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, por ejemplo, instancias EC2, contenedores y direcciones IP en una o varias 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 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. Puede seleccionar el tipo de equilibrador de carga que mejor se adapte a sus necesidades. Para obtener más información, consulte Comparaciones de productos .

Para obtener más información sobre cómo usar cada equilibrador de carga, 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
- Guía del usuario para equilibradores de carga clásicos

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.
- Interfaz de línea de comandos de AWS (AWS CLI): proporciona comandos para un amplio conjunto de servicios de AWS, incluido Elastic Load Balancing. La AWS CLI es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.
- SDK de AWS: proporcionan API específicas de cada lenguaje y se encargan de muchos de los detalles de la conexión, como el cálculo de firmas, el control de reintentos de solicitud y el control de errores. Para obtener más información, consulte SDK de AWS.
- 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 lo siguiente:
  - Equilibradores de carga de aplicaciones y equilibradores de carga de red: versión de la API 2015-12-01
  - 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 las aplicaciones en la nube. Puede configurar el equilibrador de carga de modo que direccione el tráfico a las instancias EC2. Para obtener más información, consulte la Guía del usuario de Amazon EC2 para instancias de Linux o la Guía de Amazon EC2 para instancias de Windows.
- Amazon EC2 Auto Scaling: garantiza que está ejecutando el número deseado de instancias, incluso si una instancia falla. Amazon EC2 Auto Scaling también permite aumentar o disminuir automáticamente el número de instancias a medida que cambie la demanda de las instancias. 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 de Amazon EC2 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: permite monitorizar el equilibrador de carga y adoptar las medidas necesarias. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.
- Amazon ECS: permite ejecutar, detener y administrar contenedores Docker en un clúster de instancias EC2. 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 equilibradores de carga en una o varias regiones de AWS. Para obtener más información, consulte AWS Global Accelerator Developer Guide.
- 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 traduciría `www.example.com` en la dirección IP numérica `192.0.2.1`. AWSasigna direcciones URL a los recursos, como los equilibradores 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: 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). Para obtener más información, consulte AWS WAF Developer Guide.

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 equilibrador de carga acepta el tráfico entrante de los clientes y direcciona las solicitudes a sus destinos registrados (como por ejemplo instancias EC2) en una o varias 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.

Elastic Load Balancing admite los siguientes tipos de equilibradores de carga.

- equilibrador de carga de aplicaciones
- Equilibrador de carga de red
- Equilibradores de carga de puerta de enlace
- Equilibradores de carga clásicos

Hay una diferencia clave en el modo en que se configuran los tipos de equilibrador de carga. Con los equilibradores de carga de aplicaciones, los Equilibradores de carga de red y los equilibradores de carga de puerta de enlace, se registran los destinos en grupos de destino se dirige el tráfico a los grupos de destino. Con los Equilibradores de carga clásicos, las instancias se registran directamente con el equilibrador de carga.

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.

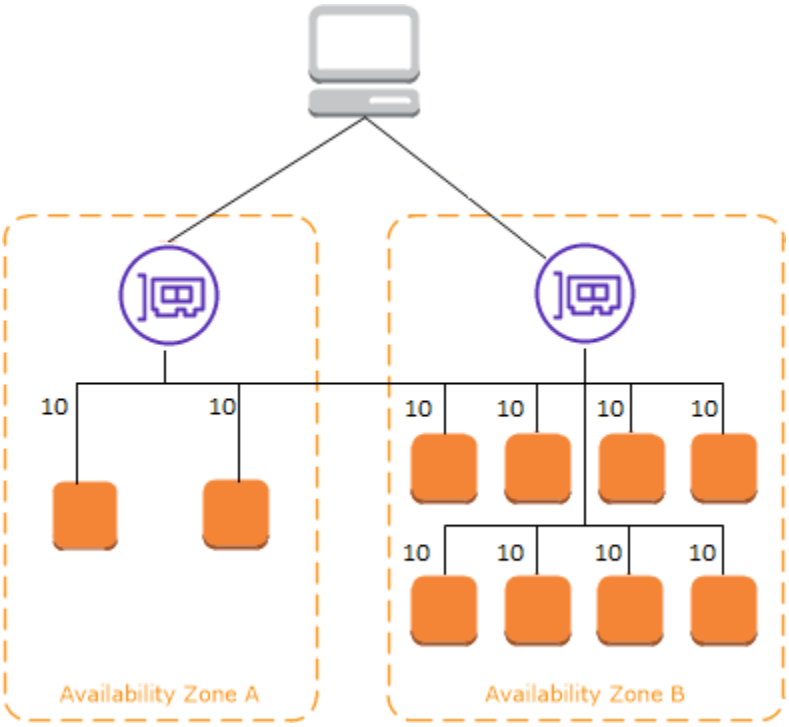
Después de deshabilitar una zona de disponibilidad, los destinos de esa zona de disponibilidad permanecen registrados en el equilibrador de carga. Sin embargo, aunque permanezcan registrados, el equilibrador de carga no envía el tráfico hacia ellos.

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.

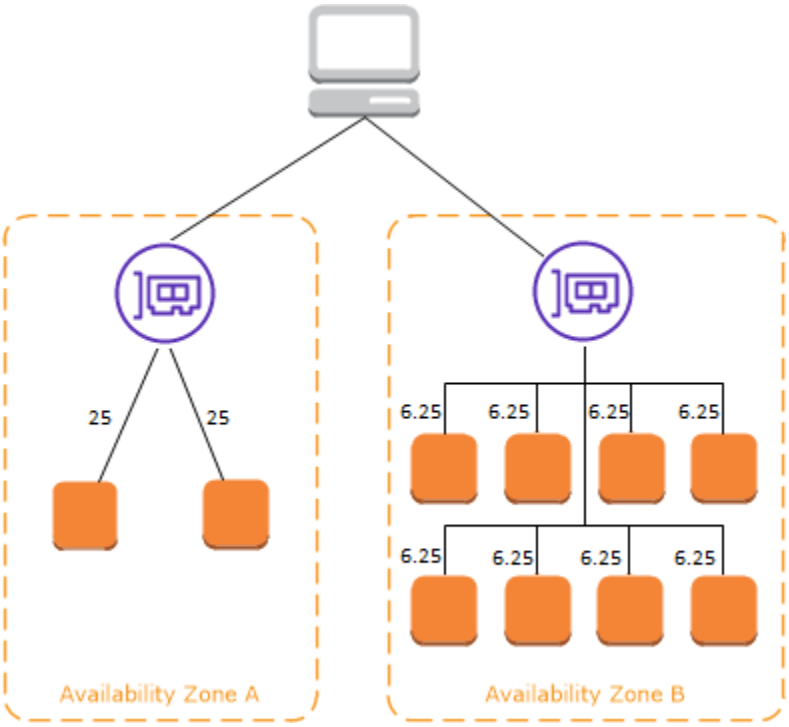
Si el equilibrio de carga entre zonas está habilitado, cada uno de los diez destinos recibirá un 10% del tráfico. Esto se debe a que cada nodo del equilibrador de carga puede dirigir el 50% del tráfico de los clientes a los diez destinos.



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.

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 para 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 de Amazon Route 53 (Route 53 ARC). 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. Route 53 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 de Amazon Route 53.

Los cambios de zona solo se admiten en los Equilibradores de carga de aplicación y en los Equilibradores de carga de red con el equilibrio de carga entre zonas desactivado. Si activa el equilibrio de carga entre zonas, no podrá iniciar un cambio de zona. Para obtener más información, consulte Recursos compatibles con los cambios de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

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

- El equilibrio de carga entre zonas no se admite con cambios de zona. Debe desactivar el equilibrio de carga entre zonas para utilizar esta capacidad.
- El cambio de zona no se admite cuando se utiliza un Equilibrador de carga de aplicación como punto de conexión del acelerador en AWS Global Accelerator.
- 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.
- Cuando un Equilibrador de carga de aplicación sea el destino de un Equilibrador de carga de red, comience siempre el cambio de zona desde el Equilibrador de carga de red. Si comienza un cambio de zona desde el Equilibrador de carga de aplicación, el Equilibrador de carga de red no reconoce el cambio y continúa enviando tráfico al Equilibrador de carga de aplicación.

A fin de obtener más información y orientación, consulte Prácticas recomendadas con los cambios de zona de Route 53 ARC en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

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 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.

Los balanceadores de carga de aplicaciones admiten 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.

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 paquete, o los datos reales 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 la detección de la MTU de ruta y sobre la activación de marcos gigantes, consulte Detección de la MTU de ruta en la Guía del usuario de Amazon EC2.

Introducción a Elastic Load Balancing

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. Puede seleccionar el tipo de equilibrador de carga que mejor se adapte a sus necesidades. Para obtener más información, consulte Comparaciones de productos .

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 equilibrador de carga de aplicación mediante la AWS Management Console, consulte Introducción al equilibrador de carga de redes en la Guía del usuario para equilibrador de carga de redes.

Para crear un equilibrador de carga de aplicación con AWS CLI, consulte Crear un equilibrador de carga de aplicación con AWS CLI en la Guía del usuario para equilibrador de carga de aplicaciones.

Crear un equilibrador de carga de red

Para crear un equilibrador de carga de red mediante la AWS Management Console, consulte Introducción al equilibrador de carga de redes en la User Guide for equilibrador de carga de redes.

Para crear un equilibrador de carga de red mediante la AWS CLI, consulte Crear un equilibrador de carga de red mediante AWS CLI en la Gía del usuario del equilibrador de carga de redes.

Creación del equilibrador de carga de puerta de enlace

Para crear un equilibrador de carga de puerta de enlace mediante la AWS Management Console, consulte Introducción al equilibrador de carga de puerta de enlace en la Guía del usuario del equilibrador de carga de redes.

Para crear un equilibrador de carga de puerta de enlace mediante la AWS CLI, consulte Introducción al equilibrador de carga de puerta de enlace de AWS CLI en la Guía del usuario del equilibrador de carga de puerta de enlace.

Para crear un equilibrador de carga clásico

Para crear un equilibrador de carga clásico mediante la AWS Management Console, consulte Crear un equilibrador de carga clásico en la Guía del usuario del equilibrador de carga clásico.

Seguridad en Elastic Load Balancing

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos que están diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Terceros clientes prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS. Para conocer los programas de conformidad que se aplican a Elastic Load Balancing, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS 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 puede aprender a utilizar otros servicios de AWS que ayudan a monitorear y proteger los 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 con 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. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte 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:

- Utilice 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
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice 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 140-2 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, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

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 otros dispositivos Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos 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 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 equilibrador de carga realiza el trabajo de cifrar y descifrar el tráfico, en lugar de requerir que cada instancia EC2 gestione el trabajo para la terminación de 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 un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos)

para utilizar recursos de Elastic Load Balancing. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Contenido

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que 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 ayudarlo 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 administrador 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 manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del IAM Identity Center), 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 administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

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

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de solicitudes, consulte Firma de solicitudes API de AWS 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, AWS le recomienda el uso de 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 Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice 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, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

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

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

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

Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de 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 puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo 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 permanentes a largo plazo y los roles proporcionan credenciales temporales.

Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del Usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de tu Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM 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 para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El 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, consulte 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. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común 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 a servicios.

  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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.
  - Rol vinculado a servicios: un rol vinculado a servicios 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 a servicios aparecen en la 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: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del Usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario

raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS 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. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. 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 utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del rol de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las 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. 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. Las entidades 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 se puede utilizar políticas de IAM administradas de AWS en una política basada en recursos.

Listas de control de acceso (ACL)

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

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. 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). Puede 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 servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de

la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.

- 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 obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte 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
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí

Característica de IAM	Elastic Load Balancing admite
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 identidades	Sí

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 adjunto. Para obtener más información sobre los elementos que puede utilizar en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Políticas basadas en recursos en Elastic Load Balancing

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. 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. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de 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 la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un 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 en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del Usuario de IAM.

Acciones de políticas de Elastic Load Balancing

Admite acciones de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS 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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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

Para obtener más información sobre los permisos necesarios para cada acción de Elastic Load Balancing, consulte Permisos de la API de Elastic Load Balancing.

Recursos de políticas de Elastic Load Balancing

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede 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). Puede 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, utilice 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 única instrucción, separe los ARN con comas.

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

Para ver una lista de los tipos de recursos de Elastic Load Balancing y sus ARN, consulte Recursos definidos por Elastic Load Balancing en la Referencia de autorizaciones de servicio. 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

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede 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. Puede crear expresiones condicionales que utilicen 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 lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte 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 globales de AWS, consulte Claves de contexto de condición globales de AWS 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 de condición `elasticloadbalancing:ResourceTag/`*`clave`* 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 elasticloadbalancing:ListenerProtocol condición 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 balanceadores de carga de aplicaciones, los balanceadores de carga de red y los balanceadores 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": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                    "elasticloadbalancing:ListenerProtocol": [
                    "HTTPS",
                    "TLS"
                    ]
```

```
            },
        }
```

Clave de condición de **elasticloadbalancing:SecurityPolicy**

La clave de `elasticloadbalancing:SecurityPolicy` condición se puede usar para las condiciones que definen y aplican políticas de seguridad específicas en los balanceadores 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 balanceadores de carga de aplicaciones, los balanceadores de carga de red y los balanceadores 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 balanceador de cargas.

```
"Resource": [
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals":{
                "elasticloadbalancing:SecurityPolicy": [
                    "ELBSecurityPolicy-TLS13-1-2-2021-06",
                    "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
                    "ELBSEcurityPolicy-TLS13-1-1-2021-06"
                ]
            },
```

```
        }
]
```

Clave de condición de `elasticloadbalancing:Scheme`

La clave de `elasticloadbalancing:Scheme` condición se puede usar para las condiciones que definen qué esquema se puede seleccionar durante la creación del balanceador 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 balanceadores de carga de aplicaciones, los balanceadores de carga de red y los balanceadores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar uno de los esquemas especificados para su balanceador de cargas.

```
"Version": "2015-12-01",
    "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 los ID de subred. Sin embargo, asegúrese de utilizar los operadores de condición adecuados que no distingan mayúsculas de minúsculas, por ejemplo. `StringEqualsIgnoreCase`

La clave de `elasticloadbalancing:Subnet` condición se puede usar para las condiciones que definen qué subredes se pueden crear y conectar a los balanceadores 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 balanceadores de carga de aplicaciones, los balanceadores de carga de red, los balanceadores de carga de gateway y los balanceadores de carga clásicos. El siguiente es un ejemplo de política que solo permite a los usuarios seleccionar una de las subredes especificadas para su balanceador de carga.

```
"Version": "2015-12-01",
    "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 los ID. Sin embargo, asegúrese de utilizar los operadores de condición adecuados que no distingan mayúsculas de minúsculas, por ejemplo. `StringEqualsIgnoreCase`

La clave de `elasticloadbalancing:SecurityGroup` condición se puede usar para las condiciones que definen qué grupos de seguridad se pueden aplicar a los balanceadores 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 balanceadores de carga de aplicaciones, los balanceadores de carga de red y los balanceadores 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 balanceador de cargas.

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

```
                "sg-51530144",
                "sg-51530139"
            ]
        },
    }
```

ACL en Elastic Load Balancing

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 entidades de IAM (usuarios o roles) y a muchos recursos de AWS. 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 ¿Qué es 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

Admite el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

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

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

Permisos de entidades principales entre servicios para Elastic Load Balancing

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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 servicios 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 a servicios aparecen en la 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

Debe conceder a los usuarios permisos para llamar a las acciones de la API de Elastic Load Balancing que necesiten. Además, para algunas acciones de Elastic Load Balancing, debe conceder a los usuarios permisos para llamar a acciones específicas de la API de Amazon EC2.

Permisos necesarios para la API 2015-12-01

Cuando llame a las siguientes acciones de la API 2015-12-01, debe conceder a los usuarios permiso para llamar a las acciones especificadas.

`CreateLoadBalancer`

- `elasticloadbalancing:CreateLoadBalancer`

- ec2:DescribeAccountAttributes
- ec2:DescribeAddresses
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- iam:CreateServiceLinkedRole

CreateTargetGroup

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

RegisterTargets

- elasticloadbalancing:RegisterTargets
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

SetIpAddressType

- elasticloadbalancing:SetIpAddressType
- ec2:DescribeSubnets

SetSubnets

- elasticloadbalancing:SetSubnets
- ec2:DescribeSubnets

Permisos necesarios para la API 2012-06-01

Cuando llame a las siguientes acciones de la API 2012-06-01, debe conceder a los usuarios permiso para llamar a las acciones especificadas.

ApplySecurityGroupsToLoadBalancer

- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer

- ec2:DescribeAccountAttributes
- ec2:DescribeSecurityGroups

AttachLoadBalancerToSubnets

- elasticloadbalancing:AttachLoadBalancerToSubnets
- ec2:DescribeSubnets

CreateLoadBalancer

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

DeregisterInstancesFromLoadBalancer

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

DescribeInstanceHealth

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

DescribeLoadBalancers

- elasticloadbalancing:DescribeLoadBalancers
- ec2:DescribeSecurityGroups

DisableAvailabilityZonesForLoadBalancer

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

`EnableAvailabilityZonesForLoadBalancer`

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

`RegisterInstancesWithLoadBalancer`

- `elasticloadbalancing:RegisterInstancesWithLoadBalancer`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeClassicLinkInstances`
- `ec2:DescribeInstances`
- `ec2:DescribeVpcClassicLink`

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 Uso de roles vinculados a servicios en la Guía del usuario de IAM de .

Permisos concedidos por el rol vinculado a servicios

Elastic Load Balancing utiliza el rol vinculado al servicio denominado AWSServiceRoleForElasticLoadBalancingpara realizar las siguientes acciones en su nombre:

- `ec2:AssignIpv6Addresses`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssociateAddress`
- `ec2:AttachNetworkInterface`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateNetworkInterface`
- `ec2:CreateSecurityGroup`
- `ec2:DeleteNetworkInterface`

- ec2:DescribeAccountAttributes
- ec2:DescribeAddresses
- ec2:DescribeClassicLinkInstances
- ec2:DescribeCoipPools
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcClassicLink
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DetachNetworkInterface
- ec2:DisassociateAddress
- ec2:GetCoipPoolUsage
- ec2:ModifyNetworkInterfaceAttribute
- ec2:ReleaseAddress
- ec2:UnassignIpv6Addresses
- logs:CreateLogDelivery
- logs:DeleteLogDelivery
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:UpdateLogDelivery
- outposts:GetOutpostInstanceTypes

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

Creación del rol vinculado a servicios

No necesita crear manualmente un rol AWSServiceRoleForElasticLoadBalancing. 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.

Si creaste un balanceador de cargas antes del 11 de enero de 2018, Elastic Load Balancing lo creó AWSServiceRoleForElasticLoadBalancingen tu AWS cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de AWS en la Guía del usuario de IAM.

Editar el rol vinculado a servicios

Puede editar la descripción del AWSServiceRoleForElasticLoadBalancinguso de IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar el rol vinculado a un servicio

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

Solo puede eliminar este rol vinculado a servicio después de eliminar todos los equilibradores de carga de su cuenta de 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.

Tras la eliminación AWSServiceRoleForElasticLoadBalancing, Elastic Load Balancing vuelve a crear el rol si se crea un balanceador de carga.

Políticas administradas por AWS para Elastic Load Balancing

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar rápidamente, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas administradas de AWS. En ocasiones, los servicios pueden agregar permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess administrada por AWS proporciona acceso de solo lectura a todos los servicios y recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de roles de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWSpolítica gestionada: AWSElasticLoadBalancingClassicServiceRolePolicy

Esta política incluye todos los permisos que Elastic Load Balancing (Equilibrador de carga clásico) 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 AWSElasticLoadBalancingClassicServiceRolePolicyla Referencia de políticas AWS gestionadas.

Política administrada de AWS: 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 AWSElasticLoadBalancingServiceRolePolicyla Referencia de políticas AWS administradas.

Política administrada de AWS: ElasticLoadBalancingFullAccess

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

Para ver los permisos de esta política, consulte ElasticLoadBalancingFullAccessla Referencia de políticas AWS administradas.

Política administrada de AWS: 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 ElasticLoadBalancingReadOnlyla Referencia de políticas AWS administradas.

Actualizaciones de Elastic Load Balancing para las políticas administradas por AWS.

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Elastic Load Balancing debido a que este servicio comenzó a realizar un seguimiento de estos cambios.

Cambio	Descripción	Fecha
Política administrada de AWS: ElasticLoadBalancingFullAccess: actualización de una política existente.	Elastic Load Balancing agregó una nueva acción para conceder permisos para usar el cambio de zona. Esta acción se agregó a la política de acceso completo de Elastic Load Balancing. Está asociada a las operaciones de la API de `arc-zonal-shift:*` .	28 de noviembre de 2022
Política administrada de AWS: ElasticLoadBalancingReadOnly: actualización de una política existente.	Elastic Load Balancing agregó una nueva acción para conceder permisos para usar el cambio de zona. Esta acción se agregó a la política de solo lectura de Elastic Load Balancing. Está asociada a las operaciones de la API de `arc-zonal-shift:GetManagedResource` , `arc-zonal-`	28 de noviembre de 2022

Cambio	Descripción	Fecha
	`shift:ListManagedResources` y `arc-zonal-shift:ListZonalShifts` .	
Política administrada de AWS: AWSElasticLoadBalancingServiceRolePolicy: actualización de una política existente.	Elastic Load Balancing agregó una nueva acción para conceder permisos para usar interconexiones. Esta acción se agregó a la política de roles vinculados al servicio, para el plano de control de Elastic Load Balancing . Está asociada a las operaciones de la API de `ec2:DescribeVpcPeeringConnections` .	11 de octubre de 2021
Política administrada de AWS: ElasticLoadBalancingFullAccess: actualización de una política existente.	Elastic Load Balancing agregó una nueva acción para conceder permisos para usar interconexiones. Esta acción se agregó a la política de acceso completo de Elastic Load Balancing. Está asociada a las operaciones de la API de `ec2:DescribeVpcPeeringConnections` .	11 de octubre de 2021
AWSpolítica gestionada: AWSElasticLoadBalancingClassicServiceRolePolicy: actualización de una política existente.	Elastic Load Balancing agregó una política de roles vinculados al servicio (para el plano de control) para el Equilibrador de carga clásico. Esta actualización es para la versión 2 (predeterminado).	7 de octubre de 2019
Política administrada de AWS: ElasticLoadBalancingReadOnly	Proporciona acceso de solo lectura a los servicios de Elastic Load Balancing y a los servicios dependientes. Esta es la versión 1 (predeterminada).	20 de septiembre de 2018
Elastic Load Balancing comenzó el seguimiento de los cambios	Elastic Load Balancing comenzó el seguimiento de los cambios de las políticas administradas de AWS.	23 de julio de 2021

Validación de conformidad para Elastic Load Balancing

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

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

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de conformidad de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

  > **Note**
  >
  > No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.

- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su conformidad con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en Elastic Load Balancing

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. 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 latencia. 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 centros de datos únicos o múltiples.

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

Además de la infraestructura global de AWS, Elastic Load Balancing ofrece las siguientes características que le ayudan con sus necesidades de resiliencia:

- Distribuye el tráfico entrante entre las distintas instancias en una única o en varias zonas de disponibilidad.
- Puede utilizar AWS Global Accelerator con sus equilibradores de carga de aplicaciones para distribuir el tráfico entrante entre varios equilibradores de carga en una o más regiones de AWS. Para obtener más información, consulte AWS Global Accelerator Developer Guide.
- Amazon ECS permite ejecutar, detener y administrar contenedores Docker en un clúster de instancias EC2. 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 se trata de un servicio administrado, Elastic Load Balancing está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS conforme a las prácticas recomendadas de seguridad de la infraestructura, consulte Protección de la infraestructura en Pilar de seguridad del Marco de AWS Well-Architected.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso 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 puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una Virtual Private Cloud (VPC) es una red virtual en su propia área, aislada lógicamente en la nube de 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 instancias EC2 en las subredes de su VPC y registrarlas con el equilibrador 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. Puede utilizar AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) para administrar los certificados de servidor instalados en el equilibrador de carga. 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.
- Configure los grupos de seguridad para que las instancias de Amazon EC2 acepten tráfico solo del equilibrador de carga. 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 de conexión de VPC de interfaz utilizan la tecnología de AWS PrivateLink, una característica que permite la comunicación entre lsa aplicaciones y los Servicios de AWS mediante direcciones IP privadas. Para obtener más información, consulte AWS PrivateLink.

Límite

AWS PrivateLink no admite un equilibrador 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 puntos de conexión de la VPC en la Guía del usuario de AWS PrivateLink.

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 más información sobre las diferentes características de cada tipo de equilibrador de carga, consulte Comparación de productos de Elastic Load Balancing.

También puede optar por migrar un Classic Load Balancer existente en una VPC a un Application Load Balancer o a un Network Load Balancer.

Ventajas de migrar desde un Equilibrador de carga clásico

Cada tipo de balanceador de cargas tiene sus propias características, funciones y configuraciones únicas. Revisa las ventajas de cada balanceador de carga para decidir cuál es el mejor para ti.

Application Load Balancer

El uso de un Application Load Balancer en lugar de un Load Balancer clásico ofrece las siguientes ventajas:

Support para:

- 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 instancia de EC2.
- Devolver respuestas HTTP personalizadas.
- Registrar los destinos por dirección IP y registrar las funciones Lambda como objetivos. Incluir objetivos fuera de la VPC para el balanceador de cargas.
- Autenticar a los usuarios mediante identidades corporativas o sociales.
- Aplicaciones contenerizadas de Amazon Elastic Container Service (Amazon ECS).
- Supervise de forma independiente el estado de cada servicio.

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

Rendimiento general mejorado del balanceador de carga.

Network Load Balancer

El uso de un Network Load Balancer en lugar de un Load Balancer clásico ofrece las siguientes ventajas:

Support para:

- Direcciones IP estáticas, que permiten asignar una dirección IP elástica por cada subred habilitada para el balanceador de cargas.
- Registrar los destinos por dirección IP, incluidos los destinos fuera de la VPC para el balanceador de cargas.
- Enrutamiento de solicitudes a varias aplicaciones en una sola instancia de EC2.
- Aplicaciones contenerizadas de Amazon Elastic Container Service (Amazon ECS).
- Supervise de forma independiente el estado de cada servicio.

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

Migre mediante el asistente de migración

El asistente de migración utiliza la configuración del Classic Load Balancer para crear un Application Load Balancer o Network Load Balancer equivalentes. Reduce el tiempo y el esfuerzo necesarios para migrar un Classic Load Balancer en comparación con otros métodos.

> **Note**
>
> El asistente crea un nuevo balanceador de cargas. El asistente no convierte el Classic Load Balancer existente en un Application Load Balancer o Network Load Balancer. Debes redirigir manualmente el tráfico al balanceador de cargas recién creado.

Limitaciones

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

- Si el Classic Load Balancer tiene alguna etiqueta que contenga el `aws:` prefijo en su clave, esas etiquetas no se migran.

Al migrar a un Application Load Balancer

- Si el Classic Load Balancer solo tiene una subred, debes especificar una segunda subred.
- Si el Classic Load Balancer tiene detectores HTTP/HTTPS que utilizan comprobaciones de estado de TCP, el protocolo de comprobación de estado se actualiza a HTTP y la ruta se establece en «/».
- Si el Classic Load Balancer tiene agentes de escucha 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 balanceador de carga.

Al migrar a un Network Load Balancer

- Los siguientes tipos de instancias no se registrarán en el nuevo grupo de destino: C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M2, M3, T1
- Es posible que algunos ajustes de control de estado de tu Classic Load Balancer no se puedan transferir al nuevo grupo objetivo. Estos casos se indicarán como un cambio en la sección de resumen del asistente de migración.
- Si el Classic Load Balancer tiene agentes de escucha SSL, el asistente de migración crea un agente de escucha de TLS utilizando el certificado y la política de seguridad del agente de escucha de SSL.

Proceso del asistente de migración

Para migrar un Classic Load Balancer mediante el asistente de migración

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Selecciona el Classic Load Balancer que quieras migrar.
4. En la sección Detalles de los balanceadores de carga, selecciona Iniciar el asistente de migración.
5. Seleccione Migrar a Application Load Balancer o Migrar a Network Load Balancer para abrir el asistente de migración.

6. En Nombre del nuevo balanceador de cargas, en Nombre del balanceador de cargas ingresa un nombre para el nuevo balanceador de cargas.
7. En Nombre del nuevo grupo objetivo y revisar los objetivos, en Nombre del grupo objetivo introduce un nombre para el nuevo grupo objetivo.
8. (Opcional) En Objetivos, puede revisar las instancias de destino que se registrarán en el nuevo grupo objetivo.
9. (Opcional) En Revisar etiquetas, puedes revisar las etiquetas que se aplicarán a tu nuevo balanceador de cargas
10. En Resumen de Application Load Balancer o Resumen de Network Load Balancer, revise y verifique las opciones de configuración asignadas por el asistente de migración.
11. Cuando esté satisfecho con el resumen de la configuración, elija Create Application Load Balancer o Create Network Load Balancer para iniciar la migración.

Realice la migración mediante la utilidad de copia del balanceador 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 de Classic Load Balancer a Application Load Balancer
- Utilidad de copia de Classic Load Balancer a Network Load Balancer

Migre su balanceador de carga manualmente

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 acciones siguientes:
   - 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 las instancias EC2 en el grupo de destino.
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 (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.

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.