Elastic Load Balancing

Application Load Balancers

Elastic Load Balancing: Application Load Balancers

Table of Contents

¿Qué es un Application Load Balancer?

Elastic Load Balancing admite tres tipos de balanceadores de carga: Application Load Balancers, Network Load Balancers y Classic Load Balancers. En esta guía, se explican los Application Load Balancers. Para obtener más información sobre Network Load Balancers, consulte la Guía del usuario de Network Load Balancers. Para obtener más información sobre Classic Load Balancers, consulte Guía del usuario de Classic Load Balancers.

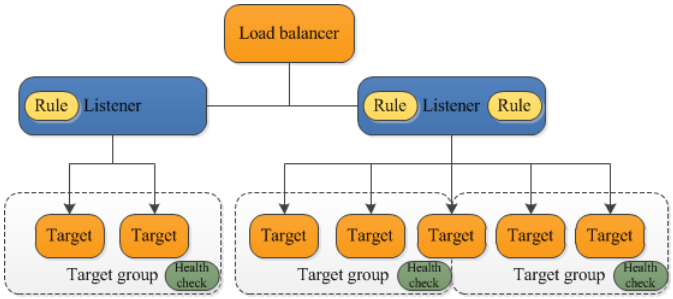
Componentes de Balanceador de carga de aplicaciones

Un balanceador de carga actúa como único punto de contacto para los clientes. El balanceador de carga distribuye el tráfico entrante de aplicaciones entre varios destinos, tales como instancias EC2, en varias zonas de disponibilidad. Esto aumenta la disponibilidad de la aplicación. Puede agregar uno o varios agentes de escucha al balanceador de carga.

Un agente de escucha comprueba las solicitudes de conexión de los clientes mediante el protocolo y el puerto que haya configurado; a continuación, reenvía las solicitudes a uno o más grupos de destino, según las reglas que haya definido. Cada regla especifica un grupo de destino, una condición y una prioridad. Cuando se cumple la condición, el tráfico se reenvía al grupo de destino. Debe definir una regla predeterminada para cada agente de escucha y agregar reglas que especifiquen diferentes grupos de destino en función del contenido de la solicitud (esto también se denomina direccionamiento basado en contenido).

Cada grupo de destino direcciona las solicitudes a uno o varios destinos registrados (tales como instancias EC2) utilizando el protocolo y el número de puerto que ha especificado. Puede registrar un destino en varios grupos de destino. Puede configurar las comprobaciones de estado de cada grupo de destino. Las comprobaciones de estado se llevan a cabo en todos los destinos registrados en un grupo de destino especificado en la regla del agente de escucha del balanceador de carga.

En el siguiente diagrama se ilustran los componentes básicos. Observe que cada agente de escucha contiene una regla predeterminada y que un agente de escucha contiene otra regla que direcciona las solicitudes a un grupo de destino diferente. Un destino se ha registrado en dos grupos de destino.



Para obtener más información, consulte la documentación siguiente:

- Balanceadores de carga (p. 17)
- Agentes de escucha (p. 28)

- Grupos de destino (p. 57)

Información general de Balanceador de carga de aplicaciones

Un Balanceador de carga de aplicaciones actúa como la capa de aplicación, es decir, la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Una vez que el balanceador de carga ha recibido una solicitud, evalúa las reglas del agente de escucha por orden de prioridad con el fin de determinar qué regla se debe aplicar. A continuación, selecciona un destino en el grupo de destino para la acción de la regla. Puede configurar las reglas del agente de escucha de tal forma que las solicitudes se direccionen a diferentes grupos de destino en función del contenido del tráfico de aplicación. El direccionamiento se lleva a cabo de manera independiente para cada grupo de destino, aunque un destino se haya registrado en varios grupos de destino.

Puede agregar y eliminar destinos del balanceador de carga en función de sus necesidades sin interrumpir el flujo general de solicitudes a la aplicación. Elastic Load Balancing escala el balanceador de carga a medida que cambia el tráfico dirigido a la aplicación y es capaz de adaptarse automáticamente a la mayoría de cargas de trabajo. Elastic Load Balancing puede escalarse automáticamente para adaptarse a la mayoría de las cargas de trabajo.

Puede configurar las comprobaciones de estado, que se utilizan para monitorizar el estado de los destinos registrados, de tal forma que el balanceador de carga solo pueda enviar solicitudes a los destinos en buen estado.

Para obtener más información, consulte Cómo funciona Elastic Load Balancing en la Guía del usuario de Elastic Load Balancing.

Beneficios de la migración desde un Classic Load Balancer

Usar un Balanceador de carga de aplicaciones en lugar de un Classic Load Balancer presenta los siguientes beneficios:

- Compatibilidad con el direccionamiento basado en rutas. Puede configurar reglas para el agente de escucha que reenvíen las solicitudes en función de la dirección URL contenida en la solicitud. Esto permite estructurar la aplicación en servicios de menor tamaño y direccionar las solicitudes al servicio correcto según el contenido de la URL.
- Compatibilidad con el direccionamiento basado en host. Puede configurar reglas para el agente de escucha que reenvíen las solicitudes en función del campo de host en el encabezado HTTP. Esto permite direccionar solicitudes a varios dominios a través de un único balanceador de carga.
- Compatibilidad para direccionamiento basado en campos en la solicitud, tales como encabezados y métodos HTTP estándar o personalizados, parámetros de la consulta y direcciones IP de origen.
- Compatibilidad con el direccionamiento de solicitudes a varias aplicaciones en una sola instancia EC2. Puede registrar cada instancia o dirección IP con el mismo grupo de destino utilizando varios puertos.
- Compatibilidad con el redireccionamiento de solicitudes de una URL a otra.
- Compatibilidad con la devolución de una respuesta HTTP personalizada.
- Compatibilidad con el registro de destinos por dirección IP, incluidos los destinos situados fuera de la VPC para el balanceador de carga.
- Compatibilidad para registrar funciones Lambda como destinos.

- Compatibilidad para que el balanceador de carga pueda autenticar a los usuarios de sus aplicaciones a través de sus identidades corporativas o sociales antes de enviar solicitudes.
- Compatibilidad con las aplicaciones en contenedores. Amazon Elastic Container Service (Amazon ECS) permite seleccionar un puerto no utilizado al programar una tarea y registrarla en un grupo de destino mediante este puerto. De este modo, puede hacer un uso eficiente de los clústeres.
- Compatibilidad con la monitorización independiente del estado de cada servicio, pues las comprobaciones de estado se definen para cada grupo de destino y muchas métricas de CloudWatch se notifican también para cada grupo de destino. Si adjunta un grupo de destino a un grupo de Auto Scaling, podrá escalar cada servicio dinámicamente en función de la demanda.
- Los logs de acceso contienen información adicional y se almacenan en formato comprimido.
- Mejora del desempeño del balanceador de carga.

Para obtener más información sobre las características admitidas por cada tipo de balanceador de carga, consulte Comparación de productos de Elastic Load Balancing.

Cómo empezar

Para crear un Balanceador de carga de aplicaciones, pruebe con uno de los siguientes tutoriales:

- Introducción a Elastic Load Balancing en la Guía del usuario de Elastic Load Balancing.
- Tutorial: Uso del direccionamiento basado en rutas con el Application Load Balancer (p. 9)
- Tutorial: Utilizar microservicios como destinos con Application Load Balancer (p. 11)

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 balanceador de carga de modo que direccione el tráfico a las instancias EC2.
- Amazon EC2 Auto Scaling: se asegura de que se ejecute la cantidad deseada de instancias, aunque una de ellas sufra un error, y permite aumentar o reducir automáticamente el número de instancias a medida que cambia la demanda de ellas. Si habilita Auto Scaling con Elastic Load Balancing, las instancias que Auto Scaling lanza se registran automáticamente en el balanceador de carga y se anula automáticamente el registro en el balanceador de carga de las instancias que se Auto Scaling termina.
- AWS Certificate Manager: al crear un agente de escucha HTTPS, puede especificar los certificados proporcionados por ACM. El balanceador de carga utiliza certificados para terminar las conexiones y descifrar las solicitudes de los clientes. Para obtener más información, consulte Certificados SSL (p. 38).
- Amazon CloudWatch — Permite monitorizar el balanceador de carga y adoptar las medidas necesarias. Para obtener más información, consulte Métricas de CloudWatch para el Application Load Balancer (p. 79).
- Amazon ECS — Permite ejecutar, detener y administrar contenedores Docker en un clúster de instancias EC2. Puede configurar el balanceador de carga de forma que direccione el tráfico a los contenedores. Para obtener más información, consulte Balanceo de carga de servicios en la Amazon Elastic Container Service Developer Guide.
- Route 53 — Ofrece una forma rentable y de confianza de direccionar a los visitantes a los sitios web convirtiendo los nombres de dominio (como `www.example.com`) en direcciones IP numéricas (como `192.0.2.1`) que los equipos utilizan para comunicarse entre sí. AWS asigna direcciones URL a los recursos, tales 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 balanceador de carga.

- AWS WAF: puede utilizar AWS WAF con su Balanceador de carga de aplicaciones 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 Application Load Balancers y AWS WAF (p. 20).

Para ver información acerca de los servicios que se integran con el balanceador de carga, seleccione el balanceador de carga en la Consola de administración de AWS y elija la pestaña Integrated services (Servicios integrados).

Precios

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

Introducción a Application Load Balancers

En este tutorial, encontrará una introducción práctica sobre el uso de Application Load Balancers a través de la Consola de administración de AWS, una interfaz web. Para crear su primer Balanceador de carga de aplicaciones, siga los pasos que se describen a continuación.

Tareas

Si prefiere crear un Balanceador de carga de red, consulte Introducción a los Network Load Balancers en la Guía del usuario de Network Load Balancers. Para crear un Classic Load Balancer, consulte Crear un Classic Load Balancer en la Guía del usuario de Classic Load Balancers.

Antes de empezar

- Decida qué dos zonas de disponibilidad va a utilizar con las instancias EC2. Configure la nube virtual privada (VPC) con al menos una subred pública en cada una de estas zonas de disponibilidad. Estas subredes públicas se utilizan para configurar el balanceador de carga. Puede lanzar las instancias EC2 en otras subredes de estas zonas de disponibilidad en su lugar.
- Lance al menos una instancia EC2 en cada zona de disponibilidad. Asegúrese de instalar un servidor web, como Apache o Internet Information Services (IIS), en cada instancia EC2. Asegúrese de que los grupos de seguridad de estas instancias permitan el acceso HTTP en el puerto 80.

Paso 1: Seleccionar un tipo de balanceador de carga

Elastic Load Balancing admite tres tipos de balanceadores de carga. En este tutorial, va a crear un Balanceador de carga de aplicaciones.

Para crear un Balanceador de carga de aplicaciones

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En la barra de navegación, elija una región para el balanceador de carga. No olvide seleccionar la misma región que utilizó con las instancias EC2.
3. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
4. Elija Create Load Balancer.
5. Para Application Load Balancer, elija Create.

Paso 2: Configurar un balanceador de carga y un agente de escucha

En la página Configure Load Balancer, realice el siguiente procedimiento.

Para configurar el balanceador de carga y el agente de escucha

1. En Name, escriba el nombre del balanceador de carga.

   El nombre del Balanceador de carga de aplicaciones debe ser único en el conjunto de Application Load Balancers y Network Load Balancers de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones, no puede comenzar ni terminar por un guion y no puede comenzar por "internal-".
2. Para Scheme y IP address type, mantenga los valores predeterminados.
3. En Listeners, mantenga el valor predeterminado, que es un agente de escucha que acepta tráfico HTTP en el puerto 80.
4. En Availability Zones, seleccione la VPC que ha usado para las instancias EC2. En cada una de las zonas de disponibilidad que utilizó para lanzar las instancias EC2, seleccione la zona de disponibilidad y seleccione después la subred pública de esa zona de disponibilidad.
5. Elija Next: Configure Security Settings.
6. En este tutorial, no va a crear un agente de escucha HTTPS. Elija Next: Configure Security Groups.

Paso 3: Configurar un grupo de seguridad para el balanceador de carga

El grupo de seguridad del balanceador de carga debe permitir que este último se comunique con los destinos registrados tanto en el puerto del agente de escucha como en el puerto de comprobación de estado. La consola puede crear en su nombre un grupo de seguridad para el balanceador de carga, con reglas que especifiquen los protocolos y los puertos correctos. Si lo prefiere, puede crear y seleccionar su propio grupo de seguridad. Para obtener más información, consulte Reglas recomendadas (p. 24).

En la página Configure Security Groups (Configurar grupos de seguridad), siga el procedimiento que se describe a continuación para que el Elastic Load Balancing cree un grupo de seguridad para el balanceador de carga de forma automática.

Para configurar un grupo de seguridad para el balanceador de carga

1. Elija Create a new security group.
2. Escriba el nombre y la descripción del grupo de seguridad o conserve los predeterminados. Este nuevo grupo de seguridad contiene una regla que permite pasar tráfico al puerto del agente de escucha del balanceador de carga que ha seleccionado en la página Configure Load Balancer.
3. Elija Next: Configure Routing.

Paso 4: Configurar el grupo de destino

Cree el grupo de destino que se va a utilizar para el direccionamiento de solicitudes. La regla predeterminada del agente de escucha direcciona las solicitudes a los destinos registrados en este grupo de destino. El balanceador de carga comprueba el estado de los destinos del grupo utilizando las opciones de comprobación de estado definidas en el grupo de destino. En la página Configure Routing, realice el siguiente procedimiento.

Para configurar el grupo de destino

1. En Target group (Grupo de destino), mantenga el valor predeterminado, New target group (Nuevo grupo de destino).
2. En Name, escriba el nombre del nuevo grupo de destino.
3. Mantenga el tipo de destino (Instance (Instancia)), el protocolo (HTTP) y el puerto (80) predeterminados.
4. En Health checks (Comprobaciones de estado), mantenga la configuración predeterminada.
5. Elija Next: Register Targets.

Paso 5: Registrar destinos con el grupo de destino

En la página Register Targets, realice el siguiente procedimiento.

Para registrar sus instancias en el grupo de destino

1. En Instances, seleccione una o varias instancias.
2. Mantenga el puerto predeterminado, (80), y elija Add to registered (Añadir a registrado).
3. Cuando haya terminado de seleccionar instancias, elija Next: Review.

Paso 6: Crear y probar el balanceador de carga

Antes de crear el balanceador de carga, revise la configuración seleccionada. Después de crear el balanceador de carga, compruebe que se puede enviar tráfico a las instancias EC2.

Para crear y probar el balanceador de carga

1. En la página Review, elija Create.
2. Una vez que se le notifique que el balanceador de carga se ha creado correctamente, elija Close.
3. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
4. Seleccione el grupo de destino que se acaba de crear.
5. En la pestaña Targets, asegúrese de que las instancias están listas. Si el estado de una instancia es `initial`, puede deberse a que la instancia sigue en proceso de registro o no ha superado el número mínimo de comprobaciones de estado para que se considere correcta. Cuando el estado de al menos una instancia sea `healthy`, podrá probar el balanceador de carga.
6. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
7. Seleccione el balanceador de carga recién creado.
8. En la pestaña Description, copie el nombre DNS del balanceador de carga (por ejemplo, mi-balanceador-de-carga-1234567890.us-west-2.elb.amazonaws.com). Pegue el nombre DNS en el campo de direcciones de un navegador web que esté conectado a Internet. Si todo funciona normalmente, el navegador mostrará la página predeterminada del servidor.

9. (Opcional) Para definir reglas de agente de escucha adicionales, consulte Agregar una regla (p. 43).

Paso 7: Eliminar el balanceador de carga (opcional)

Tan pronto como un balanceador de carga está disponible, se le facturará por cada hora u hora parcial que se mantenga en ejecución. Cuando ya no necesite un balanceador de carga, puede eliminarlo. Tan pronto como se elimina el balanceador de carga, dejan de acumularse cargos por él. Tenga en cuenta que, cuando se elimina un balanceador de carga, los destinos registrados con él no se ven afectados. Por ejemplo, las instancias EC2 seguirán en ejecución.

Para eliminar el balanceador de carga

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione la casilla de verificación para el balanceador de carga y, a continuación, elija Actions, Delete.
4. Cuando se le indique que confirme, seleccione Yes, Delete.

Tutoriales para Application Load Balancers

En los siguientes tutoriales de Elastic Load Balancing, aprenderá a realizar tareas comunes con un Balanceador de carga de aplicaciones.

- Introducción a Elastic Load Balancing (Guía del usuario de Elastic Load Balancing)
- Tutorial: Uso del direccionamiento basado en rutas con el Application Load Balancer (p. 9)
- Tutorial: Utilizar microservicios como destinos con Application Load Balancer (p. 11)
- Tutorial: Crear un Application Load Balancer con AWS CLI (p. 13)

Tutorial: Uso del direccionamiento basado en rutas con el Application Load Balancer

Puede crear un agente de escucha con reglas para reenviar las solicitudes según la ruta de la URL. Esto se denomina direccionamiento basado en rutas. Si ejecuta microservicios, puede direccionar el tráfico a diversos servicios backend mediante el direccionamiento basado en rutas. Por ejemplo, puede direccionar las solicitudes generales a un grupo de destino y las solicitudes de representación de imágenes, a otro.

Antes de empezar

- Lance las instancias EC2 en una nube virtual privada (VPC). Asegúrese de que los grupos de seguridad de estas instancias permiten obtener acceso al puerto del agente de escucha y al puerto de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino (p. 68).
- Compruebe que los microservicios están implementados en las instancias EC2 que desea registrar.

Creación del balanceador de carga

Para crear un balanceador de carga que utiliza el direccionamiento basado en rutas

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la misma región que seleccionó para las instancias EC2.
3. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
4. Cree un grupo de destino para el primer conjunto de destinos, como se indica a continuación:
   a. Elija Create target group.
   b. Especifique el nombre, protocolo, puerto y VPC para el grupo de destino y, a continuación, elija Create.
   c. Seleccione el nuevo grupo de destino.
   d. En la pestaña Targets, seleccione Edit.
   e. En Instances, seleccione una o varias instancias. Especifique un puerto para las instancias, elija Agregue al registrado y, a continuación, elija Save.

Tenga en cuenta que el estado de las instancias es `initial` hasta que se hayan registrado y superado las comprobaciones de estado. A continuación, su estado será `unused` hasta que haya configurado el grupo de destino que recibirá el tráfico del balanceador de carga.

5. Si desea crear un grupo de destino para el segundo conjunto de destinos, siga este procedimiento:
   a. Elija Create target group.
   b. Especifique el nombre, protocolo, puerto y VPC para el grupo de destino y, a continuación, elija Create.
   c. En la pestaña Targets, seleccione Edit.
   d. En Instances, seleccione una o varias instancias. Especifique un puerto para las instancias, elija Agregue al registrado y, a continuación, elija Save.

      Tenga en cuenta que el estado de las instancias es `initial` hasta que se hayan registrado y superado las comprobaciones de estado. A continuación, su estado será `unused` hasta que haya configurado el grupo de destino que recibirá el tráfico del balanceador de carga.
6. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
7. Elija Create Load Balancer.
8. En Select load balancer type, elija Application Load Balancer.
9. Elija Continue.
10. Complete los campos de esta página Configure Load Balancer de la siguiente manera:
    a. En Name, escriba el nombre del balanceador de carga.

       El nombre del Balanceador de carga de aplicaciones debe ser único en el conjunto de Application Load Balancers y Network Load Balancers de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar por un guion.
    b. En Scheme, un balanceador de carga expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta los destinos. Un balanceador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.
    c. En Listeners, el valor predeterminado es un agente de escucha que acepta tráfico HTTP en el puerto 80. Puede conservar los ajustes predeterminados del agente de escucha, modificar el protocolo o el puerto del agente de escucha o elegir Add para agregar otro agente de escucha.
    d. En Availability Zones, seleccione la VPC que ha usado para las instancias EC2. Seleccione al menos dos zonas de disponibilidad. Si hay una subred en una zona de disponibilidad, se seleccionará. Si hay más de una subred en una zona de disponibilidad, seleccione una de ellas. Tenga en cuenta que puede seleccionar una sola subred por zona de disponibilidad.
    e. Elija Next: Configure Security Settings.
11. (Opcional) Si ha creado un agente de escucha seguro en el paso anterior, debe completar la página Configure Security Settings como se indica a continuación:
    a. Si creó o importó el certificado a través de AWS Certificate Manager, seleccione Choose an existing certificate from AWS Certificate Manager (ACM) (Elegir un certificado existente desde AWS Certificate Manager (ACM)) y, a continuación, seleccione el certificado en Certificate name (Nombre de certificado).
    b. Si cargó el certificado a través de IAM, seleccione Choose an existing certificate from AWS Identity and Access Management (IAM) y, a continuación, seleccione su certificado de Certificate name.
    c. Si tiene un certificado para cargar, pero ACM no se admite en su región, elija Upload a new SSL Certificate to AWS Identity and Access Management (IAM). En Certificate name, escriba un nombre único para el certificado. En Private Key, copie y pegue el contenido del archivo de clave privada (con codificación PEM). En Public Key Certificate, copie y pegue el contenido del archivo de certificado de clave pública (con codificación PEM). En Certificate Chain, copie y pegue

el contenido del archivo de cadena del certificado (con codificación PEM), a no ser que utilice un certificado autofirmado y no sea importante que los navegadores acepten implícitamente dicho certificado.

d. Para Select policy, mantenga la política de seguridad predefinida.

12. Elija Next: Configure Security Groups.
13. Complete los campos de esta página Configure Security Groups de la siguiente manera:

    a. Seleccione Create a new security group.
    b. Escriba el nombre y la descripción del grupo de seguridad o conserve los predeterminados. Este nuevo grupo de seguridad contiene una regla que permite pasar tráfico al puerto que ha seleccionado para el balanceador de carga en la página Configure Load Balancer.
    c. Elija Next: Configure Routing.

14. Complete los campos de esta página Configure Routing de la siguiente manera:

    a. Para Target group, elija `Existing target group`.
    b. Para Name, seleccione el primer grupo de destino que ha creado.
    c. Elija Next: Register Targets.

15. En la página Register Targets, las instancias que ha registrado con el grupo de destino aparecen en Registered instances. No puede modificar los destinos registrados en el grupo de destino hasta después de haber completado el asistente. Elija Next: Review.
16. En la página Review, elija Create.
17. Una vez que se le notifique que el balanceador de carga se ha creado correctamente, elija Close.
18. Seleccione el balanceador de carga recién creado.
19. En la pestaña Listeners (Agentes de escucha), elija View/edit rules (Ver/editar reglas) y, luego, el icono Add rules (Añadir reglas) (el símbolo de suma). Especifique la regla como se indica a continuación:

    a. Elija Insert Rule.
    b. Elija Add condition (Añadir condición), Path is (La ruta es) y escriba el patrón exacto que se debe utilizar para el direccionamiento basado en rutas (por ejemplo, `/img/*`). Para guardar la condición, elija el icono de marca de verificación. Para obtener más información, consulte Reglas del agente de escucha (p. 29).
    c. Elija Add action (Añadir acción), Forward to (Reenviar a) y, luego, el segundo grupo de destino que ha creado. Para guardar la acción, seleccione el icono de marca de verificación.
    d. Elija Save (Guardar) para guardar la regla.

Tutorial: Utilizar microservicios como destinos con Application Load Balancer

Puede utilizar una arquitectura de microservicios para estructurar la aplicación en diferentes servicios que se puedan desarrollar e implementar por separado. Puede instalar uno o varios de estos servicios en cada instancia EC2, donde cada servicio aceptará las conexiones en un puerto diferente. Puede utilizar un único Balanceador de carga de aplicaciones para direccionar las solicitudes a todos los servicios de la aplicación. Cuando registre una instancia EC2 con un grupo de destino, puede realizar el registro varias veces; en cada servicio, registre la instancia usando el puerto del servicio.

Important

Cuando se implementan servicios con Amazon Elastic Container Service (Amazon ECS), puede utilizar el mapeo de puertos dinámico para realizar varias tareas desde un único servicio de la misma instancia de contenedor. Amazon ECS administra las actualizaciones de sus servicios registrando y anulando el registro automáticamente de los contenedores en el grupo de destino

utilizando el ID de instancia y el puerto de cada contenedor. Para obtener más información, consulte Balanceo de carga de servicios en la Amazon Elastic Container Service Developer Guide.

Antes de empezar

- Lance las instancias EC2. Asegúrese de que los grupos de seguridad de las instancias permiten el acceso desde el grupo de seguridad del balanceador de carga en los puertos de escucha y los puertos de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino (p. 68).
- Implemente los servicios en las instancias EC2 (por ejemplo, usando contenedores).

Creación del balanceador de carga

Para crear un balanceador de carga que utilice varios servicios como destinos

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, seleccione la misma región que seleccionó para las instancias EC2.
3. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
4. Elija Create Load Balancer.
5. En Select load balancer type, elija Application Load Balancer.
6. Elija Continue.
7. Complete los campos de esta página Configure Load Balancer de la siguiente manera:

   a. En Name, escriba el nombre del balanceador de carga.

      El nombre del Balanceador de carga de aplicaciones debe ser único en el conjunto de Application Load Balancers y Network Load Balancers de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar por un guion.

   b. En Scheme, un balanceador de carga expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta los destinos. Un balanceador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.

   c. En Listeners, el valor predeterminado es un agente de escucha que acepta tráfico HTTP en el puerto 80. Puede conservar los ajustes predeterminados del agente de escucha, modificar el protocolo o el puerto del agente de escucha o elegir Add para agregar otro agente de escucha.

   d. En Availability Zones, seleccione la VPC que ha usado para las instancias EC2. Seleccione al menos dos zonas de disponibilidad. Si hay una subred en una zona de disponibilidad, se seleccionará. Si hay más de una subred en una zona de disponibilidad, seleccione una de ellas. Tenga en cuenta que puede seleccionar una sola subred por zona de disponibilidad.

   e. Elija Next: Configure Security Settings.

8. (Opcional) Si ha creado un agente de escucha seguro en el paso anterior, debe completar la página Configure Security Settings como se indica a continuación:

   a. Si creó o importó el certificado a través de AWS Certificate Manager, seleccione Choose an existing certificate from AWS Certificate Manager (ACM) (Elegir un certificado existente desde AWS Certificate Manager (ACM)) y, a continuación, seleccione el certificado en Certificate name (Nombre de certificado).

   b. Si cargó el certificado a través de IAM, seleccione Choose an existing certificate from AWS Identity and Access Management (IAM) (Elegir un certificado existente en AES Identity and Access Management (IAM)) y, a continuación, seleccione el certificado en Certificate name (Nombre de certificado).

c. Si tiene un certificado para cargar, pero ACM no se admite en su región, elija Upload a new SSL Certificate to AWS Identity and Access Management (IAM). En Certificate name, escriba un nombre único para el certificado. En Private Key, copie y pegue el contenido del archivo de clave privada (con codificación PEM). En Public Key Certificate, copie y pegue el contenido del archivo de certificado de clave pública (con codificación PEM). En Certificate Chain, copie y pegue el contenido del archivo de cadena del certificado (con codificación PEM), a no ser que utilice un certificado autofirmado y no sea importante que los navegadores acepten implícitamente dicho certificado.

d. Para Select policy, mantenga la política de seguridad predefinida.

9. Elija Next: Configure Security Groups.
10. Complete los campos de esta página Configure Security Groups de la siguiente manera:

    a. Seleccione Create a new security group.

    b. Escriba el nombre y la descripción del grupo de seguridad o conserve los predeterminados. Este nuevo grupo de seguridad contiene una regla que permite pasar tráfico al puerto que ha seleccionado para el balanceador de carga en la página Configure Load Balancer.

    c. Elija Next: Configure Routing.

11. Complete los campos de esta página Configure Routing de la siguiente manera:

    a. Para Target group, mantener la forma predeterminada `New target group`.

    b. En Name, escriba el nombre del nuevo grupo de destino.

    c. Establezca Protocol y Port según sea necesario.

    d. En Health checks, conserve la configuración predeterminada de la comprobación de estado.

    e. Elija Next: Register Targets.

12. Para Register Targets, haga lo siguiente:

    a. En Instances, seleccione una instancia EC2.

    b. Escriba el puerto que se utiliza en el servicio y, a continuación, elija Add to registered.

    c. Repita este procedimiento con cada servicio que desee registrar. Cuando haya terminado, seleccione Next: Review.

13. En la página Review, elija Create.
14. Una vez que se le notifique que el balanceador de carga se ha creado correctamente, elija Close.

Tutorial: Crear un Application Load Balancer con AWS CLI

En este tutorial, encontrará una introducción práctica acerca de cómo crear Application Load Balancers a través de la AWS CLI.

Antes de empezar

- Utilice el siguiente comando para asegurarse de que está ejecutando una versión de la AWS CLI compatible con los Application Load Balancers.

```
aws elbv2 help
```

  Si aparece un mensaje de error en el que se indica que elbv2 no es una opción válida, actualice AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

- Lance las instancias EC2 en una nube virtual privada (VPC). Asegúrese de que los grupos de seguridad de estas instancias permiten obtener acceso al puerto del agente de escucha y al puerto de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino (p. 68).

Creación del balanceador de carga

Para crear el primer balanceador de carga, siga los pasos que se describen a continuación.

Para crear un balanceador de carga

1. Utilice el comando create-load-balancer para crear un balanceador de carga. Debe especificar dos subredes que no estén en la misma zona de disponibilidad.

```
aws elbv2 create-load-balancer --name my-load-balancer  \
--subnets subnet-12345678 subnet-23456789 --security-groups sg-12345678
```

   El resultado contiene el nombre de recurso de Amazon (ARN) del balanceador de carga con el siguiente formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/app/my-load-
balancer/1234567890123456
```

2. Utilice el comando create-target-group para crear un grupo de destino especificando la misma VPC que ha usado para las instancias EC2:

```
aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
--vpc-id vpc-12345678
```

   El resultado contiene el ARN del grupo con este formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Utilice el comando register-targets para registrar las instancias con el grupo de destino:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678 Id=i-23456789
```

4. Utilice el comando create-listener para crear un agente de escucha del balanceador de carga con una regla predeterminada que reenvíe las solicitudes al grupo de destino:

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol HTTP --port 80  \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

   El resultado contiene el ARN del agente de escucha con el siguiente formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/app/my-load-
balancer/1234567890123456/1234567890123456
```

5. (Opcional) Puede comprobar el estado de los destinos registrados en el grupo de destino con este comando describe-target-health:

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Agregar un agente de escucha HTTPS

Si tiene un balanceador de carga con un agente de escucha HTTP, puede agregar un agente de escucha HTTPS tal y como se indica a continuación.

Para agregar un agente de escucha HTTPS a un balanceador de carga

1. Cree un certificado SSL para usarlo con el balanceador de carga a través de uno de estos métodos:
   - Cree o importe el certificado con AWS Certificate Manager (ACM). Para obtener más información, consulte Solicitar un certificado o Importar certificados en la Guía del usuario de AWS Certificate Manager.
   - Cargue el certificado con AWS Identity and Access Management (IAM). Para obtener más información, consulte Uso de certificados de servidor en la Guía del usuario de IAM.
2. Utilice el comando create-listener para crear el agente de escucha con una regla predeterminada que reenvíe las solicitudes al grupo de destino. Cuando cree un agente de escucha HTTPS, deberá especificar un certificado SSL. Tenga en cuenta que puede especificar una política SSL que no sea la predeterminada a través de la opción `--ssl-policy`.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn \
--protocol HTTPS --port 443  \
--certificates CertificateArn=certificate-arn \
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Agregar destinos utilizando anulaciones de puertos

Si tiene varios contenedores de ECS en la misma instancia, cada uno de los contenedores aceptará las conexiones en un puerto distinto. La instancia se puede registrar con el grupo de destino varias veces, usando cada vez un puerto diferente.

Para agregar destinos utilizando anulaciones de puertos

1. Utilice el comando create-target-group para crear un grupo de destino:

```
aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
--vpc-id vpc-12345678
```

2. Utilice el comando register-targets para registrar las instancias con el grupo de destino. Observe que el ID de instancia es el mismo para todos los contenedores, pero que los puertos son diferentes.

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678,Port=80 Id=i-12345678,Port=766
```

3. Utilice el comando create-rule para agregar una regla al agente de escucha que reenvíe las solicitudes al grupo de destino:

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--actions Type=forward,TargetGroupArn=targetgroup-arn
```

Agregar direccionamiento basado en rutas

Si tiene un agente de escucha con una regla predeterminada que reenvía solicitudes a un grupo de destino, puede agregar otra regla para que las reenvíe a un grupo de destino diferente en función de la dirección URL. Por ejemplo, puede direccionar las solicitudes generales a un grupo de destino y las solicitudes de presentación de imágenes a otro.

Para agregar una regla a un agente de escucha usando un patrón de ruta

1. Utilice el comando create-target-group para crear un grupo de destino:

```
aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
--vpc-id vpc-12345678
```

2. Utilice el comando register-targets para registrar las instancias con el grupo de destino:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-12345678 Id=i-23456789
```

3. Utilice el comando create-rule para agregar al agente de escucha una regla que reenvíe las solicitudes al grupo de destino si la dirección URL se ajusta a un patrón específico:

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values='/img/*' \
--actions Type=forward,TargetGroupArn=targetgroup-arn
```

Eliminar el balanceador de carga

Cuando ya no necesite el balanceador de carga ni el grupo de destino, puede eliminarlos tal y como se indica a continuación:

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Application Load Balancers

Un balanceador de carga actúa como único punto de contacto para los clientes. Los clientes envía las solicitudes al balanceador de carga y este se las envía a los destinos, tales como las instancias EC2, en dos o más zonas de disponibilidad. Para configurar el balanceador de carga, debe crear grupos de destino (p. 57) y, a continuación, registrar los destinos en esos grupos. También puede crear agentes de escucha (p. 28) para comprobar la existencia de solicitudes de conexión de los clientes, así como reglas de agentes de escucha para direccionar las solicitudes de los clientes a los destinos de uno o varios grupos de destino.

Para obtener más información, consulte Cómo funciona Elastic Load Balancing en la Guía del usuario de Elastic Load Balancing.

Contenido

Subredes del balanceador de carga

Cuando cree un balanceador de carga, debe especificar una subred pública desde al menos dos zonas de disponibilidad. Solo puede especificar una subred pública por zona de disponibilidad.

Para garantizar que el balanceador de carga puede adaptarse correctamente, asegúrese de que cada subred del balanceador de carga tiene un bloque de CIDR con al menos una máscara de bits con el número `/27` (por ejemplo, `10.0.0.0/27`) y al menos ocho direcciones IP libres. El balanceador de carga utiliza estas direcciones IP para establecer conexiones con los destinos.

Grupos de seguridad de los balanceadores de carga

Un grupo de seguridad funciona como un firewall que controla el tráfico que se permite entrar o salir del balanceador de carga. Puede elegir los puertos y protocolos que se admitirán para el tráfico entrante y saliente.

Las reglas de los grupos de seguridad asociados con el grupo de seguridad del balanceador de carga deben permitir el tráfico en ambas direcciones tanto en el agente de escucha como en los puertos de

comprobación de estado. Siempre que se agrega un agente de escucha a un balanceador de carga o se actualiza el puerto de comprobación de estado de un grupo de destino, es preciso revisar las reglas del grupo de seguridad con el fin de asegurarse de que permitan el tráfico en el nuevo puerto en ambas direcciones. Para obtener más información, consulte Reglas recomendadas (p. 24).

Estado del balanceador de carga

Un balanceador de carga puede encontrarse en uno de los siguientes estados:

`provisioning`

El balanceador de carga se está configurando.

`active`

El balanceador de carga se ha configurado completamente y está listo para direccionar el tráfico.

`failed`

El balanceador de carga no se han podido configurar.

Atributos del balanceador de carga

A continuación se indican los atributos del balanceador de carga:

`access_logs.s3.enabled`

Indica si están habilitados los logs de acceso almacenados en Amazon S3. El valor predeterminado es `false`.

`access_logs.s3.bucket`

Nombre del bucket de S3 para los logs de acceso. Este atributo es obligatorio si están habilitados los registros de acceso. Para obtener más información, consulte Permisos de buckets (p. 100).

`access_logs.s3.prefix`

Prefijo de la ubicación en el bucket de S3.

`deletion_protection.enabled`

Indica si está habilitada la protección contra eliminación. El valor predeterminado es `false`.

`idle_timeout.timeout_seconds`

Valor del tiempo de inactividad, en segundos. El valor predeterminado es de 60 segundos.

`routing.http2.enabled`

Indica si HTTP/2 está habilitado. El valor predeterminado es `true`.

Tipo de dirección IP

Puede configurar el tipo de dirección IP del balanceador de carga expuesto a Internet al crearlo, o bien una vez que se encuentre activo. Tenga en cuenta que los balanceadores de carga internos deben utilizar direcciones IPv4.

A continuación se indican los tipos de direcciones IP del balanceador de carga:

`ipv4`

El balanceador de carga admite solamente las direcciones IPv4 (por ejemplo, 192.0.2.1).

`dualstack`

El balanceador de carga es compatible con las direcciones IPv4 e IPv6 (por ejemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334).

Los clientes que se comunican con el equilibrador de carga a través de direcciones IPv4 resuelven el registro A y los clientes que se comunican con el balanceador de carga a través de direcciones IPv6 resuelven el registro AAAA. Sin embargo, el balanceador de carga se comunica con sus destinos utilizando direcciones IPv4, independientemente de cómo se comunique el cliente con el balanceador de carga.

Para obtener más información, consulte Tipos de direcciones IP para el Application Load Balancer (p. 26).

Protección contra eliminación

Para evitar que el balanceador de carga se elimine por error, puede habilitar la protección contra eliminación. De forma predeterminada, la protección contra eliminación del balanceador de carga está deshabilitada.

Si habilita la protección contra eliminación del balanceador de carga, deberá deshabilitarla para poder eliminarlo.

Para habilitar la protección contra eliminación desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit load balancer attributes (Editar atributos del balanceador de carga), seleccione Enable (Habilitar) en Delete Protection (Eliminar protección) y haga clic en Save (Guardar).
6. Seleccione Save.

Para deshabilitar la protección contra eliminación desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit load balancer attributes (Editar atributos del balanceador de carga), desactive Enable (Habilitar) en Delete Protection (Eliminar protección) y haga clic en Save (Guardar).
6. Seleccione Save.

Para habilitar o deshabilitar la protección contra eliminación desde la AWS CLI

Use el comando modify-load-balancer-attributes con el atributo `deletion_protection.enabled`.

Tiempo de inactividad de conexión

Para cada solicitud que un cliente realiza a través de un balanceador de carga, este último mantiene dos conexiones. Una conexión frontend entre el cliente y el balanceador de carga, así como una conexión

backend entre este último y un destino. El balanceador de carga administra un tiempo de espera de inactividad que se aplica cuando no se han enviado datos a través de una conexión frontend durante el periodo de tiempo especificado. Si no se han enviado ni recibido datos antes de que haya transcurrido el tiempo de inactividad, el balanceador de carga cerrará la conexión.

De forma predeterminada, Elastic Load Balancing establece el valor del tiempo de inactividad en 60 segundos. Por lo tanto, si el destino no envía datos al menos cada 60 segundos mientras la solicitud está en tránsito, el balanceador de carga podría cerrar la conexión frontend. Para asegurarse de que las operaciones de larga duración (como la carga de archivos) dispongan de tiempo suficiente para completarse, envíe al menos un byte de datos antes de que finalice cada tiempo de inactividad y aumente la duración de este tiempo, según sea necesario.

Para las conexiones backend, recomendamos habilitar la opción keep-alive de HTTP en las instancias EC2. Puede habilitar keep-alive de HTTP en los ajustes del servidor web para sus instancias de EC2. Si la habilita, el balanceador de carga puede reutilizar las conexiones backend hasta que se agote el tiempo de espera de keep-alive. También recomendamos que configure el tiempo de inactividad de su aplicación para que sea mayor que el tiempo de inactividad configurado para el balanceador de carga.

Para actualizar el valor del tiempo de inactividad desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit load balancer attributes, escriba un valor por Idle timeout, en segundos. El rango válido es de 1 a 4000. El valor predeterminado es de 60 segundos.
6. Seleccione Save.

Para actualizar el valor del tiempo de inactividad desde la AWS CLI

Use el comando modify-load-balancer-attributes con el atributo `idle_timeout.timeout_seconds`.

Application Load Balancers y AWS WAF

Puede utilizar AWS WAF con su Balanceador de carga de aplicaciones para permitir o bloquear solicitudes en función de las reglas en una lista de control de acceso web (ACL web). Para obtener más información, consulte Uso de ACL web en la Guía para desarrolladores de AWS WAF.

Para comprobar si el balanceador de carga se integra con AWS WAF, seleccione el balanceador de carga en la Consola de administración de AWS y elija la pestaña Integrated services (Servicios integrados).

Creación de un Application Load Balancer

Un balanceador de carga toma las solicitudes de los clientes y las distribuye entre los destinos de un grupo de destino.

Antes de comenzar, asegúrese de que dispone de una nube virtual privada (VPC) con al menos una subred pública en cada una de las zonas de disponibilidad que utilizan sus destinos.

Para crear un balanceador de carga mediante la AWS CLI, consulte Tutorial: Crear un Application Load Balancer con AWS CLI (p. 13).

Para crear un balanceador de carga desde la Consola de administración de AWS, complete las siguientes tareas.

Tareas

Paso 1: Configurar un balanceador de carga y un agente de escucha

En primer lugar, proporcione alguna información de configuración básica para el balanceador de carga como, por ejemplo, un nombre, una red y uno o más agentes de escucha. Un agente de escucha es un proceso que comprueba solicitudes de conexión. Se configura con un protocolo y un puerto para las conexiones entre los clientes y el balanceador de carga. Para obtener más información acerca de los puertos y protocolos compatibles, consulte Configuración del agente de escucha (p. 28).

Para configurar el balanceador de carga y el agente de escucha

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Elija Create Load Balancer.
4. Para Application Load Balancer, elija Create.
5. En Name, escriba el nombre del balanceador de carga. Por ejemplo, **`my-alb`**.
6. En Scheme, un balanceador de carga expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta los destinos. Un balanceador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.
7. En IP address type (Tipo de dirección IP), elija ipv4 si sus subredes usan direcciones IPv4 o dualstack si sus subredes usan direcciones IPv4 e IPv6.
8. En Listeners, el valor predeterminado es un agente de escucha que acepta tráfico HTTP en el puerto 80. Puede conservar la configuración predeterminada del agente de escucha, modificar el protocolo o modificar el puerto. Elija Add para agregar otro agente de escucha (por ejemplo, agente de escucha HTTPS).
9. Para Availability Zones, seleccione al menos dos zonas de disponibilidad desde su VPC. Si hay una subred en una zona de disponibilidad, se seleccionará. Si hay más de una subred en una zona de disponibilidad, seleccione una de ellas. Tenga en cuenta que puede seleccionar una sola subred por zona de disponibilidad.
10. Elija Next: Configure Security Settings.

Paso 2: Configurar la seguridad para un agente de escucha HTTPS

Si ha creado un agente de escucha HTTPS en el paso anterior, configure los ajustes de seguridad requeridos. De lo contrario, vaya a la página siguiente del asistente.

Cuando se usa HTTPS para el agente de escucha del balanceador de carga, es preciso implementar en él un certificado SSL. El balanceador de carga usará dicho certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de enviárselas a los destinos. Para obtener más información, consulte Certificados SSL (p. 38). Debe especificar también la política de seguridad que el balanceador de

carga aplicará para negociar las conexiones SSL con los clientes. Para obtener más información, consulte Políticas de seguridad (p. 40).

Para configurar un certificado y una política de seguridad

1. Para Select default certificate, realice una de las operaciones siguientes:
   - Si creó o importó un certificado a través de AWS Certificate Manager, seleccione Choose a certificate from ACM (Elegir un certificado desde ACM) y, a continuación, seleccione el certificado en Certificate name (Nombre de certificado).
   - Si cargó el certificado a través de IAM, seleccione Choose a certificate from IAM (Elegir un certificado desde IAM) y, a continuación, seleccione el certificado en Certificate name (Nombre de certificado).
2. Para Security policy, le recomendamos que mantenga la política de seguridad predeterminada.
3. Elija Next: Configure Security Groups.

Paso 3: Configurar un grupo de seguridad

El grupo de seguridad del balanceador de carga debe permitir que este último se comunique con los destinos registrados tanto en el puerto del agente de escucha como en el puerto de comprobación de estado. La consola puede crear automáticamente un grupo de seguridad para el balanceador de carga con las reglas que permiten esta comunicación. Si lo prefiere, puede crear el grupo de seguridad y seleccionarlo. Para obtener más información, consulte Reglas recomendadas (p. 24).

Para configurar un grupo de seguridad para el balanceador de carga

1. Elija Create a new security group.
2. Escriba el nombre y la descripción del grupo de seguridad o conserve los predeterminados. Este nuevo grupo de seguridad contiene una regla que permite pasar tráfico al puerto que ha seleccionado para el balanceador de carga en la página Configure Load Balancer.
3. Elija Next: Configure Routing.

Paso 4: Configurar un grupo de destino

Los destinos se registran con un grupo de destino. El grupo de destino que se configura en este paso se utiliza como grupo de destino en la regla del agente de escucha predeterminado, que reenvía las solicitudes al grupo de destino. Para obtener más información, consulte Grupos de destino para los Application Load Balancers (p. 57).

Para configurar el grupo de destino

1. Para Target group, mantenga el valor predeterminado, New target group.
2. En Name, escriba el nombre del grupo de destino.
3. En Target type (Tipo de destino), seleccione Instance (Instancia) para registrar los destinos por ID de instancia, IP para registrar direcciones IP y Lambda function (Función Lambda) para registrar una función Lambda.
4. (Opcional) Si el tipo de destino es Instance (Instancia) o IP, modifique el puerto y el protocolo según corresponda.
5. (Opcional) Si el tipo de destino es Lambda function (Función Lambda), habilite las comprobaciones de estado según corresponda.
6. En Health checks, conserve la configuración predeterminada de la comprobación de estado.
7. Elija Next: Register Targets.

Paso 5: Configurar los destinos del grupo de destino

Con un Balanceador de carga de aplicaciones, el tipo de destino de su grupo de destino determina cómo se registran los destinos en el grupo de destino.

Para registrar destinos por ID de instancia

1. En Instances, seleccione una o varias instancias.
2. Escriba el puerto del agente de escucha de la instancia y, a continuación, elija Add to registered.
3. Cuando haya terminado de registrar instancias, elija Next: Review.

Para registrar direcciones IP

1. Para cada dirección IP que desee registrar, haga lo siguiente:
   a. En Network, si la dirección IP corresponde a una subred de la VPC del grupo de destino, seleccione la VPC. De lo contrario, seleccione Other private IP address.
   b. En IP, escriba la dirección IP.
   c. En Port, escriba el puerto.
   d. Elija Add to list.
2. Cuando haya terminado de agregar direcciones IP a la lista, elija Next: Review.

Para registrar una función Lambda

1. En Lambda function (Función Lambda), realice alguna de las siguientes operaciones:
   - Seleccione la función Lambda
   - Cree una nueva función Lambda y selecciónela
   - Registre la función Lambda después de crear el grupo de destino
2. Elija Next: Review.

Paso 6: Crear el balanceador de carga

Después de crear el balanceador de carga, puede comprobar que los destinos han superado la comprobación de estado inicial y, a continuación, comprobar que el balanceador de carga les envía tráfico. Cuando haya terminado de usar el balanceador de carga, puede eliminarlo. Para obtener más información, consulte Eliminación de un Application Load Balancer (p. 27).

Para crear el balanceador de carga

1. En la página Review, elija Create.
2. Una vez creado el balanceador de carga, elija Close.
3. (Opcional) Para definir reglas adicionales del agente de escucha que reenvíen las solicitudes en función de un patrón de ruta o un nombre de host, consulte Agregar una regla (p. 43).

Zonas de disponibilidad del Application Load Balancer

Puede habilitar o deshabilitar las zonas de disponibilidad del balanceador de carga en cualquier momento. Después de habilitar una zona de disponibilidad, el balanceador de carga comienza a direccionar

solicitudes a los destinos registrados contenidos en ella. El balanceador de carga es más eficaz si se asegura de que cada zona de disponibilidad habilitada tenga al menos un destino registrado.

Después de deshabilitar una zona de disponibilidad, los destinos que contiene permanecen registradas en el balanceador de carga, pero este último no direcciona solicitudes a ellos.

Para actualizar las zonas de disponibilidad desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Description en Basic Configuration, elija Edit Availability Zones.
5. Para habilitar una zona de disponibilidad, active su casilla de verificación. Si hay una subred en esa zona de disponibilidad, se seleccionará. Si hay más de una subred en esa zona de disponibilidad, seleccione una de ellas. Tenga en cuenta que puede seleccionar una sola subred por zona de disponibilidad.
6. Para cambiar la subred de una zona de disponibilidad activada, elija Change subnet y seleccione una de las demás subredes.
7. Para eliminar una zona de disponibilidad, desactive su casilla de verificación.
8. Seleccione Save.

Para actualizar las zonas de disponibilidad desde la AWS CLI

Utilice el comando set-subnets.

Grupos de seguridad para el Application Load Balancer

Debe asegurarse de que el balanceador de carga pueda comunicarse con los destinos registrados en el puerto del agente de escucha y en el puerto de comprobación de estado. Cada vez que agregue un agente de escucha al balanceador de carga o actualice la comprobación de estado de un grupo de destino que el balanceador de carga utilice para direccionar solicitudes, debe asegurarse de que los grupos de seguridad asociados a ese balanceador de carga permitan el tráfico en el nuevo puerto en ambas direcciones. Si no es así, puede editar las reglas de los grupos de seguridad que estén asociados al balanceador de carga o bien asociarle otros grupos de seguridad.

Reglas recomendadas

Las reglas recomendadas dependen del tipo de balanceador de carga (expuesto a Internet o interno).

Balanceador de carga expuesto a Internet

Inbound		
Source	Port Range	Comment
0.0.0.0/0	*agente de escucha*	Permite todo el tráfico entrante en el puerto del agente de escucha del balanceador de carga
Outbound		
Destination	Port Range	Comment

grupo de seguridad de instancia	*agente de escucha de instancia*	Permite el tráfico saliente a las instancias en el puerto del agente de escucha de la instancia
grupo de seguridad de instancia	*comprobación de estado*	Permite el tráfico saliente a las instancias en el puerto de comprobación de estado

Balanceador de carga interno

Inbound		
Source	Port Range	Comment
CIDR DE VPC	*agente de escucha*	Permitir el tráfico entrante del CIDR de VPC en el puerto del agente de escucha del balanceador de carga
Outbound		
Destination	Port Range	Comment
grupo de seguridad de instancia	*agente de escucha de instancia*	Permite el tráfico saliente a las instancias en el puerto del agente de escucha de la instancia
grupo de seguridad de instancia	*comprobación de estado*	Permite el tráfico saliente a las instancias en el puerto de comprobación de estado

También recomendamos permitir el tráfico ICMP entrante para admitir la detección de MTU de ruta. Para obtener más información, consulte Detección de la MTU de la ruta en la Guía del usuario de Amazon EC2 para instancias de Linux.

Actualización de los grupos de seguridad asociados

Puede actualizar los grupos de seguridad asociados con el balanceador de carga en cualquier momento.

Para actualizar los grupos de seguridad desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Description en Security, elija Edit security groups.
5. Para asociar un grupo de seguridad al balanceador de carga, selecciónelo. Para eliminar un grupo de seguridad del balanceador de carga, bórrelo.
6. Seleccione Save.

Para actualizar los grupos de seguridad desde la AWS CLI

Utilice el comando set-security-groups.

Tipos de direcciones IP para el Application Load Balancer

Puede configurar el Balanceador de carga de aplicaciones de modo que solo direccione el tráfico IPv4 o para que direccione tanto el tráfico IPv4 como IPv6. Para obtener más información, consulte Tipo de dirección IP (p. 18).

Requisitos de IPv6

- Balanceador de carga expuesto a Internet.
- La nube virtual privada (VPC) tiene subredes con bloques de CIDR IPv6 asociados. Para obtener más información, consulte Direcciones IPv6 en la Guía del usuario de Amazon EC2.

Para actualizar el tipo de dirección IP desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. Elija Actions, Edit IP address type.
5. En IP address type, elija ipv4 para admitir únicamente las direcciones IPv4, o bien dualstack para admitir las direcciones IPv4 e IPv6.
6. Seleccione Save.

Para actualizar el tipo de dirección IP desde la AWS CLI

Utilice el comando set-ip-address-type.

Etiquetas del Application Load Balancer

Las etiquetas le ayudan a clasificar los balanceadores de carga de diversas maneras; por ejemplo, según su finalidad, propietario o entorno.

Puede agregar varias etiquetas a cada balanceador de carga. Las claves de las etiquetas deben ser únicas en cada balanceador de carga. Si agrega una etiqueta con una clave que ya está asociada al balanceador de carga, se actualizará el valor de esa etiqueta.

Cuando haya terminado de utilizar una etiqueta, puede eliminarla del balanceador de carga.

Restricciones

- Cantidad máxima de etiquetas por recurso: 50.
- Longitud máxima de la clave: 127 caracteres Unicode.
- Longitud máxima del valor: 255 caracteres Unicode.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios anteriores o posteriores.
- No utilice el prefijo `aws:` en los nombres o valores de las etiquetas, porque está reservado para uso de AWS. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

Para actualizar las etiquetas de un balanceador de carga desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Tags, elija Add/Edit Tags y, a continuación, realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, modifique los valores Key y Value.
   b. Para agregar una nueva etiqueta, elija Create Tag y, a continuación, escriba los valores para Key y Value.
   c. Para eliminar una etiqueta, elija el icono de eliminación (X) situado junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Save.

Para actualizar las etiquetas de un balanceador de carga desde la AWS CLI

Utilice los comandos add-tags y remove-tags.

Eliminación de un Application Load Balancer

Tan pronto como un balanceador de carga está disponible, se le facturará por cada hora u hora parcial que se mantenga en ejecución. Cuando ya no necesite el balanceador de carga, puede eliminarlo. Tan pronto como se elimina el balanceador de carga, dejan de acumularse cargos por él.

No se puede eliminar un balanceador de carga si está habilitada la protección contra eliminación. Para obtener más información, consulte Protección contra eliminación (p. 19).

Tenga en cuenta que eliminar un balanceador de carga no afecta a los destinos registrados en él. Por ejemplo, las instancias EC2 continuarán ejecutándose y seguirán registradas en sus grupos de destino. Para eliminar los grupos de destino, consulte Eliminación de un grupo de destino (p. 78).

Para eliminar un balanceador de carga desde la consola

1. Si tiene un registro CNAME para el dominio que señala al balanceador de carga, apúntelo hacia una nueva ubicación y espere a que surta efecto el cambio de DNS antes de eliminar el balanceador de carga.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
4. Seleccione el balanceador de carga y, a continuación, elija Actions, Delete.
5. Cuando se le indique que confirme, seleccione Yes, Delete.

Para eliminar un balanceador de carga desde la AWS CLI

Utilice el comando delete-load-balancer.

Agentes de escucha para Application Load Balancer

Antes de comenzar a utilizar Balanceador de carga de aplicaciones, debe agregar uno o varios agentes de escucha. Un agente de escucha es un proceso que comprueba las solicitudes de conexión utilizando el protocolo y el puerto configurados. Las reglas que se definen para un agente de escucha determinan cómo el balanceador de carga va a direccionar las solicitudes a los destinos de uno o varios grupos de destino.

Contenido

Configuración del agente de escucha

Los agentes de escucha admiten los siguientes protocolos y puertos:

- Protocols: HTTP, HTTPS
- Ports: 1-65535

Puede utilizar un agente de escucha HTTPS para trasladar la carga de cifrado y descifrado al balanceador de carga, de modo que las aplicaciones puedan concentrarse en la lógica de negocio. Si el protocolo del agente de escucha es HTTPS, debe implementar al menos un certificado de servidor SSL en el agente de escucha. Para obtener más información, consulte Crear un agente de escucha HTTPS para el balanceador de carga de aplicaciones (p. 38).

Los Application Load Balancers proporcionan compatibilidad nativa con WebSockets. Puede utilizar WebSockets con los agentes de escucha HTTP y HTTPS.

Los Application Load Balancers proporcionan compatibilidad nativa con HTTP/2 con agentes de escucha HTTPS. Puede enviar hasta 128 solicitudes a la vez con una conexión HTTP/2. El balanceador de carga convierte cada una de estas solicitudes HTTP/1.1 y las distribuye a través de los destinos del grupo de destino que tienen un estado correcto. Como HTTP/2 usa las conexiones frontend de una forma más eficaz, es posible que observe que se establecen menos conexiones entre los clientes y el balanceador de carga. No puede utilizar la característica server-push de HTTP/2.

Para obtener más información, consulte Direccionamiento de solicitudes en la Guía del usuario de Elastic Load Balancing.

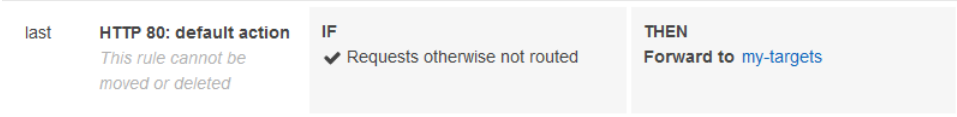
Reglas del agente de escucha

Cada agente de escucha tiene una regla predeterminada, pero, si lo desea, puede definir reglas adicionales. Cada regla consta de una prioridad, una o varias acciones y una o varias condiciones. Puede agregar y editar reglas en cualquier momento. Para obtener más información, consulte Editar una regla (p. 45).

Reglas predeterminadas

Cuando crea un agente de escucha, define acciones para la regla predeterminada. Las reglas predeterminadas no pueden tener condiciones. Si no se cumplen las condiciones de ninguna de las reglas del agente de escucha, se realiza la acción de la regla predeterminada.

A continuación, se muestra un ejemplo de una regla predeterminada vista en la consola:



Prioridad de las reglas

Cada regla tiene una prioridad. Las normas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar. Puede cambiar la prioridad de una regla no predeterminada en cualquier momento. No puede cambiar la prioridad de la regla predeterminada. Para obtener más información, consulte Reorganizar las reglas (p. 46).

Acciones de las reglas

Cada acción de regla tiene un tipo, un orden y la información necesaria para realizar la acción. Para obtener más información, consulte Tipos de acción de regla (p. 29).

Condiciones de las reglas

Cada condición de regla tiene un tipo e información de configuración. Cuando se cumplen las condiciones de una regla, se llevan a cabo sus acciones. Para obtener más información, consulte Tipos de condición de las reglas (p. 33).

Tipos de acción de regla

Se admiten los siguientes tipos de acción para una regla:

`authenticate-cognito`

[Agentes de escucha HTTPS] Utilice Amazon Cognito para autenticar a los usuarios. Para obtener más información, consulte Autenticar a usuarios usando un Balanceador de carga de aplicaciones (p. 49).

`authenticate-oidc`

[Agentes de escucha HTTPS] Utilice un proveedor de identidad compatible con OpenID Connect (OIDC) para autenticar a los usuarios.

`fixed-response`

Devuelve una respuesta HTTP personalizada. Para obtener más información, consulte Acciones de respuesta fija (p. 30).

`forward`

Reenvíe las solicitudes al grupo de destino especificado.

`redirect`

Direcciona las solicitudes de una URL a otra. Para obtener más información, consulte Acciones de redirección (p. 31).

Primero se realiza la acción con el valor de orden más bajo. Cada regla debe incluir exactamente una de las acciones siguientes: `forward`, `redirect` o `fixed-response` y debe ser la última acción que realizar.

Acciones de respuesta fija

Puede utilizar acciones `fixed-response` para omitir las solicitudes del cliente y devolver una respuesta HTTP personalizada. Puede utilizar esta acción para devolver un código de respuesta 2XX, 4XX o 5XX junto con un mensaje opcional.

Cuando se ejecuta una acción `fixed-response`, la acción y la URL del destino se graban en los registros de acceso. Para obtener más información, consulte Entradas de los logs de acceso (p. 93). El número de acciones `fixed-response` correctas se registra en la métrica `HTTP_Fixed_Response_Count`. Para obtener más información, consulte Métricas de Balanceador de carga de aplicaciones (p. 80).

Example Ejemplo de acción de respuesta fija para la AWS CLI

Puede especificar una acción al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La acción siguiente envía una respuesta fija con el código de estado y cuerpo de mensaje especificados.

```
[
  {
      "Type": "fixed-response",
      "FixedResponseConfig": {
          "StatusCode": "200",
          "ContentType": "text/plain",
          "MessageBody": "Hello world"
      }
  }
]
```

Acciones de reenvío

Puede utilizar acciones `forward` para direccionar solicitudes al grupo de destino especificado.

Example Ejemplo de acción de reenvío para la AWS CLI

Puede especificar una acción al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La acción siguiente reenvía la solicitud al grupo de destino especificado.

```
[
```

```
  {
      "Type": "forward",
      "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a06"
  }
]
```

Acciones de redirección

Puede usar acciones `redirect` para redirigir las solicitudes de los clientes de una URL a otra. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades.

Un URI está formado por los siguientes componentes:

```
protocol://hostname:port/path?query
```

Debe modificar al menos uno de los siguientes componentes para evitar que se produzca un bucle de redirección: protocolo, nombre de host, puerto o ruta. Los elementos que no se modifiquen conservarán sus valores originales.

protocolo

Protocolo (HTTP o HTTPS). Puede redirigir HTTP a HTTP, HTTP a HTTPS y HTTPS a HTTPS. No puede redirigir HTTPS a HTTP.

hostname

Nombre del host. Un nombre de host no distingue entre mayúsculas y minúsculas, puede tener hasta 128 caracteres de longitud y constar de caracteres alfanuméricos, comodines (* y ?) y guiones (-).

puerto

Puerto (entre 1 y 65535).

path

Ruta absoluta, comenzando desde la primera "/". Una ruta distingue entre mayúsculas y minúsculas, puede tener hasta 128 caracteres de longitud y constar de caracteres alfanuméricos, comodines (* y ?), & (mediante &) y los caracteres especiales siguientes: _-.$/~'"@:+.

query

Parámetros de la consulta.

Puede reutilizar los componentes del URI de la URL original en la URL de destino utilizando las siguientes palabras clave reservadas:

- `#{protocol}` - Mantiene el protocolo. Se usa en el protocolo y los componentes de consulta.
- `#{host}` - Mantiene el dominio. Se usa en el nombre de host, la ruta y los componentes de consulta.
- `#{port}` - Mantiene el puerto. Se usa en el puerto, la ruta y los componentes de consulta.
- `#{path}` - Mantiene la ruta. Se usa en la ruta y los componentes de consulta.
- `#{query}` - Mantiene los parámetros de consulta. Se usa en el componente de consulta.

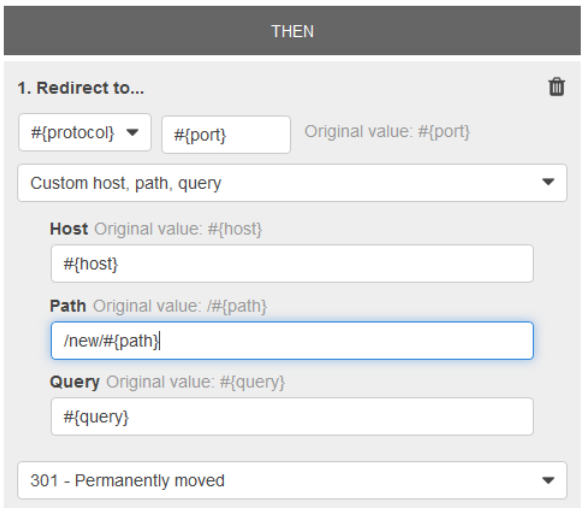
Cuando se ejecuta una acción `redirect`, esta acción se graba en los registros de acceso. Para obtener más información, consulte Entradas de los logs de acceso (p. 93). El número de acciones `redirect`

correctas se registra en la métrica `HTTP_Redirect_Count`. Para obtener más información, consulte Métricas de Balanceador de carga de aplicaciones (p. 80).

Example Ejemplo de acciones de redirección mediante la consola

La siguiente regla configura una redirección permanente a una URL que utiliza el protocolo HTTPS y el puerto especificado (40443), pero mantiene el nombre de host, la ruta y los parámetros de consulta originales. Esta pantalla es equivalente a "https://#{host}:40443/#{path}?#{query}".

La siguiente regla configura una redirección permanente a una URL que utiliza el protocolo, el puerto, el nombre de host y los parámetros de consulta originales y utiliza la palabra clave `#{path}` para crear una ruta modificada. Esta pantalla es equivalente a "#{protocol}://#{host}:#{port}/new/#{path}?#{query}".



Example Ejemplo de acción de redirección para la AWS CLI

Puede especificar una acción al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La siguiente acción redirige una solicitud HTTP a una solicitud HTTPS en el puerto 443, con el mismo nombre de host, ruta y cadena de consulta que la solicitud HTTP.

```
[
  {
      "Type": "redirect",
      "RedirectConfig": {
          "Protocol": "HTTPS",
          "Port": "443",
          "Host": "#{host}",
          "Path": "/#{path}",
          "Query": "#{query}",
          "StatusCode": "HTTP_301"
      }
  }
]
```

Tipos de condición de las reglas

Se admiten los siguientes tipos de condición para una regla:

`host-header`

Ruta basada en el nombre de host de cada solicitud. Para obtener más información, consulte Condiciones de host (p. 34).

`http-header`

Ruta basada en los encabezados HTTP de cada solicitud. Para obtener más información, consulte Condiciones de los encabezados HTTP (p. 33).

`http-request-method`

Ruta basada en el método de solicitud HTTP de cada solicitud. Para obtener más información, consulte Condiciones de método de solicitud HTTP (p. 34).

`path-pattern`

Ruta basada en patrones de ruta en las URL de la solicitud. Para obtener más información, consulte Condiciones de ruta (p. 35).

`query-string`

Ruta basada en pares clave/valor o en valores en las cadenas de consulta. Para obtener más información, consulte Condiciones de cadena de consulta (p. 36).

`source-ip`

Ruta basada en la dirección IP de origen de cada solicitud. Para obtener más información, consulte Condiciones de dirección IP de origen (p. 36).

Cada regla puede incluir cero o una de las condiciones siguientes: `host-header`, `http-request-method`, `path-pattern` y `source-ip` y cero o más de las condiciones siguientes: `http-header` y `query-string`.

Puede especificar hasta tres evaluaciones de coincidencia por condición. Por ejemplo, para cada condición `http-header`, puede especificar hasta tres cadenas que comparar con el valor del encabezado HTTP en la solicitud. La condición se satisface si una de las cadenas coincide con el valor del encabezado HTTP. Para requerir que todas las cadenas sean una coincidencia, cree una condición por evaluación de coincidencia.

Puede especificar hasta cinco evaluaciones de coincidencia por regla. Por ejemplo, puede crear una regla con cinco condiciones donde cada condición tenga una evaluación de coincidencia.

Puede incluir caracteres comodín en las evaluaciones de coincidencia para `http-header`, `host-header`, `path-pattern` y `query-string`. Hay un límite de cinco caracteres comodín por regla.

Condiciones de los encabezados HTTP

Puede utilizar las condiciones de encabezado HTTP para configurar reglas que dirijan solicitudes basadas en los encabezados HTTP para la solicitud. Puede especificar los nombres de campos de encabezado HTTP estándar o personalizados. El nombre del encabezado y la evaluación de coincidencia no distinguen entre mayúsculas y minúsculas. Los siguientes caracteres comodín se admiten en las cadenas de comparación: * (coincide con 0 o más caracteres) y ? (coincide exactamente con 1 carácter). Los caracteres comodín no se admiten en el nombre del encabezado.

Example Ejemplo de condición de encabezado HTTP para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente se satisface mediante solicitudes con un encabezado usuario-agente que coincida con una de las cadenas especificadas.

```
[
  {
      "Field": "http-header",
      "HttpHeaderConfig": {
          "HttpHeaderName": "User-Agent",
          "Values": ["*Chrome*", "*Safari*"]
      }
  }
]
```

Condiciones de método de solicitud HTTP

Puede utilizar las condiciones de método de solicitud HTTP para configurar reglas que dirijan solicitudes basadas en el método de solicitud HTTP de la solicitud. Puede especificar métodos HTTP estándar o personalizados. La evaluación de coincidencia distingue entre mayúsculas y minúsculas. Los caracteres comodín no se admiten; por tanto, el nombre del método tiene que ser una coincidencia exacta.

Le recomendamos direccionar las solicitudes GET y HEAD de la misma forma, porque la respuesta a una solicitud HEAD se podría almacenar en caché.

Example Ejemplo de condición de método HTTP para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente se satisface mediante solicitudes que utilizan el método especificado.

```
[
  {
      "Field": "http-request-method",
      "HttpRequestMethodConfig": {
          "Values": ["CUSTOM-METHOD"]
      }
  }
]
```

Condiciones de host

Puede utilizar las condiciones de host para definir reglas que direccionen solicitudes en función del nombre del host en el encabezado del host (lo que también se conoce como direccionamiento basado en host). Esto permite admitir varios dominios a través de un único balanceador de carga.

Los nombre de host distinguen entre mayúsculas y minúsculas, su longitud máxima es de 128 caracteres y pueden contener cualquiera de los siguientes caracteres:

- A–Z, a–z, 0–9
- - .
- * (coincide con 0 o más caracteres)
- ? (coincide exactamente con 1 carácter)

Debe incluir al menos un carácter ".". Solo puede contener caracteres alfabéticos detrás del carácter "." final.

Ejemplos de nombres de host

- **example.com**
- **test.example.com**
- ***.example.com**

La regla ***.example.com** coincide con **test.example.com** pero no coincide con **example.com**.

Example Ejemplo de condición de encabezado de host para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente se satisface mediante solicitudes con un encabezado de host que coincide con la cadena especificada.

```
[
  {
      "Field": "host-header",
      "HostHeaderConfig": {
          "Values": ["*.example.com"]
      }
  }
]
```

Condiciones de ruta

Puede utilizar las condiciones de ruta para definir reglas que direccionen las solicitudes en función de la dirección URL de la solicitud (lo que también se conoce como direccionamiento basado en ruta).

El patrón de ruta se aplica únicamente a la ruta de la dirección URL, no a sus parámetros de consulta.

Los patrones de ruta distinguen entre mayúsculas y minúsculas, su longitud máxima es de 128 caracteres y pueden contener cualquiera de los siguientes caracteres.

- A–Z, a–z, 0–9
- _ - . $ / ~ " ' @ : +
- & (usando &)
- * (coincide con 0 o más caracteres)
- ? (coincide exactamente con 1 carácter)

Ejemplos de patrones de ruta

- `/img/*`
- `/js/*`

El patrón de ruta se utiliza para direccionar solicitudes, no para modificarlas. Por ejemplo, si una ruta tiene el patrón `/img/*`, la regla reenviará una solicitud para `/img/picture.jpg` al grupo de destino especificado como una solicitud de `/img/picture.jpg`.

Example Ejemplo de condición de patrón de ruta para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente se satisface mediante solicitudes con una dirección URL que contenga la cadena especificada.

```
[
```

```
  {
      "Field": "path-pattern",
      "PathPatternConfig": {
          "Values": ["/img/*"]
      }
  }
]
```

Condiciones de cadena de consulta

Puede utilizar condiciones de cadena de consulta para configurar reglas que dirijan solicitudes basadas en pares clave/valor o valores en la cadena de consulta. La evaluación de coincidencia no distingue entre mayúsculas y minúsculas. Se admiten los siguientes caracteres comodín: * (coincide con 0 o más caracteres) y ? (coincide exactamente con 1 carácter).

Example Ejemplo de condición de cadena de consulta para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente la satisfacen las solicitudes con una cadena de consulta que incluye un par clave/valor de "version=v1" o cualquier clave definida en "example".

```
[
  {
      "Field": "query-string",
      "QueryStringConfig": {
          "Values": [
            {
                "Key": "version",
                "Value": "v1"
            },
            {
                "Value": "example"
            }
          ]
      }
  }
]
```

Condiciones de dirección IP de origen

Puede utilizar las condiciones de dirección IP de origen para configurar reglas que direccionen solicitudes en función de la dirección IP de origen de la solicitud. La dirección IP se debe especificar en formato CIDR. Puede utilizar tanto direcciones IPv4 como IPv6. No se admiten caracteres comodín.

Si un cliente está detrás de un proxy, esta es la dirección IP del proxy, no la dirección IP del cliente.

Esta condición no la satisfacen las direcciones en el encabezado X-Forwarded-For. Para buscar direcciones en el encabezado X-Forwarded-For, utilice una condición `http-header`.

Example Ejemplo de condición de IP de origen para la AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. La condición siguiente se satisface mediante solicitudes con una dirección IP de origen en uno de los bloques de CIDR especificados.

```
[
  {
      "Field": "source-ip",
      "SourceIpConfig": {
          "Values": ["192.0.2.0/24", "198.51.100.10/32"]
```

```
        }
    }
]
```

Crear un agente de escucha HTTP para su balanceador de carga de aplicaciones

Un agente de escucha es un proceso que comprueba solicitudes de conexión. Los agentes de escucha se definen cuando se crea el balanceador de carga, pero se pueden agregar otros agentes de escucha en cualquier momento.

La información de esta página le ayuda a crear un agente de escucha HTTP para su balanceador de carga. Para agregar un agente de escucha HTTPS a su balanceador de carga, consulte Crear un agente de escucha HTTPS para el balanceador de carga de aplicaciones (p. 38)

Requisitos previos

- Para añadir una acción de reenvío a la regla predeterminada del agente de escucha, debe especificar un grupo de destino disponible. Para obtener más información, consulte Creación de un grupo de destino (p. 62).

Agregar un agente de escucha HTTP

Los agentes de escucha se configuran con un protocolo y un puerto para las conexiones entre los clientes y el balanceador de carga, así como un grupo de destino para la regla predeterminada del agente de escucha. Para obtener más información, consulte Configuración del agente de escucha (p. 28).

Para agregar un agente de escucha HTTPS utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (EQUILIBRIO DE CARGA), elija Load Balancers (Balanceadores de carga).
3. Seleccione un balanceador de carga y elija Listeners (Agentes de escucha), Add listener (Añadir agente de escucha).
4. En Protocol : port (Protocolo: puerto), elija HTTP y mantenga el puerto predeterminado o introduzca un puerto distinto.
5. En Default actions (Acciones predeterminadas), realice una de las operaciones siguientes:
   - Seleccione Add action (Añadir acción), Forward to (Reenviar a) y un grupo de destino.
   - Seleccione Add action (Añadir acción), Redirect to (Redirigir a) y proporcione una URL para la acción de redirección. Para obtener más información, consulte Acciones de redirección (p. 31).
   - Seleccione Add action (Añadir acción), Return fixed response (Devolver respuesta fija) y proporcione un código de respuesta y un cuerpo opcional para la respuesta. Para obtener más información, consulte Acciones de respuesta fija (p. 30).

   Para guardar la acción, seleccione el icono de marca de verificación.
6. Seleccione Save.
7. (Opcional) Para definir reglas adicionales del agente de escucha que reenvíen las solicitudes en función de un patrón de ruta o un nombre de host, consulte Agregar una regla (p. 43).

Para agregar un agente de escucha HTTPS utilizando la AWS CLI

Utilice el comando create-listener para crear el agente de escucha y la regla predeterminada, y el comando create-rule para definir nuevas reglas del agente de escucha.

Crear un agente de escucha HTTPS para el balanceador de carga de aplicaciones

Un agente de escucha es un proceso que comprueba solicitudes de conexión. Los agentes de escucha se definen cuando se crea el balanceador de carga, pero se pueden agregar otros agentes de escucha en cualquier momento.

Puede crear un agente de escucha HTTPS que utilice conexiones cifradas (lo que también se conoce como descarga de SSL). Esta característica permite el cifrado del tráfico entre el balanceador de carga y los clientes que inician sesiones SSL o TLS.

La información de esta página le ayuda a crear un agente de escucha HTTPS para su balanceador de carga. Para agregar un agente de escucha HTTPS a un balanceador de carga, consulte Crear un agente de escucha HTTP para su balanceador de carga de aplicaciones (p. 37).

Contenido

Certificados SSL

Para utilizar un agente de escucha HTTPS, debe implementar al menos un certificado de servidor SSL/TLS en el balanceador de carga. El balanceador de carga usará este certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de enviárselas a los destinos.

El balanceador de carga requiere certificados X.509 (certificado de servidor SSL/TLS). Los certificados son un formulario digital de identificación emitido por una entidad de certificación (CA). Un certificado contiene información de identificación, un periodo de validez, una clave pública, un número de serie y la firma digital del emisor.

Al crear un certificado para utilizarlo con el balanceador de carga, debe especificar un nombre de dominio.

Le recomendamos que utilice AWS Certificate Manager (ACM) para crear o importar certificados en el balanceador de carga. ACM se integra con Elastic Load Balancing, lo que le permite implementar el certificado en el balanceador de carga. Para obtener más información, consulte la Guía del usuario de AWS Certificate Manager.

> **Important**
>
> ACM admite certificados RSA con una longitud de clave de 4096 bists y certificados EC. Sin embargo, no puede instalar estos certificados en el balanceador de carga a través de la integración con ACM. Debe cargar estos certificados en IAM para utilizarlos con el balanceador de carga.

Si lo desea, también puede usar herramientas de SSL/TLS para crear una solicitud de firma de certificado (CSR), obtener la CSR firmada por una CA para generar el certificado e importar el certificado en ACM

o cargarlo en AWS Identity and Access Management (IAM). Para obtener más información sobre la importación de certificados en ACM, consulte Importar certificados en la Guía del usuario de AWS Certificate Manager. Para obtener más información sobre la carga de certificados en IAM, consulte Uso de certificados de servidor en la Guía del usuario de IAM.

Certificado predeterminado

Al crear un agente de escucha HTTPS, debe especificar exactamente un certificado. Este certificado se conoce como certificado predeterminado.

Si especifica certificados adicionales en una lista de certificados (p. 39), el certificado predeterminado se utiliza solo si un cliente se conecta sin utilizar el protocolo de indicación de nombre de servidor (SNI) para especificar un nombre de host o si no hay certificados coincidentes en la lista de certificados.

Si no especifica certificados adicionales pero tiene que alojar varias aplicaciones seguras a través de un único balanceador de carga, puede utilizar un certificado comodín o añadir un nombre alternativo de asunto (SAN) para cada dominio adicional al certificado.

Lista de certificados

Después de crear un agente de escucha HTTPS, tiene un certificado predeterminado y una lista de certificados vacía. Opcionalmente puede añadir certificados a la lista de certificados para el agente de escucha. El uso de una lista de certificados permite al balanceador de carga admitir varios dominios en el mismo puerto y proporcionar un certificado diferente para cada dominio.

El balanceador de carga utiliza un algoritmo de selección de certificados inteligentes compatible con SNI. Si el nombre de host proporcionado por un cliente coincide con un único certificado en la lista de certificados, el balanceador de carga selecciona este certificado. Si un nombre de host proporcionado por un cliente coincide con varios certificados de la lista de certificados, el balanceador de carga selecciona el mejor certificado que el cliente puede admitir. La selección de certificados se basa en los siguientes criterios en este orden:

- Algoritmo de clave pública (prefieren ECDSA frente a RSA)
- Algoritmo de hash (prefieren SHA frente a MD5)
- Longitud de clave (prefieren la mayor)
- Periodo de validez

Las entradas del registro de acceso del balanceador de carga indican el nombre de host especificado por el cliente y el certificado presentado al cliente. Para obtener más información, consulte Entradas de los logs de acceso (p. 93).

Renovación de certificados

Cada certificado viene con un periodo de validez. Debe asegurarse de renovar o reemplazar cada certificado para su balanceador de carga antes de que finalice su período de validez. Esto incluye el certificado predeterminado y los certificados en una lista de certificados. La renovación o reemplazo de un certificado no afecta a las solicitudes en tránsito que ha recibido el nodo del balanceador de carga y que están pendiente de ser direccionadas a un destino con un estado correcto. Una vez que se ha renovado un certificado, las nuevas solicitudes utilizan el certificado renovado. Una vez que se ha sustituido un certificado, las nuevas solicitudes utilizan el nuevo certificado.

Puede administrar la renovación y la sustitución de certificados de la siguiente manera:

- Los certificados proporcionados por AWS Certificate Manager e implementados en el balanceador de carga se pueden renovar automáticamente. ACM intenta renovar los certificados antes de que expiren. Para obtener más información, consulte Renovación administrada en la Guía del usuario de AWS Certificate Manager.

- Si el certificado se importó en ACM, deberá supervisar la fecha de vencimiento del certificado y renovarlo antes de que venza. Para obtener más información, consulte Importar certificados en la Guía del usuario de AWS Certificate Manager.
- Si importa un certificado en IAM, debe crear un nuevo certificado, importar el nuevo certificado en ACM o IAM, añadir el nuevo certificado al balanceador de carga y eliminar el certificado caducado del balanceador de carga.

Políticas de seguridad

Elastic Load Balancing utiliza una configuración de negociación de Capa de conexión segura (SSL), lo que se conoce como política de seguridad para negociar las conexiones SSL entre un cliente y el balanceador de carga. Una política de seguridad es una combinación de protocolos y cifrados. El protocolo establece una conexión segura entre un cliente y un servidor, y garantiza que todos los datos transferidos entre el cliente y el balanceador de carga son privados. Un cifrado es un algoritmo de cifrado que usa claves de cifrado para crear un mensaje codificado. Los protocolos usan diversos cifrados para cifrar los datos a través de Internet. Durante el proceso de negociación de conexiones, el cliente y el balanceador de carga presentan una lista con los cifrados y protocolos que admite cada uno por orden de preferencia. De forma predeterminada, el primer cifrado que se va a seleccionar para la conexión segura será el primero de la lista del servidor que coincida con uno de los cifrados del cliente.

Los Application Load Balancers no admiten la renegociación de SSL para conexiones de cliente o de destino.

Puede elegir la política de seguridad que se va a utilizar con las conexiones frontend. La política de seguridad `ELBSecurityPolicy-2016-08` siempre se utiliza con las conexiones backend. Los Application Load Balancers no admiten políticas de seguridad personalizadas.

Elastic Load Balancing dispone de las siguientes políticas de seguridad para los Application Load Balancers:

- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-FS-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2015-05`
- `ELBSecurityPolicy-TLS-1-0-2015-04`

Le recomendamos que utilice la política `ELBSecurityPolicy-2016-08` de forma general. Puede utilizar la política `ELBSecurityPolicy-FS-2018-06` si necesita Forward Secrecy (FS). Puede utilizar una de las políticas `ELBSecurityPolicy-TLS` para ajustarse a los estándares de seguridad y conformidad que requieren que se deshabiliten algunas versiones del protocolo TLS o para admitir clientes heredados que utilicen cifrados en desuso. Solo un pequeño porcentaje de clientes de Internet necesitan la versión 1.0 de TLS. Para ver la versión del protocolo TLS para las solicitudes dirigidas al balanceador de carga, habilite el registro de acceso del balanceador de carga y examine los registros de acceso. Para obtener más información, consulte Access Logs (p. 91).

En la siguiente tabla se describen las políticas de seguridad definidas para los Application Load Balancers.

Política de seguridad	2016-08 *	FS-2018-0	TLS-1-2	TLS-1-2-Ext	TLS-1-1	TLS-1-0 †
Protocolos TLS						

Política de seguridad	2016-08 *	FS-2018-0	TLS-1-2	TLS-1-2-Ext	TLS-1-1	TLS-1-0 †
Protocolo-TLSv1	♦	♦				♦
Protocolo-TLSv1.1	♦	♦			♦	♦
Protocolo-TLSv1.2	♦	♦	♦	♦	♦	♦
Cifrados TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-RSA-AES128-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦
ECDHE-RSA-AES256-SHA	♦	♦		♦	♦	♦
ECDHE-ECDSA-AES256-SHA	♦	♦		♦	♦	♦
AES128-GCM-SHA256	♦		♦	♦	♦	♦
AES128-SHA256	♦		♦	♦	♦	♦
AES128-SHA	♦			♦	♦	♦
AES256-GCM-SHA384	♦		♦	♦	♦	♦
AES256-SHA256	♦		♦	♦	♦	♦
AES256-SHA	♦			♦	♦	♦
DES-CBC3-SHA						♦

* Las políticas de seguridad `ELBSecurityPolicy-2016-08` y `ELBSecurityPolicy-2015-05` para los Application Load Balancers son idénticas.

† No utilice esta política de seguridad a menos que deba admitir un cliente heredado que requiera el cifrado DES-CBC3-SHA, que es un cifrado muy débil.

Para ver la configuración de las políticas de seguridad de los Application Load Balancers a través de la AWS CLI, utilice el comando describe-ssl-policies.

Agregar un agente de escucha HTTPS

Los agentes de escucha se configuran con un protocolo y un puerto para las conexiones entre los clientes y el balanceador de carga, así como un grupo de destino para la regla predeterminada del agente de escucha. Para obtener más información, consulte Configuración del agente de escucha (p. 28).

Requisitos previos

- Para añadir una acción de reenvío a la regla predeterminada del agente de escucha, debe especificar un grupo de destino disponible. Para obtener más información, consulte Creación de un grupo de destino (p. 62).
- Para crear un agente de escucha HTTPS, debe especificar un certificado y una política de seguridad. El balanceador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de direccionarlas a los destinos. El balanceador de carga utiliza la política de seguridad para negociar conexiones SSL con los clientes.

Para agregar un agente de escucha HTTPS mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (EQUILIBRIO DE CARGA), elija Load Balancers (Balanceadores de carga).
3. Seleccione un balanceador de carga y elija Listeners (Agentes de escucha), Add listener (Añadir agente de escucha).
4. En Protocol : port (Protocolo: puerto), elija HTTPS y mantenga el puerto predeterminado o introduzca un puerto distinto.
5. (Opcional) Para autenticar a los usuarios, en Default actions (Acciones predeterminadas), elija Add action (Añadir acción), Authenticate (Autenticar) y proporcione la información solicitada. Para guardar la acción, seleccione el icono de marca de verificación. Para obtener más información, consulte Autenticar a usuarios usando un Balanceador de carga de aplicaciones (p. 49).
6. En Default actions (Acciones predeterminadas), realice una de las operaciones siguientes:
   - Seleccione Add action (Añadir acción), Forward to (Reenviar a) y un grupo de destino.
   - Seleccione Add action (Añadir acción), Redirect to (Redirigir a) y proporcione una URL para la acción de redirección. Para obtener más información, consulte Acciones de redirección (p. 31).
   - Seleccione Add action (Añadir acción), Return fixed response (Devolver respuesta fija) y proporcione un código de respuesta y un cuerpo opcional para la respuesta. Para obtener más información, consulte Acciones de respuesta fija (p. 30).

   Para guardar la acción, seleccione el icono de marca de verificación.
7. Para Security policy (Política de seguridad), le recomendamos que mantenga la política de seguridad predeterminada.
8. En Default SSL certificate (Certificado SSL predeterminado), realice una de las operaciones siguientes:
   - Si ha creado o importado un certificado mediante AWS Certificate Manager, elija From ACM (Desde ACM) y elija el certificado.
   - Si ha cargado un certificado mediante IAM, elija From IAM (Desde IAM) y elija el certificado.
9. Seleccione Save.
10. (Opcional) Para definir reglas adicionales del agente de escucha que reenvíen las solicitudes en función de un patrón de ruta o un nombre de host, consulte Agregar una regla (p. 43).
11. (Opcional) Para añadir una lista de certificados que utilizar con el protocolo SNI, consulte Añadir certificados a la lista de certificados (p. 48).

Agregar un agente de escucha HTTPS mediante la AWS CLI

Utilice el comando create-listener para crear el agente de escucha y la regla predeterminada, y el comando create-rule para definir nuevas reglas del agente de escucha.

Actualizar un agente de escucha HTTPS

Después de crear un agente de escucha HTTPS, puede reemplazar el certificado predeterminado, actualizar la lista de certificados o reemplazar la política de seguridad. Para obtener más información, consulte Actualizar un agente de escucha HTTPS para el balanceador de carga de aplicaciones (p. 47).

Reglas del agente de escucha del balanceador de carga de aplicaciones

Las reglas que se definen para el agente de escucha determinan cómo el balanceador de carga va a direccionar las solicitudes a los destinos de uno o varios grupos de destino.

Cada regla consta de una prioridad, una o varias acciones y una o varias condiciones. Para obtener más información, consulte Reglas del agente de escucha (p. 29).

> Note
>
> En la consola, aparece un número de secuencia relativo para cada regla, pero no la prioridad. Para obtener la prioridad de una regla, tiene que describirla utilizando la AWS CLI o la API de Elastic Load Balancing.

Requisitos

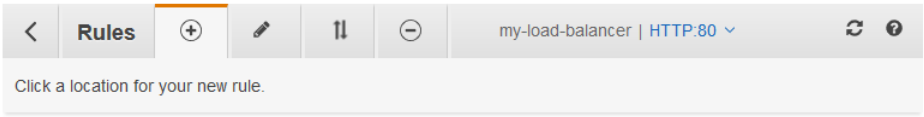
- Cada regla debe incluir exactamente una de las acciones siguientes: `forward`, `redirect` o `fixed-response` y debe ser la última acción que realizar.
- Cada regla puede incluir cero o una de las condiciones siguientes: `host-header`, `http-request-method`, `path-pattern` y `source-ip` y cero o más de las condiciones siguientes: `http-header` y `query-string`.
- Puede especificar hasta tres cadenas de comparación por condición y hasta cinco por regla.
- Una acción `forward` direcciona las solicitudes a su grupo de destino. Antes de añadir una acción `forward`, cree el grupo de destino y añada destinos al mismo. Para obtener más información, consulte Creación de un grupo de destino (p. 62).

Agregar una regla

Siempre que se crea un agente de escucha, se crea una regla predeterminada. Puede definir otras reglas no predeterminadas en cualquier momento.

Para agregar una regla a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. En el agente de escucha que desea actualizar, seleccione View/edit rules.
5. Elija el Add rules icono (signo más) de la barra de menús, lo que agregará Insert Rule el icono en los lugares en los que se puede insertar una regla por orden de prioridad.



6. Elija uno de los iconos Insert Rule (Insertar regla) añadidos en el paso anterior.
7. Añada una o varias condiciones como se indica a continuación:

   a. Para añadir una condición de encabezado de host, elija Add condition (Agregar condición), Host header (Encabezado de host) e introduzca el nombre de host (por ejemplo, **`*.example.com`**). Para guardar la condición, elija el icono de marca de verificación.

      El tamaño máximo de cada cadena es de 128 caracteres. Esta comparación no distingue entre mayúsculas y minúsculas. Se admiten los siguientes caracteres comodín: * y ?.

   b. Para añadir una condición de ruta, elija Add condition (Agregar condición), Path (Ruta) e introduzca el patrón de ruta (por ejemplo, `/img/*`). Para guardar la condición, elija el icono de marca de verificación.

      El tamaño máximo de cada cadena es de 128 caracteres. Esta comparación distingue entre mayúsculas y minúsculas. Se admiten los siguientes caracteres comodín: * y ?.

   c. Para añadir una condición de encabezado HTTP, elija Add condition (Agregar condición), Http header (Encabezado HTTP). Escriba el nombre del encabezado y añada una o varias cadenas de comparación. Para guardar la condición, elija el icono de marca de verificación.

      El tamaño máximo de cada nombre de encabezado es de 40 caracteres, el nombre del encabezado no distingue entre mayúsculas y minúsculas, no se admiten comodines. El tamaño máximo de cada cadena de comparación es de 128 caracteres y se admiten los siguientes caracteres comodín: * y ?. Esta comparación no distingue entre mayúsculas y minúsculas.

   d. Para añadir una condición de método de solicitud HTTP, elija Add condition (Agregar condición), HTTP request method (Método de solicitud HTTP) y añada uno o varios nombres de método. Para guardar la condición, elija el icono de marca de verificación.

      El tamaño máximo de cada nombre es de 40 caracteres. Los caracteres permitidos incluyen A–Z, guion (-) y guion bajo (_). La comparación distingue entre mayúsculas y minúsculas. No se admite el uso de comodines.

   e. Para añadir una condición de cadena de consulta, elija Add condition (Añadir condición), Query string (Cadena de consulta) y añada uno o varios de los pares de clave/valor. Para cada par de clave/valor, puede omitir la clave y especificar solo el valor. Para guardar la condición, elija el icono de marca de verificación.

      El tamaño máximo de cada cadena es de 128 caracteres. Esta comparación no distingue entre mayúsculas y minúsculas. Se admiten los siguientes caracteres comodín: * y ?.

   f. Para añadir una condición de IP de origen, elija Add condition (Agregar condición), Source IP (IP de origen) y añada uno o varios bloques de CIDR. Para guardar la condición, elija el icono de marca de verificación.

      Puede utilizar tanto direcciones IPv4 como IPv6. No se admite el uso de comodines.

8. (Opcional, agente de escucha HTTPS) Para autenticar a los usuarios, elija Add action (Añadir acción), Authenticate (Autenticar) y proporcione la información solicitada. Para guardar la acción, seleccione el icono de marca de verificación. Para obtener más información, consulte Autenticar a usuarios usando un Balanceador de carga de aplicaciones (p. 49).
9. Añada una de las siguientes acciones:
   - Para añadir una acción de reenvío, elija Add action (Añadir acción), Forward to (Reenviar a) y elija un grupo de destino. Para guardar la acción, seleccione el icono de marca de verificación.
   - Para añadir una acción de redirección, seleccione Add action (Añadir acción), Redirect to (Redirigir a) y proporcione una URL para la acción de redirección. Para guardar la acción,

seleccione el icono de marca de verificación. Para obtener más información, consulte Acciones de redirección (p. 31).

- Para añadir una acción de respuesta fija, seleccione Add action (Añadir acción), Return fixed response (Devolver respuesta fija) y proporcione un código de respuesta y un cuerpo opcional para la respuesta. Para guardar la acción, seleccione el icono de marca de verificación. Para obtener más información, consulte Acciones de respuesta fija (p. 30).

10. Seleccione Save.
11. (Opcional) Para cambiar el orden de la regla, utilice las flechas y, a continuación, elija Save (Guardar). La regla predeterminada siempre tiene la prioridad last (último).
12. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para agregar una regla a través de AWS CLI

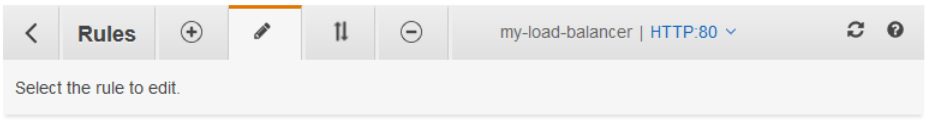
Utilice el comando create-rule para crear la regla. Utilice el comando describe-rules para ver información sobre la regla.

Editar una regla

Puede editar la acción y las condiciones de una regla en cualquier momento.

Para editar una regla a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. En el agente de escucha que desea actualizar, seleccione View/edit rules.
5. Seleccione el icono Edit rules (con forma de lápiz) de la barra de menús.



6. En la regla que desea editar, seleccione el icono Edit rules (con forma de lápiz).
7. (Opcional) Modifique las condiciones y las acciones según sea necesario. Por ejemplo, puede editar una condición o una acción (icono de lápiz), añadir una condición, añadir una acción de autenticación para una regla de un agente de escucha HTTPS o eliminar una condición o acción (icono de papelera). No puede añadir condiciones a la regla predeterminada.

8. Elija Update.
9. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para editar una regla a través de AWS CLI

Utilice el comando modify-rule.

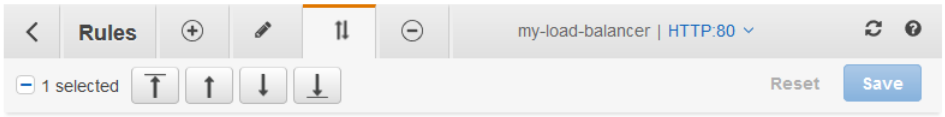
Reorganizar las reglas

Las normas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar. Puede cambiar la prioridad de una regla no predeterminada en cualquier momento. No puede cambiar la prioridad de la regla predeterminada.

> Note
>
> En la consola, aparece un número de secuencia relativo para cada regla, pero no la prioridad. Al reorganizar las reglas a través de la consola, se les asigna una nueva prioridad en función de la prioridad existente. Para establecer la prioridad de una regla en un valor específico, utilice AWS CLI o la API de Elastic Load Balancing.

Para reorganizar las reglas a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. En el agente de escucha que desea actualizar, seleccione View/edit rules.
5. Seleccione el icono Recorder rules (las flechas) de la barra de menú.



6. Active la casilla que aparece junto a la regla y utilice las flechas para asignarle una nueva prioridad. La regla predeterminada siempre tiene la última prioridad.
7. Cuando haya terminado de reorganizar las reglas, seleccione Save.
8. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para actualizar las prioridades de las reglas a través de AWS CLI

Utilice el comando set-rule-priorities.

Eliminar una regla

Puede eliminar las reglas no predeterminadas para un agente de escucha en cualquier momento. No puede eliminar la regla predeterminada de un agente de escucha. Cuando se elimina un agente de escucha, se eliminan todas sus reglas.

Para eliminar una regla a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. En el agente de escucha que desea actualizar, seleccione View/edit rules.
5. Seleccione el icono Delete rules (Eliminar reglas) (con forma de signo menos) de la barra de menús.
6. Active la casilla de la regla y elija Delete (Eliminar). No puede eliminar la regla predeterminada del agente de escucha.
7. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para eliminar una regla a través de AWS CLI

Utilice el comando delete-rule.

Actualizar un agente de escucha HTTPS para el balanceador de carga de aplicaciones

Después de crear un agente de escucha HTTPS, puede reemplazar el certificado predeterminado, actualizar la lista de certificados o reemplazar la política de seguridad.

Limitación

ACM admite certificados RSA con una longitud de clave de 4096 bists y certificados EC. Sin embargo, no puede instalar estos certificados en el balanceador de carga a través de la integración con ACM. Debe cargar estos certificados en IAM para utilizarlos con el balanceador de carga.

Tareas

- Reemplazar el certificado predeterminado (p. 47)
- Añadir certificados a la lista de certificados (p. 48)
- Quitar certificados de la lista de certificados (p. 49)
- Actualizar la política de seguridad (p. 49)

Reemplazar el certificado predeterminado

Puede reemplazar el certificado predeterminado para su agente de escucha utilizando el siguiente procedimiento. Para obtener más información, consulte Certificados SSL (p. 38).

Para cambiar el certificado predeterminado utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.

3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. Active la casilla del agente de escucha y seleccione Edit (Editar).
5. En Default SSL certificate (Certificado SSL predeterminado), realice una de las operaciones siguientes:
   - Si ha creado o importado un certificado mediante AWS Certificate Manager, elija From ACM (Desde ACM) y elija el certificado.
   - Si ha cargado un certificado mediante IAM, elija From IAM (Desde IAM) y elija el certificado.
6. Seleccione Save.

Para cambiar el certificado predeterminado utilizando la AWS CLI

Utilice el comando modify-listener.

Añadir certificados a la lista de certificados

Puede añadir certificados a la lista de certificados para su agente de escucha utilizando el siguiente procedimiento. Al crear por primera vez un agente de escucha HTTPS, la lista de certificados está vacía. Puede añadir uno o varios certificados. Como opción, añada el certificado predeterminado para asegurarse de que este certificado se utilice con el protocolo SNI incluso si se reemplaza como certificado predeterminado. Para obtener más información, consulte Certificados SSL (p. 38).

Para añadir certificados a la lista de certificados utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (EQUILIBRIO DE CARGA), elija Load Balancers (Balanceadores de carga).
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. Para que el agente de escucha HTTPS se actualice, elija View/edit certificates (Ver/editar certificados), que muestra el certificado predeterminado seguido de cualquier otro certificado que haya añadido al agente de escucha.
5. Elija el icono Add certificates (Añadir certificados) (el signo más) en la barra de menús, que muestra el certificado predeterminado seguido por otros certificados administrados por ACM y IAM. Si ya ha añadido un certificado al agente de escucha, su casilla está seleccionada y deshabilitada.
6. Para añadir certificados que ya administra ACM o IAM, seleccione las casillas de los certificados y elija Add (Añadir).
7. Si tiene un certificado que no administra ACM ni IAM, impórtelo a ACM y añádalo a su agente de escucha de la siguiente manera:
   a. Seleccione Import certificate.
   b. En Certificate private key, pegue la clave privada codificada en PEM y sin cifrar para el certificado.
   c. En Certificate body, pegue el certificado codificado en PEM.
   d. (Opcional) En Certificate chain, pegue la cadena de certificados codificada en PEM.
   e. Elija Import. El certificado que acaba de importar aparece en la lista de certificados disponibles y está seleccionado.
   f. Elija Add.
8. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para añadir un certificado a la lista de certificados utilizando la AWS CLI

Utilice el comando add-listener-certificates.

Quitar certificados de la lista de certificados

Puede quitar certificados de la lista de certificados para su agente de escucha HTTPS utilizando el siguiente procedimiento. Para quitar el certificado predeterminado para un agente de escucha HTTPS, consulte Reemplazar el certificado predeterminado (p. 47).

Para quitar certificados de la lista de certificados utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (EQUILIBRIO DE CARGA), elija Load Balancers (Balanceadores de carga).
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. Para que el agente de escucha se actualice, elija View/edit certificates (Ver/editar certificados), que muestra el certificado predeterminado seguido de cualquier otro certificado que haya añadido al agente de escucha.
5. Elija el icono Remove certificates (el signo menos) en la barra de menús.
6. Active la casillas de los certificados y elija Remove (Eliminar).
7. Para salir de esta pantalla, seleccione el icono Back to the load balancer (Volver al balanceador de carga) (botón Atrás) de la barra de menú.

Para eliminar un certificado de la lista de certificados utilizando la AWS CLI

Utilice el comando remove-listener-certificates.

Actualizar la política de seguridad

Cuando crea un agente de escucha HTTPS, puede seleccionar la política de seguridad que mejor se ajuste a sus necesidades. Cuando se agrega una nueva política de seguridad, se puede actualizar el agente de escucha HTTPS para que la utilice. Los Application Load Balancers no admiten políticas de seguridad personalizadas. Para obtener más información, consulte Políticas de seguridad (p. 40).

Para actualizar la política de seguridad a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. Active la casilla del agente de escucha HTTPS y seleccione Edit (Editar).
5. En Security policy (Política de seguridad), seleccione una política de seguridad.
6. Elija Update.

Para actualizar la política de seguridad a través de AWS CLI

Utilice el comando modify-listener.

Autenticar a usuarios usando un Balanceador de carga de aplicaciones

Puede configurar un Balanceador de carga de aplicaciones para autenticar de forma segura a los usuarios cuando obtienen acceso a sus aplicaciones. Esto le permite liberar a su balanceador de carga del trabajo de autenticación de usuarios para que sus aplicaciones puedan centrarse en su lógica de negocio.

Se admiten los siguientes casos de uso:

- Autenticar a los usuarios a través de un proveedor de identidad (IdP) compatible con OpenID Connect (OIDC).
- Autenticar a los usuarios a través de IdP sociales conocidos, como Amazon, Facebook o Google, a través de los grupos de usuarios que admite Amazon Cognito.
- Autenticar a los usuarios mediante identidades corporativas, usando SAML, LDAP o Microsoft AD, a través de grupos de usuarios que admite Amazon Cognito.

Preparativos para usar un IdP compatible con OIDC

Haga lo siguiente si utiliza un IdP compatible con OIDC con su Balanceador de carga de aplicaciones:

- Cree una nueva aplicación OIDC en su IdP. Debe configurar un ID de cliente y un secreto de cliente.
- Obtenga los siguientes puntos de enlace publicados por el IdP: autorización, token e información de usuario. Puede localizar esta información en la configuración conocida.
- Incluya en la lista blanca una de las siguientes URL de redirección en su aplicación de IdP, sea cual sea la que utilicen sus usuarios, donde DNS es el nombre de dominio del balanceador de carga y CNAME es el alias DNS de su aplicación:
  - https://*DNS*/oauth2/idpresponse
  - https://*CNAME*/oauth2/idpresponse

Preparativos para usar Amazon Cognito

Haga lo siguiente si utiliza grupos de usuarios de Amazon Cognito con su Balanceador de carga de aplicaciones:

- Cree un grupo de usuarios. Para obtener más información, consulte Grupos de usuarios de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.
- Cree un cliente de grupo de usuarios. Debe configurar el cliente para que genere un secreto de cliente, utilice el flujo de concesión de código y admita los mismos ámbitos de OAuth que utiliza el balanceador de carga. Para obtener más información, consulte Configuración de un cliente de aplicación de grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.
- Cree un dominio de grupo de usuarios. Para obtener más información, consulte Agregar un nombre de dominio para el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.
- Compruebe que el ámbito solicitado devuelve un token de ID. Por ejemplo, el ámbito predeterminado, `openid`, devuelve un token de ID pero el ámbito `aws.cognito.signin.user.admin` no.
- Para federarse con un IdP social o corporativo, habilite el IdP en la sección de federación. Para obtener más información, consulte Añadir inicio de sesión de redes sociales a un grupo de usuarios o Añadir inicio de sesión con un IdP SAML a un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.
- Incluya en la lista blanca las siguientes URL de redirección en el campo de URL de devolución de llamada para Amazon Cognito, donde DNS es el nombre de dominio del balanceador de carga y CNAME es el alias DNS de su aplicación (si utiliza uno):
  - https://*DNS*/oauth2/idpresponse
  - https://*CNAME*/oauth2/idpresponse
- Incluya en la lista blanca el dominio del grupo de usuarios en la URL de devolución de llamada de la aplicación de IdP. Utilice el formato de su IdP. Por ejemplo:
  - https://*domain-prefix*.auth.*region*.amazoncognito.com/saml2/idpresponse
  - https://*dominio-de-grupo-de-usuarios*/oauth2/idpresponse

Para permitir que un usuario de IAM pueda configurar un balanceador de carga para usar Amazon Cognito con el fin de autenticar a los usuarios, debe conceder al usuario el permiso para llamar a la acción `cognito-idp:DescribeUserPoolClient`.

Preparativos para usar Amazon CloudFront

Habilite la siguiente configuración si utiliza una distribución de CloudFront delante de su Balanceador de carga de aplicaciones:

- Reenviar encabezados de solicitud (todos): garantiza que CloudFront no almacene en caché respuestas para solicitudes autenticadas. Esto evita que se sirvan desde la caché después de que venza la sesión de autenticación. Como opción, para reducir este riesgo mientras el almacenamiento en caché está habilitado, los propietarios de una distribución CloudFront pueden establecer que el valor de tiempo de vida (TTL) venza antes de que venza la cookie de autenticación.
- Reenvío y almacenamiento en caché de cadenas de consulta (todo): garantiza que el balanceador de carga tiene acceso a los parámetros de cadena de consulta requeridos para autenticar al usuario con el IdP.
- Reenvío de cookies (todo): garantiza que CloudFront reenvíe todas las cookies de autenticación al balanceador de carga.

Configuración de la autenticación de usuarios

La autenticación de usuario se configura creando una acción de autenticación para una o varias reglas de agente de escucha. Los tipos de acción `authenticate-cognito` y `authenticate-oidc` solo se admiten con agentes de escucha HTTPS. Para conocer la descripción de los campos correspondientes, consulte AuthenticateCognitoActionConfig y AuthenticateOidcActionConfig en la Referencia de la API de Elastic Load Balancing versión 2015-12-01.

De forma predeterminada, el campo `SessionTimeout` está configurado en 7 días. Si desea sesiones más cortas, puede configurar un tiempo de espera de sesión de tan solo 1 segundo. Para obtener más información, consulte Cierre de sesión de autenticación y tiempo de espera de sesión (p. 55).

Establezca el campo `OnUnauthenticatedRequest` como apropiado para su aplicación. Por ejemplo:

- Aplicaciones que requieren que el usuario inicie sesión usando una identidad social o corporativa — Se admite mediante la opción predeterminada `authenticate`. Si el usuario no ha iniciado sesión, el balanceador de carga redirige la solicitud al punto de enlace de autorización de IdP y el IdP le pide al usuario que inicie sesión utilizando su interfaz de usuario.
- Aplicaciones que proporcionan una vista personalizada a un usuario que ha iniciado sesión o una vista general a un usuario que no ha iniciado sesión — Para admitir este tipo de aplicaciones, utilice la opción `allow`. Si el usuario ha iniciado sesión, el balanceador de carga proporciona las notificaciones de usuario y la aplicación puede ofrecer una vista personalizada. Si el usuario no ha iniciado sesión, el balanceador de carga reenvía la solicitud sin las notificaciones de usuario y la aplicación puede proporcionar la vista general.
- Aplicaciones de una sola página con JavaScript que se cargan cada pocos segundos — De forma predeterminada, después de que venza la cookie de sesión de autenticación, las llamadas AJAX se redirigen al IdP y se bloquean. Si utiliza la opción `deny`, el balanceador de carga devuelve un error HTTP 401 No autorizado a estas llamadas AJAX.

El balanceador de carga debe poder comunicarse con el punto de enlace de token de IdP (`TokenEndpoint`) y el punto de enlace de información de usuario de IdP (`UserInfoEndpoint`). Verifique que los grupos de seguridad de su balanceador de carga y las ACL de red de su VPC permiten el acceso saliente a estos puntos de enlace. Compruebe que la VPC tiene acceso a Internet. Si hay un

balanceador de carga interno, utilice una gateway NAT para permitirle que obtenga acceso a estos puntos de enlace.

Utilice el siguiente comando create-rule para configurar la autenticación de usuario.

```
aws elbv2 create-rule --listener-arn listener-arn --priority 10 \
--conditions Field=path-pattern,Values="/login" --actions file://actions.json
```

El siguiente es un ejemplo del archivo `actions.json` que especifica las acciones `authenticate-oidc` y `forward`.

```
[{
    "Type": "authenticate-oidc",
    "AuthenticateOidcConfig": {
        "Issuer": "https://idp-issuer.com",
        "AuthorizationEndpoint": "https://authorization-endpoint.com",
        "TokenEndpoint": "https://token-endpoint.com",
        "UserInfoEndpoint": "https://user-info-endpoint.com",
        "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "ClientSecret": "12345678901234567890123456789O",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

El siguiente es un ejemplo del archivo `actions.json` que especifica las acciones `authenticate-cognito` y `forward`.

```
[{
    "Type": "authenticate-cognito",
    "AuthenticateCognitoConfig": {
        "UserPoolArn": "arn:aws:cognito-idp:region-code:account-id:userpool/user-pool-id",
        "UserPoolClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "UserPoolDomain": "userPoolDomain1",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
```

```
    "Order": 2
}]
```

Para obtener más información, consulte Reglas del agente de escucha (p. 29).

Flujo de autenticación

Elastic Load Balancing utiliza el flujo de código de autorización de OIDC, que incluye los siguientes pasos.

1. Cuando se cumplen las condiciones de una regla con una acción de autenticación, el balanceador de carga comprueba si hay una cookie de sesión de autenticación en los encabezados de solicitudes. Si la cookie no está presente, el balanceador de carga redirige al usuario al punto de enlace de autorización de IdP para que el IdP pueda autenticarlo.
2. Después de autenticar al usuario, el IdP lo redirige al balanceador de carga con un código de concesión de autorización. El balanceador de carga presenta el código al punto de enlace del token de IdP para obtener el token de ID y el token de acceso.
3. Después de que el balanceador de carga valida el token de ID, intercambia el token de acceso con el punto de enlace de información de usuario de IdP para obtener las notificaciones de usuario.
4. El balanceador de carga crea la cookie de sesión de autenticación y la envía al cliente para que el agente de usuario del cliente pueda enviarla al balanceador de carga cuando realice las solicitudes. Debido a que la mayoría de los navegadores limitan una cookie a 4 KB de tamaño, el balanceador de carga fragmenta una cookie de más de 4 KB en varias cookies. Si el tamaño total de las notificaciones de usuario y el token de acceso recibido del IdP es superior a 11 KB, el balanceador de carga devuelve un error HTTP 500 al cliente y aumenta la métrica `ELBAuthUserClaimsSizeExceeded`.
5. El balanceador de carga envía las notificaciones de usuario al destino en las cabeceras HTTP. Para obtener más información, consulte Codificación de las notificaciones de usuario y verificación de firmas (p. 53).
6. Si el IdP proporciona un token de actualización válido en el token de ID, el balanceador de carga lo guarda y lo utiliza para actualizar las notificaciones de usuario cada vez que venza el token de acceso, hasta que se agote la sesión o hasta que se produzca un error en la actualización del IdP. Si el usuario cierra la sesión, se produce un error en la actualización y el balanceador de carga redirige al usuario al punto de enlace de autorización de IdP. De este modo, el balanceador de carga puede dejar de funcionar después de que el usuario cierre la sesión. Para obtener más información, consulte Cierre de sesión de autenticación y tiempo de espera de sesión (p. 55).

Codificación de las notificaciones de usuario y verificación de firmas

Después de que el balanceador de carga autentica a un usuario correctamente, envía las notificaciones de usuario recibidas del IdP al destino. El balanceador de carga firma la notificación de usuario para que las aplicaciones puedan verificar la firma y comprobar que el balanceador de carga ha enviado las notificaciones.

El balanceador de carga añade los siguientes encabezados HTTP:

`x-amzn-oidc-accesstoken`

El token de acceso del punto de enlace de token, en texto sin formato.

`x-amzn-oidc-identity`

El campo del asunto (`sub`) del punto de enlace de información de usuario, en texto sin formato.

`x-amzn-oidc-data`

Las notificaciones de usuario, en formato de tokens web de JSON (JWT).

Las aplicaciones que requieren las notificaciones de usuario completas pueden utilizar cualquier biblioteca JWT estándar para verificar los tokens de JWT. Estos tokens siguen el formato JWT, pero no son tokens de ID. El formato JWT incluye un encabezado, una carga y una firma que tienen codificación de URL en base64 e incluyen caracteres de relleno al final. La firma de JWT es ECDSA + P-256 + SHA256.

El encabezado JWT es un objeto JSON con los siguientes campos:

```
{
   "alg": "algorithm",
   "kid": "12345678-1234-1234-1234-123456789012",
   "signer": "arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/app/load-
balancer-name/load-balancer-id",
   "iss": "url",
   "client": "client-id",
   "exp": "expiration"
}
```

La carga de JWT es un objeto JSON que contiene las notificaciones de usuarios recibidas del punto de enlace de información de usuario de IdP.

```
{
   "sub": "1234567890",
   "name": "name",
   "email": "alias@example.com",
   ...
}
```

Dado que el balanceador de carga no cifra las notificaciones de usuario, le recomendamos que configure el grupo de destino para que utilice HTTPS. Si configura el grupo de destino para que utilice HTTP, asegúrese de restringir el tráfico a su balanceador de carga mediante grupos de seguridad. También le recomendamos que verifique la firma antes de realizar cualquier autorización basada en las notificaciones. Para obtener la clave pública, obtenga el ID de clave del encabezado JWT y utilícelo para buscar la clave pública desde el siguiente punto de enlace regional:

```
https://public-keys.auth.elb.region.amazonaws.com/key-id
```

Para la región AWS GovCloud (EE.UU. Oeste), el punto de enlace es el siguiente:

```
https://s3-us-gov-west-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-west-1/key-id
```

Para la región AWS GovCloud (EE.UU. Este), el punto de enlace es el siguiente:

```
https://s3-us-gov-east-1.amazonaws.com/aws-elb-public-keys-prod-us-gov-east-1/key-id
```

El siguiente ejemplo muestra cómo obtener la clave pública en Python 3.x:

```
import jwt
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-oidc-data']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
```

```
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from regional endpoint
url = 'https://public-keys.auth.elb.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES256'])
```

El siguiente ejemplo muestra cómo obtener la clave pública en Python 2.7:

```
import jwt
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-oidc-data']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from regional endpoint
url = 'https://public-keys.auth.elb.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES256'])
```

Cierre de sesión de autenticación y tiempo de espera de sesión

Cuando una aplicación necesita cerrar la sesión de un usuario autenticado, debe establecer el tiempo de vencimiento de la cookie de sesión de autenticación en -1 y redirigir al cliente al punto de enlace de cierre de sesión de IdP (si el IdP admite uno). Para evitar que los usuarios reutilicen una cookie eliminada, le recomendamos que configure un tiempo de vencimiento del token de acceso tan breve como sea razonable. Si un cliente proporciona a un balanceador de carga una cookie de sesión de autorización que tiene un token de acceso vencido con un token de actualización NULL, el balanceador de carga se pone en contacto con el IdP para determinar si el usuario aún tiene iniciada la sesión.

El token de actualización y el tiempo de espera de la sesión funcionan juntos de la siguiente manera:

- Si el tiempo de espera de la sesión es menor que el vencimiento del token de acceso, el balanceador de carga respeta el tiempo de espera de la sesión y vuelve a iniciar la sesión del usuario después de que se haya agotado el tiempo de espera de la sesión de autenticación.
- Si el tiempo de espera de la sesión es mayor que el vencimiento del token de acceso y el IdP no admite tokens de actualización, el balanceador de carga mantiene la sesión de autenticación hasta que se agota el tiempo de espera y, a continuación, vuelve a iniciar la sesión del usuario.
- Si el tiempo de espera de la sesión es mayor que el vencimiento del token de acceso y el IdP admite tokens de actualización, el balanceador de carga actualiza la sesión de usuario cada vez que vence el token de acceso. El balanceador de carga vuelve a iniciar la sesión del usuario solo después de que se agote el tiempo de la sesión de autenticación o se produzca un error en el flujo de actualización.

Eliminar un agente de escucha de Application Load Balancer

Puede eliminar un agente de escucha en cualquier momento. Cuando se elimina un balanceador de carga, se eliminan todos sus agentes de escucha.

Para eliminar un agente de escucha a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Load Balancers.
3. Seleccione el balanceador de carga y, a continuación, elija Listeners.
4. Active la casilla del agente de escucha HTTPS y seleccione Delete (Eliminar).
5. Cuando se le indique que confirme, seleccione Yes, Delete.

Para eliminar un agente de escucha a través de AWS CLI

Utilice el comando delete-listener.

Grupos de destino para los Application Load Balancers

Cada grupo de destino se utiliza para direccionar solicitudes a uno o varios destinos registrados. Cuando se crea la regla de cada agente de escucha, se especifican un grupo de destino y las condiciones. Cuando se cumple la condición de una regla, el tráfico se reenvía al grupo de destino correspondiente. Puede crear grupos de destino diferentes para los distintos tipos de solicitudes. Por ejemplo, puede crear un grupo de destino para las solicitudes generales y otros grupos de destino para las solicitudes destinadas a los microservicios de la aplicación. Para obtener más información, consulte Componentes de Balanceador de carga de aplicaciones (p. 1).

Puede definir la configuración de comprobación de estado del balanceador de carga para cada grupo de destino. Cada grupo de destino utiliza la configuración de comprobación de estado predeterminada, a menos que la anule al crear el grupo de destino o la modifique posteriormente. Después de especificar un grupo de destino en una regla para un agente de escucha, el balanceador de carga monitoriza constantemente el estado de todos los destinos registrados en el grupo de destino que se encuentran en una zona de disponibilidad habilitada para el balanceador de carga. El balanceador de carga direcciona las solicitudes a los destinos registrados que se encuentran en buen estado.

Contenido

Configuración de direccionamiento

De forma predeterminada, un balanceador de carga direcciona las solicitudes a sus destinos mediante el protocolo y el número de puerto especificados al crear el grupo de destino. Si lo prefiere, puede anular el puerto utilizado para direccionar el tráfico a un destino al registrarlo en el grupo de destino.

Los grupos de destino admiten los siguientes protocolos y puertos:

- Protocols: HTTP, HTTPS

- Ports: 1-65535

Si un grupo de destino se configura con el protocolo HTTPS o utiliza comprobaciones de estado HTTPS, las conexiones SSL a los destinos utilizarán la configuración de seguridad de la política `ELBSecurityPolicy2016-08`.

Tipo de destino

Al crear un grupo de destino, debe especificar su tipo de destino, que determina el tipo de destino que especifica al registrar los destinos en este grupo de destino. Después de crear un grupo de destino, no puede cambiar su tipo de destino.

Los tipos de destinos posibles son los siguientes:

`instance`

Los destinos se especifican por ID de instancia.

`ip`

Los destinos son direcciones IP.

`lambda`

El destino es una función Lambda.

Cuando el tipo de destino es `ip`, puede especificar direcciones IP de uno de los siguientes bloques de CIDR:

- Las subredes de la VPC para el grupo de destino
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Estos bloques de CIDR compatibles le permiten registrar lo siguiente con un grupo de destino: instancias de ClassicLink, instancias en una VPC interconectada, recursos de AWS direccionables por dirección IP y puerto (por ejemplo, bases de datos) y recursos on-premise vinculados a AWS a través de AWS Direct Connect o una conexión de VPN.

Important

No puede especificar direcciones IP direccionables públicamente.

Si especifica destinos utilizando un ID de instancia, el tráfico se redirige a las instancias utilizando la dirección IP privada principal especificada en la interfaz de red principal de la instancia. Si especifica destinos utilizando direcciones IP, puede dirigir el tráfico a una instancia utilizando cualquier dirección IP privada de una o varias interfaces de red. Esto permite que varias aplicaciones de una instancia utilicen el mismo puerto. Cada interfaz de red puede tener su propio grupo de seguridad.

Si el tipo de destino de su grupo de destino es `lambda`, puede registrar una única función Lambda. Cuando el balanceador de carga recibe una solicitud para la función Lambda, invoca la función Lambda. Para obtener más información, consulte Funciones Lambda como destinos (p. 71).

Destinos registrados

El balanceador de carga sirve como un único punto de contacto para los clientes y distribuye el tráfico entrante entre los destinos registrados en buen estado. Puede registrar cada destino en uno o varios grupos de destino. Puede registrar cada instancia EC2 o dirección IP en el mismo grupo de destino varias veces con diferentes puertos, lo que permite que el balanceador de carga direccione las solicitudes a microservicios.

Si aumenta la demanda en la aplicación, puede registrar más destinos en uno o varios grupos para controlar la demanda. El balanceador de carga comienza a direccionar las solicitudes a un destino recién registrado tan pronto como se completa el proceso de registro y el destino supera las comprobaciones de estado iniciales.

Si la demanda de la aplicación se reduce o cuando es preciso realizar el mantenimiento de los destinos, anular el registro de los destinos en los grupos de destino. Al anular el registro de un destino, este se quita del grupo de destino pero no se ve afectado de ningún otro modo. El balanceador de carga deja de direccionar solicitudes a un destino tan pronto como se anula su registro. El destino adquiere el estado `draining` hasta que se completan las solicitudes en tránsito. Puede volver a registrar el destino en el grupo de destino cuando esté preparado para reanudar la recepción de solicitudes.

Si está registrando destinos por ID de instancia, puede utilizar el balanceador de carga con un grupo de Auto Scaling. Después de asociar un grupo de destino a un grupo de Auto Scaling, Auto Scaling registra los destinos en el grupo de destino cuando los lanza. Para obtener más información, consulte Asociar un balanceador de carga a su grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Límites

- No puede registrar las direcciones IP de otro Balanceador de carga de aplicaciones en la misma VPC. Si el otro Balanceador de carga de aplicaciones está en una VPC interconectada, puede registrar sus direcciones IP.

Atributos del grupo de destino

Los siguientes atributos del grupo de destino se admiten si el tipo de grupo de destino es `instance` o `ip`:

`deregistration_delay.timeout_seconds`

Cantidad de tiempo que Elastic Load Balancing espera antes de anular el registro de un destino. El rango va de 0 a 3600 segundos. El valor de predeterminado es de 300 segundos.

`slow_start.duration_seconds`

El periodo de tiempo, en segundos, durante el cual el balanceador de carga envía al grupo de destino recién registrado una cuota linealmente mayor del tráfico. El rango va de 30 a 900 segundos (15 minutos). El valor predeterminado es 0 segundos (deshabilitado).

`stickiness.enabled`

Indica si están habilitadas las sesiones sticky.

`stickiness.lb_cookie.duration_seconds`

Periodo de vencimiento de las cookies, en segundos. Una vez transcurrido este periodo, la cookie se considera antigua. El valor mínimo es de 1 segundo y el máximo es de 7 días (604800 segundos). El valor predeterminado es de 1 día (86400 segundos).

`stickiness.type`

Tipo de persistencia. El valor posible es `lb_cookie`.

El siguiente atributo del grupo de destino se admite si el tipo de grupo de destino es `lambda`:

`lambda.multi_value_headers.enabled`

Indica si los encabezados de solicitud y respuesta intercambiados entre el balanceador de carga y la función Lambda incluyen matrices de valores o cadenas. Los valores posibles son `true` o `false`. El valor predeterminado es `false`. Para obtener más información, consulte Encabezados de varios valores (p. 74).

Retardo de anulación del registro

Elastic Load Balancing deja de enviar solicitudes a los destinos que están en proceso de anulación del registro. De forma predeterminada, Elastic Load Balancing espera 300 segundos antes de completar el proceso de anulación del registro, para ayudar a que se completen las solicitudes en tránsito hacia el destino. Para cambiar la cantidad de tiempo que Elastic Load Balancing espera, actualice el valor del retardo de anulación de registro.

El estado inicial de un destino en proceso de anulación del registro es `draining`. Una vez transcurrido el retardo de anulación del registro, el proceso de anulación del registro se completa y el estado del destino es `unused`. Si el destino forma parte de un grupo de Auto Scaling, pueden terminarse y sustituirse.

Si un destino que anula el registro no tiene ninguna solicitud en tránsito y ninguna conexión activa, Elastic Load Balancing completa inmediatamente el proceso de anulación de registro, sin esperar a que transcurra el retardo de anulación de registro. Sin embargo, aunque se haya completado el proceso de anulación del registro del destino, se mostrará el estado del destino como `draining` hasta que transcurra el tiempo de anulación de registro.

Si un destino en proceso de anulación del registro termina la conexión antes de que haya transcurrido el retardo de anulación del registro, el cliente recibe una respuesta de error de nivel 500.

Para actualizar el valor del retardo de anulación del registro desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Seleccione el grupo de destino. El valor actual se muestra en la pestaña Description (Descripción) como Deregistration delay (Retardo de anulación del registro).
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit attributes, cambie el valor de Deregistration delay según sea necesario y, a continuación, seleccione Save.

Para actualizar el valor del retardo de anulación del registro desde la AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `deregistration_delay.timeout_seconds`.

Modo de inicio lento

De forma predeterminada, un destino comienza a recibir su cuota completa de solicitudes tan pronto como se registra con un grupo de destino y pasa una comprobación de estado inicial. Usar el modo de inicio lento proporciona a los destinos tiempo para calentarse antes de que el balanceador de carga les envíe una cuota completa de solicitudes. Después de habilitar el arranque lento para un grupo de destino, los

objetivos entran en modo de inicio lento cuando se registran con el grupo de destino y salen del modo de inicio lento cuando pasa el periodo de duración de inicio lento configurado. El balanceador de carga aumenta linealmente el número de solicitudes que puede enviar a un destino en modo de inicio lento. Una vez que sale del modo de inicio lento, el balanceador de carga puede enviarle una cuota completa de solicitudes.

Consideraciones

- Al habilitar el inicio lento para un grupo de destino, los destinos ya registrados con el grupo de destino no entran en el modo de inicio lento.
- Al habilitar el inicio lento para un grupo de destino vacío y, a continuación, registrar uno o varios destinos mediante una operación de registro único, estos destinos no entran en el modo de inicio lento. Los destinos recién registrados entran en el modo de inicio lento solo cuando hay al menos un destino registrado que no está en modo de inicio lento.
- Si anula el registro de un destino en modo de inicio lento, el destino sale del modo de inicio lento. Si registra de nuevo el mismo destino, entra en modo de inicio lento de nuevo.
- Si un destino en modo de inicio lento tiene un estado incorrecto y, a continuación, vuelve a encontrarse en buen estado antes de que pase el periodo de duración, el destino permanece en modo de inicio lento y sale del modo de inicio lento cuando se agota el resto del periodo de duración. Si un destino que no se encuentra en modo de inicio lento cambia de incorrecto a correcto, no entra en el modo de inicio lento.

Para actualizar el valor de duración de inicio lento con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Seleccione el grupo de destino. El valor actual se muestra en la pestaña Description (Descripción) como Slow start duration (Duración de inicio lento).
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit attributes (Editar atributos), cambie el valor de Slow start duration (Duración de inicio lento) según sea necesario y, a continuación, seleccione Save (Guardar). Para deshabilitar el modo de inicio lento, establezca la duración en 0.

Para actualizar el valor de duración de inicio lento con AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `slow_start.duration_seconds`.

Sesiones sticky

Las sesiones sticky son un mecanismo para direccionar las solicitudes al mismo destino en un grupo de destino. Resulta útil para los servidores que mantienen información de estado, para ofrecer una experiencia de continuidad a los clientes. Para utilizar las sesiones sticky, los clientes deben admitir las cookies.

Cuando un balanceador de carga recibe una solicitud de un cliente por primera vez, la direcciona a un destino y genera una cookie que se incluye en la respuesta al cliente. La próxima solicitud de ese cliente contiene la cookie. Si las sesiones sticky están habilitadas para el grupo de destino y la solicitud se dirige al mismo grupo de destino, el balanceador de carga detecta la cookie y direcciona la solicitud al mismo destino.

Los Application Load Balancers admiten únicamente las cookies generadas por el balanceador de carga. El nombre de la cookie es AWSALB. El contenido de estas cookies se cifra mediante una clave rotativa. Las cookies generadas por el balanceador de carga no se pueden descifrar ni modificar.

Las conexiones de WebSockets son sticky de forma inherente. Si el cliente solicita una actualización de la conexión a WebSockets, el destino que devuelve un código de estado HTTP 101 para aceptar la actualización de la conexión es el destino que se usa en la conexión de WebSockets. Una vez que se ha completado la actualización de WebSockets, la persistencia basada en cookies no se utiliza.

Las sesiones sticky se habilitan para grupos de destino. También puede establecer la duración, en segundos, de la persistencia de la cookie generada por el balanceador de carga. La duración se establece con cada solicitud. Por lo tanto, si el cliente envía una solicitud antes de cada duración caduca, el período de sesión continúa.

Application Load Balancers utiliza el atributo Expires del encabezado de la cookie en lugar del encabezado Max-Age.

Para habilitar las sesiones sticky desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Seleccione el grupo de destino.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit attributes, lleve a cabo alguna de las siguientes operaciones:
   a. Seleccione Enable load balancer generated cookie stickines.
   b. Para Stickiness duration, especifique un valor comprendido entre 1 segundo y 7 días.
   c. Seleccione Save.

Para habilitar las sesiones sticky desde la AWS CLI

Utilice el comando modify-target-group-attributes con los atributos `stickiness.enabled` y `stickiness.lb_cookie.duration_seconds`.

Creación de un grupo de destino

Los destinos se registran en un grupo de destino. De forma predeterminada, el balanceador de carga envía las solicitudes a los destinos registrados mediante el protocolo y el puerto que ha especificado para el grupo de destino. Puede anular este puerto al registrar cada destino en el grupo de destino.

Una vez creado un grupo de destino, puede agregarle etiquetas.

Para direccionar el tráfico a los destinos de un grupo de destino, especifique el grupo de destino en una acción al crear un agente de escucha o crear una regla para este último. Para obtener más información, consulte Reglas del agente de escucha (p. 29).

Puede agregar o quitar destinos del grupo de destino en cualquier momento. Para obtener más información, consulte Registro de destinos en el grupo de destino (p. 67). También puede modificar la configuración de la comprobación de estado del grupo de destino. Para obtener más información, consulte Modificación de la configuración de comprobación de estado de un grupo de destino (p. 67).

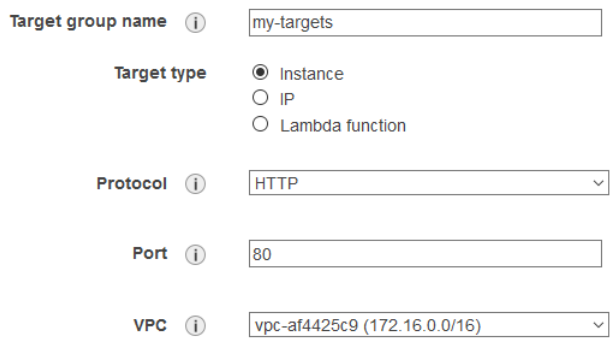
Para crear un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Elija Create target group.
4. En Target group name, escriba el nombre del nuevo grupo de destino.

5. En Target type (Tipo de destino), seleccione Instance (Instancia) para registrar los destinos por ID de instancia, IP para registrar direcciones IP y Lambda function (Función Lambda) para registrar una función Lambda.
6. Si el tipo de destino es Instance (Instancia) o IP, haga lo siguiente:

   a. (Opcional) En Protocol y Port, modifique los valores predeterminados según sea necesario.

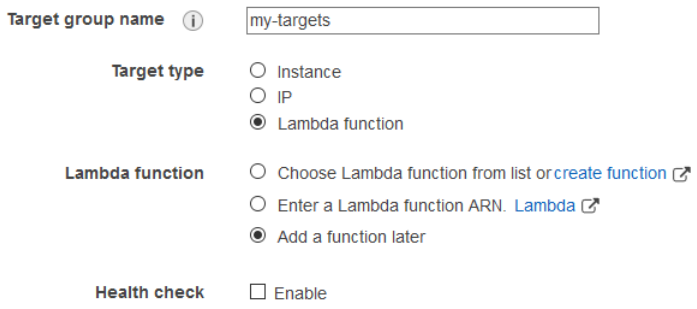
   b. En VPC, seleccione una nube virtual privada (VPC).



7. Si el tipo de destino es Lambda function (Función Lambda), haga lo siguiente:

   a. En Lambda function (Función Lambda), realice alguna de las siguientes operaciones:
      - Seleccione la función Lambda
      - Cree una nueva función Lambda y selecciónela
      - Registre la función Lambda después de crear el grupo de destino

   b. (Opcional) Para habilitar las comprobaciones, elija Health check (Comprobación de estado), Enable (Habilitar).



8. (Opcional) En Health check settings y Advanced health check settings, modificar la configuración predeterminada según sea necesario.
9. Seleccione Create.
10. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:

    a. Seleccione el grupo de destino que se acaba de crear.

    b. En la pestaña Tags, elija Add/Edit Tags.

    c. En la página Add/Edit Tags, para cada etiqueta que agregue, elija Create Tag y, a continuación, especifique la clave y el valor de la etiqueta. Cuando haya terminado de agregar etiquetas, elija Save.

11. (Opcional) Para agregar destinos al grupo de destino, consulte Registro de destinos en el grupo de destino (p. 67).

Para crear un grupo de destino desde la AWS CLI

Utilice el comando create-target-group para crear el grupo de destino, el comando add-tags para etiquetar el grupo de destino y el comando register-targets para agregar destinos.

Comprobaciones de estado de los grupos de destino

El Balanceador de carga de aplicaciones envía periódicamente solicitudes a los destinos registrados para comprobar su estado. Estas pruebas se denominan comprobaciones de estado.

Cada nodo del balanceador de carga direcciona las solicitudes únicamente a los destinos en buen estado de las zonas de disponibilidad habilitadas para el balanceador de carga. Cada nodo del balanceador de carga comprueba el estado de cada destino; para ello, utiliza la configuración de comprobación de estado de los grupos de destino en los que está registrado el destino. Una vez que el destino está registrado, debe superar una comprobación de estado para que se considere que se encuentra en buen estado. Después de completar cada comprobación de estado, el nodo del balanceador de carga cierra la conexión se estableció para la comprobación de estado.

Si un grupo de destino contiene únicamente destinos registrados que no están en buen estado, los nodos del balanceador de carga dirigen las solicitudes a estos destinos.

Las comprobaciones de estado no admiten WebSockets.

Configuración de comprobación de estado

Puede utilizar los siguientes ajustes para configurar las comprobaciones de estado de los destinos de un grupo de destino. El balanceador de carga envía una solicitud de comprobación de estado a cada destino registrado cada vez que transcurren los segundos que indica HealthCheckIntervalSeconds, utilizando el protocolo, el puerto y la ruta de ping especificados. Cada solicitud de comprobación de estado es independiente y dura todo el intervalo. El tiempo que tarda el destino en responder no afecta al intervalo de la siguiente solicitud de comprobación de estado. Si las comprobaciones de estado superan el umbral de UnhealthyThresholdCount errores consecutivos, el balanceador de carga inhabilita el destino. Cuando las comprobaciones de estado superan el umbral de HealthyThresholdCount éxitos consecutivos, el balanceador de carga vuelve a poner el destino en servicio.

Opción	Descripción
HealthCheckProtocol	Protocolo que el balanceador de carga utiliza al realizar comprobaciones de estado en los destinos. Los posibles protocolos son HTTP y HTTPS. El valor predeterminado es el protocolo HTTP.
HealthCheckPort	Puerto que el balanceador de carga utiliza al realizar comprobaciones de estado en los destinos. El valor predeterminado es el puerto en el que cada destino recibe el tráfico procedente del balanceador de carga.
HealthCheckPath	Ruta de ping que es el destino para los destinos en las comprobaciones de estado. Especifique una URI válida (/path?query). El valor predeterminado es /.

Opción	Descripción
HealthCheckTimeoutSeconds	Si durante este tiempo, en segundos, no se recibe ninguna respuesta de un destino, se considerará que la comprobación de estado no se ha superado. El rango va de 2 a 60 segundos. El valor predeterminado es de 5 segundos.
HealthCheckIntervalSeconds	Cantidad aproximada de tiempo, en segundos, que transcurre entre comprobaciones de estado de un destino individual. El rango va de 5 a 300 segundos. El valor predeterminado es de 30 segundos.
HealthyThresholdCount	Número de comprobaciones de estado consecutivas que deben superarse para considerar que un destino en mal estado vuelve a estar en buen estado. El rango va de 2 a 10. El valor predeterminado es 5.
UnhealthyThresholdCount	Número de comprobaciones de estado consecutivas no superadas que se requieren para considerar que un destino se encuentra en mal estado. El rango va de 2 a 10. El valor predeterminado es 2.
Matcher	Códigos HTTP que se deben utilizar al comprobar si se ha recibido una respuesta correcta de un destino. Puede especificar valores o rangos de valores comprendidos entre 200 y 499. El valor predeterminado es 200.

Estado del destino

Antes de que el balanceador de carga envíe a un destino una solicitud de comprobación de estado, debe registrarlo en un grupo de destino, especificar su grupo de destino en una regla del agente de escucha y asegurarse de que la zona de disponibilidad del destino esté habilitada en el balanceador de carga. Para que un destino pueda recibir solicitudes desde el balanceador de carga, debe superar las comprobaciones de estado iniciales. Una vez que ha superado estas comprobaciones de estado iniciales, su estado es `Healthy`.

En la siguiente tabla se describen los valores posibles del estado de un destino registrado.

Valor	Descripción
`initial`	El balanceador de carga se encuentra en proceso de registrar el destino o de realizar las comprobaciones de estado iniciales en el destino.
`healthy`	El destino se encuentra en buen estado.
`unhealthy`	El destino no respondió a una comprobación de estado o no la ha superado.
`unused`	El destino no está registrada en un grupo de destino, el grupo de destino no se utiliza en una regla del agente de

Valor	Descripción
	escucha del balanceador de carga o el destino se encuentra en una zona de disponibilidad que no está habilitada para el balanceador de carga.
`draining`	El destino está en proceso de anulación del registro y de vaciado de conexiones.

Códigos de motivo de comprobación de estado

Si el estado de un destino es un valor distinto de `Healthy`, el API devuelve un código de motivo y una descripción del problema. Además, la consola muestra la misma descripción en una información sobre herramientas. Los códigos de motivo que comienzan por `Elb` tienen su origen en el balanceador de carga y que los códigos de motivo que comienzan por `Target` tienen su origen en el destino.

Código de motivo	Descripción
`Elb.InitialHealthChecking`	Las comprobaciones de estado iniciales están en curso.
`Elb.InternalError`	Las comprobaciones de estado no se han superado debido a un error interno.
`Elb.RegistrationInProgress`	El registro del destino está en curso.
`Target.DeregistrationInProgress`	La anulación del registro del destino está en curso.
`Target.FailedHealthChecks`	Las comprobaciones de estado no se han superado.
`Target.InvalidState`	El destino se encuentra en estado detenido. El destino se encuentra en estado terminado. El destino se encuentra en estado terminado o detenido. El destino se encuentra en un estado no válido.
`Target.IpUnusable`	La dirección IP no se puede utilizar como destino, ya que la utiliza un equilibrador de carga.
`Target.NotInUse`	El grupo de destino no se ha configurado para recibir el tráfico del balanceador de carga. El destino se encuentra en una zona de disponibilidad que no está habilitada para el balanceador de carga.
`Target.NotRegistered`	El destino no está registrado en el grupo de destino.
`Target.ResponseCodeMismatch`	Las comprobaciones de estado no se han superado y se han emitido estos códigos: [código]
`Target.Timeout`	Se agotó el tiempo de espera de la solicitud.

Comprobación del estado de los destinos

Puede comprobar el estado de los destinos registrados en los grupos de destino.

Para comprobar el estado de los destinos desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Seleccione el grupo de destino.
4. En la pestaña Targets la Status columna indica el estado de cada destino.
5. Si el estado es cualquier valor distinto de `Healthy`, consulte la información sobre herramientas para obtener más información.

Para comprobar el estado de los destinos desde la AWS CLI

Utilice el comando describe-target-health. El resultado de este comando contiene el estado del destino. Si el estado es cualquier valor distinto de `Healthy`, la salida también incluye un código de motivo.

Modificación de la configuración de comprobación de estado de un grupo de destino

Puede modificar la configuración de comprobación de estado del grupo de destino en cualquier momento.

Para modificar la configuración de comprobación de estado de un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING, elija Target Groups.
3. Seleccione el grupo de destino.
4. En la pestaña Health check, elija Edit.
5. En la página Edit target group, modifique la configuración según sea necesario y, a continuación, elija Save.

Para modificar la configuración de comprobación de estado de un grupo de destino desde la AWS CLI

Utilice el comando modify-target-group.

Registro de destinos en el grupo de destino

Los destinos se registran en un grupo de destino. Al crear un grupo de destino, debe especificar su tipo de destino, que determina cómo se registran sus destinos. Por ejemplo, puede registrar ID de instancia, direcciones IP o funciones Lambda. Para obtener más información, consulte Grupos de destino para los Application Load Balancers (p. 57).

Si la demanda aumenta en los destinos registrados actualmente, puede registrar más para controlar esa demanda. Cuando el destino esté preparado para controlar solicitudes, regístrelo en el grupo de destino. El balanceador de carga comienza a direccionar las solicitudes al destino tan pronto como se completa el proceso de registro y el destino supera las comprobaciones de estado iniciales.

Si la demanda baja en los destinos registrados o cuando es preciso realizar tareas de mantenimiento en un destino, puede anular su registro en el grupo de destino. El balanceador de carga deja de direccionar solicitudes a un destino tan pronto como se anula su registro. Cuando el destino esté preparado para recibir solicitudes, puede registrarlo en el grupo de destino nuevo.

Cuando se anula el registro de un destino, el balanceador de carga espera hasta que se han completado las solicitudes en tránsito. Esto se denomina vaciado de conexiones. El estado de un destino es `draining` mientras se está efectuando el vaciado de conexiones.

Al anular el registro de un objetivo que se ha registrado por dirección IP, debe esperar a que se complete el retardo de anulación de registro antes de poder registrar la misma dirección IP de nuevo.

Si está registrando destinos por ID de instancia, puede utilizar el balanceador de carga con un grupo de Auto Scaling. Después de asociar un grupo de destino a un grupo de Auto Scaling y cuando el grupo se escale para ampliarlo, las instancias lanzadas por el grupo de Auto Scaling se registran automáticamente en el grupo de destino. Si separa el grupo de destino del grupo de Auto Scaling, automáticamente se anula el registro de las instancias en el grupo de destino. Para obtener más información, consulte Asociar un balanceador de carga a su grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Grupos de seguridad de destino

Cuando se registran instancias EC2 como destinos, es preciso asegurarse de que los grupos de seguridad de las instancias permitan que el balanceador de carga se comunique con ellas en el puerto del agente de escucha y en el puerto de comprobación de estado.

Reglas recomendadas

Inbound		
Source	Port Range	Comment
grupo de seguridad de balanceador de carga	*agente de escucha de instancia*	Permite el tráfico del balanceador de carga en el puerto del agente de escucha de la instancia
grupo de seguridad de balanceador de carga	*comprobación de estado*	Permite el tráfico procedente del balanceador de carga en el puerto de comprobación de estado.

También recomendamos permitir el tráfico ICMP entrante para admitir la detección de MTU de ruta. Para obtener más información, consulte Detección de la MTU de la ruta en la Guía del usuario de Amazon EC2 para instancias de Linux.

Registro o anulación de destinos

El tipo de destino de su grupo de destino determina cómo se registran los destinos en ese grupo de destino. Para obtener más información, consulte Tipo de destino (p. 58).

Contenido

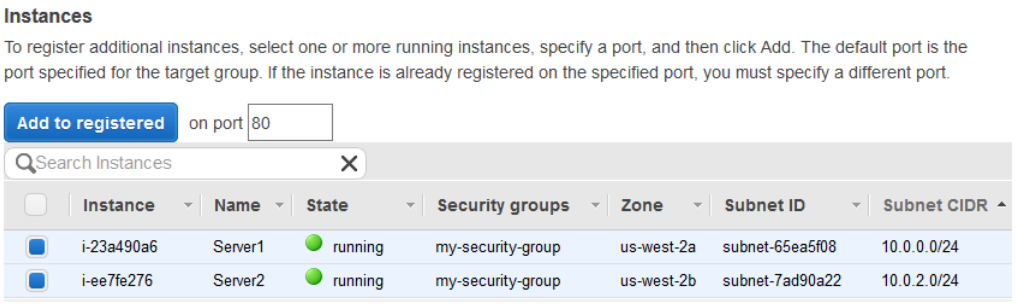
Registro o anulación del registro de destinos por ID de instancia

La instancia debe encontrarse en la nube virtual privada (VPC) que ha especificado para el grupo de destino. La instancia debe estar además en el estado `running` al registrarla.

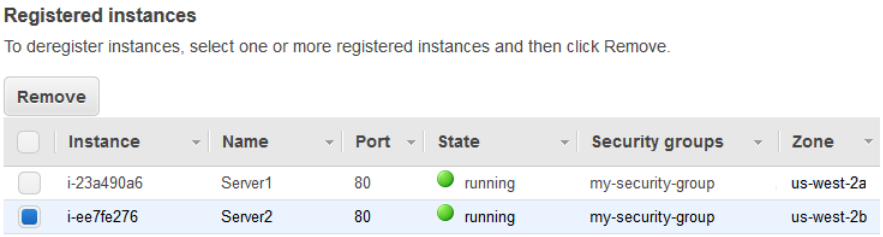
Para registrar o anular el registro de destinos por ID de instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.
4. En la pestaña Targets, seleccione Edit.
5. Para registrar instancias, selecciónelas desde Instances, modifique el puerto de instancia predeterminado según sea necesario y, a continuación, elija Add to registered.



6. Para anular el registro de instancias, selecciónelas en Registered instances y elija Remove.



7. Seleccione Save.

Registro o anulación del registro de destinos por dirección IP

Las direcciones IP que registre deben estar en uno de los siguientes bloques de CIDR:

- Las subredes de la VPC para el grupo de destino
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

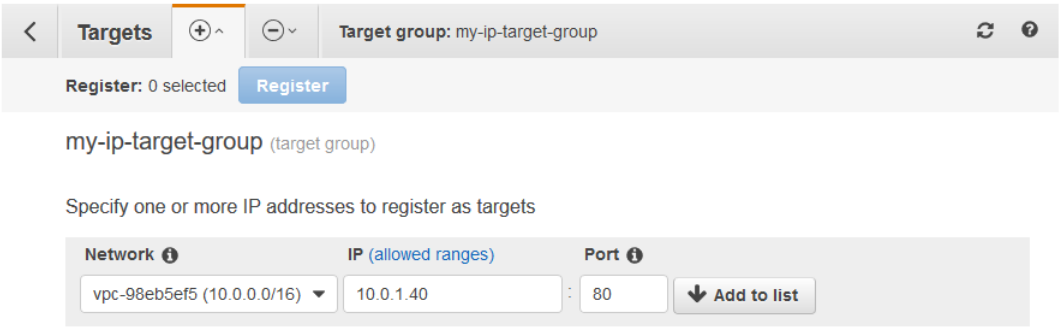
Límites

- No puede registrar las direcciones IP de otro Balanceador de carga de aplicaciones en la misma VPC. Si el otro Balanceador de carga de aplicaciones está en una VPC interconectada, puede registrar sus direcciones IP.

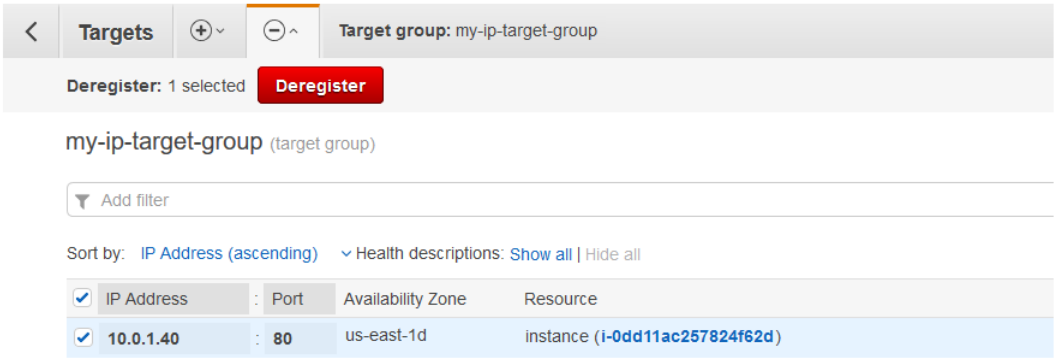
Para registrar o anular el registro de destinos por dirección IP

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.

4. En la pestaña Targets, seleccione Edit.
5. Para registrar direcciones IP, elija el icono de Register targets (el signo más) en la barra de menús. Para cada dirección IP, seleccione la red, escriba la dirección IP y el puerto y elija Add to list (Añadir a la lista). Cuando haya terminado de especificar direcciones, elija Register.



6. Para anular el registro de direcciones IP, elija el icono de Deregister targets (el signo menos) en la barra de menús. Si ha registrado muchas direcciones IP, puede que le resulte útil agregar un filtro o cambiar el orden. Seleccione las direcciones IP y, a continuación, elija Deregister.



7. Para salir de esta pantalla, elija el icono de Back to target group (Volver a grupo de destino) (botón Atrás) de la barra de menús.

Registrar o anular el registro de una función Lambda

Puede registrar una única función Lambda con cada grupo de destino. Elastic Load Balancing debe tener permisos para invocar la función Lambda. Si ya no necesita enviar tráfico a la función Lambda, puede anular su registro. Después de anular el registro de una función Lambda, las solicitudes en tránsito producirán errores HTTP 5XX. Para sustituir una función Lambda, lo mejor es que cree un nuevo grupo de destino en su lugar. Para obtener más información, consulte Funciones Lambda como destinos (p. 71).

Para registrar o anular el registro de una función Lambda

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino y elija la pestaña Targets (Destinos).
4. Si no hay ninguna función Lambda registrada, elija Register (Registrar). Seleccione la función Lambda y elija Register (Registrar).
5. Para anular el registro de una función Lambda, elija Deregister (Anular registro) Cuando se le pida que confirme, elija Deregister (Anular el registro).

Registrar o anular el registro de destinos utilizando la AWS CLI

Utilice el comando register-targets para agregar destinos y el comando deregister-targets para quitarlos.

Funciones Lambda como destinos

Puede registrar sus funciones Lambda como destinos y configurar una regla del agente de escucha para reenviar las solicitudes al grupo de destino de la función Lambda. Cuando el balanceador de carga reenvía la solicitud a un grupo de destino con una función Lambda como destino, invoca la función Lambda y pasa el contenido de la solicitud a la función Lambda, en formato JSON.

Límites

- La función Lambda y el grupo de destino deben estar en la misma cuenta.
- El tamaño máximo del cuerpo de la solicitud que puede enviar a una función Lambda es de 1 MB. Para ver límites de tamaño relacionados, consulte Límites de los encabezados HTTP.
- El tamaño máximo del JSON de respuesta que la función Lambda puede enviar es de 1 MB.
- No se admiten los sockets web. Las solicitudes de actualización se rechazan con el código HTTP 400.

Contenido

Preparar la función Lambda

Se aplican las recomendaciones siguientes si está utilizando su función Lambda con un Balanceador de carga de aplicaciones.

Permisos para invocar la función Lambda

Si crea el grupo de destino y registra la función Lambda utilizando la Consola de administración de AWS, la consola añade los permisos necesarios a la política de su función Lambda en su nombre. De lo contrario, después de crear el grupo de destino y registrar la función utilizando la AWS CLI, debe utilizar el comando add-permission para conceder a Elastic Load Balancing permiso para invocar la función Lambda. Le recomendamos que incluya el parámetro `--source-arn` para restringir la invocación de la función al grupo de destino especificado.

```
aws lambda add-permission \
--function-name lambda-function-arn-with-alias-name \
--statement-id elb1 \
--principal elasticloadbalancing.amazonaws.com \
--action lambda:InvokeFunction \
--source-arn target-group-arn
```

Control de versiones de funciones Lambda

Puede registrar una sola función Lambda por grupo de destino. Para asegurarse de que puede cambiar la función Lambda y de que el balanceador de carga siempre invoque la versión actual de la función Lambda, cree un alias de función e incluya el alias en el ARN de la función cuando registre la función Lambda en el balanceador de carga. Para obtener más información, consulte Control de versiones y alias de las funciones AWS Lambda y Cambio de tráfico mediante alias en la AWS Lambda Developer Guide.

Tiempo de espera de la función

El balanceador de carga espera hasta que la función Lambda responde o se agota el tiempo de espera. Le recomendamos que configure el tiempo de espera de la función Lambda en función del tiempo de ejecución previsto. Para obtener información acerca del valor de tiempo de espera predeterminado y cómo cambiarlo, consulte Configuración básica de funciones AWS Lambda. Para obtener información acerca del valor máximo de tiempo de espera que puede configurar, consulte Límites de AWS Lambda.

Creación de un grupo de destino para la función Lambda

Cree el grupo de destino que se va a utilizar para el direccionamiento de solicitudes. Si el contenido de la solicitud coincide con una regla del agente de escucha con una acción para reenviarlo a este grupo de destino, el balanceador de carga invoca la función Lambda registrada.

Para crear un grupo de destino y registrar la función Lambda

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Elija Create target group.
4. En Target group name, escriba el nombre del nuevo grupo de destino.
5. En Target type (Tipo de destino), seleccione Lambda function (Función Lambda).
6. En Lambda function (Función Lambda), realice alguna de las siguientes operaciones:
   - Seleccione la función Lambda
   - Cree una nueva función Lambda y selecciónela
   - Registre la función Lambda después de crear el grupo de destino
7. (Opcional) Para habilitar las comprobaciones, elija Health check (Comprobación de estado), Enable (Habilitar).
8. Seleccione Create.

Para crear un grupo de destino y anular el registro de la función Lambda mediante la AWS CLI

Use los comandos create-target-group y register-targets.

Recibir eventos del balanceador de carga

El balanceador de carga admite la invocación Lambda de solicitudes a través de HTTP y HTTPS. El balanceador de carga envía un evento en formato JSON. El balanceador de carga añade los siguientes encabezados a cada solicitud: `X-Amzn-Trace-Id`, `X-Forwarded-For`, `X-Forwarded-Port` y `X-Forwarded-Proto`.

Si el tipo de contenido es uno de los siguientes tipos, el balanceador de carga envía el cuerpo a la función Lambda tal como está y establece `isBase64Encoded` en `false`: text/*, application/json, application/javascript y application/xml. Para todos los demás tipos, el balanceador de carga codifica en Base64 el cuerpo y establece `isBase64Encoded` en `true`.

El siguiente es un evento de ejemplo.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
    "path": "/",
    "queryStringParameters": {parameters},
    "headers": {
        "accept": "text/html,application/xhtml+xml",
        "accept-language": "en-US,en;q=0.8",
        "content-type": "text/plain",
        "cookie": "cookies",
        "host": "lambda-846800462-us-east-2.elb.amazonaws.com",
        "user-agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)",
        "x-amzn-trace-id": "Root=1-5bdb40ca-556d8b0c50dc66f0511bf520",
        "x-forwarded-for": "72.21.198.66",
        "x-forwarded-port": "443",
        "x-forwarded-proto": "https"
    },
    "isBase64Encoded": false,
    "body": "request_body"
}
```

Responder al balanceador de carga

La respuesta de la función Lambda debe incluir el estado de codificación en Base64, el código de estado, la descripción del estado y los encabezados. Puede omitir el cuerpo. El encabezado `statusDescription` debe contener el código de estado y la frase del motivo, separados por un único espacio.

Para incluir contenido binario en el cuerpo de la respuesta, debe codificar en Base64 el contenido y establecer `isBase64Encoded` en `true`. El balanceador de carga descodifica el contenido para recuperar el contenido binario y lo envía al cliente en el cuerpo de la respuesta HTTP.

El balanceador de carga no admite los encabezados de saltos, como `Connection` o `Transfer-Encoding`. Puede omitir el encabezado `Content-Length` porque el balanceador de carga lo procesa antes de enviar las respuestas a los clientes.

A continuación, se muestra un ejemplo de la respuesta de una función Lambda.

```
{
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

Para conocer las plantillas de la función Lambda que funcionan con Application Load Balancers, consulte application-load-balancer-serverless-app en github. También puede abrir la consola de Lambda , crear una función y seleccionar una de las siguientes opciones de AWS Serverless Application Repository:

- ALB-Lambda-Target-HelloWorld
- ALB-Lambda-Target-UploadFiletoS3
- ALB-Lambda-Target-BinaryResponse
- ALB-Lambda-Target-WhatisMyIP

Encabezados de varios valores

Si las solicitudes de un cliente o las respuestas de una función Lambda contienen encabezados con varios valores o contienen el mismo encabezado varias veces, puede habilitar la compatibilidad con la sintaxis de encabezados de varios valores. Después de habilitar los encabezados con varios valores, los encabezados de solicitud y respuesta intercambiados entre el balanceador de carga y la función Lambda usan matrices. De lo contrario, el balanceador de carga utiliza el último valor que recibe.

Contenido

Solicitudes con encabezados de varios valores

Los nombres de los campos utilizados para los encabezados y los parámetros de cadena de consulta difieren en función de su habilita los encabezados de varios valores para el grupo de destino.

La siguiente solicitud de ejemplo tiene dos parámetros de consulta con la misma clave:

```
http://www.example.com?&myKey=val1&myKey=val2
```

Con el formato predeterminado, el balanceador de carga utiliza el último valor enviado por el cliente y le envía un evento que incluye parámetros de cadena de consulta que utilizan `queryStringParameters`. Por ejemplo:

```
"queryStringParameters": { "myKey": "val2"},
```

Si habilita los encabezados de varios valores, el balanceador de carga utiliza ambos valores de clave enviados por el cliente y le envía un evento que incluye parámetros de cadena de consulta que utilizan `multiValueQueryStringParameters`. Por ejemplo:

```
"multiValueQueryStringParameters": { "myKey": ["val1", "val2"] },
```

De forma similar, suponga que el cliente envía una solicitud con dos cookies en el encabezado:

```
"cookie": "name1=value1",
"cookie": "name2=value2",
```

Con el formato predeterminado, el balanceador de carga utiliza la última cookie enviada por el cliente y le envía un evento que incluye encabezados que utilizan `headers`. Por ejemplo:

```
"headers": {
    "cookie": "name2=value2",
    ...
```

```
},
```

Si habilita encabezados de varios valores, el balanceador de carga utiliza ambas cookies enviadas por el cliente y le envía un evento que incluye encabezados que utilizan `multiValueHeaders`. Por ejemplo:

```
"multiValueHeaders": {
    "cookie": ["name1=value1", "name2=value2"],
    ...
},
```

Respuestas con encabezados de varios valores

Los nombres de los campos utilizados para los encabezados difieren en función de si habilita encabezados de varios valores para el grupo de destino. Debe utilizar `multiValueHeaders` si ha habilitado encabezados de varios valores y `headers` de lo contrario.

Con el formato predeterminado, puede especificar una única cookie:

```
{
  "headers": {
      "Set-cookie": "cookie-name=cookie-value;Domain=myweb.com;Secure;HttpOnly",
      "Content-Type": "application/json"
  },
}
```

Con los encabezados de varios valores, puede especificar varias cookies tal y como se indica a continuación:

```
{
  "multiValueHeaders": {
      "Set-cookie": ["cookie-name=cookie-value;Domain=myweb.com;Secure;HttpOnly","cookie-
name=cookie-value;Expires=May 8, 2019"],
      "Content-Type": ["application/json"]
  },
}
```

Habilitar encabezados de varios valores

Puede habilitar o deshabilitar los encabezados de varios valores para un grupo de destino con el tipo de destino `lambda`.

Para habilitar los encabezados de varios valores con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.
4. En la pestaña Description (Descripción), elija Edit attributes (Editar atributos).
5. En Multi value headers (Encabezados de varios valores), seleccione Enable (Habilitar).
6. Seleccione Save.

Para habilitar los encabezados de varios valores con la AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `lambda.multi_value_headers.enabled`.

Deshabilitar las comprobaciones de estado

De forma predeterminada, las comprobaciones de estado están deshabilitadas para los grupos de destino de tipo `lambda`. Puede habilitar las comprobaciones de estado a fin de implementar la conmutación por error a nivel de DNS con Amazon Route 53. La función Lambda puede comprobar el estado de un servicio posterior antes de responder a la solicitud de comprobación de estado. Si la respuesta de la función Lambda indica un error en la comprobación de estado, este error se pasa a Route 53. Puede configurar Route 53 para que realice una conmutación por error a una pila de aplicaciones de reserva.

Se aplican cargos por las comprobaciones de estado, al igual que con las invocaciones a funciones Lambda.

A continuación, se muestra el formato del evento de comprobación de estado enviado a la función Lambda. Para comprobar si un evento es un evento de comprobación de estado, compruebe el valor del campo agente-usuario. El agente de usuario de las comprobaciones de estado es `ELB-HealthChecker/2.0`.

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-target-
group/6d0ecf831eec9f09"
        }
    },
    "httpMethod": "GET",
    "path": "/",
    "queryStringParameters": {},
    "headers": {
        "user-agent": "ELB-HealthChecker/2.0"
    },
    "body": "",
    "isBase64Encoded": false
}
```

Para habilitar las comprobaciones de estado para un grupo de destino

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.
4. En la pestaña Health checks (Comprobaciones de estado), elija Edit health check (Editar comprobación de estado).
5. En Health check (Comprobación de estado), seleccione Enable (Habilitar).
6. Seleccione Save.

Para habilitar las comprobaciones de estado para un grupo de destino mediante la AWS CLI

Utilice el comando modify-target-group-attributes con la opción `--health-check-enabled`.

Anular el registro de la función Lambda

Si ya no necesita enviar tráfico a la función Lambda, puede anular su registro. Después de anular el registro de una función Lambda, las solicitudes en tránsito producirán errores HTTP 5XX.

Para sustituir una función Lambda, le recomendamos que cree un nuevo grupo de destino, registre la nueva función en el nuevo grupo de destino y actualice las reglas del agente de escucha para que utilicen el nuevo grupo de destino en lugar del existente.

Para anular el registro de la función Lambda

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.
4. En la pestaña Targets (Destinos), seleccione Deregister (Anular registro).
5. Elija Deregister.

Para anular el registro de la función Lambda mediante la AWS CLI

Use el comando deregister-targets.

Etiquetas para su grupo de destino

Las etiquetas le ayudan a clasificar los grupos de destino de diversas maneras; por ejemplo, según su finalidad, propietario o entorno.

Puede agregar varias etiquetas a cada grupo de destino. Las claves de las etiquetas deben ser únicas en cada grupo de destino. Si agrega una etiqueta con una clave que ya está asociada al grupo de destino, se actualizará el valor de esa etiqueta.

Cuando ya no necesite una etiqueta, puede quitarla.

Restricciones

- Cantidad máxima de etiquetas por recurso: 50.
- Longitud máxima de la clave: 127 caracteres Unicode.
- Longitud máxima del valor: 255 caracteres Unicode.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios anteriores o posteriores.
- No utilice el prefijo `aws:` en los nombres o valores de las etiquetas, porque está reservado para uso de AWS. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

Para actualizar las etiquetas de un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino.
4. En la pestaña Tags (Etiquetas), elija Add/Edit Tags (Añadir o editar etiquetas) y realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, modifique los valores Key y Value.
   b. Para agregar una nueva etiqueta, elija Create Tag (Crear etiqueta) y escriba los valores para Key (Clave) y Value (Valor).
   c. Para eliminar una etiqueta, elija el icono de eliminación (X) situado junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Save.

Para actualizar las etiquetas de un grupo de destino mediante la AWS CLI

Utilice los comandos add-tags y remove-tags.

Eliminación de un grupo de destino

Si en un grupo de destino las acciones no hacen referencia a él, puede eliminarlo. La eliminación de un grupo de destino no afecta a los destinos registrados en él. Si ya no necesita una instancia EC2 registrada, puede detenerla o terminarla.

Para eliminar un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en LOAD BALANCING (BALANCEO DE CARGA), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino y elija Actions, Delete.
4. Cuando se le pida confirmación, elija Yes.

Para eliminar un grupo de destino desde la AWS CLI

Utilice el comando delete-target-group.

Monitorización de los Application Load Balancers

Puede utilizar las siguientes características para monitorizar los balanceadores de carga, analizar los patrones de tráfico y solucionar los problemas de los balanceadores de carga y de los destinos.

Métricas de CloudWatch

Puede utilizar Amazon CloudWatch para recuperar estadísticas sobre los puntos de datos de los balanceadores de carga y destinos en conjuntos ordenados de datos de serie temporal denominados métricas. Puede utilizar estas métricas para comprobar que el sistema funcione de acuerdo con lo esperado. Para obtener más información, consulte Métricas de CloudWatch para el Application Load Balancer (p. 79).

Logs de acceso

Puede utilizar los logs de acceso para capturar información detallada sobre las solicitudes realizadas al balanceador de carga y almacenarla en archivos log en Amazon S3. Puede utilizar estos logs de acceso para analizar los patrones de tráfico y solucionar problemas en los destinos. Para obtener más información, consulte Logs de acceso del Application Load Balancer (p. 91).

Rastreo de solicitudes

Puede utilizar el rastreo de solicitudes para realizar un seguimiento de las solicitudes HTTP. El balanceador de carga agrega un encabezado con un identificador de rastreo a cada solicitud que recibe. Para obtener más información, consulte Rastreo de solicitudes en el Balanceador de carga de aplicaciones (p. 104).

Logs de CloudTrail

Puede utilizar AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a la API de Elastic Load Balancing y almacenarlos en archivos de logs en Amazon S3. Puede utilizar estos logs de CloudTrail registros para determinar qué llamadas se han efectuado, la dirección IP de origen de la que procede la llamada, quién la ha realizado, cuándo, etc. Para obtener más información, consulte Registrar llamadas a la API del Balanceador de carga de aplicaciones a través de AWS CloudTrail (p. 106).

Métricas de CloudWatch para el Application Load Balancer

Elastic Load Balancing publica los puntos de datos en Amazon CloudWatch de los balanceadores de carga y los destinos. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos en un conjunto ordenado de datos de series temporales que reciben el nombre de métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Por ejemplo, puede monitorizar el número total de destinos en buen estado de un balanceador de carga en un periodo especificado. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Elastic Load Balancing únicamente notifica las métricas a CloudWatch mientras las solicitudes están fluyendo a través del balanceador de carga. Si hay solicitudes fluyendo a través del balanceador de carga, Elastic Load Balancing mide y envía las métricas a intervalos de 60 segundos. Si no fluye ninguna solicitud a través del balanceador de carga o no hay datos para una métrica, esta no se notifica.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Contenido

Métricas de Balanceador de carga de aplicaciones

El espacio de nombres `AWS/ApplicationELB` incluye las siguientes métricas para los balanceadores de carga.

Métrica	Descripción
`ActiveConnectionCount`	El número total de conexiones TCP simultáneas activas desde los clientes al balanceador de carga y desde el balanceador de carga a los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`
`ClientTLSNegotiationErrorCount`	El número de conexiones TLS iniciadas por el cliente que no establecieron una sesión con el balanceador de carga. Las causas posibles incluyen una discrepancia de los cifrados o los protocolos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`ConsumedLCUs`	El número de unidades de capacidad del balanceador de carga (LCU) usadas por el balanceador de carga. Se paga por el número de LCU usadas a la hora. Para obtener más información, consulte los precios de Elastic Load Balancing. Criterios del informe: Se informa siempre Estadísticas: Todas Dimensiones • `LoadBalancer`

Métrica	Descripción
`HTTP_Fixed_Response_Count`	El número de acciones de respuesta fija que se han realizado correctamente. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer`
`HTTP_Redirect_Count`	El número de acciones de redireccionamiento que se han realizado correctamente. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer`
`HTTP_Redirect_Url_Limit_Exceeded_Count`	El número de acciones de redireccionamiento que no se han podido completar porque la URL en el encabezado de la ubicación de respuesta es mayor que 8 K. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer`
`HTTPCode_ELB_3XX_Count`	El número de códigos de redireccionamiento de HTTP 3XX que proceden del balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer`

Métrica	Descripción
`HTTPCode_ELB_4XX_Count`	El número de códigos de error del cliente HTTP 4XX que proceden del balanceador de carga. Los errores del cliente se generan cuando las solicitudes no tienen el formato correcto o están incompletas. El destino no recibe estas solicitudes. Este número no incluye los códigos de respuesta generados por los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Tenga en cuenta que `Minimum`, `Maximum` y `Average` devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`HTTPCode_ELB_5XX_Count`	El número de códigos de error del servidor HTTP 5XX que proceden del balanceador de carga. Este número no incluye los códigos de respuesta generados por los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Tenga en cuenta que `Minimum`, `Maximum` y `Average` devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`HTTPCode_ELB_500_Count`	El número de códigos de error del servidor HTTP 500 que proceden del balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`.
`HTTPCode_ELB_502_Count`	El número de códigos de error del servidor HTTP 502 que proceden del balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`.
`HTTPCode_ELB_503_Count`	El número de códigos de error del servidor HTTP 503 que proceden del balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`.
`HTTPCode_ELB_504_Count`	El número de códigos de error del servidor HTTP 504 que proceden del balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`.

Métrica	Descripción
`IPv6ProcessedBytes`	El número total de bytes procesados por el balanceador de carga a través de IPv6. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`
`IPv6RequestCount`	El número de solicitudes IPv6 recibidas por el balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Tenga en cuenta que `Minimum`, `Maximum` y `Average` devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`
`NewConnectionCount`	El número total de conexiones TCP nuevas establecidas desde los clientes al balanceador de carga y desde el balanceador de carga a los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`
`ProcessedBytes`	El número total de bytes procesados por el balanceador de carga a través de IPv4 e IPv6. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`

Métrica	Descripción
`RejectedConnectionCount`	El número de conexiones que se rechazaron porque el balanceador de carga alcanzó el número máximo de conexiones. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer`
`RequestCount`	El número de solicitudes que se procesaron por IPv4 e IPv6. Este número solo incluye las solicitudes con una respuesta generadas por un destino del balanceador de carga. Criterios del informe: Se informa siempre Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`
`RuleEvaluations`	El número de reglas procesadas por el balanceador de carga dado el número medio de solicitudes por hora. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`

El espacio de nombres `AWS/ApplicationELB` incluye las siguientes métricas para los destinos.

Métrica	Descripción
`HealthyHostCount`	El número de destinos que se considera que están en buen estado. Reporting criteria (Criterios del informe): indica si se han activado las comprobaciones de estado Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. Dimensiones • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`

Métrica	Descripción
`HTTPCode_Target_2XX_Count`, `HTTPCode_Target_3XX_Count`, `HTTPCode_Target_4XX_Count`, `HTTPCode_Target_5XX_Count`	El número de códigos de respuesta HTTP generados por los destinos. Este número no incluye los códigos de respuesta generados por el balanceador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Tenga en cuenta que `Minimum`, `Maximum` y `Average` devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`
`NonStickyRequestCount`	El número de solicitudes para las que balanceador de carga eligió un nuevo destino porque no pudo utilizar una sesión sticky existente. Por ejemplo, la solicitud era la primera solicitud de un nuevo cliente y no había ninguna cookie de persistencia, se presentó una cookie de persistencia pero no se especificó un destino registrado con este grupo de destino, la cookie de persistencia tenía un formato incorrecto o había caducado o un error interno impidió que el balanceador de carga leyese la cookie de persistencia. Reporting criteria (Criterios del informe): la persistencia está habilitada en el grupo de destino. Estadísticas: la única estadística relevante es `Sum`.
`RequestCountPerTarget`	El número medio de solicitudes recibidas por cada destino de un grupo de destino. Debe especificar el grupo de destino mediante la dimensión `TargetGroup`. Esta métrica no se aplica si el destino es una función Lambda. Criterios del informe: Se informa siempre Estadísticas: la única estadística válida es `Sum`. Tenga que cuenta que representa la media, no la suma. Dimensiones • `TargetGroup` • `TargetGroup`, `LoadBalancer`

Métrica	Descripción
`TargetConnectionErrorCount`	El número de conexiones que no se establecieron correctamente entre el balanceador de carga y el destino. Esta métrica no se aplica si el destino es una función Lambda. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`
`TargetResponseTime`	El tiempo transcurrido, en segundos, desde que la solicitud abandona el balanceador de carga hasta que se recibe una respuesta del destino. Esto equivale al campo `target_processing_time` de los logs de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles). Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`
`TargetTLSNegotiationErrorCount`	El número de conexiones TLS iniciadas por el balanceador de carga que no establecieron una sesión con el destino. Las causas posibles incluyen una discrepancia de los cifrados o los protocolos. Esta métrica no se aplica si el destino es una función Lambda. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone`, `LoadBalancer` • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`

Métrica	Descripción
`UnHealthyHostCount`	El número de destinos que se considera que no están en buen estado. Reporting criteria (Criterios del informe): indica si se han activado las comprobaciones de estado Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. Dimensiones • `TargetGroup`, `LoadBalancer` • `TargetGroup`, `AvailabilityZone`, `LoadBalancer`

El espacio de nombres `AWS/ApplicationELB` incluye las siguientes métricas para las funciones Lambda que se registran como destinos.

Métrica	Descripción
`LambdaInternalError`	El número de solicitudes dirigidas a una función Lambda que produjeron un error debido a un problema con el balanceador de carga o AWS Lambda. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `TargetGroup`
`LambdaTargetProcessedBytes`	El número total de bytes procesados por el balanceador de carga para las solicitudes y las respuestas de una función Lambda. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `LoadBalancer`
`LambdaUserError`	El número de solicitudes dirigidas a una función Lambda que produjeron un error debido a un problema con la función Lambda. Por ejemplo, el balanceador de carga no tenía permiso para invocar la función, el balanceador de carga recibió JSON desde la función que no tenía el formato correcto o en el que faltaban campos, o el tamaño del cuerpo de la solicitud o respuesta superaba el tamaño máximo de 1 MB. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `TargetGroup`

El espacio de nombres `AWS/ApplicationELB` incluye las siguientes métricas para la autenticación de usuarios.

Métrica	Descripción
`ELBAuthError`	El número de autenticaciones de usuario que no se han podido completar porque se ha configurado de manera incorrecta una acción de autenticación o el balanceador de carga no ha podido establecer una conexión con el IdP o no ha podido completar el flujo de autenticación debido a un error interno. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `LoadBalancer`
`ELBAuthFailure`	El número de autenticaciones de usuario que no se han podido completar debido a que el IdP ha denegado el acceso al usuario o se ha utilizado varias veces un código de autorización. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `LoadBalancer`
`ELBAuthLatency`	El tiempo transcurrido, en milisegundos, en solicitar al IdP el token de ID y la información del usuario. Si se produce un error en una o en varias de estas operaciones, este es el tiempo transcurrido hasta el error. Criterios del informe: hay un valor distinto de cero Estadísticas: todas las estadísticas son relevantes. Dimensiones: `LoadBalancer`
`ELBAuthRefreshTokenSuccess`	El número de veces que el balanceador de carga actualizó correctamente las notificaciones de usuario con un token de actualización proporcionado por el proveedor de identidad. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `LoadBalancer`
`ELBAuthSuccess`	El número de acciones de autenticación que se han realizado correctamente. Esta métrica se incrementa al final del flujo de trabajo de autenticación, después de que el balanceador de carga haya recuperado las notificaciones de usuario del IdP. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones: `LoadBalancer`
`ELBAuthUserClaimsSizeExceeded`	El número de veces que un proveedor de identidad devolvió las notificaciones de usuario con un tamaño superior a 11 K.

Métrica	Descripción
	Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones: `LoadBalancer`

Dimensiones de métricas de Application Load Balancers

Para filtrar las métricas de su Balanceador de carga de aplicaciones, use las siguientes dimensiones.

Dimensión	Descripción
`AvailabilityZone`	Filtra los datos de métricas por zona de disponibilidad.
`LoadBalancer`	Filtra los datos de métricas por balanceador de carga. Especifique el balanceador de carga del modo siguiente: app/nombre-balanceador-carga/1234567890123456 (la última parte del ARN del balanceador de carga).
`TargetGroup`	Filtra los datos de métricas por grupo de destino. Especifique el grupo de destino del modo siguiente: targetgroup/nombre-grupo-destino/1234567890123456 (la última parte del ARN del grupo de destino).

Estadísticas de las métricas de Balanceador de carga de aplicaciones

CloudWatch proporciona estadísticas en función de los puntos de datos de las métricas publicadas por Elastic Load Balancing. Las estadísticas son agregaciones de los datos de las métricas correspondientes al periodo especificado. Cuando se solicitan estadísticas, el flujo de datos devuelto se identifica mediante el nombre de la métrica y su dimensión. Una dimensión es un par de nombre-valor que identifica una métrica de forma inequívoca. Por ejemplo, puede solicitar estadísticas para todas las instancias EC2 en buen estado que se encuentran tras un balanceador de carga lanzado en una zona de disponibilidad específica.

Las estadísticas `Minimum` y `Maximum` reflejan el mínimo y el máximo registrados en los nodos individuales del balanceador de carga. Por ejemplo, supongamos que hay dos nodos del balanceador de carga. Uno tiene la métrica `HealthyHostCount` con los siguientes valores: `Minimum`, 2; `Maximum`, 10; y `Average`, 6. En el otro nodo, los valores de la métrica `HealthyHostCount` son: `Minimum`, 1; `Maximum`, 5; y `Average`, 3. Por consiguiente, para el balanceador de carga en su conjunto, `Minimum` es 1, `Maximum` es 10 y `Average` es aproximadamente 4.

La estadística `Sum` es el valor de la suma para todos los nodos del balanceador de carga. Dado que las métricas incluyen varios informes por periodo, `Sum` solo se aplica a las métricas que se suman en todos los nodos de balanceador de carga.

La estadística `SampleCount` representa el número de muestras medidas. Dado que las métricas se recopilan en función de determinados intervalos de muestreo y eventos, esta estadística no suele resultar útil. Por ejemplo, para `HealthyHostCount`, `SampleCount` se basa en el número de muestras que notifica cada nodo del balanceador de carga, no en el número de hosts en buen estado.

Un percentil indica el peso relativo de un valor en un conjunto de datos. Puede especificar cualquier percentil con hasta dos decimales (por ejemplo, p95.45). Por ejemplo, el percentil 95 significa que el 95 %

de los datos está por debajo de este valor y el 5 % está por encima de él. Los percentiles se suelen utilizar para aislar anomalías. Por ejemplo, supongamos que una aplicación tarda entre 1 y 2 ms en atender la mayoría de las solicitudes desde una caché; pero que tarda 100-200 ms si la caché está vacía. El máximo refleja el caso más lento, de unos 200 ms. El promedio no indica la distribución de los datos. Los percentiles proporcionan una visión más significativa del desempeño de la aplicación. Si se utiliza el percentil 99 como disparador de Auto Scaling o alarma de CloudWatch, puede determinar que el número de solicitudes que tardan en procesarse más de 2 ms no supere el 1 %.

Visualización de las métricas de CloudWatch en el balanceador de carga

Puede ver las métricas de CloudWatch de los balanceadores de carga en la consola de Amazon EC2. Estas métricas se muestran en gráficos de monitorización. Los gráficos de monitorización muestran puntos de datos si el balanceador de carga se encuentra activo y recibiendo solicitudes.

Si lo prefiere, puede ver las métricas del balanceador de carga en la consola de CloudWatch.

Para consultar las métricas desde la consola de Amazon EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para ver las métricas filtradas por grupo de destino, haga lo siguiente:
   a. En el panel de navegación, elija Target Groups.
   b. Seleccione el grupo de destino y, a continuación, elija la pestaña Monitoring.
   c. (Opcional) Para filtrar los resultados por tiempo, seleccione un intervalo de tiempo en Showing data for.
   d. Para obtener una vista más amplia de una misma métrica, seleccione su gráfico.
3. Para ver las métricas filtradas por balanceador de carga, haga lo siguiente:
   a. En el panel de navegación, seleccione Load Balancers.
   b. Seleccione el balanceador de carga y, a continuación, elija la pestaña Monitoring.
   c. (Opcional) Para filtrar los resultados por tiempo, seleccione un intervalo de tiempo en Showing data for.
   d. Para obtener una vista más amplia de una misma métrica, seleccione su gráfico.

Para consultar las métricas desde la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics.
3. Seleccione ApplicationELB espacio de nombre.
4. (Opcional) Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.
5. (Opcional) Para filtrar por dimensión, seleccione una de las siguientes opciones:
   - Para mostrar solamente las métricas registradas para los balanceadores de carga, elija Per AppELB Metrics. Para ver las métricas de un solo balanceador de carga, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los grupos de destino, elija Per AppELB Metrics. Para ver las métricas de un solo grupo de destino, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los balanceadores de carga por zona de disponibilidad, elija Per AppELB, per AZ Metrics. Para ver las métricas de un solo balanceador de

carga, escriba su nombre en el campo de búsqueda. Para ver las métricas de una sola zona de disponibilidad, escriba su nombre en el campo de búsqueda.

- Para mostrar solamente las métricas registradas para los balanceadores de carga por zona de disponibilidad y el grupo de destino, elija Per AppELB, per AZ, per TG Metrics. Para ver las métricas de un solo balanceador de carga, escriba su nombre en el campo de búsqueda. Para ver las métricas de un solo grupo de destino, escriba su nombre en el campo de búsqueda. Para ver las métricas de una sola zona de disponibilidad, escriba su nombre en el campo de búsqueda.

Para ver métricas mediante la AWS CLI

Utilice el siguiente comando list-metrics para obtener una lista de las métricas disponibles:

```
aws cloudwatch list-metrics --namespace AWS/ApplicationELB
```

Para obtener las estadísticas de una métrica desde la AWS CLI

Utilice el siguiente comando get-metric-statistics para obtener las estadísticas de la métrica y dimensión especificadas. Tenga en cuenta que CloudWatch trata cada combinación exclusiva de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado expresamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

```
aws cloudwatch get-metric-statistics --namespace AWS/ApplicationELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=app/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2016-04-18T00:00:00Z --end-time 2016-04-21T00:00:00Z
```

A continuación, se muestra un ejemplo del resultado:

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2016-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Logs de acceso del Application Load Balancer

Elastic Load Balancing proporciona logs de acceso que capturan información detallada sobre las solicitudes enviadas al balanceador de carga. Cada log contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor. Puede utilizar estos logs de acceso para analizar los patrones de tráfico y solucionar problemas.

El registro de acceso es una característica opcional de Elastic Load Balancing que está deshabilitada de forma predeterminada. Una vez que se ha habilitado el registro de acceso del balanceador de carga,

Elastic Load Balancing captura los logs y los almacena en archivos comprimidos dentro del bucket de Amazon S3 que haya especificado. Puede deshabilitar el registro de acceso en cualquier momento.

Si habilita el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) para el bucket de S3, cada archivo de registro de acceso se cifra automáticamente antes de que se almacene en el bucket de S3 y se descifra al acceder al mismo. No es necesario que haga nada, ya que no hay diferencia en la forma de acceder a los archivos de registro cifrados o sin cifrar. Cada archivo de registro se cifra con una clave única, que a su vez se cifra con una clave maestra que se rota periódicamente. Para obtener más información, consulte Protección de los datos con el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) en la Guía para desarrolladores de Amazon Simple Storage Service.

Los logs de acceso no suponen ningún cargo adicional. Se le cobrarán los costos de almacenamiento en Amazon S3, pero no el ancho de banda que Elastic Load Balancing utilice para enviar los archivos log a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon S3.

Contenido

Archivos log de acceso

Elastic Load Balancing publica un archivo log por cada nodo del balanceador de carga cada 5 minutos. La entrega de logs presenta consistencia final. El balanceador de carga puede entregar varios logs para el mismo periodo. Esto suele ocurrir si el tráfico del sitio es elevado.

Los nombres de archivo de los logs de acceso utilizan el siguiente formato:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-balancer-id_end-time_ip-address_random-string.log.gz
```

bucket

Nombre del bucket de S3.

prefijo

El prefijo (jerarquía lógica) del bucket. Si no especifica un prefijo, los logs se colocan en el nivel raíz el bucket.

aws-account-id

El ID de la cuenta de AWS del propietario.

region

La región del balanceador de carga y del bucket de S3.

aaaa/mm/dd

La fecha de entrega del log.

load-balancer-id

ID de recurso del balanceador de carga. Si el ID de recurso contiene barras diagonales (/), estas se sustituyen por puntos (.).

end-time

La fecha y hora en que finalizó el intervalo de registro. Por ejemplo, si el valor de este campo es 20140215T2340Z, contiene las entradas correspondientes a las solicitudes realizadas entre las 23:35 y las 23:40.

ip-address

La dirección IP del nodo del balanceador de carga que controló la solicitud. Si se trata de un balanceador de carga interno, es una dirección IP privada.

random-string

Una cadena generada aleatoriamente por el sistema.

A continuación se muestra un ejemplo de nombre de un archivo log:

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2016/05/01/123456789012_elasticloadbalancing_us-east-2_my-
loadbalancer_20140215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Puede guardar los archivos de registro en un bucket durante todo el tiempo que desee, pero también puede definir reglas de ciclo de vida de Amazon S3 para archivar o eliminar archivos de registro automáticamente. Para obtener más información, consulte Administración del ciclo de vida de los objetos en la Guía para desarrolladores de Amazon Simple Storage Service.

Entradas de los logs de acceso

Elastic Load Balancing registra las solicitudes enviadas al balanceador de carga, incluidas las que no han llegado a los destinos. Por ejemplo, si un cliente envía una solicitud con un formato incorrecto o no hay ningún destino en buen estado para responder, la solicitud se registra igualmente. Tenga en cuenta que Elastic Load Balancing no registra las solicitudes de comprobación de estado.

Cada entrada de log contiene los detalles de una única solicitud (o conexión, en el caso de WebSockets) realizada al balanceador de carga. Para WebSockets, la entrada no se escribe hasta que se ha cerrado la conexión. Si la conexión actualizada no se puede establecer, la entrada será la misma que para una solicitud HTTP o HTTPS.

Important

Elastic Load Balancing registra las solicitudes en la medida en que sea posible. Recomendamos utilizar los logs de acceso para comprender la naturaleza de las solicitudes y no como una relación exhaustiva de todas las solicitudes.

Sintaxis

En la siguiente tabla se describen los campos de una entrada de log de acceso, por orden. Todos los campos están delimitados por espacios. Cuando se introducen campos nuevos, se añaden al final de la entrada de log. Debe hacer caso omiso de todos los campos inesperados situados al final de la entrada de log.

Campo	Descripción
type	Tipo de solicitud o conexión. Los valores posibles son los siguientes (haga caso omiso de todos los demás valores): • `http` — HTTP • `https` — HTTP sobre SSL/TLS

Campo	Descripción
	• `h2` — HTTP/2 sobre SSL/TLS • `ws` — WebSockets • `wss` — WebSockets sobre SSL/TLS
timestamp	Hora a la que el balanceador de carga generó una respuesta al cliente, en formato ISO 8601. Para WebSockets, indica el momento en que se cerró la conexión.
elb	ID de recurso del balanceador de carga. Al analizar entradas de log de acceso, tenga en cuenta que los ID de recursos pueden contener barras diagonales (/).
client:port	Dirección IP y puerto del cliente solicitante.
target:port	Dirección IP y puerto del destino que procesó esta solicitud. Si el cliente no envió una solicitud completa, el balanceador de carga no puede enviar la solicitud a un destino, en cuyo caso este valor se establece en -. Si el destino es una función Lambda, este valor se establece en -. Si AWS WAF bloquea la solicitud, este valor se establece en - y el valor de elb_status_code es 403.
request_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el balanceador de carga recibió la solicitud hasta que se la envió a un destino. Este valor también se establece en -1 si el balanceador de carga no consigue enviar la solicitud a un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto. Este valor también se puede establecer en -1 si el destino registrado no responde antes de que se agote el tiempo de inactividad.
target_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el balanceador de carga envió la solicitud a un destino hasta que este comenzó a enviar los encabezados de la respuesta. Este valor también se establece en -1 si el balanceador de carga no consigue enviar la solicitud a un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto. Este valor también se puede establecer en -1 si el destino registrado no responde antes de que se agote el tiempo de inactividad.

Campo	Descripción
response_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el balanceador de carga recibió el encabezado de respuesta del destino hasta que comenzó a enviar la respuesta al cliente. Esto incluye tanto el tiempo de cola en el balanceador de carga como tiempo de adquisición de la conexión entre el balanceador de carga y el cliente. Este valor también se establece en -1 si el balanceador de carga no consigue enviar la solicitud a un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto.
elb_status_code	Código de estado de la respuesta desde el balanceador de carga.
target_status_code	Código de estado de la respuesta desde el destino. Este valor se registra únicamente si se estableció una conexión con el destino y este envió una respuesta. De lo contrario, se establece en -.
received_bytes	Tamaño de la solicitud, en bytes, recibida desde el cliente (solicitante). Para las solicitudes HTTP, incluye los encabezados. Para WebSockets, se trata del número total de bytes recibidos del cliente en la conexión.
sent_bytes	Tamaño de la respuesta, en bytes, enviada al cliente (solicitante). Para las solicitudes HTTP, incluye los encabezados. Para WebSockets, se trata del número total de bytes enviados al cliente en la conexión.
"request"	La línea de solicitud del cliente entre comillas y registrada con el siguiente formato: Método HTTP + protocolo://host:puerto/uri + versión de HTTP. El balanceador de carga conserva la URL que envía el cliente, tal como está, al registrar el URI de la solicitud. No establece el tipo de contenido para el archivo de registro de acceso. Al procesar este campo, tenga en cuenta cómo envió el cliente la URL.
"user_agent"	Cadena User-Agent que identifica el cliente que originó la solicitud, entre comillas. La cadena consta de uno o varios identificadores de producto, con el formato producto[/versión]. Si la cadena tiene más de 8 KB, se trunca.
ssl_cipher	[Agente de escucha HTTPS] Cifrado SSL. Este valor se establece en - si el agente de escucha no es un agente de escucha HTTPS.
ssl_protocol	[Agente de escucha HTTPS] El protocolo SSL. Este valor se establece en - si el agente de escucha no es un agente de escucha HTTPS.
target_group_arn	Nombre de recurso de Amazon (ARN) del grupo de destino.
"trace_id"	El contenido del encabezado X-Amzn-Trace-Id, entre comillas.
"domain_name"	[Agente de escucha HTTPS] El dominio de SNI proporcionado por el cliente durante el protocolo de TLS, entre comillas. Este valor está establecido en - si el cliente no admite SNI o el dominio no coincide con un certificado y se presenta al cliente el certificado predeterminado.
"chosen_cert_arn"	[Agente de escucha HTTPS] El ARN del certificado presentado al cliente, entre comillas. Este valor se establece en `session-reused` si se reutiliza la sesión.

Campo	Descripción
matched_rule_priority	El valor de prioridad de la regla que coincide con la solicitud. Si hay una regla que coincide, este es un valor de 1 a 50 000. Si no hay ninguna regla que coincida, y se ha realizado la acción predeterminada, este valor se establece en 0. Si se produce un error durante la evaluación de reglas, se establece en -1. Para cualquier otro error, se establece en -.
request_creation_time	Hora a la que el balanceador de carga recibió la solicitud del cliente, en formato ISO 8601.
"actions_executed"	Las acciones realizadas al procesar la solicitud, entre comillas. Este valor es una lista separada por comas que puede incluir los siguientes valores posibles: `waf`, `waf-failed`, `authenticate`, `redirect`, `fixed-response` y `forward`. Si no se ha realizado ninguna acción, como en el caso de una solicitud con formato incorrecto, este valor se establece en -.
"redirect_url"	URL del destino de redirección incluida en el encabezado de ubicación de la respuesta HTTP entre comillas dobles. Si no se ejecutan acciones de redirección, este valor se establece en -.
"error_reason"	El código de motivo de error, entre comillas dobles. Si la solicitud produjo un error, este es uno de los códigos de error que se describen en Códigos de motivo de error (p. 96). Si las acciones realizadas no incluyen una acción de autenticación o el destino no es una función Lambda, este valor se establece en -.

Códigos de motivo de error

Si el balanceador de carga no puede completar una acción de autenticación, el balanceador de carga almacena uno de los siguientes códigos de motivo de error en el campo error_reason del registro de acceso. Asimismo, el balanceador de carga incrementa la métrica de CloudWatch correspondiente. Para obtener más información, consulte Autenticar a usuarios usando un Balanceador de carga de aplicaciones (p. 49).

Código	Descripción	Métrica
`AuthInvalidCookie`	La cookie de autenticación no es válida.	`ELBAuthFailure`
`AuthInvalidGrantError`	El código de concesión de autorización del punto de enlace del token no es válido.	`ELBAuthFailure`
`AuthInvalidIdToken`	El token de ID no es válido.	`ELBAuthFailure`
`AuthInvalidStateParam`	El parámetro de estado no es válido.	`ELBAuthFailure`
`AuthInvalidTokenResponse`	La respuesta desde el punto de enlace del token no es válida.	`ELBAuthFailure`
`AuthInvalidUserinfoResponse`	La respuesta desde el punto de enlace de información de usuario no es válida.	`ELBAuthFailure`
`AuthMissingCodeParam`	En la respuesta de autenticación desde el punto de enlace de autorización falta un parámetro de consulta denominado «code».	`ELBAuthFailure`

Código	Descripción	Métrica
`AuthMissingHostHeader`	En la respuesta de autenticación desde el punto de enlace de autorización falta un campo de encabezado de host.	`ELBAuthError`
`AuthMissingStateParam`	En la respuesta de autenticación desde el punto de enlace de autorización falta un parámetro de consulta denominado «state».	`ELBAuthFailure`
`AuthTokenEpRequestFailed`	Hay una respuesta de error (no 2XX) del punto de enlace del token.	`ELBAuthError`
`AuthTokenEpRequestTimeout`	El balanceador de carga no puede comunicarse con el punto de enlace del token.	`ELBAuthError`
`AuthUnhandledException`	El balnceador de carga encontró una excepción no administrada.	`ELBAuthError`
`AuthUserinfoEpRequestFailed`	Hay una respuesta de error (no 2XX) del punto de enlace de información de usuario de IdP.	`ELBAuthError`
`AuthUserinfoEpRequestTimeout`	El balanceador de carga no puede comunicarse con el punto de enlace de información de usuario de IdP.	`ELBAuthError`
`AuthUserinfoResponseSizeExceeded`	El tamaño de las reclamaciones devueltas por el IdP supera los 11K bytes.	`ELBAuthUserClaimsSizeExceeded`

Si una solicitud dirigida a una función Lambda produce un error, el balanceador de carga almacena uno de los siguientes códigos de motivo en el campo error_reason del registro de acceso. Asimismo, el balanceador de carga incrementa la métrica de CloudWatch correspondiente. Para obtener más información, consulte la acción Lambda Invoke.

Código	Descripción	Métrica
`LambdaAccessDenied`	El balanceador de carga no tenía permiso para invocar la función Lambda.	`LambdaUserError`
`LambdaConnectionTimeout`	Se agotó el tiempo de espera al intentar conectarse a Lambda.	`LambdaInternalError`
`LambdaEC2AccessDeniedException`	Amazon EC2 denegó el acceso a Lambda durante la inicialización de la función.	`LambdaUserError`
`LambdaEC2ThrottledException`	Amazon EC2 aplicó una restricción a Lambda durante la inicialización de la función.	`LambdaUserError`
`LambdaEC2UnexpectedException`	Amazon EC2 detectó una excepción inesperada durante la inicialización de la función.	`LambdaUserError`
`LambdaENILimitReachedException`	Lambda no pudo crear una interfaz de red en la VPC especificada en la configuración de la función Lambda porque se superó el límite de interfaces de red.	`LambdaUserError`
`LambdaInvalidResponse`	La respuesta de la función Lambda no tiene el formato correcto o no incluye campos obligatorios.	`LambdaUserError`

Código	Descripción	Métrica
LambdaInvalidRuntimeException	La versión especificada del runtime de Lambda no se admite.	LambdaUserError
LambdaInvalidSecurityGroupID	El ID de grupo de seguridad especificado en la configuración de la función Lambda no es válido.	LambdaUserError
LambdaInvalidSubnetIDException	El ID de subred especificado en la configuración de la función Lambda no es válido.	LambdaUserError
LambdaInvalidZipFileException	Lambda no pudo descomprimir el archivo zip de la función especificada.	LambdaUserError
LambdaKMSAccessDeniedException	Lambda no pudo descifrar las variables de entorno porque se denegó el acceso a la clave de KMS. Compruebe los permisos de KMS de la función Lambda.	LambdaUserError
LambdaKMSDisabledException	Lambda no pudo descifrar las variables de entorno, porque se deshabilitó la clave de KMS especificada. Compruebe la configuración de la clave de KMS de la función Lambda.	LambdaUserError
LambdaKMSInvalidStateException	Lambda no pudo descifrar las variables de entorno porque el estado de la clave de KMS no era válido. Compruebe la configuración de la clave de KMS de la función Lambda.	LambdaUserError
LambdaKMSNotFoundException	Lambda no pudo descifrar las variables de entorno porque no se encontró la clave de KMS. Compruebe la configuración de la clave de KMS de la función Lambda.	LambdaUserError
LambdaRequestTooLarge	El tamaño del cuerpo de la solicitud era superior a 1 MB.	LambdaUserError
LambdaResourceNotFound	No se pudo encontrar la función Lambda.	LambdaUserError
LambdaResponseTooLarge	El tamaño de la respuesta era superior a 1 MB.	LambdaUserError
LambdaServiceException	Lambda detectó un error interno.	LambdaInternalError
LambdaSubnetIPAddressLimitReachedException	Lambda no pudo configurar el acceso a la VPC de la función Lambda porque una o varias subredes no tenían direcciones IP disponibles.	LambdaUserError
LambdaThrottling	La función Lambda se rechazó porque había demasiadas solicitudes.	LambdaUserError
LambdaUnhandled	La función Lambda encontró una excepción no administrada.	LambdaUserError

Ejemplos

A continuación, se muestran ejemplos de entradas de log. Tenga en cuenta que el texto aparece en varias líneas únicamente para facilitar su lectura.

Ejemplo de entrada HTTP

A continuación se muestra un ejemplo de entrada de log para un agente de escucha HTTP (del puerto 80 al puerto 80):

```
http 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337262-36d228ad5d99923122bbe354" "-" "-"
0 2018-07-02T22:22:48.364000Z "forward" "-" "-"
```

Ejemplo de entrada HTTPS

A continuación se muestra un ejemplo de entrada de log para un agente de escucha HTTPS (del puerto 443 al puerto 80):

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-
east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-"
```

Ejemplo de entrada HTTP/2

A continuación se muestra un ejemplo de entrada de log para un flujo de HTTP/2.

```
h2 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.1.252:48160 10.0.0.66:9000 0.000 0.002 0.000 200 200 5 257
"GET https://10.0.2.105:773/ HTTP/2.0" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337327-72bd00b0343d75b906739c42" "-" "-"
1 2018-07-02T22:22:48.364000Z "redirect" "https://example.com:80/" "-"
```

Ejemplo de entrada de WebSockets

A continuación se muestra un ejemplo de entrada de log para una conexión de WebSockets.

```
ws 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:40914 10.0.1.192:8010 0.001 0.003 0.000 101 101 218 587
"GET http://10.0.0.30:80/ HTTP/1.1" "-" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-"
```

Ejemplo de entrada de WebSockets segura

A continuación se muestra un ejemplo de entrada de log para una conexión de WebSockets segura.

```
wss 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.0.140:44244 10.0.0.171:8010 0.000 0.001 0.000 101 101 218 786
"GET https://10.0.0.30:443/ HTTP/1.1" "-" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
1 2018-07-02T22:22:48.364000Z "forward" "-" "-"
```

Entradas de ejemplo de funciones Lambda

A continuación, se muestra una entrada de registro de ejemplo de una solicitud dirigida a una función Lambda que se realizó correctamente:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "-"
```

A continuación, se muestra una entrada de registro de ejemplo de una solicitud dirigida a una función Lambda que produjo un error:

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 502 - 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "LambdaInvalidResponse"
```

Permisos de buckets

Al habilitar el registro de acceso, es preciso especificar un bucket de S3 para los logs de acceso. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el balanceador de carga.
- El bucket debe tener una política que conceda permiso a Elastic Load Balancing para escribir los logs de acceso del bucket. Las políticas de bucket son colecciones de instrucciones JSON escritas en el lenguaje de la política de acceso para definir los permisos de acceso al bucket. Cada instrucción incluye información sobre un único permiso y contiene una serie de elementos.

Utilice una de las siguientes opciones para preparar un bucket de S3 para los logs de acceso.

Opciones

- Si necesita crear un bucket y tiene previsto utilizar la consola para habilitar el registro de acceso, puede ir directamente a Habilitación del registro de acceso (p. 103) y seleccionar la opción para que la consola cree el bucket y la política de bucket automáticamente.
- Si tiene que crear un bucket para los logs de acceso y utiliza la AWS CLI o una API, utilice el siguiente procedimiento para crearlo y agregarle la política de bucket manualmente.
- Si ya tiene un bucket para los logs de acceso, abra la consola de Amazon S3 de acuerdo con el paso 1 del siguiente procedimiento y, a continuación, vaya al paso 4 para añadir o actualizar la política del bucket.

Para crear un bucket de Amazon S3 con los permisos necesarios

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. [Omitir para utilizar un bucket existente] Seleccione la opción Create Bucket (Crear bucket).
3. [Omitir para utilizar un bucket existente] En el cuadro de diálogo Create a Bucket (Crear un bucket), haga lo siguiente:

    a. En Bucket Name, escriba el nombre del bucket (por ejemplo, `my-loadbalancer-logs`). Este nombre debe ser único entre todos los nombres de buckets de Amazon S3. En algunas regiones

de , es posible que haya restricciones adicionales para los nombres de los buckets. Para obtener más información, consulte Bucket Restrictions and Limitations en Guía para desarrolladores de Amazon Simple Storage Service.

b. En Region, seleccione la región donde ha creado el balanceador de carga.

c. Seleccione Create.

4. Seleccione el bucket y elija Permissions.
5. Elija Bucket Policy. Si el bucket ya tiene una política adjunta, puede agregar la instrucción necesaria a esta política.
6. Elija Policy generator. En la página AWS Policy Generator haga lo siguiente:

   a. Para Select Type of Policy, elija S3 Bucket Policy.

   b. En Effect, elija Allow.

   c. En Principal, especifique uno de los siguientes ID de cuenta de AWS para conceder a Elastic Load Balancing acceso al bucket de S3. Utilice el ID de la cuenta que corresponde a la región del balanceador de carga y del bucket.

Región	Nombre de la región	ID de la cuenta de Elastic Load Balancing
`us-east-1`	US East (N. Virginia)	127311923021
`us-east-2`	EE.UU. Este (Ohio)	033677994240
`us-west-1`	EE.UU. Oeste (Norte de California)	027434742980
`us-west-2`	EE.UU. Oeste (Oregón)	797873946194
`ca-central-1`	Canadá (Central)	985666609251
`eu-central-1`	UE (Fráncfort)	054676820928
`eu-west-1`	UE (Irlanda)	156460612806
`eu-west-2`	UE (Londres)	652711504416
`eu-west-3`	UE (París)	009996457667
`eu-north-1`	UE Estocolmo	897822967062
`ap-east-1`	Asia Pacífico (Hong Kong)	754344448648
`ap-northeast-1`	Asia Pacífico (Tokio)	582318560864
`ap-northeast-2`	Asia Pacífico (Seúl)	600734575887
`ap-northeast-3`	Asia Pacífico (Osaka-local)	383597477331
`ap-southeast-1`	Asia Pacífico (Singapur)	114774131450
`ap-southeast-2`	Asia Pacífico (Sídney)	783225319266
`ap-south-1`	Asia Pacífico (Mumbai)	718504428378

Región	Nombre de la región	ID de la cuenta de Elastic Load Balancing
`sa-east-1`	América del Sur (São Paulo)	507241528517
`us-gov-west-1*`	AWS GovCloud (US-West)	048591011584
`us-gov-east-1*`	AWS GovCloud (EE.UU. Este)	190560391635
`cn-north-1*`	China (Pekín)	638102146993
`cn-northwest-1*`	China (Ningxia)	037604701340

* Estas regiones requieren una cuenta independiente. Para obtener más información, consulte AWS GovCloud (EE.UU. Oeste) y China (Pekín).

d. En Actions (Acciones), elija `PutObject` para permitir que Elastic Load Balancing almacene objetos en el bucket de S3.

e. En Amazon Resource Name (ARN) (Nombre de recurso de Amazon [ARN]), escriba el ARN del bucket de S3 con el siguiente formato. En *`aws-account-id`*, especifique el ID de la cuenta de AWS propietaria del balanceador de carga (por ejemplo, *`123456789012`*). No especifique un carácter comodín para el ID de la cuenta, ya que esto permitiría que cualquier otra cuenta escriba registros de acceso en su bucket. Para utilizar un solo bucket para almacenar los registros de acceso de los balanceadores de carga en varias cuentas, especifique un ARN para cada cuenta en la política del bucket, utilizando el ID de cuenta de AWS correspondiente en cada ARN.

```
arn:aws:s3:::bucket/prefix/AWSLogs/aws-account-id/*
```

Tenga en cuenta que si utiliza la región `us-gov-west-1`, debe especificar `arn:aws-us-gov` en lugar de `arn:aws` en el ARN.

f. Elija Add Statement, Generate Policy. El documento de política debe ser similar a este:

```
{
  "Id": "Policy1429136655940",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1429136633762",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::my-loadbalancer-logs/my-app/AWSLogs/123456789012/
*",
      "Principal": {
        "AWS": [
          "797873946194"
        ]
      }
    }
  ]
}
```

g. Si va a crear una política de bucket nueva, copie el documento de política completo y, a continuación, elija Close.

Si va a modificar una política de bucket existente, copie la nueva instrucción del documento de política (el texto comprendido entre [y] del `Statement` elemento) y, a continuación, elija Close.

7. Vuelva al Amazon S3 consola y pegue la política en el área de texto según corresponda.
8. Seleccione Save.

Habilitación del registro de acceso

Al habilitar el registro de acceso del balanceador de carga, debe especificar el nombre del bucket de S3 donde el balanceador de carga almacenará los logs. Este bucket debe encontrarse en la misma región que el balanceador de carga. Además, debe contar con una política de bucket que conceda permiso a Elastic Load Balancing para escribir en los logs acceso del bucket. El bucket puede pertenecer a otra cuenta que no sea la propietaria del balanceador de carga.

Para habilitar el registro de acceso desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit load balancer attributes, lleve a cabo alguna de las siguientes operaciones:
   a. Elija Enable access logs.
   b. En S3 location, escriba el nombre del bucket de S3, incluido el prefijo, si lo hay (por ejemplo, `my-loadbalancer-logs/my-app`). Puede especificar el nombre de un bucket existente o el nombre del bucket nuevo. Si especifica un bucket que ya existe, asegúrese de que posee este bucket y de que ha configurado la política de bucket correspondiente.
   c. (Opcional) Si el depósito no existe, seleccione Crear esta ubicación. Debe especificar un nombre único entre todos los nombres de bucket existentes en Amazon S3 que respete las convenciones de nomenclatura de DNS. Para obtener más información, consulte Reglas para la nomenclatura de buckets en la Guía para desarrolladores de Amazon Simple Storage Service.
   d. Seleccione Save.

Para habilitar el registro de acceso desde la AWS CLI

Utilice el comando modify-load-balancer-attributes.

Para comprobar que Elastic Load Balancing ha creado un archivo de prueba en el bucket de S3

Cuando el registro de acceso está habilitado para el balanceador de carga, Elastic Load Balancing valida el bucket de S3 y crea un archivo de prueba para asegurarse de que la política de bucket especifique los permisos necesarios. Puede utilizar la consola de Amazon S3 para comprobar que se ha creado el archivo de prueba. Tenga en cuenta que el archivo de prueba no es un auténtico archivo log de acceso ni contiene ejemplos de registros.

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Para All Buckets, seleccione su bucket de S3.
3. Vaya al archivo log de prueba. La ruta debe ser la siguiente:

```
my-bucket/prefix/AWSLogs/123456789012/ELBAccessLogTestFile
```

Para administrar el bucket de S3 para los logs de acceso

Después de habilitar el registro de acceso, asegúrese de deshabilitarlo antes de eliminar el bucket con sus logs de acceso. De lo contrario, si existe un nuevo bucket con el mismo nombre y la política de bucket correspondiente se ha creado en una cuenta de AWS que no le pertenece, Elastic Load Balancing podría escribir los logs de acceso del balanceador de carga en este nuevo bucket.

Deshabilitación del registro de acceso

Puedes deshabilitar el registro de acceso del balanceador de carga en cualquier momento. Después de deshabilitar el registro de acceso, los logs de acceso permanecerán en el bucket de S3 hasta que los elimine. Para obtener más información, consulte Uso de buckets en la Guía del usuario de la consola de Amazon Simple Storage Service.

Para deshabilitar el registro de acceso desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el balanceador de carga.
4. En la pestaña Descriptions, elija Edit attributes.
5. En la página Edit load balancer attributes, borre Enable access logs.
6. Seleccione Save.

Para deshabilitar el registro de acceso desde la AWS CLI

Utilice el comando modify-load-balancer-attributes.

Procesamiento de archivos log de acceso

Los archivos log de acceso están comprimidos. Si abre los archivos en la consola de Amazon S3, se descomprimen y se muestra la información. Si descarga los archivos, debe descomprimirlos para ver la información.

Si existe una gran cantidad de demanda en el sitio web, el balanceador de carga puede generar archivos log con gigabytes de datos. Es posible que no pueda procesar semejante cantidad de datos con el procesamiento línea por línea. En tal caso, podría ser preciso utilizar herramientas de análisis que ofrezcan soluciones de procesamiento en paralelo. Por ejemplo, puede utilizar las siguientes herramientas de análisis para analizar y procesar los logs de acceso:

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Para obtener más información, consulte Consulta de registros de Application Load Balancer en la Guía del usuario de Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Rastreo de solicitudes en el Balanceador de carga de aplicaciones

Puede utilizar el rastreo de solicitudes para realizar el seguimiento de las solicitudes HTTP de los clientes a los destinos u otros servicios. Cuando el balanceador de carga recibe una solicitud de un cliente, agrega o actualiza el encabezado X-Amzn-Trace-Id antes de enviar la solicitud al destino. Todos los servicios

o aplicaciones entre el balanceador de carga y el destino también pueden agregar o actualizar este encabezado.

Si habilita los logs de acceso, se registra el contenido del encabezado X-Amzn-Trace-Id. Para obtener más información, consulte Logs de acceso del Application Load Balancer (p. 91).

Sintaxis

El encabezado X-Amzn-Trace-Id contiene campos con el siguiente formato:

```
Field=version-time-id
```

Campo

Nombre del campo. Los valores admitidos son `Root` y `Self`.

Una aplicación puede agregar campos arbitrarios para sus propios fines. El balanceador de carga conserva estos campos, pero no los utiliza.

version

Número de versión.

tiempo

Tiempo en formato de tiempo Unix, en segundos.

id

Identificador de rastreo.

Ejemplos

Si el encabezado X-Amzn-Trace-Id no está presente en una solicitud entrante, el balanceador de carga genera un encabezado con un campo `Root` y reenvía la solicitud. Por ejemplo:

```
X-Amzn-Trace-Id: Root=1-67891233-abcdef012345678912345678
```

Si el encabezado X-Amzn-Trace-Id está presente y tiene un campo `Root`, el balanceador de carga inserta un campo `Self` y reenvía la solicitud. Por ejemplo:

```
X-Amzn-Trace-Id: Self=1-67891234-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678
```

Si una aplicación agrega un encabezado con un campo `Root` y un campo personalizado, el balanceador de carga conserva ambos campos, inserta un campo `Self` y reenvía la solicitud:

```
X-Amzn-Trace-Id: Self=1-67891234-12456789abcdef012345678;Root=1-67891233-
abcdef012345678912345678;CalledFrom=app
```

Si el encabezado X-Amzn-Trace-Id está presente y tiene un campo `Self`, el balanceador de carga actualiza el valor del campo `Self`.

Limitaciones

- El balanceador de carga actualiza el encabezado cuando recibe una solicitud entrante, no cuando recibe una respuesta.

- Si los encabezados de HTTP tienen más de 7 KB, el balanceador de carga vuelve a escribir el encabezado X-Amzn-Trace-Id con un campo `Root` .
- Con WebSockets, solo puede efectuar el rastreo hasta que la solicitud de actualización se realiza correctamente.

Registrar llamadas a la API del Balanceador de carga de aplicaciones a través de AWS CloudTrail

Elastic Load Balancing está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, una función o un servicio de AWS en Elastic Load Balancing. CloudTrail captura todas las llamadas a la API de Elastic Load Balancing como eventos. Las llamadas capturadas incluyen las llamadas realizadas a las operaciones de la API de Elastic Load Balancing desde la Consola de administración de AWS y desde el código. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Elastic Load Balancing. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información que recopila CloudTrail, se puede determinar la solicitud que se envió a Elastic Load Balancing, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo la realizó y los detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la AWS CloudTrail User Guide.

Para monitorizar otras acciones del balanceador de carga, como, por ejemplo, cuándo un cliente realiza una solicitud al balanceador de carga, utilice los logs de acceso. Para obtener más información, consulte Logs de acceso del Application Load Balancer (p. 91).

Información de Elastic Load Balancing en CloudTrail

CloudTrail se habilita en una cuenta de AWS al crearla. Cuando se produce una actividad en Elastic Load Balancing, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en el Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Elastic Load Balancing, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, este se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También puede configurar otros servicios de AWS para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Elastic Load Balancing para los Application Load Balancers se registran en CloudTrail y se documentan en la Referencia de la API de Elastic Load Balancing versión 2015-12-01. Por ejemplo, las llamadas a las acciones `CreateLoadBalancer` y `DeleteLoadBalancer` generan entradas en los archivos de registro de CloudTrail.

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

- Si la solicitud se realizó con credenciales de usuario raíz o de AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de Elastic Load Balancing

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro al bucket de Amazon S3 que se especifique. Los archivos de registro de CloudTrail contienen una o varias entradas de registro. Un evento representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de log de CloudTrail no son un rastro de la pila ordenada de las llamadas a la API públicas, por lo que no aparecen en ningún orden específico.

Los archivos log incluyen los eventos de todas las llamadas a los API de AWS correspondientes a su cuenta de AWS, no solo las llamadas al API de Elastic Load Balancing. Puede localizar las llamadas a la API de Elastic Load Balancing comprobando si hay elementos `eventSource` con el valor `elasticloadbalancing.amazonaws.com`. Para ver un registro de una acción específica (por ejemplo, `CreateLoadBalancer`), compruebe la existencia de elementos `eventName` con el nombre de la acción.

El siguiente es un ejemplo de registros de CloudTrail para Elastic Load Balancing de un usuario que creó un Balanceador de carga de aplicaciones y, después, lo eliminó mediante la AWS CLI. Puede identificar la CLI mediante los elementos `userAgent`. Puede identificar las llamadas al API solicitadas mediante los `eventName`. Encontrará la información sobre el usuario (`Alice`) en el elemento `userIdentity`.

Example Ejemplo: CreateLoadBalancer

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

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

Example Ejemplo: DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Solución de problemas de Application Load Balancer

La siguiente información puede ayudarle a solucionar problemas con su Balanceador de carga de aplicaciones.

Problemas

Un destino registrado no está operativo

Si un destino está tardando más de lo previsto en pasar al estado `InService`, es posible que no esté superando las comprobaciones de estado. El destino no estará operativo hasta que supere la comprobación de estado. Para obtener más información, consulte Comprobaciones de estado de los grupos de destino (p. 64).

Examine la instancia para ver si hay algún error en las comprobaciones de estado y revise lo siguiente:

Hay un grupo de seguridad que no permite el tráfico

El grupo de seguridad asociado a una instancia debe permitir el tráfico del balanceador de carga a través del puerto de comprobación de estado y el protocolo de comprobación de estado. Puede agregar una regla a la instancia del grupo de seguridad que permita todo el tráfico procedente del grupo de seguridad del balanceador de carga. Además, el grupo de seguridad del balanceador de carga debe permitir el tráfico dirigido a las instancias.

Hay una lista de control de acceso (ACL) de red que no permite el tráfico

Las ACL de red asociadas a las subredes de las instancias deben permitir el tráfico entrante en el puerto de comprobación de estado y el tráfico saliente en los puertos efímeros (1024-65535). Las ACL de red asociadas a las subredes de los nodos del balanceador de carga deben permitir el tráfico entrante en los puertos efímeros y el tráfico saliente en los puertos de comprobación de estado y los puertos efímeros.

La ruta de ping no existe

Cree una página de destino para la comprobación de estado y especifique su ruta como la ruta de ping.

Se ha agotado el tiempo de espera de conexión

En primer lugar, asegúrese de que puede conectarse directamente al destino desde la red a través de la dirección IP privada del destino y el protocolo de comprobación de estado. Si no puede establecer la conexión, asegúrese de que la instancia no está sobrecargada y agregue más destinos al grupo si tarda demasiado en responder. Si puede establecer conexión, es posible que la página de destino no responda antes de que se agote el período de espera de la comprobación de estado. Elija una página de destino más sencilla o ajuste la configuración de la comprobación de estado.

El destino no devuelve un código de respuesta correcto

De forma predeterminada, el código de éxito es 200, pero, si lo desea, puede especificar otros códigos de éxito cuando configure las comprobaciones de estado. Confirme los códigos de éxito que el balanceador de carga está esperando y asegúrese de que la aplicación está configurada para devolver estos códigos de éxito.

Los clientes no pueden conectarse a un balanceador de carga orientado a Internet

Si el balanceador de carga no responde a las solicitudes, compruebe lo siguiente:

El balanceador de carga orientado a Internet está conectado a una subred privada

Asegúrese de que especificó las subredes públicas del balanceador de carga. Una subred pública tiene una ruta hacia el puerto de enlace a Internet de la nube virtual privada (VPC).

Hay un grupo de seguridad o una ACL de red que no permite el tráfico

Tanto el grupo de seguridad del balanceador de carga como las ACL de red de las subredes del balanceador de carga deben permitir el tráfico entrante procedente de los clientes y el tráfico saliente dirigido a los clientes en los puertos de escucha.

El balanceador de carga envía solicitudes a destinos que no tienen un estado correcto

Si al menos uno de los destinos de un grupo de destino está en buen estado, el balanceador de carga solamente envía las solicitudes a los destinos que tengan un estado correcto. Si un grupo de destino contiene únicamente destinos que no están en buen estado, el balanceador de carga envía las solicitudes a estos destinos.

El balanceador de carga genera un error HTTP

El balanceador de carga genera los siguientes errores HTTP. El balanceador de carga envía el código HTTP al cliente, guarda la solicitud en el log de acceso e incrementa la métrica `HTTPCode_ELB_4XX_Count` o `HTTPCode_ELB_5XX_Count`.

Errores

- HTTP 400: Solicitud errónea (p. 111)
- HTTP 401: No autorizado (p. 111)
- HTTP 403: Prohibido (p. 111)
- HTTP 408: Request Timeout (p. 111)
- HTTP 413: carga demasiado grande (p. 111)
- HTTP 414: URI demasiado largo (p. 111)
- HTTP 460 (p. 111)
- HTTP 463 (p. 112)
- HTTP 500: Error interno del servidor (p. 112)

HTTP 400: Solicitud errónea

Causas posibles:

- El cliente envió una solicitud incorrecta que no se ajusta a la especificación de HTTP.
- El cliente utilizó el método HTTP CONNECT, pero Application Load Balancers no admite este método.
- El encabezado de la solicitud supera los 16 K por línea de solicitud, los 16 K por línea de encabezado o los 64 K en el conjunto del encabezado.

HTTP 401: No autorizado

Ha configurado una regla de agente de escucha para autenticar a los usuarios. Configuró `OnUnauthenticatedRequest` para denegar el acceso a los usuarios no autenticados o el IdP denegó el acceso.

HTTP 403: Prohibido

Configuró una lista de control de acceso web (ACL web) de AWS WAF para monitorear las solicitudes a su Balanceador de carga de aplicaciones y esta bloqueó una solicitud.

HTTP 408: Request Timeout

El cliente no envió datos antes de que transcurriera el período de tiempo de espera de inactividad. El envío de una instrucción keep-alive TCP no invalida este tiempo de espera. Envíe al menos 1 byte de datos antes de que finalice el periodo de tiempo de espera de inactividad. Aumente la duración del periodo de tiempo de espera de inactividad según sea necesario.

HTTP 413: carga demasiado grande

El destino es una función Lambda y el cuerpo de la solicitud supera 1 MB.

HTTP 414: URI demasiado largo

La URL de la solicitud o los parámetros de la cadena de consulta son demasiado largos.

HTTP 460

El balanceador de carga recibió una solicitud de un cliente, pero el cliente cerró la conexión con el balanceador de carga antes de que transcurriera el período de inactividad.

Compruebe si el período de inactividad del cliente es mayor que el período de inactividad del balanceador de carga. Asegúrese de que el destino proporciona una respuesta al cliente antes de que se agote el tiempo de inactividad del cliente. Si el cliente lo permite, también puede aumentar el tiempo de espera del cliente para que coincida con el período de inactividad del balanceador de carga.

HTTP 463

El balanceador de carga recibió un encabezado de solicitud X-Forwarded-For con más de 30 direcciones IP.

HTTP 500: Error interno del servidor

Causas posibles:

- Configuró una lista de control de acceso web (ACL web) AWS WAF y se ha producido un error al ejecutar las reglas de ACL web.
- Ha configurado una regla del agente de escucha para autenticar a los usuarios, pero se cumple alguna de las condiciones siguientes:
  - El balanceador de carga no puede comunicarse con el punto de enlace del token de IdP o el punto de enlace de información de usuario de IdP. Verifique que los grupos de seguridad de su balanceador de carga y las ACL de red de su VPC permiten el acceso saliente a estos puntos de enlace. Compruebe que la VPC tiene acceso a Internet. Si hay un balanceador de carga interno, utilice una gateway NAT para permitirle que obtenga acceso a Internet.
  - El tamaño de las notificaciones devueltas por el IdP supera el tamaño máximo admitido por el balanceador de carga.
  - Un cliente ha enviado una solicitud HTTP/1.0 sin encabezado de host y el balanceador de carga no pudo generar una URL de redirección.
  - Un cliente ha enviado una solicitud sin un protocolo HTTP y el balanceador de carga no pudo generar una URL de redirección.
  - El ámbito de la solicitud no devuelve un token de ID.

HTTP 501: no implementado

El balanceador de carga recibió un encabezado Transfer-Encoding con un valor no admitido. Los valores admitidos para Transfer-Encoding son `chunked` e `identity`. Como alternativa, puede utilizar el encabezado Content-Encoding.

HTTP 502: Bad Gateway

Causas posibles:

- El balanceador de carga recibió un TCP RST desde el destino cuando intentó establecer una conexión.
- El balanceador de carga recibió una respuesta inesperada del destino, como, por ejemplo, "ICMP Destination unreachable (Host unreachable) (Destino de ICMP inaccesible (Host de destino inaccesible))", al intentar establecer una conexión. Compruebe si se permite el tráfico desde las subredes del balanceador de carga a los destinos del puerto de destino.
- El destino cerró las conexiones con un TCP RST o un TCP FIN mientras que el balanceador de carga tenía una solicitud pendiente en el destino. Compruebe si la duración de keep-alive del destino es inferior al valor del tiempo de inactividad del balanceador de carga.
- La respuesta del destino es incorrecta o contiene encabezados HTTP que no son válidos.
- El balanceador de carga ha detectado un error de protocolo SSL o de tiempo de espera del protocolo SSL (10 segundos) al conectarse a un destino.
- El período de retardo de anulación del registro para una solicitud que se maneja mediante un objetivo cuyo registro se ha anulado. Aumente el periodo de retraso de manera que las operaciones largas puedan completarse.
- El destino es una función Lambda y el cuerpo de la respuesta supera 1 MB.

- El destino es una función Lambda que no respondió antes de que se agotara el tiempo de espera configurado.

HTTP 503: Service Unavailable

Los grupos de destino del balanceador de carga no tienen destinos registrados.

HTTP 504: Gateway Timeout

Causas posibles:

- El balanceador de carga ha establecido una conexión con el destino antes de que se agotara el tiempo de espera de conexión (10 segundos).
- El balanceador de carga estableció una conexión con el destino, pero el destino no respondió antes de que transcurriera el período de inactividad.
- La ACL de red de la subred no permite el tráfico desde los destinos hasta los nodos del balanceador de carga en los puertos efímeros (1024-65535).
- El destino devuelve un encabezado de longitud de contenido que es mayor que el cuerpo de la entidad. El balanceador de carga agotó el tiempo de espera con los bytes restantes.
- El destino es una función Lambda que no respondió antes de que se agotara el tiempo de espera máximo posible configurado.

HTTP 561: No autorizado

Configuró una regla de agente de escucha para autenticar a los usuarios, pero el IdP devolvió un código de error al autenticar al usuario.

Hay un destino que genera un error HTTP

El balanceador de carga reenvía respuestas HTTP válidas desde los destinos al cliente, incluidos los errores HTTP. Los errores HTTP generados por un destino se registran en las métricas `HTTPCode_Target_4XX_Count` y `HTTPCode_Target_5XX_Count`.

Límites para sus Application Load Balancers

Para conocer los límites actuales de los Application Load Balancers, utilice la página Limits (Límites) de la consola de Amazon EC2 o el comando describe-account-limits (AWS CLI). Para solicitar un aumento de los límites, utilice el formulario Límites de Elastic Load Balancing.

La cuenta de AWS presenta los siguientes límites en relación con Application Load Balancers:

Límites regionales

- Balanceadores de carga por región: 20
- Grupos de destino por región: 3000

Límites del balanceador de carga

- Agentes de escucha por balanceador de carga: 50
- Destinos por balanceador de carga: 1000
- Subredes por zona de disponibilidad por balanceador de carga: 1
- Grupos de seguridad por balanceador de carga: 5
- Reglas (sin contar las predeterminadas) por balanceador de carga: 100
- Certificados por balanceador de carga (sin contar los predeterminados): 25
- Número de veces que se puede registrar un destino por balanceador de carga: 100

Límites de grupos de destino

- Balanceadores de carga por grupo de destino: 1
- Destinos por grupo de destino (instancias o direcciones IP): 1000
- Destinos por grupo de destino (funciones Lambda): 1

Límites de reglas

- Evaluaciones de coincidencia por regla: 5
- Comodines por regla: 5
- Acciones por regla: 2 (una acción de autenticación opcional y una acción obligatoria)

Historial de revisión de los Application Load Balancers

En la tabla siguiente se describen las versiones de Application Load Balancers.

Característica	Descripción	Fecha
Direccionamiento de solicitudes avanzado	Esta versión amplía el soporte existente para direccionamiento basado en rutas y encabezado de host añadiendo condiciones a las reglas de agente de escucha basadas en métodos y encabezados HTTP estándar y personalizados, parámetros de consulta y direcciones IP de origen. Para obtener más información, consulte Tipos de condición de las reglas (p. 33).	27 de marzo de 2019
Funciones Lambda como destino	Esta versión añade compatibilidad para registrar funciones Lambda como destino. Para obtener más información, consulte Funciones Lambda como destinos (p. 71).	29 de noviembre de 2018
Acciones de respuesta fija	Esta versión incorpora la compatibilidad con el balanceador de carga para devolver una respuesta HTTP personalizada. Para obtener más información, consulte Acciones de respuesta fija (p. 30).	25 de julio de 2018
Acciones de redirección	Esta versión incorpora la compatibilidad con el balanceador de carga para redirigir las solicitudes a una URL diferente. Para obtener más información, consulte Acciones de redirección (p. 31).	25 de julio de 2018
Políticas de seguridad para FS y TLS 1.2	En esta versión, se han añadido políticas de seguridad para Forward Secrecy (FS) y TLS 1.2. Para obtener más información, consulte Políticas de seguridad (p. 40).	6 de junio de 2018
Soporte de autenticación	Esta versión añade soporte para que el balanceador de carga pueda autenticar a los usuarios	30 de mayo de 2018

Característica	Descripción	Fecha
	de sus aplicaciones utilizando sus identidades corporativas o sociales antes de las solicitudes de direccionamiento. Para obtener más información, consulte Autenticar a usuarios usando un Balanceador de carga de aplicaciones (p. 49).	
Modo de inicio lento	Esta versión añade soporte para el modo de inicio lento, que aumenta gradualmente la cuota de solicitudes que el balanceador de carga envía a un destino recién registrado mientras se calienta. Para obtener más información, consulte Modo de inicio lento (p. 60).	24 de marzo de 2018
Permisos de nivel de recursos	Esta versión añade soporte para permisos en el nivel de recursos y claves de condición de etiquetado. Para obtener más información, consulte Autenticación y control de acceso en la Guía del usuario de Elastic Load Balancing.	10 de mayo de 2018
Compatibilidad con SNI	Esta versión incorpora soporte para Indicación de nombre de servidor (SNI). Para obtener más información, consulte Certificados SSL (p. 38).	10 de octubre de 2017
Direcciones IP como destinos	Esta versión añade soporte para registrar direcciones IP como destinos. Para obtener más información, consulte Tipo de destino (p. 58).	31 de agosto de 2017
Direccionamiento basado en host	Esta versión añade soporte para las solicitudes de direccionamiento basadas en los nombres de host del encabezado de host. Para obtener más información, consulte Condiciones de host (p. 34).	5 de abril de 2017
Políticas de seguridad para TLS 1.1 y 1.2 TLS	En esta versión, se han añadido las políticas de seguridad de TLS 1.1 y TLS 1.2. Para obtener más información, consulte Políticas de seguridad (p. 40).	6 de febrero de 2017

Característica	Descripción	Fecha
Compatibilidad con IPv6	En esta versión se agrega compatibilidad con las direcciones IPv6. Para obtener más información, consulte Tipo de dirección IP (p. 18).	25 de enero de 2017
Rastreo de solicitudes	En esta versión se agrega compatibilidad con el rastreo de solicitudes. Para obtener más información, consulte Rastreo de solicitudes en el Balanceador de carga de aplicaciones (p. 104).	22 de noviembre de 2016
Compatibilidad con percentiles para la métrica TargetResponseTime	En esta versión se agrega compatibilidad con las nuevas estadísticas de percentiles que Amazon CloudWatch admite. Para obtener más información, consulte Estadísticas de las métricas de Balanceador de carga de aplicaciones (p. 89).	17 de noviembre de 2016
Nuevo tipo de balanceador de carga	En esta versión de Elastic Load Balancing, se han incluido los Application Load Balancers.	11 de agosto de 2016