



Guía del usuario

Elastic Load Balancing



Elastic Load Balancing: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Elastic Load Balancing?	1
Beneficios del equilibrador de carga	1
Características de Elastic Load Balancing	1
Acceso a Elastic Load Balancing	2
Servicios relacionados	2
Precios	3
Cómo funciona Elastic Load Balancing	4
Zonas de disponibilidad y nodos de equilibrador de carga	4
Equilibrio de carga entre zonas	5
Cambio de zona	7
Enrutamiento de solicitudes	9
Algoritmo de direccionamiento	9
Conexiones HTTP	10
Encabezados HTTP	11
Límites de los encabezados HTTP	12
Esquema del equilibrador de carga	12
MTU de red	13
Introducción	15
Creación de un equilibrador de carga de aplicación	15
Crear un equilibrador de carga de red	15
Creación del equilibrador de carga de puerta de enlace	16
Para crear un equilibrador de carga clásico	16
Seguridad	17
Protección de datos	18
Cifrado en reposo	19
Cifrado en tránsito	19
Administración de identidades y accesos	19
Público	20
Autenticación con identidades	21
Administración de acceso mediante políticas	24
Cómo funciona Elastic Load Balancing con IAM	27
APIpermisos	40
Permisos de etiquetado de API recursos	43
Rol vinculado al servicio	45

AWS políticas gestionadas	47
Validación de conformidad	50
Resiliencia	52
Seguridad de la infraestructura	52
Aislamiento de red	53
Control del tráfico de red	53
AWS PrivateLink	54
Crear un punto de conexión de interfaz para Elastic Load Balancing	55
Crear un punto de conexión de VPC para Elastic Load Balancing	55
Migrar el Equilibrador de carga clásico	57
Ventajas de la migración	57
Asistente de migración	58
Migración de la utilidad de copia	60
Migración manual	60
.....	Ixiv

¿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.
- **AWS Interfaz de línea de comandos (AWS CLI):** proporciona comandos para un amplio conjunto de AWS servicios, incluido Elastic Load Balancing. AWS CLI Es compatible con Windows, macOS y Linux. Para obtener más información, consulte [AWS Command Line Interface](#).
- **AWS SDK:** proporcionan API específicas para cada idioma y se ocupan de muchos de los detalles de la conexión, como el cálculo de las firmas, la gestión de los reintentos de solicitudes y la gestión de los 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 más información, consulte los siguientes temas:
 - **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 dirija el tráfico a las instancias EC2. Para obtener más información, consulte la Guía del [usuario de Amazon EC2](#).
- **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: le permite monitorear su balanceador de carga y tomar las medidas necesarias. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- Amazon ECS: permite ejecutar, detener y administrar contenedores Docker en un clúster de instancias EC2. Puede configurar el equilibrador de carga de forma que dirija el tráfico a los contenedores. Para obtener más información, consulte [Amazon Elastic Container Service Developer Guide](#) (Guía para desarrolladores de Amazon Elastic Container Service).
- AWS Global Accelerator: mejora la disponibilidad y el rendimiento de la aplicación. Utilice un acelerador para distribuir el tráfico entre varios balanceadores de carga en una o más AWS regiones. Para obtener más información, consulte la [Guía para desarrolladores de AWS Global Accelerator](#).
- Route 53: ofrece una forma rentable y de confianza de direccionar a los visitantes a los sitios web convirtiendo los nombres de dominio en direcciones IP numéricas que los equipos utilizan para comunicarse entre sí. Por ejemplo, se `www.example.com` traduciría en la dirección IP numérica `192.0.2.1` AWS asigna direcciones URL a tus recursos, como los balanceadores de carga. No obstante, puede ser conveniente utilizar una URL que los usuarios puedan recordar fácilmente. Por ejemplo, puede asignar el nombre de dominio a un equilibrador de carga. Para obtener más información, consulte la [Guía para desarrolladores de Amazon Route 53](#).
- AWS WAF— Puede usarlo AWS WAF con su Application Load Balancer para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (ACL web). Para obtener más información, consulte la [Guía para desarrolladores de AWS WAF](#).

Precios

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

Cómo funciona Elastic Load Balancing

Un 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.

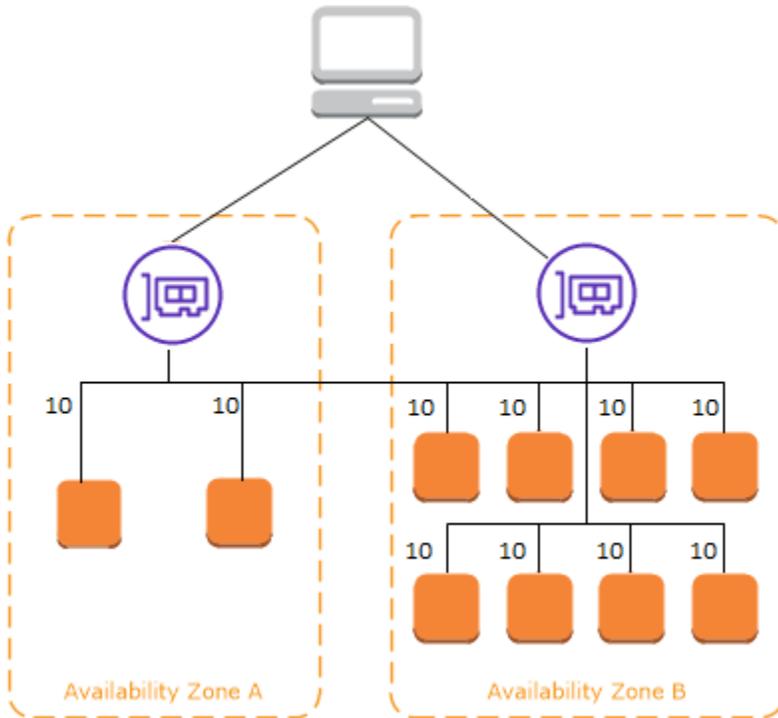
Después de deshabilitar una zona de disponibilidad, los destinos de esa zona de disponibilidad permanecen registrados en el equilibrador de carga. Sin embargo, aunque permanezcan registrados, el equilibrador de carga no envía el tráfico hacia ellos.

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.

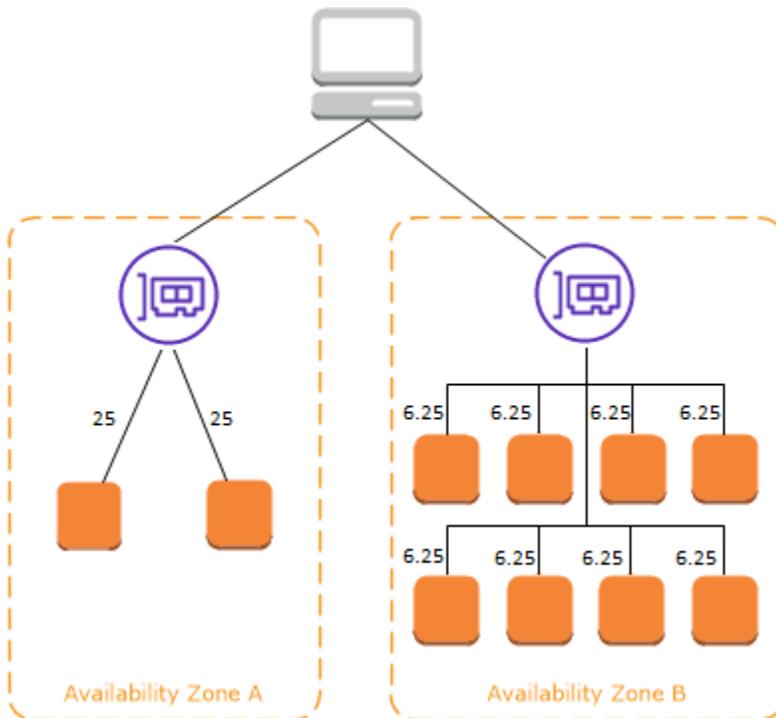
Si el equilibrio de carga entre zonas está habilitado, cada uno de los diez destinos recibirá un 10% del tráfico. Esto se debe a que cada nodo del equilibrador de carga puede dirigir el 50% del tráfico de los clientes a los diez destinos.



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](#)
- [Crear un equilibrador de carga de red](#)
- [Creación del equilibrador de carga de puerta de enlace](#)
- [Para crear un equilibrador de carga clásico](#)

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 Guía 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

- [Protección de datos en Elastic Load Balancing](#)
- [Administración de identidad y de acceso para Elastic Load Balancing](#)

- [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 la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte el [modelo de responsabilidad AWS compartida](#) y la entrada del GDPR blog sobre AWS seguridad.

Para proteger los 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 multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario 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 entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma federal de procesamiento de información \(\) FIPS 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Elastic Load Balancing u otro tipo de Servicios de AWS uso de la consola API AWS CLI,, o AWS SDKs. 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, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Cifrado en reposo

Si habilita el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) para su bucket de S3 para los registros de acceso de Elastic Load Balancing, Elastic Load Balancing cifra automáticamente cada archivo de registro de acceso antes de que se almacene en su 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 KMS clave que se rota periódicamente.

Cifrado en tránsito

Elastic Load Balancing simplifica el proceso de creación de aplicaciones web seguras mediante la terminación HTTPS y el TLS tráfico de los clientes en el balanceador de carga. El balanceador de cargas realiza el trabajo de cifrar y descifrar el tráfico, en lugar de requerir que cada EC2 instancia se encargue del trabajo de finalización. 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. Los balanceadores de carga de aplicaciones son compatibles con los HTTPS oyentes. Los balanceadores de carga de red son compatibles con los oyentes. TLS Los balanceadores de carga clásicos son compatibles con ambos HTTPS tipos de escucha. TLS

Administración de identidad y de acceso para Elastic Load Balancing

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién

puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Elastic Load Balancing. IAM es un Servicio de AWS que puede utilizarse sin costo adicional.

Contenido

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Elastic Load Balancing con IAM](#)
- [API Permisos de Elastic Load Balancing](#)
- [API Permisos de Elastic Load Balancing para etiquetar los recursos durante la creación](#)
- [Rol vinculado al servicio de Elastic Load Balancing](#)
- [AWS políticas gestionadas para Elastic Load Balancing](#)

Público

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

Usuario de servicio: si utiliza el servicio de Elastic Load Balancing para realizar el trabajo, el administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Elastic Load Balancing para realizar el trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede 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. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM.

IAM administrador: si es IAM administrador, puede que desee obtener más información sobre cómo escribir políticas para administrar el acceso a Elastic Load Balancing.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol.

Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

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

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar AWS API las solicitudes](#) en la Guía del IAM usuario.

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

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no 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 tareas que requieren que inicie sesión como usuario root, consulte [Tareas que requieren credenciales de usuario root](#) en la Guía del IAM usuario.

Identidad federada

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

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

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

Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del IAM usuario.

Un [IAMgrupo](#) es una identidad que especifica un conjunto de IAM usuarios. 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 para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdmins y concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Cuándo crear un IAM usuario \(en lugar de un rol\)](#) en la Guía del IAM usuario.

IAMroles

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a una AWS API operación AWS CLI o utilizando una operación personalizada URL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

IAMlos roles 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 sobre los roles para la federación, consulte [Creación de un rol para un proveedor de identidad externo](#) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos IAM de usuario temporales:** un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- **Acceso multicuenta:** puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a un Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan

cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar sesiones de acceso](#).

- **Función de servicio:** una función de servicio es una [IAMfunción](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro de IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol](#) en el IAM Manual del usuario.
- **Función vinculada a un servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte [Cuándo crear un IAM rol \(en lugar de un usuario\)](#) en la Guía del IAM usuario.

Administración de acceso mediante políticas

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

Los administradores pueden usar AWS JSON las políticas 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 a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAM las políticas definen los 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 esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

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

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM](#) usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

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

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

Otros tipos de políticas

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

- **Límites de permisos:** un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad IAM (IAM Usuario o rol). 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 los [límites de los permisos para IAM las entidades](#) en la Guía del IAM Usuario.
- **Políticas de control de servicios (SCPs):** SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCP Limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de 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 obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

Varios tipos de políticas

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

Cómo funciona Elastic Load Balancing con IAM

Antes de administrar el acceso IAM a Elastic Load Balancing, infórmese sobre IAM las funciones disponibles para su uso con Elastic Load Balancing.

IAM funciones que puedes usar con Elastic Load Balancing

IAM característica	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
ACLs	No
ABAC(etiquetas en las políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Políticas basadas en identidad de Elastic Load Balancing

Compatibilidad con las políticas basadas en identidad: sí

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

Con las políticas IAM basadas en la identidad, 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 todos los elementos que puede utilizar en una JSON política, consulte la [referencia sobre los elementos de la IAM JSON política](#) en la Guía del IAM usuario.

Políticas basadas en recursos en Elastic Load Balancing

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos JSON de política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) 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 obtener más información, consulte [Acceso a recursos entre cuentas IAM en](#) la Guía del IAM usuario.

Acciones de políticas de Elastic Load Balancing

Compatibilidad con las acciones de política: sí

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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 API acciones de Elastic Load Balancing, consulte la siguiente documentación:

- [Balanceadores de carga de aplicaciones, balanceadores de carga de red y balanceadores de carga de gateway: API versión de referencia 2015-12-01](#)

- [Equilibradores de carga clásicos: versión de referencia 2012-06-01 API](#)

Para obtener más información sobre los permisos necesarios para cada acción de Elastic Load Balancing, consulte [API Permisos de Elastic Load Balancing](#).

Recursos de políticas de Elastic Load Balancing

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su [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 API acciones de Elastic Load Balancing admiten varios recursos. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de Elastic Load Balancing y sus tipos ARNs, consulte [Recursos definidos por Elastic Load Balancing](#) en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar cada recurso, consulte [Actions defined by Elastic Load Balancing](#). ARN

Claves de condición de política para Elastic Load Balancing

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

Los administradores pueden usar AWS JSON políticas 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 AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte [los elementos IAM de la política: variables y etiquetas](#) en la Guía del IAM usuario.

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

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`**

El `elasticloadbalancing:ResourceTag/key` la clave de condición 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 Subnet. IDs Sin embargo, asegúrese de utilizar los operadores de condiciones 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 IDs Sin embargo, asegúrese de utilizar los operadores de condición adecuados que no distinguen 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"
        ]
      }
    }
  }
```

ACLsen Elastic Load Balancing

SoportaACLs: No

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

ABACcon Elastic Load Balancing

Soportes ABAC (etiquetas en las políticas): Sí

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

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve 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 al respecto ABAC, consulte [¿Qué es? ABAC](#) en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuración ABAC, consulte [Usar el control de acceso basado en atributos \(ABAC\)](#) en la Guía del IAM usuario.

Uso de credenciales temporales con Elastic Load Balancing

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta la sección [Servicios de AWS Cómo trabajar con credenciales temporales IAM](#) en la Guía del IAM usuario.

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

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

Permisos de entidades principales entre servicios para Elastic Load Balancing

Admite sesiones de acceso directo (FAS): Sí

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

ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar sesiones de acceso](#).

Roles de servicio para Elastic Load Balancing

Compatible con roles de servicio: No

Una función de servicio es una [IAMfunción](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte [Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario](#).

Roles vinculados a servicios para Elastic Load Balancing

Admite roles vinculados al servicio: sí

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

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](#).

APIPermisos de Elastic Load Balancing

Debe conceder a los usuarios permiso para ejecutar las API acciones de Elastic Load Balancing que necesiten. Además, para algunas acciones de Elastic Load Balancing, debes conceder a los usuarios permiso para solicitar acciones específicas desde Amazon EC2API.

Permisos necesarios para el 1 de diciembre de 2015 API

Al realizar las siguientes acciones a partir del 1 de diciembre de 2015API, debes conceder a los usuarios permiso para realizar 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 el 1 de junio de 2012 API

Al ejecutar las siguientes acciones a partir del 1 de junio de 2012API, debes conceder a los usuarios permiso para ejecutar 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`

API Permisos de Elastic Load Balancing para etiquetar los 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 IAM política de la `elasticloadbalancing:AddTags` acción, puede utilizar el `Condition` elemento con la clave de `elasticloadbalancing:CreateAction` condición para conceder 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 funciones vinculadas a servicios](#) en la Guía del IAM usuario.

Permisos concedidos por el rol vinculado a servicios

Elastic Load Balancing utiliza el rol vinculado al servicio denominado `AWSServiceRoleForElasticLoadBalancing` para 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

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

Creación del rol vinculado a servicios

No es necesario crear el `AWSServiceRoleForElasticLoadBalancing` rol manualmente. 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 los [permisos de los roles vinculados a un servicio](#) en la Guía del IAM usuario.

Si creaste un balanceador de cargas antes del 11 de enero de 2018, Elastic Load Balancing lo creó `AWSServiceRoleForElasticLoadBalancing` en tu AWS cuenta. Para obtener más información, consulte [Apareció un nuevo rol en mi AWS cuenta](#) en la Guía del IAM usuario.

Editar el rol vinculado a servicios

Puede editar la descripción de `AWSServiceRoleForElasticLoadBalancing` solo IAM. Para obtener más información, consulte [Edición de un rol vinculado a un servicio](#) en la Guía del IAM usuario.

Eliminar el rol vinculado a servicios

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

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

Puedes usar la IAM consola, la o la IAM API para eliminar IAM CLI las funciones vinculadas al servicio. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario. IAM

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

AWS políticas gestionadas para Elastic Load Balancing

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

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades

principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte [las políticas AWS administradas](#) en la Guía del IAM usuario.

AWS política gestionada: AWSElasticLoadBalancingClassicServiceRolePolicy

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

Para ver los permisos de esta política, consulte la Referencia [AWSElasticLoadBalancingClassicServiceRolePolicy](#) de políticas AWS administradas.

AWS política gestionada: AWSElasticLoadBalancingServiceRolePolicy

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

Para ver los permisos de esta política, consulte [AWSElasticLoadBalancingServiceRolePolicy](#) la Referencia de políticas AWS gestionadas.

AWS política gestionada: ElasticLoadBalancingFullAccess

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

Para ver los permisos de esta política, consulte [ElasticLoadBalancingFullAccess](#) la Referencia de políticas AWS administradas.

AWS política gestionada: ElasticLoadBalancingReadOnly

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

Para ver los permisos de esta política, consulte [ElasticLoadBalancingReadOnly](#) la Referencia de políticas AWS gestionadas.

Actualizaciones de Elastic Load Balancing a las políticas AWS gestionadas

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

Cambio	Descripción	Fecha
AWS política gestionada: 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 asociado a las <code>arc-zonal-shift:*</code> API operaciones.	28 de noviembre de 2022
AWS política gestionada: 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 asociado a <code>arc-zonal-shift:GetManagedResource</code> las <code>arc-zonal-shift:ListZonalShifts</code> API operaciones <code>arc-zonal-shift:ListManagedResources</code> y.	28 de noviembre de 2022
AWS política gestionada: 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 asociado a la <code>ec2:DescribeVpcPeerConnections</code> API operación.	11 de octubre de 2021
AWS política gestionada: ElasticLoadBalancingFullAccess	Elastic Load Balancing agregó una nueva acción para conceder permisos para usar interconexiones. Esta acción se agregó a la	11 de octubre de 2021

Cambio	Descripción	Fecha
ess : actualización de una política existente.	política de acceso completo de Elastic Load Balancing. Está asociado a la <code>ec2:DescribeVpcPeeringConnections</code> API operación.	
AWS política 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
AWS política gestionada: 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 a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	23 de julio de 2021

Validación de conformidad para Elastic Load Balancing

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

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

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

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- [Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

 Note

No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la [Referencia de servicios HIPAA aptos](#).

- [AWS Recursos](#) de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de 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 servicio gestionado, Elastic Load Balancing está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

APIs llamadas AWS publicadas se utilizan para acceder a Elastic Load Balancing a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE 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 firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una nube privada virtual (VPC) es una red virtual en su propia área aislada lógicamente en la AWS nube. Una subred es un rango de direcciones IP en un VPC. Al crear un equilibrador de carga, puede especificar una o varias subredes para los nodos del equilibrador de carga. Puede implementar EC2 instancias en sus subredes VPC y registrarlas en su balanceador de carga. Para obtener más información sobre las subredes VPC y las subredes, consulta la [Guía del VPC usuario de Amazon](#).

Al crear un balanceador de carga en un VPC, puede ser interno o conectado a Internet. Un balanceador de cargas interno solo puede enrutar las solicitudes que provienen de clientes con acceso al balanceador de VPC cargas.

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 Elastic Load Balancing API desde direcciones IP privadas, utilice AWS PrivateLink. VPC 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. Los balanceadores de carga de aplicaciones son compatibles con los HTTPS oyentes. Los balanceadores de carga de red son compatibles con los oyentes. TLS Los balanceadores de carga clásicos son compatibles con ambos HTTPS tipos de escucha. TLS

Puede elegir entre políticas de seguridad predefinidas para el equilibrador de carga con el fin de especificar los conjuntos de cifrado y las versiones de protocolo compatibles con la aplicación. Puedes usar AWS Certificate Manager (ACM) o AWS Identity and Access Management (IAM) para administrar los certificados de servidor instalados en tu balanceador de cargas. Puede utilizar el protocolo de indicación del nombre del servidor (SNI) para ofrecer servicio a varios sitios web seguros mediante un único agente de escucha seguro. SNI se habilita automáticamente para el equilibrador de cargas al asociar más de un certificado de servidor a un agente de escucha seguro.

- Configure los grupos de seguridad para sus equilibradores de carga de aplicaciones y Equilibradores de carga clásicos con el fin de aceptar tráfico solo de clientes específicos. Estos grupos de seguridad deben permitir el tráfico entrante de los clientes en los puertos de escucha y el tráfico saliente a los clientes.
- Configura los grupos de seguridad de tus EC2 instancias de Amazon para que solo acepten tráfico del balanceador de cargas. Estos grupos de seguridad deben permitir el tráfico entrante desde el equilibrador de carga en los puertos de oyente y en los puertos de comprobación de estado.
- Configure su Equilibrador de carga de aplicación para autenticar a los usuarios de forma segura a través de un proveedor de identidades o mediante identidades corporativas. Para obtener más información, consulte [Autenticar usuarios mediante un Equilibrador de carga de aplicación](#).
- Úsalo [AWS WAF](#) con tus balanceadores de carga de aplicaciones para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (webACL).

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 las 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 específica:

- 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, H11, 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. Seleccione el Classic Load Balancer que quieras migrar.
4. En la sección Detalles de los balanceadores de carga, seleccione 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, el CLI de AWS, 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. Monitoree 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 `aws/ApplicationELB` o `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.