



Guida per l'utente

Elastic Load Balancing



Elastic Load Balancing: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Cos'è l'Elastic Load Balancing?	1
Vantaggi del sistema di bilanciamento del carico	1
Funzionalità di Elastic Load Balancing	1
Accesso a Elastic Load Balancing	2
Servizi correlati	2
Prezzi	3
Funzionamento di Elastic Load Balancing	4
Zone di disponibilità e nodi del sistema di bilanciamento del carico	4
Bilanciamento del carico su più zone	5
Spostamento zonale	8
Instradamento della richiesta	8
Algoritmo di instradamento	9
Connessioni HTTP	10
Intestazioni HTTP	11
Limiti delle intestazioni HTTP	12
Schema del sistema di bilanciamento del carico	12
Tipi di indirizzi IP	13
MTU rete	14
Nozioni di base	16
Sicurezza	17
Protezione dei dati	18
Crittografia dei dati a riposo	19
Crittografia dei dati in transito	19
Gestione dell'identità e degli accessi	19
Destinatari	20
Autenticazione con identità	20
Gestione dell'accesso tramite policy	22
Funzionamento di Elastic Load Balancing con IAM	23
Autorizzazioni API per il tag delle risorse	35
Ruolo collegato al servizio	38
AWS politiche gestite	39
Convalida della conformità	41
Resilienza	42
Sicurezza dell'infrastruttura	42

Isolamento della rete	43
Controllo del traffico di rete	43
AWS PrivateLink	44
Creazione di un endpoint di interfaccia per Elastic Load Balancing	45
Creazione di una policy degli endpoint VPC per Elastic Load Balancing	45
Limitazione (della larghezza di banda della rete) delle richieste API	47
Come viene applicato il throttling	47
Limitazione del tasso di richiesta	47
Richiedi le dimensioni dei bucket di token e le tariffe di ricarica	48
Monitoraggio delle richieste API	52
Report di fatturazione e utilizzo	53
Application Load Balancer	53
Network Load Balancers	54
Gateway Load Balancers	54
Classic Load Balancer	54
Registrazione dei log di chiamate API	56
Eventi di gestione Elastic Load Balancing in CloudTrail	57
Esempi di eventi Elastic Load Balancing	58
Migrazione di Classic Load Balancer	62
Vantaggi della migrazione	62
Procedura guidata di migrazione	63
Migrazione dell'utilità di copia	65
Migrazione manuale	65
Impedisci agli utenti di creare Classic Load Balancer	68
.....	lxx

Cos'è l'Elastic Load Balancing?

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 dimensiona la capacità del sistema di bilanciamento del carico in risposta al traffico in entrata.

Vantaggi del sistema di bilanciamento del carico

Un sistema di bilanciamento del carico distribuisce i carichi di lavoro su più risorse di calcolo, ad esempio server virtuali. L'utilizzo di un sistema di bilanciamento del carico aumenta la disponibilità e la tolleranza ai guasti delle applicazioni.

È possibile aggiungere e rimuovere le risorse di calcolo dal sistema di bilanciamento del carico in base alle proprie esigenze, senza interrompere il flusso di richieste per le applicazioni.

È possibile configurare controlli dello stato, che monitorano lo stato delle risorse di calcolo in modo che il sistema di bilanciamento del carico invii le richieste solo a quelle integre. È inoltre possibile rimuovere il lavoro di crittografia e decrittazione dal tuo sistema di bilanciamento del carico, in modo che le risorse di calcolo possano concentrarsi sul loro compito principale.

Funzionalità di Elastic Load Balancing

Elastic Load Balancing supporta diversi tipi di load balancer. È possibile selezionare il tipo di load balancer più adatto alle proprie esigenze. Per ulteriori informazioni, consulta [Elastic Load Balancing features](#) Balancing Products.

Per ulteriori informazioni sui sistemi di bilanciamento del carico di ultima generazione, consulta la seguente documentazione:

- [Guida per l'utente dei sistemi Application Load Balancer](#)
- [Guida per l'utente dei sistemi Network Load Balancer](#)
- [Guida per l'utente di Gateway Load Balancer](#)

I Classic Load Balancer sono la generazione precedente di bilanciatori del carico dal bilanciamento del carico elastico. Consigliamo di eseguire la migrazione a un bilanciatore del carico di generazione attuale. Per ulteriori informazioni, consultare [Migrate your Classic Load Balancer](#).

Accesso a Elastic Load Balancing

È possibile creare, avere accesso e gestire i sistemi di bilanciamento del carico utilizzando le seguenti interfacce:

- Console di gestione AWS— Fornisce un'interfaccia Web che è possibile utilizzare per accedere a Elastic Load Balancing.
- AWS Command Line Interface (AWS CLI): fornisce comandi per un'ampia gamma di AWS servizi, tra cui Elastic Load Balancing. AWS CLI È supportato su Windows, macOS e Linux. Per ulteriori informazioni, consulta [AWS Command Line Interface](#).
- AWS SDKs— Fornisci informazioni specifiche per la lingua APIs e gestisci molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta [AWS SDKs](#).
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'utilizzo dell'API di query è il modo più diretto di accedere a Elastic Load Balancing. Tuttavia, l'API di query richiede che l'applicazione gestisca dettagli di basso livello, come la generazione dell'hash per firmare la richiesta e la gestione degli errori. Per ulteriori informazioni, consulta gli argomenti seguenti:
 - [Application Load Balancer, Network Load Balancer e Gateway Load Balancer — versione API 2015-12-01](#)
 - Classic Load Balancer: [API versione 2012-06-01](#)

Servizi correlati

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

- Amazon EC2: server virtuali che eseguono le tue applicazioni nel cloud. Puoi configurare il tuo sistema di bilanciamento del carico per indirizzare il traffico verso le tue EC2 istanze. Per ulteriori informazioni, consulta la [Amazon EC2 User Guide](#).
- Amazon EC2 Auto Scaling: assicura l'esecuzione del numero desiderato di istanze, anche in caso di guasto di un'istanza. Amazon EC2 Auto Scaling consente inoltre di aumentare o

diminuire automaticamente il numero di istanze al variare della domanda delle istanze. Se si attiva Dimensionamento automatico con Elastic Load Balancing, le istanze avviate da Dimensionamento automatico vengono registrate automaticamente nel sistema di bilanciamento del carico.

Analogamente, il sistema di bilanciamento del carico annulla automaticamente la registrazione delle istanze terminate da Dimensionamento automatico. Per ulteriori informazioni, consulta la [Amazon EC2 Auto Scaling User Guide](#).

- AWS Certificate Manager: durante la creazione di un ascoltatore HTTPS, è possibile specificare i certificati forniti da ACM. Il sistema di bilanciamento del carico utilizza i certificati per terminare le connessioni e decriptare le richieste dei client.
- Amazon CloudWatch: consente di monitorare il sistema di bilanciamento del carico e di intervenire secondo necessità. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- Amazon ECS: consente di eseguire, arrestare e gestire contenitori Docker su un cluster di EC2 istanze. È possibile configurare il sistema di bilanciamento del carico per instradare il traffico sui propri contenitori. Per ulteriori informazioni, consulta la [Guida per lo sviluppatore di Amazon Elastic Container](#).
- AWS Global Accelerator: migliora la disponibilità e le prestazioni dell'applicazione. Utilizza un acceleratore per distribuire il traffico su più sistemi di bilanciamento del carico in una o più regioni. AWS Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di AWS Global Accelerator](#).
- Route 53: offre un modo affidabile e conveniente per instradare i visitatori sui siti Web tramite la traduzione dei nomi dei domini negli indirizzi IP numerici che i computer utilizzano per connettersi tra loro. Ad esempio, si tradurrebbe `www.example.com` nell'indirizzo IP numerico `192.0.2.1`. AWS URLs assegna alle tue risorse, come i sistemi di bilanciamento del carico. Tuttavia, è possibile impostare un URL semplice da ricordare. Ad esempio, è possibile mappare il nome di dominio a un sistema di bilanciamento del carico. Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di Amazon Route 53](#).
- AWS WAF— È possibile utilizzarlo AWS WAF con Application Load Balancer per consentire o bloccare le richieste in base alle regole di una lista di controllo degli accessi Web (Web ACL). Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di AWS WAF](#).

Prezzi

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

Funzionamento di Elastic Load Balancing

Un sistema di bilanciamento del carico accetta il traffico in entrata dai client e indirizza le richieste verso le destinazioni registrate (ad esempio le EC2 istanze) in una o più zone di disponibilità. Il sistema di bilanciamento del carico monitora inoltre lo stato delle destinazioni registrate e garantisce che il traffico venga instradato solo verso quelle integre. Quando il sistema di bilanciamento del carico rileva una destinazione non integra, ne interrompe il traffico in entrata. Riprende quindi l'instradamento del traffico verso la destinazione quando ne rileva nuovamente l'integrità.

Puoi configurare il tuo sistema di bilanciamento del carico affinché accetti il traffico in entrata specificando uno o più listener. Si definisce listener il processo che verifica la presenza di richieste di connessione. È configurato con un protocollo e con un numero di porta per le connessioni dai client al sistema di bilanciamento del carico. Allo stesso modo, è configurato con un protocollo e con un numero di porta per le connessioni dal sistema di bilanciamento del carico alle destinazioni.

Indice

- [Zone di disponibilità e nodi del sistema di bilanciamento del carico](#)
- [Instradamento della richiesta](#)
- [Schema del sistema di bilanciamento del carico](#)
- [Tipi di indirizzi IP](#)
- [MTU rete per il sistema di bilanciamento del carico](#)

Zone di disponibilità e nodi del sistema di bilanciamento del carico

Quando si abilita una zona di disponibilità nel sistema di bilanciamento del carico, Elastic Load Balancing crea un nodo del sistema di bilanciamento del carico nella zona di disponibilità. Se registri le destinazioni in una zona di disponibilità, ma non abiliti la zona, queste destinazioni registrate non sono in grado di ricevere traffico. Il sistema di bilanciamento del carico è più efficace se ogni zona di disponibilità abilitata dispone di almeno una destinazione registrata.

Consigliamo di abilitare più zone di disponibilità per tutti i sistemi di bilanciamento del carico. Tuttavia, con un Application Load Balancer, è obbligatorio abilitare almeno due o più zone di disponibilità. Questa configurazione aiuta a verificare che il sistema di bilanciamento del carico possa continuare a instradare il traffico. Se una zona di disponibilità non è più disponibile o non ha destinazioni integre, il sistema di bilanciamento del carico è in grado di instradare il traffico verso le destinazioni integre in un'altra zona di disponibilità.

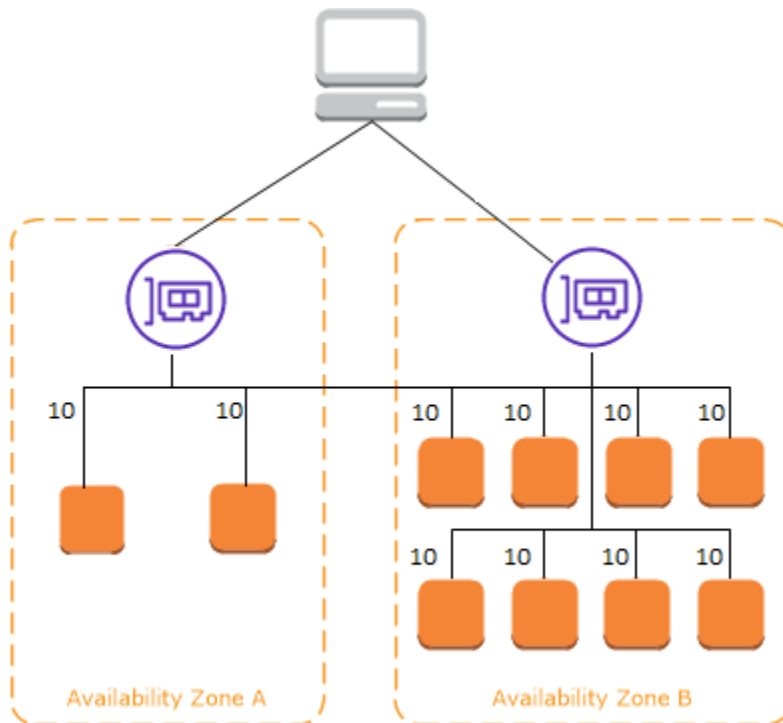
Dopo aver disabilitato un'area di disponibilità, le destinazioni in tale zona di disponibilità rimangono registrate con il sistema di bilanciamento del carico. Tuttavia, anche se rimangono registrate, il sistema di bilanciamento del carico non vi instrada alcun traffico.

Bilanciamento del carico su più zone

I nodi del sistema di bilanciamento del carico distribuiscono le richieste dei client alle destinazioni registrate. Se il bilanciamento del carico tra zone è abilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico tra le destinazioni registrate in tutte le zone di disponibilità abilitate. Se il bilanciamento del carico tra zone è disabilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella sua zona di disponibilità.

I seguenti diagrammi illustrano l'effetto del bilanciamento del carico tra zone con round robin come algoritmo di instradamento predefinito. Sono presenti due zone di disponibilità abilitate, con due destinazioni nella zona A e otto nella zona B. I client inviano le richieste, a ciascuna delle quali Amazon Route 53 risponde con l'indirizzo IP di uno dei nodi del sistema di bilanciamento del carico. In base all'algoritmo di instradamento round robin, il traffico viene distribuito in modo tale che ciascun nodo del sistema di bilanciamento del carico riceva il 50% del traffico dai client. Ogni nodo del sistema di bilanciamento del carico distribuisce la sua parte di traffico tra le destinazioni registrate nel relativo ambito.

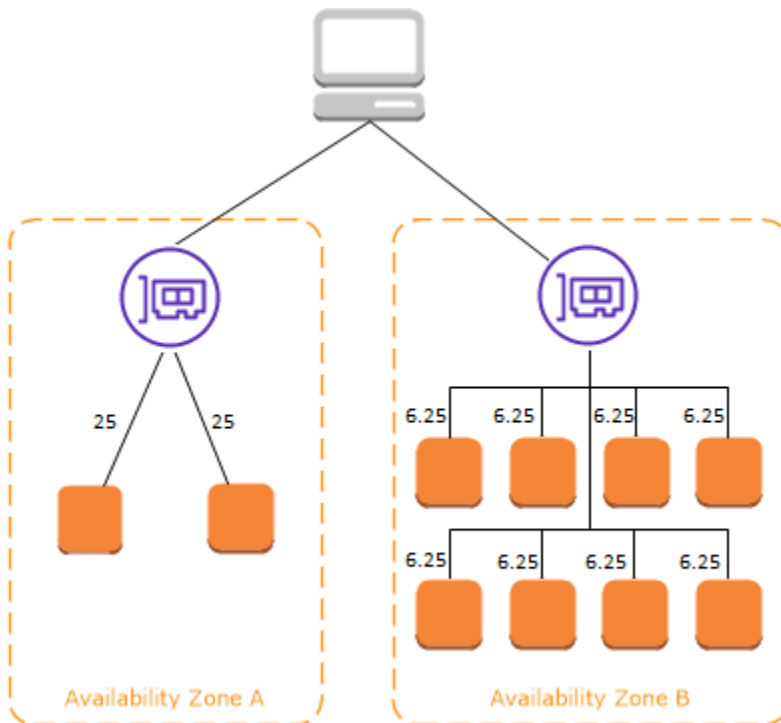
Se il bilanciamento del carico tra zone è abilitato, ciascuna delle 10 destinazioni riceve il 10% del traffico. Questo perché ogni nodo del sistema di bilanciamento del carico è in grado di instradare il 50% del traffico dei client verso tutte e 10 le destinazioni.



Se il bilanciamento del carico tra zone è disabilitato:

- Ciascuna delle due destinazioni nella zona di disponibilità A riceve il 25% del traffico.
- Ciascuna delle otto destinazioni nella zona di disponibilità B riceve il 6.25% del traffico.

Questo perché ogni nodo del sistema di bilanciamento del carico è in grado di instradare il 50% del traffico dei client solo verso le destinazioni nella sua zona di disponibilità.



Con gli Application Load Balancer, il bilanciamento del carico tra zone è sempre abilitato a livello di sistema di bilanciamento del carico. A livello di gruppo di destinazioni, il bilanciamento del carico tra zone può essere disabilitato. Per ulteriori informazioni, consulta [Disattivazione del bilanciamento del carico tra zone](#) nella Guida per l'utente dei sistemi Application Load Balancer.

Con i Network Load Balancer e i Gateway Load Balancer, il bilanciamento del carico tra zone è disabilitato per impostazione predefinita. Dopo aver creato il sistema di bilanciamento del carico, è possibile abilitare o disabilitare il bilanciamento del carico tra zone in qualsiasi momento. Per ulteriori informazioni, consulta [Bilanciamento del carico tra zone nella Guida per l'utente di Network Load Balancers](#).

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'API o la CLI, il load balancer tra zone è disabilitato per impostazione predefinita. Con Console di gestione AWS, 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. Per ulteriori informazioni, consulta [Abilita il bilanciamento del carico tra zone](#) nella Guida per l'utente dei sistemi Classic Load Balancer.

Spostamento zonale

Lo spostamento di zona è una funzionalità di Amazon Application Recovery Controller (ARC) (ARC). Con lo spostamento zonale, è possibile spostare una risorsa di un sistema di bilanciamento del carico da una zona di disponibilità danneggiata con una singola operazione. In questo modo è possibile continuare a operare da altre zone di disponibilità integre in una Regione AWS.

Quando si avvia uno spostamento zonale, il sistema di bilanciamento del carico interrompe l'invio di traffico per la risorsa alla zona di disponibilità danneggiata. ARC crea immediatamente lo spostamento zonale. Tuttavia, il completamento delle connessioni esistenti e in corso nella zona di disponibilità danneggiata può richiedere un po' di tempo, generalmente fino a qualche minuto. Per ulteriori informazioni, consulta [How a zonal shift: controlli di integrità e indirizzi IP zonali](#) nella Amazon Application Recovery Controller (ARC) Developer Guide.

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

- Lo spostamento zonale è supportato quando si utilizza un Network Load Balancer con il bilanciamento del carico tra zone attivato o disattivato.
- È possibile avviare uno spostamento zonale per uno specifico sistema di bilanciamento del carico solo per una singola zona di disponibilità. Non è possibile avviare uno spostamento zonale per più zone di disponibilità.
- AWS rimuove in modo proattivo gli indirizzi IP del sistema di bilanciamento del carico zonale dal DNS quando più problemi di infrastruttura influiscono sui servizi. Verificare sempre l'attuale capacità della zona di disponibilità prima di avviare uno spostamento zonale. Se i sistemi di bilanciamento del carico hanno il bilanciamento del carico tra zone disattivato e si utilizza uno spostamento zonale per rimuovere l'indirizzo IP zonale di un sistema di bilanciamento del carico, anche la zona di disponibilità coinvolta nello spostamento zonale perderà capacità di destinazione.

Per ulteriori indicazioni e informazioni, consulta le [migliori pratiche per i cambiamenti zonali in ARC](#) nella Guida per gli sviluppatori di Amazon Application Recovery Controller (ARC).

Instradamento della richiesta

Prima di inviare una richiesta al sistema di bilanciamento del carico, un client risolve il nome di dominio del sistema di bilanciamento del carico utilizzando un server DNS (Domain Name System). La voce DNS è controllata da Amazon perché i tuoi sistemi di bilanciamento del carico si trovano nel dominio `amazonaws.com`. I server DNS Amazon restituiscono al client uno o più indirizzi IP.

Questi sono gli indirizzi IP dei nodi del tuo sistema di bilanciamento del carico. Con i Network Load Balancer, Elastic Load Balancing crea un'interfaccia di rete per ogni zona di disponibilità abilitata e la utilizza per ottenere un indirizzo IP statico. Puoi scegliere di associare un indirizzo IP elastico a ogni interfaccia di rete quando crei il Network Load Balancer.

In base ai cambiamenti del traffico verso le applicazioni nel corso del tempo, Elastic Load Balancing dimensiona il sistema di bilanciamento del carico e aggiorna la voce DNS. La voce DNS specifica anche il time-to-live (TTL) di 60 secondi. Ciò aiuta a verificare che gli indirizzi IP possano essere rimappati rapidamente in risposta ai cambiamenti del traffico.

Il client determina quale indirizzo IP utilizzare per inviare le richieste al sistema di bilanciamento del carico. Il nodo del sistema di bilanciamento del carico che riceve la richiesta seleziona una destinazione registrata integra e invia la richiesta alla destinazione tramite il proprio indirizzo IP privato.

Per ulteriori informazioni, consulta [Routing del traffico a un load balancer ELB](#) nella Guida per gli sviluppatori di Amazon Route 53.

Algoritmo di instradamento

Con gli Application Load Balancer, il nodo del sistema di bilanciamento del carico che riceve la richiesta utilizza la procedura seguente:

1. Valuta le regole del listener in ordine di priorità per determinare quale regola applicare.
2. Seleziona una destinazione dal gruppo di destinazioni per l'operazione della regola utilizzando l'algoritmo di instradamento configurato per il gruppo di destinazioni. L'algoritmo di instradamento predefinito è quello round robin. L'instradamento avviene in maniera indipendente per ogni gruppo di destinazioni, anche nel caso in cui una destinazione sia registrata con più gruppi.

Con i Network Load Balancer, il nodo del sistema di bilanciamento del carico che riceve la connessione utilizza la procedura seguente:

1. Seleziona una destinazione dal gruppo di destinazioni per la regola predefinita utilizzando un algoritmo hash di flusso. Basa l'algoritmo su:
 - Il protocollo
 - L'indirizzo IP di origine e la porta di origine
 - L'indirizzo IP di destinazione e la porta di destinazione
 - Il numero di sequenza TCP

2. Instrada ogni singola connessione TCP verso una sola destinazione per tutta la durata della connessione. Le connessioni TCP da un client dispongono di diverse porte di origine e numeri di sequenza e possono essere instradate a target differenti.

Con Gateway Load Balancers, il nodo di bilanciamento del carico che riceve la connessione utilizza un algoritmo di flow hash a 5 tuple per selezionare un dispositivo di destinazione. Dopo aver stabilito un flusso, tutti i pacchetti per lo stesso flusso vengono instradati in modo coerente allo stesso dispositivo di destinazione. Il load balancer e le appliance di destinazione si scambiano traffico utilizzando il protocollo GENEVE sulla porta 6081.

Con i Classic Load Balancer, il nodo del sistema di bilanciamento del carico che riceve la richiesta seleziona un'istanza registrata come segue:

- Utilizza l'algoritmo di instradamento round robin per i listener TCP
- Utilizza l'algoritmo di instradamento delle richieste meno rilevanti per i listener HTTP e HTTPS

Connessioni HTTP

I Classic Load Balancer utilizzano le connessioni pre-aperte, ma gli Application Load Balancer non le utilizzano. Sia i Classic Load Balancer che gli Application Load Balancer utilizzano la connessione a multiplexing. Ciò significa che le richieste di più client su più connessioni front-end possono essere instradate a una determinata destinazione tramite una singola connessione back-end. La connessione a multiplexing migliora la latenza e riduce il carico per le tue applicazioni. Per evitare la connessione a multiplexing, disabilitare le intestazioni HTTP keep-alive impostando l'intestazione `Connection: close` nelle risposte HTTP.

Gli Application Load Balancer e i Classic Load Balancer supportano il protocollo HTTP pipelined sulle connessioni front-end, ma non su quelle back-end.

Gli Application Load Balancer supportano i seguenti metodi di richiesta HTTP: GET, HEAD, POST, PUT, DELETE, OPTIONS e PATCH.

Gli Application Load Balancer supportano i seguenti protocolli sulle connessioni front-end: HTTP/0.9, HTTP/1.0, HTTP/1.1 e HTTP/2. Puoi utilizzare il protocollo HTTP/2 solo con gli ascoltatori HTTPS e inviare fino a 128 richieste in parallelo utilizzando una connessione HTTP/2. Gli Application Load Balancer supportano anche gli aggiornamenti delle connessioni da HTTP a WebSockets. Tuttavia, in caso di aggiornamento della connessione, le regole e le AWS WAF integrazioni di routing del listener Application Load Balancer non sono più valide.

Per impostazione definita, gli Application Load Balancer utilizzano HTTP/1.1 per le connessioni back-end (da sistema di bilanciamento del carico a destinazione registrata). Tuttavia, è possibile utilizzare la versione del protocollo per inviare richieste alle destinazioni utilizzando HTTP/2 o gRPC. Per ulteriori informazioni, consulta [Versioni del protocollo](#). L'intestazione keep-alive è supportata per le connessioni back-end per impostazione predefinita. Per le richieste HTTP/1.0 dai client che non dispongono di un'intestazione host, il sistema di bilanciamento del carico genera un'intestazione host per le richieste HTTP/1.1 inviate sulle connessioni back-end. L'intestazione host contiene il nome DNS del sistema di bilanciamento del carico.

I Classic Load Balancer supportano i seguenti protocolli sulle connessioni front-end (da client a sistema di bilanciamento del carico): HTTP/0.9, HTTP/1.0 e HTTP/1.1. Utilizzano il protocollo HTTP/1.1 sulle connessioni back-end (da sistema di bilanciamento del carico a destinazione registrata). L'intestazione keep-alive è supportata per le connessioni back-end per impostazione predefinita. Per le richieste HTTP/1.0 dai client che non dispongono di un'intestazione host, il sistema di bilanciamento del carico genera un'intestazione host per le richieste HTTP/1.1 inviate sulle connessioni back-end. L'intestazione host contiene l'indirizzo IP del nodo del sistema di bilanciamento del carico.

Intestazioni HTTP

Application Load Balancer e Classic Load Balancer aggiungono automaticamente intestazioni X-Forwarded-For, X-Forwarded-Proto e X-Forwarded-Port alla richiesta.

Gli Application Load Balancer convertono i nomi host in intestazioni host HTTP in lettere minuscole prima di inviarli alle destinazioni.

Per le connessioni front-end che utilizzano HTTP/2, i nomi delle intestazioni sono in lettere minuscole. Prima che la richiesta venga inviata alla destinazione tramite HTTP/1.1, i seguenti nomi di intestazione vengono convertiti in lettere minuscole e maiuscole: X-Forwarded-For, X-Forwarded-Proto, X-Forwarded-Port, Host, X-Amzn-Trace-Id, Upgrade e Connection. Tutti gli altri nomi di intestazione sono in lettere minuscole.

Gli Application Load Balancer e i Classic Load Balancer accettano l'intestazione della connessione della richiesta in entrata del client dopo avere eseguito il proxy della risposta di nuovo al client.

Quando gli Application Load Balancer e i Classic Load Balancer che utilizzano HTTP/1.1 ricevono un'intestazione Expect 100-Continue, rispondono immediatamente con HTTP/1.1 100 Continue senza testare l'intestazione della lunghezza del contenuto. L'intestazione della richiesta Expect: 100-Continue non viene inoltrata ai relativi destinatari.

Quando utilizzano HTTP/2, gli Application Load Balancer non supportano l'intestazione Expect: 100-Continue dalle richieste client. L'Application Load Balancer non risponderà con HTTP/2 100 Continue né inoltrerà questa intestazione alle destinazioni.

Limiti delle intestazioni HTTP

I seguenti limiti di dimensione per gli Application Load Balancer sono limiti rigidi che non possono essere modificati:

- Riga di richiesta: 16 K
- Intestazione singola: 16 K
- Intestazione della risposta intera: 32 K
- Intestazione della richiesta intera: 64 K

Schema del sistema di bilanciamento del carico

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 nome DNS di un load balancer connesso a Internet è pubblicamente risolvibile agli indirizzi IP pubblici dei nodi. Di conseguenza, i bilanciatori del carico connessi a Internet possono instradare le richieste dai client tramite Internet.

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

Entrambi i sistemi di bilanciamento del carico interni e connessi a Internet instradano le richieste alle destinazioni tramite indirizzi IP privati. Pertanto, le tue destinazioni non necessitano di indirizzi IP pubblici per ricevere le richieste da un sistema di bilanciamento del carico interno o connesso a Internet.

Se la tua applicazione dispone di più livelli, puoi progettare un'architettura che utilizzi sia i bilanciamenti del carico interni che quelli connessi a Internet. Ad esempio, questo vale se l'applicazione utilizza server Web che devono essere connessi a Internet e server di applicazioni

connessi solo ai server Web. Crea un load balancer connesso a Internet e registra il server Web insieme ad esso. Crea un sistema di bilanciamento del carico interno e registra il server di applicazioni insieme ad esso. I server Web ricevono le richieste dal sistema di bilanciamento del carico connesso a Internet e inviano le richieste per i server di applicazioni al sistema di bilanciamento del carico interno. I server di applicazioni ricevono le richieste dal sistema di bilanciamento del carico interno.

Tipi di indirizzi IP

Il tipo di indirizzo IP specificato per il sistema di bilanciamento del carico determina il modo in cui i client possono comunicare con il sistema di bilanciamento del carico.

- **IPv4 solo:** i client comunicano utilizzando indirizzi pubblici e privati IPv4. Le sottoreti selezionate per il sistema di bilanciamento del carico devono avere IPv4 intervalli di indirizzi.
- **Dualstack:** i client comunicano utilizzando indirizzi pubblici e indirizzi privati IPv4 e indirizzi pubblici e privati IPv6. Le sottoreti selezionate per il sistema di bilanciamento del carico devono avere intervalli di indirizzi IPv4 e IPv6.
- **Dualstack senza pubblico IPv4:** i client comunicano utilizzando indirizzi pubblici e privati IPv6 e indirizzi privati IPv4. Le sottoreti selezionate per il sistema di bilanciamento del carico devono avere intervalli di indirizzi IPv6. Questa opzione non è supportata dallo schema di `internal` bilanciamento del carico.

La tabella seguente descrive i tipi di indirizzi IP supportati per ogni tipo di bilanciamento del carico.

Nuovo tipo di load balancer	IPv4 solo	Dualstack	Dualstack senza pubblico IPv4
Application Load Balancer	Sì	Sì	Sì
Network Load Balancer	Sì	Sì	No
Gateway Load Balancer	Sì	Sì	No
Classic Load Balancer	Sì	No	No

Il tipo di indirizzo IP specificato per il gruppo target determina il modo in cui il sistema di bilanciamento del carico può comunicare con le destinazioni.

- IPv4 solo: il load balancer comunica utilizzando indirizzi privati. IPv4 È necessario registrare destinazioni con IPv4 indirizzi appartenenti a un gruppo IPv4 target.
- IPv6 solo: il sistema di bilanciamento del carico comunica tramite IPv6 indirizzi. È necessario registrare destinazioni con IPv6 indirizzi appartenenti a un gruppo IPv6 target. Il gruppo target deve essere utilizzato con un sistema di bilanciamento del carico dualstack.

La tabella seguente descrive i tipi di indirizzi IP supportati per ogni protocollo del gruppo di destinazione.

Protocollo del gruppo di destinazione	IPv4 solo	IPv6 solo	
HTTP e HTTPS	Sì	Sì	
TCP	Sì	Sì	
TLS	Sì	Sì	
UDP e TCP_UDP	Sì	Sì	
GENEVE	-	-	

MTU rete per il sistema di bilanciamento del carico

L'unità massima di trasmissione (MTU) determina la dimensione, in byte, del pacchetto più grande che può essere inviato nella rete. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. I pacchetti Ethernet sono costituiti dal pacchetto o dai dati effettivi che invii e le informazioni sul sovraccarico della rete circostante. Il traffico inviato tramite un gateway Internet ha un MTU pari a 1.500. Questo significa che, se un pacchetto ha una dimensione superiore a 1.500 byte, viene frammentato per essere inviato in più pacchetti, oppure viene eliminato se nell'intestazione IP è impostato Don't Fragment.

La dimensione MTU per i nodi del sistema di bilanciamento del carico non è configurabile. I frame jumbo (9.001 MTU) sono standard nei nodi del sistema di bilanciamento del carico per Application Load Balancer, Network Load Balancer e Classic Load Balancer. I Gateway Load Balancer supportano 8.500 MTU. Per ulteriori informazioni, consulta [Unità massima di trasmissione \(MTU\)](#) nella Guida per l'utente di Gateway Load Balancer.

La MTU del percorso è la dimensione massima del pacchetto supportata nel percorso tra l'host di origine e quello ricevente. Il rilevamento della MTU del percorso (PMTUD) è utilizzato per determinare la MTU del percorso tra due dispositivi. Il rilevamento della MTU del percorso è particolarmente importante se il client o la destinazione non supporta i frame jumbo.

Se un host invia un pacchetto più grande della MTU dell'host ricevente o della MTU di un dispositivo lungo il percorso, l'host o il dispositivo ricevente elimina il pacchetto e restituisce il seguente messaggio ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (Type 3, Code 4)`. Questo indica all'host trasmittente di dividere il payload in più pacchetti più piccoli e di trasmetterli di nuovo.

Se i pacchetti più grandi della dimensione della MTU dell'interfaccia client o della destinazione continuano a essere rimossi, è probabile che il rilevamento della MTU del percorso (PMTUD) non stia funzionando. Per evitare questo, assicurarsi che il rilevamento della MTU del percorso funzioni end-to-end e di aver abilitato i frame jumbo per i client e le destinazioni. Per ulteriori informazioni su Path MTU Discovery e sull'abilitazione dei jumbo frame, consulta [Path MTU Discovery](#) nella Amazon EC2 User Guide.

Nozioni di base di Elastic Load Balancing

Elastic Load Balancing supporta diversi tipi di load balancer. È possibile selezionare il tipo di load balancer più adatto alle proprie esigenze. Per ulteriori informazioni, consulta [Elastic Load Balancing features](#) Balancing Products.

Sistemi di load balancer

- [Creare un Application Load Balancer](#)
- [Creare un Network Load Balancer](#)
- [Crea un sistema di bilanciamento del carico del gateway](#)

Per dimostrazioni di configurazioni comuni del sistema di bilanciamento del carico, consulta [Demo di Elastic Load Balancing](#).

Se disponi di un Classic Load Balancer esistente, puoi effettuare la migrazione ad Application Load Balancer o a Network Load Balancer. Per ulteriori informazioni, consulta [Migrazione di Classic Load Balancer](#).

Sicurezza in Elastic Load Balancing

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [modello di responsabilità condivisa](#) descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. Per ulteriori informazioni sui programmi di conformità che si applicano a Elastic Load Balancing, consulta [AWS i servizi nell'ambito del programma di conformità, i servizi nell'ambito del programma AWS di conformità](#), .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Elastic Load Balancing. Viene illustrato come configurare Elastic Load Balancing per soddisfare i gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Elastic Load Balancing.

Con un [Gateway Load Balancer](#), sei responsabile della scelta e della qualificazione del software dei fornitori di appliance. È necessario considerare attendibile il software di appliance affinché ispezioni o modifichi il traffico proveniente dal sistema di bilanciamento del carico, che opera al livello 3 del modello Open Systems Interconnection (OSI), il livello di rete. I fornitori di appliance elencati come [Elastic Load Balancing](#) Partner hanno integrato e qualificato il loro software di appliance con. AWS È possibile attribuire un grado di affidabilità maggiore ai software di appliance offerti dai fornitori presenti in questo elenco. Tuttavia, AWS non garantisce la sicurezza o l'affidabilità del software di questi fornitori.

Indice

- [Protezione dei dati in Elastic Load Balancing](#)
- [Identity and Access Management per Elastic Load Balancing](#)
- [Convalida della conformità in Elastic Load Balancing](#)

- [Resilienza in Elastic Load Balancing](#)
- [Sicurezza dell'infrastruttura in Elastic Load Balancing](#)
- [Accesso a Elastic Load Balancing utilizzando un endpoint di interfaccia \(AWS PrivateLink\)](#)

Protezione dei dati in Elastic Load Balancing

Il modello di [responsabilità AWS condivisa modello](#) di si applica alla protezione dei dati in Elastic Load Balancing. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Elastic Load Balancing o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati a riposo

Se abiliti la crittografia lato server con le chiavi di crittografia gestite da Amazon S3 (SSE-S3) per il bucket S3 per i log di accesso di Elastic Load Balancing, ogni file di log di accesso viene automaticamente crittografato da Elastic Load Balancing prima di essere archiviato nel bucket S3. Inoltre, Elastic Load Balancing decrittografa i file di log di accesso al momento dell'accesso. Ogni file di registro è crittografato con una chiave univoca, a sua volta crittografata con una chiave KMS che viene ruotata regolarmente.

Crittografia dei dati in transito

Elastic Load Balancing semplifica il processo di creazione di applicazioni Web sicure terminando il traffico HTTPS e TLS dai client al sistema di bilanciamento del carico. Il load balancer esegue il lavoro di crittografia e decrittografia del traffico, anziché richiedere a ogni EC2 istanza di gestire il lavoro di terminazione TLS. Quando configuri un listener sicuro, specifichi le suite di crittografia e le versioni del protocollo supportate dall'applicazione e un certificato del server da installare nel sistema di bilanciamento del carico. Puoi utilizzare AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) per gestire i certificati del server. I sistemi Application Load Balancer supportano gli ascoltatori HTTPS. I sistemi Network Load Balancer supportano gli ascoltatori TLS. I sistemi Classic Load Balancer supportano ascoltatori sia HTTPS che TLS.

Identity and Access Management per Elastic Load Balancing

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (chi ha effettuato l'accesso) e autorizzato (chi dispone di autorizzazioni) a utilizzare le risorse Elastic Load Balancing. IAM è un software Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Indice

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Funzionamento di Elastic Load Balancing con IAM](#)
- [Autorizzazioni API di Elastic Load Balancing per il tag delle risorse durante la creazione](#)
- [Ruolo collegato ai servizi Elastic Load Balancing](#)
- [AWS politiche gestite per Elastic Load Balancing](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Elastic Load Balancing.

Utente del servizio: se si utilizza il servizio Elastic Load Balancing per eseguire il lavoro, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare dell'uso delle funzionalità Elastic Load Balancing utilizzate per eseguire lavoro, potrebbero essere richieste autorizzazioni aggiuntive. La comprensione della gestione dell'accesso consente di richiedere le autorizzazioni corrette all'amministratore.

Amministratore del servizio: l'utente responsabile delle risorse Elastic Load Balancing presso l'azienda dispone dell'accesso completo a Elastic Load Balancing. Il suo compito è determinare le caratteristiche e le risorse Elastic Load Balancing a cui gli utenti del servizio devono accedere. Devi quindi inviare le richieste all'amministratore IAM per modificare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM.

Amministratore IAM: in qualità di amministratore IAM, potrebbe essere necessario conoscere i dettagli su come scrivere le policy di gestione dell'accesso a Elastic Load Balancing.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione

AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi

che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Funzionamento di Elastic Load Balancing con IAM

Prima di utilizzare IAM per gestire l'accesso a Elastic Load Balancing, scopri quali funzionalità di IAM sono disponibili per l'uso con Elastic Load Balancing.

Funzionalità IAM utilizzabili con Elastic Load Balancing

Funzionalità IAM	Supporto Elastic Load Balancing
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Policy basate su identità per Elastic Load Balancing

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Policy basate su risorse all'interno di Elastic Load Balancing

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni di policy per Elastic Load Balancing

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni Elastic Load Balancing, consulta [Azioni definite da Elastic Load Balancing V2 e Azioni definite da Elastic Load Balancing V1 nel Service Authorization Reference](#).

Le operazioni delle policy in Elastic Load Balancing utilizzano il seguente prefisso prima dell'operazione:

```
elasticloadbalancing
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "elasticloadbalancing:action1",  
    "elasticloadbalancing:action2"  
]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "elasticloadbalancing:Describe*"
```

Per l'elenco completo delle operazioni API di Elastic Load Balancing, consulta la documentazione seguente:

- Application Load Balancer, Network Load Balancer e Gateway Load Balancer: [Documentazione di riferimento dell'API versione 2015-12-01](#)
- Classic Load Balancer: [Documentazione di riferimento dell'API versione 2012-06-01](#)

Risorse di policy per Elastic Load Balancing

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*" 
```

Alcune operazioni dell'API Elastic Load Balancing supportano risorse multiple. Per specificare più risorse in una singola istruzione, separale ARNs con virgole.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Per visualizzare un elenco dei tipi di risorse Elastic Load Balancing e relativi ARNs, consulta [Resources defined by Elastic Load Balancing V2 e Resources defined by Elastic Load Balancing V1 nel Service Authorization Reference](#). Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta [Azioni definite da Elastic Load Balancing V2 e Azioni definite da Elastic Load Balancing V1](#).

Chiavi di condizione delle policy per Elastic Load Balancing

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di Elastic Load Balancing, consulta [Chiavi di condizione per Elastic Load Balancing V2 e Chiavi di condizione per Elastic Load Balancing V1 nel Service Authorization Reference](#). Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Elastic Load Balancing V2](#) e [Azioni definite da Elastic Load Balancing V1](#).

Chiavi di condizione

- [Chiave di condizione elasticloadbalancing:ListenerProtocol](#)
- [Chiave di condizione elasticloadbalancing:SecurityPolicy](#)
- [Chiave di condizione elasticloadbalancing:Scheme](#)
- [Chiave di condizione elasticloadbalancing:SecurityGroup](#)
- [Chiave di condizione elasticloadbalancing:Subnet](#)
- [Chiave di condizione elasticloadbalancing:ResourceTag](#)

Chiave di condizione `elasticloadbalancing:ListenerProtocol`

La chiave `elasticloadbalancing:ListenerProtocol` condition può essere utilizzata per le condizioni che definiscono i tipi di listener che possono essere creati e utilizzati. La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Le seguenti operazioni supportano questa chiave di condizione:

Versione API 2015-12-01

- `CreateListener`
- `ModifyListener`

Versione API 2012-06-01

- CreateLoadBalancer
- CreateLoadBalancerListeners

La seguente politica di esempio richiede agli utenti di selezionare il protocollo HTTPS per i listener per i propri Application Load Balancer e il protocollo TLS per i listener per i propri Network Load Balancer.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:ModifyListener"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "elasticloadbalancing:ListenerProtocol": [
            "HTTPS",
            "TLS"
          ]
        }
      }
    }
  ]
}
```

Con un Classic Load Balancer, puoi specificare più listener in una singola chiamata. Pertanto, la policy deve utilizzare una [chiave di contesto multivalore](#), come illustrato nell'esempio seguente.

JSON

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

```
{
  "Effect": "Allow",
  "Action": [
    "elasticloadbalancing:CreateLoadBalancer",
    "elasticloadbalancing:CreateLoadBalancerListeners"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "elasticloadbalancing:ListenerProtocol": [
        "TCP",
        "HTTP",
        "HTTPS"
      ]
    }
  }
}
```

Chiave di condizione elasticloadbalancing:SecurityPolicy

La chiave di `elasticloadbalancing:SecurityPolicy` condizione può essere utilizzata per condizioni che definiscono e applicano politiche di sicurezza specifiche sui sistemi di bilanciamento del carico. La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Le seguenti operazioni supportano questa chiave di condizione:

Versione API 2015-12-01

- `CreateListener`
- `ModifyListener`

Versione API 2012-06-01

- `CreateLoadBalancerPolicy`
- `SetLoadBalancerPoliciesOfListener`

La seguente politica di esempio richiede agli utenti di selezionare una delle politiche di sicurezza specificate per i propri Application Load Balancer e Network Load Balancer.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:CreateListener",
      "elasticloadbalancing:ModifyListener"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "elasticloadbalancing:SecurityPolicy": [
          "ELBSecurityPolicy-TLS13-1-2-2021-06",
          "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
          "ELBSecurityPolicy-TLS13-1-1-2021-06"
        ]
      }
    }
  }
}
```

Chiave di condizione elasticloadbalancing:Scheme

La chiave `elasticloadbalancing:Scheme` condition può essere utilizzata per le condizioni che definiscono quale schema può essere selezionato durante la creazione del load balancer. La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Le seguenti operazioni supportano questa chiave di condizione:

Versione API 2015-12-01

- `CreateLoadBalancer`

Versione API 2012-06-01

- `CreateLoadBalancer`

La seguente politica di esempio richiede agli utenti di selezionare lo schema specificato per i propri sistemi di bilanciamento del carico.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "elasticloadbalancing:CreateLoadBalancer",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "elasticloadbalancing:Scheme": "internal"
      }
    }
  }
}
```

Chiave di condizione **elasticloadbalancing:SecurityGroup**

Important

Elastic Load Balancing accetta tutte le lettere maiuscole del gruppo di sicurezza. IDs Tuttavia, assicurati di utilizzare gli operatori di condizione appropriati, senza distinzione tra maiuscole e minuscole, ad esempio. `StringEqualsIgnoreCase`

La chiave di `elasticloadbalancing:SecurityGroup` condizione può essere utilizzata per le condizioni che definiscono quali gruppi di sicurezza possono essere applicati ai sistemi di bilanciamento del carico. La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Le seguenti operazioni supportano questa chiave di condizione:

Versione API 2015-12-01

- `CreateLoadBalancer`
- `SetSecurityGroups`

Versione API 2012-06-01

- `CreateLoadBalancer`
- `ApplySecurityGroupsToLoadBalancer`

La seguente politica di esempio richiede agli utenti di selezionare uno dei gruppi di sicurezza specificati per i propri sistemi di bilanciamento del carico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:SetSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEqualsIgnoreCase": {
          "elasticloadbalancing:SecurityGroup": [
            "sg-51530134",
            "sg-51530144",
            "sg-51530139"
          ]
        }
      }
    }
  ]
}
```

Chiave di condizione `elasticloadbalancing:Subnet`

Important

Elastic Load Balancing accetta tutte le lettere maiuscole della sottorete. IDs Tuttavia, assicurati di utilizzare gli operatori di condizione appropriati, senza distinzione tra maiuscole e minuscole, ad esempio. `StringEqualsIgnoreCase`

La chiave di `elasticloadbalancing:Subnet` condizione può essere utilizzata per le condizioni che definiscono quali sottoreti possono essere create e collegate ai sistemi di bilanciamento del

carico. La policy è disponibile per Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. Le seguenti operazioni supportano questa chiave di condizione:

Versione API 2015-12-01

- `CreateLoadBalancer`
- `SetSubnets`

Versione API 2012-06-01

- `CreateLoadBalancer`
- `AttachLoadBalancerToSubnets`

La seguente politica di esempio richiede agli utenti di selezionare una delle sottoreti specificate per i propri sistemi di bilanciamento del carico.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:CreateLoadBalancer",
      "elasticloadbalancing:SetSubnets"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEqualsIgnoreCase": {
        "elasticloadbalancing:Subnet": [
          "subnet-01234567890abcdef",
          "subnet-01234567890abcdeg "
        ]
      }
    }
  }
}
```

Chiave di condizione elasticloadbalancing:ResourceTag

La chiave `elasticloadbalancing:ResourceTag/keycondition` è specifica di Elastic Load Balancing. Tutte le azioni mutanti supportano questa chiave di condizione.

ACLs in Elastic Load Balancing

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC in Elastic Load Balancing

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Uso di credenziali temporanee in Elastic Load Balancing

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Autorizzazioni del principale tra servizi per Elastic Load Balancing

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama e, in combinazione con la richiesta Servizio AWS, Servizio AWS per effettuare richieste ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio in Elastic Load Balancing

Supporta i ruoli di servizio: no

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Ruoli collegati ai servizi in Elastic Load Balancing

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi Elastic Load Balancing, consulta [Ruolo collegato ai servizi Elastic Load Balancing](#).

Autorizzazioni API di Elastic Load Balancing per il tag delle risorse durante la creazione

Affinché gli utenti possano applicare tag alle risorse durante la creazione, devono disporre delle autorizzazioni per utilizzare l'operazione che crea la risorsa, come `elasticloadbalancing:CreateLoadBalancer` o `elasticloadbalancing:CreateTargetGroup`. Se i tag vengono specificati

nell'azione di creazione delle risorse, sono richieste autorizzazioni aggiuntive per l'azione `elasticloadbalancing:AddTags` per verificare se gli utenti dispongono delle autorizzazioni per applicare tag alle risorse che vengono create. Pertanto, gli utenti devono disporre anche di autorizzazioni esplicite a utilizzare l'azione `elasticloadbalancing:AddTags`.

Nella definizione della policy IAM per l'operazione `elasticloadbalancing:AddTags`, è possibile utilizzare l'elemento `Condition` con la chiave di condizione `elasticloadbalancing:CreateAction` per assegnare autorizzazioni di applicazione di tag all'operazione che crea la risorsa.

L'esempio seguente illustra una policy che consente agli utenti di creare gruppi di destinazioni e applicarvi tag durante la creazione. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare direttamente l'operazione `elasticloadbalancing:AddTags`).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "elasticloadbalancing:CreateAction" : "CreateTargetGroup"
        }
      }
    }
  ]
}
```

In modo analogo, la seguente policy consente agli utenti di creare un sistema di bilanciamento del carico e applicarvi tag durante la creazione. Gli utenti non sono autorizzati ad applicare tag alle risorse esistenti (non possono chiamare direttamente l'operazione `elasticloadbalancing:AddTags`).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "elasticloadbalancing:CreateAction" : "CreateLoadBalancer"
        }
      }
    }
  ]
}
```

L'operazione `elasticloadbalancing:AddTags` viene valutata solo se i tag vengono applicati durante l'operazione di creazione di risorse. Pertanto, un utente con le autorizzazioni per la creazione di una risorsa (presupponendo che non siano presenti condizioni di assegnazione di tag) non necessita delle autorizzazioni per utilizzare l'operazione `elasticloadbalancing:AddTags` se nella richiesta non viene specificato alcun tag. Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta ha esito negativo se non dispone delle autorizzazioni per utilizzare l'operazione `elasticloadbalancing:AddTags`.

Ruolo collegato ai servizi Elastic Load Balancing

Elastic Load Balancing utilizza un ruolo collegato ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Per ulteriori informazioni, consulta [Ruoli collegati ai servizi](#) nella Guida per l'utente di IAM.

Autorizzazioni concesse dal ruolo collegato ai servizi

Elastic Load Balancing utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForElasticLoadBalancing` per chiamare altri AWS servizi per tuo conto.

`AWSServiceRoleForElasticLoadBalancing` ritiene che il `elasticloadbalancing.amazonaws.com` servizio assuma il ruolo.

La politica delle autorizzazioni dei ruoli è `AWSElasticLoadBalancingServiceRolePolicy`. Per vedere le autorizzazioni per questa policy, consulta [AWSElasticLoadBalancingServiceRolePolicy](#) nella Guida di riferimento sulle policy gestite da AWS.

Creazione del ruolo collegato ai servizi

Non devi creare manualmente il ruolo `AWSServiceRoleForElasticLoadBalancing`. Elastic Load Balancing crea questo ruolo per tuo conto durante la creazione di un sistema di bilanciamento del carico o di un gruppo di destinazioni.

Affinché Elastic Load Balancing crei un ruolo collegato ai servizi, è necessario disporre delle autorizzazioni richieste. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Modifica del ruolo collegato ai servizi

Puoi modificare la descrizione dell'`AWSServiceRoleForElasticLoadBalancing` di IAM. Per ulteriori informazioni, consulta [Edit a service-linked role description](#) nella Guida per l'utente IAM.

Eliminazione del ruolo collegato ai servizi

Se non hai più bisogno di usare Elastic Load Balancing, ti consigliamo di eliminarlo. `AWSServiceRoleForElasticLoadBalancing`

Puoi eliminare questo ruolo collegato al servizio solo dopo aver eliminato tutti i sistemi di bilanciamento del carico nel tuo account. AWS Questa procedura ti impedisce di rimuovere involontariamente l'autorizzazione ad accedere ai sistemi di bilanciamento del carico. Per ulteriori

informazioni, consulta [Eliminazione di un Application Load Balancer](#), [Eliminazione di un Network Load Balancer](#) ed [Eliminazione di un Classic Load Balancer](#).

Per eliminare i ruoli collegati ai servizi, puoi utilizzare la console IAM, l'interfaccia a riga di comando IAM CLI o l'API IAM. Per ulteriori dettagli, consulta [Delete a service-linked role](#) nella Guida per l'utente IAM.

Dopo l'eliminazione di `AWSServiceRoleForElasticLoadBalancing`, Elastic Load Balancing crea nuovamente il ruolo se crei un load balancer.

AWS politiche gestite per Elastic Load Balancing

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. Le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: `AWSElasticLoadBalancingClassicServiceRolePolicy`

Questa politica include tutte le autorizzazioni richieste da Elastic Load Balancing (Classic Load Balancer) per AWS chiamare altri servizi per tuo conto. I ruoli collegati ai servizi sono predefiniti. Con i ruoli predefiniti non è necessario aggiungere manualmente le autorizzazioni necessarie affinché Elastic Load Balancing completi le operazioni per tuo conto. Non è possibile collegare, scollegare, modificare o eliminare questa policy.

Per vedere le autorizzazioni per questa policy, consulta [AWSElasticLoadBalancingClassicServiceRolePolicy](#) nella Guida di riferimento sulle policy gestite da AWS.

AWS politica gestita: AWSElasticLoadBalancingServiceRolePolicy

Questa policy include tutte le autorizzazioni che Elastic Load Balancing richiede per chiamare altri servizi AWS per tuo conto. I ruoli collegati ai servizi sono predefiniti. Con i ruoli predefiniti non è necessario aggiungere manualmente le autorizzazioni necessarie affinché Elastic Load Balancing completi le operazioni per tuo conto. Non è possibile collegare, scollegare, modificare o eliminare questa policy.

Per vedere le autorizzazioni per questa policy, consulta [AWSElasticLoadBalancingServiceRolePolicy](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: ElasticLoadBalancingFullAccess

Questa policy offre accesso completo al servizio Elastic Load Balancing e accesso limitato ad altri servizi tramite la console di AWS gestione.

Per vedere le autorizzazioni per questa policy, consulta [ElasticLoadBalancingFullAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: ElasticLoadBalancingReadOnly

Questa policy concede l'accesso in sola lettura a Elastic Load Balancing e ai servizi dipendenti.

Per vedere le autorizzazioni per questa policy, consulta [ElasticLoadBalancingReadOnly](#) nella Guida di riferimento sulle policy gestite da AWS .

Elastic Load Balancing: aggiornamenti alle AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Elastic Load Balancing da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data
AWSElasticLoadBalancingServiceRolePolicy - Aggiornamento a una policy esistente	È stata aggiunta l'ec2:AllocateIpamPoolCidr azione per concedere le autorizzazioni per allocare blocchi CIDR dai pool IPAM.	17 febbraio 2025
ElasticLoadBalancingFullAccess - Aggiornamento a una policy esistente	Sono state aggiunte le arc-zonal-shift:* azioni per concedere le autorizzazioni necessarie per il cambiamento zonale.	28 novembre 2023

Modifica	Descrizione	Data
ElasticLoadBalancingReadOnly - Aggiornamento a una policy esistente	Sono state aggiunte le seguenti azioni per concedere le autorizzazioni necessarie per il cambiamento zonale; e. <code>arc-zonal-shift:GetManagedResource</code> <code>arc-zonal-shift:ListManagedResources</code> <code>arc-zonal-shift:ListZonalShifts</code>	28 novembre 2023
AWSElasticLoadBalancingServiceRolePolicy - Aggiornamento a una policy esistente	È stata aggiunta l' <code>ec2:DescribeVpcPeeringConnections</code> azione per concedere le autorizzazioni necessarie per le connessioni peering.	11 ottobre 2021
ElasticLoadBalancingFullAccess - Aggiornamento a una policy esistente	È stata aggiunta l' <code>ec2:DescribeVpcPeeringConnections</code> azione per concedere le autorizzazioni necessarie per le connessioni peering.	11 ottobre 2021
ElasticLoadBalancingFullAccess : nuova policy	Fornisce accesso completo a Elastic Load Balancing e ai servizi dipendenti.	20 settembre 2018
ElasticLoadBalancingReadOnly : nuova policy	Concede l'accesso in sola lettura a Elastic Load Balancing e ai servizi dipendenti.	20 settembre 2018
Inizio del monitoraggio delle modifiche da parte di Elastic Load Balancing	Elastic Load Balancing ha iniziato a tenere traccia delle modifiche per le sue policy AWS gestite.	20 settembre 2018

Convalida della conformità in Elastic Load Balancing

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione [Scope by Compliance Program Servizi AWS](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#).

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta [AWS la documentazione sulla sicurezza](#).

Resilienza in Elastic Load Balancing

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta [Infrastruttura AWS globale](#).

Oltre all'infrastruttura AWS globale, Elastic Load Balancing offre le seguenti funzionalità per supportare la resilienza dei dati:

- Distribuzione del traffico in entrata tra più istanze in una singola zona di disponibilità o in più zone di disponibilità.
- Puoi utilizzarlo AWS Global Accelerator con i tuoi Application Load Balancer per distribuire il traffico in entrata su più sistemi di bilanciamento del carico in una o più regioni. AWS Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di AWS Global Accelerator](#).
- Amazon ECS ti consente di eseguire, arrestare e gestire contenitori Docker su un cluster di EC2 istanze. Puoi configurare il servizio Amazon ECS in modo da utilizzare un sistema di bilanciamento del carico per distribuire il traffico in ingresso tra i servizi di un cluster. Per ulteriori informazioni, consulta la [Guida per lo sviluppatore di Amazon Elastic Container](#).

Sicurezza dell'infrastruttura in Elastic Load Balancing

In quanto servizio gestito, Elastic Load Balancing è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Elastic Load Balancing attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Isolamento della rete

Un cloud privato virtuale (VPC) è una rete virtuale nella propria area logicamente isolata nel cloud. AWS Una sottorete è un intervallo di indirizzi IP in un VPC. Quando si crea un sistema di bilanciamento del carico, occorre specificare una o più sottoreti per i nodi del sistema di bilanciamento del carico. Puoi distribuire EC2 istanze nelle sottoreti del tuo VPC e registrarle con il tuo sistema di bilanciamento del carico. Per ulteriori informazioni su VPC e sottoreti, consulta la [Guida per l'utente di Amazon VPC](#).

Quando si crea un sistema di bilanciamento del carico in un VPC, può essere collegato a Internet o interno. Un sistema di bilanciamento del carico interno può instradare solo le richieste provenienti da client con accesso al VPC per il sistema di bilanciamento del carico.

Il sistema di bilanciamento del carico invia le richieste alle destinazioni registrate utilizzando gli indirizzi IP privati. Pertanto, le tue destinazioni non necessitano di indirizzi IP pubblici per ricevere le richieste da un sistema di bilanciamento del carico.

Per chiamare l'API di Elastic Load Balancing dal tuo VPC utilizzando indirizzi IP privati, utilizza AWS PrivateLink. Per ulteriori informazioni, consulta [Accesso a Elastic Load Balancing utilizzando un endpoint di interfaccia \(AWS PrivateLink\)](#).

Controllo del traffico di rete

Considera le seguenti opzioni per proteggere il traffico di rete quando si utilizza un sistema di bilanciamento del carico:

- Utilizza ascoltatori sicuri per supportare la comunicazione crittografata tra i client e i sistemi di bilanciamento del carico. I sistemi Application Load Balancer supportano gli ascoltatori HTTPS. I sistemi Network Load Balancer supportano gli ascoltatori TLS. I sistemi Classic Load Balancer supportano ascoltatori sia HTTPS che TLS. È possibile scegliere tra le policy di sicurezza

predefinite per il sistema di bilanciamento del carico per specificare le suite di crittografia e le versioni del protocollo supportate dall'applicazione. Puoi utilizzare AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) per gestire i certificati del server installati sul tuo sistema di bilanciamento del carico. È possibile utilizzare il protocollo SNI (Server Name Indication) per servire più siti Web sicuri utilizzando un unico listener sicuro. Il protocollo SNI viene abilitato automaticamente per il sistema di bilanciamento del carico quando si associano più certificati del server a un listener sicuro.

- Configura i gruppi di sicurezza affinché i sistemi Application Load Balancer e Classic Load Balancer accettino il traffico solo da client specifici. Questi gruppi di sicurezza devono consentire il traffico in ingresso dai client sulle porte del listener e il traffico in uscita verso i client.
- Configura i gruppi di sicurezza per le tue EC2 istanze Amazon in modo che accettino il traffico solo dal sistema di bilanciamento del carico. Questi gruppi di sicurezza devono consentire il traffico in ingresso dal sistema di bilanciamento del carico sulle porte del listener e sulle porte di controllo dello stato.
- Configura l'Application Load Balancer affinché autentichi in modo sicuro gli utenti tramite un provider di identità o utilizzando le identità aziendali. Per ulteriori informazioni, consulta [Autenticazione degli utenti tramite Application Load Balancer](#).
- Utilizza [AWS WAF](#) con gli Application Load Balancers per consentire o bloccare le richieste in base alle regole in una lista di controllo accessi Web (ACL Web).

Accesso a Elastic Load Balancing utilizzando un endpoint di interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il cloud privato virtuale (VPC) e l'API Elastic Load Balancing creando un endpoint VPC di interfaccia. Puoi utilizzare questa connessione per chiamare l'API Elastic Load Balancing dal VPC senza dover collegare un gateway Internet, un'istanza NAT o una connessione VPN al VPC. L'endpoint offre una connettività affidabile e scalabile all'API Elastic Load Balancing, versioni 2015-12-01 e 2012-06-01, utilizzata per creare e gestire i sistemi di bilanciamento del carico.

Gli endpoint VPC di interfaccia sono alimentati da AWS PrivateLink, una funzionalità che consente la comunicazione tra le applicazioni e Servizi AWS l'utilizzo di indirizzi IP privati. Per ulteriori informazioni, consulta [AWS PrivateLink](#).

Limite

AWS PrivateLink non supporta Network Load Balancer con più di 50 ascoltatori.

Creazione di un endpoint di interfaccia per Elastic Load Balancing

Crea un endpoint per Elastic Load Balancing utilizzando il seguente nomi di servizio:

```
com.amazonaws.region.elasticloadbalancing
```

Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink .

Creazione di una policy degli endpoint VPC per Elastic Load Balancing

Puoi collegare una policy all'endpoint VPC per controllare l'accesso all'API Elastic Load Balancing. La policy specifica:

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite.
- La risorsa su cui è possibile eseguire le operazioni.

Nell'esempio seguente viene illustrato una policy di endpoint VPC che nega a chiunque l'autorizzazione per creare un sistema di bilanciamento del carico tramite l'endpoint. Inoltre, la policy di esempio concede a chiunque l'autorizzazione per eseguire tutte le altre operazioni.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "elasticloadbalancing:CreateLoadBalancer",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

Limitazione delle richieste per l'API Elastic Load Balancing

Elastic Load Balancing limita le richieste API per ogni AWS account in base alla regione. Lo facciamo per migliorare le prestazioni e la disponibilità del servizio. La limitazione garantisce che le richieste all'API Elastic Load Balancing non superino i limiti massimi consentiti per le richieste API. Le richieste API sono soggette ai limiti di richiesta, indipendentemente dal fatto che tu le chiami o che vengano chiamate per tuo conto (ad esempio, dall'applicazione Console di gestione AWS o da un'applicazione di terze parti).

Se superi un limite di throttling dell'API Elastic Load Balancing, ricevi il codice di errore e un `ThrottlingException` messaggio di errore. `Rate exceeded`

Ti consigliamo di prepararti a gestire il throttling con garbo. Per maggiori informazioni, consulta [Timeout, nuovi tentativi e backoff con jitter](#). Se riscontri un elevato livello di throttling, puoi contattarci Supporto AWS per aiutarti a valutare l'utilizzo delle API e le potenziali soluzioni. Ogni caso viene valutato singolarmente. Supporto potrebbe aumentare i limiti entro i limiti di sicurezza del sistema, per mantenere un'elevata disponibilità e prestazioni prevedibili.

Come viene applicato il throttling

Elastic Load Balancing utilizza l'[algoritmo token bucket](#) per implementare il throttling delle API. Con questo algoritmo, il tuo account dispone di un bucket che contiene un numero specifico di token. Il numero di token nel bucket rappresenta il limite di throttling in un dato secondo.

Elastic Load Balancing fornisce due set di azioni API. La versione 2 dell'API ELB supporta i seguenti tipi di sistemi di bilanciamento del carico: Application Load Balancer, Network Load Balancer e Gateway Load Balancer. La versione 1 dell'API ELB supporta Classic Load Balancer. Ogni versione dell'API ELB ha i propri bucket e token.

Servizi che richiamano l'API Elastic Load Balancing per tuo conto, come Amazon, Amazon ECS, EC2 Amazon EC2 Auto Scaling, e AWS CloudFormation dispongono di bucket a livello di account propri. Questi servizi non consumano i token dei tuoi bucket.

Limitazione del tasso di richiesta

Con la limitazione della frequenza delle richieste, sei limitato al numero di richieste API che effettui. Ogni richiesta effettuata rimuove un token dal bucket. Ad esempio, la dimensione del bucket di token

per le azioni API non mutanti è di 40 token. Puoi effettuare fino a 40 `Describe*` richieste in un secondo. Se superi `Describe*` le 40 richieste in un secondo, subisci una limitazione e le richieste rimanenti entro quel secondo hanno esito negativo.

I secchi si ricaricano automaticamente a una velocità prestabilita. Se un bucket è al di sotto della sua capacità massima, viene aggiunto un determinato numero di token ogni secondo finché il bucket non raggiunge la sua capacità massima. Se un secchio è pieno quando arrivano i token di ricarica, questi vengono scartati. Un bucket non può contenere più del numero massimo di token. Ad esempio, la dimensione del bucket per le azioni API non mutanti è di 40 token e la frequenza di ricarica è di 10 token al secondo. Se effettui 40 `DescribeLoadBalancers` richieste in un secondo, il bucket viene ridotto a zero (0) token. Aggiungiamo 10 gettoni di ricarica al bucket ogni secondo, fino a raggiungere la capacità massima di 40 token. Ciò significa che un bucket vuoto impiega 4 secondi per raggiungere la sua capacità massima, se non viene effettuata alcuna richiesta durante quel periodo.

Non è necessario attendere che un bucket sia completamente pieno prima di poter effettuare richieste API. È possibile utilizzare i token man mano che vengono aggiunti a un bucket. Se si utilizzano immediatamente i gettoni di ricarica, il secchio non raggiunge la sua capacità massima.

Esiste un limite di limitazione a livello di account condiviso tra tutte le azioni dell'API Elastic Load Balancing. La capacità del bucket a livello di account è di 40 token e la frequenza di ricarica è di 10 token di richiesta al secondo.

Richiedi le dimensioni dei bucket di token e le tariffe di ricarica

Ai fini della limitazione della frequenza delle richieste, le azioni API sono raggruppate in categorie. Ogni categoria ha i propri limiti.

Categories

- **Azioni mutanti:** azioni API che creano, modificano o eliminano risorse. Questa categoria include generalmente tutte le azioni API che non sono classificate come azioni non mutanti. Queste azioni hanno un limite di limitazione inferiore rispetto alle azioni API non mutanti.
- **Azioni non mutanti:** azioni API che recuperano dati sulle risorse. Queste azioni API in genere hanno i limiti di limitazione delle API più elevati.
- **Azioni che richiedono molte risorse:** azioni API che richiedono più tempo e più risorse per essere completate. Queste azioni hanno un limite di limitazione ancora più basso rispetto alle azioni mutanti. Queste azioni vengono limitate separatamente dalle altre azioni mutanti.

- Azioni di registrazione: azioni API che registrano o annullano la registrazione degli obiettivi. Queste azioni API vengono limitate separatamente dalle altre azioni mutanti.
- Azioni non categorizzate: queste azioni API ricevono le proprie dimensioni e frequenze di ricarica, anche se rientrano in una delle altre categorie.

La tabella seguente mostra la capacità e le frequenze di ricarica predefinite per i bucket di token di richiesta classificati.

Categoria	ELBv2 azioni	ELBv1 azioni	capacità del secchio	Velocità di ricarica (al secondo)
Richiede molte risorse	CreateLoadBalancer , SetSubnets	CreateLoadBalancer , AttachLoadBalancerToSubnets , DetachLoadBalancerFromSubnets , EnableAvailabilityZonesForLoadBalancer , DisableAvailabilityZonesForLoadBalancer	10	0,2 †
Registration (Registrazione)	RegisterTargets , DeregisterTargets	RegisterInstancesWithLoadBalancer , DeregisterInstancesFromLoadBalancer	20	4
Non mutante	DescribeAccountLimits , DescribeCapacityReservation , DescribeListenerAttributes , DescribeListenerCertificates , DescribeListeners ,	Describe*	40	10

Categoria	ELBv2 azioni	ELBv1 azioni	capacità del secchio	Velocità di ricarica (al secondo)
	DescribeLoadBalancers , DescribeLoadBalancers , DescribeRules , DescribeSSLPolicies , DescribeTags , DescribeTargetGroupAttributes , DescribeTargetGroups , DescribeTargetHealth			

Categoria	ELBv2 azioni	ELBv1 azioni	capacità del secchio	Velocità di ricarica (al secondo)
Mutante	AddListenerCertificates , AddTags, CreateListener , CreateRule , CreateTargetGroup , DeleteListener , DeleteLoadBalancer , DeleteRule , DeleteTargetGroup , ModifyCapacityReservation , ModifyIpPools , ModifyListener , ModifyListenerAttributes , ModifyLoadBalancerAttributes , ModifyRule , ModifyTargetGroup , ModifyTargetGroupAttributes , RemoveListenerCertificates , RemoveTags , SetIpAddressType , SetRulePriorities , SetSecurityGroups	AddTags, ApplySecurityGroupsToLoadBalancer , ConfigureHealthCheck , CreateAppCookieStickinessPolicy , CreateLbCookieStickinessPolicy , CreateLoadBalancerListener , CreateLoadBalancerPolicy , Delete*, ModifyLoadBalancerAttributes , RemoveTags , SetLoadBalancer*	20	3

La tabella seguente mostra la capacità e le frequenze di ricarica predefinite per i bucket di token di richiesta non categorizzati per. ELBv2

ELBv2 azioni	capacità del secchio	Velocità di ricarica (al secondo)
CreateTrustStore	10	0,2 †
AddTrustStoreRevocations , DeleteSharedTrustStoreAssoc iation , DeleteTrustStore , ModifyTru stStore , RemoveTrustStoreRe vocations	10	0,2 †
GetResourcePolicy , GetTrustS toreCaCertificatesBundle , GetTrustStoreRevocationContent	20	4
DescribeTrustStoreAssociations , DescribeTrustStoreRevocations , DescribeTrustStores	40	10

† Le frequenze di ricarica frazionarie richiedono diversi secondi per generare un token completo.

Monitoraggio delle richieste API

Puoi utilizzarlo AWS CloudTrail per monitorare le tue richieste API Elastic Load Balancing. Per ulteriori informazioni, consulta [Registra le chiamate API per Elastic Load Balancing utilizzando AWS CloudTrail](#).

Comprendi i codici per Elastic Load Balancing nei report di fatturazione e utilizzo

Quando utilizzi Elastic Load Balancing, includiamo i codici correlati nei report di AWS fatturazione e utilizzo. La revisione di questi codici ti aiuta a comprendere i costi e i modelli di utilizzo del sistema di bilanciamento del carico. Il monitoraggio e la gestione delle spese sono essenziali per ottimizzare i costi.

Per ulteriori informazioni, consultare [Prezzi di Elastic Load Balancing](#).

Le tabelle seguenti descrivono i codici per Elastic Load Balancing visualizzati nei report di fatturazione e utilizzo. Le unità sono ore o unità di capacità di bilanciamento del carico (LCU). Ogni tipo di sistema di bilanciamento del carico ha una definizione specifica di LCU. Per informazioni su LCUs per ogni tipo di load balancer, consulta i prezzi di [Elastic Load Balancing](#). Per un elenco dei codici regionali usati nei report di fatturazione e di utilizzo, consulta [AWS Region billing codes](#).

Application Load Balancer

Codice	Description	unità
<i>region</i> -LoadBalancerUsage	Il tempo di esecuzione.	Ore
<i>region</i> -LCUUsage	L' LCUs usato.	LCU
<i>region</i> -IdleProvisionedLBCapacity	LCUs Riservato ma non utilizzato.	LCU
<i>region</i> -TS-LoadBalancerUsage	L'ora in cui un trust store viene utilizzato da Mutual TLS.	Ore
<i>region</i> -Outposts-LoadBalancerUsage	La durata di Outposts.	Ore

Codice	Description	unità
<i>region</i> -Outposts-LCUUsage	LCUs Usato su Outposts.	LCU
<i>region</i> -Reserved LCUUsage	Il LCUs riservato.	LCU

Network Load Balancers

Codice	Description	unità
<i>region</i> -LoadBalancerUsage	Il tempo di esecuzione.	Ore
<i>region</i> -LCUUsage	L' LCUs usato.	LCU

Gateway Load Balancers

Codice	Description	unità
<i>region</i> -LoadBalancerUsage	Il tempo di esecuzione.	Ore
<i>region</i> -LCUUsage	L' LCUs usato.	LCU

Classic Load Balancer

Codice	Description	unità
<i>region</i> -LoadBalancerUsage	Il tempo di esecuzione.	Ore

Codice	Description	unità
<i>region</i> -DataProcessing-Bytes	I dati elaborati.	GB
<i>region</i> -IdleProvisionedLB Capacity	I LCUs riservati ma non utilizzati.	LCU

Registra le chiamate API per Elastic Load Balancing utilizzando AWS CloudTrail

Elastic Load Balancing è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o servizio. AWS CloudTrail acquisisce le chiamate API per Elastic Load Balancing come eventi. Le chiamate acquisite includono chiamate provenienti da Console di gestione AWS e chiamate di codice alle operazioni dell'API Elastic Load Balancing. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Elastic Load Balancing, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account.

Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

Eventi di gestione Elastic Load Balancing in CloudTrail

[Gli eventi di gestione](#) forniscono informazioni sulle operazioni di gestione eseguite sulle risorse presenti nell'ambiente Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Elastic Load Balancing registra le operazioni del piano di controllo come eventi di gestione. Per un elenco delle operazioni del piano di controllo, vedere quanto segue:

- Application Load Balancer — Versione di riferimento dell'API [Elastic Load Balancing](#) 2015-12-01
- Network Load Balancer — Versione di riferimento dell'API [Elastic Load Balancing](#) 2015-12-01
- Gateway Load Balancer — Versione di riferimento dell'API [Elastic Load Balancing](#) 2015-12-01

- Classic Load Balancer — Versione di riferimento dell'API [Elastic Load Balancing](#) 2012-06-01

Esempi di eventi Elastic Load Balancing

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Gli esempi seguenti mostrano CloudTrail gli eventi relativi a un utente che ha creato un sistema di bilanciamento del carico e poi lo ha eliminato utilizzando. AWS CLI Puoi identificare la CLI utilizzando gli elementi `userAgent`. Puoi identificare le chiamate API richieste utilizzando gli elementi `eventName`. Le informazioni relative all'utente (Alice) sono disponibili nell'elemento `userIdentity`.

Example Esempio 1: `CreateLoadBalancer` dall'API ELBv2

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-8360a9e7", "subnet-b7d581c0"],
    "securityGroups": ["sg-5943793c"],
    "name": "my-load-balancer",
    "scheme": "internet-facing"
  },
  "responseElements": {
    "loadBalancers": [{
```

```

        "type": "application",
        "loadBalancerName": "my-load-balancer",
        "vpcId": "vpc-3ac0fb5f",
        "securityGroups": ["sg-5943793c"],
        "state": {"code": "provisioning"},
        "availabilityZones": [
            {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
            {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
        ],
        "dnsName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
        "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
        "createdTime": "Apr 11, 2016 5:23:50 PM",
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0",
        "scheme": "internet-facing"
    }]
},
"requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
"eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
"eventType": "AwsApiCall",
"apiVersion": "2015-12-01",
"recipientAccountId": "123456789012"
}

```

Example Esempio 2: DeleteLoadBalancer dall' ELBv2 API

```

{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {

```

```

    "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcdace1759e1d0"
  },
  "responseElements": null,
  "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
  "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
  "eventType": "AwsApiCall",
  "apiVersion": "2015-12-01",
  "recipientAccountId": "123456789012"
}

```

Example Esempio 3: CreateLoadBalancer dall'API ELB

```

{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJDPLRKLG7UEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-12345678", "subnet-76543210"],
    "loadBalancerName": "my-load-balancer",
    "listeners": [{
      "protocol": "HTTP",
      "loadBalancerPort": 80,
      "instanceProtocol": "HTTP",
      "instancePort": 80
    }]
  },
  "responseElements": {
    "dNSName": "my-loadbalancer-1234567890.elb.amazonaws.com"
  },
  "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
}

```

```
"eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",  
"eventType": "AwsApiCall",  
"apiVersion": "2012-06-01",  
"recipientAccountId": "123456789012"  
}
```

Example Esempio 4: DeleteLoadBalancer dall'API ELB

```
{  
  "eventVersion": "1.03",  
  "userIdentity": {  
    "type": "IAMUser",  
    "principalId": "AIDAJDPLRKL7UEXAMPLE",  
    "arn": "arn:aws:iam::123456789012:user/Alice",  
    "accountId": "123456789012",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
    "userName": "Alice"  
  },  
  "eventTime": "2016-04-08T12:39:25Z",  
  "eventSource": "elasticloadbalancing.amazonaws.com",  
  "eventName": "DeleteLoadBalancer",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "198.51.100.1",  
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",  
  "requestParameters": {  
    "loadBalancerName": "my-load-balancer"  
  },  
  "responseElements": null,  
  "requestID": "f0f17bb6-b9ba-11e3-9b20-999fdEXAMPLE",  
  "eventID": "4f99f0e8-5cf8-4c30-b6da-3b69fEXAMPLE",  
  "eventType": "AwsApiCall",  
  "apiVersion": "2012-06-01",  
  "recipientAccountId": "123456789012"  
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

Migrazione di Classic Load Balancer

Elastic Load Balancing supporta i seguenti sistemi di bilanciamento del carico: Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. Per informazioni sulle diverse funzionalità di ciascun tipo di load balancer, consulta [Elastic Load Balancing](#) features.

Puoi anche scegliere di migrare un Classic Load Balancer esistente in un VPC, verso un Application Load Balancer o un Network Load Balancer.

Vantaggi della migrazione da Classic Load Balancer

Ogni tipo di sistema di bilanciamento del carico presenta caratteristiche, funzioni e configurazioni uniche. Esamina i vantaggi di ogni sistema di bilanciamento del carico per decidere qual è il migliore per te.

Application Load Balancer

L'utilizzo di un Application Load Balancer anziché di un Classic Load Balancer offre i seguenti vantaggi:

Support per:

- [Condizioni del percorso](#), [condizioni dell'host](#) e [condizioni dell'intestazione HTTP](#).
- Reindirizzamento delle richieste da un URL a un altro e instradamento delle richieste verso più applicazioni su una singola istanza. EC2
- Restituzione di risposte HTTP personalizzate.
- Registrazione delle destinazioni in base all'indirizzo IP e registrazione delle funzioni Lambda come destinazioni. Inclusi obiettivi esterni al VPC per il load balancer.
- Autenticazione degli utenti tramite identità aziendali o sociali.
- Applicazioni containerizzate Amazon Elastic Container Service (Amazon ECS).
- Monitoraggio indipendente dello stato di ogni servizio.

I log di accesso contengono informazioni aggiuntive e sono archiviati in un formato compresso.

Prestazioni complessive migliorate del load balancer.

Network Load Balancer

L'utilizzo di un Network Load Balancer anziché un Classic Load Balancer offre i seguenti vantaggi:

Support per:

- Indirizzi IP statici, che consentono di assegnare un indirizzo IP elastico per sottorete abilitata per il bilanciamento del carico.
- Registrazione delle destinazioni in base all'indirizzo IP, incluse le destinazioni esterne al VPC per il sistema di bilanciamento del carico.
- Instradamento delle richieste verso più applicazioni su una singola istanza. EC2
- Applicazioni containerizzate Amazon Elastic Container Service (Amazon ECS).
- Monitoraggio indipendente dello stato di ogni servizio.

Capacità di gestire carichi di lavoro volatili e ridimensionare milioni di richieste al secondo.

Esegui la migrazione utilizzando la procedura guidata di migrazione

La procedura guidata di migrazione utilizza la configurazione del tuo Classic Load Balancer per creare un Application Load Balancer o un Network Load Balancer equivalente. Riduce il tempo e lo sforzo necessari per migrare un Classic Load Balancer rispetto ad altri metodi.

Note

La procedura guidata crea un nuovo sistema di bilanciamento del carico. La procedura guidata non converte il Classic Load Balancer esistente in un Application Load Balancer o Network Load Balancer. È necessario reindirizzare manualmente il traffico verso il sistema di bilanciamento del carico appena creato.

Limitazioni

- Il nome del nuovo sistema di bilanciamento del carico non può essere lo stesso di un sistema di bilanciamento del carico esistente dello stesso tipo, nella stessa regione.
- Se il Classic Load Balancer contiene tag contenenti il aws : prefisso nella chiave, tali tag non vengono migrati.

Durante la migrazione a un Application Load Balancer

- Se il Classic Load Balancer dispone di una sola sottorete, è necessario specificare una seconda sottorete.
- Se il Classic Load Balancer dispone di HTTP/HTTPS listener che utilizzano i controlli di integrità TCP, il protocollo di controllo dello stato viene aggiornato a HTTP e il percorso è impostato su «/».
- Se il Classic Load Balancer dispone di listener HTTPS che utilizzano una politica di sicurezza personalizzata o non supportata, la procedura guidata di migrazione utilizza la politica di sicurezza predefinita per il nuovo tipo di load balancer.

Durante la migrazione a un Network Load Balancer

- I seguenti tipi di istanza non verranno registrati nel nuovo gruppo target: C1,,,,,, CC1 CC2, G1 CG1 CG2, G2 CR1 CS1,,, M1, M2 H11, M3 HS1, T1
- Alcune impostazioni del controllo dello stato del Classic Load Balancer potrebbero non essere trasferibili al nuovo gruppo target. Questi casi verranno indicati come modifiche nella sezione di riepilogo della procedura guidata di migrazione.
- Se Classic Load Balancer dispone di listener SSL, la procedura guidata di migrazione crea un listener TLS utilizzando il certificato e la politica di sicurezza del listener SSL.

Procedura guidata di migrazione

Per migrare un Classic Load Balancer utilizzando la procedura guidata di migrazione

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 Classic Load Balancer che desideri migrare.
4. Nella sezione Dettagli del sistema di bilanciamento del carico, scegli Avvia procedura guidata di migrazione.
5. Scegli Migrate to Application Load Balancer o Migrate to Network Load Balancer per aprire la procedura guidata di migrazione.
6. In Assegna un nome al nuovo sistema di bilanciamento del carico, per il nome del sistema di bilanciamento del carico inserisci un nome per il nuovo sistema di bilanciamento del carico.

7. In Assegna un nome al nuovo gruppo target e rivedi gli obiettivi, in Nome del gruppo target inserisci un nome per il nuovo gruppo target.
8. (Facoltativo) In Target, puoi esaminare le istanze di target che verranno registrate con il nuovo gruppo target.
9. (Facoltativo) In Review tags, puoi controllare i tag che verranno applicati al tuo nuovo load balancer
10. In Summary for Application Load Balancer o Summary for Network Load Balancer, esamina e verifica le opzioni di configurazione assegnate dalla procedura guidata di migrazione.
11. Dopo essere soddisfatto del riepilogo della configurazione, scegli Create Application Load Balancer o Create Network Load Balancer per avviare la migrazione.

Esegui la migrazione utilizzando l'utilità di copia del load balancer

Le utilità di copia del load balancer sono disponibili all'interno del repository Elastic Load Balancing Tools, nella pagina. [AWS GitHub](#)

Resources

- [Strumenti Elastic Load Balancing](#)
- [Utilità di copia da Classic Load Balancer a Application Load Balancer](#)
- [Utilità di copia da Classic Load Balancer a Network Load Balancer](#)

Esegui la migrazione manuale del sistema di bilanciamento del carico

In seguito vengono fornite istruzioni generali per la creazione manuale di un nuovo Application Load Balancer o Network Load Balancer basato su un Classic Load Balancer esistente all'interno di un VPC. È possibile eseguire la migrazione utilizzando il Console di gestione AWS, AWS CLI, o un AWS SDK. Per ulteriori informazioni, consulta [Nozioni di base di Elastic Load Balancing](#).

Dopo avere completato il processo di migrazione, puoi sfruttare le caratteristiche del nuovo sistema di bilanciamento del carico.

Processo di migrazione manuale

Fase 1: creazione di un nuovo sistema di bilanciamento del carico

Crea un sistema di bilanciamento del carico con una configurazione equivalente al Classic Load Balancer da migrare.

1. Crea un nuovo sistema di bilanciamento del carico con lo stesso schema (connessione Internet o interna), sottoreti e gruppi di sicurezza del Classic Load Balancer.
2. Crea un gruppo di destinazioni per il sistema di bilanciamento del carico, con le stesse impostazioni del controllo dell'integrità del Classic Load Balancer.
3. Esegui una delle seguenti operazioni:
 - Se il Classic Load Balancer è collegato a un gruppo con dimensionamento automatico, associa il gruppo di destinazioni a tale gruppo. In questo modo, con il gruppo di destinazioni vengono registrate anche le istanze di dimensionamento automatico.
 - Registra le tue EC2 istanze presso il tuo gruppo target.
4. Crea uno o più listener, ciascuno con una regola predefinita che inoltri le richieste al gruppo di destinazioni. Se crei un ascoltatore HTTPS, puoi specificare lo stesso certificato che hai specificato per il Classic Load Balancer. Ti consigliamo di utilizzare la policy di sicurezza di default.
5. Se il Classic Load Balancer dispone di tag, esaminali e aggiungi quelli importanti al nuovo sistema di bilanciamento del carico.

Fase 2: reindirizzamento graduale del traffico al nuovo sistema di bilanciamento del carico

Una volta che le istanze sono state registrate nel nuovo sistema di bilanciamento del carico, è possibile iniziare il processo di reindirizzamento del traffico dal vecchio al nuovo sistema. In questo modo è possibile testare il nuovo sistema di bilanciamento del carico riducendo al minimo i rischi per la disponibilità dell'applicazione.

Per reindirizzare gradualmente il traffico al nuovo sistema di bilanciamento del carico

1. Incollare il nome DNS del nuovo sistema di bilanciamento del carico nel campo dell'indirizzo di un browser Web connesso a Internet. Se tutto funziona correttamente, il browser visualizza la pagina predefinita dell'applicazione.
2. Creare un nuovo record DNS che associ il nome di dominio al nuovo sistema di bilanciamento del carico. Se il servizio DNS supporta la valutazione del peso, specificare un peso di 1 nel nuovo record DNS e un peso di 9 nel record DNS esistente per il sistema di bilanciamento del carico. In questo modo, il 10% del traffico viene indirizzato al nuovo sistema di bilanciamento del carico e il 90% verso quello vecchio.

3. Monitorare il nuovo sistema di bilanciamento del carico per verificare che stia ricevendo traffico e instradando le richieste alle istanze.

 Important

Il time-to-live (TTL) nel record DNS è di 60 secondi. Ciò significa che qualsiasi server DNS che risolve il nome di dominio mantiene le informazioni del record nella cache per 60 secondi, mentre le modifiche si propagano. Pertanto, questi server DNS possono ancora instradare il traffico verso il vecchio sistema di bilanciamento del carico per un massimo di 60 secondi dopo che è stata completata la fase precedente. Durante la propagazione, il traffico potrebbe essere indirizzato a qualunque sistema di bilanciamento del carico.

4. Continuare ad aggiornare il peso dei record DNS finché tutto il traffico non viene indirizzato al nuovo sistema di bilanciamento del carico. Al termine dell'operazione, è possibile eliminare il record DNS del vecchio sistema di bilanciamento del carico.

Fase 3: aggiornamento di policy, script e codice

Se hai effettuato la migrazione del Classic Load Balancer a un Application Load Balancer o a un Network Load Balancer, assicurati di effettuare le seguenti operazioni:

- Aggiorna le policy IAM che utilizzano la versione API 2012-06-01 affinché utilizzino la versione 2015-12-01.
- Aggiorna i processi che utilizzano CloudWatch metriche nel AWS/ELB namespace per utilizzare le metriche del namespace or. AWS/ApplicationELB AWS/NetworkELB
- Aggiorna gli script che utilizzano i comandi per utilizzare i comandi. `aws elb` AWS CLI `aws elbv2` AWS CLI
- Aggiorna CloudFormation i modelli che utilizzano la `AWS::ElasticLoadBalancing::LoadBalancer` risorsa per utilizzare le `AWS::ElasticLoadBalancingV2` risorse.
- Aggiorna il codice che utilizza la versione API 2012-06-01 Elastic Load Balancing affinché utilizzi la versione 2015-12-01.

Resources

- [elbv2](#) nella Documentazione di riferimento dei comandi della AWS CLI

- [Documentazione di riferimento dell'API Elastic Load Balancing versione 2015-12-01](#)
- [Identity and Access Management per Elastic Load Balancing](#)
- [Application Load Balancer metrics](#) nella Guida per l'utente dei sistemi Application Load Balancer
- [Network Load Balancer metrics](#) nella Guida per l'utente dei sistemi Network Load Balancer
- [AWS::ElasticLoadBalancingV2::LoadBalancer](#) nella Guida per l'utente di AWS CloudFormation

Fase 4: eliminazione del vecchio sistema di bilanciamento del carico

È possibile eliminare il vecchio Classic Load Balancer dopo:

- Il reindirizzamento di tutto il traffico dal vecchio sistema di bilanciamento del carico a quello nuovo.
- Il completamento di tutte le richieste esistenti instradate al vecchio sistema di bilanciamento del carico.

Impedisci agli utenti di creare Classic Load Balancer

Puoi creare una policy IAM che impedisca agli utenti di creare Classic Load Balancer nel tuo account.

Sia [Elastic Load Balancing V2](#) che [Elastic Load Balancing](#) APIs V1 forniscono un'azione API. `CreateLoadBalancer` Quando si crea un Classic Load Balancer, si utilizza l'azione API V1, che crea sia il load balancer che i listener. Quando si crea un Application Load Balancer, Network Load Balancer o Gateway Load Balancer, si utilizza l'azione API V2, che crea solo il load balancer. L'API V2 fornisce un'azione `CreateListener` che puoi utilizzare per creare listener per un load balancer dopo averlo creato.

La seguente politica nega agli utenti l'autorizzazione a creare un load balancer se viene specificato il protocollo listener. Poiché è necessario configurare almeno un listener quando si crea un Classic Load Balancer, questa politica impedisce agli utenti di creare Classic Load Balancer. Non impedisce agli utenti di creare altri tipi di sistemi di bilanciamento del carico, poiché esistono azioni API separate per la creazione di tali sistemi di bilanciamento del carico e dei relativi listener.

```
{
  "Version": "2012-10-17",
  "Effect": "Deny",
  "Action": "elasticloadbalancing:CreateLoadBalancer",
  "Resource": [
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
```

```
],  
  "Condition": {  
    "Null": {  
      "elasticloadbalancing:ListenerProtocol": false  
    }  
  }  
}
```

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.