aws

Guía del usuario

Elastic Load Balancing

Elastic Load Balancing: Guía del usuario

Table of Contents

¿Qué es Elastic Load Balancing?

Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en una o más zonas de disponibilidad. Monitorea el estado de los destinos registrados y enruta el tráfico solamente a destinos en buen estado. Elastic Load Balancing escala de forma automática su capacidad de equilibrador de carga en respuesta a los cambios en el tráfico entrante.

Beneficios del equilibrador de carga

Un equilibrador de carga distribuye cargas de trabajo a través de varios recursos informáticos, como, servidores virtuales. Usar un equilibrador de carga aumenta la disponibilidad y la tolerancia a errores de las aplicaciones.

Puede agregar y eliminar recursos informáticos de su equilibrador de carga en función de sus necesidades sin interrumpir el flujo general de solicitudes a las aplicaciones.

Puede configurar las comprobaciones de estado, que monitorizan el estado de los recursos informáticos, de tal forma que el equilibrador de carga solo envíe solicitudes a los que están en buen estado. También puede trasladar las tareas de cifrado y descifrado al equilibrador de carga, de forma que los recursos informáticos se pueden dedicar a su trabajo principal.

Características de Elastic Load Balancing

Elastic Load Balancing admite varios tipos de balanceadores de carga. Puede seleccionar el tipo de equilibrador de carga que mejor se adapte a sus necesidades. Para obtener más información, consulte .

Para obtener más información sobre los balanceadores de carga de la generación actual, consulte la siguiente documentación:

- Guía del usuario para equilibradores de carga de aplicaciones
- Guía del usuario para Equilibradores de carga de redes
- Guía del usuario de equilibradores de carga de puerta de enlace

Los balanceadores de carga clásicos son la generación anterior de balanceadores de carga de Elastic Load Balancing. Le recomendamos que migre a un balanceador de carga de la generación actual. Para obtener más información, consulte Migración de la versión clásica de Load Balancer.

Acceso a Elastic Load Balancing

Puede crear y administrar los equilibradores de carga y el acceso a ellos desde cualquiera de las siguientes interfaces:

- AWS Management Console: Proporciona una interfaz web que se puede utilizar para obtener acceso al Elastic Load Balancing.
- AWS Interfaz de línea de comandos (AWS CLI): proporciona comandos para un amplio conjunto de AWS servicios, incluido Elastic Load Balancing. AWS CLI Es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.
- AWS SDKs— Indique un idioma específico APIs y cuide muchos de los detalles de la conexión, como el cálculo de las firmas, la gestión de los reintentos de las solicitudes y la gestión de los errores. Para obtener más información, consulte AWS SDKs.
- Query API (API de consulta): proporciona acciones de la API de nivel bajo a las que se llama mediante solicitudes HTTPS. Utilizar la API de consulta es la forma más directa de obtener acceso a Elastic Load Balancing. Sin embargo, la API de consulta requiere que la aplicación gestione detalles de bajo nivel, como, por ejemplo, la generación del hash para firmar la solicitud y el control de errores. Para obtener más información, consulte los siguientes temas:
  - Equilibradores de carga de aplicación, Equilibradores de carga de red y equilibradores de carga de puerta de enlace: versión 2015-12-01 de API
  - Equilibradores de carga clásicos: versión de la API 2012-06-01

Servicios relacionados

Elastic Load Balancing se combina con los siguientes servicios para mejorar la disponibilidad y la escalabilidad de las aplicaciones.

- Amazon EC2: servidores virtuales que ejecutan sus aplicaciones en la nube. Puede configurar su balanceador de carga para enrutar el tráfico a sus EC2 instancias. Para obtener más información, consulta la Guía del EC2 usuario de Amazon.
- Amazon EC2 Auto Scaling: garantiza que está ejecutando el número deseado de instancias, incluso si una instancia falla. Amazon EC2 Auto Scaling también le permite aumentar o disminuir

automáticamente el número de instancias a medida que cambia la demanda de las mismas. Si habilita escalado automático con Elastic Load Balancing, las instancias que el escalado automático inicie se registrarán automáticamente en el equilibrador de carga. Del mismo modo, las instancias que el escalado automático termine se anularán automáticamente del equilibrador de carga. Para obtener más información, consulte la Guía del usuario EC2 de Amazon Auto Scaling.

- AWS Certificate Manager: al crear un oyente HTTPS, puede especificar certificados específicos provistos por ACM. El equilibrador de carga utiliza certificados para terminar las conexiones y descifrar las solicitudes de los clientes.
- Amazon CloudWatch: le permite monitorear su balanceador de carga y tomar las medidas necesarias. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon ECS: le permite ejecutar, detener y administrar contenedores de Docker en un clúster de EC2 instancias. Puede configurar el equilibrador de carga de forma que direccione el tráfico a los contenedores. Para obtener más información, consulte Amazon Elastic Container Service Developer Guide (Guía para desarrolladores de Amazon Elastic Container Service).
- AWS Global Accelerator: mejora la disponibilidad y el rendimiento de la aplicación. Utilice un acelerador para distribuir el tráfico entre varios balanceadores de carga en una o más regiones. AWS Para obtener más información, consulte la Guía para desarrolladores de AWS Global Accelerator.
- Route 53: ofrece una forma rentable y de confianza de direccionar a los visitantes a los sitios web convirtiendo los nombres de dominio en direcciones IP numéricas que los equipos utilizan para comunicarse entre sí. Por ejemplo, se `www.example.com` traduciría en la dirección IP numérica. `192.0.2.1` AWS asigna URLs a tus recursos, como los balanceadores de carga. No obstante, puede ser conveniente utilizar una URL que los usuarios puedan recordar fácilmente. Por ejemplo, puede asignar el nombre de dominio a un equilibrador de carga. Para obtener más información, consulte la Guía para desarrolladores de Amazon Route 53.
- AWS WAF— Puede usarlo AWS WAF con su Application Load Balancer para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (ACL web). Para obtener más información, consulte la Guía para desarrolladores de AWS WAF.

Precios

Con el equilibrador de carga, solo se paga por lo que se usa. Para obtener más información, consulte Precios de Elastic Load Balancing.

Cómo funciona Elastic Load Balancing

Un balanceador de cargas acepta el tráfico entrante de los clientes y enruta las solicitudes a sus destinos registrados (como EC2 las instancias) en una o más zonas de disponibilidad. Asimismo, el equilibrador de carga monitoriza el estado de los destinos registrados en él y se asegura de direccionar el tráfico únicamente a los que se encuentran en buen estado. Cuando el equilibrador de carga detecta un destino que no está en buen estado, deja de enviar tráfico a ese destino. A continuación, reanuda el tráfico a ese destino cuando detecta que el destino vuelve a estar en buen estado.

Puede configurar el equilibrador de carga para que acepte el tráfico entrante especificando uno o varios oyentes. Un oyente es un proceso que verifica solicitudes de conexión. Se configura con un protocolo y un número de puerto para las conexiones entre los clientes y el equilibrador de carga. Del mismo modo, se configura con un protocolo y un número de puerto para las conexiones del equilibrador de carga a los destinos.

Contenido

Zonas de disponibilidad y nodos de equilibrador de carga

Cuando se agrega una zona de disponibilidad al equilibrador de carga, Elastic Load Balancing crea en ella un nodo de equilibrador de carga. Si registra destinos en una zona de disponibilidad, pero no la habilita, los destinos registrados no reciben tráfico. El equilibrador de carga es más eficaz si se asegura de que cada zona de disponibilidad habilitada tenga al menos un destino registrado.

Recomendamos habilitar varias zonas de disponibilidad para todos los equilibradores de carga. Sin embargo, con un Equilibrador de carga de aplicación, es obligatorio que habilite al menos dos o más zonas de disponibilidad. Esta configuración ayuda a garantizar que el equilibrador de carga pueda continuar enviando el tráfico. Si una zona de disponibilidad deja de estar disponible o no incluye ningún destino en buen estado, el equilibrador de carga puede seguir enviando el tráfico a los destinos en buen estado de otra zona de disponibilidad.

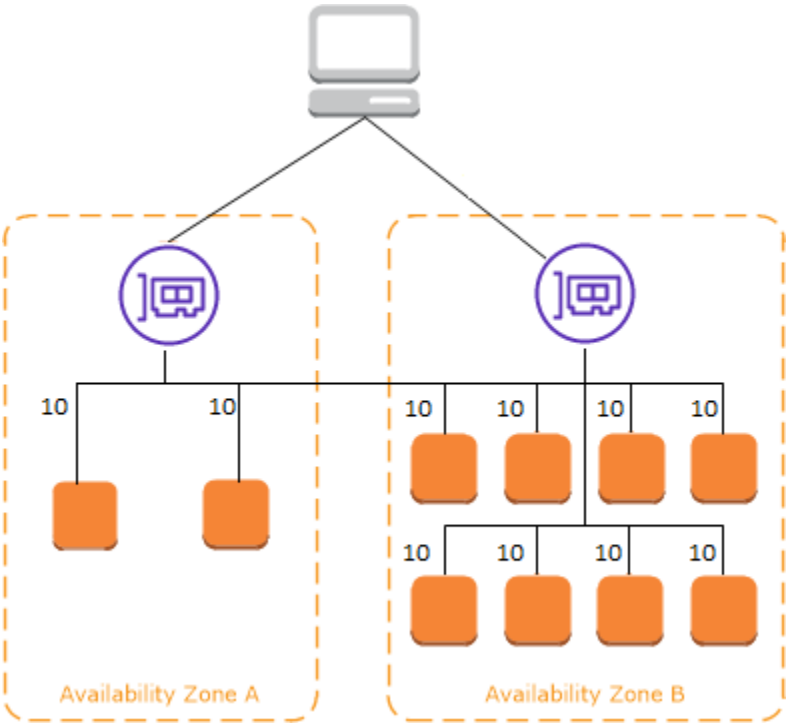
Después de deshabilitar una zona de disponibilidad, los destinos de esa zona de disponibilidad permanecen registrados en el equilibrador de carga. Sin embargo, aunque permanezcan registrados, el equilibrador de carga no envía el tráfico hacia ellos.

Equilibrio de carga entre zonas

Los nodos del equilibrador de carga distribuyen las solicitudes procedentes de los clientes entre los destinos registrados. Cuando el equilibrio de carga entre zonas está habilitado, cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados de todas las zonas de disponibilidad habilitadas. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad.

Los siguientes diagramas muestran el efecto del equilibrio de carga entre zonas, con el algoritmo de enrutamiento por turnos como algoritmo de enrutamiento predeterminado. Hay dos zonas de disponibilidad habilitadas: la zona de disponibilidad A tiene dos destinos, mientras que la zona de disponibilidad B tiene ocho. Los clientes envían solicitudes y Amazon Route 53 responde a cada una con la dirección IP de uno de los nodos del equilibrador de carga. Según el algoritmo de enrutamiento por turnos, el tráfico se distribuye de manera que cada nodo del equilibrador de carga reciba el 50 % del tráfico de los clientes. Cada nodo del equilibrador de carga distribuye su cuota de tráfico entre los destinos registrados en su ámbito.

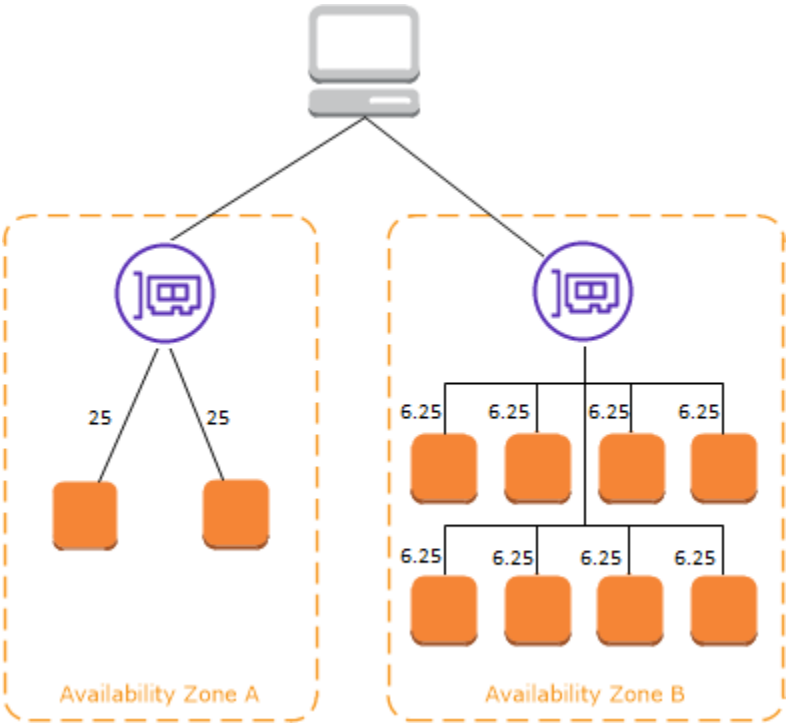
Si el equilibrio de carga entre zonas está habilitado, cada uno de los diez destinos recibirá un 10% del tráfico. Esto se debe a que cada nodo del equilibrador de carga puede dirigir el 50% del tráfico de los clientes a los diez destinos.



Cuando el equilibrio de carga entre zonas está deshabilitado:

- Cada uno de los dos destinos de la zona de disponibilidad A recibe el 25 % del tráfico.
- Cada uno de los ocho destinos de la zona de disponibilidad B recibe el 6,25 % del tráfico.

Esto se debe a que cada nodo del equilibrador de carga puede dirigir el 50 % del tráfico de los clientes únicamente a los destinos de su zona de disponibilidad.



Con los equilibradores de carga de aplicaciones, el equilibrio de carga entre zonas siempre está habilitado en el nivel del equilibrador de carga. A nivel del grupo de destino, se puede deshabilitar el equilibrio de carga entre zonas. Para obtener más información, consulte Equilibrio de carga entre zonas en la Guía del usuario de Equilibradores de carga de aplicación.

Con Equilibradores de carga de red y equilibradores de carga de puerta de enlace, el equilibrio de carga entre zonas está deshabilitado de forma predeterminada. Después de crear un equilibrador de carga, puede habilitar o desactivar el equilibrio de carga entre zonas en cualquier momento. Para obtener más información, consulte Equilibrio de carga entre zonas en la Guía del usuario de Equilibradores de carga de red.

Al crear un equilibrador de carga clásico, el valor predeterminado para el equilibrio de carga entre zonas depende de cómo se crea el equilibrador de carga. Con la API o el CLI, el equilibrio de carga entre zonas está deshabilitado de forma predeterminada. Con el AWS Management Console, la opción de habilitar el equilibrio de carga entre zonas está seleccionada de forma predeterminada. Después de crear un Equilibrador de carga clásico, puede habilitar o desactivar el equilibrio de carga entre zonas en cualquier momento. Para obtener más información, consulte Habilitar el equilibrio de carga entre zonas en la Guía del usuario de Equilibradores de carga clásicos.

Cambio de zona

El cambio de zona es una capacidad del Controlador de recuperación de aplicaciones (ARC) de Amazon. Con el cambio de zona, puede alejar un recurso del equilibrador de carga de una zona de disponibilidad afectada con una sola acción. De esta forma, podrá seguir operando desde otras zonas de disponibilidad en buen estado en una Región de AWS.

Al comenzar un cambio de zona, el equilibrador de carga deja de enviar el tráfico del recurso a la zona de disponibilidad afectada. ARC crea el cambio de zona de inmediato. Sin embargo, completar las conexiones existentes y en curso en la zona de disponibilidad afectada puede tardar un tiempo, por lo general unos minutos. Para obtener más información, consulte Cómo funciona un cambio de zona: comprobaciones de estado y direcciones IP de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones (ARC) de Amazon.

Antes de utilizar un cambio de zona, consulte lo siguiente:

- El cambio de zona no se admite cuando se utiliza un Equilibrador de carga de red con el equilibrador de carga entre zonas activado o desactivado.
- Puede comenzar un cambio de zona para un equilibrador de carga específico solo para una zona de disponibilidad única. No puede comenzar un cambio de zona para varias zonas de disponibilidad.
- AWS elimina de forma proactiva las direcciones IP del balanceador de carga zonal del DNS cuando varios problemas de infraestructura afectan a los servicios. Compruebe siempre la capacidad actual de la zona de disponibilidad antes de comenzar un cambio de zona. Si sus equilibradores de carga tienen desactivado el equilibrio de carga entre zonas y utiliza un cambio de zona para eliminar la dirección IP del equilibrador de carga de zona, la zona de disponibilidad afectada por el cambio de zona también pierde la capacidad de destino.

Para obtener más orientación e información, consulte Prácticas recomendadas para cambios zonales en ARC en la Guía para desarrolladores de Amazon Application Recovery Controller (ARC).

Enrutamiento de solicitudes

Antes de que un cliente envíe una solicitud al equilibrador de carga, resuelve el nombre de dominio de este último utilizando un servidor de sistema de nombres de dominio (DNS). Amazon controla la entrada de DNS, ya que los equilibradores de carga se encuentran en el dominio `amazonaws.com`.

Los servidores DNS de Amazon devuelven una o varias direcciones IP al cliente. Estas son las direcciones IP de los nodos del equilibrador de carga. Con los Equilibradores de carga de redes, Elastic Load Balancing crea una interfaz de red para cada zona de disponibilidad que habilite y la utiliza para obtener una dirección IP estática. Si lo desea, puede asociar una dirección IP elástica a cada interfaz de red al crear el Equilibrador de carga de red.

A medida que el tráfico de la aplicación cambia, Elastic Load Balancing escala el equilibrador de carga y actualiza la entrada de DNS. La entrada de DNS también especifica el valor time-to-live (TTL) de 60 segundos. Esto ayuda a garantizar que las direcciones IP se puedan reasignar rápidamente en respuesta al tráfico cambiante.

El cliente determina qué dirección IP se debe usar para enviar solicitudes al equilibrador de carga. El nodo de equilibrador de carga que recibe la solicitud selecciona un destino registrado en buen estado y le envía la solicitud a ese destino utilizando su dirección IP privada.

Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.

Algoritmo de direccionamiento

Con los equilibradores de carga de aplicaciones, el nodo del equilibrador de carga que recibe la solicitud realiza el siguiente proceso:

1. Evalúa las reglas del oyente en orden de prioridad para determinar qué regla se va a aplicar.
2. Selecciona un destino del grupo de destino para la acción de regla mediante el uso del algoritmo de direccionamiento configurado para el grupo de destino. El algoritmo de enrutamiento predeterminado es de turno rotativo. El enrutamiento se lleva a cabo de manera independiente para cada grupo de destino, aunque un destino se haya registrado en varios grupos de destino.

Con los Equilibradores de carga de red, el nodo del equilibrador de carga que recibe la conexión utiliza el siguiente proceso:

1. Selecciona un destino del grupo de destino para la regla predeterminada mediante un algoritmo hash de flujo. Basa el algoritmo en:
   - El protocolo.
   - La dirección IP de origen y el puerto de origen.
   - La dirección IP de destino y el puerto de destino.
   - El número de secuencia TCP.

2. Direcciona cada conexión TCP individual a un único destino durante la conexión. Las conexiones TCP desde un cliente tienen distintos puertos de origen y números de secuencia y se pueden dirigir a diferentes destinos.

Con los Equilibradores de carga clásicos, el nodo del equilibrador de carga que recibe la solicitud selecciona una instancia registrada del siguiente modo:

- Usa el algoritmo de direccionamiento de turno rotativo para oyentes TCP.
- Usa el algoritmo de direccionamiento de solicitudes menos pendientes para oyentes HTTP y HTTPS.

Conexiones HTTP

Los Equilibradores de carga clásicos utilizan conexiones preabiertas, pero los equilibradores de carga de aplicaciones no. Tanto los Equilibradores de carga clásicos como los equilibradores de carga de aplicaciones utilizan la multiplexación de conexiones. Esto significa que las solicitudes de varios clientes en varias conexiones frontend se pueden dirigir a un destino determinado a través de una única conexión backend. El multiplexado de conexión mejora la latencia y reduce la carga de sus aplicaciones. Para evitar el multiplexado de conexión, deshabilite los encabezados `keep-alive` de HTTP mediante la configuración del encabezado `Connection: close` en sus respuestas HTTP.

Los equilibradores de carga de aplicaciones y los Equilibradores de carga clásicos admiten HTTP canalizado en las conexiones front-end. Sin embargo, no admiten HTTP canalizado en las conexiones backend.

El Equilibrador de carga de aplicación es compatible con los siguientes métodos de solicitud HTTP: GET, HEAD, POST, PUT, DELETE, OPTIONS y PATCH.

Los equilibradores de carga de aplicaciones admiten los siguientes protocolos en las conexiones frontend: HTTP/0.9, HTTP/1.0, HTTP/1.1 y HTTP/2. Puede utilizar HTTP/2 solo con los oyentes HTTPS y enviar hasta 128 solicitudes en paralelo mediante una conexión HTTP/2. Los balanceadores de carga de aplicaciones también admiten actualizaciones de conexión de HTTP a. WebSockets Sin embargo, si hay una actualización de la conexión, las AWS WAF integraciones y las reglas de enrutamiento de los oyentes de Application Load Balancer ya no se aplican.

De forma predeterminada, los equilibradores de carga de aplicaciones utilizan HTTP/1.1 en las conexiones de backend (el equilibrador de carga se dirige al destino registrado). Sin embargo,

se puede usar la versión del protocolo para enviar la solicitud a los destinos mediante HTTP/2. Para obtener más información, consulte las versiones de protocolo. De forma predeterminada, el encabezado de `keep-alive` se admite en las conexiones de backend. Si las solicitudes HTTP/1.0 de los clientes no tienen un encabezado de host, el equilibrador de carga lo genera para las solicitudes HTTP/1.1 enviadas a través de las conexiones backend. El encabezado de host contiene el nombre de DNS del equilibrador de carga.

Los Equilibradores de carga clásicos admiten los siguientes protocolos en las conexiones frontend (del cliente al equilibrador de carga): HTTP/0.9, HTTP/1.0 y HTTP/1.1. Utilizan HTTP/1.1 en las conexiones backend (del equilibrador de carga al destino registrado). De forma predeterminada, el encabezado de `keep-alive` se admite en las conexiones de backend. Si las solicitudes HTTP/1.0 de los clientes no tienen un encabezado de host, el equilibrador de carga lo genera para las solicitudes HTTP/1.1 enviadas a través de las conexiones backend. El encabezado de host contiene la dirección IP del nodo del equilibrador de carga.

Encabezados HTTP

Los equilibradores de carga de aplicaciones y los Equilibradores de carga clásicos agregan automáticamente los encabezados X-Forwarded-For, X-Forwarded-Proto y X-Forwarded-Port a la solicitud.

Los equilibradores de carga de aplicaciones convierten los nombres de host de los encabezados de los hosts HTTP a letras minúsculas antes de enviarlos a los destinos.

Para las conexiones frontend que utilizan HTTP/2, los nombres de encabezado están en minúsculas. Antes de la solicitud se envía en el destino mediante HTTP/1.1, los siguientes nombres de encabezado se convierten en una combinación: X-Forwarded-For, X-Forwarded-Proto, X-Forwarded-Port, Host, X-Amzn-Trace-Id, Upgradey Connection. Todos los demás nombres de encabezado están en minúsculas.

Los Equilibradores de carga de aplicación y Equilibradores de carga clásicos respetan el encabezado de conexión de la solicitud del cliente entrante después de devolver la respuesta al cliente a través del proxy.

Cuando los equilibradores de carga de aplicaciones y los Equilibradores de carga clásicos que utilizan HTTP/1.1 reciben el encabezado Expect: 100-Continue, responden inmediatamente con HTTP/1.1 100 Continue sin probar la longitud del encabezado. El encabezado de solicitud Expect: 100-Continue no se reenvía a sus destinos.

Cuando se usa HTTP/2, los equilibradores de carga de aplicaciones no admiten el encabezado Expect: 100-Continue en las solicitudes de los clientes. El Equilibrador de carga de aplicación no responderá con HTTP/2 100 Continue ni reenviará este encabezado a sus destinos.

Límites de los encabezados HTTP

Los siguientes límites de tamaño para los Equilibradores de carga de aplicación son límites invariables que no se pueden cambiar.

- Línea de solicitud: 16 K
- Encabezado único: 16 K
- Encabezado de solicitud completo: 32 K
- Encabezado de solicitud completo: 64 K

Esquema del equilibrador de carga

Al crear un equilibrador de carga, debe decidir si va a ser un equilibrador de carga interno o va a estar expuesto a Internet.

Los nodos de un equilibrador de carga expuesto a Internet tienen direcciones IP públicas. El nombre de DNS de un equilibrador de carga expuesto a Internet se puede resolver públicamente para obtener las direcciones IP públicas de los nodos. Por tanto, los equilibradores de carga expuestos a Internet pueden dirigir las solicitudes de los clientes a través de Internet.

Los nodos de un equilibrador de carga interno solo tienen direcciones IP privadas. El nombre de DNS de un equilibrador de carga interno se puede resolver para obtener las direcciones IP privadas de los nodos. Por lo tanto, los equilibradores de carga internos solo puede direccionar las solicitudes de los clientes que tienen acceso a la VPC para el equilibrador de carga.

Tanto los equilibradores de carga expuestos a Internet como los internos direccionan las solicitudes a los destinos mediante direcciones IP privadas. Por lo tanto, los destinos no requieren direcciones IP públicas para recibir las solicitudes desde un equilibrador de carga, ya sea interno o expuesto a Internet.

Si la aplicación tiene varios niveles, puede diseñar una arquitectura que utilice tanto equilibradores de carga expuestos a Internet como internos. Por ejemplo, esto es así cuando la aplicación utiliza servidores web que deben conectarse a Internet y servidores de base de datos que solo se conectan a los servidores web. Cree un equilibrador de carga expuesto a Internet y registre los servidores

web en él. Cree un equilibrador de carga interno y registre los servidores de aplicaciones en él. Los servidores web reciben las solicitudes del equilibrador de carga expuesto a Internet y envían las solicitudes de los servidores de aplicaciones al equilibrador de carga interno. Los servidores de aplicaciones recibirán las solicitudes del equilibrador de carga interno.

Tipos de direcciones IP

El tipo de dirección IP que especifique para su equilibrador de carga determina cómo los clientes pueden comunicarse con el equilibrador de carga.

- IPv4 únicamente: los clientes se comunican mediante IPv4 direcciones públicas y privadas. Las subredes que selecciones para tu balanceador de cargas deben tener rangos de IPv4 direcciones.
- Dualstack: los clientes se comunican mediante direcciones y direcciones públicas y privadas. IPv4 IPv6 Las subredes que selecciones para tu balanceador de cargas deben tener IPv4 un rango de direcciones. IPv6
- Dualstack sin público IPv4: los clientes se comunican mediante direcciones públicas y privadas y IPv6 direcciones privadas. IPv4 Las subredes que selecciones para tu balanceador de cargas deben tener IPv4 un rango de direcciones. IPv6 Esta opción no es compatible con el esquema del equilibrador de carga `internal`.

En la siguiente tabla se describen los tipos de direcciones IP compatibles con cada tipo de equilibrador de carga.

Tipo de balanceador de carga	IPv4 únicamente	Pila doble	Dualstack sin público IPv4
Equilibrador de carga de aplicación	Sí	Sí	Sí
Equilibrador de carga de red	Sí	Sí	No
Gateway Load Balancer	Sí	Sí	No
Equilibrador de carga clásico	Sí	No	No

El tipo de dirección IP que especifique para su grupo de destino determina la forma en que el equilibrador de carga se puede comunicar con los destinos.

- IPv4 únicamente: el balanceador de cargas se comunica mediante direcciones privadas. IPv4 Debe registrar los destinos con IPv4 direcciones de un grupo IPv4 objetivo.
- IPv6 únicamente: el balanceador de cargas se comunica mediante IPv6 direcciones. Debe registrar los destinos con IPv6 direcciones en un grupo IPv6 objetivo. El grupo de destino debe usarse con un equilibrador de carga de pila doble.

En la siguiente tabla se describen los tipos de direcciones IP compatibles con cada protocolo de grupo de destino.

Protocolo del grupo de destino	IPv4 únicamente	IPv6 solo	
HTTP y HTTPS	Sí	Sí	
TCP	Sí	Sí	
TLS	Sí	Sí	
UDP y TCP_UDP	Sí	Sí	
GENEVE	-	-	

MTU de red para su equilibrador de carga

La unidad de transmisión máxima (MTU) determina el tamaño, en bytes, del mayor paquete que se puede enviar a través de la red. Cuanto mayor sea la MTU de una conexión, mayor cantidad de datos se podrán transferir en un solo paquete. Los marcos Ethernet consisten del packet, o los datos que está enviando, y de la información de sobrecarga de red que lo rodea. El tráfico enviado a través de una puerta de enlace de Internet tiene una MTU de 1500. Esto significa que si un paquete tiene más de 1500 bytes, se fragmenta para enviarlo mediante varios marcos, o se descarta si `Don't Fragment` está establecido en el encabezado de IP.

El tamaño de la MTU en los nodos del equilibrador de carga no se puede configurar. Los marcos gigantes (MTU 9001) son estándar en todos los nodos de equilibradores de carga para los equilibradores de carga de aplicaciones, Equilibradores de carga de red y Equilibradores de carga clásicos. Los equilibradores de carga de puerta de enlace admiten 8500 MTU. Para obtener más información, consulte Unidad de transmisión máxima (MTU) en la Guía del usuario de equilibradores de carga de puerta de enlace.

La MTU de la ruta es tamaño máximo del paquete admitido en la ruta entre el host de origen y el host receptor. La detección de la MTU de la ruta (PMTUD) se utiliza para determinar la MTU de la ruta entre dos dispositivos. La detección de la MTU de la ruta es especialmente importante si el cliente o el destino no admiten marcos gigantes.

Cuando un host envía un paquete mayor que la MTU del host receptor o que es mayor que la MTU de un dispositivo a lo largo de la ruta, el host o dispositivo receptor descarta el paquete y, a continuación, devuelve el siguiente mensaje ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (Type 3, Code 4)`. Esto indica al host transmisor que divida la carga útil en varios paquetes más pequeños y los retransmita.

Si se siguen descartando paquetes con un tamaño superior al de la MTU de la interfaz de cliente o de destino, es probable que la detección de la MTU de ruta (PMTUD) no funcione. Para evitarlo, asegúrese de que la detección de la MTU de ruta funcione de principio a fin y de que haya habilitados marcos gigantes en sus clientes y destinos. Para obtener más información sobre Path MTU Discovery y la activación de tramas gigantes, consulte Path MTU Discovery en la Guía del usuario de Amazon EC2 .

Introducción a Elastic Load Balancing

Elastic Load Balancing admite varios tipos de balanceadores de carga. Puede seleccionar el tipo de equilibrador de carga que mejor se adapte a sus necesidades. Para obtener más información, consulte .

Para ver demostraciones de configuraciones del equilibrador de carga, consulte Demostraciones de Elastic Load Balancing.

Si ya posee un Equilibrador de carga clásico existente, puede migrar a un Equilibrador de carga de aplicación o a un Equilibrador de carga de red. Para obtener más información, consulte Migrar el Equilibrador de carga clásico.

Contenido

Creación de un Equilibrador de carga de aplicación

Para crear un balanceador de carga de aplicaciones mediante el AWS Management Console, consulte Introducción a los balanceadores de carga de aplicaciones en la Guía del usuario de balanceadores de carga de aplicaciones.

Para crear un balanceador de carga de aplicaciones mediante el AWS CLI, consulte Creación de un balanceador de carga de aplicaciones mediante AWS CLI el en la Guía del usuario de balanceadores de carga de aplicaciones.

Crear un equilibrador de carga de red

Para crear un balanceador de carga de red mediante el AWS Management Console, consulte Introducción a los balanceadores de carga de red en la Guía del usuario de los balanceadores de carga de red.

Para crear un balanceador de carga de red mediante el AWS CLI, consulte Creación de un balanceador de carga de red mediante AWS CLI el en la Guía del usuario de balanceadores de carga de red.

Creación de un equilibrador de carga de puerta de enlace

Para crear un balanceador de carga de puerta de enlace con AWS Management Console, consulte Introducción a los balanceadores de carga de puerta de enlace en la Guía del usuario de los balanceadores de carga de puerta de enlace.

Para crear un balanceador de carga de puerta de enlace mediante el AWS CLI, consulte Cómo empezar a utilizar los balanceadores de carga de puerta de enlace AWS CLI en la Guía del usuario de los balanceadores de carga de puerta de enlace.

Seguridad en Elastic Load Balancing

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de un centro de datos y una arquitectura de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a Elastic Load Balancing, consulte AWS los servicios incluidos en el ámbito por programa de conformidad y .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Este documento ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Elastic Load Balancing. Muestra cómo configurar Elastic Load Balancing para satisfacer sus destinos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que le ayudan a monitorear y proteger sus recursos de Elastic Load Balancing.

Con un equilibrador de carga de puerta de enlace, usted es responsable de elegir y calificar el software de los proveedores de dispositivos. Debe confiar en el software del dispositivo para inspeccionar o modificar el tráfico del equilibrador de carga, que opera en la capa 3 del modelo de interconexión de sistemas abiertos (OSI), es decir, la capa de red. Los proveedores de dispositivos que figuran como socios de Elastic Load Balancing han integrado y calificado el software de sus dispositivos AWS. Puede depositar un mayor grado de confianza en el software para dispositivos por parte de los proveedores de esta lista. Sin embargo, AWS no garantiza la seguridad ni la fiabilidad del software de estos proveedores.

Contenido

- Validación de conformidad para Elastic Load Balancing
- Resiliencia en Elastic Load Balancing
- Seguridad de infraestructuras en Elastic Load Balancing
- Acceder a Elastic Load Balancing mediante un punto de conexión de interfaz (AWS PrivateLink)

Protección de datos en Elastic Load Balancing

El modelo de se aplica a protección de datos en Elastic Load Balancing. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información

sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Elastic Load Balancing u otro dispositivo Servicios de AWS mediante la consola AWS CLI, la API o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Si habilita el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) para el bucket de S3 para los registros de acceso de Elastic Load Balancing, y este cifra automáticamente cada archivo de registro de acceso antes de que se almacene en el bucket de S3. Elastic Load Balancing también descifra los archivos de registro de acceso cuando se accede a ellos. Cada archivo de registro se cifra con una clave única, que a su vez se cifra con una clave de KMS que se rota periódicamente.

Cifrado en tránsito

Elastic Load Balancing simplifica el proceso de creación de aplicaciones web seguras al terminar el tráfico HTTPS y TLS de los clientes en el equilibrador de carga. El balanceador de cargas se encarga de cifrar y descifrar el tráfico, en lugar de requerir que cada EC2 instancia se encargue del trabajo antes de la finalización del TLS. Al configurar un oyente seguro, se especifican los conjuntos de cifrado y las versiones de protocolo compatibles con la aplicación, así como un certificado de servidor para instalar en el equilibrador de carga. Puede usar AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) para administrar los certificados de su servidor. Oyentes HTTPS para Equilibrador de carga de aplicación Oyentes TLS para Equilibradores de carga de red Los Equilibradores de carga clásicos son compatibles con los oyentes HTTPS y TLS.

Administración de identidad y de acceso para Elastic Load Balancing

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Elastic Load Balancing. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Contenido

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en Elastic Load Balancing.

Usuario de servicio: si utiliza el servicio de Elastic Load Balancing para realizar el trabajo, el administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Elastic Load Balancing para realizar el trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador.

Administrador de servicio: si está a cargo de los recursos de Elastic Load Balancing en la empresa, probablemente tenga acceso completo a Elastic Load Balancing. Su trabajo consiste en determinar a qué características y recursos de Elastic Load Balancing deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM.

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Elastic Load Balancing.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren

que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales

temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, en algunos casos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre

la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad

principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.

- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Elastic Load Balancing con IAM

Antes de utilizar IAM para administrar el acceso a Elastic Load Balancing, conozca qué características de IAM se pueden utilizar con Elastic Load Balancing.

Características de IAM que puede utilizar con Elastic Load Balancing

Característica de IAM	Elastic Load Balancing admite
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí

Característica de IAM	Elastic Load Balancing admite
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Políticas basadas en identidad de Elastic Load Balancing

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Políticas basadas en recursos en Elastic Load Balancing

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las

políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones de políticas de Elastic Load Balancing

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Elastic Load Balancing, consulte Acciones definidas por Elastic Load Balancing en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Elastic Load Balancing utilizan el siguiente prefijo antes de la acción:

```
elasticloadbalancing
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver la lista completa de las acciones del API para Elastic Load Balancing, consulte la documentación siguiente:

- Equilibradores de carga de aplicaciones, Equilibradores de carga de red y equilibradores de carga de puerta de enlace: versión 2015-12-01 de referencia de API
- Equilibradores de carga clásicos: Referencia del API versión 2012-06-01

Recursos de políticas de Elastic Load Balancing

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Algunas acciones de la API de Elastic Load Balancing admiten varios recursos. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de Elastic Load Balancing y sus tipos ARNs, consulte Recursos definidos por Elastic Load Balancing en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Elastic Load Balancing.

Claves de condición de política para Elastic Load Balancing

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Elastic Load Balancing, consulte Claves de condición para Elastic Load Balancing en la Referencia de autorizaciones de servicio. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Elastic Load Balancing.

Clave de condición de **`elasticloadbalancing:ResourceTag`**

La clave`elasticloadbalancing:ResourceTag/`*`key`*condition es específica de Elastic Load Balancing. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

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

API versión 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

Clave de condición de **elasticloadbalancing:ListenerProtocol**

La clave de condición elasticloadbalancing:ListenerProtocol se puede usar para las condiciones que definen los tipos de oyentes que se pueden crear y usar. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

- CreateListener
- ModifyListener

API versión 2012-06-01

- CreateLoadBalancer
- CreateLoadBalancerListeners

La política está disponible para los Equilibradores de carga de aplicación, los Equilibradores de carga de red y los Equilibradores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar uno de los protocolos especificados para su oyente.

Protocolos admitidos:

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

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

Clave de condición de **`elasticloadbalancing:SecurityPolicy`**

La clave de condición `elasticloadbalancing:SecurityPolicy` se puede usar en las condiciones que definen y aplican políticas de seguridad específicas en los equilibradores de carga. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

- `CreateListener`
- `ModifyListener`

API versión 2012-06-01

- `CreateLoadBalancerPolicy`
- `SetLoadBalancerPoliciesOfListener`

La política está disponible para los Equilibradores de carga de aplicación, los Equilibradores de carga de red y los Equilibradores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar una de las políticas de seguridad especificadas para su equilibrador de carga.

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

Clave de condición de `elasticloadbalancing:Scheme`

La clave de condición `elasticloadbalancing:Scheme` se puede usar para las condiciones que definen qué esquema se puede seleccionar durante la creación del equilibrador de carga. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

- `CreateLoadBalancer`

API versión 2012-06-01

- `CreateLoadBalancer`

La política está disponible para los Equilibradores de carga de aplicación, los Equilibradores de carga de red y los Equilibradores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar uno de los esquemas especificados para su equilibrador de carga.

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

Clave de condición de `elasticloadbalancing:Subnet`

> **Important**
>
> Elastic Load Balancing acepta todas las mayúsculas de Subnet. IDs Sin embargo, asegúrese de utilizar los operadores de condición adecuados que no distingan mayúsculas de minúsculas; por ejemplo, `StringEqualsIgnoreCase`.

La clave de condición `elasticloadbalancing:Subnet` se puede usar en las condiciones que definen qué subredes se pueden crear y conectar a los equilibradores de carga. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

- `CreateLoadBalancer`
- `SetSubnets`

API versión 2012-06-01

- `CreateLoadBalancer`
- `AttachLoadBalancerToSubnets`

La política está disponible para los Equilibradores de carga de aplicación, los Equilibradores de carga de red, los Equilibradores de carga de puerta de enlace y los Equilibradores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar una de las subredes especificadas para su equilibrador de carga.

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

Clave de condición de **elasticloadbalancing:SecurityGroup**

> **Important**
>
> Elastic Load Balancing acepta todas las mayúsculas de. SecurityGroup IDs Sin embargo, asegúrese de utilizar los operadores de condición adecuados que no distingan mayúsculas de minúsculas; por ejemplo, `StringEqualsIgnoreCase`.

La clave de condición `elasticloadbalancing:SecurityGroup` se puede usar en las condiciones que definen qué grupos de seguridad se pueden aplicar a los equilibradores de carga. Las siguientes acciones admiten esta clave de condición:

API versión 2015-12-01

- `CreateLoadBalancer`
- `SetSecurityGroups`

API versión 2012-06-01

- `CreateLoadBalancer`
- `ApplySecurityGroupsToLoadBalancer`

La política está disponible para los Equilibradores de carga de aplicación, los Equilibradores de carga de red y los Equilibradores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar uno de los grupos de seguridad especificados para su equilibrador de carga.

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

```
                "elasticloadbalancing:SecurityGroup": [
                    "sg-51530134",
                    "sg-51530144",
                    "sg-51530139"
                ]
            },
        }
    }
}
```

ACLs en Elastic Load Balancing

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Elastic Load Balancing

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Elastic Load Balancing

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios para Elastic Load Balancing

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Elastic Load Balancing

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Roles vinculados a servicios para Elastic Load Balancing

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de Elastic Load Balancing, consulte Rol vinculado al servicio de Elastic Load Balancing.

Permisos de la API de Elastic Load Balancing para etiquetar recursos durante la creación

Para que los usuarios etiqueten los recursos durante su creación, es preciso que tengan permisos para utilizar la acción que crea el recurso, como `elasticloadbalancing:CreateLoadBalancer` o `elasticloadbalancing:CreateTargetGroup`. Si se especifican etiquetas en la acción de creación de recursos, se requieren una autorización adicional en la acción `elasticloadbalancing:AddTags` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, los usuarios también deben tener permisos explícitos para usar la acción `elasticloadbalancing:AddTags`.

En la definición de la política de IAM de la acción `elasticloadbalancing:AddTags`, puede utilizar el elemento `Condition` con la clave de condición `elasticloadbalancing:CreateAction` para otorgar permisos de etiquetado a la acción que crea el recurso.

En el ejemplo siguiente se muestra una política que permite a los usuarios crear grupos de destino y aplicarles cualquier etiqueta durante la creación. No se permite a los usuarios etiquetar ningún recurso (no pueden llamar directamente a la acción `elasticloadbalancing:AddTags`).

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

Asimismo, la siguiente política permite a los usuarios crear un equilibrador de carga y aplicar etiquetas durante la creación. No se permite a los usuarios etiquetar ningún recurso (no pueden llamar directamente a la acción `elasticloadbalancing:AddTags`).

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

```
      "Action": [
         "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
             "elasticloadbalancing:CreateAction" : "CreateLoadBalancer"
          }
       }
    }
  ]
}
```

La acción `elasticloadbalancing:AddTags` solo se evalúa si se aplican etiquetas durante la acción de creación de recursos. Por lo tanto, un usuario que tenga permisos para crear un recurso (suponiendo que no existan condiciones de etiquetado) no necesita permisos para utilizar la acción `elasticloadbalancing:AddTags` si no se especifica ninguna etiqueta en la solicitud. Sin embargo, si el usuario intenta crear un recurso con etiquetas, la solicitud dará un error si el usuario no tiene permisos para utilizar la acción `elasticloadbalancing:AddTags`.

Rol vinculado al servicio de Elastic Load Balancing

Elastic Load Balancing utiliza un rol vinculado a servicios para los permisos que necesita para llamar a otros servicios de AWS en su nombre. Para obtener más información, consulte Roles vinculados al servicio en la Guía del usuario de IAM.

Permisos concedidos por el rol vinculado a servicios

Elastic Load Balancing usa el rol vinculado al servicio denominado AWSServiceRoleForElasticLoadBalancing para llamar a otros AWS servicios en su nombre.

AWSServiceRoleForElasticLoadBalancing confía en que el `elasticloadbalancing.amazonaws.com` servicio asuma la función.

La política de permisos del rol es AWSElasticLoadBalancingServiceRolePolicy. Para ver los permisos de esta política, consulte AWSElasticLoadBalancingServiceRolePolicyen la Referencia de políticas AWS gestionadas.

Creación del rol vinculado a servicios

No es necesario crear manualmente el AWSServiceRoleForElasticLoadBalancing rol. Elastic Load Balancing crea este rol automáticamente al crear un equilibrador de carga o un grupo de destino.

Para que Elastic Load Balancing cree un rol vinculado a servicio en su nombre, debe contar con los permisos necesarios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Editar el rol vinculado a servicios

Puede editar la descripción de AWSServiceRoleForElasticLoadBalancing utilizando IAM. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminar el rol vinculado a servicios

Si ya no necesita usar Elastic Load Balancing, le recomendamos que elimine AWSServiceRoleForElasticLoadBalancing.

Puede eliminar este rol vinculado al servicio solo después de eliminar todos los balanceadores de carga de su cuenta. AWS Esto garantiza que no pueda eliminar accidentalmente el permiso para acceder a sus equilibradores de carga. Para obtener más información, consulte Eliminar un equilibrador de carga de aplicaciones, Eliminar un Equilibrador de carga de red y Eliminar un Equilibrador de carga clásico.

Puede utilizar la consola, la CLI o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Después de eliminarlo AWSServiceRoleForElasticLoadBalancing, Elastic Load Balancing vuelve a crear el rol si se crea un balanceador de carga.

AWS políticas gestionadas para Elastic Load Balancing

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen

todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSElasticLoadBalancingClassicServiceRolePolicy

Esta política incluye todos los permisos que Elastic Load Balancing (Classic Load Balancer) requiere para llamar a otros AWS servicios en su nombre. Los roles vinculados a servicios están predefinidos. Con los roles predefinidos, ya no tendrá que agregar manualmente los permisos necesarios para que Elastic Load Balancing complete acciones en su nombre. No puede adjuntar, separar, modificar ni eliminar esta política.

Para ver los permisos de esta política, consulte AWSElasticLoadBalancingClassicServiceRolePolicyen la Referencia de políticas AWS gestionadas.

AWS política gestionada: AWSElasticLoadBalancingServiceRolePolicy

Esta política incluye todos los permisos que Elastic Load Balancing requiere para llamar a otros servicios de AWS en su nombre. Los roles vinculados a servicios están predefinidos. Con los roles predefinidos, ya no tendrá que agregar manualmente los permisos necesarios para que Elastic Load Balancing complete acciones en su nombre. No puede adjuntar, separar, modificar ni eliminar esta política.

Para ver los permisos de esta política, consulte AWSElasticLoadBalancingServiceRolePolicyen la Referencia de políticas AWS gestionadas.

AWS política gestionada: ElasticLoadBalancingFullAccess

Esta política proporciona acceso total al servicio Elastic Load Balancing y acceso limitado a otros servicios a través de la consola AWS de administración.

Para ver los permisos de esta política, consulte ElasticLoadBalancingFullAccessen la Referencia de políticas AWS gestionadas.

AWS política gestionada: ElasticLoadBalancingReadOnly

Esta política proporciona acceso de solo lectura a los servicios de Elastic Load Balancing y a los servicios dependientes.

Para ver los permisos de esta política, consulte ElasticLoadBalancingReadOnlyen la Referencia de políticas AWS gestionadas.

Actualizaciones de Elastic Load Balancing a las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas de Elastic Load Balancing desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
AWSElasticLoadBalancingServiceRolePolicy: actualización de una política existente	Se agregó la `ec2:AllocateIpamPoolCidr` acción para conceder permisos para asignar bloques de CIDR de los grupos de IPAM.	17 de febrero de 2025
ElasticLoadBalancingFullAccess: actualización de una política existente	Se agregaron las `arc-zonal-shift:*` acciones para conceder los permisos necesarios para el cambio zonal.	28 de noviembre de 2023
ElasticLoadBalancingReadOnly: actualización de una política existente	Se agregaron las siguientes acciones para conceder los permisos necesarios para el cambio zonal:`arc-zonal-shift:GetManagedResource` , `yarc-zonal-shift:ListManagedResources` . `arc-zonal-shift:ListZonalShifts`	28 de noviembre de 2023
AWSElasticLoadBalancingServiceRolePolicy: actualización de una política existente	Se agregó la `ec2:DescribeVpcPeeringConnections` acción para conceder los permisos necesarios para las conexiones entre pares.	11 de octubre de 2021
ElasticLoadBalancingFullAccess: actualización de una política existente	Se agregó la `ec2:DescribeVpcPeeringConnections` acción para conceder	11 de octubre de 2021

Cambio	Descripción	Fecha
	los permisos necesarios para las conexiones entre pares.	
ElasticLoadBalancingFullAccess: política nueva	Proporciona acceso completo a Elastic Load Balancing y a los servicios dependientes.	20 de septiembre de 2018
ElasticLoadBalancingReadOnly: política nueva	Proporciona acceso de solo lectura a los servicios de Elastic Load Balancing y a los servicios dependientes.	20 de septiembre de 2018
Elastic Load Balancing comenzó el seguimiento de los cambios	Elastic Load Balancing comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	20 de septiembre de 2018

Validación de conformidad para Elastic Load Balancing

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Elastic Load Balancing

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Además de la infraestructura AWS global, Elastic Load Balancing ofrece las siguientes funciones para respaldar la resiliencia de los datos:

- Distribuye el tráfico entrante entre las distintas instancias en una única o en varias zonas de disponibilidad.
- Puede utilizarlos AWS Global Accelerator con sus balanceadores de carga de aplicaciones para distribuir el tráfico entrante entre varios balanceadores de carga en una o más regiones. AWS Para obtener más información, consulte la Guía para desarrolladores de AWS Global Accelerator.
- Amazon ECS le permite ejecutar, detener y gestionar contenedores de Docker en un clúster de EC2 instancias. Puede configurar el servicio de Amazon ECS para que utilice un equilibrador de carga para distribuir el tráfico entrante entre los servicios de un clúster. Para obtener más información, consulte Amazon Elastic Container Service Developer Guide (Guía para desarrolladores de Amazon Elastic Container Service).

Seguridad de infraestructuras en Elastic Load Balancing

Como servicio gestionado, Elastic Load Balancing está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Elastic Load Balancing a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una nube privada virtual (VPC) es una red virtual en su propia área aislada lógicamente en la nube. AWS Una subred es un rango de direcciones IP de una VPC. Al crear un equilibrador de

carga, puede especificar una o varias subredes para los nodos del equilibrador de carga. Puede implementar EC2 instancias en las subredes de su VPC y registrarlas en su balanceador de carga. Para obtener más información sobre la VPC y subredes en la Guía del usuario de Amazon VPC.

Cuando crea un equilibrador de carga en una VPC, puede estar orientado a Internet o ser interno. Un equilibrador de carga interno solo puede direccionar las solicitudes que proceden de los clientes que tienen acceso a la VPC para el equilibrador de carga.

El equilibrador de carga envía solicitudes a sus destinos registrados mediante direcciones IP privadas. Por lo tanto, los destinos no necesitan direcciones IP públicas para recibir solicitudes de un equilibrador de carga.

Para llamar a la API de Elastic Load Balancing desde la VPC mediante direcciones IP privadas, use AWS PrivateLink. Para obtener más información, consulte Acceder a Elastic Load Balancing mediante un punto de conexión de interfaz (AWS PrivateLink).

Control del tráfico de red

Tenga en cuenta las siguientes opciones para proteger el tráfico de red cuando utilice un equilibrador de carga:

- Utilice oyentes seguros para respaldar la comunicación cifrada entre los clientes y sus equilibradores de carga. Oyentes HTTPS para Equilibrador de carga de aplicación Oyentes TLS para Equilibradores de carga de red Los Equilibradores de carga clásicos son compatibles con los oyentes HTTPS y TLS. Puede elegir entre políticas de seguridad predefinidas para el equilibrador de carga con el fin de especificar los conjuntos de cifrado y las versiones de protocolo compatibles con la aplicación. Puedes usar AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) para administrar los certificados de servidor instalados en tu balanceador de cargas. Puede utilizar el protocolo de indicación de nombre de servidor (SNI) para servir a varios sitios web seguros mediante un único oyente seguro. SNI se habilita automáticamente para el equilibrador de carga cuando asocia más de un certificado de servidor a un oyente seguro.
- Configure los grupos de seguridad para sus equilibradores de carga de aplicaciones y Equilibradores de carga clásicos con el fin de aceptar tráfico solo de clientes específicos. Estos grupos de seguridad deben permitir el tráfico entrante de los clientes en los puertos de escucha y el tráfico saliente a los clientes.
- Configura los grupos de seguridad de tus EC2 instancias de Amazon para que solo acepten tráfico del balanceador de cargas. Estos grupos de seguridad deben permitir el tráfico entrante desde el equilibrador de carga en los puertos de oyente y en los puertos de comprobación de estado.

- Configure su Equilibrador de carga de aplicación para autenticar a los usuarios de forma segura a través de un proveedor de identidades o mediante identidades corporativas. Para obtener más información, consulte Autenticar usuarios mediante un Equilibrador de carga de aplicación.
- Use AWS WAF con su Equilibrador de carga de aplicación para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (ACL web).

Acceder a Elastic Load Balancing mediante un punto de conexión de interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre su nube privada virtual (VPC) y la API de Elastic Load Balancing al crear un punto de conexión de VPC de tipo interfaz. Puede utilizar esta conexión para llamar a la API de Elastic Load Balancing desde su VPC sin necesidad de conectar una puerta de enlace de Internet, una instancia de NAT o una conexión de VPN a su VPC. El punto de conexión proporciona conectividad confiable y escalable a la API de Elastic Load Balancing, versiones 2015-12-01 y 2012-06-01, que se usa para crear y administrar los equilibradores de carga.

Los puntos finales de la VPC de interfaz cuentan con una función que permite la comunicación entre sus aplicaciones y el Servicios de AWS uso de direcciones IP privadas. AWS PrivateLink Para obtener más información, consulte AWS PrivateLink.

Límite

AWS PrivateLink no admite balanceadores de carga de red con más de 50 oyentes.

Crear un punto de conexión de interfaz para Elastic Load Balancing

Cree un punto de conexión para Elastic Load Balancing utilizando el siguiente nombre de servicio:

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

Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Crear un punto de conexión de VPC para Elastic Load Balancing

Puede asociar una política a su punto de conexión de VPC para controlar el acceso a la API de Elastic Load Balancing. La política especifica:

- La entidad de seguridad que puede realizar acciones.
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

En el ejemplo siguiente se muestra una política de punto de conexión de VPC que deniega a todos los usuarios el permiso para crear un equilibrador de carga a través del punto de conexión. La política de ejemplo también concede permiso a todos los usuarios para realizar todas las demás acciones.

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

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Registra las llamadas a la API para Elastic Load Balancing mediante AWS CloudTrail

Elastic Load Balancing está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura las llamadas a la API de Elastic Load Balancing como eventos. Las llamadas capturadas incluyen llamadas desde AWS Management Console y llamadas de código a las operaciones de la API de Elastic Load Balancing. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Elastic Load Balancing, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en su cuenta Cuenta de AWS cuando crea la cuenta y tiene acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Cómo trabajar con el historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

> Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu

Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Eventos de administración de Elastic Load Balancing en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Elastic Load Balancing registra las operaciones de plano de control como eventos de administración. Para ver la lista de operaciones del plano de control, consulte lo siguiente:

- Equilibradores de carga de aplicación: versión 2015-12-01 de la referencia de API de Elastic Load Balancing
- Equilibradores de carga de red: versión 2015-12-01 de la referencia de API de Elastic Load Balancing
- Equilibradores de carga de puerta de enlace: versión 2015-12-01 de la referencia de API de Elastic Load Balancing
- Equilibradores de carga de clásicos: versión 2012-06-01 de la referencia de API de Elastic Load Balancing

Ejemplos de eventos de Elastic Load Balancing

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

En los siguientes ejemplos, se muestran CloudTrail los eventos de un usuario que creó un balanceador de cargas y, después, lo eliminó con. AWS CLI Puede identificar la CLI mediante los elementos `userAgent`. Puede identificar las llamadas al API solicitadas mediante los `eventName`. Encontrará la información sobre el usuario (`Alice`) en el elemento `userIdentity`.

Example Ejemplo 1: CreateLoadBalancer desde la API ELBv2


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "application",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```


Example Ejemplo 2: DeleteLoadBalancer desde la ELBv2 API


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
```

```
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Ejemplo 3: CreateLoadBalancer desde la API del ELB

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-12345678","subnet-76543210"],
        "loadBalancerName": "my-load-balancer",
```

```
        "listeners": [{
           "protocol": "HTTP",
           "loadBalancerPort": 80,
           "instanceProtocol": "HTTP",
           "instancePort": 80
        }]
    },
    "responseElements": {
        "dNSName": "my-loadbalancer-1234567890.elb.amazonaws.com"
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Example Ejemplo 4: DeleteLoadBalancer desde la API del ELB

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-08T12:39:25Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerName": "my-load-balancer"
    },
    "responseElements": null,
    "requestID": "f0f17bb6-b9ba-11e3-9b20-999fdEXAMPLE",
    "eventID": "4f99f0e8-5cf8-4c30-b6da-3b69fEXAMPLE"
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
```

```
    "recipientAccountId": "123456789012"
}
```

Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Migrar el Equilibrador de carga clásico

Elastic Load Balancing admite los siguientes equilibradores de carga: equilibradores de carga de aplicaciones, Equilibradores de carga de red, equilibradores de carga de puerta de enlace y Equilibradores de carga clásicos. Para obtener información sobre las distintas funciones de cada tipo de balanceador de carga, consulta Características de Elastic Load Balancing.

También tiene la opción de migrar un Equilibrador de carga clásico existente en una VPC a un Equilibrador de carga de aplicación o a un Equilibrador de carga de red.

Ventajas de migrar desde un Equilibrador de carga clásico

Cada tipo de equilibrador de carga tiene sus propias características, funciones y configuraciones únicas. Revise las ventajas de cada equilibrador de carga para decidir cuál es el mejor para usted.

Application Load Balancer

Utilizar un Equilibrador de carga de aplicación en lugar de un Equilibrador de carga clásico tiene los siguientes beneficios:

Compatibilidad con:

- Condiciones de ruta, Condiciones de host y Condiciones de encabezado HTTP.
- Redirigir las solicitudes de una URL a otra y enrutar las solicitudes a varias aplicaciones en una sola EC2 instancia.
- Devolución de respuestas HTTP personalizadas.
- Registro de destinos por dirección IP y registro de funciones de Lambda como destinos. Inclusión de destinos situados fuera de la VPC para el equilibrador de carga.
- Autenticación de los usuarios mediante identidades corporativas o sociales.
- Aplicaciones en contenedores de Amazon Elastic Container Service (Amazon ECS).
- Supervisión independiente del estado de cada servicio.

Los registros de acceso contienen información adicional y se almacenan en formato comprimido.

Mejora del rendimiento general del equilibrador de carga.

Network Load Balancer

Utilizar un equilibrador de carga de red en lugar de un equilibrador de carga clásico tiene los siguientes beneficios:

Compatibilidad con:

- Direcciones IP estáticas, que permiten asignar una dirección IP elástica por cada subred habilitada en el equilibrador de carga.
- Registro de destinos por dirección IP, incluidos los destinos situados fuera de la VPC para el equilibrador de carga.
- Enrutamiento de solicitudes a varias aplicaciones en una sola EC2 instancia.
- Aplicaciones en contenedores de Amazon Elastic Container Service (Amazon ECS).
- Supervisión independiente del estado de cada servicio.

Capacidad para gestionar cargas de trabajo volátiles y escalar hasta millones de solicitudes por segundo.

Migración mediante el asistente de migración

El asistente de migración utiliza la configuración de su Equilibrador de carga clásico para crear un Equilibrador de carga de aplicación o un Equilibrador de carga de red equivalente. Reduce el tiempo y el esfuerzo necesarios para migrar un Equilibrador de carga clásico en comparación con otros métodos.

> **Note**
>
> El asistente crea un nuevo equilibrador de carga. El asistente no convierte el Equilibrador de carga clásico existente en un Equilibrador de carga de aplicación o un Equilibrador de carga de red. Debe redirigir el tráfico de forma manual al equilibrador de carga recién creado.

Limitaciones

- El nombre del nuevo equilibrador de carga no puede ser el mismo que el de un equilibrador de carga existente del mismo tipo y en la misma región.

- Si el Equilibrador de carga clásico tiene alguna etiqueta que contenga el prefijo `aws:` en su clave, esas etiquetas no se migran.

Al migrar a un Equilibrador de carga de aplicación

- Si el Equilibrador de carga clásico tiene una sola subred, debe especificar una segunda subred.
- Si el Equilibrador de carga clásico tiene oyentes HTTP/HTTPS que utilizan comprobaciones de estado TCP, el protocolo de comprobación de estado se actualiza a HTTP y la ruta se establece en "/".
- Si el Equilibrador de carga clásico tiene oyentes HTTPS que utilizan una política de seguridad personalizada o no compatible, el asistente de migración utiliza la política de seguridad predeterminada para el nuevo tipo de equilibrador de carga.

Al migrar a un Equilibrador de carga de red

- Los siguientes tipos de instancias no se registrarán en el nuevo grupo de destino: C1,, CC1, CC2, CG1, CG2, CR1, G1 CS1, G2,,, M1 HI1 HS1, M2, M3, T1
- Es posible que algunos parámetros de la comprobación de estado del Equilibrador de carga clásico no se puedan transferir al nuevo grupo de destino. Estos casos se indicarán como un cambio en la sección de resumen del asistente de migración.
- Si el Equilibrador de carga clásico tiene oyentes de SSL, el asistente de migración crea un oyente de TLS mediante el certificado y la política de seguridad del oyente de SSL.

Proceso del asistente de migración

Migración de un Equilibrador de carga clásico mediante el asistente de migración

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el Equilibrador de carga clásico que quiera migrar.
4. En la sección Detalles de los equilibradores de carga, seleccione Iniciar el asistente de migración.
5. Seleccione Migrar a Equilibrador de carga de aplicación o Migrar al Equilibrador de carga de red para abrir el asistente de migración.

6. En Asignar un nombre al nuevo equilibrador de carga, vaya a la opción Nombre del equilibrador de carga e introduzca un nombre para el nuevo equilibrador de carga.
7. En Asignar un nombre al nuevo grupo de destino y revisar destinos, vaya a Nombre del grupo de destino e introduzca un nombre para el nuevo grupo de destino.
8. (Opcional) En Destinos, puede revisar las instancias de destino que se registrarán en el nuevo grupo de destino.
9. (Opcional) En Revisar etiquetas, puede revisar las etiquetas que se aplicarán al nuevo equilibrador de carga
10. En Resumen del Equilibrador de carga de aplicación o en Resumen del Equilibrador de carga de red, revise y verifique las opciones de configuración que asignó el asistente de migración.
11. Cuando tenga un resumen de configuración que le satisfaga, elija Crear el Equilibrador de carga de aplicación o Crear el Equilibrador de carga de red para iniciar la migración.

Migración mediante la utilidad de copia del equilibrador de carga

Las utilidades de copia del balanceador de carga están disponibles en el repositorio de Elastic Load Balancing Tools, en la AWS GitHub página.

Recursos

- Herramientas de Elastic Load Balancing
- Utilidad de copia del Equilibrador de carga clásico al Equilibrador de carga de aplicación
- Utilidad de copia del Equilibrador de carga clásico al Equilibrador de carga de red

Migración manual del equilibrador de carga

La siguiente información proporciona instrucciones generales para crear manualmente un nuevo Equilibrador de carga de aplicación o Equilibrador de carga de red basado en un Equilibrador de carga clásico existente en una VPC. Puede migrar mediante el AWS Management Console AWS CLI, el o un AWS SDK. Para obtener más información, consulte Introducción a Elastic Load Balancing.

Una vez completado el proceso de migración, podrá sacar partido de las características del nuevo equilibrador de carga.

Proceso de migración manual

Paso 1: Crear un nuevo equilibrador de carga

Cree un equilibrador de carga con una configuración equivalente al Equilibrador de carga clásico para migrar.

1. Puede crear un nuevo equilibrador de carga con el mismo esquema (expuesto a Internet o interno), subredes y grupos de seguridad que el Equilibrador de carga clásico.
2. Cree un grupo de destino para el equilibrador de carga que tenga la misma configuración de comprobación de estado que el Equilibrador de carga clásico.
3. Realice una de las siguientes acciones:
   - Si el Equilibrador de carga clásico está asociado a un grupo de escalado automático, asocie su grupo de destino al grupo de escalado automático. Al hacerlo, además, se registran las instancias de escalado automático en el grupo de destino.
   - Registre sus EC2 instancias con su grupo objetivo.
4. Cree uno o varios oyentes, cada uno de ellos con una regla predeterminada que reenvíe las solicitudes al grupo de destino. Si crea un oyente HTTPS, puede especificar el mismo certificado que especificó para su Equilibrador de carga clásico. Le recomendamos que utilice la política de seguridad predeterminada.
5. Si el Equilibrador de carga clásico tiene etiquetas, revíselas y agregue las que sean pertinentes al nuevo equilibrador de carga.

Paso 2: Redireccionar gradualmente el tráfico al nuevo equilibrador de carga

Una vez registradas las instancias con el nuevo equilibrador de carga, puede comenzar el proceso de redireccionamiento del tráfico desde el anterior equilibrador de carga hacia este. Esto le permite probar su nuevo equilibrador de carga y, al mismo tiempo, minimizar el riesgo para la disponibilidad de su aplicación.

Para redireccionar gradualmente el tráfico al nuevo equilibrador de carga

1. Pegue el nombre de DNS del nuevo equilibrador de carga en el campo de direcciones de un navegador web conectado a Internet. Si todo funciona normalmente, el navegador mostrará la página predeterminada de la aplicación.
2. Cree un nuevo registro DNS que asocie el nombre de dominio con el nuevo equilibrador de carga. Si el servicio DNS admite la ponderación, especifique un peso de 1 en el nuevo registro

DNS y un peso de 9 en el registro DNS que ya existe del equilibrador de carga. De este modo, se redirigirá el 10 % del tráfico al nuevo equilibrador de carga y el 90 % del tráfico al equilibrador de carga.

3. Monitorice el nuevo equilibrador de carga para comprobar que recibe el tráfico y direcciona las solicitudes a las instancias.

> **Important**
>
> El time-to-live valor (TTL) del registro DNS es de 60 segundos. Esto significa que cualquier servidor DNS que resuelva el nombre de su dominio conserva la información de registro en su caché durante 60 segundos, mientras que los cambios se propagan. Por lo tanto, estos servidores DNS todavía pueden dirigir el tráfico a su anterior equilibrador de carga durante un máximo de 60 segundos después de completar el paso anterior. Durante la propagación, el tráfico podría dirigirse a cualquiera de los equilibradores de carga.

4. Continúe para actualizar la ponderación de los registros DNS hasta que todo el tráfico se dirija al nuevo equilibrador de carga. Cuando haya terminado, puede eliminar el registro DNS del anterior equilibrador de carga.

Paso 3: Actualizar las políticas, los scripts y el código

Si migró el Equilibrador de carga clásico a un Equilibrador de carga de aplicación o un Equilibrador de carga de red, asegúrese de hacer lo siguiente:

- Actualice las políticas de IAM que utilizan la versión 2012-06-01 del API para usar la versión 2015-12-01.
- Actualice los procesos que usan CloudWatch métricas del espacio de `AWS/ELB` nombres para que usen métricas del espacio de nombres or. `AWS/ApplicationELB` `AWS/NetworkELB`
- Actualice los scripts que usan aws elb AWS CLI comandos para usar comandos. aws elbv2 AWS CLI
- Actualice AWS CloudFormation las plantillas que utilizan el `AWS::ElasticLoadBalancing::LoadBalancer` recurso para utilizar los `AWS::ElasticLoadBalancingV2` recursos.
- Actualice el código que utiliza la versión 2012-06-01 de la API de Elastic Load Balancing a la versión 2015-12-01.

Recursos

- elbv2 en la Referencia del comando AWS CLI
- Versión 2015-12-01 de la referencia del API de Elastic Load Balancing
- Administración de identidad y de acceso para Elastic Load Balancing
- Métricas del Equilibrador de carga de aplicación en la Guía del usuario de equilibradores de carga de aplicaciones
- Métricas del Equilibrador de carga de red en la Guía del usuario para Equilibradores de carga de red
- AWS::ElasticLoadBalancingV2::LoadBalancer en la Guía del usuario de AWS CloudFormation .

Paso 4: Eliminar el Equilibrador de carga clásico

Puede eliminar el Equilibrador de carga clásico anterior después de lo siguiente:

- Haber redirigido todo el tráfico al nuevo equilibrador de carga.
- Haber completado todas las solicitudes existentes que se direccionaron al equilibrador de carga.

Impida que los usuarios creen balanceadores de carga clásicos

Puedes crear una política de IAM que impida a los usuarios crear balanceadores de carga clásicos en tu cuenta.

Tanto Elastic Load Balancing V2 como Elastic Load Balancing V1 APIs proporcionan una acción de `CreateLoadBalancer` API. Cuando creas un Classic Load Balancer, utilizas la acción de la API V1, que crea tanto el balanceador de cargas como los oyentes. Al crear un Application Load Balancer, Network Load Balancer o Gateway Load Balancer, se utiliza la acción de la API V2, que crea solo el balanceador de cargas. La API de la versión 2 proporciona una `CreateListener` acción que se utiliza para crear agentes de escucha para un balanceador de cargas después de crearlo.

La siguiente política deniega a los usuarios el permiso para crear un balanceador de cargas si se especifica el protocolo de escucha. Como debes configurar al menos un listener al crear un Classic Load Balancer, esta política impide que los usuarios creen Classic Load Balancer. No impide que los usuarios creen otros tipos de balanceadores de carga, ya que existen acciones de API independientes para crear esos balanceadores de carga y sus agentes de escucha.

```
{
    "Version": "2012-10-17",
    "Effect": "Deny",
    "Action": "elasticloadbalancing:CreateLoadBalancer",
    "Resource": [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    ],
    "Condition": {
        "Null": {
            "elasticloadbalancing:ListenerProtocol": false
        }
    }
}
```

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.