. AWSELB Quando il load balancer riceve una richiesta, verifica innanzitutto se questo cookie è presente nella richiesta. In questo caso, la richiesta viene inviata all'istanza specificata nel cookie. Se non sono presenti cookie, il load balancer sceglie un'istanza in base all'algoritmo di bilanciamento del carico esistente. Viene inserito un cookie nella risposta per le richieste successive vincolanti dallo stesso utente a quell'istanza. La configurazione della policy di persistenza definisce la scadenza di un cookie, che stabilisce la durata della validità per ciascun cookie. Il load balancer non aggiorna il periodo di scadenza del cookie e non verifica se il cookie è scaduto prima di utilizzarlo. Una volta scaduto un cookie, la sessione non è più una sticky session. Il client deve rimuovere il cookie dal rispettivo archivio alla scadenza.

Con le richieste CORS (condivisione di risorse tra origini), alcuni browser richiedono di `SameSite=None; Secure` abilitare la persistenza. In questo caso, Elastic Load Balancing crea un secondo cookie di adesività AWSELBCORS, che include le stesse informazioni del cookie di adesività originale più questo attributo. `SameSite` I clienti ricevono entrambi i cookie.

Se un'istanza non riesce o diventa non integra, il load balancer interrompe il routing delle richieste a quell'istanza e sceglie una nuova istanza integra in base all'algoritmo del load balancer esistente. La richiesta viene instradata verso la nuova istanza, come se non vi fosse alcun cookie e la sessione non è più una sticky session.

Se un client passa a un listener con una porta di back-end diversa, la persistenza viene persa.

Per abilitare le sticky session basate sulla durata per un load balancer utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Gestisci ascoltatori.
5. Nella pagina Gestisci ascoltatori, individua l'ascoltatore da aggiornare e scegli Modifica in Viscosità dei cookie.

6. Nel pop-up Modifica l'impostazione della persistenza dei cookie, seleziona Generato dal bilanciamento del carico.
7. (Facoltativo) Per Periodo di scadenza, digita il periodo di scadenza del cookie espresso in secondi. Se non si specifica un periodo di scadenza, la sticky session ha la stessa durata della sessione del browser.
8. Scegli Salva modifiche per chiudere la finestra pop-up.
9. Scegli Salva modifiche per tornare alla pagina dei dettagli del sistema di bilanciamento del carico.

Per abilitare le sticky session basate sulla durata per un load balancer utilizzando l AWS CLI

1. Utilizza il seguente comando create-lb-cookie-stickiness-policy per creare una politica di persistenza dei cookie generata dal sistema di bilanciamento del carico con un periodo di scadenza dei cookie di 60 secondi:

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

2. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la persistenza della sessione per il sistema di bilanciamento del carico specificato:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-duration-cookie-policy
```

> **Note**
>
> Il comando `set-load-balancer-policies-of-listener` sostituisce il set di policy corrente associato alla porta del load balancer specificata. Ogni volta che si utilizza il comando, specificare l'opzione `--policy-names` per elencare tutte le policy da abilitare.

3. (Facoltativo) Utilizzate il describe-load-balancerscomando seguente per verificare che la policy sia abilitata:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La risposta include le seguenti informazioni, che mostrano che la policy è abilitata per il listener sulla porta specificata:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-duration-cookie-policy",
                        "ELBSecurityPolicy-TLS-1-2-2017-01"
                    ]
                },
                ...
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [
                 {
                        "PolicyName": "my-duration-cookie-policy",
                        "CookieExpirationPeriod": 60
                    }

                ],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": [
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

Persistenza della sessione controllata dalle applicazioni

Il load balancer utilizza un cookie speciale per associare la sessione all'istanza che ha gestito la richiesta iniziale, ma segue il ciclo di vita del cookie dell'applicazione specificato nella configurazione della policy. Il load balancer inserisce solo un nuovo cookie di persistenza, se la risposta dell'applicazione include un nuovo cookie dell'applicazione. Il cookie di persistenza del load balancer non si aggiorna con ogni richiesta. Se il cookie dell'applicazione viene rimosso esplicitamente o scade, la sessione smette di essere un sticky session fino a quando non viene rilasciato un nuovo cookie dell'applicazione.

I seguenti attributi impostati dalle istanze back-end vengono inviati ai client nel cookie: `path`, `port`, `domain`, `secure`, `httponly`, `discard`, `max-age`, `expires`, `version`, `comment`, `commenturl` e `samesite`.

Se un'istanza non riesce o diventa non integra, il load balancer interrompe il routing delle richieste a quell'istanza e sceglie una nuova istanza integra in base all'algoritmo del load balancer esistente. Il load balancer tratta la sessione come bloccata sulla nuova istanza integra e continua a instradare le richieste verso quell'istanza, anche se l'istanza non riuscita torna indietro.

Per abilitare la persistenza della sessione controllata dall'applicazione utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Gestisci ascoltatori.
5. Nella pagina Gestisci ascoltatori, individua l'ascoltatore da aggiornare e scegli Modifica in Viscosità dei cookie.
6. Seleziona Generato dall'applicazione.
7. Per Cookie Name (Nome cookie), digitare il nome del cookie dell'applicazione.
8. Scegli Save changes (Salva modifiche).

Per abilitare la persistenza della sessione controllata dall'applicazione utilizzando il AWS CLI

1. Utilizzate il seguente comando create-app-cookie-stickiness-policy per creare una politica di persistenza dei cookie generata dall'applicazione:

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

2. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la persistenza della sessione per un sistema di bilanciamento del carico:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-app-cookie-policy
```

> **Note**
>
> Il comando `set-load-balancer-policies-of-listener` sostituisce il set di policy corrente associato alla porta del load balancer specificata. Ogni volta che si utilizza il comando, specificare l'opzione `--policy-names` per elencare tutte le policy da abilitare.

3. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che la policy permanente sia abilitata:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

4. La risposta include le seguenti informazioni, che mostrano che la policy è abilitata per il listener sulla porta specificata:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-app-cookie-policy",
```

```
                        "ELBSecurityPolicy-TLS-1-2-2017-01"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "TCP",
                        "InstanceProtocol": "TCP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [
                {
                        "PolicyName": "my-app-cookie-policy",
                        "CookieName": "my-app-cookie"
                    }

                ],
                "OtherPolicies": [
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

Configura la modalità di attenuazione della desincronizzazione per Classic Load Balancer

La modalità di mitigazione Desync protegge l'applicazione dai problemi dovuti a Desync. 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 una mitigazione duratura contro la

HTTP desincronizzazione mantenendo al contempo la disponibilità dell'applicazione. È possibile passare alla modalità più rigorosa per garantire che l'applicazione riceva solo le richieste conformi alla norma 7230. RFC

La libreria http_desync_guardian analizza le richieste per prevenire gli attacchi Desync. HTTP HTTP Per ulteriori informazioni, consulta Desync Guardian su github. HTTP

Indice

> **Tip**
>
> Questa configurazione si applica solo ai Classic Load Balancer. Per informazioni valide per Application Load Balancer, consulta Modalità di attenuazione della desincronizzazione per gli Application Load Balancer.

Classificazioni

Le classificazioni sono le seguenti.

- Conforme: Request è conforme allo standard RFC 7230 e non presenta minacce note alla sicurezza.
- Accettabile: la richiesta non è conforme allo standard RFC 7230 ma non presenta minacce note alla sicurezza.
- Ambiguo: la richiesta non è conforme allo standard RFC 7230 ma rappresenta un rischio, in quanto diversi 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.

Gli elenchi seguenti descrivono i problemi di ogni classificazione.

Accettabile

- Un'intestazione contiene un carattere diverso o di controllo. ASCII

- La versione della richiesta contiene un valore non valido.
- Esiste un'intestazione Content-Length con un valore 0 per una richiesta or. GET HEAD
- La richiesta URI contiene uno spazio non codificato. URL

Ambiguo

- La richiesta URI contiene caratteri di controllo.
- La richiesta contiene sia un'intestazione Transfer-Encoding che un'intestazione Content-Length.
- Esistono più intestazioni Content-Length con lo stesso valore.
- Un'intestazione è vuota o c'è una riga con solo spazi.
- C'è un'intestazione che può essere normalizzata per Transfer-Encoding o Content-Length utilizzando tecniche comuni di normalizzazione del testo.
- Esiste un'intestazione Content-Length per una GET richiesta or. HEAD
- Esiste un'intestazione Transfer-Encoding per una richiesta or. GET HEAD

Grave

- La richiesta URI contiene un carattere nullo o un valore di riferimento.
- L'intestazione Content-Length contiene un valore che non può essere analizzato o non è un numero valido.
- Un'intestazione contiene un carattere nullo o un'andata a capo.
- L'intestazione Transfer-Encoding contiene un valore non valido.
- Il formato del metodo di richiesta è errato.
- Il formato della versione della richiesta è errato.
- Esistono più intestazioni Content-Length con valori diversi.
- Esistono più Transfer-Encoding: intestazioni a blocchi.

Se una richiesta non è conforme alla norma RFC 7230, il sistema di bilanciamento del carico incrementa la metrica. `DesyncMitigationMode_NonCompliant_Request_Count` Per ulteriori informazioni, consulta Parametri Classic Load Balancer.

Modalità

La tabella seguente descrive come i Classic 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.

Modifica la modalità di attenuazione della desincronizzazione

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. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella pagina Modifica attributi del sistema di bilanciamento del carico, nella sezione Configurazione del traffico, scegli Difensivo - scelta consigliata, Rigido 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'`elb.http.desyncmitigationmode`attributo impostato su `monitor`o `defensive`. `strictest`

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-balancer-attributes file://attribute.json
```

Di seguito sono riportati i contenuti di `attribute.json`.

```
{
    "AdditionalAttributes": [
        {
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }
    ]
}
```

Configura il protocollo proxy per il tuo Classic Load Balancer

Il protocollo proxy è un protocollo internet utilizzato per trasportare informazioni di connessione dall'origine che richiede la connessione alla destinazione per la quale la connessione è stata richiesta. Elastic Load Balancing utilizza il protocollo proxy versione 1, che adotta un formato di intestazione leggibile.

Per impostazione predefinita, quando si utilizza Transmission Control Protocol (TCP) per connessioni front-end e back-end, Classic Load Balancer inoltra le richieste alle istanze senza modificare le intestazioni delle richieste. Se abiliti il protocollo proxy, alla richiesta viene aggiunta un'intestazione leggibile con le informazioni di connessione, ad esempio l'indirizzo IP di origine, l'indirizzo IP di destinazione e i numeri di porta. L'intestazione viene quindi inviata all'istanza come parte della richiesta.

> **Note**
>
> Non supporta l'abilitazione del protocollo proxy. AWS Management Console

Indice

Intestazione del protocollo proxy

L'intestazione del protocollo proxy consente di identificare l'indirizzo IP di un client quando si dispone di un sistema di bilanciamento del carico che lo utilizza TCP per le connessioni di back-end. Poiché i bilanciatori del carico intercettano il traffico tra i client e le istanze, i log di accesso della tua istanza contengono l'indirizzo IP del load balancer anziché il client di origine. È possibile analizzare la prima riga della richiesta per recuperare l'indirizzo IP e il numero di porta del client.

L'indirizzo del proxy nell'intestazione di IPv6 è l'IPv6indirizzo pubblico del sistema di bilanciamento del carico. Questo IPv6 indirizzo corrisponde all'indirizzo IP che viene risolto in base al DNS nome del sistema di bilanciamento del carico, che inizia con o. `ipv6` `dualstack` Se il client si connette conIPv4, l'indirizzo del proxy nell'intestazione è l'IPv4indirizzo privato del load balancer, che non è risolvibile tramite una ricerca. DNS

La riga del protocollo proxy è una riga singola che termina con un'andata a capo e un feed di riga (`"\r\n"`) e ha il formato seguente:

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP + single space +
 PROXY_IP + single space + CLIENT_PORT + single space + PROXY_PORT + "\r\n"
```

Esempio: IPv4

Di seguito è riportato un esempio della riga del protocollo proxy perIPv4.

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

Prerequisiti per l'abilitazione del protocollo proxy

Prima di iniziare, esegui queste attività:

- Verifica che il tuo load balancer non si trovi dietro un server proxy con il protocollo proxy abilitato. Se il protocollo proxy è abilitato sia sul server proxy sia sul load balancer, quest'ultimo aggiunge un'altra intestazione alla richiesta, oltre a quella già aggiunta dal server proxy. A seconda della configurazione dell'istanza, questa duplicazione potrebbe causare errori.
- Verifica che le tue istanze siano in grado di elaborare le informazioni del protocollo proxy.
- Verifica che le impostazioni del listener supportino il protocollo proxy. Per ulteriori informazioni, consulta Configurazioni del listener per i Classic Load Balancer.

Abilita il protocollo proxy utilizzando la AWS CLI

Per abilitare il protocollo proxy, devi creare una policy del tipo `ProxyProtocolPolicyType`, quindi abilitarla sulla porta dell'istanza.

Utilizza la procedura seguente per creare una nuova policy per il tuo load balancer del tipo `ProxyProtocolPolicyType`, impostare la policy appena creata per l'istanza sulla porta `80` e verificare che la policy sia abilitata.

Per abilitare il protocollo proxy per il proprio load balancer

1. (Facoltativo) Utilizzate il seguente comando describe-load-balancer-policy-types per elencare le politiche supportate da Elastic Load Balancing:

   ```
   aws elb describe-load-balancer-policy-types
   ```

   La risposta include i nomi e le descrizioni dei tipi di policy supportati. L'output per il tipo `ProxyProtocolPolicyType` è il seguente:

   ```
   {
       "PolicyTypeDescriptions": [
           ...
           {
               "PolicyAttributeTypeDescriptions": [
                   {
                       "Cardinality": "ONE",
                       "AttributeName": "ProxyProtocol",
                       "AttributeType": "Boolean"
                   }
               ],
               "PolicyTypeName": "ProxyProtocolPolicyType",
               "Description": "Policy that controls whether to include the IP address
    and port of the originating
   request for TCP messages. This policy operates on TCP/SSL listeners only"
           },
           ...
       ]
   }
   ```

2. Utilizzate il create-load-balancer-policycomando seguente per creare una policy che abiliti il protocollo proxy:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-attributes AttributeName=ProxyProtocol,AttributeValue=true
```

3. Utilizzate il seguente for-backend-server comando set-load-balancer-policies- per abilitare la policy appena creata sulla porta specificata. Questo comando sostituisce il set corrente di policy abilitate. Pertanto, l'opzione `--policy-names` deve specificare sia la policy che si aggiunge all'elenco (ad esempio `my-ProxyProtocol-policy`) sia eventuali policy che al momento sono abilitate (ad esempio `my-existing-policy`).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-ProxyProtocol-policy my-existing-policy
```

4. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che il protocollo proxy sia abilitato:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La risposta include le seguenti informazioni, che mostrano che la policy `my-ProxyProtocol-policy` è associata alla porta `80`.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "BackendServerDescriptions": [
                {
                    "InstancePort": 80,
                    "PolicyNames": [
                        "my-ProxyProtocol-policy"
                    ]
                }
            ],
            ...
        }
    ]
}
```

Disabilita il protocollo proxy utilizzando la AWS CLI

Puoi disabilitare le policy associate alla tua istanza e abilitarle in un secondo momento.

Per disabilitare la policy del protocollo proxy

1. Utilizzate il seguente for-backend-server comando set-load-balancer-policies- per disabilitare la politica del protocollo proxy omettendola dall'`--policy-names`opzione, ma includendo le altre politiche che dovrebbero rimanere abilitate (ad esempio,`my-existing-policy`).

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-existing-policy
   ```

   Se non ci sono altre politiche da abilitare, specificare una stringa vuota con l'opzione `--policy-names` come segue:

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names "[]"
   ```

2. (Facoltativo) Utilizzate il describe-load-balancerscomando seguente per verificare che la policy sia disabilitata:

   ```
   aws elb describe-load-balancers --load-balancer-name my-loadbalancer
   ```

   La risposta include le seguenti informazioni, che mostrano che alla policy non è associata alcuna porta.

   ```
   {
       "LoadBalancerDescriptions": [
           {
               ...
               "BackendServerDescriptions": [],
               ...
           }
       ]
   }
   ```

Assegna un tag a Classic Load Balancer

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

Puoi aggiungere più tag a ciascun Classic Load Balancer. Le chiavi dei tag devono essere univoche per ogni load balancer. Se aggiungi un tag con una chiave già associata al load balancer, il valore del tag viene aggiornato.

Quando il tag non è più necessario, è possibile eliminarlo dal load balancer.

Indice

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- 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 UTF -8, più i seguenti 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.

Aggiungere un tag

Puoi aggiungere tag al load balancer in qualsiasi momento.

Per aggiungere un tag utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Tag scegliere Gestisci tag.
5. Nella pagina Gestisci i tag, per ogni tag scegli Aggiungi nuovo tag, quindi specifica una chiave e un valore.
6. Dopo aver terminato di aggiungere tag, scegli Salva modifiche.

Per aggiungere un tag utilizzando il AWS CLI

Utilizzare il comando add-tags seguente per aggiungere il tag specificato:

```
aws elb add-tags --load-balancer-name my-loadbalancer --tag "Key=project,Value=lima"
```

Rimuovi un tag

Quando non ne hai più bisogno, puoi rimuovere i tag dal tuo load balancer.

Per rimuovere un tag utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Tag scegliere Gestisci tag.
5. Nella pagina Gestisci i tag, scegli Rimuovi accanto a ogni tag che si desidera rimuovere.
6. Dopo aver completato la rimozione dei tag, scegli Salva modifiche.

Per rimuovere un tag utilizzando il AWS CLI

Utilizzare il comando remove-tags seguente per rimuovere il tag con la chiave specificata:

```
aws elb remove-tags --load-balancer-name my-loadbalancer --tag project
```

Configura le sottoreti per il tuo Classic Load Balancer

Quando aggiungi una sottorete al load balancer, Elastic Load Balancing crea un nodo del load balancer nella zona di disponibilità. I nodi del load balancer accettano traffico dai client e inoltrano le richieste alle istanze integre registrate in una o più zone di disponibilità. Si consiglia di aggiungere una sottorete per zona di disponibilità per almeno due zone di disponibilità. Questo consente di migliorare la disponibilità del load balancer. Ricorda che puoi modificare le sottoreti per il load balancer in qualsiasi momento.

Seleziona le sottoreti dalle stesse zona di disponibilità delle istanze. Se il load balancer in uso è connesso a Internet, occorre selezionare sottoreti pubbliche affinché le istanze di back-end ricevano il traffico dal load balancer (anche se le istanze di back-end si trovano in sottoreti private). Se il load balancer in uso è interno, ti consigliamo di selezionare sottoreti private. Per ulteriori informazioni relative alle sottoreti per il load balancer, consulta Raccomandazioni per il tuo VPC.

Per aggiungere una sottorete, registra le istanze nella zona di disponibilità con il sistema di bilanciamento del carico, quindi collega una sottorete da quella zona di disponibilità al sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Registra le istanze con il tuo Classic Load Balancer.

Dopo aver aggiunto una sottorete, il load balancer inizia a instradare le richieste verso le istanze registrate nella zona di disponibilità corrispondente. Per impostazione predefinita, il load balancer instrada le richieste in modo uniforme verso le zone di disponibilità per le sue sottoreti. Per instradare le richieste in modo uniforme verso le istanze registrate nelle zone di disponibilità per le sue sottoreti, abilita il bilanciamento del carico tra zone. Per ulteriori informazioni, consulta Configura il load balancer tra zone per il Classic Load Balancer.

Potrebbe essere necessario rimuovere una sottorete dal load balancer temporaneamente quando la sua zona di disponibilità non contiene istanze integre registrate o quando si desidera risolvere problemi relativi alle istanze registrate o aggiornare le istanze registrate. Dopo aver rimosso una sottorete, il load balancer interrompe il routing delle richieste alle istanze registrate nella sua zona di disponibilità, ma continua a instradare le richieste verso le istanze registrate nelle zone di disponibilità per le sottoreti rimanenti. Tieni presente che dopo aver rimosso una sottorete, le istanze in quella sottorete rimangono registrate con il sistema di bilanciamento del carico, ma puoi annullarne la registrazione se lo desideri. Per ulteriori informazioni, consulta Registra le istanze con il tuo Classic Load Balancer.

Indice

Requisiti

Quando si aggiornano le sottoreti per load balancer, occorre soddisfare i seguenti requisiti:

- Il load balancer devono disporre di almeno una sottorete in qualsiasi momento.
- È possibile aggiungere al massimo una sottorete per zona di disponibilità.
- Non è possibile aggiungere una sottorete di zona locale.

Poiché esistono sottoreti separate da APIs aggiungere e rimuovere da un sistema di bilanciamento del carico, è necessario considerare attentamente l'ordine delle operazioni quando si sostituiscono le sottoreti correnti con nuove sottoreti per soddisfare questi requisiti. Inoltre, occorre aggiungere temporaneamente una sottorete da un'altra zona di disponibilità se è necessario scambiare tutte le sottoreti nel load balancer. Ad esempio, se il load balancer dispone di una singola zona di disponibilità ed è necessario scambiare le sottoreti con un'altra sottorete, occorre innanzitutto aggiungere una sottorete da una seconda zona di disponibilità. Quindi puoi rimuovere la sottorete dalla zona di disponibilità originale (senza passare sotto una sottorete), aggiungere una nuova sottorete dalla zona di disponibilità originale (senza superare una sottorete per zona di disponibilità) e rimuovere la sottorete dalla seconda zona di disponibilità (se è necessaria solo per eseguire lo scambio).

Configura le sottoreti utilizzando la console

Utilizzare la procedura seguente per aggiungere o rimuovere sottoreti utilizzando la console.

Per configurare le sottoreti utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Mappatura di rete, scegli Modifica sottoreti.

5. Nella pagina Modifica sottoreti, nella sezione Mappatura della rete, aggiungi e rimuovi le sottoreti in base alle esigenze.
6. Al termine, scegliere Save changes (Salva le modifiche).

Configura le sottoreti utilizzando CLI

Utilizza gli esempi seguenti per aggiungere o rimuovere sottoreti utilizzando. AWS CLI

Per aggiungere una sottorete al sistema di bilanciamento del carico utilizzando il CLI

Usa il seguente comando attach-load-balancer-to-subnets per aggiungere due sottoreti al tuo sistema di bilanciamento del carico:

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --
subnets subnet-dea770a9 subnet-fb14f6a2
```

La risposta elenca tutte le sottoreti per il load balancer. Per esempio:

```
{
    "Subnets": [
        "subnet-5c11033e",
        "subnet-dea770a9",
        "subnet-fb14f6a2"
    ]
}
```

Per rimuovere una sottorete utilizzando AWS CLI

Utilizzate il seguente comando detach-load-balancer-from-subnets per rimuovere le sottoreti specificate dal sistema di bilanciamento del carico specificato:

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-loadbalancer --
subnets subnet-450f5127
```

La risposta elenca le sottoreti rimanenti per il load balancer. Per esempio:

```
{
    "Subnets": [
```

```
        "subnet-15aaab61"
    ]
}
```

Configurazione dei gruppi di sicurezza per Classic Load Balancer

Quando si utilizza il AWS Management Console per creare un sistema di bilanciamento del carico, è possibile scegliere un gruppo di sicurezza esistente o crearne uno nuovo. Se si sceglie un gruppo di sicurezza esistente, occorre consentire il traffico in entrambe le direzioni al listener e alle porte del controllo dello stato per il load balancer. Se si sceglie di creare un gruppo di sicurezza, la console aggiunge automaticamente le regole per consentire tutto il traffico su queste porte.

[Non predefinitoVPC] Se si utilizza AWS CLI o si API crea un sistema di bilanciamento del carico in un gruppo di sicurezza non predefinitoVPC, ma non si specifica un gruppo di sicurezza, il sistema di bilanciamento del carico viene automaticamente associato al gruppo di sicurezza predefinito per. VPC

[PredefinitoVPC] Se utilizzi AWS CLI o API per creare un sistema di bilanciamento del carico come impostazione predefinitaVPC, non puoi scegliere un gruppo di sicurezza esistente per il tuo sistema di bilanciamento del carico. In alternativa, Elastic Load Balancing fornisce un gruppo di sicurezza con regole per consentire tutto il traffico sulle porte specificate per il load balancer. Elastic Load Balancing crea un solo gruppo di sicurezza di questo tipo per AWS account, con un nome nel formato default_elb_*id* `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`(ad esempio,). VPCAnche i sistemi di bilanciamento del carico successivi creati in modo predefinito utilizzano questo gruppo di sicurezza. Assicurati di esaminare le regole del gruppo di sicurezza per verificare che consentano il traffico sulle porte del listener e del controllo dello stato per il nuovo load balancer. Quando elimini il load balancer, questo gruppo di sicurezza non viene eliminato automaticamente.

Se si aggiunge un listener a un load balancer esistente, occorre esaminare i gruppi di sicurezza per assicurarsi che consentano il traffico sulla nuova porta del listener in entrambe le direzioni.

Indice

Regole consigliate per gruppi di sicurezza di bilanciamento del carico

I gruppi di sicurezza per i bilanciatori del carico devono consentirne la comunicazione con le istanze. Le regole consigliate dipendono dal tipo di bilanciamento del carico, connesso a Internet o interno.

Sistema di bilanciamento del carico con connessione a Internet

La tabella seguente mostra le regole in entrata consigliate per un sistema di bilanciamento del carico connesso a Internet.

Crea	Protocollo	Intervallo porte	Commento
0.0.0.0/0	TCP	*listener*	Consente tutto il traffico in entrata sulla porta del listener del load balancer

La tabella seguente mostra le regole in uscita consigliate per un sistema di bilanciamento del carico connesso a Internet.

Destinazione	Protocollo	Intervallo porte	Commento
instance security group	TCP	*instance listener*	Consente il traffico in uscita verso le istanze sulla porta del listener dell'istanza
instance security group	TCP	*health check*	Permette il traffico in uscita verso le istanze attraverso la porta di controllo dello stato

bilanciatori del carico interni

La tabella seguente mostra le regole in entrata consigliate per un sistema di bilanciamento del carico interno.

Crea	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	*listener*	Consenti il traffico in entrata dalla porta listener VPC CIDR del load balancer

La tabella seguente mostra le regole in uscita consigliate per un sistema di bilanciamento del carico interno.

Destinazione	Protocollo	Intervallo porte	Commento
instance security group	TCP	*instance listener*	Consente il traffico in uscita verso le istanze sulla porta del listener dell'istanza
instance security group	TCP	*health check*	Permette il traffico in uscita verso le istanze attraverso la porta di controllo dello stato

Assegna gruppi di sicurezza utilizzando la console

Usa la seguente procedura per modificare i gruppi di sicurezza associati al tuo sistema di bilanciamento del carico.

Per aggiornare un gruppo di sicurezza assegnato al sistema di bilanciamento del carico utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Sicurezza, scegli Modifica.
5. Nella pagina Modifica gruppi di sicurezza, sotto Gruppi di sicurezza, aggiungi o rimuovi i gruppi di sicurezza in base alle esigenze.

   Puoi aggiungere fino a cinque gruppi di sicurezza.

6. Al termine, scegliere Save changes (Salva le modifiche).

Assegna i gruppi di sicurezza utilizzando il AWS CLI

Utilizzate il seguente comando apply-security-groups-to-load-balancer per associare un gruppo di sicurezza a un sistema di bilanciamento del carico. I gruppi di sicurezza specificati sovrascrivono i gruppi di sicurezza associati in precedenza.

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-loadbalancer --
security-groups sg-53fae93f
```

Di seguito è riportata una risposta di esempio:

```
{
  "SecurityGroups": [
     "sg-53fae93f"
  ]
}
```

Configura ACLs la rete per il tuo Classic Load Balancer

L'elenco di controllo degli accessi alla rete predefinito (ACL) per a VPC consente tutto il traffico in entrata e in uscita. Se si crea una rete personalizzataACLs, è necessario aggiungere regole che consentano la comunicazione tra il sistema di bilanciamento del carico e le istanze.

Le regole consigliate per la sottorete del sistema di bilanciamento del carico dipendono dal tipo di bilanciamento del carico, connesso a Internet o interno.

Sistema di bilanciamento del carico con connessione a Internet

Di seguito sono riportate le regole in entrata consigliate per un sistema di bilanciamento del carico connesso a Internet.

Crea	Protocollo	Intervallo porte	Commento
0.0.0.0/0	TCP	*listener*	Consente tutto il traffico in entrata sulla porta del listener del load balancer

Crea	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	1024-65535	Consenti il traffico in entrata da porte temporanee VPC CIDR

Di seguito sono riportate le regole in uscita consigliate per un sistema di bilanciamento del carico connesso a Internet.

Destinazione	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	*instance listener*	Consente tutto il traffico in uscita sulla porta del listener dell'istanza
VPC CIDR	TCP	*health check*	Consente tutto il traffico in uscita sulla porta di controllo dello stato
0.0.0.0/0	TCP	1024-65535	Consente tutto il traffico in uscita sulle porte temporanee

Sistema di bilanciamento del carico interno

Di seguito sono riportate le regole in entrata consigliate per un sistema di bilanciamento del carico interno.

Crea	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	*listener*	Consenti il traffico in entrata dalla porta listener del sistema VPC CIDR di bilanciamento del carico
VPC CIDR	TCP	1024-65535	Consenti il traffico in entrata dalle porte temporanee VPC CIDR

Di seguito sono riportate le regole in uscita consigliate per un sistema di bilanciamento del carico interno.

Destinazione	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	*instance listener*	Consenti il traffico in uscita verso la porta del listener VPC CIDR dell'istanza
VPC CIDR	TCP	*health check*	Consenti il traffico in uscita verso la porta di controllo dello VPC CIDR stato di salute
VPC CIDR	TCP	1024-65535	Consenti il traffico in uscita verso le VPC CIDR porte temporanee

Configura un nome di dominio personalizzato per il Classic Load Balancer

Ogni Classic Load Balancer riceve un nome Domain Name System (DNS) predefinito. Questo DNS nome include il nome della AWS regione in cui viene creato il load balancer. Ad esempio, se si crea un sistema di bilanciamento del carico denominato `my-loadbalancer` nella regione Stati Uniti occidentali (Oregon), il sistema di bilanciamento del carico riceve un DNS nome simile a. `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com` Per accedere al sito Web sulle tue istanze, incolla questo DNS nome nel campo degli indirizzi di un browser Web. Tuttavia, questo DNS nome non è facile da ricordare e utilizzare per i tuoi clienti.

Se preferisci utilizzare un DNS nome descrittivo per il tuo sistema di bilanciamento del carico, ad esempio`www.example.com`, anziché il DNS nome predefinito, puoi creare un nome di dominio personalizzato e associarlo al DNS nome del tuo sistema di bilanciamento del carico. Quando un client effettua una richiesta utilizzando questo nome di dominio personalizzato, il DNS server la risolve con il nome del sistema di bilanciamento del DNS carico.

Indice

Associazione del nome di dominio personalizzato al nome del bilanciamento del carico

Per prima cosa, se non lo hai ancora fatto, registra il tuo nome dominio. La Internet Corporation for Assigned Names and Numbers (ICANN) gestisce i nomi di dominio su Internet. Registrate un nome di dominio utilizzando un registrar di nomi di dominio, un'organizzazione ICANN accreditata che gestisce il registro dei nomi di dominio. Il sito Web per il tuo registrar fornirà istruzioni dettagliate e informazioni sui prezzi per la registrazione del tuo nome dominio. Per ulteriori informazioni, consulta le seguenti risorse:

- Per utilizzare Amazon Route 53 per registrare un nome di dominio, consulta Registrazione dei nomi di dominio utilizzando Route 53 nella Guida per gli sviluppatori di Amazon Route 53.
- Per un elenco dei registrar accreditati, consulta la directory dei registrar accreditati.

Successivamente, utilizza il tuo DNS servizio, ad esempio il registrar di domini, per creare un CNAME record per indirizzare le richieste al tuo sistema di bilanciamento del carico. Per ulteriori informazioni, consulta la documentazione del servizio. DNS

In alternativa, puoi utilizzare Route 53 come DNS servizio. Puoi creare una zona ospitata, che contiene informazioni su come eseguire il routing del traffico su Internet per il tuo dominio, e un set di record della risorsa alias, che esegue il routing delle query per il nome di dominio al bilanciamento del carico. Route 53 non addebita alcun costo per DNS le query per i set di record di alias e puoi utilizzare i set di record di alias per indirizzare DNS le query al tuo sistema di bilanciamento del carico per l'apice di zona del tuo dominio (ad esempio,). `example.com` Per informazioni sul trasferimento di DNS servizi per domini esistenti su Route 53, consulta Configuring Route 53 as your DNS service nella Amazon Route 53 Developer Guide.

Infine, crea una zona ospitata e un set di record di alias per il tuo dominio utilizzando Route 53. Per ulteriori informazioni, consulta Routing traffic to a load balancer (Routing del traffico a un load balancer) nella Guida per gli sviluppatori di Amazon Route 53.

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

Se utilizzi Route 53 per indirizzare DNS le query al sistema di bilanciamento del carico, puoi anche configurare il DNS failover per il sistema di bilanciamento del carico utilizzando Route 53. In una configurazione di failover, Route 53 verifica lo stato delle EC2 istanze registrate per il load balancer

per determinare se sono disponibili. Se non ci sono EC2 istanze integre registrate con il sistema di bilanciamento del carico o se il sistema di bilanciamento del carico stesso non è integro, Route 53 indirizza il traffico verso un'altra risorsa disponibile, ad esempio un sistema di bilanciamento del carico funzionante 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 il DNS failover, puoi specificare i bilanciatori del carico primari e secondari (di backup). Route 53 indirizza il traffico verso il bilanciamento del carico principale, se è disponibile, in caso contrario, al load balancer secondario.

Utilizzo della valutazione dello stato di destinazione

- Quando la valutazione dello stato di destinazione è impostata su `Yes` su un record alias di un Classic Load Balancer, Route 53 valuta lo stato della risorsa specificata dal valore `alias target`. Per un sistema Classic Load Balancer, Route 53 utilizza i controlli dell'integrità delle istanze associati al sistema di bilanciamento del carico.
- Quando almeno una delle istanze registrate in un Classic Load Balancer è integra, Route 53 contrassegna il record alias integro. Route 53 restituisce quindi i record in base alla policy di routing. Se viene utilizzata la policy di routing di failover, Route 53 restituisce il record principale.
- Quando tutte le istanze registrate per un Classic Load Balancer non sono integre, Route 53 contrassegna il record alias come non integro. Route 53 restituisce quindi i record in base alla policy di routing. Se viene utilizzata la policy di routing di failover, Route 53 restituisce il record secondario.

Per ulteriori informazioni, consulta la sezione Configurazione del DNS failover nella Amazon Route 53 Developer Guide.

Disassociazione del nome di dominio personalizzato dal bilanciamento del carico

Puoi annullare l'associazione del tuo nome di dominio personalizzato da un load balancer eliminando prima i set di record di risorse nella tua zona ospitata, quindi eliminando la zona ospitata. Per ulteriori informazioni, consulta Modifica di record e Eliminazione di una zona ospitata pubblica nella Guida per gli sviluppatori di Amazon Route 53.

Listener per il Classic Load Balancer

Prima di iniziare a utilizzare Elastic Load Balancing, è necessario configurare uno o più listener per il Classic Load Balancer. Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e una porta sia per connessioni front-end (dal client al load balancer) sia per connessioni back-end (dal load balancer all'istanza di back-end).

Elastic Load Balancing supporta i seguenti protocolli:

- HTTP
- HTTPS(sicuro) HTTP
- TCP
- SSL(sicuroTCP)

Il HTTPS protocollo utilizza il SSL protocollo per stabilire connessioni sicure su tutto il HTTP livello. È inoltre possibile utilizzare il SSL protocollo per stabilire connessioni sicure sul TCP livello.

Se la connessione front-end utilizza TCP oSSL, le connessioni back-end possono utilizzare uno dei due o. TCP SSL Se la connessione front-end utilizza HTTP oHTTPS, le connessioni back-end possono utilizzare uno o. HTTP HTTPS

Le istanze di back-end possono essere in ascolto sulle porte 1-65535.

I sistema di bilanciamento del carico possono essere in ascolto sulle seguenti porte: 1-65535

Indice

Protocolli

La comunicazione per una tipica applicazione Web avviene attraverso livelli di hardware e software. Ogni livello fornisce una funzione di comunicazione specifica. Il controllo sulla funzione

di comunicazione viene trasferito da un livello a quello successivo, in sequenza. Open System Interconnection (OSI) definisce un framework modello per l'implementazione di un formato standard per la comunicazione, chiamato protocollo, in questi livelli. Per ulteriori informazioni, consultate il OSImodello in Wikipedia.

Quando si utilizza Elastic Load Balancing, serve una comprensione di base del livello 4 e del livello 7. Il livello 4 è il livello di trasporto che descrive la connessione Transmission Control Protocol (TCP) tra il client e l'istanza di back-end, tramite il load balancer. Il livello 4 è il livello minimo configurabile per il load balancer. Il livello 7 è il livello applicativo che descrive l'uso delle connessioni Hypertext Transfer Protocol (HTTP) e delle connessioni HTTPS (sicureHTTP) dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico all'istanza di back-end.

Il protocollo Secure Sockets Layer (SSL) viene utilizzato principalmente per crittografare dati riservati su reti non sicure come Internet. Il SSL protocollo stabilisce una connessione sicura tra un client e il server di back-end e garantisce che tutti i dati trasmessi tra il client e il server siano privati e integrali.

TCP/SSLprotocollo

Quando si utilizza TCP (layer 4) per connessioni front-end e back-end, il sistema di bilanciamento del carico inoltra la richiesta alle istanze di back-end senza modificare gli header. Dopo aver ricevuto la richiesta, il load balancer tenta di aprire una TCP connessione all'istanza di back-end sulla porta specificata nella configurazione del listener.

Poiché i bilanciatori del carico intercettano il traffico tra i client e le tue istanze di back-end, i log di accesso per la tua istanza di back-end contengono l'indirizzo IP del load balancer invece del client di origine. È possibile abilitare il protocollo proxy, che aggiunge un'intestazione con le informazioni di connessione del client, ad esempio l'indirizzo IP di origine, l'indirizzo IP di destinazione e i numeri di porta. L'intestazione viene quindi inviata all'istanza di back-end come parte della richiesta. Puoi analizzare la prima riga nella richiesta per recuperare le informazioni di connessione. Per ulteriori informazioni, consulta Configura il protocollo proxy per il tuo Classic Load Balancer.

Utilizzando questa configurazione, non ricevi cookie per la persistenza della sessione o le intestazioni X-Forwarded.

HTTP/protocollo HTTPS

Quando si utilizza HTTP (layer 7) per connessioni front-end e back-end, il sistema di bilanciamento del carico analizza le intestazioni della richiesta prima di inviare la richiesta alle istanze di back-end.

Per ogni istanza registrata e integra di un sistema di bilanciamento HTTPS del caricoHTTP/, Elastic Load Balancing apre e mantiene una o TCP più connessioni. Queste connessioni assicurano che esista sempre una connessione stabilita pronta a ricevere HTTP HTTPS /richieste.

Le HTTP richieste e HTTP le risposte utilizzano i campi di intestazione per inviare informazioni sui HTTP messaggi. Elastic Load Balancing supporta le intestazioni `X-Forwarded-For`. Poiché i bilanciatori del carico intercettano il traffico tra client e server, i log di accesso al server contengono solo l'indirizzo IP del load balancer. Per visualizzare l'indirizzo IP del client, utilizza l'intestazione della richiesta `X-Forwarded-For`. Per ulteriori informazioni, consulta X-Forwarded-For.

Quando usiHTTP/HTTPS, puoi abilitare le sessioni permanenti sul tuo sistema di bilanciamento del carico. Una sticky session associa una sessione utente ad una determinata istanza di back-end. Questo garantisce che tutte le richieste provenienti dall'utente durante la sessione vengano inviate alla stessa istanza di back-end. Per ulteriori informazioni, consulta Configura le sticky session per il Classic Load Balancer.

Non tutte le HTTP estensioni sono supportate nel sistema di bilanciamento del carico. Potrebbe essere necessario utilizzare un TCP listener se il load balancer non è in grado di terminare la richiesta a causa di metodi imprevisti, codici di risposta o altre implementazioni 1.0/1.1 non standard. HTTP

HTTPS/ascoltatori SSL

È possibile creare un load balancer con le seguenti caratteristiche di sicurezza.

SSLcertificati del server

Se si utilizza HTTPS o SSL per le connessioni front-end, è necessario distribuire un certificato X.509 (certificato SSL server) sul sistema di bilanciamento del carico. Il load balancer decrittografa le richieste dei client prima di inviarle alle istanze di back-end (operazione nota come terminazione). SSL Per ulteriori informazioni, consulta SSL/TLScertificati per Classic Load Balancers.

Se non desideri che il sistema di bilanciamento del carico gestisca la SSL terminazione (operazione nota come SSLoffloading), puoi utilizzarla sia TCP per le connessioni front-end che per quelle back-end e distribuire certificati sulle istanze registrate che gestiscono le richieste.

SSLnegoziazione

Elastic Load Balancing fornisce configurazioni di SSL negoziazione predefinite che vengono utilizzate per la SSL negoziazione quando viene stabilita una connessione tra un client e il sistema

di bilanciamento del carico. Le configurazioni di SSL negoziazione garantiscono la compatibilità con un'ampia gamma di client e utilizzano algoritmi crittografici ad alta resistenza chiamati cifrari. Tuttavia, alcuni casi d'uso potrebbero richiedere la crittografia di tutti i dati sulla rete e consentire solo cifrari specifici. Alcuni standard di conformità alla sicurezza (ad esempio PCISOX, e così via) potrebbero richiedere ai client un set specifico di protocolli e cifrari per garantire il rispetto degli standard di sicurezza. In questi casi, è possibile creare una configurazione di SSL negoziazione personalizzata, in base a requisiti specifici. I tuoi cifrari e protocolli devono essere applicati entro 30 secondi. Per ulteriori informazioni, consulta SSLconfigurazioni di negoziazione per Classic Load Balancer.

Autenticazione server back-end

Se utilizzi HTTPS o SSL per le tue connessioni back-end, puoi abilitare l'autenticazione delle istanze registrate. Puoi quindi utilizzare il processo di autenticazione per assicurarti che le istanze accettino solo le comunicazioni crittografate e che ogni istanza registrata disponga della chiave pubblica corretta.

Per ulteriori informazioni, consulta Configurazione dell'autenticazione del server back-end.

Configurazioni del listener per i Classic Load Balancer

La tabella seguente descrive le possibili configurazioni HTTP e i HTTPS listener per un Classic Load Balancer.

Caso d'uso	Protocollo front-end	Opzioni di front-end	Protocollo back-end	Opzioni di back-end	Note
Load Balancer di base HTTP	HTTP	N/A	HTTP	N/A	• Supporta le intestazioni X-Forwarded
Proteggi il sito Web o l'applicazione utilizzando Elastic Load Balancing per ridurre	HTTPS	SSLnegoziazione	HTTP	N/A	• Supporta le intestazioni X-Forwarded • Richiede un SSLcertif

Caso d'uso	Protocollo front-end	Opzioni di front-end	Protocollo back-end	Opzioni di back-end	Note
il carico e la decrittografia SSL					icato distribuito sul load balancer
Sito Web o applicazione sicuri tramite crittografia end-to-end	HTTPS	SSLnegoziazione	HTTPS	Autenticazione di back-end	• Supporta le intestazioni X-Forwarded • Richiede SSLi certificati distribuiti sul sistema di bilanciamento del carico e sulle istanze registrate

La tabella seguente descrive le possibili configurazioni TCP e i SSL listener per un Classic Load Balancer.

Caso d'uso	Protocollo front-end	Opzioni di front-end	Protocollo back-end	Opzioni di back-end	Note
Load Balancer di base TCP	TCP	N/A	TCP	N/A	• Supporta l'intestazione del protocollo proxy

Caso d'uso	Protocollo front-end	Opzioni di front-end	Protocollo back-end	Opzioni di back-end	Note
Proteggi il sito Web o l'applicazione utilizzando Elastic Load Balancing per ridurre il carico e la decrittografia SSL	SSL	SSLnegoziazione	TCP	N/A	• Richiede un SSLcertificato distribuito sul load balancer • Supporta l'intestazione del protocollo proxy

Caso d'uso	Protocollo front-end	Opzioni di front-end	Protocollo back-end	Opzioni di back-end	Note
Sito Web o applicazione sicuri utilizzando end-to-end la crittografia con Elastic Load Balancing	SSL	SSLnegoziazione	SSL	Autenticazione di back-end	• Richiede SSLi certificati distribuiti sul sistema di bilanciamento del carico e sulle istanze registrate • Non inserisce SNI intestazioni nelle connessioni back-end SSL • Non supporta l'intestazione del protocollo proxy

HTTPheader e Classic Load Balancer

HTTPle richieste e HTTP le risposte utilizzano i campi di intestazione per inviare informazioni sui messaggi. HTTP I campi intestazione sono costituti da coppie nome-valore separati da due punti e intervallati da un ritorno a capo e un avanzamento riga. Un set standard di campi di HTTP

intestazione è definito in RFC 2616, Message Headers. Sono disponibili anche HTTP intestazioni non standard (e aggiunte automaticamente) che sono ampiamente utilizzate dalle applicazioni. Alcune HTTP intestazioni non standard hanno un prefisso. `X-Forwarded` I Classic Load Balancer supportano le seguenti intestazioni `X-Forwarded`.

Per ulteriori informazioni sulle HTTP connessioni, consulta Request routing nella Elastic Load Balancing User Guide.

Prerequisiti

- Verifica che le impostazioni del tuo listener supportino le intestazioni X-Forwarded. Per ulteriori informazioni, consulta Configurazioni del listener per i Classic Load Balancer.
- Configura il server Web per registrare gli indirizzi IP del client.

Intestazioni X-Forwarded

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

X-Forwarded-For

L'intestazione della `X-Forwarded-For` richiesta viene aggiunta automaticamente e consente di identificare l'indirizzo IP di un client quando si utilizza un sistema di bilanciamento del carico HTTP oHTTPS. Poiché i bilanciatori del carico intercettano il traffico tra client e server, i log di accesso al server contengono solo l'indirizzo IP del load balancer. Per visualizzare l'indirizzo IP del client, utilizza l'intestazione della richiesta `X-Forwarded-For`. Elastic Load Balancing 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, il bilanciamento del carico ne crea una con l'indirizzo IP del client come valore della richiesta. In caso contrario, il load balancer aggiunge l'indirizzo IP del client all'intestazione esistente e passa l'intestazione al server. L'intestazione della richiesta `X-Forwarded-For` può contenere più indirizzi IP separati da virgole. L'indirizzo più a sinistra è l'IP del client in cui è stata effettuata la richiesta per la prima volta. È quindi seguito da eventuali identificatori proxy successivi, in una catena.

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 IPv6 indirizzo di. `2001:DB8::21f:5bff:febf:ce22:8a2e`

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

X-Forwarded-Proto

L'intestazione della `X-Forwarded-Proto` richiesta consente di identificare il protocollo (HTTPoHTTPS) utilizzato da un client per connettersi al sistema di bilanciamento del carico. 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.

L'applicazione o il sito Web possono utilizzare il protocollo memorizzato nell'intestazione della `X-Forwarded-Proto` richiesta per fornire una risposta che reindirizza a quella appropriata. URL

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

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

L'esempio seguente contiene un'intestazione di `X-Forwarded-Proto` richiesta per una richiesta proveniente 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.

HTTPSascoltatori per il tuo Classic Load Balancer

È possibile creare un sistema di bilanciamento del carico che utilizzi il TLS protocolloSSL/per le connessioni crittografate (noto anche come SSL offload). Questa funzionalità consente la crittografia del traffico tra il sistema di bilanciamento del carico e i client che avviano HTTPS le sessioni e per le connessioni tra il sistema di bilanciamento del carico e le istanze. EC2

Elastic Load Balancing utilizza le configurazioni di negoziazione Secure Sockets Layer (SSL), note come politiche di sicurezza, per negoziare le connessioni tra i client e il sistema di bilanciamento del carico. Quando si utilizzaHTTPS/SSLper le connessioni front-end, è possibile utilizzare una politica di sicurezza predefinita o una politica di sicurezza personalizzata. È necessario distribuire un SSL certificato sul sistema di bilanciamento del carico. Il load balancer utilizza questo certificato per terminare la connessione e decrittografare le richieste provenienti dai client prima di inviarle alle istanze. Il load balancer utilizza una suite di crittografia statica per connessioni back-end. Facoltativamente, puoi scegliere di abilitare l'autenticazione sulle tue istanze.

I sistemi Classic Load Balancer non supportano l'indicazione del nome del server (). SNI Puoi utilizzare invece una delle seguenti alternative:

- Implementate un certificato sul sistema di bilanciamento del carico e aggiungete un Subject Alternative Name (SAN) per ogni sito Web aggiuntivo. SANsconsentono di proteggere più nomi host utilizzando un unico certificato. Rivolgiti al tuo fornitore di certificati per ulteriori informazioni sul numero di SANs certificati supportati per certificato e su come aggiungere e rimuovereSANs.
- Usa i TCP listener sulla porta 443 per le connessioni front-end e back-end. Il load balancer trasmette la richiesta così com'è, quindi puoi gestire la terminazione sull'istanza. HTTPS EC2

I Load Balancer classici non supportano l'TLSautenticazione reciproca (m). TLS Per il mio TLS supporto, crea un TCP listener. Il load balancer passa la richiesta così com'è, quindi puoi implementare m TLS sull'EC2istanza.

Indice

- Configura un HTTPS listener per il tuo Classic Load Balancer
- Sostituisci il SSL certificato per il tuo Classic Load Balancer
- Aggiorna la configurazione di SSL negoziazione del tuo Classic Load Balancer

SSL/TLScertificati per Classic Load Balancers

Se utilizzi HTTPS (SSLorTLS) per il tuo listener front-end, devi distribuire un TLS certificatoSSL/ sul tuo sistema di bilanciamento del carico. Il load balancer utilizza il certificato per terminare la connessione e decrittografare le richieste provenienti dai client prima di inviarle alle istanze.

I TLS protocolli SSL and utilizzano un certificato X.509 (SSL/TLSserver certificate) per autenticare sia il client che l'applicazione back-end. Un certificato X.509 è una forma di identificazione digitale rilasciata da un'autorità di certificazione (CA) e contiene informazioni di identificazione, un periodo di validità, una chiave pubblica, un numero di serie e la firma digitale dell'emittente.

È possibile creare un certificato utilizzando AWS Certificate Manager o uno strumento che supporti i TLS protocolli SSL and, come Open. SSL Specificherai questo certificato quando creerai o aggiornerai un HTTPS listener per il tuo sistema di bilanciamento del carico. Quando si crea un certificato da utilizzare con il load balancer, occorre specificare un nome di dominio.

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. Se non corrispondono, il traffico non verrà crittografato poiché la TLS connessione non può essere verificata.

È necessario specificare un nome di dominio completo (FQDN) per il certificato, ad esempio `www.example.com` o un nome di dominio apex come`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 apparirà nel campo Oggetto e nell'estensione Nome oggetto alternativo del certificato. Per ulteriori informazioni sui certificati pubblici, consulta Richiesta di un certificato pubblico nella Guida per l'utente di AWS Certificate Manager .

Crea o importa un TLS certificatoSSL/utilizzando AWS Certificate Manager

Ti consigliamo di utilizzare AWS Certificate Manager (ACM) per creare o importare certificati per il tuo sistema di bilanciamento del carico. ACMsi integra con Elastic Load Balancing in modo da poter distribuire il certificato sul sistema di bilanciamento del carico. Per implementare un certificato sul load balancer, esso deve trovarsi nella stessa regione del load balancer. Per ulteriori informazioni, consulta Richiesta di un certificato pubblico o Importazione di certificati nella Guida per l'utente di AWS Certificate Manager .

Per consentire a un utente di distribuire il certificato sul sistema di bilanciamento del carico utilizzando il AWS Management Console, è necessario consentire l'accesso all'azione. ACM `ListCertificates` API Per ulteriori informazioni, consulta Elenco dei certificati nella Guida per l'utente di AWS Certificate Manager .

> **Important**
>
> Non è possibile installare certificati con chiavi a 4096 bit o RSA chiavi EC sul sistema di bilanciamento del carico tramite l'integrazione con. ACM È necessario caricare certificati con chiavi a 4096 bit o RSA chiavi EC per IAM poterli utilizzare con il sistema di bilanciamento del carico.

Importa un certificato/utilizzando SSL TLS IAM

Se non lo utilizziACM, puoi usareSSL/TLStools, come OpenSSL, per creare una richiesta di firma del certificato (CSR), farla CSR firmare da una CA per produrre un certificato e caricarlo suIAM. Per ulteriori informazioni, consulta Lavorare con i certificati del server nella Guida IAM per l'utente.

SSLconfigurazioni di negoziazione per Classic Load Balancer

Elastic Load Balancing utilizza una configurazione di negoziazione Secure Socket Layer (SSL), nota come policy di sicurezza, per negoziare SSL le connessioni tra un client e il load balancer. Una policy di sicurezza è una combinazione di SSL protocolli, SSL cifrari e l'opzione Server Order Preference. Per ulteriori informazioni sulla configurazione di una SSL connessione per il sistema di bilanciamento del carico, consulta. Listener per il Classic Load Balancer

Indice

- SSLprotocolli
- Preferenza ordine server
- SSLcifrari

Policy di sicurezza

Una politica di sicurezza determina quali cifrari e protocolli sono supportati durante le SSL negoziazioni tra un client e un sistema di bilanciamento del carico. Puoi configurare i Classic Load Balancer per utilizzare policy predefinite o policy di sicurezza personalizzate.

Nota che un certificato fornito da AWS Certificate Manager (ACM) contiene una RSA chiave pubblica. Pertanto, è necessario includere una suite di crittografia che utilizzi RSA nella politica di sicurezza se si utilizza un certificato fornito daACM; in caso contrario, la TLS connessione fallisce.

Policy di sicurezza predefinite

I nomi delle policy di sicurezza predefinite più recenti includono informazioni sulla versione in base all'anno e al mese in cui sono state rilasciate. Ad esempio, la policy di sicurezza predefinita di default è `ELBSecurityPolicy-2016-08`. Ogni volta che una nuova policy di sicurezza predefinita viene rilasciata, puoi aggiornare la configurazione per utilizzarla.

Per informazioni sui protocolli e le crittografie abilitate per le policy di sicurezza predefinite, consulta Politiche di sicurezza predefinite SSL per Classic Load Balancers.

Policy di sicurezza personalizzate

Puoi creare una configurazione di negoziazione personalizzata con le crittografie e i protocolli che ti servono. Ad esempio, alcuni standard di conformità alla sicurezza (come PCI eSOC) potrebbero richiedere un set specifico di protocolli e codici per garantire il rispetto degli standard di sicurezza. In questi casi, puoi creare una policy di sicurezza personalizzata per soddisfare tali standard.

Per informazioni sulla creazione di una policy di sicurezza personalizzata, consulta Aggiorna la configurazione di SSL negoziazione del tuo Classic Load Balancer.

SSLprotocolli

Il SSLprotocollo stabilisce una connessione sicura tra un client e un server e garantisce che tutti i dati trasmessi tra il client e il sistema di bilanciamento del carico siano privati.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono protocolli crittografici utilizzati per crittografare dati riservati su reti non sicure come Internet. Il TLS protocollo è una versione più recente del protocollo. SSL Nella documentazione di Elastic Load Balancing, facciamo riferimento a entrambi SSL i TLS protocolli come protocollo. SSL

Protocollo consigliato

Consigliamo il TLS 1.2, che viene utilizzato nella politica di sicurezza predefinita ELBSecurityPolicy - TLS -1-2-2017-01. È inoltre possibile utilizzare TLS 1.2 nelle politiche di sicurezza personalizzate. La politica di sicurezza predefinita supporta sia la TLS 1.2 che le versioni precedenti diTLS, quindi è meno sicura di ELBSecurityPolicy - TLS -1-2-2017-01.

Protocollo obsoleto

Se in precedenza hai abilitato il protocollo SSL 2.0 in una politica personalizzata, ti consigliamo di aggiornare la politica di sicurezza con una delle politiche di sicurezza predefinite.

Preferenza ordine server

Elastic Load Balancing supporta l'opzione Preferenza ordine server per la negoziazione delle connessioni tra un client e un load balancer. Durante il processo di negoziazione della SSL connessione, il client e il sistema di bilanciamento del carico presentano un elenco di cifrari e protocolli supportati ciascuno, in ordine di preferenza. Per impostazione predefinita, per la connessione viene selezionata la prima cifra dell'elenco del client che corrisponde a uno qualsiasi dei codici del sistema di bilanciamento del carico. SSL Se il load balancer è configurato per supportare l'opzione Preferenza ordine server, seleziona la prima crittografia nel suo elenco che si trova nell'elenco di crittografie del client. Ciò garantisce che il load balancer determini quale cifrario viene utilizzato per la connessione. SSL Se l'opzione Preferenza ordine server non è abilitata, l'ordine delle cifrature presentate dal client viene utilizzato per negoziare le connessioni tra il client e il load balancer.

SSLcifrari

Un SSLcodice è un algoritmo di crittografia che utilizza chiavi di crittografia per creare un messaggio in codice. SSLi protocolli utilizzano diversi codici SSL per crittografare i dati su Internet.

Nota che un certificato fornito da AWS Certificate Manager (ACM) contiene una RSA chiave pubblica. Pertanto, è necessario includere una suite di crittografia che utilizzi RSA nella politica di sicurezza se si utilizza un certificato fornito daACM; in caso contrario, la TLS connessione fallisce.

Elastic Load Balancing supporta le seguenti crittografie da utilizzare con Classic Load Balancer. Un sottoinsieme di questi codici viene utilizzato dalle politiche predefinite. SSL Tutte queste crittografie sono disponibili per l'utilizzo in un criterio personalizzato. Ti consigliamo di utilizzare solo le crittografie incluse nella policy di sicurezza di default (quelle con un asterisco). Molte altre crittografie non sono sicure e il loro utilizzo è a proprio rischio.

Crittografie

- ECDHE-ECDSA-AES128-GCM-SHA256 *
- ECDHE-RSA-AES128-GCM-SHA256 *
- ECDHE-ECDSA-AES128-SHA256 *
- ECDHE-RSA-AES128-SHA256 *
- ECDHE-ECDSA-AES128-SHA *
- ECDHE-RSA-AES128-SHA *
- DHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384 *
- ECDHE-RSA-AES256-GCM-SHA384 *
- ECDHE-ECDSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA *
- ECDHE-ECDSA-AES256-SHA *
- AES128-GCM-SHA256 *
- AES128-SHA256 *
- AES128-SHA *
- AES256-GCM-SHA384 *
- AES256-SHA256 *
- AES256-SHA *
- DHE-DSS-AES128-SHA
- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- ECDHE-RSA-RC4-SHA

- RC4-SHA
- ECDHE-ECDSA-RC4-SHA
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA256-SHA
- CAMELLIA256-SHA
- EDH-DSS-DES-CBC3-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA128-SHA
- ADH-AES128-GCM-SHA256
- ADH-AES128-SHA
- ADH-AES128-SHA256
- ADH-AES256-GCM-SHA384
- ADH-AES256-SHA
- ADH-AES256-SHA256
- ADH-CAMELLIA128-SHA
- ADH-CAMELLIA256-SHA
- ADH-DES-CBC3-SHA
- ADH-DES-CBC-SHA
- ADH-RC4-MD5
- ADH-SEED-SHA

- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- IDEA-CBC-SHA
- RC4-MD5
- SEED-SHA
- DES-CBC3-MD5
- DES-CBC-MD5
- RC2-CBC-MD5
- PSK-AES256-CBC-SHA
- PSK-3 - - - DES EDE CBC SHA
- KRB5-DES-CBC3-SHA
- KRB5-DES-CBC3-MD5
- PSK-AES128-CBC-SHA
- PSK-RC4-SHA
- KRB5-RC4-SHA
- KRB5-RC4-MD5
- KRB5-DES-CBC-SHA
- KRB5-DES-CBC-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-ADH-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-KRB5-RC2-CBC-SHA
- EXP-KRB5-DES-CBC-SHA
- EXP-KRB5-RC2-CBC-MD5
- EXP-KRB5-DES-CBC-MD5

- EXP-ADH-RC4-MD5
- EXP-RC4-MD5
- EXP-KRB5-RC4-SHA
- EXP-KRB5-RC4-MD5

* Questi sono i codici inclusi nella politica di sicurezza predefinita, ELBSecurityPolicy -2016-08.

Politiche di sicurezza predefinite SSL per Classic Load Balancers

Puoi scegliere una delle politiche di sicurezza predefinite per i tuoi HTTPS /listener. SSL È possibile utilizzare una delle `ELBSecurityPolicy-TLS` politiche per soddisfare gli standard di conformità e sicurezza che richiedono la disabilitazione di determinate TLS versioni del protocollo. In alternativa, puoi creare una policy di sicurezza personalizzata. Per ulteriori informazioni, consulta Aggiorna la configurazione di negoziazione SSL.

I RSA codici - e DSA basati su sono specifici dell'algoritmo di firma utilizzato per creare il certificato. SSL Assicurati di creare un SSL certificato utilizzando l'algoritmo di firma basato sui codici abilitati per la tua politica di sicurezza.

Se selezioni una policy abilitata per Preferenza ordine server, il load balancer utilizza le crittografie nell'ordine in cui sono specificate qui per negoziare le connessioni tra il client e il load balancer. In caso contrario, il load balancer usa le crittografie nell'ordine in cui sono presentate dal client.

Le sezioni seguenti descrivono le politiche di sicurezza predefinite più recenti per i Classic Load Balancer, inclusi i protocolli e i codici abilitati. SSL SSL È inoltre possibile descrivere le politiche predefinite utilizzando il comando. describe-load-balancer-policies

> **Tip**
>
> Queste informazioni si applicano solo ai Classic Load Balancer. Per informazioni relative ad altri sistemi di bilanciamento del carico, consulta Policy di sicurezza per l'Application Load Balancer e Policy di sicurezza per il Network Load Balancer.

Indice

- Politiche per cifratura

Protocolli per policy

La tabella seguente descrive i TLS protocolli supportati da ciascuna politica di sicurezza.

Policy di sicurezza	TLS1.2	TLS1.1	TLS 1.0
ELBSecurityPolicy- TLS -1-2-2017-01	Sì	No	No
ELBSecurityPolicy- TLS -1-1-2017-01	Sì	Sì	No
ELBSecurityPolicy-2016-08	Sì	Sì	Sì
ELBSecurityPolicy-2015-05	Sì	Sì	Sì
ELBSecurityPolicy-2015-03	Sì	Sì	Sì
ELBSecurityPolicy-2015-02	Sì	Sì	Sì

Cifre per politica

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

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

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

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

Policy di sicurezza	Crittografie
ELBSecurityPolicy-2015-05	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DES-CBC3-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolicy-2015-03	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA-AES128-SHA • DHE-DSS-AES128-SHA • DES-CBC3-SHA

Policy di sicurezza	Crittografie
ELBSecurityPolicy-2015-02	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA • DHE-RSA-AES128-SHA • DHE-DSS-AES128-SHA

Politiche per cifratura

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

Nome del cifrario	Policy di sicurezza	Suite di cifratura
Aperto SSL — ECDHE-ECDSA-AES 128- - GCM SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01	c02b

Nome del cifrario	Policy di sicurezza	Suite di cifratura
IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES GCM _128_ _ SHA256	• ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	
Aperto SSL — ECDHE-RSA-AES 128- - GCM SHA256 IANA— TLS _ _ ECDHE _ RSA WITH _ AES GCM _128_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c 02f
Aperto SSL — 128 - ECDHE-ECDSA-AES SHA256 IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES CBC _128_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c023
Aperto SSL — 128 - ECDHE-RSA-AES SHA256 IANA— TLS _ _ ECDHE _ RSA WITH _ AES CBC _128_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c027

Nome del cifrario	Policy di sicurezza	Suite di cifratura
Aperto SSL — 128 - ECDHE-ECDSA-AES SHA IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES CBC _128_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c009
Aperto SSL — 128 - ECDHE-RSA-AES SHA IANA— TLS _ _ ECDHE _ RSA WITH _ AES CBC _128_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c013
Aperto SSL — ECDHE-ECDSA-AES 256- - GCM SHA384 IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES GCM _256_ _ SHA384	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	-c 02c
Aperto SSL — ECDHE-RSA-AES 256- - GCM SHA384 IANA— TLS _ _ ECDHE _ RSA WITH _ AES GCM _256_ _ SHA384	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c030

Nome del cifrario	Policy di sicurezza	Suite di cifratura
Aperto SSL — 256 - ECDHE-ECDSA-AES SHA384 IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES CBC _256_ _ SHA384	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c024
Aperto SSL — 256 - ECDHE-RSA-AES SHA384 IANA— TLS _ _ ECDHE _ RSA WITH _ AES CBC _256_ _ SHA384	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c028
Aperto SSL — 256 - ECDHE-ECDSA-AES SHA IANA— TLS _ _ ECDHE _ RSA WITH _ AES CBC _256_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c014
Aperto SSL — 256 - ECDHE-RSA-AES SHA IANA— TLS _ _ ECDHE _ ECDSA WITH _ AES CBC _256_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	c00a

Nome del cifrario	Policy di sicurezza	Suite di cifratura
Aperto SSL — - - AES128 GCM SHA256 IANA— TLS _ _ RSA WITH _ AES GCM _128_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	9c
Aperto SSL — - AES128 SHA256 IANA— TLS _ _ RSA WITH _ AES CBC _128_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	3c
Aperto SSL — - AES128 SHA IANA— TLS _ _ RSA WITH _ AES CBC _128_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	2f
Aperto SSL — AES256 - - GCM SHA384 IANA— TLS _ _ RSA WITH _ AES GCM _256_ _ SHA384	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	9d

Nome del cifrario	Policy di sicurezza	Suite di cifratura
Aperto SSL — - AES256 SHA256 IANA— TLS _ _ RSA WITH _ AES CBC _256_ _ SHA256	• ELBSecurityPolicy- -1-2-2017-01 TLS • ELBSecurityPolicy- TLS -1-1-2017-01 • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	3d
Apri SSL — AES256 - SHA IANA— TLS _ _ RSA WITH _ AES CBC _256_ _ SHA	• ELBSecurityPolicy- -1-1-2017-01 TLS • ELBSecurityPolicy-2016-08 • ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	35
Aperto — 128- SSL DHE-RSA-AES SHA IANA— TLS _ _ DHE _ RSA WITH _ AES CBC _128_ _ SHA	• ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	33
Aperto — 128- SSL DHE-DSS-AES SHA IANA— TLS _ _ DHE _ DSS WITH _ AES CBC _128_ _ SHA	• ELBSecurityPolicy-2015-03 • ELBSecurityPolicy-2015-02	32
Aperto — - - SSL DES CBC3 SHA IANA— TLS _ RSA _ WITH _3 DES _ EDE _ CBC SHA	• ELBSecurityPolicy-2015-05 • ELBSecurityPolicy-2015-03	0a

Crea un Classic Load Balancer con un listener HTTPS

Un sistema di bilanciamento del carico riceve le richieste dei client e le distribuisce tra le EC2 istanze registrate con il sistema di bilanciamento del carico.

È possibile creare un sistema di bilanciamento del carico che ascolti su entrambe le porte HTTP (80) e (443). HTTPS Se si specifica che il HTTPS listener invia le richieste alle istanze sulla porta 80, il sistema di bilanciamento del carico termina le richieste e la comunicazione dal sistema di bilanciamento del carico alle istanze non viene crittografata. Se il HTTPS listener invia richieste alle istanze sulla porta 443, la comunicazione dal load balancer alle istanze viene crittografata.

Se il load balancer utilizza una connessione crittografata per comunicare con le istanze, puoi anche opzionalmente abilitare l'autenticazione delle istanze. Questo garantisce che il load balancer comunica con un'istanza solo se la sua chiave pubblica corrisponde alla chiave specificata per il load balancer per questo scopo.

Per informazioni sull'aggiunta di un HTTPS listener a un sistema di bilanciamento del carico esistente, consulta. Configura un HTTPS listener per il tuo Classic Load Balancer

Indice

Prerequisiti

Prima di iniziare, assicurati che i seguenti prerequisiti siano soddisfatti:

- Completa le fasi descritte in Raccomandazioni per il tuo VPC.
- Avvia le EC2 istanze che intendi registrare con il tuo sistema di bilanciamento del carico. I gruppi di sicurezza per queste istanze devono consentire il traffico dal load balancer.
- Le EC2 istanze devono rispondere all'obiettivo del controllo di integrità con un codice di HTTP stato 200. Per ulteriori informazioni, consulta Controlli dello stato delle istanze del tuo Classic Load Balancer.
- Se prevedi di abilitare l'opzione keep-alive sulle tue EC2 istanze, ti consigliamo di impostare le impostazioni keep-alive almeno sulle impostazioni di timeout di inattività del tuo sistema di

bilanciamento del carico. Se desideri garantire che il load balancer sia responsabile della chiusura delle connessioni all'istanza, assicurati che il valore impostato sull'istanza per il tempo di keep-alive sia superiore all'impostazione del timeout di inattività sul load balancer. Per ulteriori informazioni, consulta Configura il timeout per connessione inattiva per il Classic Load Balancer.

- Se crei un listener sicuro, devi distribuire un certificato server sul tuo sistema di bilanciamento del carico. SSL Il load balancer utilizza il certificato per terminare e quindi decrittografare le richieste prima di inviarle alle istanze. Se non disponi di un SSL certificato, puoi crearne uno. Per ulteriori informazioni, consulta SSL/TLScertificati per Classic Load Balancers.

Crea un sistema HTTPS di bilanciamento del carico utilizzando la console

In questo esempio, vengono configurati due listener per il load balancer. Il primo listener accetta HTTP le richieste sulla porta 80 e le invia alle istanze sulla porta 80 utilizzando. HTTP Il secondo listener accetta HTTPS le richieste sulla porta 443 e le invia alle istanze utilizzando la porta 80 (o utilizzando HTTP la porta 443 se si desidera configurare l'HTTPSautenticazione dell'istanza di back-end).

Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e una porta sia per connessioni front-end (dal client al load balancer) sia per connessioni back-end (dal load balancer all'istanza). Per informazioni sulle configurazioni di porte, protocolli e listener supportati da Elastic Load Balancing, consulta Listener per il Classic Load Balancer.

Per creare il tuo Classic Load Balancer sicuro 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 selezionare la stessa regione che hai selezionato per le tue EC2 istanze.
3. Nel pannello di navigazione, sotto Load Balancing (Bilanciamento del carico), scegli Load Balancers (Load balancer).
4. Seleziona Create Load Balancer (Crea load balancer).
5. Espandi la sezione Classic Load Balancer, quindi scegli Crea.
6. Configurazione di base

    a. In Nome del sistema di bilanciamento del carico, immetti un nome per il sistema di bilanciamento del carico.

Il nome del Classic Load Balancer deve essere univoco nel set di Classic Load Balancer della regione, può essere composto da un massimo di 32 caratteri, può contenere solo caratteri alfanumerici e trattini e non deve iniziare o finire con un trattino.

b. In Schema, seleziona Con connessione Internet.

7. Mappatura della rete

   a. Per VPC, seleziona la stessa VPC che hai selezionato per le tue istanze.

   b. In Mappature, seleziona innanzitutto una zona di disponibilità, quindi scegli una sottorete pubblica tra quelle disponibili. Puoi selezionare solo una sottorete per ogni zona di disponibilità. Per migliorare la disponibilità del sistema di bilanciamento del carico, seleziona più zone di disponibilità e sottoreti.

8. Gruppi di sicurezza

   - Per i gruppi di sicurezza, seleziona un gruppo di sicurezza esistente configurato per consentire il HTTP traffico richiesto sulla porta 80 e il HTTPS traffico sulla porta 443.

     Se non è presente, puoi creare un nuovo gruppo di sicurezza con le regole necessarie.

9. Ascoltatori e instradamento

   a. Lascia l'ascoltatore predefinito con le impostazioni di default e seleziona Aggiungi listener.

   b. In Listener sul nuovo ascoltatore, seleziona `HTTPS` come protocollo e la porta verrà aggiornata a `443`. Per impostazione predefinita, Istanza utilizza il protocollo `HTTP` sulla porta `80`.

   c. Se è necessaria l'autenticazione back-end, modifica il protocollo dell'istanza su `HTTPS`. In questo modo, anche la porta dell'istanza viene aggiornata in `443`.

10. Impostazioni listener sicuro

    Quando utilizzi HTTPS o SSL per il tuo listener front-end, devi distribuire un SSL certificato sul tuo sistema di bilanciamento del carico. Il load balancer utilizza il certificato per terminare la connessione e decrittografare le richieste provenienti dai client prima di inviarle alle istanze. Inoltre, occorre specificare una policy di sicurezza. Elastic Load Balancing fornisce policy di sicurezza con configurazioni di SSL negoziazione predefinite, oppure puoi creare policy di sicurezza personalizzate. Se hai configuratoHTTPS/SSLsulla connessione back-end, puoi abilitare l'autenticazione delle tue istanze.

a. Per quanto riguarda la politica di sicurezza, ti consigliamo di utilizzare sempre la politica di sicurezza predefinita più recente o di creare una politica personalizzata. Vedi Aggiornamento della configurazione di SSL negoziazione.

b. Per DefaultSSL/TLScertificate, 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 utilizzandoIAM, seleziona Da IAM, quindi seleziona il certificato da Seleziona un certificato.
- Se hai un certificato da importare ma non ACM è disponibile nella tua regione, seleziona Importa, quindi seleziona IAM A. 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 (PEMcon codifica). Nel Corpo del certificato, copia e incolla il contenuto del file del certificato a chiave pubblica (PEM-encoded). In Certificate Chain, copia e incolla il contenuto del file della catena del certificato (PEM-encoded), a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.

c. (Facoltativo) Se hai configurato il HTTPS listener per comunicare con le istanze utilizzando una connessione crittografata, puoi facoltativamente impostare l'autenticazione delle istanze nel certificato di autenticazione Backend.

> **Note**
>
> Se non vedi la sezione Certificato di autenticazione di back-end, torna a Listener e routing e seleziona HTTPS come protocollo per Istanza.

i. Per Certificate name (Nome certificato), digita il nome del certificato a chiave pubblica.

ii. Per Certificate Body (PEMcodificato), copia e incolla il contenuto del certificato. Il load balancer comunica con un'istanza solo se la sua chiave pubblica corrisponde a questa chiave.

iii. Per aggiungere un altro certificato, scegli Aggiungi nuovo certificato di back-end. Il limite è cinque.

11. Controlli dell'integrità

a. Nella sezione Ping della destinazione, seleziona un Protocollo Ping e una Porta Ping. Le EC2 istanze devono accettare il traffico sulla porta ping specificata.

b. In Porta Ping, assicurati che la porta sia `80`.

c. In Percorso ping, sostituisci il valore predefinito con una barra singola (`/`). In questo modo Elastic Load Balancing invierà le richieste di controllo dell'integrità alla home page predefinita del server web, ad esempio `index.html`.

d. In Impostazioni avanzate del controllo dell'integrità, utilizza i valori predefiniti.

12. Istanze

a. Seleziona Aggiungi istanze per visualizzare la schermata di selezione delle istanze.

b. In Istanze disponibili puoi selezionare le istanze attualmente disponibili per il sistema di bilanciamento del carico, in base alle impostazioni di rete selezionate in precedenza.

c. Dopo aver effettuato le selezioni, scegli Conferma per aggiungere le istanze da registrare al sistema di bilanciamento del carico.

13. Attributes

- Mantieni i valori predefiniti per Abilita il sistema di bilanciamento del carico tra zone, Abilita svuotamento della connessione e Timeout (intervallo di svuotamento).

14. Tag del sistema di bilanciamento del carico (facoltativo)

a. Il campo Chiave è obbligatorio.

b. Il campo Valore è facoltativo.

c. Per aggiungere un altro tag, seleziona Aggiungi nuovo tag, quindi inserisci i valori nel campo Chiave e facoltativamente nel campo Valore.

d. Per rimuovere un tag esistente, seleziona Rimuovi accanto al tag da rimuovere.

15. Riepilogo e creazione

a. Se hai bisogno di modificare le impostazioni, seleziona Modifica accanto all'impostazione da cambiare.

b. Dopo aver verificato le impostazioni mostrate nel riepilogo, seleziona Crea sistema di bilanciamento del carico per iniziare a creare il sistema di bilanciamento del carico.

c. Nella pagina di creazione finale, seleziona Visualizza sistema di bilanciamento del carico per visualizzare il sistema di bilanciamento del carico nella console AmazonEC2.

16. Verify

a. Seleziona il nuovo load balancer.

b. Nella scheda Istanze di destinazione, verifica la colonna Stato di integrità. Dopo che almeno una delle tue EC2 istanze è in servizio, puoi testare il tuo sistema di bilanciamento del carico.

c. Nella sezione Dettagli, copia il DNSnome del sistema di bilanciamento del carico, che sarà simile a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`

d. Incolla il DNSnome del sistema di bilanciamento del carico nel campo dell'indirizzo di un browser web pubblico connesso a Internet. Se il sistema di bilanciamento del carico funziona correttamente, verrà visualizzata la pagina predefinita del server.

17. Rimozione (facoltativa)

a. Se hai un CNAME record per il tuo dominio che punta al sistema di bilanciamento del carico, indirizzalo verso una nuova posizione e attendi che la DNS modifica abbia effetto prima di eliminare il sistema di bilanciamento del carico.

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

c. Selezionare il load balancer.

d. Seleziona Operazioni, Elimina sistema di bilanciamento del carico.

e. Quando viene richiesta la conferma, digita `confirm`, quindi scegli Elimina.

f. Dopo aver eliminato un sistema di bilanciamento del carico, le EC2 istanze registrate con il sistema di bilanciamento del carico continuano a funzionare. Verranno addebitate le spese per ogni ora parziale o intera in cui continuano a funzionare. Quando non hai più bisogno di un'EC2istanza, puoi interromperla o chiuderla per evitare di incorrere in costi aggiuntivi.

Crea un sistema di HTTPS bilanciamento del carico utilizzando il AWS CLI

Utilizza le seguenti istruzioni per creare un sistema di SSL bilanciamento del caricoHTTPS/ utilizzando. AWS CLI

Attività

- Fase 1: configurare i listener
- Fase 2: Configurare la politica SSL di sicurezza
- Fase 3: configurare l'autenticazione dell'istanza di back-end (facoltativo)
- Fase 4: configurare i controlli dell'integrità (facoltativo)

- Fase 5: EC2 Registrare le istanze
- Fase 6: verificare le istanze
- Fase 7: eliminare il load balancer (facoltativo)

Fase 1: configurare i listener

Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e una porta per connessioni front-end (dal client al load balancer) e connessioni back-end (dal load balancer all'istanza). Per informazioni sulle configurazioni di porte, protocolli e listener supportati da Elastic Load Balancing, consulta Listener per il Classic Load Balancer.

In questo esempio, puoi configurare due listener per il load balancer specificando le porte e i protocolli da usare per le connessioni front-end e back-end. Il primo listener accetta HTTP le richieste sulla porta 80 e le invia alle istanze sulla porta 80 utilizzando. HTTP Il secondo listener accetta HTTPS le richieste sulla porta 443 e invia le richieste alle istanze utilizzando la porta 80. HTTP

Poiché il secondo listener lo utilizza HTTPS per la connessione front-end, è necessario distribuire un SSL certificato server sul sistema di bilanciamento del carico. Il load balancer utilizza il certificato per terminare e quindi decrittografare le richieste prima di inviarle alle istanze.

Per configurare i listener per il load balancer

1. Ottieni l'Amazon Resource Name (ARN) del SSL certificato. Per esempio:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Usa il seguente create-load-balancercomando per configurare il load balancer con i due listener:

   ```
   aws elb create-load-balancer --load-balancer-name my-load-balancer --listeners
    "Protocol=http,LoadBalancerPort=80,InstanceProtocol=http,InstancePort=80"
    "Protocol=https,LoadBalancerPort=443,InstanceProtocol=http,InstancePort=80,SSLCertificateI
    --availability-zones us-west-2a
   ```

Di seguito è riportata una risposta di esempio:

```
{
  "DNSName": "my-loadbalancer-012345678.us-west-2.elb.amazonaws.com"
}
```

3. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per visualizzare i dettagli del sistema di bilanciamento del carico:

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

Fase 2: Configurare la politica SSL di sicurezza

Puoi selezionare una delle policy di sicurezza predefinite oppure creare la tua policy di sicurezza personalizzata. In caso contrario, Elastic Load Balancing configura il load balancer con la policy di sicurezza predefinita `ELBSecurityPolicy-2016-08`. Per ulteriori informazioni, consulta SSLconfigurazioni di negoziazione per Classic Load Balancer.

Per verificare che il load balancer sia associato alla policy di sicurezza di default

Utilizzando il seguente comando describe-load-balancers:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Di seguito è riportata una risposta di esempio. Ricorda che `ELBSecurityPolicy-2016-08` è associato a load balancer sulla porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
```

```
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Se preferisci, puoi configurare la politica di SSL sicurezza per il tuo sistema di bilanciamento del carico anziché utilizzare la politica di sicurezza predefinita.

(Facoltativo) per utilizzare una politica di sicurezza predefinita SSL

1. Utilizzate il describe-load-balancer-policiescomando seguente per elencare i nomi delle politiche di sicurezza predefinite:

   ```
   aws elb describe-load-balancer-policies
   ```

   Per informazioni sula configurazione delle policy di sicurezza predefinite, consulta Politiche di sicurezza predefinite SSL per Classic Load Balancers.

2. Utilizzate il create-load-balancer-policycomando seguente per creare una politica di SSL negoziazione utilizzando una delle politiche di sicurezza predefinite descritte nel passaggio precedente:

   ```
   aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
   --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
   --policy-attributes AttributeName=Reference-Security-
   Policy,AttributeValue=predefined-policy
   ```

3. (Facoltativo) Utilizzate il describe-load-balancer-policiescomando seguente per verificare che la politica sia stata creata:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La risposta include la descrizione della policy.

4. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la policy sulla porta 443 di load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Il comando `set-load-balancer-policies-of-listener` sostituisce l'insieme di policy corrente per la porta del load balancer con l'insieme di policy specificato. L'elenco `--policy-names` deve includere tutte le policy da abilitare. Se si omette una policy attualmente abilitata, questa viene disabilitata.

5. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che la policy sia abilitata:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Di seguito è riportato un esempio di risposta che mostra che la policy è abilitata sulla porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
```

```
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Quando si crea una policy di sicurezza personalizzata, occorre abilitare almeno un protocollo e una crittografia. I DSA codici e RSA sono specifici dell'algoritmo di firma e vengono utilizzati per creare il SSL certificato. Se disponi già del SSL certificato, assicurati di abilitare il codice utilizzato per creare il certificato. Il nome della policy personalizzata non deve iniziare con `ELBSecurityPolicy-` o `ELBSample-`, poiché questi prefissi sono prenotati per i nomi delle policy di sicurezza predefinite.

(Facoltativo) per utilizzare una politica di sicurezza personalizzata SSL

1. Utilizzare il create-load-balancer-policycomando per creare una politica di SSL negoziazione utilizzando una politica di sicurezza personalizzata. Per esempio:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name
 SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

2. (Facoltativo) Utilizzate il seguente describe-load-balancer-policiescomando per verificare che la politica sia stata creata:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La risposta include la descrizione della policy.

3. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la policy sulla porta 443 di load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Il comando `set-load-balancer-policies-of-listener` sostituisce l'insieme di policy corrente per la porta del load balancer con l'insieme di policy specificato. L'elenco `--policy-names` deve includere tutte le policy da abilitare. Se si omette una policy attualmente abilitata, questa viene disabilitata.

4. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che la policy sia abilitata:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Di seguito è riportato un esempio di risposta che mostra che la policy è abilitata sulla porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
```

```
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Fase 3: configurare l'autenticazione dell'istanza di back-end (facoltativo)

Se configuriHTTPS/SSLsulla connessione back-end, puoi facoltativamente configurare l'autenticazione delle tue istanze.

Durante l'autenticazione dell'istanza di back-end crei una policy per la chiave pubblica. Quindi, utilizza questa policy per la chiave pubblica per creare una policy per l'autenticazione dell'istanza di back-end. Infine, imposti la politica di autenticazione dell'istanza di back-end con la porta dell'istanza per il protocollo. HTTPS

Il load balancer comunica con un'istanza solo se la chiave pubblica presentata dall'istanza al load balancer corrisponde a una chiave pubblica nella policy di autenticazione per il load balancer.

Per configurare l'autenticazione dell'istanza di back-end

1. Utilizzare il comando seguente per recuperare la chiave pubblica:

   ```
   openssl x509 -in your X509 certificate PublicKey -pubkey -noout
   ```

2. Utilizzate il seguente create-load-balancer-policycomando per creare una politica a chiave pubblica:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-PublicKey-policy \
--policy-type-name PublicKeyPolicyType --policy-attributes
 AttributeName=PublicKey,AttributeValue=MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
```

> **Note**
>
> Per specificare un valore della chiave pubblica per `--policy-attributes`, rimuovere la prima e l'ultima riga della chiave pubblica (la riga contenente"`-----BEGIN PUBLIC KEY-----`"e la riga contenente"`-----END PUBLIC KEY-----`"). AWS CLI Non accetta spazi bianchi in`--policy-attributes`.

3. Utilizzare il create-load-balancer-policycomando seguente per creare una politica di autenticazione dell'istanza di back-end utilizzando. `my-PublicKey-policy`

```
aws elb create-load-balancer-policy --load-balancer-name my-
loadbalancer --policy-name my-authentication-policy --policy-type-
name BackendServerAuthenticationPolicyType --policy-attributes
 AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-policy
```

Opzionalmente, è possibile utilizzare più criteri della chiave pubblica. Il load balancer prova tutte le chiavi, una alla volta. Se la chiave pubblica presentata da un'istanza corrisponde a una di queste chiavi pubbliche, l'istanza viene autenticata.

4. Utilizzate il seguente for-backend-server comando set-load-balancer-policies- per impostare la `my-authentication-policy` porta dell'istanza per. HTTPS In questo esempio, la porta dell'istanza è 443.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 443 --policy-names my-authentication-policy
```

5. (Facoltativo) Utilizzate il seguente describe-load-balancer-policiescomando per elencare tutte le politiche per il sistema di bilanciamento del carico:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer
```

6. (Facoltativo) Utilizzate il seguente describe-load-balancer-policiescomando per visualizzare i dettagli della politica:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-names my-authentication-policy
```

Fase 4: configurare i controlli dell'integrità (facoltativo)

Elastic Load Balancing controlla regolarmente lo stato di ogni EC2 istanza registrata in base ai controlli di integrità configurati. Se Elastic Load Balancing trova un'istanza non integra, interrompe l'invio del traffico all'istanza e indirizza il traffico verso le istanze integre. Per ulteriori informazioni, consulta Controlli dello stato delle istanze del tuo Classic Load Balancer.

Quando crei il load balancer, Elastic Load Balancing utilizza le impostazioni predefinite per i controlli dell'integrità. Se preferisci, puoi modificare la configurazione del controllo dello stato per il load balancer anziché utilizzare le impostazioni di default.

Per configurare i controlli dello stato per le istanze

Utilizzando il seguente comando configure-health-check:

```
aws elb configure-health-check --load-balancer-name my-loadbalancer --health-check
 Target=HTTP:80/ping,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Di seguito è riportata una risposta di esempio:

```
{
```

```
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/ping",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    }
}
```

Fase 5: EC2 Registrare le istanze

Dopo aver creato il sistema di bilanciamento del carico, è necessario registrare EC2 le istanze con il sistema di bilanciamento del carico. È possibile selezionare EC2 istanze da una singola zona di disponibilità o da più zone di disponibilità all'interno della stessa regione del sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Istanze registrate per Classic Load Balancer.

Utilizzate il comando register-instances-with-load-balancer come segue:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

Di seguito è riportata una risposta di esempio:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

Fase 6: verificare le istanze

Il load balancer è utilizzabile non appena una qualsiasi delle istanze registrate si trova nello stato `InService`.

Per verificare lo stato delle nuove EC2 istanze registrate, utilizzate il seguente comando: describe-instance-health

```
aws elb describe-instance-health  --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Di seguito è riportata una risposta di esempio:

```
{
    "InstanceStates": [
        {
            "InstanceId": "i-4f8cf126",
            "ReasonCode": "N/A",
            "State": "InService",
            "Description": "N/A"
        },
        {
            "InstanceId": "i-0bb7ca62",
            "ReasonCode": "Instance",
            "State": "OutOfService",
            "Description": "Instance registration is still in progress"
        }
    ]
}
```

Se il campo `State` di un'istanza è `OutOfService`, è probabile che le istanze siano ancora in corso di registrazione. Per ulteriori informazioni, consulta Risoluzione dei problemi di un Classic Load Balancer: registrazione dell'istanza.

Quando lo stato di almeno delle istanze è `InService`, puoi testare il load balancer. Per testare il sistema di bilanciamento del carico, copia il DNS nome del sistema di bilanciamento del carico e incollalo nel campo dell'indirizzo di un browser Web connesso a Internet. Se il sistema di bilanciamento del carico funziona, viene visualizzata la pagina predefinita del server. HTTP

Fase 7: eliminare il load balancer (facoltativo)

L'eliminazione di un sistema di bilanciamento del carico annulla automaticamente la registrazione delle istanze associate. EC2 Non appena il load balancer viene eliminato, i relativi addebiti vengono bloccati. Tuttavia, le EC2 istanze continuano a funzionare e tu continui a incorrere in addebiti.

Per eliminare il sistema di bilanciamento del carico, utilizza il seguente comando: delete-load-balancer

```
aws elb delete-load-balancer --load-balancer-name my-loadbalancer
```

Per interrompere le EC2 istanze, usa il comando stop-instances. Per terminare le istanze, usa il comando EC2 terminate-instances.

Configura un HTTPS listener per il tuo Classic Load Balancer

Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e una porta sia per connessioni front-end (dal client al load balancer) sia per connessioni back-end (dal load balancer all'istanza). Per informazioni sulle configurazioni di porte, protocolli e listener supportati da Elastic Load Balancing, consulta Listener per il Classic Load Balancer.

Se disponi di un sistema di bilanciamento del carico con un listener che accetta HTTP richieste sulla porta 80, puoi aggiungere un listener che accetta HTTPS richieste sulla porta 443. Se si specifica che il HTTPS listener invia richieste alle istanze sulla porta 80, il sistema di bilanciamento del carico termina le SSL richieste e la comunicazione dal sistema di bilanciamento del carico alle istanze non viene crittografata. Se il HTTPS listener invia richieste alle istanze sulla porta 443, la comunicazione dal load balancer alle istanze viene crittografata.

Se il load balancer utilizza una connessione crittografata per comunicare con le istanze, puoi opzionalmente abilitare l'autenticazione delle istanze. Questo garantisce che il load balancer comunica con un'istanza solo se la sua chiave pubblica corrisponde alla chiave specificata per il load balancer per questo scopo.

Per informazioni sulla creazione di un nuovo listener, consulta. HTTPS Crea un Classic Load Balancer con un listener HTTPS

Indice

Prerequisiti

Per abilitare HTTPS il supporto per un HTTPS listener, è necessario distribuire un certificato del SSL server sul sistema di bilanciamento del carico. Il load balancer utilizza il certificato per terminare e quindi decrittografare le richieste prima di inviarle alle istanze. Se non disponi di un SSL certificato, puoi crearne uno. Per ulteriori informazioni, consulta SSL/TLScertificati per Classic Load Balancers.

Aggiungi un HTTPS ascoltatore utilizzando la console

È possibile aggiungere un HTTPS listener a un sistema di bilanciamento del carico esistente.

Per aggiungere un HTTPS listener al sistema di bilanciamento del carico utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Gestisci ascoltatori.
5. Nella scheda Gestisci ascoltatori, all'interno della sezione Listener, scegli Aggiungi listener.
6. Per il protocollo Listener, seleziona HTTPS.

   > **Important**
   >
   > Per impostazione predefinita, il protocollo Instance èHTTP. Se desideri configurare l'autenticazione dell'istanza di back-end, modifica il protocollo di istanza in. HTTPS

7. Per la politica di sicurezza, ti consigliamo di utilizzare la politica di sicurezza predefinita più recente. Se è necessario utilizzare una politica di sicurezza predefinita diversa o creare una politica personalizzata, vedere Aggiornamento della configurazione di SSL negoziazione.
8. Per SSLCertificato predefinito, scegliete Modifica, quindi effettuate una delle seguenti operazioni:

   - Se avete creato o importato un certificato utilizzando AWS Certificate Manager, scegliete Da ACM, selezionate il certificato dall'elenco, quindi scegliete Salva modifiche.

     > **Note**
     >
     > Questa opzione è disponibile solo nelle regioni che supportano AWS Certificate Manager.

   - Se hai importato un certificato utilizzando IAMIAM, scegli Da, seleziona il certificato dall'elenco, quindi scegli Salva modifiche.
   - Se hai un SSL certificato in cui importareACM, seleziona Importa e To ACM. In Chiave privata del certificato, copia e incolla il contenuto del file PEM di chiave privata con codifica. In Certificate body, copia e incolla il contenuto del file di certificato a chiave pubblica PEM -

encoded. In Certificate chain, facoltativo, copia e incolla il contenuto del file PEM -encoded certificate chain, a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.

- Se hai un SSL certificato da importare ma non ACM è supportato in questa regione, seleziona Importa e To. IAM In Nome del certificato, digita il nome del certificato. In Chiave privata del certificato, copia e incolla il contenuto del file PEM di chiave privata con codifica. In Certificate body, copia e incolla il contenuto del file di certificato a chiave pubblica PEM -encoded. In Certificate chain, facoltativo, copia e incolla il contenuto del file PEM -encoded certificate chain, a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.
- Scegli Save changes (Salva modifiche).

9. Per Viscosità dei cookie, l'impostazione predefinita è Disabilitato. Per cambiarlo, scegli Modifica. Se scegli l'opzione Generato dal sistema di bilanciamento del carico, devi specificare un Periodo di scadenza. Se scegli l'opzione Generato dall'applicazione, devi specificare un Nome cookie. Dopo aver effettuato la selezione, scegli Salva modifiche.
10. (Facoltativo) Scegli Aggiungi listener per aggiungere ulteriori ascoltatori.
11. Scegli Salva modifiche per aggiungere gli ascoltatori appena configurati.
12. (Facoltativo) Per configurare l'autenticazione dell'istanza di back-end per un sistema di bilanciamento del carico esistente, è necessario utilizzare AWS CLI o unAPI, poiché questa attività non è supportata dall'utilizzo della console. Per ulteriori informazioni, consulta Configurazione dell'autenticazione dell'istanza di back-end.

Aggiungete un listener utilizzando HTTPS il AWS CLI

È possibile aggiungere un HTTPS listener a un sistema di bilanciamento del carico esistente.

Per aggiungere un HTTPS listener al sistema di bilanciamento del carico, utilizzare il AWS CLI

1. Ottieni l'Amazon Resource Name (ARN) del SSL certificato. Per esempio:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

```
arn:aws:iam::123456789012:server-certificate/my-server-certificate
```

2. Usa il seguente create-load-balancer-listenerscomando per aggiungere un listener al tuo sistema di bilanciamento del carico che accetti HTTPS le richieste sulla porta 443 e le invii alle istanze sulla porta 80 utilizzando: HTTP

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
listeners
 Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80,SSLCertificateId
```

Se desideri configurare l'autenticazione dell'istanza di back-end, usa il seguente comando per aggiungere un listener che accetti le HTTPS richieste sulla porta 443 e invii le richieste alle istanze sulla porta 443 utilizzando: HTTPS

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
listeners
 Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTPS,InstancePort=443,SSLCertificate
```

3. (Facoltativo) È possibile utilizzare il seguente describe-load-balancerscomando per visualizzare i dettagli aggiornati del sistema di bilanciamento del carico:

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
```

```
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

4. (Facoltativo) Il HTTPS listener è stato creato utilizzando la politica di sicurezza predefinita. Se desideri specificare una politica di sicurezza predefinita diversa o una politica di sicurezza personalizzata, usa i comandi create-load-balancer-policye set-load-balancer-policies-of-listener. Per ulteriori informazioni, consulta Aggiornare la configurazione di negoziazione utilizzando il SSL AWS CLI.
5. (Facoltativo) Per configurare l'autenticazione dell'istanza di back-end, utilizzate il comando -. set-load-balancer-policies for-backend-server Per ulteriori informazioni, consulta Configurazione dell'autenticazione dell'istanza di back-end.

Sostituisci il SSL certificato per il tuo Classic Load Balancer

Se disponi di un HTTPS listener, hai distribuito un certificato SSL server sul tuo sistema di bilanciamento del carico al momento della creazione del listener. Ogni certificato include un periodo di validità. Devi assicurarti di rinnovare o sostituire il certificato prima della fine del suo periodo di validità.

I certificati forniti AWS Certificate Manager e distribuiti sul sistema di bilanciamento del carico possono essere rinnovati automaticamente. ACMtenta 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 inACM, devi monitorare la data di scadenza del certificato e rinnovarlo prima che scada. Per ulteriori informazioni, consulta Importazione di certificati nella Guida

per l'utente di AWS Certificate Manager . Dopo che un certificato che è stato distribuito su un load balancer viene rinnovato, le nuove richieste utilizzano il certificato rinnovato.

Per sostituire un certificato, occorre innanzitutto creare un nuovo certificato seguendo la stessa procedura utilizzata per creare il certificato corrente. Quindi, puoi sostituire il certificato. Dopo che un certificato che è stato distribuito su un load balancer viene sostituito, le nuove richieste utilizzano il nuovo certificato.

Nota che il rinnovo o la sostituzione di un certificato non influenza le richieste che erano già state ricevute da un nodo del load balancer e che sono in attesa di essere instradate verso una destinazione integra.

Indice

Sostituisci il SSL certificato utilizzando la console

Puoi sostituire il certificato distribuito sul tuo sistema di bilanciamento del carico con un certificato fornito da ACM o caricato su. IAM

Per sostituire il SSL certificato per un sistema di HTTPS bilanciamento del carico utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Gestisci ascoltatori.
5. Nella pagina Gestisci i listener, individua il listener da aggiornare, scegli Modifica in SSLCertificato predefinito ed esegui una delle seguenti operazioni:
    - Se avete creato o importato un certificato utilizzando AWS Certificate Manager, scegliete Da ACM, selezionate il certificato dall'elenco, quindi scegliete Salva modifiche.

> **Note**
>
> Questa opzione è disponibile solo nelle regioni che supportano AWS Certificate Manager.

- Se hai importato un certificato utilizzando IAMIAM, scegli Da, seleziona il certificato dall'elenco, quindi scegli Salva modifiche.
- Se hai un SSL certificato in cui importareACM, seleziona Importa e To ACM. In Chiave privata del certificato, copia e incolla il contenuto del file PEM di chiave privata con codifica. In Certificate body, copia e incolla il contenuto del file di certificato a chiave pubblica PEM -encoded. In Certificate chain, facoltativo, copia e incolla il contenuto del file PEM -encoded certificate chain, a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.
- Se hai un SSL certificato da importare ma non ACM è supportato in questa regione, seleziona Importa e To. IAM In Nome del certificato, digita il nome del certificato. In Chiave privata del certificato, copia e incolla il contenuto del file PEM di chiave privata con codifica. In Certificate body, copia e incolla il contenuto del file di certificato a chiave pubblica PEM -encoded. In Certificate chain, facoltativo, copia e incolla il contenuto del file PEM -encoded certificate chain, a meno che non stiate utilizzando un certificato autofirmato e non sia importante che i browser accettino implicitamente il certificato.
- Scegli Save changes (Salva modifiche).

Sostituisci il certificato usando il SSL AWS CLI

Puoi sostituire il certificato distribuito sul tuo sistema di bilanciamento del carico con un certificato fornito da ACM o caricato su. IAM

Per sostituire un SSL certificato con un certificato fornito da ACM

1. Utilizzare il comando request-certificate seguente per richiedere un nuovo certificato:

```
aws acm request-certificate --domain-name www.example.com
```

2. Usa il seguente comando set-load-balancer-listener-ssl-certificate per impostare il certificato:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Per sostituire un SSL certificato con un certificato caricato su IAM

1. Se disponi di un SSL certificato ma non lo hai caricato, consulta Caricamento di un certificato server nella Guida per l'IAMutente.
2. Usa il seguente get-server-certificatecomando per ottenere ARN il certificato:

```
aws iam get-server-certificate --server-certificate-name my-new-certificate
```

3. Usa il seguente comando set-load-balancer-listener-ssl-certificate per impostare il certificato:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:iam::123456789012:server-certificate/my-new-certificate
```

Aggiorna la configurazione di SSL negoziazione del tuo Classic Load Balancer

Elastic Load Balancing fornisce policy di sicurezza con configurazioni di SSL negoziazione predefinite da utilizzare per negoziare le SSL connessioni tra i client e il sistema di bilanciamento del carico. Se utilizzi il SSL protocolloHTTPS/per il tuo listener, puoi utilizzare una delle politiche di sicurezza predefinite o utilizzare una politica di sicurezza personalizzata.

Per ulteriori informazioni sulle policy di sicurezza, consulta SSLconfigurazioni di negoziazione per Classic Load Balancer. Per informazioni sulle configurazioni delle policy di sicurezza fornite da Elastic Load Balancing, consulta Politiche di sicurezza predefinite SSL per Classic Load Balancers.

Se crei un SSL listenerHTTPS/senza associare una policy di sicurezza, Elastic Load Balancing associa la policy di sicurezza predefinita predefinita al tuo load balancer`ELBSecurityPolicy-2016-08`.

Se preferisci, puoi creare una configurazione personalizzata. Ti consigliamo vivamente di testare la tua politica di sicurezza prima di aggiornare la configurazione del load balancer.

Gli esempi seguenti mostrano come aggiornare la configurazione di SSL negoziazione per un HTTPS SSL /listener. Nota che la modifica non influenza le richieste che erano state ricevute da un nodo del load balancer e che sono in attesa del routing a un'istanza integra, ma la configurazione aggiornata verrà utilizzata con le nuove richieste ricevute.

Indice

Aggiornate la configurazione di SSL negoziazione utilizzando la console

Per impostazione predefinita, Elastic Load Balancing associa le policy predefinite più recenti al tuo load balancer. Quando una nuova policy predefinita viene aggiunta, è consigliabile aggiornare il load balancer in modo che utilizzi la nuova policy predefinita. In alternativa, puoi selezionare un'altra policy di sicurezza predefinita oppure creare una policy personalizzata.

Per aggiornare la configurazione di SSL negoziazione per un sistema di bilanciamento SSL del caricoHTTPS/utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Listener, scegli Gestisci ascoltatori.
5. Nella pagina Gestisci ascoltatori, individua l'ascoltatore da aggiornare, scegli Modifica in Policy di sicurezza e seleziona una policy di sicurezza utilizzando una delle seguenti opzioni:
   - Mantieni la politica predefinita, ELBSecurityPolicy-2016-08, quindi scegli Salva modifiche.
   - Seleziona una policy predefinita diversa da quella di default, quindi scegli Salva modifiche.
   - Seleziona Personalizzato e abilita almeno un protocollo e una crittografia come segue:
     a. Per SSLProtocolli, seleziona uno o più protocolli da abilitare.
     b. Per SSLOpzioni, seleziona Preferenza ordine server per utilizzare l'ordine elencato nella sezione Politiche di sicurezza predefinite SSL per Classic Load Balancers per la SSL negoziazione.

c. Per SSLCifre, seleziona uno o più codici da abilitare. Se disponi già di un SSL certificato, devi abilitare il codice utilizzato per creare il certificato, poiché DSA i codici sono RSA specifici dell'algoritmo di firma.

d. Scegli Save changes (Salva modifiche).

Aggiornare la configurazione di negoziazione utilizzando il SSL AWS CLI

Puoi utilizzare la policy di sicurezza predefinita di default, `ELBSecurityPolicy-2016-08`, una policy di sicurezza predefinita diversa oppure una policy di sicurezza personalizzata.

Per utilizzare una politica di sicurezza predefinita SSL

1. Usa il describe-load-balancer-policiescomando seguente per elencare le politiche di sicurezza predefinite fornite da Elastic Load Balancing. La sintassi utilizzata dipende dal sistema operativo e dalla shell in uso.

   Linux

   ```
   aws elb describe-load-balancer-policies --query 'PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}' --output table
   ```

   Windows

   ```
   aws elb describe-load-balancer-policies --query "PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}" --output table
   ```

   Di seguito è riportato un output di esempio:

   ```
   ----------------------------------------
   |      DescribeLoadBalancerPolicies      |
   +----------------------------------------+
   |               PolicyName               |
   +----------------------------------------+
   |  ELBSecurityPolicy-2016-08             |
   |  ELBSecurityPolicy-TLS-1-2-2017-01     |
   |  ELBSecurityPolicy-TLS-1-1-2017-01     |
   |  ELBSecurityPolicy-2015-05             |
   |  ELBSecurityPolicy-2015-03             |
   |  ELBSecurityPolicy-2015-02             |
   ```

```
|  ELBSecurityPolicy-2014-10             |
|  ELBSecurityPolicy-2014-01             |
|  ELBSecurityPolicy-2011-08             |
|  ELBSample-ELBDefaultCipherPolicy      |
|  ELBSample-OpenSSLDefaultCipherPolicy  |
+----------------------------------------+
```

Per determinare quali crittografie sono abilitate per una policy, utilizzare il comando seguente:

```
aws elb describe-load-balancer-policies --policy-names ELBSecurityPolicy-2016-08 --
output table
```

Per informazioni sula configurazione delle policy di sicurezza predefinite, consulta Politiche di sicurezza predefinite SSL per Classic Load Balancers.

2. Utilizzate il create-load-balancer-policycomando per creare una politica di SSL negoziazione utilizzando una delle politiche di sicurezza predefinite descritte nel passaggio precedente. Ad esempio, il comando seguente utilizza la policy di sicurezza predefinita di default:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy  --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=ELBSecurityPolicy-2016-08
```

Se superi il limite del numero di policy per il load balancer, usa il delete-load-balancer-policycomando per eliminare tutte le politiche non utilizzate.

3. (Facoltativo) Utilizzate il seguente describe-load-balancer-policiescomando per verificare che la policy sia stata creata:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La risposta include la descrizione della policy.

4. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la policy sulla porta 443 di load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> Il comando `set-load-balancer-policies-of-listener` sostituisce l'insieme di policy corrente per la porta del load balancer specificata con l'insieme di policy specificato. L'elenco `--policy-names` deve includere tutte le policy da abilitare. Se si omette una policy attualmente abilitata, questa viene disabilitata.

5. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che la nuova policy sia abilitata per la porta di bilanciamento del carico:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La risposta mostra che la policy è abilitata sulla porta 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Quando si crea una policy di sicurezza personalizzata, occorre abilitare almeno un protocollo e una crittografia. I DSA codici e RSA sono specifici dell'algoritmo di firma e vengono utilizzati per creare il certificato. SSL Se disponi già di un SSL certificato, assicurati di abilitare il codice utilizzato per creare il certificato. Il nome della policy personalizzata non deve iniziare con `ELBSecurityPolicy-` o `ELBSample-`, poiché questi prefissi sono prenotati per i nomi delle policy di sicurezza predefinite.

Per utilizzare una politica di sicurezza personalizzata SSL

1. Utilizzare il create-load-balancer-policycomando per creare una politica di SSL negoziazione utilizzando una politica di sicurezza personalizzata. Per esempio:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name
 SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

   Se superi il limite del numero di policy per il load balancer, usa il delete-load-balancer-policycomando per eliminare tutte le politiche non utilizzate.

2. (Facoltativo) Utilizzate il seguente describe-load-balancer-policiescomando per verificare che la policy sia stata creata:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

   La risposta include la descrizione della policy.

3. Utilizzate il seguente comando set-load-balancer-policies-of-listener per abilitare la policy sulla porta 443 di load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

   > **Note**
   >
   > Il comando `set-load-balancer-policies-of-listener` sostituisce l'insieme di policy corrente per la porta del load balancer specificata con l'insieme di policy specificato. L'elenco `--policy-names` deve includere tutte le policy da abilitare. Se si omette una policy attualmente abilitata, questa viene disabilitata.

4. (Facoltativo) Utilizzate il seguente describe-load-balancerscomando per verificare che la nuova policy sia abilitata per la porta di bilanciamento del carico:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La risposta mostra che la policy è abilitata sulla porta 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Istanze registrate per Classic Load Balancer

Dopo aver creato il Classic Load Balancer, è necessario registrare le EC2 istanze con il sistema di bilanciamento del carico. Puoi selezionare EC2 istanze da una singola zona di disponibilità o da più zone di disponibilità all'interno della stessa regione del sistema di bilanciamento del carico. Elastic Load Balancing esegue regolarmente controlli di integrità sulle EC2 istanze registrate e distribuisce automaticamente le richieste in entrata al DNS nome del sistema di bilanciamento del carico tra le istanze registrate e integre. EC2

Indice

Best practice per le istanze

- Occorre assicurarsi che il load balancer sia in grado di comunicare con le istanze sulla porta del listener e sulla porta di controllo dello stato. Per ulteriori informazioni, consulta Configurazione dei gruppi di sicurezza per Classic Load Balancer. Il gruppo di sicurezza per le istanze devono consentire il traffico in entrambe le direzioni su entrambe le porte per ogni sottorete per il load balancer.
- Installa un server web, come Apache o Internet Information Services (IIS), su tutte le istanze che intendi registrare con il tuo sistema di bilanciamento del carico.
- Per HTTP HTTPS gli ascoltatori, consigliamo di abilitare l'opzione keep-alive nelle EC2 istanze, che consente al sistema di bilanciamento del carico di riutilizzare le connessioni alle istanze per più richieste client. Ciò consente di ridurre il carico sul server Web e migliorare il throughput del load balancer. Il timeout keep-alive deve essere di almeno 60 secondi per garantire che il load balancer sia responsabile della chiusura della connessione a un'istanza.
- Elastic Load Balancing supporta Path Maximum Transmission Unit (MTU) Discovery. Per garantire che Path MTU Discovery funzioni correttamente, è necessario assicurarsi che il gruppo di

sicurezza dell'istanza consenta la ICMP frammentazione dei messaggi richiesti (tipo 3, codice 4). Per ulteriori informazioni, consulta Path MTU Discovery nella Amazon EC2 User Guide.

Raccomandazioni per il tuo VPC

Cloud privato virtuale (VPC)

A meno che tu non ne abbia creato uno Account AWS prima del 2014, hai un valore predefinito VPC in ogni regione. Puoi utilizzare un'impostazione predefinita VPC per il tuo sistema di bilanciamento del carico, se ne hai uno, oppure puoi crearne uno nuovoVPC. Per ulteriori informazioni, consulta la Amazon VPC User Guide.

Sottoreti per il sistema di bilanciamento del carico

Per assicurarti che il sistema di bilanciamento del carico sia scalabile correttamente, verifica che ogni sottorete del sistema di bilanciamento del carico abbia un CIDR blocco con almeno una `/27` maschera di bit (ad esempio`10.0.0.0/27`) e abbia almeno 8 indirizzi IP liberi. Il sistema di bilanciamento del carico utilizza questi indirizzi IP per stabilire connessioni con le istanze e per aumentare orizzontalmente quando necessario. Se gli indirizzi IP non sono sufficienti, il sistema di bilanciamento del carico potrebbe non essere in grado di scalare, causando errori 503 dovuti a una capacità insufficiente.

Crea una sottorete in ogni zona di disponibilità in cui desideri avviare istanze. A seconda dell'applicazione, puoi avviare le istanze in sottoreti pubbliche, sottoreti private o una combinazione di sottoreti pubbliche e private. Una sottorete pubblica dispone di una route a un gateway Internet. Tieni presente che per impostazione predefinita è VPCs prevista una sottorete pubblica per zona di disponibilità.

Quando si crea un load balancer, occorre aggiungere ad esso una o più sottoreti pubbliche. Se le istanze si trovano in sottoreti private, crea sottoreti pubbliche nelle stesse zone di disponibilità delle sottoreti con le istanze; aggiungerai queste sottoreti pubbliche al load balancer.

Rete ACLs

La rete utilizzata ACLs VPC deve consentire il traffico in entrambe le direzioni sulla porta listener e sulla porta per il controllo dello stato di salute. Per ulteriori informazioni, consulta Rete ACLs per le istanze del vostro Classic Load Balancer.

Registra le istanze con il tuo Classic Load Balancer

La registrazione di un'EC2istanza la aggiunge al sistema di bilanciamento del carico. Il load balancer monitora continuamente l'integrità delle istanze registrate nelle zone di disponibilità abilitate e instrada le richieste verso le istanze integre. Se la richiesta per le istanze aumenta, puoi registrare istanze aggiuntive con il load balancer per gestire la richiesta.

L'annullamento della registrazione di un'EC2istanza la rimuove dal sistema di bilanciamento del carico. Il load balancer arresta il routing delle richieste verso un'istanza non appena la sua registrazione viene annullata. In caso di riduzione della richiesta o se è necessario eseguire la manutenzione delle istanze, puoi annullare la registrazione delle istanze dal load balancer. Un'istanza la cui registrazione viene annullata rimane in esecuzione, ma non riceve più il traffico dal load balancer e può essere nuovamente registrata con il load balancer quando si è pronti.

Quando annulli la registrazione di un'istanza, Elastic Load Balancing attende finché le richieste in transito non sono completate, se è stato abilitato Connection Draining. Per ulteriori informazioni, consulta Configura il Connection Draining per il Classic Load Balancer.

Se il load balancer è collegato a un gruppo Auto Scaling, le istanze nel gruppo vengono registrate automaticamente con il load balancer. Se annulli il collegamento di un load balancer dal gruppo Auto Scaling, la registrazione delle istanze nel gruppo viene annullata.

Elastic Load Balancing registra l'EC2istanza con il sistema di bilanciamento del carico utilizzando il relativo indirizzo IP.

[EC2-VPC] Quando si registra un'istanza con un'interfaccia di rete elastica (ENI) collegata, il load balancer indirizza le richieste all'indirizzo IP primario dell'interfaccia primaria (eth0) dell'istanza.

Indice

Registrazione di un'istanza

Quando sei pronto, registra l'istanza con il load balancer. Se l'istanza si trova in una zona di disponibilità che è abilitata per il load balancer, l'istanza è pronta per ricevere il traffico dal load balancer non appena supera il numero richiesto di controlli dello stato.

Per registrare le istanze mediante 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Istanze di destinazione, seleziona Gestisci le istanze.
5. Nella pagina Gestisci le istanze, all'interno della tabella Istanze disponibili, seleziona le istanze da registrare con il sistema di bilanciamento del carico.
6. Assicurati che le istanze da registrare siano popolate nella tabella Esamina le istanze selezionate.
7. Scegli Save changes (Salva modifiche).

Per registrare le tue istanze utilizzando il AWS CLI

Utilizzate il seguente comando register-instances-with-load-balancer:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --instances i-4e05f721
```

Di seguito è riportata una risposta di esempio che elenca le istanze registrate con il load balancer:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        },
        {
            "InstanceId": "i-4e05f721"
        }
    ]
}
```

Visualizza le istanze registrate con un load balancer

Utilizzate il describe-load-balancerscomando seguente per elencare le istanze registrate con il sistema di bilanciamento del carico specificato:

```
aws elb describe-load-balancers --load-balancer-names my-load-balancer --output text --
query "LoadBalancerDescriptions[*].Instances[*].InstanceId"
```

Di seguito è riportato un output di esempio:

```
i-e905622e
i-315b7e51
i-4e05f721
```

Determinazione del bilanciamento del carico per un'istanza registrata

Utilizzate il describe-load-balancerscomando seguente per ottenere il nome del sistema di bilanciamento del carico in cui è registrata l'istanza specificata:

```
aws elb describe-load-balancers --output text --query "LoadBalancerDescriptions[?
Instances[?InstanceId=='i-e905622e']].[LoadBalancerName]"
```

Di seguito è riportato un output di esempio:

```
my-load-balancer
```

Annullamento della registrazione di un'istanza

Puoi annullare la registrazione di un'istanza dal load balancer se tale capacità non è più necessaria o se devi eseguire la manutenzione dell'istanza.

Se il load balancer è collegato a un gruppo Auto Scaling, scollegando l'istanza dal gruppo viene anche annullata la registrazione dal load balancer. Per ulteriori informazioni, consulta Scollegare EC2 le istanze dal gruppo Auto Scaling nella Amazon Auto Scaling User EC2 Guide.

Per annullare la registrazione delle istanze mediante 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Istanze di destinazione, seleziona Gestisci le istanze.
5. Nella pagina Gestisci le istanze, all'interno della tabella Istanze disponibili, deseleziona le istanze di cui annullare la registrazione dal sistema di bilanciamento del carico.
6. Assicurati che le istanze da registrare non siano popolate nella tabella Esamina le istanze selezionate.
7. Scegli Save changes (Salva modifiche).

Per annullare la registrazione delle istanze utilizzando il AWS CLI

Utilizzate il seguente deregister-instances-from-load comando -balancer:

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-loadbalancer --instances i-4e05f721
```

Di seguito è riportato un esempio di risposta che elenca le istanze rimanenti registrate con il load balancer:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        }
    ]
}
```

Controlli dello stato delle istanze del tuo Classic Load Balancer

Il Classic Load Balancer invia periodicamente delle richieste alle istanze registrate per testare il loro stato. Questi test sono chiamati controlli dello stato. Lo stato delle istanze che sono integre al momento del controlli dello stato è `InService`. Lo stato di qualsiasi istanza che non è integra al momento del controllo dello stato è `OutOfService`. Il load balancer esegue controlli dello stato su tutte le istanze registrate, a prescindere che lo stato dell'istanza sia integro o non integro.

Il load balancer instrada le richieste solo verso le istanze integre. Quando il load balancer determina che un'istanza non è integra, interrompe il routing delle richieste a tale istanza. Il load balancer riprende il routing delle richieste all'istanza quando viene ripristinata in uno stato integro.

Il load balancer controlla l'integrità delle istanze registrate utilizzando la configurazione di controllo dell'integrità predefinita fornita da Elastic Load Balancing o una configurazione di controllo dell'integrità impostata dall'utente.

Se hai associato il gruppo Auto Scaling a un Classic Load Balancer, puoi utilizzare il controllo dell'integrità del bilanciamento del carico per determinare lo stato di integrità delle istanze nel gruppo Auto Scaling. Per impostazione predefinita, un gruppo Auto Scaling determina periodicamente lo stato di integrità di ogni istanza. Per ulteriori informazioni, consulta Aggiungi i controlli di integrità di Elastic Load Balancing al tuo gruppo Auto Scaling nella Amazon Auto Scaling User EC2 Guide.

Indice

Configurazione del controllo dell'integrità

La configurazione dello stato contiene le informazioni utilizzate da un load balancer per determinare lo stato di integrità delle istanze registrate. La tabella seguente descrive i campi della configurazione di controllo dello stato.

Campo	Descrizione
Protocollo	Il protocollo da utilizzare per connettersi all'istanza. Valori validi: `TCP`, `HTTP`, `HTTPS` e `SSL` Impostazione predefinita della console: `HTTP` CLI/impostazione predefinita: API `TCP`
Porta	La porta da utilizzare per connettersi all'istanza, come una coppia `protocol:port` . Se il load balancer non è in grado di connettersi all'istanza sulla porta specificata

Campo	Descrizione
	entro il periodo di timeout di risposta configurato, l'istanza è considerata non integra. Protocolli: `TCP`, `HTTP`, `HTTPS` e `SSL` Intervallo porta: da 1 a 65535 Impostazione predefinita della console: `HTTP:80` CLI/APIimpostazione predefinita: `TCP:80`
Path	La destinazione per la HTTPS richiesta HTTP or. Viene emessa una HTTPS GET richiesta HTTP or all'istanza sulla porta e sul percorso. Se il load balancer riceve una risposta diversa da "200 OK" entro il periodo di timeout della risposta, l'istanza viene considerata non integra. Se la risposta include un corpo, l'applica zione deve impostare l'intestazione Content-Length su un valore maggiore o uguale a zero oppure specificare Transfer-Encoding con un valore impostato su "chunked". Impostazione predefinita: `/index.html`
Response Timeout (Timeout di risposta)	Il periodo di tempo di attesa quando si riceve una risposta dal controllo dello stato, in secondi. Valori validi: da 2 a 60. Impostazione predefinita: 5
HealthCheck Intervallo	Il periodo di tempo tra i controlli dello stato di una singola istanza, in secondi. Valori validi: da 5 a 300. Impostazione predefinita: 30

Campo	Descrizione
Unhealthy Threshold (Soglia di mancata integrità)	Il numero di controlli di integrità consecutivi non riusciti che devono essere eseguiti prima di dichiarare un'EC2istanza non integra. Valori validi: da 2 a 10. Impostazione predefinita: 2
Soglia di integrità	Il numero di controlli di integrità consecutivi che devono essere eseguiti con successo prima di dichiarare un'EC2istanza integra. Valori validi: da 2 a 10. Impostazione predefinita: 10

Il load balancer invia una richiesta di controllo dell'integrità a ciascuna istanza registrata ogni `Interval` secondi, utilizzando la porta, il protocollo e il percorso specificati. Ogni richiesta di controllo dello stato è indipendente e dura l'intero intervallo. Il tempo di risposta dell'istanza non influenza l'intervallo per il controllo dello stato successivo. Se i controlli di integrità superano gli errori UnhealthyThresholdCountconsecutivi, il sistema di bilanciamento del carico mette fuori servizio l'istanza. Quando i controlli di integrità superano i successi HealthyThresholdCountconsecutivi, il load balancer rimette l'istanza in servizio.

Un controlloHTTP/HTTPShealth ha esito positivo se l'istanza restituisce un codice di risposta di 200 entro l'intervallo del controllo di integrità. Un controllo di TCP integrità ha esito positivo se la TCP connessione ha esito positivo. Un controllo dello SSL stato di SSL salute ha esito positivo se la stretta di mano ha esito positivo.

Aggiornamento della configurazione di controllo dell'integrità

Puoi aggiornare la configurazione di controllo dello stato per il load balancer in qualsiasi momento.

Per aggiornare la configurazione di controllo dello stato per il load balancer utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Controlli dello stato, seleziona Modifica.
5. Nella pagina Modifica le impostazioni di controllo dello stato, in Controlli dell'integrità, aggiorna la configurazione in base alle esigenze.
6. Dopo aver effettuato le selezioni, scegli Salva modifiche.

Per aggiornare la configurazione del controllo dello stato del tuo sistema di bilanciamento del carico, utilizza il AWS CLI

Utilizzando il seguente comando configure-health-check:

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-check
 Target=HTTP:80/path,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Controllo dell'integrità delle istanze

Puoi controllare lo stato di integrità delle istanze registrate.

Per controllare lo stato di integrità delle istanze utilizzando 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. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella sezione Dettagli, il campo Stato indica quante istanze sono in servizio.
5. Nella scheda Istanze di destinazione, all'interno della tabella Istanze di destinazione, la colonna Stato di integrità indica lo stato specifico di ogni istanza registrata.

Per verificare lo stato di integrità delle tue istanze, utilizza il AWS CLI

Utilizzando il seguente comando describe-instance-health:

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

Risoluzione dei problemi dei controlli dell'integrità

Il controllo dello stato del load balancer per le istanze registrate può non riuscire per diversi motivi. I motivi più comuni per cui non si riesce a superare un controllo dello stato sono EC2 le istanze che interrompono le connessioni al sistema di bilanciamento del carico o il timeout della risposta delle istanze. EC2 Per informazioni sulle cause potenziali e la procedura che è possibile eseguire per risolvere i problemi di controllo dello stato non riuscito, consulta Risoluzione dei problemi di un Classic Load Balancer: controlli dello stato.

Gruppi di sicurezza per le istanze del tuo Classic Load Balancer

Un gruppo di sicurezza agisce come un firewall che controlla il traffico consentito verso o da una o più istanze. Quando avvii un'EC2istanza, puoi associare uno o più gruppi di sicurezza all'istanza. Per ogni gruppo di sicurezza, aggiungi una o più regole per consentire il traffico. Puoi modificare le regole per un gruppo di sicurezza in qualunque momento; le nuove regole vengono applicate automaticamente a tutte le istanze associate al gruppo di sicurezza. Per ulteriori informazioni, consulta i gruppi EC2 di sicurezza Amazon nella Amazon EC2 User Guide.

I gruppi di sicurezza per le istanze devono consentirne la comunicazione con il load balancer. La tabella seguente mostra le regole di entrata consigliate.

Crea	Protocollo	Intervallo porte	Commento
load balancer security group	TCP	*instance listener*	Consente il traffico dal load balancer sulla porta del listener dell'istanza
load balancer security group	TCP	*health check*	Autorizza il traffico dal load balancer sulla porta di controllo dello stato

Ti consigliamo inoltre di consentire al ICMP traffico in entrata di supportare Path MTU Discovery. Per ulteriori informazioni, consulta Path MTU Discovery nella Amazon EC2 User Guide.

Rete ACLs per le istanze del vostro Classic Load Balancer

Una lista di controllo degli accessi alla rete (ACL) consente o nega un traffico specifico in entrata o in uscita a livello di sottorete. È possibile utilizzare la rete ACL predefinita oppure creare una rete personalizzata VPC con regole simili a quelle ACL per i gruppi di sicurezza in modo da aggiungere un ulteriore livello di sicurezza al proprio. VPC VPC

L'elenco di controllo degli accessi alla rete predefinito (ACL) VPC consente tutto il traffico in entrata e in uscita. Se si crea una rete personalizzataACLs, è necessario aggiungere regole che consentano la comunicazione tra il sistema di bilanciamento del carico e le istanze.

Le regole consigliate per la sottorete per le istanze variano a seconda che la sottorete sia privata o pubblica. Le seguenti regole sono relative a una sottorete privata. Se le istanze si trovano in una sottorete pubblica, modificate l'origine e la destinazione dall'inizio allaCIDR. VPC `0.0.0.0/0`

Di seguito sono riportate le regole di ingresso consigliate.

Crea	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	*instance listener*	Consenti il traffico in entrata dalla porta del VPC CIDR listener sull'istanza
VPC CIDR	TCP	*health check*	Consenti il traffico in entrata dalla porta di controllo dello VPC CIDR stato di salute

Di seguito sono riportate le regole in uscita consigliate.

Destinazione	Protocollo	Intervallo porte	Commento
VPC CIDR	TCP	1024-65535	Consenti il traffico in uscita verso le VPC CIDR porte temporanee

Monitoraggio del Classic Load Balancer

Per monitorare i bilanciatori del carico, analizzare i modelli di traffico e risolvere i problemi relativi ai bilanciatori del carico e alle istanze di back-end, puoi utilizzare le seguenti risorse.

CloudWatch metriche

Elastic Load Balancing pubblica punti dati CloudWatch su Amazon sui tuoi sistemi di bilanciamento del carico e sulle istanze di back-end. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Classic Load Balancer.

Log di accesso per Elastic Load Balancing

I log di accesso per Elastic Load Balancing acquisiscono informazioni dettagliate per le richieste inviate al load balancer e le archiviano come file di log nel bucket Amazon S3 specificato. Ogni log contiene dettagli come l'ora in cui è stata ricevuta una richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server. Puoi utilizzare questi log di accesso per analizzare i modelli di traffico e risolvere i problemi relativi alle applicazioni di back-end. Per ulteriori informazioni, consulta Log di accesso di Classic Load Balancer.

CloudTrail registri

AWS CloudTrail ti consente di tenere traccia delle chiamate effettuate all'Elastic Load Balancing API da o per conto del tuo AWS account. CloudTrail archivia le informazioni nei file di registro nel bucket Amazon S3 specificato. Puoi utilizzare questi file di log per monitorare l'attività dei tuoi bilanciatori del carico determinando quali richieste sono state effettuate, gli indirizzi IP di origine da cui provengono le richieste, l'autore della richiesta, il momento in cui è stata effettuata e così via. Per ulteriori informazioni, consulta Registrare API le chiamate per l'utilizzo di Elastic Load Balancing. CloudTrail

CloudWatch metriche per il tuo Classic Load Balancer

Elastic Load Balancing pubblica punti dati su Amazon CloudWatch per i tuoi sistemi di bilanciamento del carico e le tue istanze di back-end. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a un

parametro come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. Ad esempio, è possibile monitorare il numero totale di EC2 istanze integre per un sistema di bilanciamento del carico in un periodo di tempo specificato. A ogni punto di dati sono associati un timestamp e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un 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 supera quello che consideri un intervallo accettabile.

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

Per ulteriori informazioni su Amazon CloudWatch, consulta la Amazon CloudWatch User Guide.

Indice

Parametri Classic Load Balancer

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

Metrica	Descrizione
`BackendConnectionErrors`	Il numero di connessioni che non sono state stabilite tra il load balancer e le istanze registrate. In caso di errori il load balancer ritenta la connessione, pertanto questo conteggio può essere superiore al tasso di richiesta. Il conteggio include anche eventuali errori di connessione relativi al controllo dello stato. Criteri di segnalazione: è presente un valore diverso da zero

Metrica	Descrizione
	Statistiche: la statistica più utile è `Sum`. Le statistiche `Average`, `Minimum` e `Maximum` sono segnalate per nodo del load balancer e in genere non sono utili. Tuttavia, la differenza tra il valore minimo e il massimo (o tra picco e media o tra media e minimo) potrebbe essere utile per determinare se un nodo del load balancer è un outlier. Esempio: supponiamo che il load balancer includa 2 istanze in us-west-2a e 2 istanze in us-west-2b e che i tentativi di connettersi a 1 istanza in us-west-2a causino errori di connessione back-end. La somma per us-west-2a include questi errori di connessione, mentre la somma per us-west-2b non li include. Pertanto, la somma per il load balancer è uguale alla somma per us-west-2a.
`DesyncMitigationMode_NonCompliant_Request_Count`	[HTTPlistener] Il numero di richieste non conformi al RFC 7230. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`.

Metrica	Descrizione
`HealthyHostCount`	Il numero di istanze integre registrate con il load balancer. Una nuova istanza registrata viene considerata integra dopo aver superato il primo controllo dello stato. Se il load balancer è abilitato , il numero di istanze integre per la dimensione `LoadBalancerName` viene calcolato in tutte le zone di disponibilità. In caso contrario, viene calcolato per zona di disponibilità. Criteri di segnalazione: sono presenti istanze registrate Statistiche: le statistiche più utili sono `Average` e `Maximum`. Queste statistiche sono determinate dai nodi del load balancer. Alcuni nodi del load balancer potrebbero determinare la mancata integrità di un'istanza per un breve periodo, mentre altri nodi ne determinano l'integrità. Esempio: supponiamo che il load balancer includa 2 istanze in us-west-2a e 2 istanze in us-west-2b. Us-west-2a include 1 istanza non integra, us-west-2b non include alcuna istanza non integra. Con la dimensione `AvailabilityZone` , si ottiene una media di 1 istanza integra e 1 non integra in us-west-2a e una media di 2 istanze integre e 0 istanze non integre in us-west-2b.

Metrica	Descrizione
`HTTPCode_Backend_2XX` , `HTTPCode_Backend_3XX` , `HTTPCode_Backend_4XX` , `HTTPCode_Backend_5XX`	[HTTPlistener] Il numero di codici di HTTP risposta generati dalle istanze registrate. Questo conteggio non include i codici di risposta generati 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 tutti il valore 1. Esempio: supponiamo che il sistema di bilanciamento del carico abbia 2 istanze in us-west-2a e 2 istanze in us-west-2b e che le richieste inviate a 1 istanza in us-west-2a generino 500 risposte. HTTP La somma per us-west-2a include queste risposte di errore, mentre la somma per us-west-2b non le include. Pertanto, la somma per il load balancer è uguale alla somma per us-west-2a.
`HTTPCode_ELB_4XX`	[HTTPlistener] Il numero di codici di errore del client 4XX generati dal load balancer. HTTP Gli errori client vengono generati quando una richiesta non ha formato corretto oppure è incompleta. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. `Minimum`, `Maximum` e `Average` restituiscono tutti il valore 1. Esempio: supponiamo che il sistema di bilanciamento del carico abbia abilitato us-west-2a e us-west-2b e che le richieste del client includano una richiesta con formato errato. URL Di conseguen za, è probabile che gli errori del client aumentino in tutte le zone di disponibilità. La somma per il load balancer corrisponde alla somma dei valori per le zone di disponibilità.

Metrica	Descrizione
HTTPCode_ELB_5XX	[HTTPlistener] Il numero di codici di errore del server 5XX generati dal load balancer. HTTP Questo conteggio non include i codici di risposta generati dalle istanze registrate. Il parametro viene segnalato se non sono presenti istanze integre registrate nel load balancer o se il tasso di richiesta supera la capacità delle istanze (spillover) o del load balancer. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è Sum. Minimum, Maximum e Average restituiscono tutti il valore 1. Esempio: supponiamo che nel load balancer siano abilitate us-west-2a e us-west-2b e che le istanze in us-west-2a abbiano una latenza elevata e siano lente nella risposta alle richieste. Di conseguenza, la coda per i nodi del load balancer nel client e negli inserimenti di us-west-2a e generano un errore 503. Se us-west-2b continua a rispondere normalmente, la somma per il load balancer è uguale alla somma per us-west-2a.

Metrica	Descrizione
`Latency`	[HTTPlistener] Il tempo totale trascorso, in secondi, dal momento in cui il load balancer ha inviato la richiesta a un'istanza registrata fino a quando l'istanza ha iniziato a inviare le intestazioni di risposta. [TCPlistener] Il tempo totale trascorso, in secondi, dal sistema di bilanciamento del carico per stabilire correttamente una connessio ne a un'istanza registrata. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Average`. Utilizzare `Maximum` per determinare se alcune richieste richiedono molto più tempo rispetto alla media. Il valore `Minimum` in genere non è utile. Esempio: supponiamo che il load balancer includa 2 istanze in us-west-2a e 2 istanze in us-west-2b e che per le richieste inviate a 1 istanza in us-west-2a si riscontri una latenza superiore. La media per us-west-2a ha un valore superiore rispetto alla media per us-west-2b.

Metrica	Descrizione
`RequestCount`	Il numero di richieste completate o connessioni effettuate durante l'intervallo specificato (1 o 5 minuti). [HTTPlistener] Il numero di richieste ricevute e instradate, incluse le risposte di HTTP errore dalle istanze registrate. [TCPlistener] Il numero di connessioni effettuate alle istanze registrate. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. `Minimum`, `Maximum` e `Average` restituiscono tutti 1. Esempio: supponiamo che il load balancer includa 2 istanze in us-west-2a e 2 istanze in us-west-2b e che 100 richieste vengano inviate al load balancer. Sono presenti 60 richieste inviate a us-west-2a per le quali ogni istanza riceve 30 richieste e 40 richieste inviate a us-west-2b per le quali ogni istanza riceve 20 richieste. Con la dimensione `AvailabilityZone` , si ottiene una somma di 60 richieste in us-west-2a e di 40 richieste in us-west-2b. Con la dimensione `LoadBalancerName` , si ottiene una somma di 100 richieste.

Metrica	Descrizione
`SpilloverCount`	Il numero totale di richieste respinte perché la coda è completa. [HTTPlistener] Il load balancer restituisce un HTTP codice di errore 503. [TCPlistener] Il load balancer chiude la connessione. Criteri di segnalazione: è presente un valore diverso da zero Statistiche: la statistica più utile è `Sum`. Le statistiche `Average`, `Minimum` e `Maximum` sono segnalate per nodo del load balancer e in genere non sono utili. Esempio: supponiamo che nel load balancer siano abilitate us-west-2a e us-west-2b e che le istanze in us-west-2a abbiano una latenza elevata e siano lente nella risposta alle richieste. Di conseguenza, la coda per il nodo del load balancer in us-west-2 a determina uno spillover. Se us-west-2b continua a risponder e normalmente, la somma per il load balancer sarà uguale alla somma per us-west-2a.

Metrica	Descrizione
SurgeQueueLength	Il numero totale di richieste (HTTPlistener) o connessioni (TCPlistener) in attesa di routing verso un'istanza integra. La dimensione massima della coda è di 1.024. Quando la coda è completa, eventuali richieste o connessioni aggiuntive vengono rifiutate. Per ulteriori informazioni, consulta SpilloverCount . Criteri di segnalazione: vi è un valore diverso da zero. Statistics (Statistiche): la statistica più utile è Maximum, poiché rappresenta il picco delle richieste in coda. La statistica Average può essere utile in combinazione con Minimum e Maximum per determinare l'intervallo delle richieste in coda. Il valore Sum non è utile. Esempio: supponiamo che nel load balancer siano abilitate us-west-2a e us-west-2b e che le istanze in us-west-2a abbiano una latenza elevata e siano lente nella risposta alle richieste. Quindi, la coda per i nodi del load balancer in us-west-2a aumenta e raggiunge il limite e, probabilmente, nel client i tempi di risposta sono più lunghi. Se la situazione persiste, probabilmente nel load balancer si verificheranno degli spillover (vedere il parametro SpilloverCount). Se us-west-2b continua a rispondere normalmente, il valore max per il load balancer sarà uguale al max per us-west-2a.

Metrica	Descrizione
`UnHealthyHostCount`	Il numero di istanze non integre registrate per il load balancer. Un'istanza viene considerata non integra quando supera la soglia di mancata integrità configurata per il controllo dello stato. Un'istanza non integra viene considerata di nuovo integra quando soddisfa la soglia di integrità configurata per il controllo dello stato. Criteri di segnalazione: sono presenti istanze registrate Statistiche: le statistiche più utili sono `Average` e `Minimum`. Queste statistiche sono determinate dai nodi del load balancer. Alcuni nodi del load balancer potrebbero determinare la mancata integrità di un'istanza per un breve periodo, mentre altri nodi ne determinano l'integrità. Esempio: vedi `HealthyHostCount` .

I seguenti parametri ti consentono di effettuare una stima dei costi se esegui la migrazione da un Classic Load Balancer a un Application Load Balancer. Queste metriche sono destinate esclusivamente all'uso informativo, non all'uso con gli allarmi. CloudWatch Se Classic Load Balancer è dotato di più listener, questi parametri vengono aggregati nei listener.

Queste stime sono basate su un load balancer con una regola predefinita e un certificato di dimensione 2K. Se utilizzi un certificato di dimensioni pari o superiori a 4K, ti consigliamo di effettuare la stima dei costi come segue: crea un Application Load Balancer basato su Classic Load Balancer tramite lo strumento di migrazione e monitora il parametro `ConsumedLCUs` per Application Load Balancer. Per ulteriori informazioni, consulta Migrazione da un Classic Load Balancer a un Application Load Balancer nella Guida per l'utente Elastic Load Balancing.

Parametro	Descrizione
`EstimatedALBActive ConnectionCount`	Il numero stimato di TCP connessioni simultanee attive dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico agli obiettivi.

Parametro	Descrizione
`EstimatedALBConsumedLCUs`	Il numero stimato di unità di capacità del load balancer (LCU) utilizzate da un Application Load Balancer. Paghi per il numero di LCUs quello che usi all'ora. Per ulteriori informazioni, consulta Prezzi di Elastic Load Balancing.
`EstimatedALBNewConnectionCount`	Il numero stimato di nuove TCP connessioni stabilite dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico agli obiettivi.
`EstimatedProcessedBytes`	Il numero stimato di byte elaborati da un Application Load Balancer.

Dimensioni di parametro per Classic Load Balancer

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

Dimensione	Descrizione
`AvailabilityZone`	Consente di filtrare i dati del parametro per la zona di disponibilità specificata.
`LoadBalancerName`	Consente di filtrare i dati del parametro per il load balancer specificato.

Statistiche per i parametri di Classic 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 `Minimum` e `Maximum` rispecchiano i valori minimo e massimo riportati dai singoli nodi del load balancer. Supponiamo ad esempio che ci siano 2 nodi del load balancer. 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.

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 load balancer, ad esempio `RequestCount`, `HTTPCode_ELB_XXX`, `HTTPCode_Backend_XXX`, `BackendConnectionErrors` e `SpilloverCount`.

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 le metriche per il tuo sistema di bilanciamento del carico utilizzando 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. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Scegli il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Scegliere la scheda Monitoring (Monitoraggio).
5. Per ingrandire la visualizzazione di un singolo parametro, passa il mouse sul relativo grafico, quindi scegli l'icona `Maximize`. Sono disponibili i seguenti parametri:

   - Host integri – `HealthyHostCount`
   - Host non integri – `UnHealthyHostCount`
   - Latenza media – `Latency`
   - Richieste - `RequestCount`
   - Errori di connessione del back-end – `BackendConnectionErrors`
   - Lunghezza della coda in aumento – `SurgeQueueLength`
   - Numero di spillover – `SpilloverCount`
   - HTTP2 XXs — `HTTPCode_Backend_2XX`
   - HTTP3 XXs — `HTTPCode_Backend_3XX`
   - HTTP4 XXs — `HTTPCode_Backend_4XX`
   - HTTP5 XXs — `HTTPCode_Backend_5XX`
   - ELBHTTP4 XXs — `HTTPCode_ELB_4XX`
   - ELBHTTP5 XXs — `HTTPCode_ELB_5XX`
   - Numero stimato di byte elaborati - `EstimatedProcessedBytes`
   - ALBConsumo stimato LCUs — `EstimatedALBConsumedLCUs`
   - Numero stimato di connessioni ALB attive: `EstimatedALBActiveConnectionCount`
   - Numero stimato di ALB nuove connessioni: `EstimatedALBNewConnectionCount`

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 ELB.
4. Esegui una di queste operazioni:

- Selezionare una dimensione di parametro per visualizzare i parametri per il load balancer in base alla zona di disponibilità o su tutti i bilanciatori del carico.
- Per visualizzare tutte le dimensioni di un parametro, digitarne il nome nel campo di ricerca.
- Per visualizzare i parametri di un singolo load balancer, digitare il relativo nome nel campo di ricerca.
- Per visualizzare i parametri di una singola zona di disponibilità, digitare il relativo nome nel campo di ricerca.

Log di accesso di Classic 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 per impostazione predefinita è disabilitata. Dopo aver abilitato i log di accesso per il load balancer, Elastic Load Balancing acquisisce i log e li archivia nel bucket Amazon S3 specificato. Puoi disabilitare la registrazione degli accessi in qualsiasi momento.

Ogni file di registro degli accessi viene automaticamente crittografato utilizzando SSE -S3 prima di essere archiviato nel bucket S3 e decrittografato quando vi si accede. Non sono necessari interventi; la crittografia e decrittografia vengono eseguite in modo trasparente. Ogni file di registro è crittografato con una chiave univoca, a sua volta crittografata con una KMS chiave che viene ruotata regolarmente. Per ulteriori informazioni, consulta Protezione dei dati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) nella Guida per l'utente di Amazon Simple Storage Service.

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

Indice

- Abilitazione dei log di accesso di Classic Load Balancer
- Disabilitazione dei log di accesso di Classic Load Balancer

File di log di accesso

Elastic Load Balancing pubblica un file di log per ogni nodo del load balancer all'intervallo specificato. Puoi specificare un intervallo di pubblicazione di 5 o 60 minuti quando abiliti il log di accesso per il load balancer. Per impostazione predefinita, Elastic Load Balancing pubblica log a intervalli di 60 minuti. Se l'intervallo è impostato su 5 minuti, i log vengono pubblicati all'1:05, 1:10, 1:15 e così via. L'avvio della distribuzione dei log viene ritardato fino a 5 minuti se l'intervallo è impostato su 5 minuti e fino a 15 minuti se l'intervallo è impostato su 60 minuti. Puoi modificare l'intervallo di pubblicazione in qualsiasi momento.

Il load balancer è in grado di consegnare più log per lo stesso periodo. In genere questo accade se il sito presenta un traffico elevato, più nodi del load balancer e un breve intervallo di pubblicazione dei log.

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

```
amzn-s3-demo-loadbalancer-logs[/logging-prefix]/AWSLogs/aws-account-id/
elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-
balancer-name_end-time_ip-address_random-string.log
```

amzn-s3- demo-loadbalancer-logs

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 dell' AWS 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-name

Il nome del load balancer.

end-time

La data e l'ora di fine dell'intervallo dei log. Ad esempio, l'ora di fine 20140215T2340Z contiene voci per le richieste effettuate tra le 23:35 e le 23:40 se l'intervallo di pubblicazione è di 5 minuti.

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 registro con il prefisso»my-app":

```
s3://amzn-s3-demo-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

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

```
s3://amzn-s3-demo-loadbalancer-logs/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

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

Voci dei log di accesso

Elastic Load Balancing registra le richieste inviate al load balancer, incluse le richieste mai effettuate alle istanze di back-end. Ad esempio, se un client invia una richiesta errata o se non sono presenti istanze integre per rispondere alle richieste, queste vengono comunque registrate.

> **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.

Sintassi

Ogni voce di log contiene i dettagli di una singola richiesta inviata al load balancer. Tutti i campi nella voce di log sono delimitati da spazi. Ogni voce del file di log ha il formato seguente:

```
timestamp elb client:port backend:port request_processing_time backend_processing_time
 response_processing_time elb_status_code backend_status_code received_bytes sent_bytes
 "request" "user_agent" ssl_cipher ssl_protocol
```

La seguente tabella descrive i campi di una voce di un log di accesso.

Campo	Descrizione
time	L'ora in cui il load balancer ha ricevuto la richiesta dal client, in formato ISO 8601.
elb	Il nome del load balancer
client:port	L'indirizzo IP e la porta del client che esegue la richiesta.
backend:port	L'indirizzo IP e la porta dell'istanza registrata che ha elaborato la richiesta. Se il load balancer non può inviare la richiesta a un'istanza registrat a oppure se l'istanza chiude la connessione prima che possa essere inviata una risposta, questo valore è impostato su `-`.

Campo	Descrizione
	Questo valore può anche essere impostato su - se l'istanza registrata non risponde prima del timeout di inattività.
request_processing_time	[HTTPlistener] Il tempo totale trascorso, in secondi, dal momento in cui il load balancer ha ricevuto la richiesta fino al momento in cui l'ha inviata a un'istanza registrata. [TCPlistener] Il tempo totale trascorso, in secondi, dal momento in cui il load balancer ha accettato una SSL connessioneTCP/da un client al momento in cui il load balancer invia il primo byte di dati a un'istanza registrata. Questo valore è impostato su -1 se il load balancer non è in grado di inviare la richiesta a un'istanza registrata. Questo può accadere se l'istanza registrata chiude la connessione prima del timeout di inattivit à o se il client invia una richiesta errata. Inoltre, per TCP gli ascoltatori, ciò può accadere se il client stabilisce una connessione con il sistema di bilanciamento del carico ma non invia alcun dato. Questo valore può anche essere impostato su -1 se l'istanza registrata non risponde prima del timeout di inattività.
backend_processing_time	[HTTPlistener] Il tempo totale trascorso, in secondi, dal momento in cui il load balancer ha inviato la richiesta a un'istanza registrata fino a quando l'istanza ha iniziato a inviare le intestazioni di risposta. [TCPlistener] Il tempo totale trascorso, in secondi, dal sistema di bilanciamento del carico per stabilire correttamente una connessione a un'istanza registrata. Questo valore è impostato su -1 se il load balancer non è in grado di inviare la richiesta a un'istanza registrata. Questo può accadere se l'istanza registrata chiude la connessione prima del timeout di inattività o se il client invia una richiesta errata. Questo valore può anche essere impostato su -1 se l'istanza registrata non risponde prima del timeout di inattività.

Campo	Descrizione
response_processing_time	[HTTPlistener] Il tempo totale trascorso (in secondi) dal momento in cui il load balancer ha ricevuto l'intestazione di risposta dall'istanza registrata fino a quando 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. [TCPlistener] Il tempo totale trascorso, in secondi, dal momento in cui il load balancer ha ricevuto il primo byte dall'istanza registrata fino a quando non ha iniziato a inviare la risposta al client. Questo valore è impostato su `-1` se il load balancer non è in grado di inviare la richiesta a un'istanza registrata. Questo può accadere se l'istanza registrata chiude la connessione prima del timeout di inattività o se il client invia una richiesta errata. Questo valore può anche essere impostato su `-1` se l'istanza registrata non risponde prima del timeout di inattività.
elb_status_code	[HTTPlistener] Il codice di stato della risposta dal load balancer.
backend_status_code	[HTTPlistener] Il codice di stato della risposta dall'istanza registrata.
received_bytes	Le dimensioni della richiesta, in byte, ricevuta dal client (richiedente). [HTTPlistener] Il valore include il corpo della richiesta ma non le intestazioni. [TCPlistener] Il valore include il corpo della richiesta e le intestazioni.
sent_bytes	Le dimensioni della risposta, in byte, inviata al client (richiedente). [HTTPlistener] Il valore include il corpo della risposta ma non le intestazioni. [TCPlistener] Il valore include il corpo della richiesta e le intestazioni.

Campo	Descrizione
richiesta	La riga di richiesta del client racchiusa tra virgolette e registrata nel seguente formato: HTTP Method + Protocol: //Host header:port + Path + version. HTTP Il load balancer conserva l'URLinvio dal client, così com'è, durante la registrazione della richiesta. URI Non imposta il tipo di contenuto per il file di log di accesso. Quando elabori questo campo, considera come il client ha inviato il. URL [TCPlistener] Sono tre trattini, ciascuno separato da uno spazio e terminanti con uno spazio («- - - «). URL
user_agent	[HTTP/HTTPSlistener] Una stringa User-Agent che identifica il client che ha originato la richiesta. 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	[HTTPS/SSLlistener] Il codice. SSL Questo valore viene registrato solo se la TLS connessioneSSL/in entrata è stata stabilita dopo una negoziazi one riuscita. In caso contrario, il valore è impostato su -.
ssl_protocol	[HTTPS/SSLlistener] Il protocollo. SSL Questo valore viene registrat o solo se la TLS connessioneSSL/in entrata è stata stabilita dopo una negoziazione riuscita. In caso contrario, il valore è impostato su -.

Esempi

Esempio di immissione HTTP

Di seguito è riportato un esempio di voce di registro per un HTTP listener (dalla porta 80 alla porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000073
 0.001048 0.000057 200 200 0 29 "GET http://www.example.com:80/ HTTP/1.1" "curl/7.38.0"
 - -
```

Esempio HTTPS di voce

Di seguito è riportato un esempio di voce di registro per un HTTPS listener (dalla porta 443 alla porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80
 0.000086 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1"
 "curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2
```

Esempio di voce TCP

Di seguito è riportato un esempio di voce di registro per un TCP listener (dalla porta 8080 alla porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001069
 0.000028 0.000041 - - 82 305 "- - - " "-" - -
```

Esempio di voce SSL

Di seguito è riportato un esempio di voce di registro per un SSL listener (dalla porta 8443 alla porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001065
 0.000015 0.000023 - - 57 502 "- - - " "-" ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
```

Elaborazione dei log di accesso

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 utilizzando standard. SQL Per ulteriori informazioni, consulta la sezione relativa all'Esecuzione di query sui log Classic Load Balancer nella Guida per l'utente di Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Abilitazione dei log di accesso di Classic Load Balancer

Per abilitare i log di accesso per il tuo load balancer, devi specificare il nome del bucket Amazon S3 in cui il load balancer archivierà i log. Devi anche collegare a questo bucket una policy bucket che conceda a Elastic Load Balancing l'autorizzazione per 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 abiliti i log di accesso, devi specificare un bucket S3 per i relativi file. 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 sono le chiavi gestite da Amazon S3 (-S3). SSE 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 dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

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 bucket sono una raccolta di JSON istruzioni scritte nel linguaggio delle 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 del bucket che utilizzerai dipende dal tipo di bucket. Regione AWS

Regioni disponibili a partire da agosto 2022

Questa policy concede le autorizzazioni al servizio di consegna dei log specificato. Utilizza questa policy per i sistemi di bilanciamento del carico nelle zone di disponibilità e zone locali delle seguenti regioni:

- Asia Pacific (Hyderabad)
- Asia Pacifico (Malesia)
- Asia Pacifico (Melbourne)
- Canada occidentale (Calgary)
- Europa (Spagna)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente () UAE

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/
AWSLogs/012345678912/*"
    }
  ]
}
```

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 policy per i sistemi di bilanciamento del carico nelle zone di disponibilità o locali nelle regioni elencate qui sotto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "s3-bucket-arn"
    }
  ]
}
```

Replace (Sostituisci) *elb-account-id* con l'ID di Elastic Load Balancing per la tua regione: Account AWS

- 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

Replace (Sostituisci) *s3-bucket-arn* con la posizione ARN dei log di accesso. ARNCiò che viene specificato dipende dal fatto che si intenda specificare un prefisso quando si abilitano i registri di accesso nel passaggio 3.

- ARNesempio con un prefisso

```
arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/AWSLogs/012345678912/*
```

- ARNesempio senza prefisso

```
arn:aws:s3:::amzn-s3-demo-loadbalancer-logs/AWSLogs/012345678912/*
```

AWS GovCloud (US) Regions

Questa policy concede le autorizzazioni all'ID dell'account del sistema di bilanciamento del carico elastico 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "s3-bucket-arn"
    }
  ]
}
```

Replace (Sostituisci) *elb-account-id* con l'ID di Elastic Load Balancing per la tua Account AWS regione: Account AWS

- AWS GovCloud (Stati Uniti occidentali) — 048591011584
- AWS GovCloud (Stati Uniti orientali) — 190560391635

Replace (Sostituisci) *s3-bucket-arn* con la posizione dei log ARN di accesso. ARNCiò che viene specificato dipende dal fatto che si intenda specificare un prefisso quando si abilitano i registri di accesso nel passaggio 3.

- ARNesempio con un prefisso

```
arn:aws-us-gov:s3:::amzn-s3-demo-loadbalancer-logs/logging-prefix/
AWSLogs/012345678912/*
```

- ARNesempio senza prefisso

```
arn:aws-us-gov:s3:::amzn-s3-demo-loadbalancer-logs/AWSLogs/012345678912/*
```

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 si specifica un prefisso, questo non deve includere la stringa "». AWSLogs

Configurazione dei log di accesso per il load balancer 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. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella sezione Monitoraggio della pagina Modifica attributi del sistema di bilanciamento del carico, procedi come segue:
   a. Abilita l'opzione Log di accesso.
   b. Per S3 URI, inserisci il codice S3 URI per i tuoi file di registro. URICiò che specifichi dipende dal fatto che tu stia usando un prefisso.
      - URIcon un prefisso: `s3://amzn-s3-demo-loadbalancer-logs/logging-prefix`
      - URIsenza prefisso: `s3://amzn-s3-demo-loadbalancer-logs`
   c. Mantieni Intervallo di registrazione su `60 minutes - default`.

d. Scegli Save changes (Salva modifiche).

Per configurare i log di accesso per il sistema di bilanciamento del carico utilizzando il AWS CLI

Per prima cosa crea un file .json che consenta a Elastic Load Balancing di acquisire e distribuire i log ogni 60 minuti nel bucket S3 creato per i log:

```
{
  "AccessLog": {
    "Enabled": true,
    "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
    "EmitInterval": 60,
    "S3BucketPrefix": "my-app"
  }
}
```

Quindi, specifica il file.json nel comando come segue modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes file://my-json-file.json
```

Di seguito è riportata una risposta di esempio.

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
            "EmitInterval": 60,
            "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Per gestire il bucket S3 per i log di accesso

Assicurati di disabilitare i log di accesso prima di eliminare il bucket configurato. Altrimenti, se esiste un nuovo bucket con lo stesso nome e la policy del bucket richiesta creata in un bucket di Account AWS cui non sei proprietario, Elastic Load Balancing potrebbe scrivere i log di accesso per il tuo load balancer 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 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 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 S3 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-loadbalancer-logs*/*logging-prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - Ubicazione senza prefisso: *amzn-s3-demo-loadbalancer-logs*/AWSLogs/*123456789012*/ELBAccessLogTestFile

Risoluzione dei problemi

Accesso negato per il bucket: ***bucket-name***. Controlla l'autorizzazione di S3bucket

Questo errore può essere provato 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 hai abilitato i log di accesso. Verifica che la risorsa ARN non includa un prefisso se non lo hai specificato quando hai abilitato i log di accesso.
- 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 di Classic Load Balancer

Puoi disabilitare i log di accesso per il tuo load balancer in qualsiasi momento. Dopo avere disabilitato i log di accesso, questi rimarranno nel tuo Amazon S3 finché non saranno eliminati. Per ulteriori informazioni, consulta Working with S3 bucket nella Amazon Simple Storage Service User Guide.

Per disabilitare i log di accesso del sistema di bilanciamento del carico mediante 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. Seleziona il nome del sistema di bilanciamento del carico per aprirne la pagina dei dettagli.
4. Nella scheda Attributi, scegli Modifica.
5. Nella sezione Monitoraggio della pagina Modifica attributi del sistema di bilanciamento del carico, disabilita l'opzione Log di accesso.

Per disabilitare i log di accesso utilizzando il AWS CLI

Utilizzate il seguente modify-load-balancer-attributescomando per disabilitare i log di accesso:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"AccessLog\":{\"Enabled\":false}}"
```

Di seguito è riportata una risposta di esempio:

```
{
    "LoadBalancerName": "my-loadbalancer",
    "LoadBalancerAttributes": {
        "AccessLog": {
            "S3BucketName": "amzn-s3-demo-loadbalancer-logs",
            "EmitInterval": 60,
            "Enabled": false,
            "S3BucketPrefix": "my-app"
        }
    }
}
```

Risoluzione dei problemi di Classic Load Balancer

Le tabelle seguenti elencano le risorse per la risoluzione dei problemi che possono essere utili durante l'utilizzo di un Classic Load Balancer.

APIerrori

Errore
CertificateNotFound: Non definito
OutofService: si è verificato un errore temporaneo

HTTPerrori

Errore
HTTP400: BAD _ REQUEST
HTTP405: METHOD _ _ NOT ALLOWED
HTTP408: timeout della richiesta
HTTP502: gateway non valido
HTTP503: Servizio non disponibile
HTTP504: timeout del gateway

Parametri dei codici di risposta

Parametro del codice di risposta
HTTPCode_ _4XX ELB
HTTPCode_ _5XX ELB
HTTPCode_Backend_2xx

Parametro del codice di risposta
HTTPCode_Backend_3xx
HTTPCode_Backend_4xx
HTTPCode_Backend_5xx

Problemi relativi al controllo dell'integrità

Problema
Errore della pagina di destinazione del controllo dello stato
Si è verificato il timeout della connessione alle istanze
L'autenticazione della chiave pubblica non riesce
L'istanza non riceve traffico dal load balancer
Le porte sull'istanza non sono aperte
Le istanze in un gruppo di Auto Scaling non superano il controllo di integrità ELB

Problemi di connettività

Problema
I client non sono in grado di connettersi a un sistema di bilanciamento del carico connesso a Internet
Le richieste inviate a un dominio personalizzato non vengono ricevute dal sistema di bilanciamento del carico
HTTPSIe richieste inviate al sistema di bilanciamento del carico restituiscono "NET:: ERR _ _ _» CERT COMMON NAME INVALID

Problemi di registrazione delle istanze

Problema
La registrazione di un'istanza richiede troppo tempo EC2
Impossibile registrare un'istanza avviata da un'istanza a pagamento AMI

Risoluzione dei problemi relativi a un Classic Load Balancer: errori API

Di seguito sono riportati i messaggi di errore restituiti da Elastic Load BalancingAPI, le possibili cause e i passaggi che è possibile eseguire per risolvere i problemi.

Messaggi di errore

- CertificateNotFound: Non definito
- OutofService: si è verificato un errore temporaneo

CertificateNotFound: Non definito

Causa 1: si è verificato un ritardo nella propagazione del certificato a tutte le regioni al momento della creazione mediante la AWS Management Console. Quando si verifica questo ritardo, il messaggio di errore viene visualizzato nell'ultima fase del processo di creazione del load balancer.

Soluzione 1: attendi circa 15 minuti, quindi riprova. Se il problema persiste, rivolgiti al Centro AWS Supportper ricevere assistenza.

Causa 2: se utilizzi AWS CLI o API direttamente, potresti ricevere questo errore se fornisci un Amazon Resource Name (ARN) per un certificato che non esiste.

Soluzione 2: usa l'azione AWS Identity and Access Management (IAM) GetServerCertificateper ottenere il certificato ARN e verifica di aver fornito il valore corretto perARN.

OutofService: si è verificato un errore temporaneo

Causa: si è verificato un problema temporaneo all'interno del servizio Elastic Load Balancing o della rete sottostante. Questo problema temporaneo potrebbe verificarsi anche quando Elastic Load Balancing esegue query sullo stato del load balancer e sulle sue istanze registrate.

Soluzione: riprova la chiamata. API Se il problema persiste, rivolgiti al Centro AWS Supportper ricevere assistenza.

Risoluzione dei problemi relativi a un Classic Load Balancer: errori HTTP

Il HTTP metodo (chiamato anche verbo) specifica l'azione da eseguire sulla risorsa che riceve una richiesta. HTTP I metodi standard per HTTP le richieste sono definiti in RFC 2616, Definizioni dei metodi. I metodi standard includonoGET,POST, PUTHEAD, eOPTIONS. Alcune applicazioni Web richiedono (e talvolta introducono) metodi che sono estensioni dei metodi HTTP /1.1. Esempi comuni di metodi HTTP estesi includono PATCHREPORT,MKCOL, PROPFINDMOVE, eLOCK. Elastic Load Balancing accetta tutti i metodi standard e non HTTP standard.

HTTPle richieste e le risposte utilizzano i campi di intestazione per inviare informazioni sui messaggi. HTTP I campi intestazione sono costituti da coppie nome-valore separate da due punti e intervallate da un ritorno a capo e un avanzamento riga. Un set standard di campi di HTTP intestazione è definito in RFC 2616, Message Headers. Per ulteriori informazioni, consulta HTTPheader e Classic Load Balancer.

Quando un load balancer riceve una HTTP richiesta, verifica la presenza di richieste non corrette e la lunghezza del metodo. La lunghezza totale del metodo in una HTTP richiesta a un sistema di bilanciamento del carico non deve superare i 127 caratteri. Se la HTTP richiesta supera entrambi i controlli, il load balancer invia la richiesta all'EC2istanza. Se il campo del metodo nella richiesta non ha un formato corretto, il load balancer risponde con un errore HTTP400: BAD _ REQUEST. Se la lunghezza del metodo nella richiesta supera i 127 caratteri, il load balancer risponde con un errore HTTP405: METHOD _ _ NOT ALLOWED.

L'EC2istanza elabora una richiesta valida implementando il metodo nella richiesta e inviando una risposta al client. Le istanze devono essere configurate per gestire sia i metodi supportati che quelli non supportati.

Di seguito sono elencati i messaggi di errore restituiti dal load balancer, le possibili cause e le operazioni che puoi eseguire per risolvere i problemi.

Messaggi di errore

- HTTP400: BAD _ REQUEST
- HTTP405: METHOD _ _ NOT ALLOWED

HTTP400: BAD _ REQUEST

Descrizione: indica che il client ha inviato una richiesta errata.

Causa 1: il client ha inviato una richiesta non valida che non soddisfa le HTTP specifiche. Ad esempio, una richiesta non può avere spazi in. URL

Causa 2: il client ha utilizzato il HTTP CONNECT metodo, che non è supportato da Elastic Load Balancing.

Soluzione: connettiti direttamente all'istanza e acquisisci i dettagli della richiesta client. Controlla gli header e verifica se ci sono richieste non URL corrette. Verifica che la richiesta soddisfi le HTTP specifiche. Verifica che non HTTP CONNECT sia utilizzata.

HTTP405: METHOD _ _ NOT ALLOWED

Descrizione: indica che la lunghezza del metodo non è valida.

Causa: la lunghezza del metodo nell'intestazione della richiesta supera i 127 caratteri.

Soluzione: controlla la lunghezza del metodo.

HTTP408: timeout della richiesta

Descrizione: indica che il client ha annullato la richiesta o non è riuscito a inviare una richiesta completa.

Causa 1: un'interruzione della rete o una costruzione errata della richiesta, ad esempio intestazioni con un formato definito solo in parte; la dimensione del contenuto specificata non corrisponde alla dimensione del contenuto effettivamente trasmessa e così via.

Soluzione 1: ispeziona il codice da cui proviene la richiesta e prova a inviarlo direttamente alle tue istanze registrate (o un ambiente di sviluppo/test) in cui disponi di maggiore controllo per l'ispezione della richiesta effettiva.

Causa 2: la connessione al client è chiusa (il load balancer non ha potuto inviare una risposta)

Soluzione 2: verifica che il client non stia chiudendo la connessione prima che una risposta venga inviata utilizzando uno sniffer di pacchetto sul computer da cui proviene la richiesta.

HTTP502: gateway non valido

Descrizione: indica che il load balancer non è riuscito ad analizzare la risposta inviata da un'istanza registrata.

Causa: l'istanza ha inviato una risposta in formato errato o è possibile che si sia verificato un problema con il load balancer.

Soluzione: verifica che la risposta inviata dall'istanza sia conforme alle HTTP specifiche. Rivolgiti al CentroAWS Supportper ricevere assistenza.

HTTP503: Servizio non disponibile

Descrizione: indica che l'errore è causato dal load balancer o dalle istanze registrate.

Causa 1: il load balancer dispone di una capacità insufficiente per gestire la richiesta.

Soluzione 1: questo problema dovrebbe essere transitorio e non dovrebbe durare più di pochi minuti. Se persiste, rivolgiti al CentroAWS Supportper ricevere assistenza.

Causa 2: non è presente alcuna istanza registrata.

Soluzione 2: registra almeno un'istanza in ogni zona di disponibilità in cui il load balancer è configurato per rispondere. Verifica ciò esaminando le `HealthyHostCount` metriche in. CloudWatch Se non sei in grado di assicurare che un'istanza sia registrata in ogni zona di disponibilità, ti consigliamo di abilitare il bilanciamento del carico in più zone. Per ulteriori informazioni, consulta Configura il load balancer tra zone per il Classic Load Balancer.

Causa 3: non è presente alcuna istanza integra.

Soluzione 3: verifica di disporre di istanze integre in ogni zona di disponibilità in cui il load balancer è configurato per rispondere. Verifica questo dettaglio osservando il parametro `HealthyHostCount`.

Causa 4: la coda è piena.

Soluzione 4: assicurati che le istanze abbiano la capacità sufficiente per gestire la richiesta. Verifica questo dettaglio osservando il parametro `SpilloverCount`.

HTTP504: timeout del gateway

Descrizione: indica che il load balancer ha chiuso una connessione perché una richiesta non è stata completata entro il periodo di timeout di inattività.

Causa 1: per poter rispondere, l'applicazione richiede più tempo rispetto al timeout di inattività configurato.

Soluzione 1: monitorare i parametri `HTTPCode_ELB_5XX` e `Latency`. Un eventuale incremento del valore di queste parametri potrebbe essere dovuto alla mancata risposta dell'applicazione entro il periodo di timeout di inattività configurato. Per informazioni dettagliate sulle richieste in fase di timeout, abilita i log di accesso nel load balancer ed esamina i codici di risposta 504 nei log generati da Elastic Load Balancing. Se necessario, puoi aumentare la capacità o il timeout di inattività configurato in modo da poter completare le operazioni più lunghe, ad esempio il caricamento di un file di grandi dimensioni. Per ulteriori informazioni, consulta Configura il timeout per connessione inattiva per il Classic Load Balancer e Risoluzione dei problemi di latenza elevata in Elastic Load Balancing.

Causa 2: le istanze registrate chiudono la connessione a Elastic Load Balancing.

Soluzione 2: abilita le impostazioni keep-alive sulle tue EC2 istanze e assicurati che il timeout keep-alive sia maggiore delle impostazioni di timeout di inattività del tuo load balancer.

Risoluzione dei problemi di un Classic Load Balancer: parametri dei codici di risposta

Il sistema di bilanciamento del carico invia le metriche ad Amazon CloudWatch per i codici di HTTP risposta inviati ai clienti, identificando l'origine degli errori nel sistema di bilanciamento del carico o nelle istanze registrate. Puoi utilizzare le metriche restituite da CloudWatch per il tuo sistema di bilanciamento del carico per risolvere i problemi. Per ulteriori informazioni, consulta CloudWatch metriche per il tuo Classic Load Balancer.

Di seguito sono riportate le metriche del codice di risposta restituite da CloudWatch per il sistema di bilanciamento del carico, le cause potenziali e i passaggi che è possibile eseguire per risolvere i problemi.

Parametri dei codici di risposta

- HTTPCode_ _4XX ELB
- HTTPCode_ _5XX ELB

- HTTPCode_Backend_2xx
- HTTPCode_Backend_3xx
- HTTPCode_Backend_4xx
- HTTPCode_Backend_5xx

HTTPCode_ _4XX ELB

Causa: una richiesta in formato errato o annullata dal client.

Soluzioni

- Per informazioni, consulta HTTP400: BAD _ REQUEST.
- Per informazioni, consulta HTTP405: METHOD _ _ NOT ALLOWED.
- Per informazioni, consulta HTTP408: timeout della richiesta.

HTTPCode_ _5XX ELB

Causa: il load balancer o l'istanza registrata sta causando l'errore o il load balancer non è in grado di analizzare la risposta.

Soluzioni

- Per informazioni, consulta HTTP502: gateway non valido.
- Per informazioni, consulta HTTP503: Servizio non disponibile.
- Per informazioni, consulta HTTP504: timeout del gateway.

HTTPCode_Backend_2xx

Causa: una normale risposta di esito positivo inviata dalle istanze registrate.

Soluzione: nessuna.

HTTPCode_Backend_3xx

Causa: una risposta di reindirizzamento inviata dalle istanze registrate.

Soluzione: visualizza i log di accesso o i log di errore relativi alla tua istanza per determinare la causa. Invia le richieste direttamente all'istanza (ignorando il load balancer) per visualizzare le risposte.

HTTPCode_Backend_4xx

Causa: una risposta di errore del client inviata dalle istanze registrate.

Soluzione: visualizza i log di accesso o i log di errore relativi alle tue istanze per determinare la causa. Invia le richieste direttamente all'istanza (ignorando il load balancer) per visualizzare le risposte.

> **Note**
>
> Se il client annulla una HTTP richiesta iniziata con un'`Transfer-Encoding: chunked`intestazione, esiste un problema noto per cui il load balancer inoltra la richiesta all'istanza anche se il client l'ha annullata. Questo comportamento può provocare errori di back-end.

HTTPCode_Backend_5xx

Causa: una risposta di errore del server inviata dalle istanze registrate.

Soluzione: visualizza i log di accesso o i log di errore relativi alle tue istanze per determinare la causa. Invia le richieste direttamente all'istanza (ignorando il load balancer) per visualizzare le risposte.

> **Note**
>
> Se il client annulla una HTTP richiesta iniziata con un'`Transfer-Encoding: chunked`intestazione, esiste un problema noto per cui il load balancer inoltra la richiesta all'istanza anche se il client l'ha annullata. Questo comportamento può provocare errori di back-end.

Risoluzione dei problemi di un Classic Load Balancer: controlli dello stato

Il load balancer controlla lo stato delle istanze registrate utilizzando la configurazione di controllo dello stato predefinita fornita da Elastic Load Balancing o una configurazione di controllo dello stato personalizzata specificata dall'utente. La configurazione di controllo dello stato contiene informazioni quali il protocollo, la porta di ping, il percorso di ping, il timeout della risposta e l'intervallo dei controlli dello stato. Un'istanza è considerata integra se restituisce un codice di risposta 200 durante l'intervallo di controllo dello stato. Per ulteriori informazioni, consulta Controlli dello stato delle istanze del tuo Classic Load Balancer.

Se lo stato attuale di alcune o di tutte le istanze è `OutOfService` e il campo descrizione mostra il messaggio `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`, le istanze non hanno superato il controllo dello stato del load balancer. Di seguito sono elencati i problemi da cercare, le potenziali cause e le operazioni che è possibile eseguire per risolverli.

Problemi

- Errore della pagina di destinazione del controllo dello stato
- Si è verificato il timeout della connessione alle istanze
- L'autenticazione della chiave pubblica non riesce
- L'istanza non riceve traffico dal load balancer
- Le porte sull'istanza non sono aperte
- Le istanze in un gruppo di Auto Scaling non superano il controllo di integrità ELB

Errore della pagina di destinazione del controllo dello stato

Problema: una HTTP GET richiesta inviata all'istanza sulla porta ping e sul percorso ping specificati (ad esempio, :80/index.html) riceve un codice di risposta diverso da 200HTTP.

Causa 1: non è stata configurata alcuna pagina di destinazione per l'istanza.

Soluzione 1: crea una pagina di destinazione (ad esempio `index.html`) per ciascuna istanza registrata e specifica il percorso come percorso di ping.

Causa 2: il valore dell'intestazione Content-Length nella risposta non è impostato.

Soluzione 2: se la risposta include un corpo, impostare l'intestazione Content-Length su un valore maggiore o uguale a zero oppure impostare il valore di Transfer-Encoding su "chunked".

Causa 3: l'applicazione non è configurata per ricevere richieste dal load balancer o per restituire un codice di risposta 200.

Soluzione 3: controlla l'applicazione sulla tua istanza per individuare la causa.

Si è verificato il timeout della connessione alle istanze

Problema: le richieste di Health Check dal sistema di bilanciamento del carico alle EC2 istanze scadono o falliscono a intermittenza.

In primo luogo, verifica il problema connettendoti direttamente all'istanza. Ti consigliamo di connetterti alla tua istanza dalla rete utilizzando l'indirizzo IP privato dell'istanza.

Usa il seguente comando per una connessione: TCP

```
telnet private-IP-address-of-the-instance port
```

Utilizzate il seguente comando per una HTTPS connessione HTTP or:

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Se si utilizza una HTTPS connessioneHTTP/e si ottiene una risposta diversa da 200, vedereErrore della pagina di destinazione del controllo dello stato. Se riesci a connetterti direttamente all'istanza, controlla quanto segue:

Causa 1: l'istanza non risponde entro il periodo di timeout di risposta configurato.

Soluzione 1: regola le impostazioni del timeout di risposta nella configurazione del controllo dello stato del load balancer.

Causa 2: l'istanza è sottoposta a un carico significativo e richiede più tempo del periodo di timeout di risposta configurato per rispondere.

Soluzione 2:

- Controlla il grafico di monitoraggio per un utilizzo eccessivo di. CPU Per informazioni, consulta Ottieni statistiche per un'EC2istanza specifica nella Amazon EC2 User Guide.

- Verifica l'utilizzo di altre risorse applicative, come memoria o limiti, collegandoti alle tue EC2 istanze.
- Se necessario, aggiungi altre istanze o abilita l'Auto Scaling. Per ulteriori informazioni, consulta la Amazon EC2 Auto Scaling User Guide.

Causa 3: se utilizzi una connessione HTTP o una HTTPS connessione e il controllo dello stato viene eseguito su una pagina di destinazione specificata nel campo del percorso di ping (ad esempio,`HTTP:80/index.html`), la pagina di destinazione potrebbe impiegare più tempo a rispondere rispetto al timeout configurato.

Soluzione 3: utilizza una pagina di destinazione del controllo dello stato più semplice o regola le impostazioni dell'intervallo del controllo dello stato.

L'autenticazione della chiave pubblica non riesce

Problema: un sistema di bilanciamento del carico configurato per utilizzare il SSL protocollo HTTPS or con l'autenticazione di back-end abilitata fallisce l'autenticazione a chiave pubblica.

Causa: la chiave pubblica sul SSL certificato non corrisponde alla chiave pubblica configurata sul load balancer. Utilizza il comando `s_client` per visualizzare l'elenco dei certificati server nella catena di certificati. Per ulteriori informazioni, consulta s_client nella documentazione di Open. SSL

Soluzione: potrebbe essere necessario aggiornare il SSL certificato. Se il SSL certificato è aggiornato, prova a reinstallarlo sul sistema di bilanciamento del carico. Per ulteriori informazioni, consulta Sostituisci il SSL certificato per il tuo Classic Load Balancer.

L'istanza non riceve traffico dal load balancer

Problema: il gruppo di sicurezza per l'istanza sta bloccando il traffico dal load balancer.

Esegui un'acquisizione di pacchetti sull'istanza per verificare il problema. Utilizza il seguente comando:

```
# tcpdump port health-check-port
```

Causa 1: il gruppo di sicurezza associato all'istanza non consente il traffico dal load balancer.

Soluzione 1: modifica il gruppo di sicurezza associato all'istanza in modo da consentire il traffico dal load balancer. Aggiungi una regola per consentire tutto il traffico dal gruppo di sicurezza del load balancer.

Causa 2: il gruppo di sicurezza del sistema di bilanciamento del carico non consente il traffico verso le istanze. EC2

Soluzione 2: modifica il gruppo di sicurezza del sistema di bilanciamento del carico per consentire il traffico verso le sottoreti e le istanze. EC2

Per informazioni sulla gestione dei gruppi di sicurezza, consulta Configurazione dei gruppi di sicurezza per Classic Load Balancer.

Le porte sull'istanza non sono aperte

Problema: il controllo di integrità inviato all'EC2istanza dal load balancer è bloccato dalla porta o da un firewall.

Verifica il problema utilizzando il seguente comando:

```
netstat –ant
```

Causa: la porta del controllo dello stato o la porta listener specificata (se configurata in modo diverso) non è aperta. Sia la porta specificata per il controllo dello stato che la porta listener devono essere aperte e in ascolto.

Soluzione: apri la porta listener e la porta specificata nella configurazione del controllo dello stato (se configurata diversamente) sulle tue istanze per ricevere il traffico del load balancer.

Le istanze in un gruppo di Auto Scaling non superano il controllo di integrità ELB

Problema: le istanze del gruppo Auto Scaling superano il controllo di integrità predefinito di Auto Scaling ma non lo superano. ELB

Causa: Auto Scaling utilizza controlli di EC2 stato per rilevare problemi hardware e software con le istanze, ma il load balancer esegue controlli di integrità inviando una richiesta all'istanza e aspettando un codice di risposta di 200 oppure stabilendo una TCP connessione (per un controllo dello stato TCP basato) con l'istanza.

Un'istanza potrebbe non superare il controllo di ELB integrità perché un'applicazione in esecuzione sull'istanza presenta problemi che inducono il sistema di bilanciamento del carico a considerare l'istanza fuori servizio. Questa istanza potrebbe superare il controllo di integrità di Auto Scaling; non

verrebbe sostituita dalla politica Auto Scaling perché è considerata integra in base EC2 al controllo dello stato.

Soluzione: utilizzate il controllo ELB dello stato del vostro gruppo Auto Scaling. Quando si utilizza il ELB controllo dello stato dell'istanza, Auto Scaling determina lo stato di integrità delle istanze controllando i risultati sia del controllo dello stato dell'istanza che del controllo dello stato dell'ELBistanza. Per ulteriori informazioni, consulta Aggiungere controlli di integrità al gruppo Auto Scaling nella Amazon Auto EC2 Scaling User Guide.

Risoluzione dei problemi di un Classic Load Balancer: connettività client

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 ha un percorso verso il gateway Internet per il tuo cloud privato virtuale (). VPC

Un gruppo o una rete di sicurezza ACL 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. Per ulteriori informazioni, consulta Configurazione dei gruppi di sicurezza per Classic Load Balancer.

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 riferisce il nome del sistema di bilanciamento del carico utilizzando un'interfaccia a riga di comandoDNS.
- Confronta i risultati dei due output. Gli indirizzi IP devono corrispondere.

HTTPSIe richieste inviate al sistema di bilanciamento del carico restituiscono "NET:: ERR _ _ _» CERT COMMON NAME INVALID

Se vengono HTTPS ricevute richieste `NET::ERR_CERT_COMMON_NAME_INVALID` dal sistema di bilanciamento del carico, verifica le seguenti possibili cause:

- Il nome di dominio utilizzato nella HTTPS richiesta non corrisponde al nome alternativo specificato nel certificato associato al listener. ACM
- Viene utilizzato il DNS nome predefinito del sistema di bilanciamento del carico. Il DNS nome predefinito non può essere utilizzato per effettuare HTTPS richieste poiché non è possibile richiedere un certificato pubblico per il `*.amazonaws.com` dominio.

Risoluzione dei problemi di un Classic Load Balancer: registrazione dell'istanza

Quando registri un'istanza nel tuo load balancer, devi eseguire una serie di operazioni perché il load balancer sia in grado di iniziare a inviare le richieste alla tua istanza.

Di seguito sono riportati i problemi che il sistema di bilanciamento del carico potrebbe riscontrare durante la registrazione EC2 delle istanze, le possibili cause e i passaggi da intraprendere per risolverli.

Problemi

- La registrazione di un'istanza richiede troppo tempo EC2

- Impossibile registrare un'istanza avviata da un'istanza a pagamento AMI

La registrazione di un'istanza richiede troppo tempo EC2

Problema: EC2 le istanze registrate impiegano più tempo del previsto per essere disponibili nello `InService` stato.

Causa: è possibile che il controllo dello stato dell'istanza abbia avuto esito negativo. Dopo il completamento della procedura iniziale di registrazione dell'istanza (che può richiedere fino a circa 30 secondi), il load balancer inizia a inviare richieste di controllo dello stato. L'istanza non risulta `InService` finché un controllo dello stato non ha esito positivo.

Soluzione: consulta Si è verificato il timeout della connessione alle istanze.

Impossibile registrare un'istanza avviata da un'istanza a pagamento AMI

Problema: Elastic Load Balancing non registra un'istanza avviata utilizzando un'istanza a pagamento. AMI

Causa: le tue istanze potrebbero essere state avviate utilizzando un servizio a pagamento AMI di Amazon DevPay.

Soluzione: Elastic Load Balancing non supporta la registrazione di istanze avviate utilizzando Amazon a pagamento. AMIs DevPay Tieni presente che puoi utilizzare la versione a pagamento AMIs di AWS Marketplace. Se stai già utilizzando un modulo a pagamento AMI Marketplace AWS e non riesci a registrare un'istanza avviata da quel modulo a pagamentoAMI, rivolgiti al AWS Support Centro per ricevere assistenza.

Quote per il Classic 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.

Per visualizzare le quote per i Classic Load Balancer, aprire 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.

Il tuo AWS account ha le seguenti quote relative ai Classic Load Balancers.

Nome	Predefinita	Adattabile
Classic Load Balancer per regione	20	Sì
Listener per Classic Load Balancer	100	Sì
Istanze registrate per Classic Load Balancer	1.000	Sì

Cronologia dei documenti per Classic Load Balancer

La tabella seguente descrive le release dei Classic Load Balancer.

Modifica	Descrizione	Data
Modalità di mitigazione della desincronizzazione	Aggiunto il supporto per la modalità di attenuazione della desincronizzazione. Per ulteriori informazioni, consulta Configurare la modalità di mitigazione della desincronizzazione per Classic Load Balancer.	17 agosto 2020
Classic Load Balancer	Con l'introduzione degli Application Load Balancer e dei Network Load Balancer, i load balancer creati con il 01/06/2016 API sono ora noti come Classic Load Balancer. Per ulteriori informazioni sulle differenze tra questi tipi di sistemi di bilanciamento del carico, consulta le funzionalità di Elastic Load Balancing.	11 agosto 2016
Support per AWS Certificate Manager (ACM)	Puoi richiedere un TLS certificatoSSL/ACMe distribuirlo sul tuo sistema di bilanciamento del carico. Per ulteriori informazioni, consulta SSL/TLScertificates for Classic Load Balancers.	21 gennaio 2016
Support per porte aggiuntive	I sistemi di bilanciamento del carico possono ascoltare su	15 settembre 2015

	qualsiasi porta nell'intervallo 1-65535. Per ulteriori informazioni, consulta Listeners for your Classic Load Balancer.	
Campi aggiuntivi per le voci del registro di accesso	Aggiunti i campi `user_agent` , `ssl_cipher` e `ssl_protocol` . Per ulteriori informazioni, consulta Access log files.	18 maggio 2015
Support per l'etichettatura del sistema di bilanciamento del carico	A partire da questa versione, Elastic Load Balancing CLI (ELBCLI) è stato sostituito da AWS Command Line Interface (AWS CLI), uno strumento unificato per gestire più servizi. AWS Le nuove funzionalità rilasciate dopo la ELB CLI versione 1.0.35.0 (datata 24/07/14) saranno incluse nell'unica. AWS CLI Se attualmente utilizzi il ELBCLI, ti consigliamo di iniziare a utilizzare invece il. AWS CLI Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface .	11 agosto 2014
Timeout della connessione inattiva	Puoi configurare il tempo di inattività della connessione per il sistema di bilanciamento del carico.	24 luglio 2014

Support per concedere a utenti e gruppi l'accesso a specifici sistemi di bilanciamento del carico o azioni API	È possibile creare una politica per concedere a utenti e gruppi l'accesso a specifici sistemi di bilanciamento del carico o azioni. API	12 maggio 2014
Support per AWS CloudTrail	È possibile utilizzare CloudTrail per acquisire API le chiamate effettuate da o per conto dell'utente Account AWS utilizzando il ELB API AWS Management Console, il ELBCLI, o il AWS CLI. Per ulteriori informazioni, consulta Registrazione delle API chiamate per l'utilizzo di Classic Load AWS CloudTrail Balancer.	4 aprile 2014
Drenaggio della connessione	Aggiunte le informazioni relative a connection draining. Con questo supporto puoi configurare il load balancer per interrompere l'invio di nuove richieste all'istanza registrata durante l'annullamento della registrazione dell'istanza o quando l'istanza diventa non integra, mantenendo le connessioni esistenti aperte. Per ulteriori informazioni, consulta Configurare il drenaggio della connessione per Classic Load Balancer.	20 marzo 2014

Registri di accesso	Puoi abilitare il tuo sistema di bilanciamento del carico per acquisire informazioni dettagliate sulle richieste inviate al sistema di bilanciamento del carico e archiviarle in un bucket Amazon S3. Per ulteriori informazioni, consulta Access logs for Classic Load Balancer.	6 marzo 2014
Support per TLSv1 1.1-1.2	Sono state aggiunte informazioni sul supporto del TLSv1 protocollo.1-1.2 per i sistemi di bilanciamento del carico configurati con/listener. HTTPS SSL Con questo supporto, Elastic Load Balancing aggiorna anche le configurazioni di negoziazione predefiniteSSL. Per informazioni sulle configurazioni di negoziazione predefinite aggiornate, SSL consulta le configurazioni di SSL negoziazione per Classic Load Balancers. Per informazioni sull'aggiornamento della configurazione di SSL negoziazione corrente, consulta SSLAggiornare la configurazione di negoziazione del Classic Load Balancer.	19 febbraio 2014

Bilanciamento del carico su più zone	Aggiunte le informazioni relative all'abilitazione del bilanciamento del carico tra zone per il load balancer. Per ulteriori informazioni, consulta Configurare il bilanciamento del carico tra zone per Classic Load Balancer.	6 Novembre 2013
Metriche aggiuntive CloudWatch	Aggiunte le informazioni relative ai parametri Cloudwatch aggiuntivi segnalati da Elastic Load Balancing. Per ulteriori informazioni, consulta le CloudWatch metriche per il tuo Classic Load Balancer.	28 Ottobre 2013
Support per il protocollo proxy	Sono state aggiunte informazioni sul supporto del protocollo proxy per i sistemi di bilanciamento del carico configurati per le connessioni TCP SSL /. Per ulteriori informazioni, vedere Proxy protocol header.	30 luglio 2013
Support per il DNS failover	Sono state aggiunte informazioni sulla configurazione del DNS failover di Amazon Route 53 per i sistemi di bilanciamento del carico. Per ulteriori informazioni, consulta Usare il DNS failover di Amazon Route 53 per il bilanciamento del carico.	3 giugno 2013

Supporto da console per la visualizzazione delle CloudWatch metriche e la creazione di allarmi	Sono state aggiunte informazioni sulla visualizzazione delle CloudWatch metriche e sulla creazione di allarmi per uno specifico sistema di bilanciamento del carico tramite la console. Per ulteriori informazioni, consulta le CloudWatch metriche per il tuo Classic Load Balancer.	28 marzo 2013
Support per la registrazione delle EC2 istanze in modo predefinito VPC	È stato aggiunto il supporto per EC2 le istanze avviate come impostazione predefinita. VPC	11 marzo 2013
Bilanciatori di carico interni	Con questa versione, è possibile creare un sistema di bilanciamento del carico in un cloud privato virtuale (VPC) interno o rivolto a Internet. Un load balancer interno ha un DNS nome risolvibile pubblicamente che si risolve in indirizzi IP privati. Un sistema di bilanciamento del carico connesso a Internet ha un nome risolvibile pubblicamente che si risolve in indirizzi IP pubblici. DNS Per ulteriori informazioni, consulta Creare un Classic Load Balancer interno.	10 giugno 2012

Supporto da console per la gestione dei listener, delle impostazioni di cifratura e dei certificati SSL	Per informazioni, consulta Configurare un HTTPS listener per il Classic Load Balancer e Sostituire SSL il certificato per il Classic Load Balancer.	18 maggio 2012
Supporto per Elastic Load Balancing in Amazon VPC	È stato aggiunto il supporto per la creazione di un sistema di bilanciamento del carico in un cloud privato virtuale ()VPC.	21 Novembre 2011
Amazon CloudWatch	Puoi monitorare il tuo sistema di bilanciamento del carico utilizzando CloudWatch. Per ulteriori informazioni, consulta le CloudWatch metriche per il tuo Classic Load Balancer.	17 ottobre 2011
Funzionalità di sicurezza aggiuntive	È possibile configurare SSL cifrari, back-end e autentica zione del server di back-endS SL. Per ulteriori informazioni, consulta Creare un Classic Load Balancer con un HTTPS listener.	30 agosto 2011
Nome di dominio Zone Apex	Per ulteriori informazioni, consulta Configurare un nome di dominio personalizzato per Classic Load Balancer.	24 maggio 2011

Support per gli header X-Forwarded-Proto e X-Forwarded-Port	L'intestazione X-Forwarded-Proto indica il protocollo della richiesta iniziale e l'intestazione X-Forwarded-Port indica la porta dell'intestazione della richiesta iniziale. L'aggiunta di queste intestazioni alle richieste consente ai clienti di determinare se una richiesta in entrata al load balancer è crittografata e la porta specifica sul load balancer su cui è stata ricevuta la richiesta. Per ulteriori informazioni, consulta HTTPheader e Classic Load Balancers.	27 Ottobre 2010
Support per HTTPS	Con questa versione, è possibile sfruttare il TLS protocolloSSL/per crittografare il traffico e trasferire l'SSLelaborazione del carico dall'istanza dell'applicazione al sistema di bilanciamento del carico. Questa funzionalità fornisce anche la gestione centralizzata dei certificati del SSL server tramite il sistema di bilanciamento del carico, anziché gestire i certificati su singole istanze dell'applicazione.	14 Ottobre 2010
Support per AWS Identity and Access Management (IAM)	Aggiunto supporto per IAM.	2 settembre 2010

Sessioni permanenti	Per ulteriori informazioni, consulta Configurare le sessioni permanenti per Classic Load Balancer.	7 aprile 2010
AWS SDK for Java	È stato aggiunto il supporto SDK per Java.	22 marzo 2010
AWS SDK for .NET	È stato aggiunto il supporto per AWS SDK for .NET.	11 Novembre 2009
Nuovo servizio	Versione beta pubblica iniziale di Elastic Load Balancing.	18 maggio 2009

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.