aws

Guida per l'utente

Sistema di bilanciamento del carico elastico

Sistema di bilanciamento del carico elastico: Guida per l'utente

Table of Contents

Cos'è l'Elastic Load Balancing?

Il servizio Elastic Load Balancing distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una o più zone di disponibilità. Monitora lo stato di integrità delle destinazioni registrate e instrada il traffico solo verso le destinazioni integre. Elastic Load Balancing 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 decriptazione 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 i seguenti bilanciatori del carico: Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. È possibile selezionare il tipo di load balancer più adatto alle proprie esigenze. Per ulteriori informazioni, consulta Confronti di prodotti.

Per ulteriori informazioni sull'utilizzo di ogni sistema di bilanciamento del carico, 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
- Guida per l'utente dei sistemi 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:

- AWS Management Console: fornisce un'interfaccia Web da 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 SDK: forniscono API specifiche per la lingua e gestiscono molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta SDK di AWS.
- 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 e Network 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 permettono di eseguire le proprie applicazioni nel cloud. È possibile configurare il sistema di bilanciamento del carico per instradare il traffico sulle istanze EC2. Per ulteriori informazioni, consulta la Guida per l'utente di Amazon EC2.
- Dimensionamento automatico Amazon EC2: assicura l'esecuzione del numero di istanze desiderato, anche in caso di guasto di un'istanza. Dimensionamento automatico Amazon EC2 consente di aumentare o diminuire automaticamente il numero di istanze in base alla domanda. 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 Guida per l'utente di Dimensionamento automatico Amazon EC2.

- 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: permette di eseguire, arrestare e gestire i container Docker su un cluster di istanze EC2. 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 assegna gli URL alle risorse, ad esempio 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, consulta Prezzi di Elastic Load Balancing.

Funzionamento di Elastic Load Balancing

Un sistema di bilanciamento del carico accetta traffico in entrata dai client e instrada le richieste alle sue destinazioni (come le istanze EC2) 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.

Elastic Load Balancing supporta i seguenti tipi di sistemi di bilanciamento del carico:

- Application Load Balancer
- Network Load Balancers
- Gateway Load Balancers
- Classic Load Balancer

Esiste una differenza fondamentale nel modo in cui i tipi di sistema di bilanciamento del carico vengono configurati. Con Application Load Balancer, Network Load Balancer e Gateway Load Balancer le istanze vengono registrate come destinazioni in gruppi di destinazioni verso i quali viene instradato il traffico. Con Classic Load Balancer le istanze vengono registrate direttamente nel 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.

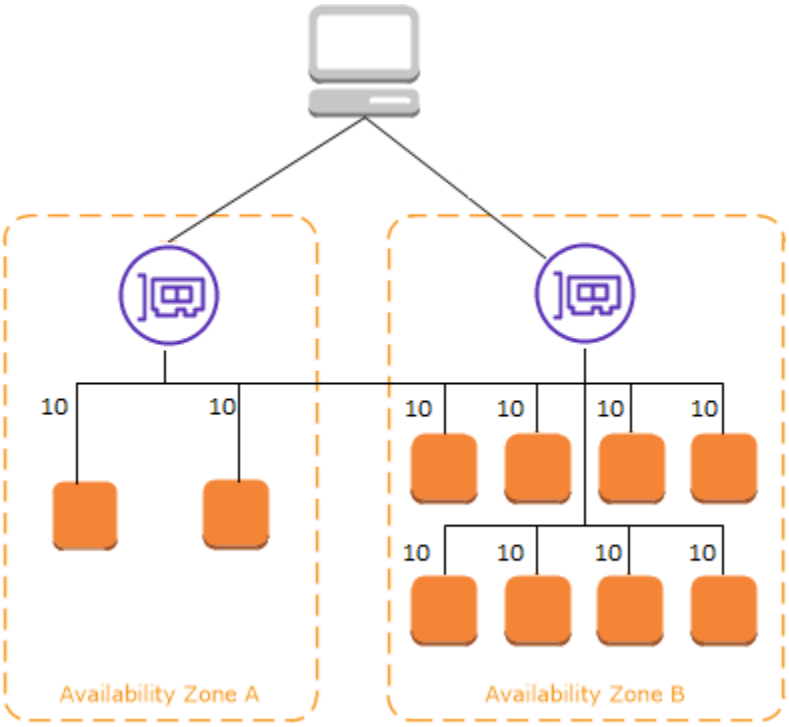
Dopo aver disabilitato un'area di disponibilità, le destinazioni in tale zona di disponibilità rimangono registrate con il sistema di bilanciamento del carico. Tuttavia, anche se rimangono registrate, il sistema di bilanciamento del carico non vi instrada alcun traffico.

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.

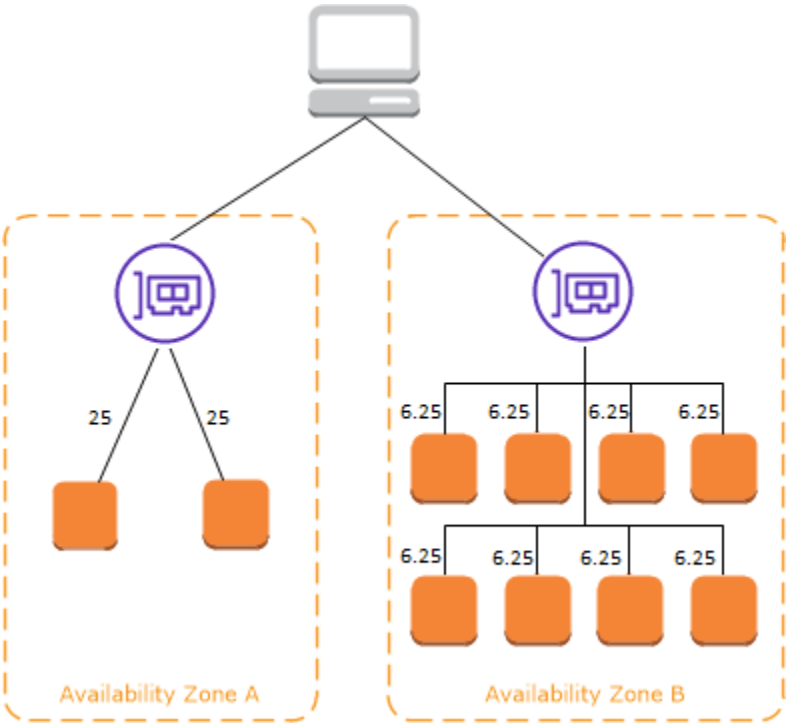
Se il bilanciamento del carico tra zone è abilitato, ciascuna delle 10 destinazioni riceve il 10% del traffico. Questo perché ogni nodo del sistema di bilanciamento del carico è in grado di instradare il 50% del traffico dei client verso tutte e 10 le destinazioni.



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.

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 AWS Management Console, l'opzione per abilitare il bilanciamento del carico tra zone è selezionata per impostazione predefinita. Dopo aver creato un Classic Load Balancer, è possibile abilitare o disabilitare il load balancer tra zone in qualsiasi momento. 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 zonale è una funzionalità di Sistema di controllo Amazon Route 53 per il ripristino di applicazioni (Route53 ARC). Con lo spostamento zonale, è possibile spostare una risorsa di un sistema di bilanciamento del carico da una zona di disponibilità danneggiata con una singola

operazione. In questo modo è possibile continuare a operare da altre zone di disponibilità integre in una Regione AWS.

Quando si avvia uno spostamento zonale, il sistema di bilanciamento del carico interrompe l'invio di traffico per la risorsa alla zona di disponibilità danneggiata. Route 53 ARC crea immediatamente lo spostamento zonale. Tuttavia, il completamento delle connessioni esistenti e in corso nella zona di disponibilità danneggiata può richiedere un po' di tempo, generalmente fino a qualche minuto. Per ulteriori informazioni, consulta How a zonal shift works: health checks and zonal IP addresses nella Guida per gli sviluppatori di Sistema di controllo Amazon Route 53 per il ripristino di applicazioni.

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

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

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

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

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 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 alle destinazioni.

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.

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 inviati e dalle 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 sul rilevamento della MTU del percorso e sull'abilitazione dei frame jumbo, consulta Rilevamento della MTU del percorso nella Guida per l'utente di Amazon EC2.

Nozioni di base di Elastic Load Balancing

Elastic Load Balancing supporta i seguenti bilanciatori del carico: Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. È possibile selezionare il tipo di load balancer più adatto alle proprie esigenze. Per ulteriori informazioni, consulta Confronti di prodotti.

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.

Indice

Creazione di un Application Load Balancer

Per creare un Application Load Balancer tramite la AWS Management Console, consulta Nozioni di base di Application Load Balancer nella Guida per l'utente dei sistemi Application Load Balancer.

Per creare un Application Load Balancer tramite la AWS CLI, consulta Creazione di un Application Load Balancer tramite la AWS CLI nella Guida per l'utente dei sistemi Application Load Balancer.

Creazione di un Network Load Balancer

Per creare un Network Load Balancer tramite la AWS Management Console, consulta Nozioni di base di Network Load Balancer nella Guida per l'utente dei sistemi Network Load Balancer.

Per creare un Network Load Balancer tramite la AWS CLI, consulta Creazione di un Network Load Balancer tramite la AWS CLI nella Guida per l'utente dei sistemi Network Load Balancer.

Creazione di un Gateway Load Balancer

Per creare un Gateway Load Balancer tramite la AWS Management Console, consulta Nozioni di base di Gateway Load Balancer nella Guida per l'utente di Gateway Load Balancer.

Per creare un Gateway Load Balancer tramite la AWS CLI, consulta Nozioni di base di Gateway Load Balancer tramite la AWS CLI nella Guida per l'utente di Gateway Load Balancer.

Creazione di un Classic Load Balancer

Per creare un Classic Load Balancer tramite la AWS Management Console, consulta Creazione di un Classic Load Balancer tramite la nella Guida per l'utente dei sistemi Classic Load Balancer.

Sicurezza in Elastic Load Balancing

La sicurezza del cloud in AWS ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Gli auditor di terze parti testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di conformità AWS. Per avere maggiori informazioni sui programmi di conformità applicabili a Elastic Load Balancing, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS 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. Vengono inoltre fornite informazioni su come utilizzare altri servizi AWS che consentono di monitorare e proteggere le risorse di Elastic Load Balancing.

Con un Gateway Load Balancer, sei è 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 presenti nell'elenco degli Elastic Load Balancing Partners hanno integrato e qualificato il proprio software di appliance con AWS. È possibile attribuire un grado di affidabilità maggiore ai software di appliance offerti dai fornitori presenti in questo elenco. Tuttavia, AWS non garantisce la sicurezza o l'affidabilità dei software di questi fornitori.

Indice

- 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 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 AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- 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 FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard () 140-3. FIPS

Ti consigliamo vivamente 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 AWS servizi utilizzando la console, API

AWS CLI, o. 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. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia a riposo

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

Crittografia in transito

Elastic Load Balancing semplifica il processo di creazione di applicazioni Web sicure HTTPS interrompendo il TLS traffico proveniente dai client sul 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. È possibile utilizzare AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) per gestire i certificati del server. Gli Application Load Balancer supportano HTTPS i listener. I Network Load Balancer supportano gli ascoltatori. TLS I Classic Load Balancer supportano sia gli ascoltatori che gli ascoltatori. HTTPS TLS

Identity and Access Management per Elastic Load Balancing

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

Indice

- Gestione dell'accesso con policy
- Come funziona Elastic Load Balancing con IAM
- Autorizzazioni Elastic Load Balancing API
- APIAutorizzazioni Elastic Load Balancing per etichettare le risorse durante la creazione
- Ruolo collegato ai servizi Elastic Load Balancing
- AWS politiche gestite per Elastic Load Balancing

Destinatari

Il modo in cui usi 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 ti 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. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM.

IAMamministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere policy per gestire l'accesso a Elastic Load Balancing.

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando

accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM
- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

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

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come funziona Elastic Load Balancing con IAM

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

IAMfunzionalità utilizzabili con Elastic Load Balancing

IAMcaratteristica	Supporto Elastic Load Balancing
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	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 su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Policy basate su risorse all'interno di Elastic Load Balancing

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni di policy per Elastic Load Balancing

Supporta le operazioni di policy: si

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

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di operazioni Elastic Load Balancing, consulta Operazioni definite da Elastic Load Balancing in Riferimento per l'autorizzazione del servizio.

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 API azioni per Elastic Load Balancing, consulta la seguente documentazione:

- Application Load Balancer, Network Load Balancer e Gateway Load Balancer — Versione di riferimento 2015-12-01 API
- Classic Load Balancers — Versione di riferimento 2012-06-01 API

Per ulteriori informazioni sulle autorizzazioni richieste da ogni operazione di Elastic Load Balancing, consulta Autorizzazioni Elastic Load Balancing API.

Risorse di policy per Elastic Load Balancing

Supporta le risorse di policy: sì

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

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Alcune API azioni Elastic Load Balancing supportano più risorse. 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 relativiARNs, consulta Resources defined by Elastic Load Balancing nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, consulta Azioni definite da Elastic Load Balancing.

Chiavi di condizione delle policy per Elastic Load Balancing

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

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi 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.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione

logica0R. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Per visualizzare un elenco di chiavi di condizione Elastic Load Balancing, consulta Chiavi di condizione per Elastic Load Balancing in Riferimento per l'autorizzazione del servizio. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta la sezione Operazioni definite da Elastic Load Balancing.

Chiave di condizione **`elasticloadbalancing:ResourceTag`**

Il`elasticloadbalancing:ResourceTag/`*`key`* la chiave di condizione è specifica di Elastic Load Balancing. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `AddTags`
- `CreateListener`
- `CreateLoadBalancer`
- `DeleteLoadBalancer`
- `DeleteTargetGroup`
- `DeregisterTargets`
- `ModifyLoadBalancerAttributes`
- `ModifyTargetGroup`
- `ModifyTargetGroupAttributes`
- `RegisterTargets`
- `RemoveTags`
- `SetIpAddressType`
- `SetSecurityGroups`

- SetSubnets

APIversione 2012-06-01

- AddTags
- ApplySecurityGroupsToLoadBalancer
- AttachLoadBalancersToSubnets
- ConfigureHealthCheck
- CreateAppCookieStickinessPolicy
- CreateLBCookieStickinessPolicy
- CreateLoadBalancer
- CreateLoadBalancerListeners
- CreateLoadBalancerPolicy
- DeleteLoadBalancer
- DeleteLoadBalancerListeners
- DeleteLoadBalancerPolicy
- DeregisterInstancesFromLoadBalancer
- DetachLoadBalancersFromSubnets
- DisableAvailabilityZonesForLoadBalancer
- EnableAvailabilityZonesForLoadBalancer
- ModifyLoadBalancerAttributes
- RegisterInstancesWithLoadBalancer
- RemoveTags
- SetLoadBalancerListenerSSLCertificate
- SetLoadBalancerPoliciesForBackendServer
- SetLoadBalancerPoliciesOfListener

Chiave di condizione **elasticloadbalancing:ListenerProtocol**

La chiave elasticloadbalancing:ListenerProtocol condition può essere utilizzata per condizioni che definiscono i tipi di ascoltatori che possono essere creati e utilizzati. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `CreateListener`
- `ModifyListener`

APIversione 2012-06-01

- `CreateLoadBalancer`
- `CreateLoadBalancerListeners`

La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Di seguito è riportato un esempio di policy che consente agli utenti di selezionare solo uno dei protocolli specificati per il proprio listener.

Protocolli supportati:

- HTTPS
- HTTP
- TCP
- SSL
- TLS
- UDP
- TCP_UDP

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                    "elasticloadbalancing:ListenerProtocol": [
                    "HTTPS",
                    "TLS"
                    ]
```

```
            },
        }
```

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. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `CreateListener`
- `ModifyListener`

APIversione 2012-06-01

- `CreateLoadBalancerPolicy`
- `SetLoadBalancerPoliciesOfListener`

La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Di seguito è riportato un esempio di politica che consente agli utenti di selezionare solo una delle politiche di sicurezza specificate per il proprio sistema di bilanciamento del carico.

```
"Resource": [
"Version": "2015-12-01",
    "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 di `elasticloadbalancing:Scheme` condizione può essere utilizzata per le condizioni che definiscono lo schema che può essere selezionato durante la creazione del sistema di bilanciamento del carico. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `CreateLoadBalancer`

APIversione 2012-06-01

- `CreateLoadBalancer`

La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Di seguito è riportato un esempio di politica che consente agli utenti di selezionare solo uno degli schemi specificati per il proprio sistema di bilanciamento del carico.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action":"elasticloadbalancing:CreateLoadBalancer",
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                "elasticloadbalancing:Scheme": "internal"
            },
        }
```

Chiave di condizione **elasticloadbalancing:Subnet**

> **Important**
>
> Elastic Load Balancing accetta tutte le lettere maiuscole di Subnet. 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. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `CreateLoadBalancer`
- `SetSubnets`

APIversione 2012-06-01

- `CreateLoadBalancer`
- `AttachLoadBalancerToSubnets`

La policy è disponibile per Application Load Balancer, Network Load Balancer, Gateway Load Balancer e Classic Load Balancer. Di seguito è riportato un esempio di policy che consente agli utenti di selezionare solo una delle sottoreti specificate per il proprio sistema di bilanciamento del carico.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSubnets"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:Subnet": [
                    "subnet-01234567890abcdef",
                    "subnet-01234567890abcdeg "
                ]
            },
        }
```

Chiave di condizione **elasticloadbalancing:SecurityGroup**

> **Important**
>
> Elastic Load Balancing accetta tutte le lettere maiuscole di. SecurityGroup 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. Le seguenti operazioni supportano questa chiave di condizione:

APIversione 2015-12-01

- `CreateLoadBalancer`
- `SetSecurityGroups`

APIversione 2012-06-01

- `CreateLoadBalancer`
- `ApplySecurityGroupsToLoadBalancer`

La policy è disponibile per Application Load Balancer, Network Load Balancer e Classic Load Balancer. Di seguito è riportato un esempio di politica che consente agli utenti di selezionare solo uno dei gruppi di sicurezza specificati per il proprio sistema di bilanciamento del carico.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSecurityGroup"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:SecurityGroup": [
                    "sg-51530134",
                    "sg-51530144",
```

```
                "sg-51530139"
            ]
        },
    }
```

ACLsin Elastic Load Balancing

SupportiACLs: 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. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon Elastic Load Balancing

Supporti ABAC (tag nelle politiche): Sì

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Uso di credenziali temporanee in Elastic Load Balancing

Supporta le credenziali temporanee: sì

Alcuni AWS servizi non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni del principale tra servizi per Elastic Load Balancing

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio in Elastic Load Balancing

Supporta i ruoli di servizio: No

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

Ruoli collegati ai servizi in Elastic Load Balancing

Supporta ruoli collegati ai servizi: Sì

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

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 Elastic Load Balancing API

È necessario concedere agli utenti l'autorizzazione a chiamare le API azioni Elastic Load Balancing di cui hanno bisogno. Inoltre, per alcune azioni Elastic Load Balancing, devi concedere agli utenti l'autorizzazione a richiamare azioni specifiche da Amazon. EC2 API

Autorizzazioni richieste per il 01/12/2015 API

Quando si richiamano le seguenti azioni a partire dal 01/12/2015API, è necessario concedere agli utenti l'autorizzazione a eseguire le azioni specificate.

`CreateLoadBalancer`

- `elasticloadbalancing:CreateLoadBalancer`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeAddresses`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `iam:CreateServiceLinkedRole`

`CreateTargetGroup`

- `elasticloadbalancing:CreateTargetGroup`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeVpcs`

`RegisterTargets`

- `elasticloadbalancing:RegisterTargets`

- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

SetIpAddressType

- elasticloadbalancing:SetIpAddressType
- ec2:DescribeSubnets

SetSubnets

- elasticloadbalancing:SetSubnets
- ec2:DescribeSubnets

Autorizzazioni richieste per il 2012-06-01 API

Quando si richiamano le seguenti azioni a partire dal 01/06/2012, è necessario concedere agli utenti l'autorizzazione a eseguire le azioni API specificate.

ApplySecurityGroupsToLoadBalancer

- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeSecurityGroups

AttachLoadBalancerToSubnets

- elasticloadbalancing:AttachLoadBalancerToSubnets
- ec2:DescribeSubnets

CreateLoadBalancer

- elasticloadbalancing:CreateLoadBalancer
- ec2:CreateSecurityGroup
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- iam:CreateServiceLinkedRole

DeregisterInstancesFromLoadBalancer

- elasticloadbalancing:DeregisterInstancesFromLoadBalancer
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeInstanceHealth

- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeLoadBalancers

- elasticloadbalancing:DescribeLoadBalancers
- ec2:DescribeSecurityGroups

DisableAvailabilityZonesForLoadBalancer

- elasticloadbalancing:DisableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeVpcs

EnableAvailabilityZonesForLoadBalancer

- elasticloadbalancing:EnableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

RegisterInstancesWithLoadBalancer

- elasticloadbalancing:RegisterInstancesWithLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeClassicLinkInstances

- `ec2:DescribeInstances`
- `ec2:DescribeVpcClassicLink`

APIAutorizzazioni Elastic Load Balancing per etichettare le 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 delle autorizzazioni esplicite per utilizzare l'operazione `elasticloadbalancing:AddTags`.

Nella definizione della IAM politica per l'`elasticloadbalancing:AddTags`sazione, è possibile utilizzare l'`Condition`elemento con la chiave `elasticloadbalancing:CreateAction` condition per concedere le autorizzazioni di etichettatura all'azione 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`).

```
{
  "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`).

```
{
  "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 necessità 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, vedere Utilizzo dei ruoli collegati ai servizi nella Guida per l'utente. IAM

Autorizzazioni concesse dal ruolo collegato ai servizi

Elastic Load Balancing utilizza il ruolo collegato al servizio denominato AWSServiceRoleForElasticLoadBalancingper richiamare le seguenti azioni per tuo conto:

- `ec2:AssignIpv6Addresses`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssociateAddress`
- `ec2:AttachNetworkInterface`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateNetworkInterface`
- `ec2:CreateSecurityGroup`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeAddresses`
- `ec2:DescribeClassicLinkInstances`
- `ec2:DescribeCoipPools`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeSubnets`
- `ec2:DescribeVpcClassicLink`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DetachNetworkInterface`
- `ec2:DisassociateAddress`
- `ec2:GetCoipPoolUsage`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:ReleaseAddress`
- `ec2:UnassignIpv6Addresses`
- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:UpdateLogDelivery`
- `outposts:GetOutpostInstanceTypes`

AWSServiceRoleForElasticLoadBalancingritiene che il `elasticloadbalancing.amazonaws.com` servizio assuma il ruolo.

Creazione del ruolo collegato ai servizi

Non è necessario creare manualmente il AWSServiceRoleForElasticLoadBalancingruolo. 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 dei ruoli collegati ai servizi nella Guida per l'IAMutente.

Se hai creato un sistema di bilanciamento del carico prima dell'11 gennaio 2018, Elastic Load Balancing lo hai AWSServiceRoleForElasticLoadBalancingcreato nel AWS tuo account. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio AWS account nella Guida per l'IAMutente.

Modifica del ruolo collegato ai servizi

È possibile modificare la descrizione dell'AWSServiceRoleForElasticLoadBalancingutilizzoIAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

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.

È possibile utilizzare la IAM console, il o il per eliminare i IAM CLI ruoli collegati IAM API al servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Dopo l'eliminazione 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 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 Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS 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 ne AWS servizio viene lanciata una nuova o quando diventano disponibili nuove API operazioni per i servizi esistenti.

Per ulteriori informazioni, consulta le politiche AWS gestite nella Guida IAM per l'utente.

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 visualizzare le autorizzazioni per questa politica, consulta il Managed Policy AWSElasticLoadBalancingClassicServiceRolePolicyReference.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 visualizzare le autorizzazioni per questa policy, consulta AWSElasticLoadBalancingServiceRolePolicyil AWS Managed Policy Reference.

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 visualizzare le autorizzazioni per questa politica, consulta ElasticLoadBalancingFullAccessil AWS Managed Policy Reference.

AWS politica gestita: ElasticLoadBalancingReadOnly

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

Per visualizzare le autorizzazioni per questa policy, consulta ElasticLoadBalancingReadOnlyil AWS Managed Policy Reference.

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
AWS politica gestita: ElasticLoadBalancingFullAccess: aggiornamento a una policy esistente.	Elastic Load Balancing ha aggiunto una nuova operazione per concedere l'autorizzazione a usare lo spostamento zonale. Questa operazione è stata aggiunta alla policy di accesso completo di Elastic Load Balancing. È associato alle `arc-zonal-shift:*` API operazioni.	28 novembre 2022
AWS politica gestita: ElasticLoadBalancingReadOnly: aggiornamento a una policy esistente.	Elastic Load Balancing ha aggiunto una nuova operazione per concedere l'autorizzazione a usare lo spostamento zonale. Questa operazione è stata aggiunta alla policy di sola lettura di Elastic Load Balancing. È associato alle `arc-zonal-shift:GetManagedResource` `arc-zonal-shift:ListZonalShifts` API operazioni `arc-zonal-shift:ListManagedResources` e.	28 novembre 2022
AWS politica gestita: AWSElasticLoadBalancingServiceRolePolicy: aggiornamento a una policy esistente.	Elastic Load Balancing ha aggiunto una nuova operazione per concedere l'autorizzazione a usare le connessioni in peering. Questa operazione è stata aggiunta alla policy di ruolo collegato ai servizi per il piano di controllo (control-plane) di Elastic Load Balancing. È associato all'`ec2:DescribeVpcPeeringConnections` APIoperazione.	11 ottobre 2021
AWS politica gestita: ElasticLoadBalancingFullAccess: aggiornamento a una policy esistente.	Elastic Load Balancing ha aggiunto una nuova operazione per concedere l'autorizzazione a usare le connessioni in peering. Questa operazione è stata aggiunta alla policy di accesso completo di Elastic Load Balancing. È associata all'`ec2:DescribeVpcPeeringConnections` APIoperazione.	11 ottobre 2021

Modifica	Descrizione	Data
AWS politica gestita: AWSElasticLoadBalancingClassicServiceRolePolicy: aggiornamento a una policy esistente.	Elastic Load Balancing ha aggiunto una policy di ruolo collegato ai servizi (per il piano di controllo (control-plane)) per Classic Load Balancer. Questo aggiornamento è destinato alla versione 2 (predefinita).	7 ottobre 2019
AWS politica gestita: ElasticLoadBalancingReadOnly	Concede l'accesso in sola lettura a Elastic Load Balancing e ai servizi dipendenti. Si tratta della versione 1 (predefinita).	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.	23 luglio 2021

Convalida della conformità in Elastic Load Balancing

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione Scope by Compliance Program AWS servizi e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi 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 AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

> **Note**
>
> Non tutte sono idonee. AWS servizi HIPAA Per ulteriori informazioni, consulta la Guida ai servizi HIPAA idonei.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione AWS servizi e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- Evaluating Resources with Rules nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Ciò AWS servizio fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: AWS servizio rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Elastic Load Balancing

L'infrastruttura globale di AWS è basata su regioni AWS 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.

Per ulteriori informazioni sulle Regioni AWS e sulle zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale di AWS, 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 utilizzare AWS Global Accelerator con gli Application Load Balancer per distribuire il traffico in ingresso tra 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 permette di eseguire, arrestare e gestire i contenitori Docker su un cluster di istanze EC2. 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.

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

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

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Isolamento della rete

Un cloud privato virtuale (VPC) è una rete virtuale nella propria area logicamente isolata nel AWS Cloud. 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 sistema VPC e registrarle con il tuo sistema di bilanciamento del carico. Per ulteriori informazioni sulle sottoreti VPC e sulle sottoreti, consulta la Amazon VPC User Guide.

Quando crei un sistema di bilanciamento del carico in unVPC, questo può essere rivolto a Internet o interno. Un sistema di bilanciamento del carico interno può indirizzare solo le richieste provenienti da client con accesso al sistema di bilanciamento del carico per il VPC sistema.

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 Elastic Load Balancing API dai tuoi indirizzi IP privati, VPC usa. 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. Gli Application Load Balancer supportano gli ascoltatori. HTTPS I Network Load Balancer supportano gli ascoltatori. TLS I Classic Load Balancer supportano sia gli ascoltatori che gli ascoltatori. HTTPS 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. È possibile utilizzare AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) per gestire i certificati del server installati sul sistema di bilanciamento del carico. È possibile utilizzare il protocollo Server Name Indication (SNI) per servire più siti Web sicuri utilizzando un unico listener sicuro. SNIviene abilitato automaticamente per il sistema di bilanciamento del carico quando si associano più di un certificato 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.
- Utilizzalo AWS WAFcon i tuoi Application Load Balancer per consentire o bloccare le richieste in base alle regole di una lista di controllo degli accessi Web (web). ACL

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 si basano sulla tecnologia AWS PrivateLink, una funzionalità che abilita la comunicazione tra le applicazioni e AWS servizi utilizzando 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.

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 caratteristiche di ogni tipo di sistema di bilanciamento del carico, consulta Confronti di prodotti Elastic Load Balancing.

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 load balancer ha 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 per 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 per 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 listener HTTP/HTTPS 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 istanze non verranno registrati nel nuovo gruppo target: C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M2, M3, 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 console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, sotto Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. 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

Risorse

- 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 AWS Management Console 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 di queste 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 istanze EC2 con il gruppo di destinazioni.
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 registrare 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 AWS 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.

Risorse

- 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.

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.